Acuitas User's Guide

Updated: March 2019

Inside ...

- Getting Started
- Topology
- Configuration
- Fault
- Performance
- VNF Manager
- Security
- Tools
- CUPS Manager
- Affirmed Open Workflow
- Configuration Navigator
- Network Element
- Interfacing with Northbound Interfaces
- Key Performance Indicators (KPIs) Metrics

Affirmed Networks Inc.
35 Nagog Park
Acton, MA 01720
USA
Tel: +1-978-268-0800
www.affirmednetworks.com

Acuitas User's Guide, Release 9.2.0.0
Part Number: 550-01043 Revision: A

Copyright© 2019 Affirmed Networks, Inc. All Rights Reserved.

AFFIRMED & DESIGN®, ACUITAS SERVICE MANAGEMENT SYSTEM®, AFFIRMED NETWORKS MOBILE CONTENT CLOUD™, AFFIRMED OPEN WORKFLOW™, AFFIRMED MOBILE CONTENT CLOUD™ and other trademarks and designs are the registered or unregistered trademarks of Affirmed Networks, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are the property of their respective owners. The Affirmed Networks, Inc. trademarks may not be used in connection with any product or service that is not Affirmed Networks' in any manner that is likely to cause confusion among customers or in any manner that disparages or discredits Affirmed Networks, Inc.

This document contains information that is the property of Affirmed Networks, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Affirmed Networks, Inc.

Affirmed NETWORKS, INC. SOFTWARE LICENSE AGREEMENT

AFFIRMED NETWORKS, INC. (“AFFIRMED”) IS WILLING TO LICENSE THE ENCLOSED SOFTWARE AND ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE “PROGRAM”) TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE (S) OR USING THE AFFIRMED PRODUCTS CONTAINING THE SOFTWARE, AND BEFORE USING THE ACCOMPANYING USER DOCUMENTATION. OPENING THE PACKAGE (S) OR USING THE AFFIRMED PRODUCTS CONTAINING THE PROGRAM WILL INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, AFFIRMED IS UNWILLING TO LICENSE THE PROGRAM TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE PROGRAM WITHIN TEN (10) DAYS FROM SHIPMENT TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR LICENSE FEE WILL BE REFUNDED. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE PROGRAM BETWEEN YOU AND AFFIRMED, AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION OR UNDERSTANDING BETWEEN THE PARTIES.

License Grant

Subject to the provisions of this License, Affirmed grants to Licensee, and Licensee accepts, a non-exclusive, non-transferable license to use the object code form of the software supplied by Affirmed, including all patches, error corrections, updates and revisions thereto in machine-readable, object code form only (the “Software”), and the user documentation, including all updates and revisions thereto (the “User Documentation”) for Licensee’s internal business purposes (including, without limitation, in conjunction with Licensee’s provision of services to its customers) on or in conjunction with the hardware product with which it was originally delivered or on a single designated computer. The Software and User Documentation are sometimes collectively referred to as the “Program”. *Licensee acknowledges that certain Software provided by Affirmed may contain other restrictions and Licensee must refer to accompanying license certificates for each such Software licensed.* Licensee agrees that Licensee will not pledge, lease, rent, or share Licensee's rights under this License Agreement, and that Licensee will not, without Affirmed’s prior written consent, assign or transfer Licensee's rights hereunder. Licensee agrees that Licensee may not duplicate (except as set forth below), decompile, disassemble, reverse engineer, modify, or otherwise translate the Software or permit a third party to do so and that Licensee shall not make the Program available to any other third party, or create works derivative of the Program, without Affirmed’s express written consent. Licensee agrees it shall not publish in any fashion any results of benchmark tests run on the Program.

The Program is copyrighted and is only authorized to reproduce one copy of the Software and the User Documentation solely for backup purposes. Licensee is hereby prohibited from otherwise copying or translating, modifying or adapting the Program or, incorporating in whole or any part in any other product or creating derivative works based on all or any part of the Program. Licensee is not authorized to license others to reproduce any copies of the Program, except as expressly provided in this Agreement. Licensee agrees to ensure that all copyright, trademark and other proprietary notices of Affirmed affixed to or displayed on the Program will not be removed or modified. Licensee shall not decompile, disassemble or reverse engineer, the licensed software or any component thereof, except as may be permitted by applicable law, in which case Licensee must notify Affirmed in writing and Affirmed may provide review and assistance.

U.S. Government Restricted Rights. Notice - Distribution and use of products including computer programs and any related documentation and derivative works thereof, to and by the U.S. Government, are subject to the Restricted Rights provisions of FAR 52.227-19, paragraph (c)(2) as applicable, except for purchases by agencies of the Department of Defense (DOD). If the software is acquired under the terms of a Department of Defense or civilian agency contract, the software is a “commercial item” as that term is defined at 48 C.F.R. 2.101 (Oct. 1995), consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212 of the

Federal Acquisition Regulations and its successors and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995) of the DoD FAR Supplement and its successors. All U.S. Government end users acquire the software with only those rights set forth in this Agreement. Manufacturer is Affirmed Networks, Inc., 35 Nagog Park, Acton MA 01720. Unpublished - rights reserved under the copyright laws of the United States.

Affirmed's Rights

Licensee agrees that the Software and the User Documentation are proprietary, confidential products of Affirmed or Affirmed's licensor protected under U.S. copyright law and Licensee will use Licensee's best efforts to maintain their confidentiality. Licensee further acknowledges and agrees that all right, title and interest in and to the Program, including associated intellectual property rights, are and shall remain with Affirmed or Affirmed's licensor. This License Agreement does not convey to Licensee an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this License Agreement.

License Fees

The license fees paid by Licensee are paid in consideration of the license granted under this License Agreement.

Term

This License Agreement is effective upon Licensee's execution of this License Agreement and payment of the license fees and shall continue until terminated. Licensee may terminate this License Agreement at any time by returning the Program and all copies or portions thereof to Affirmed. Affirmed may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by Affirmed, Licensee agrees to return to Affirmed the Program and all copies or portions thereof. Termination of this License Agreement shall not prejudice Affirmed's rights to damages or any other available remedy.

Limited Warranty

Affirmed warrants that with normal use and service each Software product shall materially conform to Affirmed's then current published specifications for the most current release of such Software product for a period of ninety (90) days from the date of shipment by Affirmed. Program media is warranted for ninety- (90) days from the date of shipment by Affirmed. Software support beyond these periods is available at additional cost under the terms of Affirmed's Annual Maintenance Service Agreement. During the warranty period, as Licensee's sole and exclusive remedy, Affirmed will correct a Software product's failure to conform to the warranty provided that Licensee has notified Affirmed in writing of the nature of the non-conformity. This warranty shall not apply if any Software product has been (i) modified or altered by anyone other than Affirmed, (ii) abused or misapplied, or (iii) used in combination with hardware or software other than the Affirmed manufactured products for which it was designed. Affirmed shall incur no liability under this warranty if Affirmed's tests disclose that the alleged defect is due to causes not within Affirmed's reasonable control, including alteration or abuse of the goods. If a Program is determined not to be defective or to have a defect due to causes not within Affirmed's reasonable control, Licensee agrees to pay for such repair at the repair price as listed in Affirmed's then current applicable price list. In no event does Affirmed warrant that the use of Software products will be error free or uninterrupted. Affirmed's sole obligation under the Software warranty shall be to provide the remedies described above.

EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS WARRANTY, THE PROGRAM IS LICENSED "AS IS", AND Affirmed DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY WITH RESPECT TO THE SOFTWARE PROVIDED UNDER THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY WARRANTIES OF NONINFRINGEMENT AS WELL AS ANY WARRANTIES ARISING FROM COURSE OF DEALING, USEAGE OR TRADE PRACTICE.

Limitation of Liability

Affirmed's cumulative liability to Licensee or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the greater of: (i) ten thousand U.S. dollars ($10,000) or (ii) the total license fee paid to Affirmed for the use of the Program. In no event shall Affirmed be liable for any indirect, incidental, consequential, special, punitive or exemplary damages or lost profits or the loss of software or data, even if Affirmed has been

advised of the possibility of such damages. In the event that the Program contains the intellectual property of a third party pursuant to a license in favor of Affirmed, with a right to sublicense to Licensee, Affirmed hereby disclaims, to the extent permitted by law, such third party's liability of any damages, whether direct, indirect, incidental or consequential, arising out the use of the Program

Export Control

Licensee shall not export or re-export, directly or indirectly, any of the Programs (including any part of a Program or any direct product of such Program), Affirmed's Confidential Information or related technical data (a) into, or to a national resident of, any of those countries listed at the time of any shipment of the Products in the applicable U.S. export regulations as "prohibited or restricted" countries, or any other country to which such exports or re-exports may be restricted (collectively, the "Prohibited Countries") or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nations or the U.S. Commerce Department's Table of Denial Orders. At Licensee's request, Affirmed shall provide a list of the Prohibited Countries, Specially Designated Nations and/or Table of Denial Orders in order to assist Licensee to comply with such requirement.

Governing Law

This License Agreement shall be construed and governed in accordance with the laws and under the jurisdiction of the Commonwealth of Massachusetts, U.S.A. Any dispute arising out of this Agreement shall be referred to an arbitration proceeding in Boston, Massachusetts, U.S.A. by the American Arbitration Association.

Miscellaneous

If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorneys' fees and expenses of arbitration. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

Affirmed has made no commitments or promises orally or in writing with respect to delivery of any future software features or functions. In relation to any future software features or functions, all presentations, RFP responses and/or product outlook documents, information or discussions, either prior to or following the date herein, are for informational purposes only, and Affirmed has no obligation to provide any future releases or upgrades or any features, enhancements or functions, unless specifically agreed to in writing by both parties. Reseller acknowledges that no purchasing decisions are based upon any future software features or functions.

Third Party Beneficiary

If the Program incorporates or otherwise contains any intellectual Property of any third party pursuant to a license agreement in favor of Affirmed and sublicensed to Licensee, such third party shall, to the extent permitted by law, be a third party beneficiary of the terms and conditions of this Agreement.

Contents

Preface

Audience xlvii
Release Information xlvii
How to Use This Guide xlviii
Features in this Release xlix
Conventions xciv
How to Obtain Product Documentation xcv
Technical Assistance Center xcv

Chapter 1 Getting Started

Overview 1-1
Logging Into Acuitas 1-5
    Acuitas Password Policies 1-7
    securityconfiguration.properties 1-8
Using Certificates Issued by Trusted Certificate Authorities 1-9
Viewing Product Version Information 1-10
Using Online Help 1-11
Logging Out of Acuitas 1-13
Navigating the System 1-14
    Tree Display 1-14
    Tabs 1-15
        Network View 1-15
        Element Details 1-20
        Alarms 1-21
        Host System Alarms 1-21
        Event Logs 1-21
        PM Dashboard 1-21
        System Availability 1-21
Using Icons 1-22
Changing Screen Background Color (Theme) 1-31
Changing Your User Password 1-32
Common Functionality 1-33
    Filter Management 1-33
        Creating Filters 1-33
        Applying a Filter 1-35
        Modifying Filters 1-35

Deleting a Filter 1-36
Using Quick Filters 1-36
Setting Column Properties 1-37
Sorting Column Data 1-37
Navigating through Records 1-38
Exporting Records 1-38
Printing Records 1-39
Refreshing the Screen 1-39

Chapter 2 Topology

Groups 2-2
Adding Groups 2-2
Modifying Groups 2-3
Deleting Groups 2-3
Network Elements 2-4
Adding Network Elements 2-4
Adding a Network Element 2-4
Viewing Network Elements 2-8
Modifying Network Elements 2-8
Configuring Blade System Blades 2-12
Configuring Servers in a Group 2-13
Adding Network Element Remarks 2-14
Deleting Network Elements 2-14
Managing/Unmanaging Network Elements 2-15
Audit Trail 2-16
Configuring Audit Trail Purge Settings 2-16
Viewing the Topology Audit Trail 2-16
Exporting Topology Audit Trail 2-17
Streaming Acuitas Audit Trails and Alarms to syslog 2-18
Using rsyslog Server 2-19
Configuring the Mail Server 2-21
Configuring SNMP Settings 2-22
Configuring Message Prompt on Locked User Accounts 2-23

Chapter 3 Configuration

CUPS Manager 3-2
Using the Main Menu 3-4
Configuring a CUPS Group 3-5
Adding Another User Plane to the Control Plane 3-9
Removing a User Plane from the Control Plane 3-9
Viewing the Details of a Control Plane/User Plane Pair 3-10
Auditing and Replicating Configuration 3-11
Entities Replicated 3-12
Use Cases 3-17
Configuring a PGW-based CUPS Group 3-17
Configuring a SGW-based CUPS Group 3-19
Configuring a PGW- and SGW-based CUPS Group 3-20
Software Releases 3-22
Adding Software Releases 3-22
Viewing Software Releases 3-24

Modifying Software Releases 3-25
Setting Software Releases Obsolete 3-26
Deleting Software Releases 3-26
Acuitas Support for Managing MME Software Updates 3-27
Software Schedules 3-32
Adding Software Schedules 3-32
Viewing Software Schedules 3-34
Viewing Software Schedule Subtask Status 3-35
Copying Software Schedules 3-36
Enabling/Disabling Software Schedules 3-37
Quick Start Software Schedules 3-38
Modifying Software Schedules 3-38
Deleting Software Schedules 3-39
Software Rollback 3-40
Performing Software Rollback 3-40
Viewing Software Rollback Progress 3-41
Viewing Software Rollback Status 3-42
Configuration Templates 3-44
Adding Configuration Templates 3-44
Viewing Configuration Templates 3-45
Copying Configuration Templates 3-46
Modifying Configuration Templates 3-47
Setting Configuration Templates Obsolete 3-48
Deleting Configuration Templates 3-49
Exporting Configuration Templates 3-50
Importing Configuration Templates 3-51
Template Schedules 3-52
Adding Template Schedules 3-52
Copying Template Schedules 3-55
Viewing Template Schedules 3-56
Viewing Template Schedule Execution Status 3-57
Enabling/Disabling Template Schedules 3-58
Quick Start Template Schedules 3-59
Modifying Template Schedules 3-59
Deleting Template Schedules 3-60
Alarm Triggered Configurations 3-61
Adding Alarm Triggered Configuration 3-61
Modifying Alarm Triggered Configurations 3-62
Deleting Alarm Triggered Configurations 3-63
Use Case: Alarm Triggered Configuration 3-64
Create an Configuration Maintenance Template 3-64
Create a Decreasing Threshold of 80% 3-66
Create an Alarm Filter for the Decreasing Threshold 3-68
Create an Alarm Triggered Configuration 3-70
Modify the Performance Schedule to Add the Threshold Alarm to the Specific KPI 3-71
View Execution Status 3-73
Audit Trail 3-76
Viewing the Audit Trail 3-76
Exporting Audit Trail 3-77
File Servers 3-78

Adding File Servers 3-78
Viewing File Servers 3-79
Modifying File Servers 3-79
Deleting File Servers 3-80
Geographic Redundancy Manager 3-81
Viewing Geographic Redundancy Groups 3-84
Adding Geographic Redundancy Groups 3-85
Prerequisites 3-85
Modifying Geographic Redundancy Groups 3-91
Comparing Configurations 3-96
Replicating Configurations 3-98
Entities Not Replicated 3-98
Switching Over to the Standby Node 3-101
Viewing Recent Activities 3-102
Viewing Chronological Switchover Log of Geo Redundancy Groups 3-104
Deleting Geographic Redundancy Groups 3-105
Configuration when Primary System is Out of Service 3-107
Scenario 1: Active System is Manageable Prior to Going Out of Service . 3-107
Scenario 2: Active System *is not* Manageable Prior to Going Out of Service 3-108
Scenario 3: Active System *is not* Manageable Prior to Going Out of Service and is Manually Disconnected from the Network 3-108
Troubleshooting Problems with Geographic Redundancy Groups 3-109
Geographic Redundancy Group Icon Not Visible 3-109
Last Discovery Status is Mismatch 3-109
How to Enable/Disable a Geographic Redundancy Group on a Node 3-111
Geographic Redundancy Group is Operationally Up on Primary and Secondary Nodes 3-112
Configuration Comparison Report Lists Differences 3-113
Error When Replicating Configuration 3-114
Failure Due to Unchangeable Entities 3-115
Configuration Export Manager 3-116
Viewing Configuration Files 3-116
Viewing Configuration Details 3-116
Printing Configuration File 3-117
Saving Configuration Files 3-117
Downloading Configuration Files 3-118
Comparing Configuration Files 3-119
Deleting Configuration Files 3-120
URL List Management 3-121
Viewing URL List Files 3-122
Specifying to Auto-Push File to Destination Network Elements 3-123
Specifying Auto-Push Settings 3-124
Review and Edit 3-125
Editing a Single URL 3-125
Deleting a Single URL 3-126
Adding URL(s) to a File 3-127
Overwrite 3-127
Mark As Reviewed 3-128
Compare 3-128
URL List Schedules 3-130

Adding URL List Schedules 3-130
Viewing URL List Schedules 3-131
Viewing URL List Schedule Subtask Status 3-132
Copying URL List Schedules 3-133
Enabling/Disabling URL List Schedules 3-134
Quick Start Software Schedules 3-134
Modifying URL List Schedules 3-135
Deleting URL List Schedules 3-136

Chapter 4 Fault

Alarms 4-2
Identifying Network Elements with Alarms 4-2
Managing Network Element Fault Management State 4-4
Configuring Trap OID Display Length 4-7
Viewing Alarms 4-8
Viewing Host System Alarms 4-9
Filtering Alarms 4-12
Severity Filter 4-12
Custom Filter 4-14
Quick Filter 4-14
Viewing/Editing Alarm Details 4-14
Assigning Alarm Owners 4-16
Acknowledging Alarms 4-16
Clearing Alarms 4-17
Showing/Hiding Cleared Alarms 4-18
Purging Cleared Alarms 4-18
Deleting Alarms 4-19
Forwarding Alarms 4-20
Streaming Alarms to syslog 4-21
Using rsyslog Server 4-22
Viewing Alarm Statistics 4-23
Exporting Alarms 4-26
Printing Alarms 4-27
Generating an Alarm Report 4-28
Configuring Alarm Purge Settings 4-29
Configuring SNMP Alarm Forwarding 4-30
NorthboundTrapConfig.properties File 4-32
NMSSNMPAgent.properties File 4-33
Configuring Alarm E-mail Notification 4-34
Events 4-36
Viewing Event Logs 4-36
Viewing Event Details 4-37
Printing Event Logs 4-38
Exporting Event Logs 4-39
Purging Event Logs 4-40
Configuring Purge Interval for Event Logs 4-41
Purging a Specific Log 4-41
Purging All Event Logs 4-41

Chapter 5 Performance

Exporting Performance Management Data 5-2
Enabling/Disabling Performance Collections 5-3
Performance Reports 5-4
Configuring Data Type and Unit Conversion at the Global Level 5-4
Understanding Delta Value and Rate Value Effects on Charts 5-4
Configuring Data Type and Unit Conversion 5-9
Viewing Historical Statistics 5-9
Configuring Historical Report Data Purging 5-10
Exporting Historical Statistics Reports 5-17
Viewing Real Time Statistics 5-18
Viewing Outage Reports 5-21
Configuring Export Reports 5-21
Triggering Report Export on Demand 5-22
Configuring Export Purge Interval 5-23
Thresholds 5-24
Adding Thresholds 5-24
Viewing Thresholds 5-26
Modifying Thresholds 5-27
User Tasks Templates 5-28
Viewing User Tasks Templates 5-28
Modifying User Tasks Templates 5-28
Users Tasks Scheduler 5-30
Viewing User Tasks Scheduler 5-30
Enabling/Disabling User Tasks Schedules 5-30
Associating a Threshold with a PM Collection Task 5-31
Prerequisite to Configure a Metric-based Threshold 5-31
Prerequisites to Configure an Instance-based Threshold 5-31
Modifying User Tasks Scheduler 5-34
Quick Start Data Collection 5-36
Exporting User Tasks Scheduler 5-36
CSV Stats Recovery 5-38
Launching a CSV Stats Recovery 5-38
Viewing Statistics Recovery Schedule Details 5-40
Viewing Statistics Recovery Schedule Status 5-41
Deleting Statistics Recovery Schedules 5-43
Viewing Key Performance Indicators 5-44
Configuring the Dashboard 5-47
Using the Dashboard Filter Manager to Filter Records 5-52
Example Dashboards 5-55
Exporting KPI Data from the Dashboard 5-59

Chapter 6 VNF Manager

Prerequisites 6-3
vCenter Requirements 6-3
Install Acuitas Packages for VMware 6-3
Adding Host Resolution Information in /etc/hosts 6-3
Importing the vCenter Certificate 6-4
Adding the vCenter Network Element 6-4
Requirement to Install ovatools to Enable Features 6-6

vCloud Director Requirements 6-7
Importing the vCloud Director Certificate 6-7
Adding the vCloud Director Network Element 6-7
VNF Manager Support for Managing Anti-affinity Rule 6-9
OpenStack Requirements 6-10
Preconfiguration Requirements for OpenStack 6-10
Importing the SSL Certificate 6-12
Adding the OpenStack Network Element 6-12
Configuring Hosts 6-14
Configuring Servers in a Group 6-14
Configuring Blade IP Addresses 6-15
Administering the VNF Manager 6-16
Commissioning Clusters 6-18
vCenter Only: Uploading Open Virtualization Archive (OVA) Packages 6-19
Deleting an Uploaded OVA package 6-20
OpenStack and vCloud Director Only: Viewing VIM Configuration 6-20
OpenStack Only: Managing Availability Zones 6-21
vCloud Director Only: Managing Organization vDCs 6-22
vCenter Only: Discovering and Configuring Hosts 6-24
vCenter Only: Adding a Managed Host 6-24
vCenter Only: Viewing Host Configuration 6-25
vCenter Only: Modifying Host Configuration 6-25
vCenter Only: Unmanaging a Host 6-26
Configuring a Cluster with a CSV File 6-26
Creating the CSV File 6-26
Importing the CSV File 6-57
Validating Cluster Configuration 6-58
Cluster-Level Configuration 6-59
Modifying Cluster Configuration 6-68
Configuring Nodes in the Cluster 6-69
Modifying VM Configuration 6-79
Deleting a VM 6-79
Validating Cluster Configuration 6-80
Instantiating the Cluster 6-81
Checking Operation Progress 6-81
Scaling In Cluster to Remove Nodes in an Inconsistent State 6-82
Scaling Out Cluster to Instantiate Nodes 6-83
Scaling Out Nodes 6-83
Scaling In Nodes 6-84
Healing Nodes 6-85
Terminating the Cluster 6-88
Aborting Cluster Operation 6-88
Downloading Cluster Configuration 6-88
Using Cluster View 6-89
Viewing Cluster Alarms 6-92
Viewing Cluster Details 6-93
Viewing Physical and Logical Topology 6-93
Viewing Key Performance Indicators 6-96
Viewing Cluster Reports (*MCC Clusters and MCC MME Clusters*) 6-99
Network Elasticity Report 6-100
Network Inventory Report 6-103

Configuring Dynamic Scale Out/Scale In 6-106
Prerequisite When a Cluster was not Instantiated by VNF Manager 6-106
Configuring Scaling Policy 6-113
Monitoring Dynamic Scale Out/Scale In 6-120
Alarm Notifications 6-122
Overload/Underload Conditions 6-122
Scale Out/Scale In Faults 6-122
Using the VNF Manager and Provisioning API 6-123
VNF Manager and Provisioning API Audit Logs 6-123
Troubleshooting Problems with OpenStack Cluster Commissioning 6-124
Host has Multiple SSM Nodes Instantiated 6-124
Problem 6-124
Cause 6-124
Solution 6-124
VNF Manager Fails to Show VIM Configuration 6-125
Problem 6-125
Cause 6-125
Solution 6-125

Chapter 7 Security

Security Groups 7-2
Adding Security Groups 7-4
Associating Resources with Security Groups 7-5
Viewing Security Groups 7-6
Copying Security Groups 7-7
Exporting Security Groups 7-8
Modifying Security Groups 7-9
Deleting Security Groups 7-10
Specifying Permissions by Security Group 7-10
Users 7-33
Adding Users 7-33
Viewing Users 7-34
Modifying Users 7-36
Exporting Users 7-37
Changing User Password 7-38
Viewing User Audit Trail 7-39
Managing Active User Sessions 7-45
Unlocking Users 7-46
Deleting Users 7-46

Chapter 8 Tools

Database Administration 8-2
Adding User Triggered Database Backup 8-2
Viewing Database Backup Details 8-3
Scheduling Database Backup 8-3
Viewing Scheduled Database Backup 8-4
Deleting Database Backup 8-5
Restoring Database from Backup 8-6
Standalone Acuitas Server 8-6
Acuitas Server Cluster (HA or HA + DR) 8-8

Configuring Alarm Severity Color Settings. 8-9
Network Configuration Backup. 8-9
Triggering Configuration Backup on Demand. 8-10
Scheduling Configuration Backup 8-10
NE Configuration Backup and Restore 8-12
Adding User Triggered NE Configuration Backup 8-12
Viewing NE Configuration Backup Details 8-13
Purging NE Configuration Backup Files 8-14
Downloading NE Configuration Backup File 8-14
Restoring NE Configuration Backup File. 8-15
Deleting NE Configuration Backup 8-15
Scheduling NE Configuration Backup 8-16
Viewing Scheduled NE Configuration Backup Details 8-17
Modifying Scheduled NE Configuration Backup. 8-18
Enabling/Disabling NE Configuration Backup Schedules. 8-19
Quick Start NE Configuration Backup Schedules 8-20
Exporting NE Configuration Backup Schedules 8-21
Deleting NE Configuration Backup Schedules 8-22

Chapter 9 Affirmed Open Workflow

Overview 9-2
Service Flow Switching 9-10
Permissions Required for Workflow Access 9-10
Build Out Functions. 9-11
Build a Workflow. 9-15
Control Profile 9-16
Data Profile Reselection Trigger Template 9-23
Subscriber Analyzer 9-23
Service Flow. 9-26
Creating a New Service Flow 9-26
Selecting an Existing Service Flow. 9-26
Creating a Service to Add 9-32
Validating Workflow 9-36
Workflow Service Evaluation. 9-40
Example Use Case for Service Comparison 9-40
Workflow Service Evaluation 9-41
Workflow Service Comparison 9-45
Workflow Tracing. 9-51
Comparing/Synchronizing a Workflow on Separate Devices 9-58
Comparing Two Workflows on Separate Devices 9-58
Synchronizing a Workflow to Another Device. 9-58
Service Functions. 9-59
ACL List. 9-63
ACL Policy. 9-65
Advice of Charge 9-66
Aoc Hardware ID Format. 9-69
APN Mapping List 9-71
Application Rule Group (MCC versions prior to 8.4) 9-72
CA Certificate List 9-103
Content Filter Blacklist File 9-104
DHCP Local Server Profile 9-105

DHCP Service Profile 9-106
DiffServ Profile Class Mapping 9-108
DiffServ Profile DSCP Mapping 9-111
Domain Rule Group 9-112
EDR Server Profile 9-114
Encryption Profile 9-115
File Download Profile 9-116
Filter Database Size 9-118
Host List 9-119
HTTP Header Enrichment 9-120
Adding an HTTP Header Enrichment 9-121
Removing an HTTP Header Enrichment 9-127
Rewriting an HTTP Header Enrichment 9-127
HTTP Rule Group 9-128
HTTP URL Rewrite 9-132
Insertion Object List 9-134
IP List 9-136
LDAP Interface 9-138
LDAP Server 9-138
LDAP Profile 9-139
LDAP Feature Group 9-142
Loopback IP List 9-144
Malware Category 9-145
Multimedia Messaging Service 9-146
Multimedia Messaging Service Center 9-146
Multimedia Messaging Service Center Group 9-148
MMS Error Response 9-149
MMS Blacklist 9-150
MMS MM3 Profile 9-151
MMS STI Profile 9-152
Packet Filter 9-153
QoS 9-155
SCTP Profile 9-157
Service Rule 9-158
Session Rule Group 9-163
Short Message Service 9-165
Short Message Service Center Profile 9-165
Short Message Service Center Group 9-166
Short Message Service Notification 9-167
Static DNS Map 9-168
TCP Optimization Profile 9-169
Time of Day Rule Group 9-171
TLS Rule Group 9-172
TLS Termination Policy 9-174
UA Profile 9-176
URL List 9-178
Services 9-180
Charging 9-182
Rating Group 9-183
Billing Plan 9-187
Charging Instance 9-188

Content Cache 9-190
Content Cache Service 9-190
Content Cache Instance 9-191
Content Filter 9-193
Global Content Filters 9-193
Content Filter Static Category Filters 9-194
Content Filter Service Rule Filters 9-194
Content Filter Online Category Group Filters 9-195
Content Filter Malware Category Group Filters 9-200
Content Filter IWF Category Filters 9-201
Content Filter Service 9-203
Content Filter Instance 9-204
Static Category 9-212
Online Category Group 9-213
Content HTTP Server Instance 9-214
Content Insertion Profile 9-216
Default Policy Cause Code List 9-218
DNS Proxy Service 9-220
DNS Proxy Service Instance 9-221
DNS Policy 9-222
DNS Reverse Cache 9-224
DNS IP Flow 9-225
Domain Tunnel Age Time 9-226
Tunnel Detection Profile 9-227
Fair Bandwidth Usage 9-229
HTTP Proxy (MCC versions prior to 8.4) 9-231
HTTP Proxy Service 9-235
HTTP Request Policy 9-238
HTTP Response Policy 9-241
HTTP IP Flow 9-242
Encryption Profile 9-244
HTTP Proxy Instance 9-245
Server Connections 9-248
ABR Optimization Profile 9-249
Explicit Proxy Profile 9-250
Fraud Detection Profile 9-252
HTTPS Profile 9-254
HTTP Transaction Record Profile 9-255
Long Term Mobile ID 9-258
Steering GW Group 9-260
TCP Splicing Policy 9-261
TCP Splicing Profile 9-262
Toll Free Profile 9-264
Web Image Optimization Profile 9-266
HTTP Server Entitlement Service 9-268
HTTP Server Policy 9-270
Metering Service 9-271
Multi Protocol Proxy (8.4 and later MCC versions) 9-272
Multi Protocol Proxy Service 9-276
HTTP Request Policy 9-279
HTTP Response Policy 9-282

IP Flow 9-283
Encryption Profile 9-285
Proxy Instance 9-286
Server Connections 9-289
ABR Optimization Profile 9-290
Explicit Proxy Profile 9-292
Fraud Detection Profile 9-293
HTTPS Profile 9-295
HTTP Transaction Record Profile 9-296
Long Term Mobile ID 9-299
Steering GW Group 9-301
TCP Splicing Policy 9-302
Traffic Control Profile 9-303
Toll Free Profile 9-305
Web Image Optimization Profile 9-307
Protocol Application Rule Group (8.4 and later MCC version) 9-309
Quality of Service 9-315
QoS Flow 9-315
QoS Policy 9-318
Realm List 9-320
SMTP Proxy 9-322
Steering Service 9-323
Steering Flow 9-324
Steering Policy 9-325
Subscriber Firewall 9-326
Subscriber Firewall Flow 9-327
Subscriber Firewall Policy 9-329
Video Adaptation (MCC versions prior to 9.0) 9-330
Video Adaptation Service 9-333
Video Adaptation Instance 9-334
Offline Transcoding Policy 9-336
Offline Serving Policy 9-337
Transcoding Map 9-338
Transcoding Rule 9-341
Online Transcoding Policy 9-342
WAP Gateway 9-344
WAP Gateway Instance 9-344
WAP IP Flow 9-345
HTTP Filter File Management 9-347
Adding URL Lists 9-348
Modifying or Deleting URL Lists 9-349
Viewing the Contents of a URL List File 9-349
Adding Categories 9-350
Modifying or Deleting Categories 9-351
Viewing the Contents of a Category File 9-351
Viewing HTTP Filter File List 9-352

Chapter 10 Configuration Navigator

Navigating the System 10-2
Tree Display 10-2
Refreshing the Tree 10-4

Paging and Filtering Configuration Object Instances 10-4
Configuration Window 10-6
Alarms 10-7
Cluster 10-8
Node Personalities 10-10
Value-Added Services Guidelines 10-13
Scale In Limitations 10-14
Control Plane Protection 10-16
Data Plane Protection 10-17
GNP Sub Pool 10-20
Node 10-21
RAMDISK 10-26
Statistics 10-27
Summary 10-27
TND Peer Statistics 10-28
TND Total Statistics 10-28
Data Path 10-29
Data Records 10-30
Detail 10-30
Statistics 10-30
Fault Management 10-31
Flow Idle Timeout Profile 10-32
Geographic Redundancy Group 10-33
Net Link Status 10-35
Image Management 10-36
Online Software Upgrade 10-38
Prerequisites 10-38
prepare Command 10-38
onlineupgrade Command 10-39
rollback Command 10-42
releasemodifier Command 10-42
Card Status 10-44
Release Modifier Status 10-45
Status 10-45
Infrastructure 10-47
Dynamic Scale 10-47
EDR 10-48
Export IP 10-48
File Management 10-49
Use Case: Storing Gz/Rf SGW CDRs to a File in the Event of a Failure . 10-49
Event Logging 10-55
Sample Use Case 10-55
Viewing Protocol Logs with Packet Analyzers 10-58
System Logging 10-59
NTP Server 10-60
Status 10-60
OOM 10-61
Peer Overload Control 10-63
Profile 10-63
Configuration 10-64
Counters Detail 10-65

Counters Detail Cumulative 10-66
Counters Summary 10-67
Counters Summary Cumulative 10-67
Pacer Rates 10-67
Time Zone 10-68
IP Protocols 10-69
BFD 10-69
BGP Routers 10-71
BGP VPN Routers 10-79
NAT 10-89
save-map Command 10-89
View UE IP Address Details 10-89
View Deterministic NAT Resources 10-90
NSM Logging 10-91
OSPFv2 Routers 10-91
OSPFv3 Routers 10-93
Policy 10-93
Routing Options 10-96
TCP 10-97
Statistics 10-100
MME 10-101
Viewing MME Real Time Statistics 10-101
Network Context 10-104
VRF Lightweight 10-107
Example Network Context Scenarios 10-108
Limitations 10-108
Neighbor Discovery Profile 10-109
Performance Statistics Management 10-110
Pki 10-111
install Command 10-111
From http/https 10-112
From a Local Disk 10-112
Using Cut and Paste 10-112
Using scp/sftp 10-113
remove Command 10-114
update Command 10-115
Viewing pki Objects 10-116
Security 10-117
Debug 10-132
History 10-132
Redundancy Stats 10-133
Statistics 10-134
Service Constructs 10-136
ACL List 10-142
Advice of Charge 10-144
Aoc Hardware ID Format 10-146
Application Rule Group (MCC versions prior to 8.4) 10-147
CA Certificate List 10-176
Code Mapping Lists 10-177
Content Insertion 10-178
Insertion Object List 10-178

Content Insertion Profile 10-179
Data Record Template 10-181
Deep Packet Inspection (MCC versions prior to 8.4) 10-182
Device Database 10-183
Import Command 10-184
Device Database Statistics 10-185
DHCP Local Server Profile 10-186
DHCP Local Server Statistics 10-186
DHCP Mapping Template 10-187
DHCP Mapping Template Statistics 10-191
Diameter Result Code Policy List 10-192
DHCP Service Profile 10-195
Diffserv Profile 10-196
Domain Rule Group 10-200
EDR Flow Network Stats Profile 10-201
EDR Interface Profile 10-202
EDR Server Profile 10-211
EDR Session Data Stats Profile 10-212
Encryption Profile 10-213
Event Trigger Template 10-215
File Download Profile 10-217
Filter Hash List 10-218
Filter Hash List Import History 10-218
Filter Hash List Summary 10-219
Flow Idle Timeout Filter 10-220
Flow Idle Timeout Rule 10-220
Geo Redundancy Server 10-221
Gy Event Trigger Template 10-223
Health Check Profile 10-224
Host List 10-225
HTTP Header Enrichment 10-226
HTTP Rule Group 10-234
HTTP Server 10-237
HTTP Server List 10-237
HTTP URL Rewrite 10-239
IMSI Range 10-241
IMSI Range List 10-242
Interface: Accounting Service 10-243
Interface: Authorization Service 10-248
Interface: Flow Authorization Interface 10-251
Interface: Gateway Session Learner 10-253
Interface: IPMS Interface 10-262
Server Status 10-263
Statistics 10-263
Interface: AAA Interface Group 10-265
AVP Flags 10-265
Diameter Node Admin 10-266
Diameter Node Status 10-270
Peer Command Statistics 10-271
Peer Statistics 10-272
Peer Status 10-273

Diameter Performance Statistics 10-274
GTPP Node Admin 10-274
GTPP Node Status 10-277
Peer Command Statistics 10-278
Peer Statistics 10-279
Peer Status 10-281
GTPP Performance Statistics 10-282
RADIUS Client Server Group 10-283
RADIUS Procedure Statistics 10-288
RADIUS Client Server Status 10-289
RADIUS Server Server Group 10-291
Statistics 10-293
Interface: Offline Charging 10-294
Interface: Online Charging 10-304
Interface: PCRF Charging 10-314
Interface: Policy Server Interface 10-321
Interface: Port NBR Service 10-322
Interface: Rx Interface 10-323
Interface: S6b Interface 10-323
IP List 10-326
LDAP 10-327
LDAP Remote Server 10-327
LDAP Feature Group 10-328
LDAP Profile 10-330
Loopback IP List 10-333
Multimedia Messaging Service 10-334
Supported MIME Types 10-334
Multimedia Messaging Service Center 10-336
Multimedia Messaging Service Center Group 10-338
MM3 Profile 10-338
MMS Error Response 10-339
STI Profile 10-340
MMS Blacklist 10-340
Network Profile 10-341
Packet Filter 10-342
PLMN ID List 10-344
Protocol Application Rule Group (8.4 and later MCC version) 10-345
Quality of Service 10-350
RADIUS Mapping Template 10-351
RADIUS Attribute Mapping Template Statistics 10-354
Realm List 10-355
SCTP Profile 10-356
Service Rule 10-357
Session Rule Group 10-361
Short Message Service 10-363
Short Message Service Center Profile 10-363
Short Message Service Center Group 10-364
Short Message Service Notification 10-364
Static DNS Map 10-365
Static DNS Map 10-365
Subscriber Group 10-366

TCP Optimization Profile 10-367
Time of Day Rule Group 10-369
TLS Rule Group 10-370
TLS Termination Policy 10-371
UA Profile 10-372
URL List 10-373
Import Command 10-375
URL List Statistics 10-375
Workflow Data Stats 10-376
Services 10-378
ACL 10-382
Charging: Rating Group 10-383
Charging: Billing Plan 10-387
Charging: Charging Instance 10-388
Charging: Service Data Flow 10-390
Content Cache 10-390
Content Cache Service 10-390
Eviction Threshold Disk 10-391
Eviction Threshold Memory 10-392
Content Cache Instance 10-392
Content Filter 10-394
Global Content Filters 10-394
Content Filter Static Category Filters 10-395
Content Filter Service Rule Filters 10-395
Content Filter Online Category Group Filters 10-396
Content Filter Malware Category Group Filters 10-401
Content Filter IWF Category Filters 10-402
Content Filter Service 10-402
Static Category Source 10-403
Content Categorization 10-403
Filter Database Size 10-406
Content Filter Import History 10-406
Content Database Summary 10-407
Black List 10-407
White List 10-409
Service Rule 10-409
Content Filter Instance 10-410
CRBN Profile 10-420
DNS Proxy 10-422
DNS IP Flow 10-423
DNS Policy 10-424
DNS Reverse Cache 10-426
DNS Proxy Instance 10-427
Cache Display 10-427
Cache Statistics 10-428
Module Statistics 10-428
Domain Clean Time 10-429
Tunnel Detection Profile 10-430
Tunnel Blocked Domain 10-430
Fair Bandwidth Usage 10-431
Health Check 10-432

Statistics 10-432
HTTP Proxy (MCC versions prior to 8.4) 10-433
HTTP Proxy Service 10-435
HTTP Request Policy 10-436
HTTP Response Policy 10-438
HTTP IP Flow 10-440
HTTP Proxy Instance 10-442
ABR Optimization Profile 10-445
Client Connections 10-447
Back End Forwarding 10-447
Encryption Profile 10-447
Explicit Proxy Profile 10-449
Fraud Detection Profile 10-450
HTTP Transaction Record Profile 10-451
HTTPS Profile 10-453
Long Term Mobile ID 10-455
LTMI Import History 10-457
LTMI Key Status 10-457
Minify 10-458
Optimization Overload Control 10-458
Preemptive DNS 10-458
Server Connections 10-459
Steering Group 10-460
TCP Splicing 10-461
TCP Splicing Policy 10-461
Toll Free Profile 10-462
Traffic Control Profile 10-464
UDP 10-466
UDP Policy 10-467
Video Pacing 10-467
Web Image Optimization Profile 10-468
Service Data Flow 10-469
HTTP Server 10-470
HTTP Server Service Instance 10-470
Entitlement Service 10-472
HTTP Server Policy 10-473
Statistics 10-474
Metering Service 10-475
Service Data Flow 10-476
Multi Protocol Proxy (8.4 and later MCC versions) 10-477
Multi Protocol Proxy Service 10-479
HTTP Request Policy 10-480
HTTP Response Policy 10-482
IP Flow 10-484
Multi Protocol Proxy Instance 10-487
ABR Optimization Profile 10-489
Client Connections 10-491
Back End Forwarding 10-491
Encryption Profile 10-492
Explicit Proxy Profile 10-493
Fraud Detection Profile 10-494

HTTP Transaction Record Profile 10-495
HTTPS Profile 10-497
Long Term Mobile ID 10-499
LTMI Import History 10-501
LTMI Key Status 10-501
Minify 10-502
Optimization Overload Control 10-502
Preemptive DNS 10-502
Server Connections 10-503
Steering Group 10-504
TCP Splicing 10-505
TCP Splicing Policy 10-505
Toll Free Profile 10-506
Traffic Control Profile 10-508
UDP 10-510
UDP Policy 10-511
Video Pacing 10-511
Web Image Optimization Profile 10-512
Service Data Flow 10-513
Quality of Service 10-514
QoS Flow 10-514
QoS Policy 10-516
Service Data Flow 10-518
Rate Limiting Subscriber Group 10-519
SMTP Proxy 10-520
Steering Service 10-521
Steering Flow 10-521
Steering Policy 10-523
Service Data Flow 10-523
Subscriber Firewall 10-524
Subscriber Firewall Flow 10-524
Subscriber Firewall Policy 10-526
Service Data Flow 10-526
ALG Packet Statistics 10-527
Video Adaptation (MCC versions prior to 8.2) 10-528
Video Adaptation Service 10-528
Video Adaptation Instance 10-530
Offline Transcoding Policy 10-531
Online Transcoding Policy 10-533
Target Media Profile 10-534
Transcoding Map 10-535
Transcoding Rule 10-538
WAP Gateway 10-539
WAP Gateway Service Instance 10-539
WAP Gateway IP Flow 10-540
Service Data Flow 10-541
SNMP 10-542
System 10-543
TAM 10-544
User Access 10-546
vTap 10-551

Workflow 10-555
APN Mapping List 10-556
Control Profile 10-557
Data Profile 10-565
Data Profile Switching 10-567
Data Profile Reselection Trigger Template 10-568
Subscriber Analyzer 10-569
Zone 10-574

Chapter 11 Network Element

Log Viewer 11-1
Event Logs 11-4
Protocol Logs 11-4
Messages 11-6
Fault Files 11-7
Console Files 11-7
Trace Files 11-7
Viewing Trace File with Wireshark 11-8
Support Tarball 11-10
Save Tech Support Information 11-11
Device Audit Trail 11-13
Viewing the Device Audit Trail 11-13
Exporting Device Audit Trail 11-14
Rate Limiting Subscriber Group File Management 11-15
Adding Subscriber Groups 11-16
Prerequisites 11-16
Modifying or Deleting Subscriber Groups 11-17
Viewing the Contents of a Subscriber Group File 11-18
Viewing Subscriber Group File List 11-18
Geographic Redundancy Considerations 11-20
Accessing Siemens SPCRF EMS 11-21
Accessing HPE HSS EMS EMS 11-22
Accessing Device Gateway Application 11-23

Appendix A Interfacing with Northbound Interfaces

Acuitas TACACS+ Authentication, Authorization, and Accounting A-2
Overview A-2
Acuitas Security Module Authentication Order A-2
Authentication Configuration A-3
Acuitas LDAP Authentication and Authorization A-6
Overview A-6
Authentication A-6
Authorization A-7
Acuitas Security Module Authentication Order A-7
LDAP Authentication Configuration A-8
Downloading Server (LDAP Server) Certificate A-11
Configuration Required on the LDAP Server A-11
Acuitas RADIUS Authentication and Authorization A-13
Overview A-13
Acuitas Security Module Authentication Order A-13

RADIUS Authentication Configuration A-14
RADIUS Authorization Prerequisites A-14
RADIUS Authentication Procedure A-14
RADIUS Authorization Configuration A-17
Acuitas Triggered Alarm Detail. A-18
Acuitas Trap Format A-25
Third-party Traps A-26
HP Blade System Enclosure iLO Traps A-26
HP Blade iLO Traps A-30
VMware Traps. A-32
Siemens PCRF and AAA Traps A-37
Forwarded Trap Mappings A-38
vCenter Traps A-44
vpxdAlarmInfo A-44
vpxdDiagnostic A-45
Receiving vCenter Traps A-47
HP 3PAR SAN Traps A-49
HPE HSS Traps A-51
VERTICA Traps. A-53
Exported Performance Management Data A-56
PerformanceConfiguration.properties. A-56
Export Schedule Interval A-56
File Purge Interval A-57
File Time Offset. A-57
Raw Performance Management Data A-58
Calculated KPI Data A-59
Copying Performance Management Statistics Files to Destination Server A-61
Prerequisites. A-61
Initial Set Up A-62
Running the Script. A-63
VNF Manager and Provisioning REST API A-65
Authentication and Authorization. A-65
Accept Request Header (Optional) A-65
Error Handling A-66
Response Parameters A-66
Sample Response. A-66
Audit Log A-66
Sample Log A-66
VIM Management APIs A-67
List VIMs. A-68
List OVAs A-69
List Hosts. A-70
Get Host Details. A-71
List Images A-73
List Networks A-74
List Availability Zones A-75
List Server Groups. A-76
List Flavors A-77
Cluster Configuration Management APIs. A-78
List Cluster Configurations A-85
Put Cluster Configurations A-86

Put Cluster OVA Configuration A-93
Put Cluster Image Configuration A-94
Get Cluster Configuration Details A-95
List Node Configurations A-101
Put Node Configuration A-104
Get Node Configuration Details A-109
Delete Node Configuration. A-116
Delete Cluster Configuration A-117
Lifecycle Management APIs A-119
Instantiate Cluster A-120
Scale Out Cluster A-121
Scale Out Node A-122
Scale In Node A-123
Terminate Cluster A-125
List Clusters A-126
GET Cluster Details A-129
List Nodes A-133
Get Node Details A-136
Heal Node A-139
Scale In Node A-140
Dynamic Scaling APIs A-143
List Policies A-143
Get Policy Details A-144
Associate Policy A-148
Disassociate Policy A-149
MCC Configuration APIs A-150
Execute EMS Template A-150
Execute Template A-152
Network Configuration APIs A-154
Execute EMS Template A-154
Execute Template A-157
Use Cases A-160
Create Cluster Configuration A-160
Create Node Configuration. A-161
Instantiate MCC Cluster A-162
Scale Out a Node for MCC Cluster A-162
Scale In a Node for MCC Cluster. A-163
Terminate MCC Cluster A-164
Remove Cluster Configuration. A-164
Security REST API A-165
Authentication and Authorization A-165
Accept Request Header (Optional) A-165
Error Handling A-166
Response Parameters A-166
Sample Response A-166
Security Group APIs A-167
List Groups A-167
Get Group Details A-168
List Roles A-170
List Hierarchy Roles A-171
Create Group A-172

Copy Group A-173
Modify Group A-174
Add Roles (Permissions) to Group A-175
Remove Roles (Permissions) from Group A-176
Delete Group A-177
Security User APIs A-178
List All Users A-178
Get User Details A-181
Create User A-184
Modify User A-186
Delete User A-188
Reset User Password A-189
Assign Groups to User A-190
Remove Groups from User A-191

Appendix B Key Performance Indicators (KPIs) Metrics

Derived Metrics B-1
Raw Metrics B-41

Index

List of Figures

Figure 1-1 Accessing Acuitas Modules 1-3
Figure 1-2 Accessing NE Applications 1-4
Figure 1-3 Firefox Warning Screen 1-5
Figure 1-4 Firefox Add Security Exception Screen 1-6
Figure 1-5 Acuitas Login Screen 1-6
Figure 1-6 Top-level Help Window 1-11
Figure 1-7 Devices in the Network View 1-15
Figure 1-8 Filter Manager 1-34
Figure 1-9 Select the Filter 1-35
Figure 1-10 Page Navigation Bar 1-38
Figure 1-11 Configure Export Parameters Window 1-39
Figure 2-1 Accessing Topology Applications 2-1
Figure 2-2 Configure Blades Screen 2-12
Figure 2-3 Configure Server Screen 2-13
Figure 3-1 Accessing Configuration Applications 3-2
Figure 3-2 CUPS Manager Window 3-3
Figure 3-3 Selecting a Registered Cluster 3-5
Figure 3-4 Removing a User Plane from the Control Plane 3-10
Figure 3-5 Selecting an Entity in the CUPS Group 3-10
Figure 3-6 Viewing a Control Plane/User Plane Pair 3-11
Figure 3-7 Audit Window 3-12
Figure 3-8 New Software Maintenance Window 3-22
Figure 3-9 New Software Schedule Window 3-32
Figure 3-10 Software Rollback Window 3-40
Figure 3-11 Software Rollback View Window 3-42
Figure 3-12 View Status Window for a Software Rollback 3-43
Figure 3-13 View Status Window for a DPI Signature Rollback 3-43
Figure 3-14 New Template Schedule Window 3-53
Figure 3-15 Configuration Command List 3-54
Figure 3-16 Template Maintenance Window 3-65
Figure 3-17 Template Maintenance Window 3-66
Figure 3-18 Configure New Threshold Window 3-67
Figure 3-19 Filter Manager 3-68
Figure 3-20 Filter Manager 3-69
Figure 3-21 Alarm Triggered Configuration 3-70
Figure 3-22 Alarm Triggered Configuration 3-71
Figure 3-23 Edit Task Scheduler 3-72
Figure 3-24 Edit Task Scheduler 3-72
Figure 3-25 Select the Filter 3-73
Figure 3-26 Template Execution Status 3-74
Figure 3-27 Geographic Redundancy Manager 3-85
Figure 3-28 Configuration Comparison Report 3-97
Figure 3-29 Configuration Mismatch 3-97
Figure 3-30 Replication Activities Report 3-100
Figure 3-31 Recent Activities Report 3-103
Figure 3-32 Chronological Switchover Log 3-105
Figure 3-33 Configuration Comparison Report 3-119
Figure 3-34 URL List File Lifecycle Management 3-121

Figure 3-35 URL List Maintenance Window 3-122
Figure 3-36 Edit URL List Schedule Window 3-124
Figure 3-37 URLs in the File 3-125
Figure 3-38 Comparison File 3-129
Figure 3-39 New URL List Schedule Window 3-130
Figure 3-40 URL Config Schedule View Status Window 3-133
Figure 4-1 Accessing Fault Applications 4-1
Figure 4-2 Alarm Propagation 4-3
Figure 4-3 FM Manage/Unmanage 4-5
Figure 4-4 Alarms tab 4-8
Figure 4-5 Configure Blades Screen 4-10
Figure 4-6 Host System Alarms tab 4-11
Figure 4-7 Filtered Alarms - Critical Severity 4-12
Figure 4-8 Alarm Details Window 4-15
Figure 4-9 Alarm Stats 4-24
Figure 4-10 Alarm Trap Forwarding 4-30
Figure 4-11 Create New SNMP Listener 4-31
Figure 4-12 Alarm Trap Forwarding 4-32
Figure 4-13 Event Logs tab 4-36
Figure 5-1 Accessing Performance Applications 5-2
Figure 5-2 Delta Chart with Collection Time Period 1 Hour 5-6
Figure 5-3 Rate Chart with Collection Time Period 1 Hour 5-6
Figure 5-4 Delta Chart with Collection Time Period 7 Days 5-7
Figure 5-5 Rate Chart with Collection Time Period 7 Days 5-7
Figure 5-6 Delta Chart with Collection Time Period > 7 Days 5-8
Figure 5-7 Rate Chart with Collection Time Period > 7 Days 5-8
Figure 5-8 Historical Statistics 5-13
Figure 5-9 Example Tabular View 5-15
Figure 5-10 Example Chart View 5-16
Figure 5-11 Real Time Statistics 5-18
Figure 5-12 Example Pie Chart 5-20
Figure 5-13 Configure New Threshold 5-25
Figure 5-14 User Task Template Details Edit 5-29
Figure 5-15 Task Schedule Edit 5-34
Figure 5-16 Task Schedule Edit with Expanded Metric 5-35
Figure 5-17 CSV Stats Recovery Launch Screen 5-39
Figure 5-18 Stats Recovery Status Screen 5-42
Figure 5-19 Dashboard Filter Manager 5-53
Figure 5-20 Filter Conditions 5-54
Figure 6-1 Configure Server Screen 6-14
Figure 6-2 Accessing VNF Manager Application 6-16
Figure 6-3 VNF Manager Administration 6-17
Figure 6-4 Accessing VNF Manager Application 6-18
Figure 6-5 Cluster Configuration Screens 6-59
Figure 6-6 vCenter VM Configuration Screen 6-70
Figure 6-7 vCloud Director VM Configuration Screen 6-71
Figure 6-8 OpenStack VM Configuration Screen for MCC 6-72
Figure 6-9 OpenStack VM Configuration Screen for MCC MME 6-73
Figure 6-10 Console Window 6-82
Figure 6-11 Accessing VNF Manager Application 6-89
Figure 6-12 Cluster View 6-90

Figure 6-13 Cluster Alarms 6-92
Figure 6-14 Physical View of a Blade System 6-93
Figure 6-15 Physical View of a Server Group 6-94
Figure 6-16 Blade Details 6-95
Figure 6-17 Key Performance Indicators 6-96
Figure 6-18 Network Elasticity Report 6-100
Figure 6-19 Network Inventory Report 6-103
Figure 6-20 Scale-in/out Monitor Examples 6-121
Figure 7-1 Accessing Security Applications 7-2
Figure 7-2 Setting Permissions for Group Members 7-11
Figure 8-1 Accessing Tools Applications 8-1
Figure 9-1 Accessing the Affirmed Open Workflow Application 9-1
Figure 9-2 Workflow Components 9-2
Figure 9-3 Sample Service Flow 9-9
Figure 9-4 Select a Category 9-11
Figure 9-5 Search Box 9-12
Figure 9-6 Workflow Components 9-15
Figure 9-7 Workflow Validation Report 9-39
Figure 9-8 Detailed Validation Messages 9-39
Figure 9-9 Workflow Evaluation Summary 9-43
Figure 9-10 Workflow Evaluation Details 9-44
Figure 9-11 Object Instance Details 9-45
Figure 9-12 Workflow Comparison Summary 9-48
Figure 9-13 Workflow Comparison Details 9-50
Figure 9-14 Object Instance Details 9-51
Figure 9-15 Workflow Trace – PDN Session 9-53
Figure 9-16 Service Data Flow List 9-55
Figure 9-17 Charging Service Attribute List 9-55
Figure 9-18 Build Out Functions 9-59
Figure 9-19 Search Box 9-60
Figure 9-20 Build a Workflow Functions 9-61
Figure 9-21 Search Box 9-61
Figure 9-22 HTTP Rule Group Components 9-128
Figure 9-23 Service Rule Components 9-159
Figure 9-24 Build Out Functions 9-180
Figure 9-25 User Created Workflow Functions 9-181
Figure 9-26 New Workflow Functions 9-181
Figure 9-27 Charging Components 9-182
Figure 9-28 Content Cache Components 9-190
Figure 9-29 Content Filter Components 9-202
Figure 9-30 Fair Bandwidth Usage Components 9-229
Figure 9-31 HTTP Proxy Components 9-234
Figure 9-32 Multi Protocol Proxy Components 9-275
Figure 9-33 Protocol Application Rule Group Components 9-310
Figure 9-34 Quality of Service Components 9-315
Figure 9-35 Steering Service Components 9-323
Figure 9-36 Subscriber Firewall Service Components 9-326
Figure 9-37 Video Adaptation Components 9-332
Figure 9-38 HTTP Filter File Management 9-347
Figure 10-1 Accessing the Configuration Navigator Application 10-1
Figure 10-2 Configuration Navigator Tree 10-2

Figure 10-3 Search Box 10-4
Figure 10-4 Filtered Instances 10-5
Figure 10-5 Configuration Parameters for Selected Card 10-6
Figure 10-6 Active Alarm Details 10-7
Figure 10-7 Available Alarm 10-7
Figure 10-8 Monitor Interval 10-102
Figure 10-9 Graphic Format 10-102
Figure 10-10 Data Point Details 10-103
Figure 10-11 Graph with Legend 10-103
Figure 10-12 Workflow Components 10-555
Figure 11-1 Log Viewer 11-2
Figure 11-2 Sample Event Log Files 11-3
Figure 11-3 Sample Trace Files 11-9
Figure 11-4 Save Tech Support Information 11-11
Figure 11-5 Recent Changes 11-13
Figure 11-6 Subscriber Group File Management 11-15
Figure 11-7 Subscriber Groups 11-16
Figure 11-8 File List 11-19
Figure 11-9 Configure Siemens SPCRF EMS 11-21
Figure 11-10 Configure HPE HSS EMS 11-22
Figure 11-11 Manage Device Gateway 11-23

List of Tables

Table 1-1	Acuitas Icons	1-22
Table 2-1	Add Network Element Parameters	2-4
Table 2-2	Edit Network Element Parameters	2-8
Table 3-1	CUPS Group Configuration Parameters	3-5
Table 3-2	Common Service-Construct Configuration	3-13
Table 3-3	Common Services Configuration	3-14
Table 3-4	Common Network-Context Configuration	3-16
Table 3-5	Common Workflow Configuration	3-16
Table 3-6	Common Zone Configuration	3-16
Table 3-7	Other Configuration	3-17
Table 3-8	Geographic Redundancy Group Parameters	3-86
Table 3-9	Geographic Redundancy Group Parameters	3-91
Table 3-10	Discovery Mismatch Conditions	3-110
Table 5-1	Changed Default Purging Interval	5-12
Table 5-2	Changed Dashboard Reports	5-12
Table 5-3	Changed Historical Reports	5-12
Table 5-4	Instance Filter Configuration	5-33
Table 5-5	Dashboard Parameters	5-47
Table 6-1	Add Network Element Parameters	6-4
Table 6-2	Add Network Element Parameters	6-8
Table 6-3	Add Network Element Parameters	6-13
Table 6-4	VNF Manager Administration Parameters	6-17
Table 6-5	Manage Host Parameters	6-24
Table 6-6	vCenter Initialization Worksheet	6-27
Table 6-7	vCloud Director Initialization Worksheet	6-35
Table 6-8	OpenStack Initialization Worksheet for MCC	6-39
Table 6-9	OpenStack Initialization Worksheet for MCC MME	6-49
Table 6-10	Cluster Configuration Parameters	6-57
Table 6-11	Cluster Configuration Parameters	6-62
Table 6-12	VM Configuration Parameters	6-73
Table 6-13	Cluster KPIs	6-97
Table 6-14	Network Elasticity Report Fields	6-100
Table 6-15	Network Inventory Report Fields	6-103
Table 6-16	Add Network Element Parameters	6-107
Table 6-17	Add Network Element Parameters	6-108
Table 6-18	Manage Host Parameters	6-110
Table 6-19	Cluster Configuration Parameters	6-111
Table 6-20	Policy Parameters	6-113
Table 6-21	Threshold and Action Parameters	6-114
Table 6-22	Overload/Underload Alarms	6-122
Table 6-23	Scale Out/Scale In Alarms	6-122
Table 7-1	Group Permissions	7-11
Table 7-2	Audit Trail Operations	7-39
Table 9-1	Functions and Services	9-3
Table 9-2	Control Profile Parameters	9-17
Table 9-3	Data Profile Reselection Trigger Template Parameters	9-23
Table 9-4	Subscriber Analyzer Triggers	9-24
Table 9-5	Service Flow Parameters	9-27

Table 9-6 Flow Parameters 9-41
Table 9-7 Flow Parameters 9-45
Table 9-8 Counters 9-52
Table 9-9 ACL List Parameters 9-64
Table 9-10 ACL Filter Parameters 9-64
Table 9-11 ACL Policy Parameters 9-65
Table 9-12 Advice of Charge Parameters 9-66
Table 9-13 Charge Notification Parameters 9-67
Table 9-14 Aoc Hardware ID Format Parameters 9-69
Table 9-15 APN Mapping List Parameters 9-71
Table 9-16 APN Mapping Parameters 9-71
Table 9-17 Application Rule Group Settings 9-74
Table 9-18 Blacklist Filter Parameters 9-104
Table 9-19 DHCP Local Server Profile Parameters 9-105
Table 9-20 DHCP Service Profile Parameters 9-106
Table 9-21 External DHCP Server Parameters 9-107
Table 9-22 DiffServ Profile Class Mapping Parameters 9-109
Table 9-23 DiffServ Profile DSCP Mapping Parameters 9-111
Table 9-24 Domain Rule Group Parameters 9-112
Table 9-25 EDR Server Profile Parameters 9-114
Table 9-26 Encryption Profile Parameters 9-115
Table 9-27 File Download Profile Parameters 9-116
Table 9-28 Filter Database Size Parameters 9-118
Table 9-29 Add Request Cookie Custom String Parameters 9-121
Table 9-30 Add Request Cookie String Parameters 9-122
Table 9-31 Request Header Custom String Parameters 9-122
Table 9-32 Request Header String Parameters 9-124
Table 9-33 Add Response Header String Parameters 9-126
Table 9-34 Rewrite Request Header String Parameters 9-127
Table 9-35 Rule Condition Parameters 9-129
Table 9-36 Rewrite Rule Parameters 9-132
Table 9-37 Insertion Object List Parameters 9-134
Table 9-38 Insertion Object Parameters 9-134
Table 9-39 IP List Parameters 9-136
Table 9-40 IP Address Parameters 9-136
Table 9-41 IP Range Parameters 9-137
Table 9-42 LDAP Server Parameters 9-138
Table 9-43 LDAP Profile Parameters 9-141
Table 9-44 LDAP Feature Group Parameters 9-142
Table 9-45 Multimedia Messaging Service Center Parameters 9-147
Table 9-46 Error Response Parameters 9-149
Table 9-47 User Agent Prefix Parameters 9-150
Table 9-48 MM3 Profile Parameters 9-151
Table 9-49 STI Profile Parameters 9-152
Table 9-50 Packet Filter Parameters 9-153
Table 9-51 QoS Parameters 9-155
Table 9-52 SCTP Profile Parameters 9-157
Table 9-53 Service Rule Parameters 9-160
Table 9-54 Rule Condition Parameters 9-163
Table 9-55 Short Message Service Center Profile Parameters 9-166
Table 9-56 Short Message Service Center Group Parameters 9-167

Table 9-57 Short Message Service Notification Parameters **9-167**
Table 9-58 Static DNS Map Parameters **9-168**
Table 9-59 TCP Optimization Profile Parameters **9-169**
Table 9-60 Time of Day Rule Group Parameters **9-171**
Table 9-61 Rule Condition Parameters **9-172**
Table 9-62 TLS Termination Policy Parameters **9-174**
Table 9-63 Sites Parameters **9-175**
Table 9-64 User Agent Key Parameters **9-176**
Table 9-65 Default User Agent Key Parameters **9-177**
Table 9-66 URL List Parameters **9-179**
Table 9-67 Rating Group Parameters **9-183**
Table 9-68 Billing Plan Parameters **9-187**
Table 9-69 Service Rule Parameters **9-188**
Table 9-70 Charging Instance Parameters **9-189**
Table 9-71 Billing Plan Parameters **9-189**
Table 9-72 Content Cache Service Parameters **9-191**
Table 9-73 Service Rule Parameters **9-192**
Table 9-74 Online Categories **9-195**
Table 9-75 Content Categorization Parameters **9-203**
Table 9-76 IWF Category Parameters **9-205**
Table 9-77 Malware Category Parameters **9-206**
Table 9-78 Online Category Parameters **9-207**
Table 9-79 Phishing Parameters **9-208**
Table 9-80 Filter Hash List Parameters **9-208**
Table 9-81 Service Rule Parameters **9-209**
Table 9-82 Static Category Parameters **9-211**
Table 9-83 Safe Search Parameters **9-212**
Table 9-84 Static Category Parameters **9-213**
Table 9-85 Content HTTP Server Instance Parameters **9-214**
Table 9-86 Content Insertion Profile Parameters **9-217**
Table 9-87 Banner Parameters **9-217**
Table 9-88 Overlay Parameters **9-217**
Table 9-89 Range Parameters **9-218**
Table 9-90 DNS Proxy Parameters **9-221**
Table 9-91 DNS Proxy Instance Parameters **9-221**
Table 9-92 DNS Policy Parameters **9-222**
Table 9-93 Configuration Guidelines for Policy Action **9-223**
Table 9-94 DNS Reverse Cache Parameters **9-225**
Table 9-95 DNS IP Flow Parameters **9-226**
Table 9-96 Domain Tunnel Age Time Parameters **9-227**
Table 9-97 Tunnel Detection Profile Parameters **9-228**
Table 9-98 Fair Bandwidth Usage Parameters **9-229**
Table 9-99 Shortcut Keys to Load Unoptimized Content **9-232**
Table 9-100 HTTP Proxy Parameters **9-235**
Table 9-101 HTTP Request Policy Parameters **9-238**
Table 9-102 HTTP Response Policy Parameters **9-241**
Table 9-103 HTTP IP Flow Parameters **9-243**
Table 9-104 Encryption Profile Parameters **9-245**
Table 9-105 HTTP Proxy Instance Parameters **9-246**
Table 9-106 Server Connections Parameters **9-248**
Table 9-107 ABR Optimization Profile Parameters **9-249**

Table 9-108 Explicit Proxy Address Parameters **9-251**
Table 9-109 Fraud Detection Profile Parameters **9-252**
Table 9-110 HTTPS Profile Parameters **9-255**
Table 9-111 HTTP Transaction Record Profile Parameters **9-257**
Table 9-112 LTMI Parameters **9-259**
Table 9-113 Steering GW Parameters **9-260**
Table 9-114 TCP Splicing Policy Parameters **9-261**
Table 9-115 TCP Splicing Profile Parameters **9-262**
Table 9-116 Toll Free Profile Parameters **9-265**
Table 9-117 Web Image Optimization Profile Parameters **9-266**
Table 9-118 HTTP Server Entitlement Service Parameters **9-269**
Table 9-119 HTTP Server Parameters **9-270**
Table 9-120 Metering Instance Parameters **9-271**
Table 9-121 Shortcut Keys to Load Unoptimized Content **9-273**
Table 9-122 Multi Protocol Proxy Parameters **9-276**
Table 9-123 HTTP Request Policy Parameters **9-279**
Table 9-124 HTTP Response Policy Parameters **9-282**
Table 9-125 IP Flow Parameters **9-284**
Table 9-126 Encryption Profile Parameters **9-286**
Table 9-127 Instance Parameters **9-287**
Table 9-128 Server Connections Parameters **9-290**
Table 9-129 ABR Optimization Profile Parameters **9-290**
Table 9-130 Explicit Proxy Address Parameters **9-292**
Table 9-131 Fraud Detection Profile Parameters **9-293**
Table 9-132 HTTPS Profile Parameters **9-296**
Table 9-133 HTTP Transaction Record Profile Parameters **9-298**
Table 9-134 LTMI Parameters **9-300**
Table 9-135 Steering GW Parameters **9-301**
Table 9-136 TCP Splicing Policy Parameters **9-302**
Table 9-137 Traffic Control Profile Parameters **9-303**
Table 9-138 Toll Free Profile Parameters **9-306**
Table 9-139 Web Image Optimization Profile Parameters **9-307**
Table 9-140 Protocol Application Rule Group Parameters **9-311**
Table 9-141 QoS Flow Parameters **9-316**
Table 9-142 QoS Policy Parameters **9-319**
Table 9-143 Qci Dscp Map Parameters **9-320**
Table 9-144 Realm List Parameters **9-321**
Table 9-145 SMTP Proxy Instance Parameters **9-322**
Table 9-146 Steering Flow Parameters **9-324**
Table 9-147 Steering Policy Parameters **9-325**
Table 9-148 Subscriber Firewall Flow Parameters **9-327**
Table 9-149 Subscriber Firewall Policy Parameters **9-329**
Table 9-150 Video Adaptation Service Parameters **9-333**
Table 9-151 Offline Transcoding Parameters **9-335**
Table 9-152 Online Transcoding Parameters **9-335**
Table 9-153 Transcoding Policy Parameters **9-336**
Table 9-154 Serving Policy Parameters **9-337**
Table 9-155 Transcoding Map Parameters **9-338**
Table 9-156 Transcoding Rule Parameters **9-341**
Table 9-157 Transcoding Policy Parameters **9-342**
Table 9-158 WAP Gateway Instance Parameters **9-344**

Table 9-159 WAP IP Flow Parameters **9-345**
Table 9-160 URL List Parameters **9-348**
Table 9-161 URL List Parameters **9-349**
Table 9-162 Category Parameters **9-350**
Table 9-163 Category Parameters **9-351**
Table 10-1 Cluster Parameters **10-8**
Table 10-2 Personalities **10-12**
Table 10-3 Control Plane Protection Child Objects and Parameters **10-16**
Table 10-4 Data Plane Protection Parameters **10-17**
Table 10-5 Data Plane Protection Child Objects and Parameters **10-18**
Table 10-6 GNP Sub Pool Parameters **10-20**
Table 10-7 Node Parameters **10-21**
Table 10-8 Node Child Objects and Parameters **10-23**
Table 10-9 RAMDISK Parameters **10-26**
Table 10-10 Data Path Child Objects and Parameters **10-29**
Table 10-11 Throttle Limit Parameters **10-31**
Table 10-12 Geographic Redundancy Parameters **10-33**
Table 10-13 Image Management Card Status Parameters **10-44**
Table 10-14 Image Management Release Modifier Status Parameters **10-45**
Table 10-15 Image Management Status Parameters **10-45**
Table 10-16 Dynamic Scale Parameters **10-47**
Table 10-17 Mgmt Ip Parameters **10-49**
Table 10-18 Data File Management Profile Parameters **10-50**
Table 10-19 Event Log Policy Parameters **10-56**
Table 10-20 Event Log Policy Child Objects and Parameters **10-56**
Table 10-21 System Log Policy Parameters **10-59**
Table 10-22 OOM Parameters **10-61**
Table 10-23 Memory Limit Parameters **10-62**
Table 10-24 Profile Parameters **10-63**
Table 10-25 Pacer Parameters **10-64**
Table 10-26 BFD Timer Profile Parameters **10-69**
Table 10-27 BFD Instance Parameters **10-69**
Table 10-28 BFD Instance Child Objects and Parameters **10-70**
Table 10-29 BGP Router Parameters **10-71**
Table 10-30 BGP Router Child Objects and Parameters **10-72**
Table 10-31 BGP VPN Router Parameters **10-79**
Table 10-32 BGP VPN Router Child Objects and Parameters **10-80**
Table 10-33 Nat to UE Binding Parameters **10-90**
Table 10-34 UE to Nat Binding Parameters **10-90**
Table 10-35 NSM Parameters **10-91**
Table 10-36 Router Parameters **10-91**
Table 10-37 Restart Response Child Objects and Parameters **10-92**
Table 10-38 Router Parameters **10-93**
Table 10-39 Policy Child Objects and Parameters **10-93**
Table 10-40 TCP Parameters **10-97**
Table 10-41 Auto Tuning Recv Buffer Parameters **10-99**
Table 10-42 Auto Tuning Send Buffer Parameters **10-99**
Table 10-43 Network Context Parameters **10-104**
Table 10-44 Network Context Child Objects **10-105**
Table 10-45 Neighbor Discovery Profile Parameters **10-109**
Table 10-46 install Command Parameters **10-112**

Table 10-47 remove Command Parameters **10-115**
Table 10-48 update Command Parameters **10-116**
Table 10-49 IPSec Security Tunnel Configuration Guidelines **10-118**
Table 10-50 Security Parameters **10-119**
Table 10-51 Domain Parameters **10-119**
Table 10-52 PKI Certificate Management Parameters **10-120**
Table 10-53 Remote Secret Parameters **10-121**
Table 10-54 Tunnel Parameters **10-122**
Table 10-55 IKE Transform Parameters **10-125**
Table 10-56 IPSec Transform Parameters **10-126**
Table 10-57 Manual Key Parameters **10-127**
Table 10-58 Local Identity Parameters **10-127**
Table 10-59 Remote Identity Parameters **10-128**
Table 10-60 Rule Parameters **10-128**
Table 10-61 Source Packet Filter Parameters **10-130**
Table 10-62 Destination Packet Filter Parameters **10-131**
Table 10-63 History Parameters **10-133**
Table 10-64 Network Context Statistics Parameters **10-134**
Table 10-65 Rule Statistics Parameters **10-135**
Table 10-66 Service Constructs **10-136**
Table 10-67 ACL Filter Parameters **10-143**
Table 10-68 HTTP Parameters **10-144**
Table 10-69 Charging Notification List Parameters **10-145**
Table 10-70 Aoc Hardware ID Format Parameters **10-146**
Table 10-71 Application Rule Group Settings **10-148**
Table 10-72 Code Mapping Lists Parameters **10-177**
Table 10-73 Insertion Object List Parameters **10-178**
Table 10-74 Insertion Object Parameters **10-179**
Table 10-75 Content Insertion Profile Parameters **10-179**
Table 10-76 Banner Parameters **10-180**
Table 10-77 Overlay Parameters **10-180**
Table 10-78 Device Database Parameters **10-183**
Table 10-79 DHCP Local Server Profile Parameters **10-186**
Table 10-80 Attribute Parameters **10-188**
Table 10-81 Policy Parameters **10-192**
Table 10-82 DHCP Service Profile Parameters **10-195**
Table 10-83 DSCP Mapping Parameters **10-197**
Table 10-84 Class Mapping Parameters **10-198**
Table 10-85 Rule Condition Parameters **10-200**
Table 10-86 EDR Flow Network Stats Profile Parameters **10-201**
Table 10-87 EDR Interface Profile Parameters **10-202**
Table 10-88 EDR Service Profile Parameters **10-202**
Table 10-89 Record Info Parameters **10-203**
Table 10-90 Record Type Parameters **10-209**
Table 10-91 EDR Server Profile Parameters **10-211**
Table 10-92 EDR Session Data Stats Profile Parameters **10-212**
Table 10-93 Encryption Profile Parameters **10-213**
Table 10-94 Event Trigger Template Parameters **10-215**
Table 10-95 File Download Profile Parameters **10-217**
Table 10-96 Flow Idle Timeout Filter Parameters **10-220**
Table 10-97 Flow Idle Timeout Rule Parameters **10-220**

Table 10-98 Geo Redundancy Server Parameters **10-221**
Table 10-99 Gy Event Trigger Template Parameters **10-224**
Table 10-100 Gy Event Trigger Template Parameters **10-224**
Table 10-101 Request Header String Parameters **10-227**
Table 10-102 Request Header Custom String Parameters **10-230**
Table 10-103 Add Request Cookie String Parameters **10-232**
Table 10-104 Add Request Cookie Custom String Parameters **10-232**
Table 10-105 Add Response Header String Parameters **10-232**
Table 10-106 Remove Header String Parameters **10-233**
Table 10-107 Rewrite Request Header String Parameters **10-233**
Table 10-108 Rule Condition Parameters **10-234**
Table 10-109 HTTP Server Parameters **10-237**
Table 10-110 Rewrite Rule Parameters **10-239**
Table 10-111 IMSI Range Parameters **10-241**
Table 10-112 IMSI Range List Parameters **10-242**
Table 10-113 Accounting Service Parameters **10-243**
Table 10-114 Rg Quota List to Report Parameters **10-247**
Table 10-115 Authorization Service Parameters **10-248**
Table 10-116 Flow Authorization Interface Parameters **10-251**
Table 10-117 Flow Authorization Diameter Interface Parameters **10-252**
Table 10-118 RADIUS Proxy Parameters **10-253**
Table 10-119 Server Group Mapping Parameters **10-253**
Table 10-120 RADIUS Server Parameters **10-254**
Table 10-121 RADIUS Server Parameters **10-255**
Table 10-122 TWAG Inband Authentication Parameters **10-255**
Table 10-123 DHCP Trigger Tunnel Interface Parameters **10-256**
Table 10-124 VLAN Parameters **10-256**
Table 10-125 TWAG RADIUS Client Parameters **10-257**
Table 10-126 DHCP Mapping Parameters **10-258**
Table 10-127 DHCP Trigger Tunnel Interface Parameters **10-258**
Table 10-128 RADIUS Client Parameters **10-259**
Table 10-129 RADIUS Mapping Parameters **10-259**
Table 10-130 GiGw LDAP Client Parameters **10-260**
Table 10-131 GiGw IP Local Parameters **10-260**
Table 10-132 Non 3gpp Access Diameter Client Parameters **10-260**
Table 10-133 Server Group Mapping Parameters **10-261**
Table 10-134 Server Group Parameters **10-262**
Table 10-135 IPMS Server Parameters **10-262**
Table 10-136 APV Flags Parameters **10-265**
Table 10-137 Diameter Node Admin Parameters **10-266**
Table 10-138 Peer Parameters **10-269**
Table 10-139 Diameter Node Status Parameters **10-271**
Table 10-140 Peer Command Status Parameters **10-271**
Table 10-141 Peer Statistics Parameters **10-272**
Table 10-142 Peer Status Parameters **10-273**
Table 10-143 GTPP Node Admin Parameters **10-275**
Table 10-144 GA Record Version Parameters **10-276**
Table 10-145 Peer Parameters **10-276**
Table 10-146 GTPP Node Status Parameters **10-278**
Table 10-147 Peer Command Status Parameters **10-278**
Table 10-148 Peer Statistics Parameters **10-280**

Table 10-149 Peer Status Parameters **10-281**
Table 10-150 Server Group Parameters **10-283**
Table 10-151 Peer Parameters **10-286**
Table 10-152 RADIUS Service Procedure Statistics Parameters **10-288**
Table 10-153 Server Group Peer Status Parameters **10-289**
Table 10-154 Server Group Status Parameters **10-290**
Table 10-155 Server Group Peer Status Parameters **10-290**
Table 10-156 Server Parameters **10-291**
Table 10-157 Client Parameters **10-292**
Table 10-158 Offline Charging Parameters **10-294**
Table 10-159 Online Charging Parameters **10-304**
Table 10-160 PCRF Charging Parameters **10-314**
Table 10-161 Policy Server Interface Parameters **10-321**
Table 10-162 Port NBR Local Parameters **10-322**
Table 10-163 Rx Interface Parameters **10-323**
Table 10-164 S6b Interface Parameters **10-323**
Table 10-165 Diameter Interface Parameters **10-324**
Table 10-166 IP List Parameters **10-326**
Table 10-167 IP Address Parameters **10-326**
Table 10-168 IP Range Parameters **10-326**
Table 10-169 LDAP Remote Server Parameters **10-327**
Table 10-170 LDAP Feature Group Parameters **10-328**
Table 10-171 LDAP Profile Parameters **10-330**
Table 10-172 Multimedia Messaging Service Center Parameters **10-336**
Table 10-173 MM3 Profile Parameters **10-338**
Table 10-174 Default Error Response Parameters **10-339**
Table 10-175 User Agent Prefix Parameters **10-339**
Table 10-176 STI Profile Parameters **10-340**
Table 10-177 Network Profile Parameters **10-341**
Table 10-178 Packet Filter Parameters **10-342**
Table 10-179 Home List Parameters **10-344**
Table 10-180 Roaming List Parameters **10-344**
Table 10-181 Protocol Application Rule Group Parameters **10-346**
Table 10-182 Quality of Service Parameters **10-350**
Table 10-183 Attribute Parameters **10-351**
Table 10-184 Realm List Parameters **10-355**
Table 10-185 Realm Parameters **10-355**
Table 10-186 SCTP Profile Parameters **10-356**
Table 10-187 Service Rule Parameters **10-357**
Table 10-188 Rule Condition Parameters **10-361**
Table 10-189 Short Message Service Center Profile Parameters **10-363**
Table 10-190 Short Message Service Notification Parameters **10-364**
Table 10-191 Static DNS Map Parameters **10-365**
Table 10-192 Host Parameters **10-365**
Table 10-193 Subscriber Group Parameters **10-366**
Table 10-194 TCP Optimization Profile Parameters **10-367**
Table 10-195 Time of Day Rule Group Parameters **10-369**
Table 10-196 Rule Condition Parameters **10-370**
Table 10-197 TLS Termination Policy Parameters **10-371**
Table 10-198 Sites Parameters **10-371**
Table 10-199 User Agent Key Parameters **10-372**

Table 10-200 UA Profile Default Parameters **10-372**
Table 10-201 URL List Parameters **10-373**
Table 10-202 Services **10-378**
Table 10-203 ACL Network Context Parameters **10-382**
Table 10-204 Rating Group Parameters **10-383**
Table 10-205 Billing Plan Parameters **10-387**
Table 10-206 Service Rule Parameters **10-388**
Table 10-207 Charging Instance Parameters **10-388**
Table 10-208 Billing Plan Parameters **10-389**
Table 10-209 Content Cache Service Parameters **10-391**
Table 10-210 Eviction Threshold Disk Parameters **10-391**
Table 10-211 Eviction Threshold Memory Parameters **10-392**
Table 10-212 Service Rule Parameters **10-393**
Table 10-213 Online Categories **10-396**
Table 10-214 Static Category Parameters **10-403**
Table 10-215 Content Categorization Parameters **10-404**
Table 10-216 Malware Category Parameters **10-405**
Table 10-217 Filter Database Size Parameters **10-406**
Table 10-218 Black List Parameters **10-407**
Table 10-219 White List Parameters **10-409**
Table 10-220 Black List Parameters **10-410**
Table 10-221 Category Parameters **10-411**
Table 10-222 Malware Category Parameters **10-411**
Table 10-223 Online Category Parameters **10-413**
Table 10-224 Phishing Parameters **10-414**
Table 10-225 Service Rule Map Parameters **10-414**
Table 10-226 Static Category Parameters **10-416**
Table 10-227 Filter Hash List Parameters **10-417**
Table 10-228 Safe Search Parameters **10-418**
Table 10-229 CRBN Profile Parameters **10-421**
Table 10-230 DNS Proxy Parameters **10-422**
Table 10-231 DNS IP Flow Parameters **10-423**
Table 10-232 DNS Policy Parameters **10-424**
Table 10-233 Configuration Guidelines for Policy Action **10-425**
Table 10-234 DNS Reverse Cache Parameters **10-426**
Table 10-235 DNS Proxy Instance Parameters **10-427**
Table 10-236 Domain Clean Time Parameters **10-429**
Table 10-237 Tunnel Detection Profile Parameters **10-430**
Table 10-238 Fair Bandwidth Usage Parameters **10-431**
Table 10-239 Shortcut Keys to Load Unoptimized Content **10-434**
Table 10-240 HTTP Proxy Parameters **10-435**
Table 10-241 HTTP Request Policy Parameters **10-436**
Table 10-242 Minify Parameters **10-438**
Table 10-243 HTTP Response Policy Parameters **10-439**
Table 10-244 HTTP Proxy IP Flow Parameters **10-440**
Table 10-245 HTTP Proxy Instance Parameters **10-442**
Table 10-246 ABR Optimization Profile Parameters **10-445**
Table 10-247 Encryption Profile Parameters **10-448**
Table 10-248 Explicit Proxy Address Parameters **10-449**
Table 10-249 Fraud Detection Profile Parameters **10-450**
Table 10-250 HTTP Transaction Record Profile Parameters **10-452**

Table 10-251 HTTPS Profile Parameters **10-454**
Table 10-252 LTMI Parameters **10-455**
Table 10-253 Preemptive DNS Parameters **10-459**
Table 10-254 Server Connections Parameters **10-459**
Table 10-255 Steering Destination Parameters **10-460**
Table 10-256 TCP Splicing Policy Parameters **10-461**
Table 10-257 Certificate Server Parameters **10-462**
Table 10-258 Data Record Configuration Parameters **10-463**
Table 10-259 TF Header Names Parameters **10-464**
Table 10-260 Traffic Control Profile Parameters **10-464**
Table 10-261 UDP Parameters **10-466**
Table 10-262 UDP Policy Parameters **10-467**
Table 10-263 Web Image Optimization Profile Parameters **10-468**
Table 10-264 HTTP Server Service Instance Parameters **10-470**
Table 10-265 Network Context Parameters **10-470**
Table 10-266 Content Insertion Parameters **10-471**
Table 10-267 Entitlement Service Parameters **10-473**
Table 10-268 HTTP Server Parameters **10-473**
Table 10-269 Metering Service Instance Parameters **10-475**
Table 10-270 Shortcut Keys to Load Unoptimized Content **10-478**
Table 10-271 Multi Protocol Proxy Parameters **10-479**
Table 10-272 HTTP Request Policy Parameters **10-480**
Table 10-273 Minify Parameters **10-482**
Table 10-274 HTTP Response Policy Parameters **10-483**
Table 10-275 IP Flow Parameters **10-484**
Table 10-276 Multi Protocol Proxy Instance Parameters **10-487**
Table 10-277 ABR Optimization Profile Parameters **10-490**
Table 10-278 Encryption Profile Parameters **10-492**
Table 10-279 Explicit Proxy Address Parameters **10-493**
Table 10-280 Fraud Detection Profile Parameters **10-494**
Table 10-281 HTTP Transaction Record Profile Parameters **10-496**
Table 10-282 HTTPS Profile Parameters **10-498**
Table 10-283 LTMI Parameters **10-499**
Table 10-284 Preemptive DNS Parameters **10-503**
Table 10-285 Server Connections Parameters **10-503**
Table 10-286 Steering Destination Parameters **10-504**
Table 10-287 TCP Splicing Policy Parameters **10-505**
Table 10-288 Certificate Server Parameters **10-506**
Table 10-289 Data Record Configuration Parameters **10-507**
Table 10-290 TF Header Names Parameters **10-508**
Table 10-291 Traffic Control Profile Parameters **10-508**
Table 10-292 UDP Parameters **10-510**
Table 10-293 UDP Policy Parameters **10-511**
Table 10-294 Web Image Optimization Profile Parameters **10-512**
Table 10-295 QoS Flow Parameters **10-514**
Table 10-296 QoS Policy Parameters **10-516**
Table 10-297 Qci Dscp Map Parameters **10-518**
Table 10-298 Rate Limiting Subscriber Group Parameters **10-519**
Table 10-299 SMTP Proxy Instance Parameters **10-520**
Table 10-300 Network Context Parameters **10-520**
Table 10-301 Steering Flow Parameters **10-521**

Table 10-302 Steering Policy Parameters **10-523**
Table 10-303 Subscriber Firewall Flow Parameters **10-524**
Table 10-304 Subscriber Firewall Policy Parameters **10-526**
Table 10-305 Video Adaptation Service Parameters **10-529**
Table 10-306 Offline Transcoding Parameters **10-531**
Table 10-307 Online Transcoding Parameters **10-531**
Table 10-308 Offline Transcoding Parameters **10-532**
Table 10-309 Serving Policy Parameters **10-532**
Table 10-310 Transcoding Policy Parameters **10-533**
Table 10-311 Transcoding Policy Parameters **10-533**
Table 10-312 Transcoding Map Entry Parameters **10-536**
Table 10-313 Transcoding Rule Parameters **10-538**
Table 10-314 WAP Gateway Instance Parameters **10-540**
Table 10-315 WTLS Parameters **10-540**
Table 10-316 WAP IP Flow Parameters **10-541**
Table 10-317 Community Entry Parameters **10-542**
Table 10-318 User Parameters **10-543**
Table 10-319 TAM Parameters **10-544**
Table 10-320 TAM Profile Parameters **10-544**
Table 10-321 Loopback IP Parameters **10-545**
Table 10-322 TIP Subpool Parameters **10-545**
Table 10-323 Admin Parameters **10-547**
Table 10-324 TACACS+ Server Parameters **10-547**
Table 10-325 Remote Exclude Parameters **10-548**
Table 10-326 Allow Local Parameters **10-549**
Table 10-327 Remote Exclude Parameters **10-549**
Table 10-328 Timers Parameters **10-550**
Table 10-329 Sink Config Parameters **10-551**
Table 10-330 Packet Metadata Parameters **10-551**
Table 10-331 Key Parameters **10-552**
Table 10-332 Range Parameters **10-553**
Table 10-333 Subscriber Tap Parameters **10-553**
Table 10-334 APN Mapping List Parameters **10-556**
Table 10-335 APN Mapping Parameters **10-556**
Table 10-336 Workflow Control Profile Parameters **10-557**
Table 10-337 Data Profile Parameters **10-565**
Table 10-338 Data Profile Reselection Trigger Template Parameters **10-568**
Table 10-339 Subscriber Analyzer Parameters **10-569**
Table 10-340 Key Parameters **10-570**
Table 10-341 Zone Child Objects **10-574**
Table 11-1 Subscriber Group Parameters **11-17**
Table 11-2 Subscriber Group Parameters **11-17**
Table A-1 LDAP Authentication Parameters **A-9**
Table A-2 Alarm Detail **A-18**
Table A-3 HP Blade System Enclosure iLO Traps **A-26**
Table A-4 HP Blade iLO Traps **A-30**
Table A-5 VMware Traps **A-32**
Table A-6 Mapped VMware ESXi Traps **A-33**
Table A-7 VMware ESXi Trap Variable Bindings **A-34**
Table A-8 Forwarded Traps **A-38**
Table A-9 vpxdAlarmInfo Trap Variable Bindings **A-44**

Table A-10 vCenter Trap Variable Bindings **A-45**
Table A-11 Add Network Element Parameters **A-47**
Table A-12 alertNotify Trap Variable Bindings **A-49**
Table A-13 HPE HHS Traps **A-51**
Table A-14 RTMS Event Trap Variable Bindings and Event Mappings **A-51**
Table A-15 VERTICA Traps **A-53**
Table A-16 VERTICA Database Trap Variable Bindings and Event Log Mappings **A-55**
Table A-17 Transformed Tables **A-58**
Table A-18 Exported KPI Filenames and Contents **A-59**
Table A-19 VIM Management APIs **A-67**
Table A-20 Cluster Configuration Management APIs **A-78**
Table A-21 Cluster Configuration Attributes (R = Required, A = Applicable) **A-79**
Table A-22 Node Configuration Attributes (R = Required, A = Applicable). **A-82**
Table A-23 Lifecycle Management APIs **A-119**
Table A-24 Dynamic Scaling APIs **A-143**
Table A-25 MCC Configuration APIs **A-150**
Table A-26 Network Configuration APIs **A-154**
Table A-27 Security Group APIs **A-167**
Table A-28 Security User APIs **A-178**
Table B-1 Derived Metrics **B-1**
Table B-2 Raw Metrics **B-41**

Preface

This document describes how to use the Acuitas Service Management System to perform tasks, such as adding Network Elements and using Topology, Configuration, Fault, Performance, Virtual Network Function Manager, Security, Tools, Workflow, and Configuration Navigator applications.

Note: *The Affirmed Networks Mobile Content Cloud™ is the mobile services software solution that operates on virtual platforms such as blade systems.*

Audience

This guide is written for the Operator who runs Acuitas to manage Affirmed Networks network elements. As a reader of this guide, you should be familiar with network management tasks such as configuring network components, managing services, managing network faults, and monitoring network performance. You should be familiar with the configuration of long-term evolution (LTE) and 3G or 4G networks.

Release Information

See the Release Notes for important information, requirements, limitations, and restrictions that apply to this release.

How to Use This Guide

This guide contains the following chapters and appendices:

Chapter/Appendix	Describes
Chapter 1, Getting Started	Basic tasks such as navigating the system and accessing information about network objects.
Chapter 2, Topology	Using the Topology applications to build a physical and logical topological model of the network.
Chapter 3, Configuration	Using the Configuration applications to manage Control and User Plane Separation (CUPS) MCC devices, software releases, schedules, templates, file servers, audit trail, Geographic Redundancy groups, and configuration export.
Chapter 4, Fault	Using the Fault applications to manage network alarms and events.
Chapter 5, Performance	Using the Performance applications to monitor performance data.
Chapter 6, VNF Manager	Using the Virtual Network Function (VNF) Manager to control and monitor virtualized MCC clusters in real-time.
Chapter 7, Security	Using the Security applications to control and monitor user access to the network through user authentication, user authorization, and user privileges.
Chapter 8, Tools	Using the Tools application to manage database backups and configure alarm severity color settings.
Chapter 9, Affirmed Open Workflow	Using the Affirmed Open Workflow application to define the treatment of a service flow across various services offered by the network element.
Chapter 10, Configuration Navigator	Using the Configuration Navigator application to configure parameters on the network element.
Chapter 11, Network Element	Using Acuitas to monitor the network element.
Appendix A, Interfacing with Northbound Interfaces	Interfacing with northbound interfaces, such as to OSS systems.
Appendix B, Key Performance Indicators (KPIs) Metrics	Key Performance Indicators (KPIs) Metrics

Features in this Release

This release includes the following new features:

Note: *For a complete list of the new features supported in this release, see the release notes. In addition to the information in this guide, see the additional Affirmed Networks documentation listed in the Affirmed Networks Documentation Library. For a comprehensive list of terms and acronyms used in Affirmed Networks documentation, see Affirmed Networks Terms and Acronyms.*

Feature	Description

OSPF route summarization
See the *Affirmed Networks System Administration Guide.*
	Added the **summary** command to create an aggregate address to replace a series of more specific addresses. The metric used to advertise the summary is the smallest metric of the more specific routes. This command helps to reduce the size of the routing table.
	Configure MCC to advertise one external route as an aggregate for all loopbacks or UE sub-pools that are covered by the address. The summary command supports the following options:
	■ ip-prefix – IP prefix designated for a range of addresses, including the prefix length. Specify the ip-prefix as an IP address. Specify the length as a number from 1 to 31. For example, 49.1.1.0/24
	■ not-advertise – (Optional) When set to false, suppresses routes that match the specified prefix/length pair.
	■ tag – (Optional) Specify the tag value that is used in the summary route being advertised. The range is 1 to 65535.
	`an3000-mcm-slot7cpu1(config-router-temp)# summary 49.1.1.0/24`
	`an3000-mcm-slot7cpu1(config-summary-49.1.1.0/24)# ?`
	`Possible completions:`
	`not-advertise  Do not advertise when translating OSPF type-7 LSA`
	`tag  Set tag`
	
	`an3000-mcm-slot7cpu1(config-router-temp)# show full-configuration`
	`ip-protocols`
	`ospfv2`
	`router temp`
	`:`
	`:`
	`summary 49.1.1.0/24`
	`not-advertise false`

Feature	Description
Gx interface support for Application Detection and Control (ADC)	This feature adds support for Application Detection and Control (ADC) on the Gx interface. The ADC function enables the PGW to detect applications and send notifications to the Policy and Charging Rules Function (PCRF) with application identifiers, flow information, and application Start/Stop events. Based on the PGW-reported information, the PCRF can install, remove, or modify PCC or ADC rules, and the PGW can perform service control, charging, and bearer management (bearer creation, update, and deletion) based on new PCC/ADC rules. The PGW supports the TDF-Application-Identifier AVP in the Charging-Rule-Definition and Adc-Rule Definition AVPs for dynamic PCC rules. The TDF-Application-Identifier identifies an application of the ADC or PCC rule and enables the service-rule for reporting of application Start/Stop notifications to the PCRF. ■ For predefined and dynamic rules, the TDF-Application-Identifier is included when the PGW reports application Start/Stop notifications for traffic matching these rules. The PGW dynamically assigns the TDF-Application-Instance-Identifier to allow correlation of application Start/Stop events. ■ If the TDF-Application-Identifier is not configured or sent by the PCRF, the application Start/Stop notifications are not enabled for the service-rule. If any rule activation fails, the PGW generates a Credit-Control-Request (CCR) with the Charging/Adc-Rule-Report AVP, depending on whether the rule install came through the Charging/Adc-Rule-Install AVP. To configure the TDF-Application-Identifier: `an3000-mcm-slot7cpu1(config)# service-construct service-rule <name> tdf-application-id <name>`
Support for extracting information from the Trusted WLAN IPv4 Parameters IE received on the S2a interface and sending it in the DHCP Offer message See the *Affirmed Networks TWAG/TWAP Administration Guide* and the *Affirmed Networks Gateway Administration Guide*.	When the TWAG/TWAP receives a Create Session Response message on the S2a interface containing the Trusted WLAN IPv4 Parameters IE, the TWAG/TWAP extracts the Subnet Prefix Length & IPv4 Default Router Address, contained within the Trusted WLAN IPv4 Parameters IE, and sends this information as part of the Subnet Mask Option (1) and Router Option (3) in the DHCP Offer message.

Feature	Description
MCC Statistics for Diameter Result Codes on Gx and Gy Interface	This feature supports the ability of the Packet Data Network Gateway (PGW) to dynamically capture and use cluster-level Diameter result code statistics for each message type (i.e., CCA-I, CCA-U, CCA-T) for Gx and Gy peers in each node. These result code statistics for each peer will be registered dynamically as they are received from the Online Charging System (OCS) and Policy and Charging and Rules Function (PCRF). To display Diameter result code statistics: **`show service-construct interface aaa-interface-group diameter statistics cluster-level peer result-code-statistics IntfType nodeName peerName resultCode`** where: ■ ***`IntfType`*** - specifies the interface type. ■ ***`nodeName`*** - specifies the name of the node. ■ ***`peerName`*** - specifies the peer name. ■ ***`resultCode`*** - specifies the result code received from the OCS/PCRF. To clear Diameter result code statistics: **`service-construct interface aaa-interface-group diameter statistics cluster-level peer result-code-statistics IntfType nodeName peerName resultCode clear`** ***Note:*** *If a non-redundant Control/Content Services Module (CSM) reboots, the PGW may delete the result code statistics table.*

Feature	Description
Added delay timer for LTE to Wi-Fi (non-3GPP) handovers See the *Affirmed Networks Gateway Administration Guide*.	When a handover is initiated from 3GPP to non-3GPP, packets are occasionally dropped due to a delay of IPSEC establishment between the ePDG and UE. This may result in a few seconds of service interruption. This feature enables Operators to control the handoff completion (that is, when to send a Delete Bearer Request (DBR) to the 3GPP tunnel). In other words, this feature enables Operators to delay the DBR to the 3GPP tunnel until after the MCC receives the first uplink packet on the non-3GPP tunnel, or until a configured timer expires (whichever occurs first). During a handover delay, MCC continues to send downlink packets on the 3GPP tunnel and receive and process uplink packets from both 3GPP and non-3GPP tunnels. This configuration is supported for non-CUPS and CUPS non-standard interface deployments, however, this timer is not supported for a CUPS standard PFCP interface. To configure the handover delay timer: **`zone default gateway apn 3gpp-to-non3gpp-handover-delay <value>`** where: **`<value>`** - specifies the amount of time to delay (0 to 5000 ms) (default is 0) ***Note:*** *Changes to the* ***3gpp-to-non3gpp-handover-delay*** *value apply to new handovers only.* ***Note:*** *A value of* ***0*** *indicates that existing behavior remains active (that is, sending a DBR on an LTE bearer immediately after sending Create Session Response to ePDG or TWAG).* To display statistics associated with the handover delay timer: **`show zone default gateway statistics cluster-level call-performance [pgw|apn]`** ***Note:*** *For more information about the associated statistic, see the following tables in Acuitas Performance Statistics: APNCALLPERFSTATSGRID, APNCALLPERFSTATSCHASSIS, APNCALLPERFSTATSSLOT, PGWCALLPERFSTATSGRID, PGWCALLPERFSTATSCHASSIS and PGWCALLPERFSTATSSLOT.*

Feature	Description

Added support for the RC4MD5 encryption standard in HHE request/response headers
See the *Affirmed Networks Value Added Services Guide*.
	Added support for the RC4MD5 encryption standard in HHE request/response headers. RC4MD5 is a stream cipher symmetric key encryption standard. The current implementation of RC4MD5 uses a 128 bit key value length and supports both the hex and base64 encoding format.
	Configure the RC4MD5 standard in the encryption-profile as follows:
	`an3000-mcm-slot8cpu1(config)# service-construct encryption-profile <profile-name>`
	`Possible completions:`
	`admin-state  Enable/Disable encryption profile`
	`aes-128-cbc  Encrypted by Advanced Encryption Standard 128-bit Cipher Block Chaining`
	`aes-192-cbc  Encrypted by Advanced Encryption Standard 192-bit Cipher Block Chaining`
	`aes-256-cbc  Encrypted by Advanced Encryption Standard 256-bit Cipher Block Chaining`
	`rc4md5-128  Encrypted by Rivest Cipher 4 128-bit Stream Cipher encryption`
	The key value is converted into a 128 bit format using the MD-5 hashing technique. Configure the RC4MD5 key as follows:
	`an3000-mcm-slot8cpu1(config)# service-construct encryption-profile <profile-name> rc4md5-128 ?`
	`Possible completions:`
	`key  Key for RC4 encryption, please input alphanumeric string of 8 through 15 characters without space`

Feature	Description
ePDG processing of 3xxx/4xxx Error Result Codes See the *Affirmed Networks ePDG Administration Guide*.	This feature supports the ePDG processing of either a 3xxx/4xxx DEA/AAA/STA error **result-code** sent by a primary/secondary AAA server in reply to initial/mid-session SWm request(s). If an ePDG sends SWm request(s) to the primary AAA server and the server is unable to process the request and replies with a 3xxx/4xxx error **result-code**, the ePDG can process the code. If the primary AAA server sends the code, the ePDG retries sending the SWm requests to the secondary AAA server. If the secondary AAA server sends the 3xxx/4xxx code, the ePDG processes the code and terminates the session. When the ePDG receives a 3xxx/4xxx error **result-code** in reply to a SWm request(s) from a AAA server, the ePDG performs the following actions: ■ Determine if the SWm-interface **result-code-policy-list** is configured. ■ Match the response **result-code** with the configured **result-code** range. ■ Determine if the **result-code-policy-list retry-second** is enabled. ■ Determine if the secondary AAA server is available. If all of these conditions are met, the ePDG proceeds with its current action. Otherwise, the ePDG retries according to the retry count configured on the primary AAA server. The following commands are related to configuring/viewing a result-code or result-code-policy-list: ■ To create a list of **result-code** policies: – **service-construct diameter-result-code-policy-list <name>** where: **diameter-result-code-policy-list** — specifies the name of the policy list. ■ To create a **result-code** policy and range of values for it: – **service-construct diameter-result-code-policy-list <*name*> result-code-range [high|low]** where: **diameter-result-code-policy-list** — specifies the name of the result-code policy list. **result-code-range [high|low]** — specifies the range of result-code values. **high** — specifies the highest value for the result-code. **low** — specifies the lowest value for the result-code. – **retry-secondary [enabled|disabled]** where: **enabled** — enables the ePDG to retry sending the request(s) to the secondary AAA server using the SWm interface. **disabled** — disables the ePDG's ability to retry sending the request(s) to the secondary AAA server using the SWm interface. ■ To view a list of result-code policies: **show running-config service-construct diameter-result-code-policy-list** ■ To view the total number of Diameter responses that match the configured **swm-interface result-code-policy-list**: **show zone default gateway statistics grid-level call-performance epdg | include num-responses-matching-result-code-policy-list**

Feature	Description
Deploying RHOSP13 (OSP Queens) Using RHOSP Director on the MCC Using SR-IOV with 25GB NICs	This feature validates and documents the deployment process of Red Hat OpenStack Platform 13 (RHOSP13) (OpenStack Queens) using RHOSP Director on the MCC using SR-IOV with HPE/Mellanox 25GB and Dell/Intel Fortville 25GB NICs.
Upgrade Path from RHOSP10 Director SR-IOV EW/NS to RHOSP13/RHEL7.5 (Queens) Director SR-IOV EW/NS	This feature validates and documents the deployment process of Red Hat OpenStack Platform 10 (RHOSP10) (OpenStack Newton) Director using SR-IOV EW/NS to RHOSP13/RHEL7.5 (OpenStack Queens) Director using SR-IOV EW/NS.
TWAG support for Context-Identifier AVP in Diameter- EAP-Answer (DEA) on STa interface See the *Affirmed Networks TWAG/TWAP Administration Guide*.	The TWAG now processes the Context-Identifier AVP when received from the AAA server in the DEA message over the STa interface, as defined in 3GPP TS 29.273. The Context-Identifier AVP is used to apply the APN provided by the AAA server to a PDN session. If the RADIUS Access-Request message from the User Equipment (UE) does not contain an APN in the Called-Station-ID AVP, the TWAG uses the configured default APN, which is the configured `mapped-apn-name` for the STa session learner interface (`non-3gpp-access-diameter-client`), to initiate the DER with the AAA server. The AAA server responds with a DEA message: ■ If the DEA command-level Context-Identifier matches a Context-Identifier within the APN-Configuration AVP, the TWAG will use the APN name in the associated Service-Selection AVP (within the APN-Configuration AVP) as the session APN name. ■ If the DEA command-level Context-Identifier does not match any Context-Identifier within the APN-Configuration AVP, the TWAG checks if the requested APN matches an APN name listed in the APN-Configuration AVP. If there is a match, the requested APN is authorized by the AAA server and the TWAG uses this APN for the session. ***Note:*** *The TWAG ignores the Context-Identifier information received from the AAA server if the session is an emergency session.* ***Note:*** *With Release 9.2, the TWAG/TWAP, by default, processes the Context-Identifier AVP when provided by the AAA server in the Diameter- EAP-Answer (DEA) message to select an APN for the session. The Context-Identifier AVP cannot be suppressed when received in the DEA message.*

Increased support to 10 million URL hashes for URL filtering	Increased the maximum services content-filter filter-database-size filter-hash-list range from 5 million to 10 million. The default is 500,000. For example:
	`an3000-mcm-slot7cpu1(config)# services content-filter filter-database-size filter-hash-list ?`
	`Possible completions:`
	`<unsignedLong, 100000 .. 10000000>[500000]`

Feature	Description
Added support for Secure HTTP Identity Protocol (SHIP) See the *Affirmed Networks Value Added Services Guide*.	Traditionally, HTTP Header Enrichment (HHE) is used to pass information from a Network Operator to a Content Provider (CP). However, HHE is not practical when using an encrypted HTTPS connection. Therefore, SHIP is used to convey information from the Network Operator to the Content Provider when using HTTPS. The SHIP protocol consists of two forms: ■ Redirect based (Browser) – This interface allows information exchange between the Network Operator when HTTPs connections are initiated from the UE's Internet browser. ■ Web API based (for Applications) – This interface allows information exchange between the Network Operator, User Equipment (UE), and the CP by allowing an application running on a UE access to a WEB API from a SHIP server.
Added a new configuration command to customize the file naming convention for local CDRs (ASN.1 only)	This feature adds a new configuration command to customize the file naming convention for local CDRs (ASN.1 only). This feature only applies to the datarecord profile. `an3000-mcm-slot7cpu1(config)#` **`infrastructure file-management profile datarecord <filename-prefix> file-name-format [default|custom1]`** ■ **`default`** – The MCC uses the default file naming convention for local CDR files: `<filename-prefix><YYYYMMDDHHMMSS>_<123>.csv` ■ **`custom1`** – The MCC uses the following custom file naming convention for local CDR files (ASN.1 only): `<filename-prefix>_MM_DD_YYYY_hh_mm_ss_<#records>_file<123>.u` where – `filename-prefix` – Indicates the prefix of the filename in which to store CDRs. – `MM_DD_YYYY_hh_mm_ss` – Represents the timestamp. – `#records` – Represents the number of records stored in the file, starting with 0. – `123` – Represents the file sequence number. The number of leading zeros prepended to the file sequence number depends on the value configured for the `sequence-field-width`. For example, if the `sequence-field-width` is set to 6, the sequence number will start with 000001. ***Note:*** *In the rare case of an uncontrolled MCM switchover caused by a crash in the DataRecordAgentMCM process or an MCM kernel crash, the currently open CDR files will remain with a record count of 0, indicating that the number of records could not be determined when the file was closed.*
CUPS Lawful-Intercept - support for dynamic LI targets on UPF See the *Affirmed Networks Lawful Intercept Module Specification and Provisioning Guide*.	Added support to the calea target CLI to allow specification of dynamic LI targets on UPF: ■ ADMF provisions LI targets only on the CPF ■ CPF delivers HI2 IRI to the LEMF ■ CPF signals target information to the UPF when the session is intercepted ■ UPF creates UPF dynamic target based on target information sent from the CPF ■ UPF delivers HI3 CC-data directly to the LEMF

Feature	Description
Support for Geo-Redundancy on CUPS Control Plane Function	This feature adds Geo-Redundancy support in the Control and User Plane Separation (CUPS) Control Plane Function (CPF). The CPFs are configured with the same Sxa/b PFCP endpoint parameters, and their loopback-IPs are the same as the loopback-IPs for the associated geo-redundant-groups. The two CPFs have the same PFCP peer which points to the same User Plane Function (UPF). If the geo-redundant-group on CPF1 has an *active* runtime-state, CPF1 will communicate with the UPF. If the geo-redundant-group runtime-state is active on both CPF1 and CPF2, only the CPF on the *primary* geo-redundant-group will communicate with the UPF. Sessions are preserved across the CPFs. Before and after a switchover, the CPF points to the same session on the UPF. PFCP peer status (associations and heartbeat messaging) is also maintained before and after a switchover. The CUPS Geo-Redundancy configuration is the same as for non-CUPS, with the `geo-redundant-group` name specified in the `workflow subscriber-analyzer` object. `an3000-mcm-slot7cpu1(config)#` **`workflow subscriber-analyzer <name> analyzer-type user-plane-selector geo-redundant-group <name> priority <value> action user-plane-profile <name> key <name>`** Where `geo-redundant-group` is the same geo-redundant-group referenced by the ue-pools in the ip-subpools associated with the specified `user-plane-profile`.
Support for SR-IOV/non-SR-IOV Base Networks Regardless of Management Network and Unbonded Base Ports See the appropriate deployment guide for more information.	This feature supports these changes in the Ethernet port assignments in the MCC network topology: ■ **SR-IOV/non-SR-IOV base network support** — MCC base devices can be either SR-IOV or non-SR-IOV, even if the management device is non-SR-IOV. The Eth0 and Eth1 Ethernet port mapping of network devices (automatically configured) is dependent on whether the management device is SR-IOV or non-SR-IOV. When all network devices (including the management device) are SR-IOV, Eth0 is assigned to the Base Ethernet port, and Eth1 is assigned to the Management port. However, when the management device is non-SR-IOV and the remainder of the devices are SR-IOV, then the Base/Management port assignments are reversed. In that case, Eth0 is assigned to the Management Ethernet port and Eth1 is assigned to the Base port. ■ **Unbonded Base ports** — In redundant MCC systems, Base and Base 2 Ethernet ports are no longer bonded. Each separate base port now is assigned a unique MAC address.

Feature	Description
Support of Configuring TAM with MH-BGP	This feature supports configuring Traffic Anchoring Mode (TAM) with the Multi Hop Border Gateway Protocol (MH-BGP). Just as with Single Hop Border Gateway Protocol (SH-BGP), for each session the routes are advertised with the lower cost for IP addresses anchored on the local TAM and with a higher cost for other addresses. Although MH-BGP is designed to distribute traffic over all nodes, when MH-BGP is configured on TAM there is only one MH-BGP session per TAM node (ISM/SSM). To configure TAM with MH-BGP: ■ Configure one loopback per TAM node. ■ Configure static routes from the TAM node to point to the loopback of the MH-BGP peer. ■ Configure one MH-BGP session per TAM node. ■ Configure the loopback as the update-source interface for the MH-BGP peer. ***Note:*** *When TAM is configured with MH-BGP, it behaves much like SH-BGP.*
Support for multiple X2/X3 Delivery Destinations See the *Affirmed Networks Lawful Intercept Module Specification and Provisioning Guide*.	Added support to the calea target CLI to allow explicit specification of LEMF IP addresses and ports for X2 and X3 traffic from the target. ADMF provisions calea target with new options: ■ primary LEMF IP addresses and ports (X2 and X3) ■ secondary LEMF IP addresses and ports (X2 and X3) ■ interface-group-source-profiles (X2 and X3) MCC first attempts to establish a connection and send to the primary IP addresses. If unable to establish connection to primary, MCC attempts to connect and send to secondary IP addresses.
MCM Switchover Enhancements	This feature reduces the MCM switchover response time from approximately 60 seconds to 20 seconds. This enhancement applies to all MCM switchovers, including manual switchovers, failure scenarios, power outages, and so on.
Added support to include IMSI in the bearerInfo data record of the Start/Stop/Interim/Attempt BEARER EDR	Added support to include IMSI in the bearerInfo data record of the Start/Stop/Interim/Attempt BEARER Event Data Record.
Increased disk space for */tosdb/content/* subfolders	This feature increases the available disk space for files in the *tosdb/content/contentinsertion* and *tosdb/content/policylists* folders by moving the files to an external storage partition. Added the **tosdb-content** file management rule to manage the use of the disk space.

Feature	Description

Added enhancements to LTMI payload (x-acr header). MCC supports a combination of MSISDN, IMSI, SUBID, and mapped APNs
See the *Affirmed Networks Value Added Services Guide*.
	Added support to allow the request add-header value to be encoded using ltmi-dynamic-trusted, ltmi-static-trusted, and ltmi-external algorithm in HHE module.
	This release supports LTMI encryption of a custom string. The string may include any sequence of variables separated by a user-defined character (for example “/”).
	For example:
	<subID> + “/” + <IMSI> + “/” + <MSISDN> + “/” + <mapped APN>
	Configure the LTMI encryption value string as follows:
	an3000-mcm-slot7cpu1(config)# service-construct http-header-enrichment ACR-HHE request add-header header-string X-ACR value
	`ltmi-dynamic-trusted  Encrypt data using Dynamic Trusted LTMI algorithm in the header`
	`ltmi-external  Encrypt data using External LTMI algorithm in the header`
	`ltmi-static-trusted  Encrypt data using Static Trusted LTMI algorithm in the header`
	The following statistics apply to this feature:
	services multi-protocol-proxy statistics cluster-level header-enrichment 43
	`Ltmi Plain Text ID  0`
	`Ltmi Static Trusted ID  7`
	`Ltmi Dynamic Trusted ID 6`
	`Ltmi External ID  6`

Feature	Description

Static configuration of Initialization Vector (IV) for encrypted <request/response> headers.
See the *Affirmed Networks Value Added Services Guide*.
	Added support for static configuration of Initialization Vector (IV) for encrypted <request/response> headers. This feature adds the TIMESTAMP macro under the <request/response> custom header-string value. The TIMESTAMP macro is represented in Epoch format. This feature also adds the IV string under encryption-profile. Configure these attributes as follows:
	`an3000-mcm-slot8cpu1(config)# service-construct http-header-enrichment <HHE name> request add-header header-string <string> value`
	`Possible completions:`
	`<String, may include variable such as IMSI, MSISDN, HTTPVERSION, UEIPADDR, ORIGINALAPN, IMEI, ULICGI, RATTYPE, GWIPADDR, PLMNID, CHARGINGCHAR, TIMESTAMP example: $(MSISDN)>`
	`encrypted  Include encrypted custom value in the header by the algorithm configured in encryption profile`
	`md5  Include MD5 hashed custom value in the header`
	
	`an3000-mcm-slot7cpu1(config)# service-construct encryption-profile HHE aes-128-cbc|aes-192-cbc|ase-256-cbc ?`
	`Possible completions:`
	`key  Key for AES encryption, please input HEX format without space`
	`IV  Static Initialization Vector for AES encryption, please input a unique IV in HEX format without space equal 16bytes of length.`

Added new SNMP trap variable bindings See the *Affirmed Networks SNMP MIB and Alarm Reference Guide*.	Added the following new SNMP trap variable bindings: ■ affirmedVmSourceIpAddress ■ affirmedVmSourceName

Feature	Description

Shared subnet support for SH-BGP within a single network-context.	This release adds support for SH-BGP within a single network-context.
	MCC supports multiple IP interfaces and BGP sessions in the shared subnet. MCC is dually homed to two routers for redundancy and each router belongs to a distinct shared subnet. MCC uses a common VLAN 1000.
	For example:
	■ Router 1 belongs to 1.1.1.0/24
	■ Router 2 belongs to 2.2.2.0/24
	MCC's routing table accounts for route updates and withdrawals from multiple neighbors with same remote address. For example, if peering session 1 fails (but other sessions remain active), the routing table does not lose the route to 10.10.10.0/24.
	You can configure multiple neighbors with the same remote address but you must configure a different **update-source** address for each neighbor. MCC uses the **update-source** address as the local address for the neighbor. For example:
	`neighbor BGP-vth-2-1-gi`
	`  neighbor-addr 107.243.141.14`
	`  remote-as  64903`
	`  timers keep-alive 30`
	`  timers hold-time 90`
	`  update-source phy-interface GI_2_1_5`
	`  fall-over-bfd single-hop`
	`  !`
	`  neighbor BGP-vth-3-1-gi`
	`  neighbor-addr 107.243.141.14`
	`  remote-as  64903`
	`  timers keep-alive 30`
	`  timers hold-time 90`
	`  update-source phy-interface GI_3_1_5`
	`  fall-over-bfd single-hop`

Feature	Description

Changed the measurement of the Diameter `retransmit-timeout` CLI parameter from seconds to milliseconds	The `retransmit-timeout` CLI parameter for Diameter interfaces is now measured in milliseconds instead of seconds. The range is 1000-30,000 milliseconds. The default value for the Gy/Gx/Gz/S6b interfaces is 5000 and the default value for the Flow Authorization interface is 3000.
	Gy and Gx Interfaces
	`an3000-mcm-slot7cpu1(config)# service-construct interface [online-charging|pcrf-charging] <interface-name> retransmit-timeout <value-in-milliseconds>`
	Gz/Rf Interface
	`an3000-mcm-slot7cpu1(config)# service-construct interface offline-charging <interface-name> [pgw|sgw] diameter retransmit-timeout <value-in-milliseconds>`
	S6b Interface
	`an3000-mcm-slot7cpu1(config)# service-construct interface s6b-interface <name> retransmit-timeout <value-in-milliseconds>`
	Flow Authorization Interface
	`an3000-mcm-slot7cpu1(config)# service-construct interface flow-authorization-interface <name> retransmit-timeout <value-in-milliseconds>`

Added a new configuration parameter to specify whether to encode the IMEISV in TBCD format in the User-Equipment-Info AVP See the *Affirmed Networks Gy Interface Specification.*	The IMEISV sent within the User-Equipment-Info AVP in the CCR message on the Gy interface is encoded in Octet String format, by default. This feature adds a new configuration parameter to specify whether to encode the IMEISV in Telephony Binary Coded Decimal (TBCD) format. Changes to this parameter take effect immediately. `an3000-mcm-slot7cpu1(config)# service-construct interface online-charging <interface-name> avp-customization user-equipment-info-imeisv format-tbcd [enabled|disabled]` ■ **`enabled`** – The IMEISV sent within the User-Equipment-Info AVP in the CCR message on the Gy interface is encoded in TBCD format. ■ **`disabled`** – The IMEISV sent within the User-Equipment-Info AVP in the CCR message on the Gy interface is encoded in Octet String format.

Feature	Description
Modified the rating group memory allocation when a billing plan is applied to a subscriber	Previously, when a billing plan was applied to a subscriber, the MCC allocated memory for all the rating groups configured under that billing plan for the session. This feature modifies the rating group memory allocation, so that when a billing plan is applied to a session, the MCC: ■ Allocates memory for all rating groups that have at least one service rule configured with the `service-activation` parameter set to `always-on`. ■ Does not allocate memory for rating groups that only have service rules configured with the `service-activation` parameter set to `external-activation`. When applying the billing plan for a Charging-Rule-Base-Name (CRBN) profile, the MCC only allocates memory for rating groups that have at least one service rule configured with the `service-activation` parameter set to `always-on` or that have a service rule that is part of the CRBN service rule list. ***Note:*** *The MCC does not deallocate memory for a rating group within a billing plan even if the last service rule is removed from that rating group.* **Upgrade Considerations** If a session is established using an older version of software (prior to 9.2), the system will allocate memory for all the rating groups in a billing plan and will sync these rating groups with the new version of software (9.2 or greater), which comes up as standby. If a session is established using a new version of software (9.2 or greater), the system does not allocate memory for rating groups that only have externally-activated service rules. However, the system will sync these rating groups with the standby, which might be using an older version of software (prior to 9.2). In this case, if the standby is using on older version of software and becomes active, subsequent rules received from the PCRF might fail to install if these rules belong to a rating group that only has externally-activated service rules.

Feature	Description
Added support for QoS-Group-Rule VSAs on the Gx interface See the *Affirmed Networks Gx Interface Specification.*	Added support for the following vendor-specific attributes (VSAs) on the Gx interface: ■ QoS-Group-Rule-Install – The PCRF uses this VSA to activate predefined service rules on the MCC gateway. ■ QoS-Group-Rule-Remove – The PCRF uses this VSA to deactivate predefined service rules on the MCC gateway. ■ QoS-Group-Rule-Definition – The PCRF uses this VSA to define the parameters for a pre-configured service rule whose name matches the QoS-Group-Rule-Name. For example, if the received QoS-Group-Rule-Definition VSA has a redirect server address, the MCC will apply redirection to the associated flows. ■ QoS-Group-Rule-Name – The MCC tries to match the service rule name, received in the QoS-Group-Rule-Name VSA, to a service rule name configured locally on the MCC gateway (`service-construct` –> `service-rule`). – If a match is found, the MCC activates the matching service rule and all services associated with the received QoS-Rule-Group-Name. – If a match is not found, the MCC sends the Charging-Rule-Report AVP with the QoS-Group-Rule-Name VSA to the PCRF. The QoS-Group-Rule-Install and QoS-Group-Rule-Remove VSAs are configurable in Credit-Control-Answer (CCA) data record templates. The default `presentFlag` setting is `no`, indicating the field is ignored when received in the CCA message. `an3000-mcm-slot7cpu1(config)#` **`service-construct data-record-template [pgw|ggsn] pcrf diameter cca <template-name> [qosgroupruleinstall|qosgroupruleremove] presentFlag [yes|no]`** ***Note:*** *If the QoS-Group-Rule-Install and QoS-Group-Rule-Remove VSAs are received in the Re-Auth-Request (RAR) message, they will be processed.*
Added support for MAC algorithms at the **maximum** pki ssh security level	Added support for the following MAC algorithms at the **maximum** pki ssh security level: ■ hmac-sha2-512 ■ hmac-sha2-256

Feature	Description

Added enhancements to the **show subscriber** command on the user plane	Added enhancements to the following show commands on the user plane:
	show subscriber summary
	Previously, this command displayed 0. With this enhancement, the system displays the actual bearer-id.
	show subscriber pdn-session
	Previously, the workflow data-profile was not displayed. With this enhancement, the system displays the workflow data-profile name. In addition, the system displays the charging rules.
	show subscriber pdn-bearer
	Displays the correct value for is-cups-session. Previously, the system displayed this value as false.
	show subscriber pdn-service-data-flow
	Displays all service-data-flow related information.
	Removed the following output from the **show subscriber pdn-session** command:
	`original-apn-name`
	`prior-apn-name`
	`incoming-apn-name`
	`reporting-apn-name`
	`workflow-gn-next-hop-network-context`
	`workflow-gn-next-hop-ip`
	`workflow-gn-next-hop-interface-index`
	`idle-timer-state`
	`idle-timer-duration`
	`maximal-duration-timer-state`
	`maximal-duration-timer-duration`
	`uplink-activity-duration`
	`downlink-activity-duration`
	Removed the following output from the **show subscriber pdn-bearer** command:
	`idle-timer-state`
	`qci-profile`

Gx interface support for CUPS See the *Affirmed Networks Gateway Administration Guide* for Gx interface information	This feature adds Gx interface support, including predefined and dynamic Policy and Charging Control (PCC) rules, for Control and User Plane Separation (CUPS) architecture. The Gx interface is configured between the PGW-C and the PCRF. There is no change to the Gx interface configuration. The PGW-C sends PCC rules and event triggers over PFCP to the PGW-U via the Sx interface using vendor-specific information elements (IEs). The PGW-U reports traffic usage to the PGW-C via the Sx interface. The PGW-C then reports the usage information to the PCRF via the Gx interface. ***Note:*** *The user-plane cluster configuration must match the configuration for the control-plane cluster, including data profiles, charging-instances, billing-plans, rating-groups, service-rules, and packet-filters.*

Feature	Description
Gy interface support for CUPS See the *Affirmed Networks Gateway Administration Guide* for Gy interface information	This feature adds Gy interface support for CUPS architecture. The Gy interface is configured between the PGW-C and the OCS. There is no change to the Gy interface configuration. The PGW-C sends charging information over PFCP to the PGW-U via the Sx interface using vendor-specific information elements (IEs). The PGW-U reports traffic usage information to the PGW-C via the Sx interface. The PGW-C then reports the usage information to the OCS via the Gy interface. ***Note:*** *The user-plane cluster configuration must match the configuration for the control-plane cluster, including data profiles, charging-instances, billing-plans, rating-groups, service-rules, and packet-filters.*
Control and User Plane Separation (CUPS) – User Plane Function (UPF) selection based on existing subscriber analyzer keys and additional UE capabilities key	Added support to select UPF based on existing subscriber analyzer keys and additional key for UE's support for Dual Connectivity with New Radio (DCNR). To do so, configure a **`workflow subscriber-analyzer`** of **`analyzer-type user-plane-selector`**. For example: `an3000-mcm-slot7cpu1(config)#` **`workflow subscriber-analyzer UPLANE-1-SA analyzer-type user-plane-selector priority 10 key ue-capabilities dcnr`** ***Note:*** *Subscriber analyzer key value* ***`ue-capabilities dcnr`*** *is supported for* ***`workflow subscriber-analyzer`*** *of* ***`analyzer-type user-plane-selector`*** *and* ***`workflow-profile`***.
UE IP sub-pool management per User Plane Function (UPF)	This feature allocates UE IP addresses based on the selected UPF and advertises the UE IP sub-pool routes on the appropriate UPF. IP sub-pools are configured on the Control Plane Function (CPF) and UPFs. The IP sub-pool in the CPF is divided among the UPFs. In other words, the CPF contains a superset of the IP sub-pools from all UPFs. The CPF allows this division by linking associated IP sub-pools with the user-plane-profile configuration.

Feature	Description

PFCP session monitoring over the Sx interface	Added support for PFCP Sx interface session monitoring between the Control Plane Function (CPF) and the User Plane Function (UPF) to detect and close sessions when there is no response from the peer or the request times out.
	
	When this feature is enabled, session monitoring starts when no activity is detected during the configured **pfcp-session-monitor-interval** time. Each node periodically checks its peer for a corresponding Sx session according to what is configured for the interval time. The CPF sends a dummy Sx Session Modification Request to the UPF, and the UPF sends a dummy Sx Session Report Request to the CPF. The dummy requests set a flag to indicate to the peer node that it is a dummy request. If the peer node responds with rejection cause code “Session Context Not Found”, the session is locally closed.
	
	When this feature is disabled, sessions are not closed when there is no response from the peer or the request times out, but monitoring is enabled if the configured interval time is between 60 and 1440 minutes. If the interval time is 0 (zero), session monitoring is disabled even when **pfcp-clear-on-session-monitor-timeout** is set to **enabled**.
	
	Use the following command to enable/disable session monitoring. By default, this parameter is set to **enabled**.
	
	`(config)# zone default gateway profile pfcp-profile <profile-name> pfcp-clear-on-session-monitor-timeout [enabled|disabled]`
	
	Use the following command to set the amount of time in minutes to wait before sending monitor messages to a peer. By default, this value is set to 300 minutes.
	
	`(config)# zone default gateway profile pfcp-profile <profile-name> pfcp-session-monitor-interval <value>`
	
	Use the following command to display the session monitoring state and whether activity was detected during the interval:
	
	`show zone default gateway pdn-session <pdn-session-id> [pdn-session-monitor-timer-state|received-pfcp-message-in-monitor-interval]`
	
	Added the following PFCP peer statistic:
	
	`show zone default gateway statistics cluster-level pfcp peer <table-name>`
	
	`num-pfcp-session-context-not-found-received  Total number of PFCP Session Context Not Found received`

Feature	Description

Support for Sx Node Related Procedures – Heartbeat and Association Procedures	This feature adds support for Sx Node Related procedures, defined in 3GPP TS 29.244 V2.0.1, for Control and User Plane Separation (CUPS) architecture.
	
	Sx Association Setup/Update/Release Procedures – An Sx association is set up between the control plane function (CPF) and user plane function (UPF) prior to establishing Sx sessions. Only one Sx association is setup between a given pair of CPF and UPF.
	
	■ Sx Association Setup Procedure – Initiated by either the CPF or the UPF. The Sx Association Setup Request includes:
	– Node ID (IPv4/IPv6), which identifies the Sx association.
	– List of optional features that the node supports. In this release, the UP supports TRST, FTUP, TREU and EMPU.
	
	■ Sx Association Update Procedure – The UPF initiates an Sx Association Update Request to modify an existing Sx association when the UPF is administered down. Use the following command to change the UPF admin-state:
	`an3000-mcm-slot7cpu1(config)# zone <name> gateway user-plane-service <uplane-service-name> admin-state [enabled|disabled]`
	
	Note: *All sessions on the user plane will be deleted if the* `user-plane-service admin-state` *is* `disabled`*.*
	
	■ Sx Association Release Procedure – The CPF initiates an Sx Association Release Request to release the Sx association if any of the associated PGW/SGW services are administered down. Upon receiving the Sx Association Release Request, the UPF deletes all Sx sessions, Sx associations and any related information locally before sending an Sx Association Release Response with a successful cause code.
	
	If the UPF is administered down, the UPF sends the CPF an Sx Association Update Request to notify the CPF to send an Sx Association Release Request to release the Sx association. Upon receiving the Sx Association Update Request, the CPF starts a configurable guard timer. When the guard timer expires, the CPF sends an Sx Association Release Request to the UPF and deletes all Sx sessions to the UPF.
	
	Use the following command to configure the guard timer:
	`an3000-mcm-slot7cpu1(config)# zone <name> gateway profile pfcp-profile <profile-name> pfcp-guard-time-interval <value>`
	
	The default value for the `pfcp-guard-time-interval` is 60000 milliseconds (ms).
	
	Heartbeat Procedure – The CPF/UPF exchange Heartbeat Request/Response messages to check if a PFCP peer is alive once the Sx association between the CPF and UPF is established. The CPF will periodically send the Heartbeat Request to the UPF according to what is configured for the following command:
	`an3000-mcm-slot7cpu1(config)# zone <name> gateway profile pfcp-profile <profile-name> pfcp-heartbeat-periodic-interval <value>`
	
	The default value for the `pfcp-heartbeat-periodic-interval` is 60000 ms.

Feature	Description
Support for Sx Session Related Procedures over PFCP with proprietary vendor-specific IEs	This feature adds support for Sx Session Related procedures for CUPS architecture. This release supports Packet Forwarding Control Protocol (PFCP), defined in 3GPP TS 29.244 V2.0.1, with proprietary vendor-specific IEs for session-related messages. ■ Sx Session Establishment Procedure – Used to setup an Sx session between the control plane function (CPF) and user plane function (UPF) and to configure rules in the UPF so that the UPF can handle incoming packets. – CPF: The CPF initiates an Sx Session Establishment Request to setup an Sx Session for a PDN Connection/IP-CAN Session. – UPF: When the UPF receives an Sx Session Establishment Request message, it establishes the UP session based on proprietary vendor-specific IEs. ■ Sx Session Modification Procedure – Used to modify an existing Sx session. For example, to configure a new rule, to modify an existing rule, or to delete an existing rule. – CPF: The CPF initiates an Sx Session Modification Request to modify a session. – UPF: When the UPF receives an Sx Session Modification Request, it processes the modification request if the session is present, otherwise it sends an Sx Session Modification Response with rejection cause code “Session Context Not Found”. ■ Sx Session Deletion Procedure – Used to delete an existing Sx session between the CPF and the UPF. – CPF: The CPF initiates an Sx Session Deletion Request to delete an existing session. – UPF: When the UPF receives an Sx Session Deletion Request, it process the session deletion request if the session is present, otherwise it sends an Sx Session Deletion Response with rejection cause code “Session Context Not Found”. ■ Sx Session Report Procedure – Used by the UPF to report information related to the Sx session to the CPF. – UPF: The UPF initiates an Sx Session Report Request to report information related to an Sx session. – CPF: When the CPF receives an Sx Session Report Request, it processes the information being reported as appropriate, otherwise it sends an Sx Session Report Response with rejection cause code “Session context not found”.

Feature	Description
Support User Plane Functions (UPF)	The UPF is horizontally scalable and supports various User Plane Functions such as: ■ GTP-U, IP forwarding ■ GTP-U TEID allocation ■ PCEF, DPI/TF ■ DNS proxy, NAT/firewall, steering ■ NAT functionality ■ Traffic steering, redirection, enforcement ■ F-TEID allocation/release ■ Header enrichment of uplink traffic ■ Packet buffering ■ Sending end marker packets Configure the user-plane-service follows: **zone default gateway user-plane-service ACTON-USER-PLANE-SERVICE** admin-state enabled pfcp-endpoint-params network-context GN pfcp-endpoint-params loopback-ip PGW_LOOP pfcp-profile PFCP-PROF pfcp-link-down-queue-messages disabled network-profile NW-PROFILE-S1U ! network-profile NW-PROFILE-S5-S8 ! network-profile NW-PROFILE-SGW-S5-S8 ! pfcp-peer-list CP-PFCP-PEER ! pfcp-peer-list CP-SGW-PFCP-PEER ! pfcp-peer-list CPF-SXA-161-83 ! pfcp-peer-list CPS_SXA_83 ! pfcp-peer-list CPS_SXB_83 !

Feature	Description
Support for CUPS (Control and User Plane Separation) statistics	Added support for CUPS performance statistics viewable through the MCC CLI and the Acuitas Service Management System: **CUPS Session Statistics** To view these statistics with the MCC CLI, use the following commands: **show zone <name> gateway statistics [cluster-level | grid-level | node-level] call-performance apn <name>** **show zone <name> gateway statistics [cluster-level | grid-level | node-level] call-performance pgw <name>** **show zone <name> gateway statistics [cluster-level | grid-level | node-level] call-performance sgw-apn <name>** **show zone <name> gateway statistics [cluster-level | grid-level | node-level] call-performance sgw <name>** To view these statistics with Acuitas Performance Management, use the following metrics tables: ■ **APNCALLPERFSTATSGRID**, **APNCALLPERFSTATSCHASSIS**, **APNCALLPERFSTATSSLOT** ■ **PGWCALLPERFSTATSGRID**, **PGWCALLPERFSTATSCHASSIS**, **PGWCALLPERFSTATSSLOT** ■ **SGWAPNCALLPERFSTATSGRID**, **SGWAPNCALLPERFSTATSCHASSIS**, **SGWAPNCALLPERFSTATSSLOT** ■ **SGWCALLPERFSTATSGRID**, **SGWCALLPERFSTATSCHASSIS**, **SGWCALLPERFSTATSSLOT** **Message-Level PFCP Peer Statistics** To view these statistics with the MCC CLI, use the following command: **show zone <name> gateway statistics cluster-level pfcp peer <name>** View these statistics in the **PFCPMESSAGESTATSCHASSIS** metrics table. **User Plane Service Statistics** To view these statistics with the MCC CLI, use the following command: **show zone <name> gateway statistics [cluster-level | grid-level | node-level] call-performance user-plane-service <name>** View these statistics in the following metrics tables: ■ **UPLANECALLPERFSTATSGRID**, **UPLANECALLPERFSTATSCHASSIS**, **UPLANECALLPERFSTATSSLOT**
Lawful Intercept for Control and User Plane Separation (CUPS) as specified in *3GPP TS 33.107 Section 12.9 Functional Requirements for LI in case of Control and User Plane Separation*	Added support for Lawful Intercept for Control Plane Function (CPF) and User Plane Function (UPF) as specified in *3GPP TS 33.107 Section 12.9 Functional Requirements for LI in case of Control and User Plane Separation*.
Lawful Intercept for Control and User Plane Separation (CUPS) - - User Plane Function (UPF) solution with UPF sending X3 directly to LEMF	Added support for Lawful Intercept with UPF sending X3 CC-data directly to the LEMF. ADMF must provision calea interfaces and calea targets on both the CPF MCC and UPF MCC.

Feature	Description
Optimization of 80K Per Second Session Setup Rate for CPM/DCM VMs	This feature supports optimizations to achieve session setup rates of 10K per second for both the CPM (Control Plane Module) and DCM (Distributed Control Module) VMs. These rates scale linearly with the addition of each new VM added. For example, if eight DCM/CPM VMs are added, then the setup rate supported is 80K sessions per second. The session setup rate is not impacted by the number of existing sessions in the cluster.

Added retransmission counts and transmit timeouts to ensure reliable message delivery between the CPF and UPF
See the *Affirmed Networks Gateway Administration Guide*.
	This feature adds configurable retransmission counts and transmit timeouts to ensure reliable message delivery between the Control Plane Function (CPF) and the User Plane Function (UPF) on the SGW and PGW.
	Use the following commands to configure the retransmission counts and transmit timeouts on the CPF:
	`(config) zone default gateway [sgw|pgw] <name> pfcp-profile <profile-name> [sxa-interface|sxb-interface] [n3-count|t3-timeout]`
	■ **n3-count** – Specifies the N3 retry count. Range is 0-20; default is 2.
	■ **t3-timeout** – Specifies the T3 response timeout in milliseconds. Range is 100-3600000; default is 3000.
	Use the following commands to configure the retransmission counts and transmit timeouts on the UPF:
	`(config) zone default gateway profile pfcp-profile <name> [pfcp-node-response-timeout|pfcp-node-retransmit-count]`
	■ **pfcp-node-response-timeout** – Specifies the amount of time in milliseconds the SGW/PGW UPF waits for the peer to respond. If it does not receive a response, the message is retransmitted based on the configured pfcp-node-retransmit-count. Range is 100-3600000; default is 2000.
	■ **pfcp-node-retransmit-count** – Specifies the number of message retransmissions to send before declaring a path down. Range is 1-5; default is 3.

RADIUS interface support for CUPS See the *Affirmed Networks RADIUS Interface Specification* for RADIUS interface information.	This feature adds RADIUS interface support for CUPS architecture. The RADIUS interface is configured between the PGW-C and the AAA server. There is no change to the RADIUS interface configuration. The PGW-C sends authentication, authorization, and accounting information over PFCP to the PGW-U via the Sx interface using vendor-specific information elements (IEs). The PGW-U sends traffic usage information to the PGW-C via the Sx interface. The PGW-C then reports the usage information to the AAA server via the RADIUS interface.

Feature	Description
Offline charging support for CUPS (local interface, Ga interface, and Gz/Rf interface) See the *Affirmed Networks Charging Data Records Specification* for offline charging interface information.	This feature adds support for the following offline charging interfaces used to transfer Charging Data Records (CDRs) to an Offline Charging System (OFCS) for CUPS architecture. ■ Local Interface – Stores local CDRs in text files (CSV/ASN.1 format). ■ Ga Interface – Transfers CDRs using GTP Prime (GTPP). ■ Gz/Rf Interface – Transfers CDRs using Diameter. These offline charging interfaces are configured on the PGW-C. There is no change to the interface configuration. The PGW-C sends charging information over PFCP to the PGW-U via the Sx interface using vendor-specific information elements (IEs). The PGW-U reports traffic usage information to the PGW-C via the Sx interface. The PGW-C then uses the traffic usage information to generate CDRs and transfers them via the offline charging interface. All existing event triggers, including time and volume, are supported using vendor-specific information elements (IEs).

Robustness - Enhanced Session Load Balancing Algorithm to take gateway instance load into account	Enhanced the gateway selection algorithm to consider the gateway overload level and select least-loaded gateways more than other (overloaded) gateway tasks. Overall load is balanced across all gateway tasks when overload thresholds vary.
	Use the following CLI command to set the maximum number of sessions supported per gateway task:
	`an3000-mcm-slot7cpu1(config)# zone default gateway session-load-balancer max-absolute-load-val-per-gw-process`
	`Possible completions:`
	`  <unsignedInt, 100 .. 262144>[131072]`
	The recommended value for this parameter depends on the allocated memory and vCPUs for CPM/CSM/DCM VM. Contact Affirmed Networks Technical Assistance Center (TAC) for the recommended value.

Added support for Sx session establishment scenarios and GTP Mobility Procedures when the MCC is deployed as a CUPS system	This feature adds support for the following Sx session establishment scenarios and GTP Mobility Procedures when the MCC is deployed as a CUPS system. Mobility is supported for the following scenarios: ■ Standalone PGW-C/PGW-U to co-located SAEGW-C/SAEGW-U ■ Co-located SAEGW-C/SAEGW-U to standalone PGW-C/PGW-U ■ Standalone SGW-C/SGW-U ■ SGW relocation and S1 handover ***Note:*** *The SAEGW is a combined PGW/SGW control plane function (CPF) and user plane function (UPF).*

Feature	Description
Added support for 1:1 NAT or static NAT in Guaranteed, Deterministic, and Statistical NAT pools with CUPS User Plane Function (UPF)	Added support for 1:1 NAT in Guaranteed, Deterministic, and Statistical NAT pools with CUPS UPF. This feature adds the capability to assign an IP address to a subscriber for NAT, either during session creation or flow creation. With 1:1 NAT, only the IP address is transformed; the port on the NAT side is the same as the source port. This feature supports: ■ NAT Address intra-cluster and inter-cluster redundancy in Guaranteed and Deterministic modes ■ NAT 64 and EIM/EIF (all filtering options) for NAT 1:1 pools (similar to M:1 pools). ■ NAT binding records and pilot packets. ■ OSU ■ Enhanced Debug commands for reporting 1:1 NAT
5G NSA Support of UP Selection Indication Flags IE on the S4/S11 and S5/S8 Interfaces	This feature supports the following 5G-NSA Information Elements (IEs) on the S4/S11 and S5/S8 interfaces that are described below and are supported by 3GPP TS 29.274 V15.3.0 (2018-03): ■ **UP (User Plane) Selection Indication Flags IE**— Based on operator policy, the MME/S4-SGSN shall include this IE on the S4/S11 interface, if any of the applicable flags is set to 1. The applicable flag is DCNR, which shall be set to 1 if it is desired to select a specific SGW-U and PGW-U for UEs supporting Dual Connectivity with NR (DCNR) and not restricted to use NR by user subscription (e.g., due to requirements of higher bit rates). This information is used for the SGW-U, PGW-U or combined SGW-U/PGW-U selection (see Annex B.2 of 3GPP TS 29.244 [80]).
5G NSA Support of Secondary RAT Usage Data Reporting IE on the S11 and S5/S8 Interfaces	This feature supports the following 5G-NSA Information Elements (IEs) on the S11 and S5/S8 interfaces that are described below and are supported by 3GPP TS 29.274 V15.3.0 (2018-03): ■ **Secondary RAT Usage Data Reporting IE** — Secondary radio access technology (RAT) usage data can optionally be reported on a periodic basis. When the eNB is configured with a minimum time interval for secondary RAT usage data reporting, the eNB sends a radio access network (RAN) request message to the MME when the timer expires for each UE for which the MME has requested reporting. The timer begins with the last usage report for the UE. Periodic reporting of secondary RAT usage data is provided to the SGW and (optionally) to the PGW. When configured, the MME reports uplink and downlink data volumes to the SGW for the secondary RAT on a per Evolved Packet System (EPS) bearer basis using the secondary RAT usage data reporting procedure.

Feature	Description
Gx interface enhancements to support 5G NSA	The existing QoS AVPs defined on the Gx interface represent values in bits-per-second (bps) with a 32-bit integer data type. However, the 5G non-standalone (NSA) solution requires higher QoS bit rate values (up to 4 Tbps). To accommodate the higher 5G NSA throughput rates, the following AVPs have been added within the QoS-Information AVP on the Gx interface. These QoS AVPs represent values in kilobits-per-second (Kbps). ■ Extended-APN-AMBR-DL ■ Extended-APN-AMBR-UL ■ Extended-GBR-DL ■ Extended-GBR-UL ■ Extended-Max-Requested-BW-DL ■ Extended-Max-Requested-BW-UL Added a new configuration parameter to enable the "Extended-BW-For-NR" flag in the Supported-Features AVP on the MCC. The "Extended-BW-NR" feature is sent in the Features-List-ID (2), within the Supported-Features AVP, to indicate support for the extended QoS-Information AVP values in Kbps. `an3000-mcm-slot7cpu1(config)# zone <name> gateway enhanced-features-list <list-name> extended-bw-nr [enabled|disabled]`
Gy interface enhancements to support 5G NSA	Added support for the following extended bit rate AVPs (within the Service-Information –> PS-Information –> QoS-Information AVP) to support 5G NSA. ■ Extended-APN-AMBR-DL ■ Extended-APN-AMBR-UL ■ Extended-GBR-DL ■ Extended-GBR-UL ■ Extended-Max-Requested-BW-DL ■ Extended-Max-Requested-BW-UL These extended bit rate AVPs are configurable in Gy CCR data record templates using the `epcqosinfoextendedbitrates` field. The default `presentFlag` setting is `no`, indicating the field is not sent. `an3000-mcm-slot7cpu1(config)# service-construct data-record-template [pgw|sgw] ocs diameter [start|interim|stop] <template-name> epcqosinfoextendedbitrates presentFlag [yes|no|conditional]`

Feature	Description
Added support for new local (ASN.1/CSV) and GTPP CDR fields to support 5G NSA	Added the following local (ASN.1/CSV) and GTPP CDR fields to support the higher throughput rates required for the 5G non-standalone (NSA) solution. ■ Extended Max Requested BW UL ■ Extended Max Requested BW DL ■ Extended GBR UL ■ Extended GBR DL ■ Extended APN AMBR UL ■ Extended APN AMBR DL **Local CSV CDRs** ■ Added within the List of Service Data –> QoS Information field (PGW CDRs only) ■ Added within the List of Traffic Data Volumes –> QoS Information field (PGW/SGW CDRs) ***Note:*** *The new extended bit rate fields are not configurable in local CSV data record templates and therefore will be present in CDRs within the QoS-Information field.* **Local ASN.1 and GTPP CDRs** ■ Added within the Change of Service Condition –> EPC QoS Information field (PGW CDRs only) ■ Added within the Change of Charging Condition –> EPC QoS Information field (PGW/SGW CDRs) These CDR fields are configurable in local ASN.1 and GTPP Interim and Stop data record templates. The default `presentFlag` setting is `no`, indicating the data field is not present in CDRs. For example: `an3000-mcm-slot7cpu1(config)#` **`service-construct data-record-template [sgw|pgw] ofcs gtpp [interim|stop] <template-name> changeofcharconditionepcqosinformationextendedapnambrdl presentFlag [yes|no|conditional]`** Added a new configuration parameter to specify whether the EPC QoS Information fields in CDRs should report values in Kilobits-per-second (Kbps). `an3000-mcm-slot7cpu1(config)#` **`service-construct interface offline-charging <interface-name> [pgw|sgw] [local|gtpp] report-epcqos-in-kbps [enabled|disabled]`** ■ **`enabled`** – The EPC QoS information fields in CDRs are filled as follows: – Sets the current (non-extended) bit rates in Kbps. – Sets the extended bit rates in Kbps if the current bit rates are greater than 2^32-1. ■ **`disabled`** – (default) The EPC QoS information fields in CDRs are filled as follows: – Sets the current (non-extended) bit rates in bps. For bandwidth values greater than 2^32-1, sets the value to 2^32-1. – Sets the extended bit rates in Kbps if the current bit rates are greater than 2^32-1.

Feature	Description
Added support for new local (ASN.1/CSV) and GTPP CDR fields to support 5G NSA (*continued*)	Added the following local (ASN.1/CSV) and GTPP CDR field to SGW and PGW CDRs, as defined in 3GPP 32.298 version 15.2.0. ■ List of RAN Secondary RAT Usage Reports – This list includes one or more containers reported per bearer from the RAN for a secondary RAT. Each container includes the following fields: – Data Volume Uplink – Data Volume Downlink – Start Time – End Time – Secondary RAT Type The List of RAN Secondary RAT Usage Reports field and its subfields are configurable in local ASN.1 and GTPP Interim and Stop data record templates. The default `presentFlag` setting is `no`, indicating the data field is not present in CDRs. `an3000-mcm-slot7cpu1(config)#` **`service-construct data-record-template [sgw|pgw] ofcs gtpp [interim|stop] <template-name> secondaryratusagereports presentFlag [yes|no|conditional]`** The List of RAN Secondary RAT Usage Reports field is configurable in local CSV Interim and Stop data record templates. The default `presentFlag` setting is `no`, indicating the data field is not present in CDRs. `an3000-mcm-slot7cpu1(config)#` **`service-construct data-record-template [pgw|sgw] charging-local [interim|stop] <template-name> secondaryratusagereports presentFlag [yes|no|conditional]`**

Feature	Description

Added support for new Diameter AVPs on the Gz/Rf interface to support 5G NSA	Added support for the following AVPs on the Gz/Rf interface to support 5G NSA.
	■ Added the following extended bit rate AVPs (within the Traffic-Data-Volume –> QoS-Information AVP, Service-Data-Container –> QoS-Information AVP, and Service-Information –> PS-Information –> QoS-Information AVP).
	– Extended MRB Uplink
	– Extended MRB Downlink
	– Extended GBR Uplink
	– Extended GBR Downlink
	– Extended APN AMB Uplink
	– Extended APN AMB Downlink
	These extended bit rate AVPs are configurable in ACR data record templates using the `epcqosinfoextendedbitrates` field. The default `presentFlag` setting is `no`, indicating the field is not sent.
	`an3000-mcm-slot7cpu1(config)# service-construct data-record-template [pgw|sgw] ofcs diameter [start|interim|stop] <template-name> epcqosinfoextendedbitrates presentFlag [yes|no|conditional]`
	■ Added the RAN-Secondary-RAT-Usage-Report AVP (within the Service-Information –> PS-Information AVP) in ACR messages. This AVP is configurable in ACR data record templates and by default is set to **no**, indicating the field is not sent.
	`an3000-mcm-slot7cpu1(config)# service-construct data-record-template [pgw|sgw] ofcs diameter [start|interim|stop] <template-name> secondaryratusageinfo presentFlag [yes|no|conditional]`

Feature	Description
Traffic Anchoring Mode (TAM) - minimizing East/West traffic by anchoring loopbacks/sub-pools per node	Traffic Anchoring Mode (TAM) is a feature supported on existing VM types, specifically the Subscriber Services Module (SSM) and Integrated Services Module (ISM). This feature applies only to SSM/ISM VM personalities where I/O and workflow services are co-located. This feature adds TAM functionality to the MCC and CUPS platforms. TAM is used to reduce East-West traffic within an MCC or U-Plane cluster for SAEGW traffic. TAM is supported on a standalone PGW, standalone SGW, co-located PGW/SGW, and GGSN. ***Note:*** *TAM is not supported in GiGW deployments.* When TAM mode is enabled, session establishment and distribution logic is optimized to reduce East/West hops for all user traffic, reducing the percentage of user traffic across East/West interfaces under normal operating conditions. When TAM is combined with ISM, East-West Value Added Services (VAS) traffic is also reduced. Proxy services result in East/West traffic if SSMs are used. The following VAS features are supported with TAM: ■ HTTP proxy initiated HTTP and HTTPS ■ TCP proxy initiated TCP ■ DNS ■ LTMI downloads ■ Symantec downloads ■ URL-list file downloads ■ Device database file downloads Guidelines and limitations: ■ Adding new SSMs/ISMs to an MCC or CUPS U-Plane cluster does not require a cluster reboot. Non-CUPS and CUPS U-Plane clusters do not support a mix of TAM and non-TAM sessions. ■ A change to the TAM configuration requires a cluster reboot. ■ Moving from non-TAM to TAM requires reconfiguration of IP sub-pools and loopbacks. ■ Dynamic scale-in/scale-out of SSMs/ISMs is not supported when TAM mode is enabled. ■ Manual scale-in/scale-out of SSMs/ISMs is supported when TAM mode is enabled, but may affect service (depending on UE and NAT address management). ■ VAS for the TAM feature is not supported on ASMs/CSMs. Intra-cluster redundancy (non-CUPS and CUPS U-plane): ■ Existing redundancy mechanisms remain unchanged. When TAM is active in a cluster, the failure of an SSM/ISM results in redistributing the sessions anchored on that node across the remaining SSMs/ISMs.East/west traffic associated with affected sessions will exist until the failed node becomes operational.

Feature	Description

Support statistical NAT mode in relation to TAM mode setting	This feature supports the following two dependent functions:
	■ TAM mode disabled – Redesigned statistical M:1 NAT (SNAT) (many-to-one statistical NAT) to follow 1:1 SNAT-like behavior. Similar to 1:1 SNAT (one-to-one statistical NAT), M:1 SNAT sub-pool IP addresses are divided across available SSMs/ISMs. Each SSM/ISM is allotted its respective chunk of NAT IP addresses. Also, the entire port range (1024 – 65535) is available to each NAT IP on the SSM/ISM. Multiple subscribers can use the same NAT IP on an SSM/ISM, but each subscriber is allotted different port chunks. In 1:1 SNAT, a single IP and the entire port range is allocated to a subscriber, whereas in M:1 SNAT, a single IP can be shared by multiple subscribers.
	■ The statistical NAT ip-sub-pool range must be greater than or equal to the **`max-nat-workflow-modules`** value configured under **`cluster <id>`**.
	■ TAM mode enabled – Added support for TAM mode for M:1 SNAT and 1:1 SNAT. The TAM configuration determines which SSM/ISM advertises a favorable route for a NAT pool. Since this is done at an IP address level, the entire port range must be used by the NAT module. If other SSMs/ISMs use the NAT IP address, it results in east-west traffic. When operating in TAM mode, separate/non-overlapping NAT ip-sub-pools must be configured for each TAM node (or SSM/ISM). The entire NAT ip-sub-pool is available to a single SSM/ISM and each SSM/ISM has its own entire ip-sub-pool. An ip-sub-pool associated with one SSM/ISM cannot be used by another SSM/ISM.
	To configure TAM:
	`an3000-mcm-slot7cpu1(config)# tam policy mode enabled-for-cluster`
	Configure the TAM profile:
	`an3000-mcm-slot7cpu1(config)# tam profile ip-subpool <clusterId nodeSlot> <ip-subpoolName>`
	`an3000-mcm-slot7cpu1(config)# tam profile <clusterId nodeSlot> loopback-ip <network-contextName> <loopback-ipValue>`
	`an3000-mcm-slot7cpu1(config)# commit`
	`The following warnings were generated:`
	`'tam policy':`
	`Changing TAM Mode to "Enabled" will force a cluster reboot.`
	where:
	■ ***`clusterId`*** — specifies the cluster to which the profile is anchored.
	■ ***`nodeSlot`*** — specifies the node to which the profile is anchored.
	■ **`ip-subpool`** — specifies the IP subpool to which the profile is anchored.
	■ ***`ip-subpoolName`*** — specifies the IP subpool name to which the profile is anchored.
	■ **`loopback-ip`** — specifies the loopback IP address to which the profile is anchored.
	■ ***`network-contextName`*** — specifies the context name.
	■ ***`loopback-ipValue`*** — specifies the loopback IP address value.

Feature	Description

Support statistical NAT mode in relation to TAM mode setting
(*continued*)
	To view the TAM statistics:
	`an3000-mcm-slot7cpu1# show tam`
	To view a TAM policy configuration:
	`an3000-mcm-slot7cpu1# show running-config tam`

Support for ISM and IWM to Reduce East/West Traffic	The Integrated Workflow Module (IWM) and the Integrated Services Module (ISM) MCC VMs minimize inter-VM proxy user plane traffic (also known as *East/West* (E/W) *traffic*) during non-failure modes of operation. E/W traffic between VMs in the MCC results in increased end-to-end delays and significantly reduces throughput. The ISM/IWM VMs minimize multiple hops within the MCC platform of upstream and downstream user packets. Each packet hop decreases data throughput and increases end-to-end delays. ISM/ISM VMs significantly speed up traffic throughput by minimizing E/W traffic hops. The solution also reduces the server footprint that results in lower cost per bit.
	The goal of the ISM is to minimize E/W user packets between workflow sessions and proxies. The ISM transforms the SSM and ASM functions into one VM. In an integrated-services mode cluster, the ISM effectively reduces the number of E/W hops by 1 for VAS traffic. The integrated-services strategy is an E/W reduction strategy that integrates I/O and workflow functions into one VM that reduces proxy E/W traffic by using the ISM along with the CPM and MCM.
	The IWM integrates WSM and ASM functions into one VM. In an integrated-workflow mode cluster, the IWM transforms IOM/WSM/ASM functions into an IOM/IWM that effectively reduces the number of E/W hops by 1 for VAS traffic. The integrated-workflow strategy is an E/W reduction strategy that integrates workflow and VAS functions into one VM using the IWM as well as the CPM, IOM and MCM.
	To configure ISM:
	`an3000-mcm-slot7cpu1(config)# cluster <id> building-block-strategy integrated-services`
	`an3000-mcm-slot7cpu1(config)# cluster <id> node <nodeValue> type <type> personality <PersonalityType>`
	where:
	■ **`building-block-strategy`** — specifies the strategy used to create VM personalities.
	■ **`integrated-services`** — specifies the use of the integrated-services strategy VM personality.
	■ **`node`** — specifies the card configuration/status.
	■ **`type`** — specifies the VM personality card type.
	■ **`id`** — specifies the cluster value.
	■ **`personality`** — specifies the VM personality.

Support of the Intel XXV710 4x25GB NIC on Skylake Processor on Dell R470 Server	This feature supports the use of the Intel XXV710 4x25GB NIC on Skylake processor using the Ubuntu 16.04-based and OpenStack Ocata-based KVM hypervisor on the Dell R740 PowerEdge Rack Server.

Feature	Description
PFCP link failure handling for user data messages on the UPF	This feature adds a configurable option to buffer data usage messages on the User Plane Function (UPF) when the Packet Forwarding Control Protocol (PFCP) link is down between the UPF and Control Plane Function (CPF). The UPF transmits the buffered data usage messages (as Sx Session Report messages) when the PFCP link is restored. This allows the CPF to more accurately report data usage for CDRs and offline interfaces even with intermittent PFCP link failures. Use the following command to enable/disable message buffering. By default, this parameter is set to **`disabled`**. `an3000-mcm-slot7cpu1(config)# zone default gateway user-plane-service <name> pfcp-link-down-queue-messages [disabled|enabled]`
PFCP link failure handling for default Gy quota and data usage messages	This feature supports handling of default Gy quota allocations and buffering of data usage messages on the User Plane Function (UPF) when there is a Packet Forwarding Control Protocol (PFCP) link failure or the charging information messages time out. The Control Plane Function (CPF) sends the default Gy quota configuration to the UPF upon initial session setup. When default Gy quota is enabled and the PFCP link is down when the current default quota is exhausted or the quota request to the CPF times out, the UPF allocates the default quota up to the maximum configured value received from the CPF. If the PFCP link is still down or the quota request times out when the maximum default quota is exhausted, the UPF closes the session. All default quota allocations are reset to 0 if the PFCP link is restored and CPF response messages are successfully received. If default Gy quota is disabled and the PFCP link is down or the request message times out when the quota is exhausted, the UPF closes the session. When **`pfcp-link-down-queue-messages`** is enabled on the UPF and the PFCP link is down or the charging information message times out, the UPF aggregates and buffers data usage messages for all rating groups and sends those messages to the CPF when the PFCP link is restored. If this configuration is disabled and the PFCP link is down or the charging information message times out, the UPF drops the messages and data usage is not reported to the OCS. ***Note:*** *If sessions are closed on the UPF before the PFCP link is restored, user data is lost and not reported to the OCS.* ***Note:*** *If the default Gy quota configuration is modified on the CPF, the new configuration will only be replicated on the UPF for new session setups or if the CPF sends any messages to the UPF for existing sessions.*

Feature	Description

PFCP protocol logging	Added Packet Forwarding Control Protocol (PFCP) protocol logging to capture Sx Node Related messages and Sx Session Related messages sent/received by the PGW-C, SGW-C, PGW-U and SGW-U in the Evolved Packet Core (EPC) Control and User Plane Separation (CUPS) architecture. The MCC captures the packets and stores them as pcapng capture files in *var/log/eventlog* on both the control plane function (CPF) and user plane function (UPF). These files can be viewed in Wireshark.
	Set parameters for this feature using the following commands:
	1 Create a local file in which to store packets.
	`an3000-mcm-slot7cpu1(config)# infrastructure file-management profile eventlog <filename>`
	2 Create a log policy.
	`an3000-mcm-slot7cpu1(config)# infrastructure logging event-log policy <policy-name> admin-state enabled log-type protocol protocol-logging-filter-field protocol filter-value pfcp`
	To disable the log policy, change the `admin-state` to `disabled`.
	3 Create a sink under the log policy.
	`an3000-mcm-slot7cpu1(config)# infrastructure logging event-log policy <policy-name> sinks <sinks-name> type file file-name <file-name> file-format pcapng`
	Note: *Secondary level filters, such as IMSI, IMEI and MSISDN, can be configured on both the CPF and UPF. The Policies/Filters on the CPF and UPF work independently of each other and do not have to match.*

Added vProbe support for PFCP protocol logging	■ Added vProbe support for PFCP protocol logging: ■ Control Plane packet mirroring support for PFCP protocol Support to populate control plane function or user plane function session IDs in SESSION, BEARER, FLOW, and HTTP Transaction EDRs. Added the following fields to the RecordKeys data records: **SessionRecordKeys** – 2 = optional uint64 uPlaneSessionId **BearerRecordKeys** – 3 = optional uint64 uPlaneSessionId **FlowRecordKeys** – 4 = optional uint64 cPlaneSessionId **HTTPRecordKeys** – 5 = optional uint64 cPlaneSessionId
CUPS C-plane gateway and non-CUPS gateway	This release supports CUPS and non-CUPS sessions concurrently in the same MCC control-plane cluster. This assumes appropriate configuration for both CUPS and non-CUPS. A non-CUPS session is established when no user-plane selector matches the session setup. An ip-sub-pool must be configured and not associated with any user-plane-profiles.

Feature	Description
Geo-redundant non-CUPS SAEGW co-resident with non geo-redundant CUPS SAEGW-C	This release adds support for a geo-redundant non-CUPS SAEGW co-resident with a non geo-redundant CUPS SAEGW-C, operating as *different* services on a single MCC cluster in hybrid CUPS mode. In other words, the geo-redundant non-CUPS service uses its own PGW and SGW service, for example, PGW-1 and SGW-1, and the non geo-redundant CUPS service uses PGW-2 and SGW-2.
Increased limit on the number of rating-groups per billing plan	This feature increases the limit from 64 to 1024 on the number of rating-groups that can be configured for a single billing plan, based on the following settings: ■ Supports up to 1024 rating-groups if *all* the service-rules configured under those rating-groups have the `service-activation` field set to `external-activation`. ■ Supports up to 64 rating-groups if *any* service-rule configured under those rating-groups has the `service-activation` field set to `always-on`. `an3000-mcm-slot7cpu1(config)#` **`services charging rating-group <ratingGroupName>`** `an3000-mcm-slot7cpu1(config)#` **`service-construct service-rule service-activation [always-on|external-activation]`** ***Note:*** *In this release, each additional rating-group under a billing plan increases the memory requirement for a session by approximately 2K bytes. This feature was qualified with 256 rating-groups under a billing plan, on a CSM with 120G memory and 100K sessions, each with 30 active rating-groups.*
Support for up to 256 rating-groups per metering service instance	This feature increases the number of rating-groups that can be associated with a metering service instance from 64 to 256. `an3000-mcm-slot7cpu1(config)#` **`services metering metering-instance <metering-instance-name> admin-state enabled rating-group <rating-group-name>`** ***Note:*** *This feature was qualified with 256 rating-groups configured under a metering instance with a maximum of 30 usage-monitoring groups active for a subscriber.*
Support for PCRF metering of GSUs from 3GB to 100GB	This feature increases the Diameter-based PCRF metering of the Granted Service Unit (GSU) maximum value from 3GB to 100GB. The GSU specifies the total service units that the Direct Client-to-Client (DCC) client can provide for end users. The MCC GGSN/PGW supports the USAGE_REPORT (26) or USAGE_REPORT (33) PCRF event trigger, which is used when the PCRF requests usage monitoring. The PCRF includes the Usage-Monitoring-Information AVP(s), the Monitoring-Key AVP and the Granted-Service-Unit AVP. The MCC gateway reports the accumulated subscriber usage in a CCR-U to the PCRF when the allocated quota in the Granted-Service-Unit AVP (included within the Usage-Monitoring-Information AVP) is exhausted.

Feature	Description
Added support for the Redirect-Host AVP in the CCA message on the Gx interface	This feature adds support for processing the Redirect-Host AVP received in the Credit-Control-Answer (CCA) message on the Gx interface. If the PGW receives a CCA (Initial, Update or Terminate) message from the PCRF and the Result-Code AVP is set to DIAMETER_REDIRECT_INDICATION, the PGW will forward the CCR message for that session to the host contained in the Redirect-Host AVP. The PCRF can send multiple Redirect-Host AVPs in the CCA message and if one fails, the MCC selects the next one in the list. The Redirect-Host AVP is configurable in CCA data record templates. The default `presentFlag` setting is `yes`, indicating the AVP is processed when received in the CCA message. `an3000-mcm-slot7cpu1(config)# service-construct data-record-template [pgw|ggsn] pcrf diameter cca <template-name> redirecthost presentFlag [yes|no]`
Support of Secure Neighbor Discovery protocol (SEND) as described in RFC 3971/3972 for secure Neighbor Discovery	This release adds support of Secure Neighbor Discovery protocol (SEND) as described in RFC 3971/3972 for secure Neighbor Discovery (ND). To support this feature, MCC acts as a host and discovers its router (Router Discovery) and the subnet prefix. MCC supports SEND at the IP interface level for the following Neighbor Discovery Protocol (NDP) messages: RS (Router Solicitation), RA (Router Advertisement), CPS (Certification Path Solicitation), CPA (Certification Path Advertisement), NS (Neighbor Solicitation), and NA (Neighbor Advertisement). MCC connects to the router only if the router has a certification path to one of the trust anchors proposed by MCC. MCC also supports secure discovery of its on-link neighbors (Neighbor Discovery). MCC supports a Cryptographically Generated Address (CGA) corresponding to the interface link local address prefix. This address is generated using the 64bit prefix of the default link local address of the interface, RSA public key, and the configured security level. The CGA remains valid for as long as the interface is up. MCC mitigates threats related to the NDP protocol using secure neighbor discovery options such as CGA, RSA, Timestamp, and Nonce. Rivest, Shamir, Adleman (RSA) is an asymmetric key algorithm for the key-pair generation. The algorithm generates a private-public key pair for digital signatures. MCC adds a new TOS task to support the SEND user space daemon that handles all NDP messages to add secure functionality. MCC supports the SEND feature in full secure mode at the interface level and global level. ■ When enabled at interface level – MCC process only NDP messages received with SEND payload options and drops NDP messages without SEND options. ■ When enabled at the global level – The configuration applies to all interfaces but the SEND functionality is applied only for NDP messages that are sent on link local addresses. ***Note:*** *MCC does not support the SEND protocol as a router. In other words, MCC does not support RS (Router Solicitation) requests from the peer.*

Feature	Description

Added support for advertising the UE static IPv4 address as a /32 host route and the IPv6 address as a /64 route on the Gi network	This feature adds support for advertising the UE static IPv4 address as a /32 host route and the IPv6 address as a /64 route on the Gi network after the IP address is allocated to the UE. After the UE session is deleted, the UE IP address is released to the pool and the corresponding host-based route is withdrawn. This feature enables the PGW to handle a maximum of 10,000 UE routes.
	
	This feature adds the **advertise-host-based-routes** parameter in the PGW remote/local UE ip-sub-pool object to control the advertisement of UE routes during subscriber attachment, instead of advertising routes during configuration.
	
	After the subscriber attaches to the network and MCC assigns the IP address, the PGW installs the host-based route corresponding to the UE IP address (/32 for IPv4 and /64 for IPv6) to the NetAgent for advertisement.
	
	Note: *This feature does not apply to delegated IPv6 prefixes.*
	
	Note: *These attributes are supported during call/session creation only. Any changes to* ***ip-sub-pool advertise*** *or* ***advertise-host-based-routes*** *after call/session creation may result in undefined behavior.*
	
	The **advertise-host-based-routes** parameter indicates to the gateway whether a subscriber assigned from this pool should be advertised. Options include:
	■ no (default) – MCC does not advertise the route.
	■ yes – MCC advertises the UE IP as a /32 or /64 route received from AAA during session establishment. This parameter can be set to **yes** only when **advertise** is set to **no** and **ip-sub-pool-type** is set to **UE-IP-Pool**.
	
	For example:
	`an3000-mcm-slot7cpu1(config)# network-context <NC-Name> ip-sub-pool <name>`
	`admin-state enabled`
	`ip-sub-pool-type UE-IP-Pool`
	`ue-pool REMOTEPOOL`
	`range-start 10.53.161.5`
	`range-end 10.53.161.5`
	`advertise no`
	`advertise-host-based-routes <yes/no>`
	`route-tag 1`
	`suppressicmp false`

Added support for configuring RADIUS peers with vrf-lightweight network contexts to increase the maximum number of configurable RADIUS-client server groups and RADIUS peers	This feature adds support for configuring RADIUS peers with Virtual Routing and Forwarding (VRF) lightweight network contexts. This feature allows Operators to configure 2000 vrf-lightweight network contexts with a maximum of 4000 RADIUS-client server groups and a total of 12,000 peers across these server groups. ***Note:*** *RADIUS peers associated with vrf-lightweight network-contexts and RADIUS peers associated with normal (non-vrf-lightweight) network-contexts are configurable within the same RADIUS-client server group or across RADIUS-client server groups.* ***Note:*** *This feature does not apply to RADIUS-server server groups.*

Feature	Description

Support for RAN-NAS reporting to the PCRF when RAN/NAS Release Cause is included in the Update Bearer Response on the S5/S8 interface	Previously, RAN/NAS cause codes were sent to the PCRF based on RAN-NAS cause information received in Delete Session Request or Delete Bearer Response messages only. This feature allows RAN/NAS cause codes to be sent to the PCRF based on RAN-NAS cause information received in Update Bearer Response messages as well.
	With this feature, when the PGW receives an Update Bearer Response with a RAN-NAS Cause indication, the PGW reports detailed release or failure code information in the Charging-Rule-Report –> RAN-NAS-Release-Cause AVP in a CCR-U to the PCRF.
	As part of this feature, the RAN/NAS Cause information element (IE) is added to the Bearer Context IE within the Update Bearer Response message on the S5/S8 interface.
	To configure this feature, you must use the following existing commands to enable RAN-NAS reporting in the enhanced-feature-list associated with the gateway APN:
	1 Enable RAN-NAS reporting. By default, the parameters in this list are disabled:
	`an3000-mcm-slot7cpu1(config)# zone default gateway enhanced-features-list <list-name> ran-nas enabled`
	2 Map the configured enhanced-features-list to an APN:
	`an3000-mcm-slot7cpu1(config)# zone default gateway apn <apn-name> enhanced-features <list-name>`

Formatting Encoded AVPs in the AAR Message See the *Affirmed Networks Gateway Administration Guide*.	This feature supports replacing certain ASCII control characters used as delimiters in a received Server Identifier (ID) name and realm from a Create Session Request (CSR) message while encoding them as Destination-Host and Diameter-Realm AVPs in the AA-Request (AAR) message used to select the S6b Diameter peer for authentication. When a Server ID name and realm from a CSR message are received over the S2b/S2a interfaces that contain ASCII control characters used as delimiters, the characters are replaced during encoding by the PGW with dot (.) delimiters when they are used as S6b Diameter Destination-Host and Diameter-Realm AVPs, respectively. During encoding, any non-printable or space characters that appear at the start or end of these Destination-Host and Diameter-Realm AVPs are removed.

Feature	Description
Added support for weighted round-robin distribution to multiple Diameter peers	Operators can configure the MCC to use a weighted round-robin algorithm to distribute initial session requests among the available Diameter peers within a Diameter server group based on the configured weight assigned to each peer. The Diameter peer with the highest weight (with 10 being the highest and 1 being the lowest) receives the most distribution of new session requests. The MCC only uses the configured weight for the initial peer selection (for example, CCR-Initial). For example, if Peer A is set to 4 and Peer B is set 2, the MCC will distribute the initial session requests as ABABAA. In this example, the MCC alternates between both peers starting with Peer A because it has the highest weight. When a Diameter peer is configured with a weight of 0, the MCC places the peer in "maintenance mode" and stops sending new session requests (for example, CCR-I) to this peer, but continues to send requests (for example, CCR-Update/CCR-Terminate) for existing sessions. If the Diameter peer with the highest weight is unavailable, the request is sent to the peer with the next highest weight in the same Diameter server group. If multiple Diameter peers are assigned the highest weight (10), the MCC uses a round-robin approach to select from among those peers for new requests. Operators can configure the MCC to use a weighted round-robin algorithm to select a Diameter peer from among a list of primary peers or from among a list of secondary peers, but not *across* primary and secondary peers. Use the following command to assign a weight to a Diameter peer: `an3000-mcm-slot7cpu1(config)# service-construct interface aaa-interface-group diameter node-admin <node-name> peer <peer-host-name> weight <value>` ■ **`weight`** – Specifies the weight allocated to this Diameter peer. The Diameter peer with the highest weight (10) receives the most distribution of new session requests. The default is 1 (lowest weight). When set to 0, the MCC places the peer in "maintenance mode" and stops sending new session requests (for example, CCR-I) to this peer, but continues to send requests (for example, CCR-Update/CCR-Terminate) for existing sessions. *Applies to Gy/Gx/Gz/STa/Swm/S6b interfaces.*
Added DPI detection of the IMO application-related protocol traffic	Added DPI detection of the IMO application-related protocol traffic to classify subprotocols (audio/video) traffic separately from rest of the IMO traffic

Feature	Description

Proxy bypass	This feature enables Operators to bypass proxy for a specific IP address or domain.
	Affirmed Networks recommends having a small number of packet-filters to bypass; the maximum is 256.
	This feature applies only to proxy bypass external server (s) configured through http-ip-flow. This feature does not apply to the explicit proxy where a loopback is configured.
	Configure the bypass http-ip-flow object with a higher priority than the non-bypassed http-ip-flow object. The proxy-bypass object defaults to **disabled**.
	Configure this feature as follows:
	`an3000-mcm-slot7cpu1(config)# services http-proxy http-ip-flow <name> proxy-bypass?`
	`Possible Completions:`
	`<admin state {enabled | disabled}>`
	Added the proxyBypass subfield field to the FlowRecord field of the Flow Event Data Record.

Added support for anBfdSessionDown alarm	Added support for the anBfdSessionDown alarm. When enabled, this alarm is generated when an existing or new BFD session goes down, and automatically clears when the session is restored. A gratuitous clear is performed the first time a BFD session is restored, even if there are no active BFD session down alarms. This alarm has Critical severity. Use the following command to enable/disable the alarm. By default, this parameter is set to **disabled**. `an3000-mcm-slot7cpu1(config)# ip-protocols bfd common send-bfd-session-down-alarms [enabled|disabled]`
Acuitas support to configure instance-based thresholds	Added support to configure instance-based thresholds. To configure an instance-based threshold: ■ Create a Threshold and a global set of instance filters (from the **Settings** icon on the toolbar, select **Performance** => **Instance Filter Configuration**). Complete the Conditions fields by selecting appropriate values for Parameter, Operator, Value, and Condition. To associate a Threshold with a PM Collection Task: ■ In the User Task Scheduler (from the **Settings** icon on the toolbar, select **Performance** => **User Tasks** => **Schedule** => **Edit User Task Scheduler**), expand the Performance object name to list the metrics. Expand the metric to list the instance-based thresholds. In the Threshold field, select an instance-based threshold to be associated with the desired metric. Acuitas matches each instance-level value in the collected data with its associated threshold value and based on the results, raises a threshold event with the specified severity.
Acuitas support for management of MCC-based SCEF 1.0	Acuitas supports management of MCC-based Affirmed Networks Enhanced Service Capability Exposure Function (SCEF) 1.0, including real-time statistics in tabular and chart/graph view, traps, and configuration commands.

Feature	Description
Acuitas support for management of VERTICA database	Acuitas supports management of VERTICA database including managing a VERTICA device and processing SNMP traps generated from VERTICA database.
Acuitas CUPS Manager support for geo-redundant Control Planes	Acuitas CUPS Manager supports geo-redundant Control Planes. You can use the CUPS Manager to: ■ Configure the required Sx interfaces and Packet Forwarding Control Protocol (PFCP) objects on the Control Plane and User Plane. ■ Configure geo-redundant Control Planes in a Geographic Redundancy group: – Use the Geographic Redundancy Manager to set up the Geographic Redundancy group of Control Planes. Specify the primary Control Plane and secondary Control Plane. – Use the CUPS Manager to configure the primary Control Plane to Sxa/Sxb endpoints. Use the Geographic Redundancy Manager to replicate this configuration to the secondary Control Plane. – In the Geographic Redundancy group, only the active Control Plane can communicate with the User Plane. If both Control Planes have active state, only the primary Control Plane can communicate with the User Plane. ■ View the grouping for geo-redundant Control Plane(s) and associated User Plane(s). ■ Perform an audit report to identify configuration differences between the active Control Plane in the Geographic Redundancy group and the User Plane. ■ Replicate common configuration from the active Control Plane in the Geographic Redundancy group to the User Plane.
Performance Manager support for additional statistics	Added statistics to the following statistics tables: ■ CONTENTHTTPCACHESTATSSLOT ■ CONTENTHTTPPROXYDETAILSTASCHASSIS ■ CONTENTHTTPPROXYOVERLOADCONTROLSTATSCHASSIS ■ HTTPPROXYMEDIATYPEBYTESCHASSIS
Added Acuitas support for backup/restore with tar file format for SSF version 2.2 and later devices	Acuitas supports backup/restore with tar file format for SSF version 2.2 and later devices. Acuitas continues to support backup/restore with xml file format for pre-version 2.2 SSF devices.
Enhancement to the configureRemoteServerForCsvPush .sh script	Enhancement to the configureRemoteServerForCsvPush.sh script to specify the destination on a local or remote server to copy daily-exported CSV files.
Acuitas support for new SNMP variable bindings in MCC traps	Acuitas supports the following new SNMP variable bindings in MCC traps: ■ affirmedVmSourceIpAddress ■ affirmedVmSourceName The variable bindings are displayed in the Additional Info field in the Alarms and Event Logs tabs and are included in northbound forwarded traps.

Feature	Description
Acuitas support for HPE HSS traps and alarms	Acuitas support for HPE HSS traps and alarms
Acuitas support for MME13.0.28.1	Added Acuitas support for MME13.0.28.1, including: **Configuration:** ■ Billing output controls: – omit-local-time-differential – omit-record-extensions – msisdn-format – suppress-zero-volume-cdrs ■ AAA for system users: – password-complexity minlen ■ MME: – masked-imeisv for S1 interface to control sending masked IMEISV to eNB – location-update-intra-mme-tau to determine when MME sends LUR to SGs VLR – release-access-bearer-on-geran-csfb-with-no-dtm to determine when MME sends GTP Release Access Bearers Request to SGW during CSFB – multipdn-sameapn-pdnreject-cause – voice-domain-profile-hlr – suppress-single-registration-indication – hss-default-map for APN mapping – tmsi-allocation config to enable basic or enhanced algorithm – Subscriber bearer limits profile support for more QCI ■ SGSN – SIGTRAN GTT support for round robin with up to 8 results – SIGTRAN ASP support for two local IP and two routing-instances **Statistics:** ■ New registers in the umtsSm statistics group set: – primaryActFail VS.SM.FailActPdpCtxtMs.Insfr_26.Ggsn.U – secondaryActFail VS.SM.FailActSecondPdpContextMs.Insfr_26.Ggsn.U
Acuitas support for SSF version 2.2	Added Acuitas support for SSF version 2.2, including: ■ Routing Control Plane (OSPF) Feature: – SSF backup/restore changed from XML to binary tar format

Feature	Description
Acuitas support for SSF version 2.3	Added Acuitas support for SSF version 2.3, including: ■ DNS configuration modeling enhancements for local records: – dns static-cache index obsoleted as key in all four record types – dns static-cache naptr-record status enable/disable ■ Automatic Configuration Sync Between SSF: – sync config-interval ■ Enhanced GTP error and timeout handling: – gtp interface csr-procedure-timer – gtp interface csr-procedure-timeout-gtpv1-cause – gtp interface csr-procedure-timeout-gtpv2-cause ■ Trap: anSsfAlarmConfigSync ■ Gateway group controls ■ GTP V1/V2 statistics for detailed failure reasons ■ Statistics for Subscriber Analyzer selection profiling ■ Changed the following KPI formulas: – GTP V1 Left Side CSR Nodal Success Rate – GTP V2 Left Side CSR Nodal Success Rate
Support to deploy Acuitas in an OpenStack high performance SR-IOV setup using Huge memory pages	Support to deploy Acuitas in an OpenStack high performance SR-IOV setup using Huge memory pages.
VNF Manager support to individually scale-in/out MCMs	Added VNF Manager support to individually scale-in/out MCC MCMs. This feature allows the Operator to perform maintenance on an existing cluster deployed by the VNF Manager without having to terminate and re-instantiate VMs (which would cause lifecycle management synchronization between the VNF Manager and the cluster it manages). You can perform scale-in only on the current standby node. If you select the active node, you are prompted to first perform a manual switchover to the standby node (to do so, issue the mcmswitchover command at the Cluster <*ID*>). This feature is supported on: ■ MCC clusters on vCenter and OpenStack
VNF Manager support to scale-in/out MCC MME MGMT and RM VMs	Added VNF Manager support to scale-in/out MCC MME MGMT and RM VMs. You can perform scale-in only on the current standby node. If you select the active node, you are prompted to first perform a manual switchover to the standby node. This feature is supported on: ■ MCC MME MGMT and RM VMs with specialized Building Block Strategy on OpenStack ■ MCC MME MRM with compact Building Block Strategy on OpenStack

Feature	Description
Acuitas VNF Manager support for MCC and MCC MME lifecycle management with Red Hat OpenStack Platform 13 (RHOSP13) (OpenStack Queens) using RHOSP Director	Acuitas VNF Manager support for MCC and MCC MME lifecycle management with Red Hat OpenStack Platform 13 (RHOSP13) (OpenStack Queens) using RHOSP Director.
Acuitas VNF Manager support for MCC and MCC MME lifecycle management in an OVS-DPDK enabled OpenStack environment	Acuitas VNF Manager support for MCC and MCC MME lifecycle management in an OVS-DPDK enabled OpenStack environment.
Acuitas VNF Manager and VNF Manager and Provisioning API support to apply VM instantiation order during cluster instantiation	Acuitas VNF Manager and VNF Manager and Provisioning API support to apply VM instantiation order during cluster instantiation. This feature is supported on: ■ MCC clusters on vCenter and OpenStack ■ MCC MME clusters on OpenStack only
Acuitas SNMPv3 support for northbound integration of alarms	Acuitas SNMPv3 support for northbound integration of alarms. To forward SNMPv3 traps to any northbound trap destination, in the **Create New SNMP Listener** window (from the **Settings** icon on the toolbar, select **Fault** => **Manage** => **Trap Forwarding**), set the **Trap Forward Type** to SNMPv3 and specify the SNMPv3 user settings.
Acuitas support for TACAS+ authentication and authorization for RedHat Linux operating system	Acuitas support for TACAS+ authentication and authorization for RedHat Linux operating system.
Acuitas support to manage an MCC with **maximum** pki ssh security level	Acuitas can manage a 9.2 or greater MCC with **maximum** pki ssh security level. However, Acuitas cannot manage an earlier version MCC with **maximum** pki ssh security level.
Acuitas VNF Manager support for root or non-root user access of vCenter host	Added support to specify a Host Username and Host Password to access the vCenter host. VNF Manager uses the username and password during cluster deployment.

Conventions

This guide uses the following conventions, when applicable:

Description	Convention	Examples
Command names, keywords, dialog boxes, buttons, icons, menus	**Times New Roman bold font**	Use **configure_ha** to configure... Enter **y**. To continue, press **Enter**.
Selecting a menu item	**Menu => Option**	Select **Security** => **Group Management**.
Variable parameters for which you supply values	***<courier bold italic blue font>***	**configure_dr --host *<host name>***
User input	**Courier bold blue font**	**cd /opt/Affirmed/NMS/bin**
Screen messages, system output, sample source code	Courier regular blue font	Checking for License...
Required keywords and arguments in square brackets	**[ ]**	**cluster [*id*] node [*id*] reboot**
Optional keywords and arguments in curly brackets	**{ }**	***{cdr-file-name}***
Keywords separated by the pipe symbol. Requires you to specify only one item from the set.	|	Is this correct? [y|n]
Keywords representing a single element in angle brackets	**< >**	***<host name>***
Asterisk after a CLI object indicates a required object	*	**name***
Variables, book and chapter titles, file path names, new terms, and emphasized text	*Times New Roman italic font*	See the *Acuitas User's Guide*. *Workflow* is an application running on the network element.

CAUTION: Proceed carefully to avoid possible equipment damage or data loss.

Note: *Additional information that may apply to the subject text.*

Tip: Helpful suggestions.

How to Obtain Product Documentation

Documentation is available for currently supported product releases. Documentation is available online in Adobe PDF format. You can view PDFs online using the Adobe Reader®. To download the latest version of the Adobe Reader software from the Adobe web site, go to http://get.adobe.com/reader/

You can access Affirmed Networks documentation from the SFTP server. Contact Affirmed Networks for instructions on how to access the SFTP server.

See the *Affirmed Networks Documentation Library* for a complete list of Affirmed Networks product documentation.

Technical Assistance Center

Affirmed Networks Technical Assistance Center (TAC) provides technical support 24 hours a day, 7 days a week (24 x 7) for any customer with an active maintenance contract.

To contact the TAC:

E-mail: prodsupport@affirmednetworks.com

24 x 7 Telephone support:
Local: 1-978-268-0871
Toll-free: 1-888-283-2838

Chapter 1

Getting Started

Overview

Acuitas™ Service Management System is the application that Operators use to navigate, monitor, and manage mobile functions and services.

Acuitas contains the following modules:

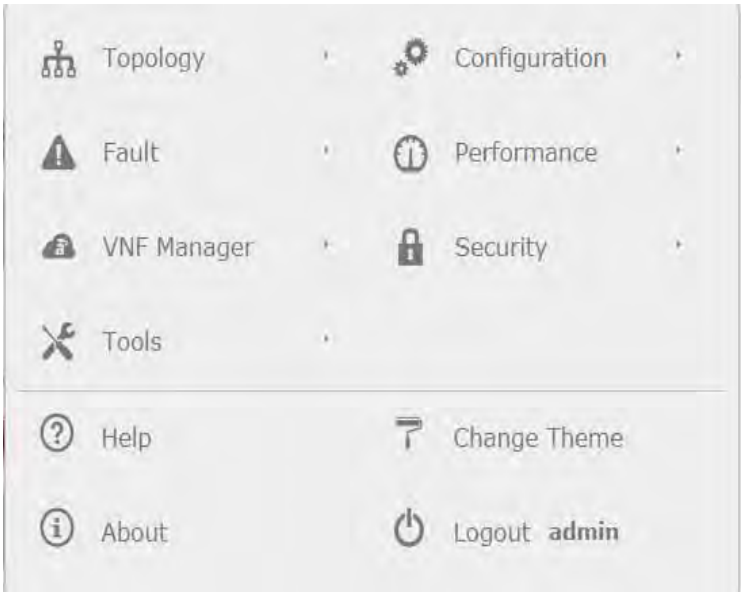
- Topology –
  - Manage Network Elements
  - Manage Groups (logical collections of network elements)
  - Configure Audit Trail Purge Settings
  - Configure Mail Server
  - Configure Global SNMP Settings
  - Configure Message Prompt on Locked User Accounts
- Configuration –
  - Manage Control and User Plane Separation (CUPS)
  - Manage Software Releases
  - Manage Software Upgrade Schedules
  - Manage Configuration Templates (to apply similar configurations to multiple elements)
  - Schedule Templates (to be periodically executed)
  - Manage Audit Trail (to record all configuration operations and activities)
  - Manage Alarm Triggered Configuration Templates
  - Manage File Servers (to maintain network element database backups and network element software)
  - Manage and Monitor Geographic Redundancy Groups
  - Manage NE Configuration Files

  - Manage URL Lists

- Fault –
  - View and Manage Alarms and Events
- Performance –
  - Manage Performance Collection and Export
  - Define Performance Statistic Thresholds
  - Manage Users Tasks Scheduler (that triggers data collection tasks based on task templates to be periodically executed)
  - Manage Users Tasks Templates (the metrics to be collected for performance statistics)
  - Configure Performance Reports
- VNF Manager –
  - Control and monitor virtualized MCC clusters in real-time
- Security –
  - Control User Authentication, Authorization, and Privileges
- Tools –
  - Administer Database
  - Configure Alarm Severity Color Settings
  - Configure Backup and Restore of NE Configuration

You access these modules from the **Settings** icon on the toolbar.

Figure 1-1 Accessing Acuitas Modules

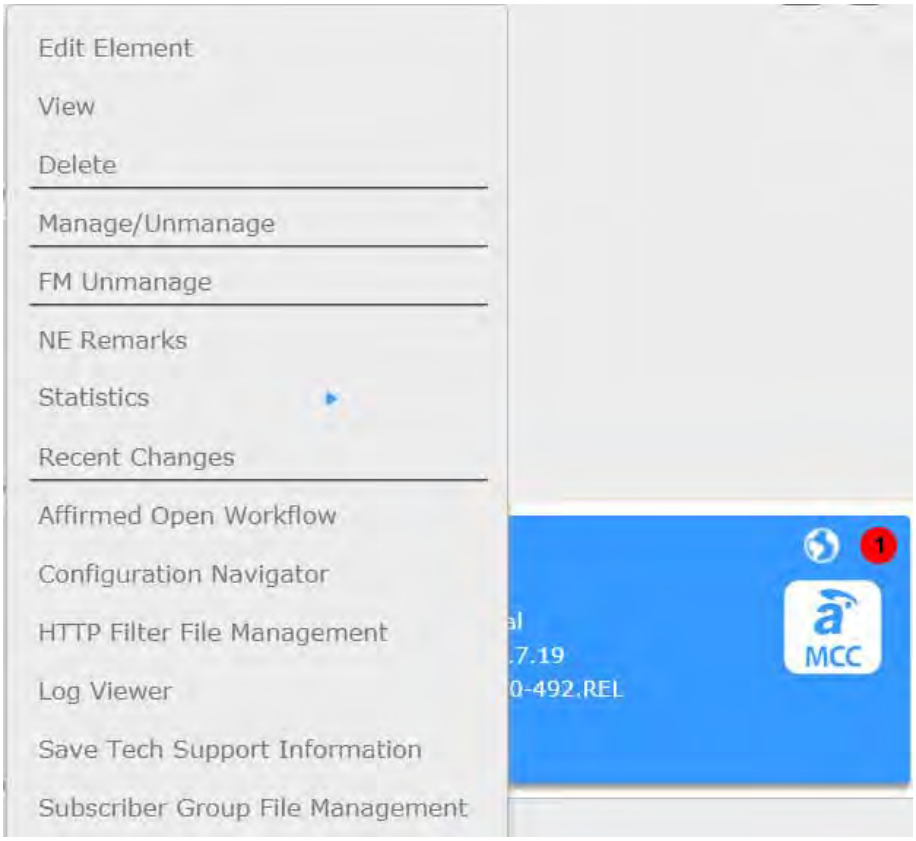


In addition, Acuitas contains the following applications on an NE:

- Affirmed Open Workflow – Defines the treatment of a service flow across various services offered by the system.
- Configuration Navigator – Defines configuration parameters on the system.
- HTTP Filter File Management – Defines control lists to either allow or deny content requests to a specific list of network addresses.
- Log Viewer – Monitors the system.
- Save Tech Support Information – Collects detailed debugging information about a Network Element (such as fault files and logs).
- Rate Limiting Subscriber Group File Management – Configures a group of subscribers whose traffic is rate-limited to a configured aggregate QoS Policy.

To access these applications, right-click an NE and select the application from the pop-up menu.

Figure 1-2 Accessing NE Applications



Logging Into Acuitas

To log into Acuitas, you need a User name and Password, which are provided by your system administrator.

Acuitas uses secure communication (HTTPS). Acuitas uses a self-signed certificate. If you prefer to use certificates issued by trusted Certificate Authorities, install those certificates on the Acuitas server. Follow the instructions in Using Certificates Issued by Trusted Certificate Authorities.

If you use the Acuitas self-signed certificate, use the following procedure to log into Acuitas.

To log into Acuitas:

1. Start the Mozilla Firefox web browser.
2. In the browser's address bar, enter the appropriate information:
   - **For Standalone Acuitas server**: Enter the IP address of the machine where the Acuitas server is started, using either of the following URLs (the `http:` URL redirects you to the `https:` URL):

     `http://<Acuitas server IP address>`

     `https://<Acuitas server IP address>`
   - **For HA Acuitas server cluster**: Enter the Virtual IP address of the HA cluster, using either of the following URLs:

     `http://<Acuitas cluster virtual IP address>/`

     `https://<Acuitas cluster virtual IP address>/`

Firefox warns you that Acuitas is an untrusted site.

Figure 1-3 Firefox Warning Screen

3. Click **I Understand the Risks**.

4 To eliminate the Firefox warning screen from appearing any time you log into this Acuitas server, click **Add Exception**.

Firefox displays the following screen.

Figure 1-4 Firefox Add Security Exception Screen

5 Mark the **Permanently store this exception** checkbox and click **Confirm Security Exception**.

Figure 1-5 Acuitas Login Screen

6 At the Acuitas login screen, enter your User name and Password.

7 If you want Acuitas to remember your User name, toggle **remember username**.

8 Click **Login**.

9 If your user account is configured by the administrator to force a password change after the first login, you are prompted to change your password. Enter the **Old Password**, **New Password**, and **Confirm Password** and click **Save**.

Note: *If you attempt to log into Acuitas six consecutive times (by default), but fail (because you supplied the wrong password), Acuitas automatically locks your account. You cannot log into Acuitas until your administrator unlocks your account. For instructions, see Unlocking Users.*

Acuitas Password Policies

Acuitas enforces the following Acuitas password policies. For any existing user, Acuitas enforces these password policies whenever the user or administrator changes the user account.

- Password must contain:
  - At least nine characters for newly-created users.

    Existing users with a password of at least six characters remain valid. When updating the password, existing users must create a new password at least nine characters long.
  - At least one upper case letter (A-Z)
  - At least one lower case letter (a-z)
  - At least one number (0-9)
  - At least one of the following special characters: ([!@#$%^&*])
- Password *cannot* contain the user name with which it is associated
- Password *cannot* be reused until either of the following rules is met:
  - Minimum number of other passwords (default 4 with a range 1-12) to be used before allowing a reused password

    or
  - Minimum number of days (default 120 with a range of 0-365) to pass before allowing a reused password
- After consecutive failed logon attempts (default 6), Acuitas automatically disables the user account, which must be unlocked by the administrator.

The rules for password use and account lockout are configurable in the securityconfiguration.properties file. For instructions, see securityconfiguration.properties.

securityconfiguration.properties

The securityconfiguration.properties file contains configurable attributes that control user account lockout and password use:

- The maximum number of consecutive failed logins (when the user supplied the wrong password) before the user is locked out.
- Acuitas idle time (in minutes) before the user is locked out.
- Acuitas dormancy time (in days) before the user is locked out, including the following scenarios:
  - User attempts to login for first time, but the number of days between the account creation and the attempted login is greater than the dormancy period.
  - User attempts to login, but the number of days between the last successful login and the current login is greater than system's dormancy period.
- Password reuse rules. A password *cannot* be reused until either of the following rules is met:
  - Minimum number of other passwords (default 4 with a range 1-12) to be used before allowing a reused password.
  - Minimum number of days (default 120 with a range of 0-365) to pass before allowing a reused password.

A locked out user cannot log into Acuitas until the administrator unlocks the account. For instructions, see Unlocking Users.

The securityconfiguration.properties file is in the directory:

/opt/Affirmed/NMS/server/ems/conf

The configurable attributes are:

```
## Maximum Failed Login Count

MXIMUM_LOGIN_FAILED_COUNT= 6

## Lockout time(in minutes) to enable automatically

LOCKOUT_TIME=30

## Dormancy Period is to be given in days

DORMANCY_PERIOD=30

## Minimum number of other passwords to be used before allowing a
reused password

PWD_REUSE_NUM_COUNT=4

## Minimum number of days to pass before allowing a reused password
```

```
PWD_REUSE_DAY_COUNT=120

## Minimum number of password characters

passwordConfig.minSize = 6
```

Any reconfiguration requires restart of the Acuitas server to take effect.

Using Certificates Issued by Trusted Certificate Authorities

To use certificates issued by trusted Certificate Authorities (CA), use the following procedure.

To use certificates issued by trusted Certificate Authorities:

1. Issue the appropriate command to generate a private key.

   For example, the following command creates a 2048-bit RSA key using Triple-DES (OpenSSL):

   ```
   openssl genrsa -des3 -out server.pem 2048
   ```

2. Issue the following command to generate a Certificate Signing Request (CSR) using the private key:

   ```
   openssl req -new -key server.pem -out server.csr
   ```

3. Enter the appropriate information at the prompts:

   ```
   Country Name (2 letter code) [GB]:CH

   State or Province Name (full name) [Berkshire]:

   Locality Name (eg, city) [Newbury]:

   Organization Name (eg, company) [My Company Ltd]:

   Organizational Unit Name (eg, section) []:

   Common Name (eg, your name or your server's hostname) []:

   Email Address []:

   Please enter the following 'extra' attributes to be sent with your
   certificate request

   A challenge password []:

   An optional company name []:
   ```

4. Issue the following commands to remove the Passphrase from the key:

   ```
   cp server.key server.pem.org

   openssl rsa -in server.pem.org -out server.pem
   ```

5. Submit the CSR to the CA. When you receive the certificate, save it as a .crt file. If the CA requires a chain certificate, save it as a separate .crt file.

6. Place the certificate and private key files on the Acuitas server. Copy the server.pem and server.crt files to /opt/Affirmed/NMS/server/ems/conf.

7 If the CA requires a chain certificate, edit the server.xml file to reference the chain file (default location /opt/Affirmed/NMS/server/ems/deploy/jbossweb.sar/server.xml).

a Locate the section that defines the SSL connector. For example:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 443 -->
```

b Add the SSLCertificateChainFile line at the following location in that section of server.xml:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 443 -->
      <Connector
          port="443" acceptCount="100"
address="${jboss.bind.address}" connectionTimeout="20000"
disableUploadTimeout="true"
          emptySessionPath="true" enableLookups="false"
maxHttpHeaderSize="8192"
          maxThreads="150"
          scheme="https" secure="true" SSLEnabled="true"

SSLCertificateFile="${jboss.server.home.dir}/conf/server.crt"

SSLCertificateKeyFile="${jboss.server.home.dir}/conf/server.pem"

SSLCertificateChainFile="${jboss.server.home.dir}/conf/trial-cert.
crt"
          clientAuth="false"
          SSLProtocol="SSLv3+TLS"
          SSLCipherSuite="ALL:!ADH:!RC4:!SSLv2:!EXPORT40:!EXP:!LOW"
       />
```

c Save the server.xml file.

8 Restart the Acuitas Server (which restarts Tomcat).

Viewing Product Version Information

To view version information for the Acuitas application:

1 Click **About** from the **Settings** icon on the toolbar.

Acuitas displays a window listing the version number, release date, last server start date, and copyright information.

2 Click **Close** to close the window.

Using Online Help

Acuitas provides online Help. You can access online Help in the following ways:

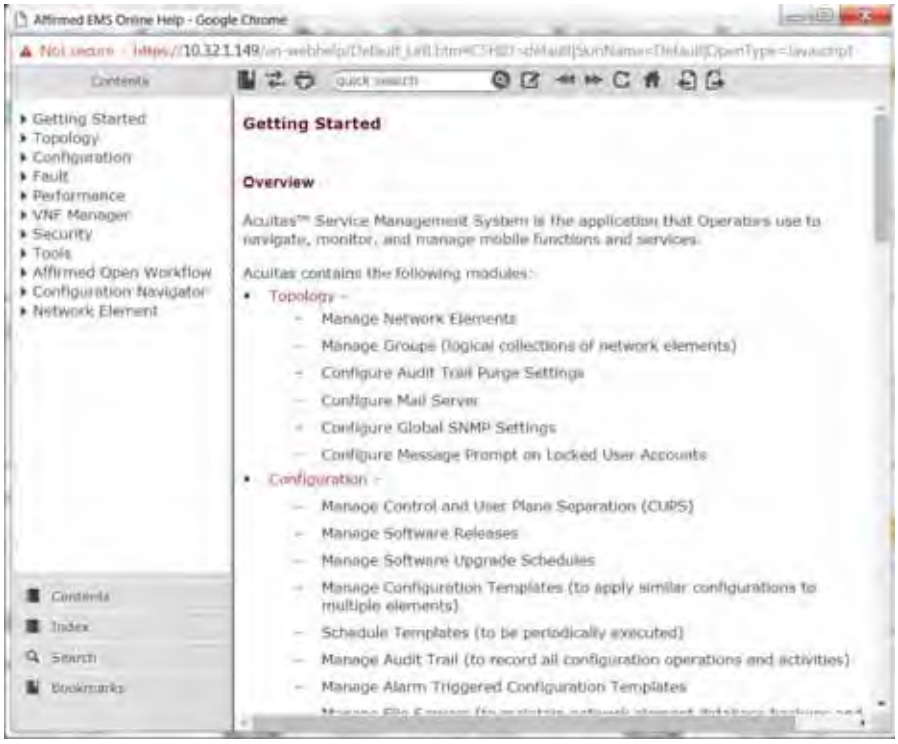
- Click **Help** from the **Settings** icon on the toolbar.

  Acuitas displays Help in a separate window, showing the context-sensitive help for Acuitas.

- Click **Help** or the **Help** icon ? from any dialog box.

  Acuitas displays Help in a separate window, showing the context-sensitive help topic for the particular dialog box.

Figure 1-6 Top-level Help Window



The Help window has the following areas:

- **Content pane** – The right pane displays the help information for a topic.
- **Navigation pane** – The left navigation pane allows you to select and move to specific topics of Help. This pane includes the following functions:
  - **Contents tab** displays the table of contents in the left pane with an expansion icon to list subtopics. Click an entry to display that topic in the content pane.
  - **Index tab** displays the index entries in the left pane. Click an index entry to display the referenced topic in the content pane.

  - **Search tab** displays the Search box and search results. Enter a search term to search for specific word(s) within Help and click **Search**. Topics containing the words are listed below the **Search** box. The results are ranked, with the most relevant topic listed first. Click a topic to display the topic in the content pane. The words in the topic that match the search term are highlighted in yellow.

    To add a search string to your favorites, click the **Add Search to Favorites** icon.
  - **Bookmarks tab** displays your Favorite topics and searches. Click a Favorite topic to display it in the content pane. Click a Favorite search to search for the saved search term.

    To delete a Favorite, mark its checkbox and click the **Delete Selected Favorite** icon.

- **Toolbar** – The toolbar icons allow you to move through Help and manage the display.
  - **Add Topic to Favorites** icon adds the active topic to your Favorites so that you can quickly access the topic later.
  - **Show/Hide Navigation** icon toggles between showing and hiding the navigation pane in the Help window.
  - **Print** icon opens the Print dialog so you can send the open topic to the printer.
  - **Quick Search** box initiates a search in the active topic for the word or phrase. Enter a search term and click the **Quick Search** icon.

    The words in the topic that match the search term are highlighted in yellow.
  - **Remove Search Highlighting** icon removes the highlighting from matching words of a previous search.
  - **Back and Forward** icons sequentially display a previously viewed sequence. Click Back to display the previously displayed topic in the content pane. Click Forward to display the next topic in a previously viewed sequence.
  - **Refresh** icon updates the content of the current topic.
  - **Home** icon opens the top-level help topic for Acuitas.
  - **Previous Topic and Next Topic** icons sequentially display information. Click **Next Topic** to display the next topic in the table of contents in the

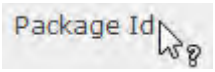
content pane. Click **Previous Topic** to display the previous topic in the table of contents.

In addition, the Configuration Navigator and the Affirmed Open Workflow applications provide ‘What’s This?’ Help on parameters.

To access ‘What’s This?’ Help:

1. Point the cursor at the parameter name for which you want Help.

   The cursor changes to the arrow and question mark icon.

2. Click the parameter name.

   Acuitas opens a pop-up window that displays the description of the parameter.

   The window remains open until you close it or click another parameter.

Logging Out of Acuitas

To log out of Acuitas:

1. Click **Logout** from the **Settings** icon on the toolbar.
2. At the confirmation prompt, click **OK**.
3. At the Logout Successful screen, click **Close**.

Navigating the System

Acuitas has an easy-to-use graphical user interface with a tree-based representation of the network in the left pane and tabs in the right pane.

Tree Display

The tree display allows you to view devices deployed in different locations.

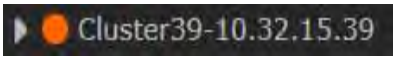
To open the tree display, click the **Toggle Resource Selection View** icon (next to the **Settings** icon) to expand the left pane.

The tree hierarchy includes:

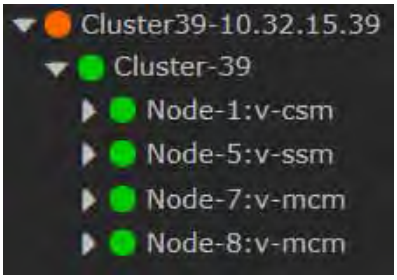
- Global Group – A global view of all the devices deployed. It depicts the topology of the elements installed in all the groups.
- Group – A logical group composed of few network elements/sub-groups. It depicts the topology of the sub-groups/elements deployed in the selected group.
- Devices – Depicts the deployed network elements.

In the tree display, the expansion icon indicates which objects contain other objects:

- If the expansion icon points to the right, the object is closed.



- If the expansion icon points down, the object is open, and the names of its contained objects are listed below it.



You navigate through objects in the tree much like you navigate through folders and files listed in a file management program. Click the expansion icons to open and close objects in the tree display.

Tabs

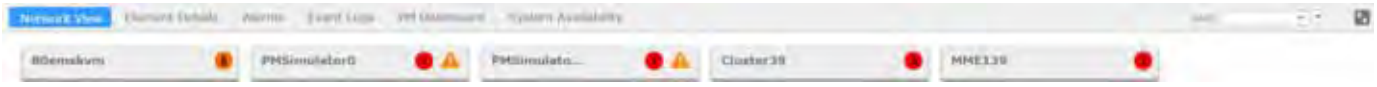
Tabs on the right panel apply to the Global level and the group level. The data displayed in each tab is filtered based on the elements in the selected group:

Network View

The Network View tab displays the devices connected to Acuitas in a grid.

By default, the Acuitas server is added the first time the server starts up. Each network element is added when you explicitly add it (see Adding Network Elements).

Figure 1-7 Devices in the Network View



Use the Sort box and the Ascending icon or Descending icon on the toolbar to sort the devices in the Network View. You can sort the devices alphabetically by:

- Name
- Status
- Resource Type

The sort is dynamic: Acuitas re-sorts the order every time you refresh the screen, you access the Network View tab, or the display updates.

To reposition a device in the grid, click the device and drag it to a location in the grid. When the highlighted rectangle appears, drop the device to that location. When you reposition a device, you override any previous sort (the sort is now in Manual mode) and the device position becomes fixed. Thereafter, any new devices are added at the end of the Network View, until you specify to sort the devices dynamically.

To view information for a device, double-click it to expand it in the Network View. To collapse the device, double-click it again.

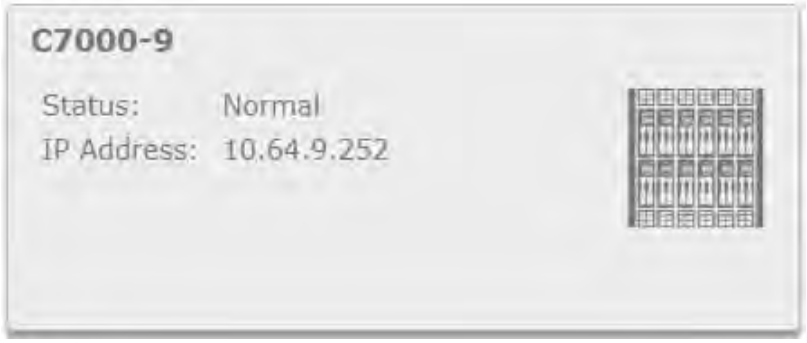
To expand all devices, click the Expand All icon on the toolbar.
To collapse all devices, click the icon again.

An expanded device lists the following information:

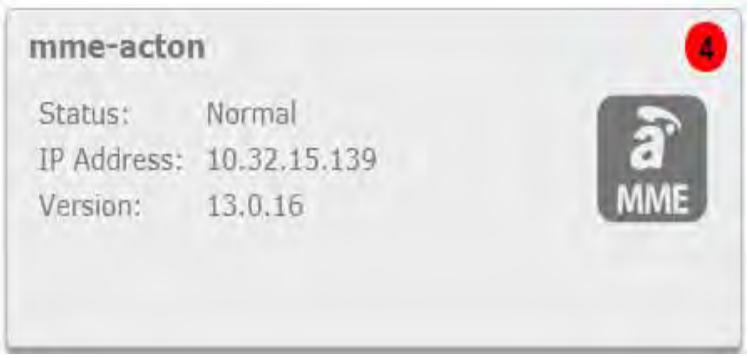
- Status
- IP Address
- Software Version
- *MCC Only*: Services deployed on the device (EPDG, GGSN, GTPPROXY, PGW, SGW, WAG, CPLANE, UPLANE)
- Alarm icon with color and count representing the highest severity alarms on the device
- Device type icon

MCC Icon

Blade System Device Icon



MME Device Icon



Server Group Device Icon

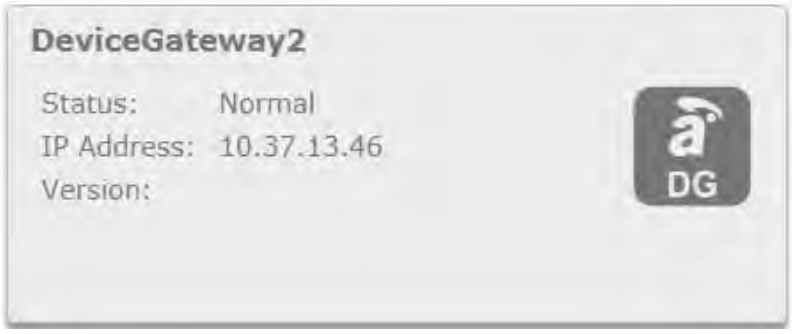
HPE HSS Icon

SPCRF EMS

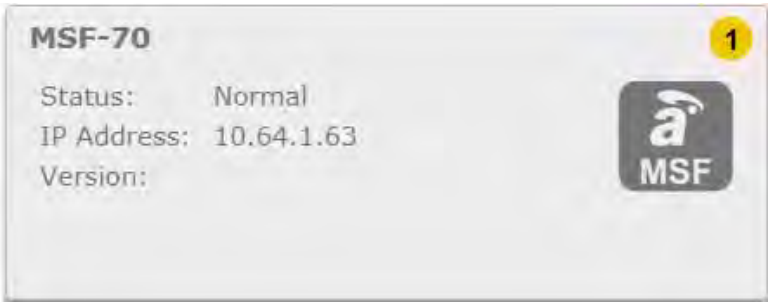
SSF Icon

SCEF Icon

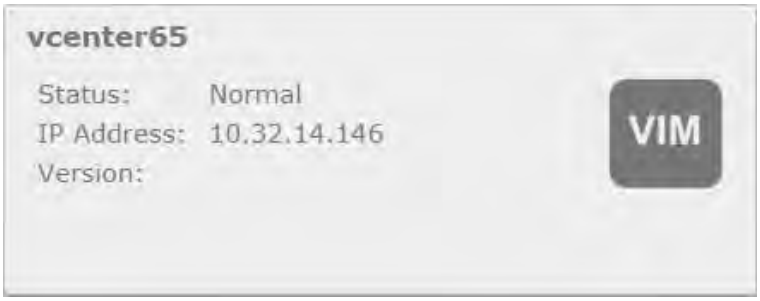
Device Gateway Icon



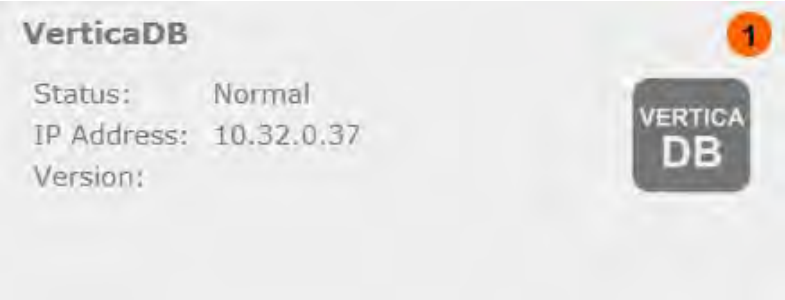
MSF Icon



VIM Icon



Vertica Icon



If the device is unreachable or unmanaged, the device lists the Status as Not Reachable, Unmanaged, or both.

If the device is collapsed, the device includes a status icon indicating whether it is:

- Not reachable
- Unmanaged
- Both

If the device is a member of a Geographic Redundancy Group, the device includes a **Geo Redundancy Group** icon.

If the device's Managed Fault management state is set to Managed but Acuitas is not configured as a trap destination of the network element, the device includes a red state icon.

If the device's Managed Fault management state is set to Unmanaged, the device lists the Status as FM Unmanaged and the device includes a grey state icon.

Element Details

The Element Details tab lists the details of the devices in the Network View, including Element Name, IP Address, Group, Type, Status, and Reachability.

Various operations can be performed on the devices from the toolbar and from the pop-up menu (right-click an NE and select the operation from the pop-up menu.)

To move a device to a different group, click the **Move to Group** icon on the toolbar. Select the group you want the device to reside and click **Save**.

Alarms

The Alarms tab lists the details of the alarms generated by the network system. Various operations can be performed on the alarms from the toolbar.

Host System Alarms

The Host System Alarms tab is visible only when a virtual node or cluster is selected in the tree. It lists the details of the alarms generated by host system components, such as iLO and Host alarms associated with a virtual node.

Event Logs

The Event Logs tab lists the details of the events occurring on devices.

PM Dashboard

The PM Dashboard displays the Key Performance Indicators (KPIs) collected during the previous 24 hours. For more information, see Viewing Key Performance Indicators.

System Availability

The System Availability tab displays a graphical representation of the following device metrics:

- Uptime % Meter: Uptime / (Uptime + Downtime) * 100
- Mean Time To Failure: Mean Uptime

  which equals (Sum of all Uptime/Number of Failures)
- Mean Time To Repair: Mean Downtime

  which equals (Sum of all Downtime/Number of Failures)
- Mean Time Between Failure: Mean Uptime + Mean Downtime

  which equals (Mean Time To Failure) + (Mean Time To Repair)

Note: *To view system availability, you must have the Performance > System Reachability security group permission. For instructions, see Specifying Permissions by Security Group.*

Using Icons

The following table defines Acuitas icons.

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
General icons:		
Add, Create, New		Add a new record
Apply Page Size		Specify how many records you want displayed per page
Ascending Order		Sort devices in the Network View in ascending order
Calendar		Select the required date from the calendar
Change Theme		Change the screen background color (dark or light)
Close, Exit		Close a window
Copy		Copy an existing configuration
Descending Order		Sort devices in the Network View in descending order
Delete		Delete a record
Edit, Modify		Modify a record
Expand All/Collapse All		Expand All/Collapse All devices in the network view.
Export		Export records to a file
First Page		Navigate to first page of records

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Import		Import a configuration template
Last Page		Navigate to last page of records
Manage/Unmanage		Manage/Unmanage a network element
Next Page		Navigate to next page of records
Obsolete		Set a software release obsolete so that it can no longer be used
Previous Page		Navigate to previous page of records
Print		Print the contents of the window or a specific record
Purge Now		Purge a record immediately
Refresh		Refresh display
Save		Save settings
Search		Search for records that meet a condition
Settings		Present list of operations to perform
Stop		Stop the ongoing activity in the current context
View		Display the details of the current record

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Alarm icons:		
Acknowledge Alarm		Acknowledge an alarm
Alarm Details		View alarm details
Alarm Forwarding		Forward an alarm to a user
Alarm Severity – Cleared		View Cleared alarms
Alarm Severity – Critical		View Critical alarms
Alarm Severity – Major		View Major alarms
Alarm Severity – Minor		View Minor alarms
Alarm Severity – Warning		View Warning alarms
Alarm Stats		View pie charts of the alarm statistics
Assign Owner		Assign a user to an alarm
Clear Alarm		Clear an alarm
Hide Cleared Alarms		Hide cleared alarms
Show Cleared Alarms		Show cleared alarms

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Reports and Performance icons:		
Bar Chart		Display data as a Bar Chart
Clear Chart		Clear a plotted chart
Column Properties		Configure column properties
Export as Chart PDF		Save data in the chart as a .pdf file
Export as CSV		Save data in the grid as a .csv file
Export as HTML		Save data in the grid as an .html file
Export as PDF		Save data in the grid as a .pdf file
Export as XLS		Save data in the grid as an .xls file
Export as XML		Save data in the grid as an .xlm file
Inspect Description		View description of an instance
Launch		Launch CSV statistics recovery schedule
Line Chart		Display data as a Line Chart
Metric Configuration		Specify metric to display in Dashboard
Outage Report		Display an Outage Report

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Pie Chart		Display data as a Pie Chart
Purge Data		Purges data older than a specified number of days
Stacked Area Chart		Display data as a Stacked Area Chart
Stacked Bar Chart		Display data as a Stacked Bar Chart
Rollback icons:		
Rollback		Rollback the specified software: ■ Network element software to the previous version ■ Network element DPI signature file to the previous version
Schedule icons:		
Disable		Disable a schedule
Enable		Enable a schedule
Quick Start		Implement a task immediately
Filter Management icons:		
Add Condition		Configure a filter based on specific parameters, values, and conditions
Apply to Table		Apply the filter to the Tabular view
Create AND Group		Create AND conditions
Create OR Group		Create OR conditions
Filter		Set up conditions to filter records

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Recurrence Pattern		Specify the recurrence details of a schedule
Reset Filter		Restore the existing filter
Show Filter Manager		Display dropdown of configured filters on the toolbar
Show Quick Filter		Display the Quick Filter on the toolbar
Backup and Restore icons:		
Restore Database		Restore the Acuitas database to an older backed up version
Scheduled Backup		Configure the Acuitas server to backup the database based on a schedule
Scheduled Backup View		View a scheduled database backup
CUPS Manager icons:		
Add New Control Plane/User Plane Pair		Add another User Plane to a Control Plane
Create CUPS Group		Add new group and configure the required objects on the Control Plane and User Plane
CUPS Group Description		View the details of the CUPS group
Delete		Remove a User Plane from the Control Plane
Edit		Perform an audit report of the configuration on the Control Plane and associated User Plane to identify differences. Replicate (synchronize) the configuration from the Control Plane to the User Plane.
View Fullscreen		Expand/collapse a CUPS group.

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Geographic Redundancy Manager icons:		
Compare Configuration		Compare configurations on primary and standby nodes in a geographic redundancy group
Geo Redundancy Group		Access the Geographic Redundancy Group Manager
Replicate Configuration		Replicate configurations between primary and standby nodes in a geographic redundancy group
Switchover		Trigger the standby node in a geographic redundancy group to become operationally active and take over service
View Chronological Switchover Log		View the chronological log of switchover events of each Geographic Redundancy group
View Recent Activities		View recent geographic redundancy activities
URL List Maintenance icons:		
Auto-Push		Enable Auto-Push to automatically push a clear-text URL file to all managed network elements every hour
Compare		Compare a clear-text URL file's current contents to its earlier file contents
Comparison File		View a comparison file listing URLs added or removed since the last time the file was marked as reviewed
Mark As Reviewed		Mark a clear-text URL file that is in the MODIFIED state as reviewed
Overwrite		Overwrite a clear-text URL file
Review and Edit		Review and edit URLs in a clear-text URL file

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
User Management icons:		
Active Users List		List active users
Audit Trail		List the activities for the user
Terminate User Sessions		Terminate active user sessions
Unlock User		Unlock a user whose access was blocked
Workflow icons:		
Close Carousel		Close Carousel
Create New		Create new referenced construct
Expand/Collapse All Rows		Expands/collapses all rows in the Service Evaluation report
Inspect Details		View details of an instance
Overview		View overview of all instances of a service function or service
Pause Update		Pause the workflow trace chart from updating
Plus		Drag and drop a service from the New list to the service flow
Remove		Remove an item
Start Update		Resume the workflow trace chart updating
Show Differences/Sync a Workflow		Compare/Synchronize a workflow on separate devices

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Service Flow Settings		Display additional Service Flow parameters.
Synchronize Scrolling		Controls the right and left scroll bars of the Service Comparison Details window. When the icon is selected, changing one scroll bar simultaneously changes the other scroll bar. When the icon is not selected, the scroll bars separately control their respective panes.
Validate Workflow		Validate the workflow
View/Modify		View/Modify an item
Zoom In/Zoom Out		Increase/decrease magnification of a workflow trace chart
VNF Manager icons:		
Add Managed Availability Zones		Add OpenStack Availability Zones to be managed by a Virtualized Infrastructure Manager (VIM)
Add /Create		Add new cluster, managed host, OVA template, or VM
Cluster Operations Virtual Machine Operations Graph Settings		Present list of operations to perform on a cluster Present list of operations to perform on a virtual machine Toggle a graph to full screen
Import Cluster Configuration		Import a csv file into the cluster
Manage Templates View VIM Configuration		Manage OVA templates View VIM configuration prerequisites
Policy Management		Manage scaling policies
Reports		View a cluster report (Network Elasticity or Network Inventory)
Scale In		View scale in activity
Scale Out		View scale out activity

Table 1-1 Acuitas Icons

Option	Icon	Use this option to...
Search Host		Search for available hosts
Unmanage		Unmanage an item
View Cluster Configuration		View or modify cluster configuration

Changing Screen Background Color (Theme)

To change the screen background color (dark or light):

1 Click the **Settings** icon on the toolbar and select **Change Theme**.

Changing Your User Password

You can change your user password.

To change your user password:

1. Click the **Settings** icon on the toolbar and select **Security => Change Password**.

   Acuitas displays the Change Password window.
2. Enter the new password in the **New Password** and **Confirm Password** fields.
3. Mark the **Send mail notification** checkbox to send an email notification.
4. To force a password change on next login, mark the **Password Change on Re Login** checkbox.
5. Click **Apply**.

Common Functionality

Acuitas uses common functionality in various areas of the application. They are:

- Filters – Customize the details that Acuitas displays based on specific parameters, values, and conditions.
- Column Properties – Specify which columns you want displayed and whether you want them to remain displayed so that you do not have to scroll to see them.
- Record Navigation – Specify how many records you want displayed per page. Navigate through multiple pages of records.
- Export Records
- Print Records
- Refresh the Screen

Filter Management

Creating Filters

You can configure filters to customize the details that Acuitas displays based on specific parameters, values, and conditions.

To create a filter:

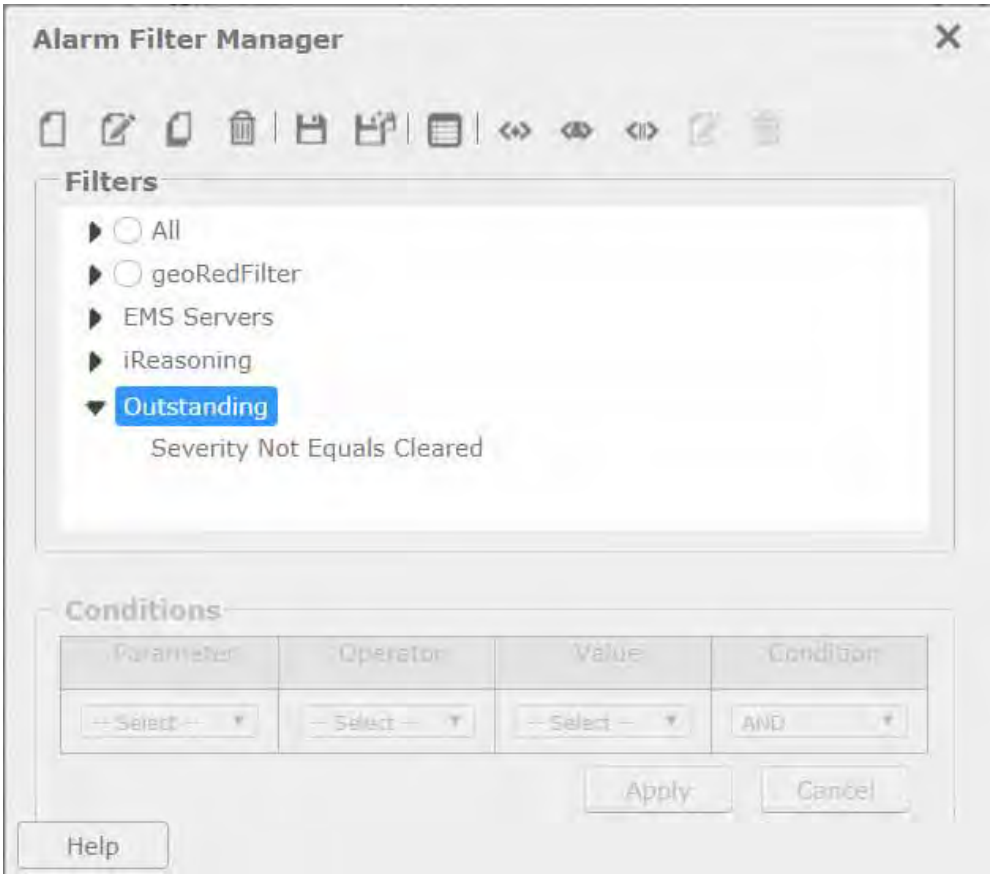
1. From the tab or window, click the **Filter** icon.

   Acuitas displays the **Filter Manager**.

2. Click the **New Filter** icon.
3. In the **Add Filter** dialog, enter the Filter Name and click **Add**. A filter with that name is created.
4. In the **Filter Manager**, select the filter and click the **Add Condition** icon:
   a. Complete the Conditions fields by selecting appropriate values for **Parameter**, **Operator**, **Value**, and **Condition**.

      The following example creates a filter of all outstanding alarms (filter name **Outstanding**). The Conditions are **Parameter** = Severity, **Operator** = Not Equals, and **Value** = Cleared.

Figure 1-8 Filter Manager



b Click **Apply**.

5 To add additional Conditions, repeat step 4. Specify **Condition** = AND or OR.

6 If the filter needs a combination of AND and OR conditions to achieve the desired result:

a In the **Filter Manager**, select the filter and click the **Create AND group** icon (or **Create OR Group** icon).

b In the **Filter Manager**, select the AND... (or OR...) group and click the **Add Condition** icon and complete the Conditions for the group.

c Click **Apply**.

7 To apply the filter to the table (to restrict the data in the table), click the **Apply to Table** icon.

8 Click the **Save Filter** icon.

Applying a Filter

Once you create a filter, you apply it to filter the details that Acuitas displays. From the tab or window, select your filter from the filter list to apply it.

If the filter list is hidden, click the **Show Filter Manager** icon to display the dropdown list.

Acuitas lists the details that meet the filter conditions. The following example shows an alarm filter that limits the list of alarms to all Outstanding alarms (alarms that have not cleared).

Figure 1-9 Select the Filter

Modifying Filters

To modify a filter:

1. From the tab or window, click the **Filter** icon.

   Acuitas displays the **Filter Manager**.

2. To change the filter name:

   a. Select the name and click the **Edit Filter Name** icon.

   b. Enter the new Filter Name and click **Update**.

3. To change a filter condition:

   a. Select the condition and click the **Edit** icon.

   b. Complete the Conditions fields by selecting appropriate values for **Parameter**, **Operator**, **Value**, and **Condition**.

      For example, to create a filter of all outstanding alarms, the Conditions could be **Parameter** = Severity, **Operator** = Not Equals, **Value** = Cleared.

   c. Click **Apply**.

4. To delete a filter condition:

   a. Select the condition and click the **Remove** icon.

b At the confirmation prompt, click **OK**.

5 To change an AND or OR group:

a Select the AND or OR group and click the **Edit** icon.

b Complete the Conditions fields by selecting appropriate values for **Parameter**, **Operator**, **Value**, and **Condition**.

c Click **Apply**.

6 To delete an AND or OR group:

a Select the AND or OR group and click the **Remove** icon.

b At the confirmation prompt, click **OK**.

7 To apply the filter to the table (to restrict the data in the table), click the **Apply to Table** icon.

8 Click the **Save Filter** icon.

Deleting a Filter

To delete a filter:

1 From the tab or window, click the **Filter** icon.

Acuitas displays the **Filter Manager**.

2 Select the name and click the **Delete Filter** icon.

3 At the confirmation prompt, click **OK**.

Using Quick Filters

You can use the Quick Filter to customize the details that Acuitas displays based on a specific parameter and value.

To use Quick Filter:

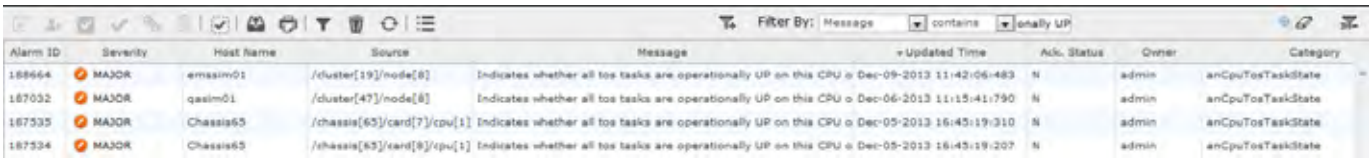
1 From the tab or window, click the **Show Quick Filter** icon.

2 In the **Filter By** field, specify the filter conditions (parameter, operator, and value).

The following example creates a Quick Filter of alarms where the **Message** field contains **operationally up**.

3 Click the **Search** icon to apply the Quick Filter.

Acuitas lists the details that meet the filter condition. The following example shows a Quick Filter that limits the list of alarms to alarms where the **Message** field contains **operationally up**.



To reset the Quick Filter to its original setting, click the **Reset Filter** icon.

Setting Column Properties

In various screens, you can specify which columns you want displayed and whether you want them to remain displayed so that you do not have to scroll to see them.

To configure column properties:

1. From the tab or window, click the **Column Properties** icon.
2. Mark the **Enabled** checkbox of the columns you want displayed. Unmark the checkbox of the columns you want hidden.
3. Mark the **Freeze** checkbox of the columns you want to remain displayed without requiring scrolling. Unmark the checkbox of the columns you want unfrozen.
4. Click **Apply**.

Sorting Column Data

To sort the data in a column in ascending alphanumeric order, click the column title. An up arrow in the column indicates ascending sort order.

To sort the data in a column in descending alphanumeric order, click the column title again. A down arrow in the column indicates descending sort order.

To return the sort order to the default setting, click the column title a third time.

Navigating through Records

In the case of a large number of record, Acuitas displays them over multiple pages. The current page and record count are listed at the bottom of the window.

Figure 1-10 Page Navigation Bar

To specify how many records you want displayed per page, enter the value in the **Page Size** box and click the **Apply Page Size** icon.

Use the icons to navigate over multiple pages:

- Previous Page
- Next Page
- First Page
- Last Page

To navigate to a specific page, enter the page number in the **Page** box.

Exporting Records

To export records:

1. From the tab or window, if desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.
2. Select the record(s) to be exported. To select multiple records, Shift-click or Control-click the records in the list. To export the Whole Data or Current View, do not select any records.
3. Click the **Export** icon.

   Acuitas displays the **Configure Export Parameters** window.

Figure 1-11 Configure Export Parameters Window

4 Configure the parameters as follows:

- **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
- **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
- **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
- **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.

5 Click **Apply**.

Acuitas displays the **Download Files** window.

6 Click **Download Exported File**.

7 From the **Download File**s window, click **Close**.

Printing Records

To print records:

1 From the tab or window, click the **Print** icon.

Acuitas displays the records in the **Print Preview** screen.

2 Click **Print** to print.

3 Select the printer and click **Print**.

Refreshing the Screen

Click the **Refresh** icon to refresh the screen with the latest data.

Chapter 2

Topology

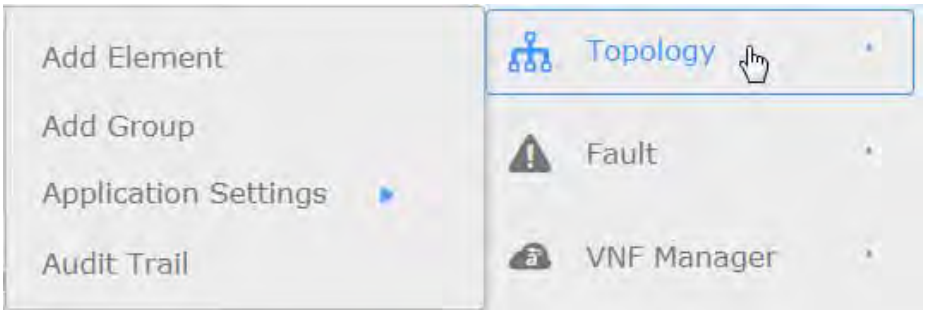
The Topology application provides tools to build a physical and logical topological model of the network. Network elements can be modeled as objects that are stored in the database, thus helping to manage individual or sets of network elements.

The following topics describe how to access and use the Topology applications:

- Groups
- Network Elements
- Audit Trail
- Configuring the Mail Server
- Configuring SNMP Settings
- Configuring Message Prompt on Locked User Accounts

To access Topology applications, select the applicable Topology option from the **Settings** icon on the toolbar.

Figure 2-1 Accessing Topology Applications



Groups

A group is a logical collection of network elements. The Global group is a parent group under which all groups reside.

You create a group to aggregate network elements for ease in monitoring and control. For example, you can create a group to represent a single customer, or customers located in a city or state, based on the purpose of deployment of the network elements.

Note: *For information on user-access control, see Adding Users.*

Adding Groups

Note: *To add a group, you must have the Topology > Group Details > Add Group security group permission. For instructions, see Specifying Permissions by Security Group.*

To add a group:

1. Use any of the following methods to add a group:

   Settings icon on the toolbar: Select **Topology => Add Group**.

   Pop-up menu: Right-click a group in the tree view and click **Add Group**.

   Acuitas displays the **Add Group** window.

2. In the **General Details** section, enter a name and description for the group.
3. In the **Group Details** section, expand the tree and mark the checkboxes of the devices you want in the group.
4. In the **Map Location Details** section, specify the location of the device (address or longitude and latitude of the location).
5. Click **Save**.
6. At the confirmation prompt, click **OK**.

Modifying Groups

Note: *To modify a group, you must have the Topology > Group Details > Edit Group security group permission. For instructions, see Specifying Permissions by Security Group.*

To modify a group:

1. Right-click the group in the tree view and click **Edit Group**.

   Acuitas displays the **Edit Group** window.

2. Make the necessary changes:
   - In the **General Details** section, enter a name and description for the group.
   - In the **Group Details** section, expand the tree and mark the checkboxes of the devices you want in the group.
   - In the **Map Location Details** section, specify the location of the device (address or longitude and latitude of the location).
3. Click **Save**.
4. At the confirmation prompt, click **OK**.

Deleting Groups

When you delete a group, all groups and network elements under that group are also deleted.

Note: *To delete a group, you must have the Topology > Group Details > Delete Group security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete a group:

1. Right-click the group in the tree view and click **Delete**.
2. At the confirmation prompt, click **OK**.

Network Elements

This topic describes how to manage the network element.

Adding Network Elements

You must explicitly add each network element.

Note: *To add a network element, you must have the Topology > Element Details > Add Element security group permission. For instructions, see Specifying Permissions by Security Group.*

Adding a Network Element

To add a network element:

1 Use any of the following methods to add network elements to a group:

Settings icon on the toolbar: Select **Topology => Add Element**.

Pop-up menu: Right-click an object in the tree and click **Add Element**.

Acuitas displays the **Add Network Element** window.

2 Configure the parameters as follows:

Table 2-1 Add Network Element Parameters

Parameter	Description
Device Type	Select the device type: ■ MCC (for MCC and SCEF) ■ c7000 blade system ■ MME ■ Server Group of virtual nodes ■ VIM ■ SSF ■ Siemens SPCRF ■ HPE HSS ■ Device Gateway ■ MSF ■ Vertica

Table 2-1 Add Network Element Parameters

Parameter	Description
General Details	
IP Version	Select IPv4 or IPv6. *(only IPv4 for Device Gateway)*
IP Address	The value you enter depends on the device type: ■ MCC or SCEF: Enter the Management Configuration Module (MCM) IP address. ■ c7000 blade system: Enter the IP address of the chassis, such as the blade system's enclosure iLO IP address. ■ MME: Enter the IP address of the MME ■ HP ProLiant DL380 virtual node: Enter the server iLO IP address (which is the IP address for which Acuitas should collect traps). ■ vCenter VIM: Enter the IP address of the vCenter server. ■ vCloud Director VIM: Enter the IP address of the vCloud Director server. ■ OpenStack VIM: Enter the IP address of the OpenStack controller. ■ SSF: Enter the IP address of the SSF ■ Siemens SPCRF: Enter the IP address of the Siemens SPCRF EMS ■ HPE HSS: Enter the IP address of the HPE HSS ■ Device Gateway: Enter the IP address of the Device Gateway ■ MSF: Enter the IP address of the MSF ■ Vertica: Enter the IP address of the VERTICA database
Name	Enter the display name of the network element. For MCC, MME, and SSF, the maximum allowed characters is 50 with no blank spaces allowed.
Description	Enter the description of the network element.
File Server	*(Applies to HPE HSS, MCC, MME, Siemens SPCRF, SSF, VIMS and MSFs only)* Select the file server.
VIM Protocol Details (Applies to VIMs only)	
Type	Select the VIM type: ■ vCenter ■ vCloudDirector ■ OpenStack

Table 2-1 Add Network Element Parameters

Parameter	Description
User Name	Enter the username. In the case of vCloud Director, enter the vCloud Director Organization login name
Password/Confirm Password	Enter the password for the user. Acuitas allows upper and lower case letters, numbers, and the following special characters for the CLI/NETCONF password: ([!@#$%^&*]) ***Note:*** *If you change the password on the network element, you must also change that account information here.*
FQDN *(Applies to vCenter only)*	The vCenter certificate is generated based on a Fully Qualified Domain Name. You must enter it so that Acuitas can access the vCenter server.
Connection URL*(Applies to vCloud Director only)*	Set the parameter to match the vCloud Director connection URL. For example, https://172.18.255.204
Organization Name *(Applies to vCloud Director only)*	Enter the vCloud Director organization name.
Admin User Name *(Applies to vCloud Director only)*	Enter the user name for the vCloud Director account with vCloud Director system administration privileges. This account is used by the VNF Manager to correlate hosting relationships between VMs and hosts. ***Note:*** *Without the Admin User Name and Admin Password, VNF Manager cannot correlate hosting relationships between VMs and hosts.*
Admin Password/Confirm Password *(Applies to vCloud Director only)*	Enter the password for the vCloud Director account with vCloud Director system administration privileges. ***Note:*** *Without the Admin User Name and Admin Password, VNF Manager cannot correlate hosting relationships between VMs and hosts.*
Identity Service Endpoint *(Applies to OpenStack only)*	Enter the Identity Service Endpoint, such as http://127.0.0.1:5000/v2.0 for REST API v2, or https://identity.affirmed.com:443/identity/v3 for REST API v3
Project/Tenant Name *(Applies to OpenStack only)*	Enter the OpenStack tenant (project)
Domain Name *(Applies to OpenStack only)*	Enter the Domain name. *Required for REST API v3.*
CLI & NETCONF (Applies to MCC, MME, SSF, MSF, and Vertica only)	
User Name	For an MCC, enter `emsadmin`. For an MME, enter `ems`. For an SSF, enter `admin`. For an MSF and Vertica, enter `root`.

Table 2-1 Add Network Element Parameters

Parameter	Description
Password/Confirm Password	Enter the password for the user. Acuitas allows upper and lower case letters, numbers, and the following special characters for the CLI/NETCONF password: ([!@#$%^&*]) ***Note:*** *If the MCC is configured to use pki (public key infrastructure) for ssh access, and the ssh key is protected by a passphrase, enter the passphrase.* ***Note:*** *If you change the password on the network element, you must also change that account information here.*
Port	For an MCC, enter port 2022. For an MME and SSF, enter port 830. For MSF and Vertica, enter port 22.
CLI Time Out	Leave as default value.
SFTP (Applies to MCC, MME, SSF, and MSF only)	
User Name	For an MCC and Vertica, enter `emsadmin`. For an MME and SSF, enter `ems`. For an MSF, enter `root`.
Password	Enter the password for the user. ***Note:*** *If the MCC is configured to use pki (public key infrastructure) for ssh access, and the ssh key is protected by a passphrase, enter the passphrase.*
Port	For an MCC and Vertica, enter port 2222. For an MME and SSF, enter port 22. For MSF, enter port 21.
SNMP	
SNMP Community	The Community string used for sending SNMP requests for data collection from the device. This value must match the value on the network element. The default community string is **affirmed**. For the c7000, Acuitas allows special characters.
Location Details Enter the Address of the network element.	

3 Click **Save**.

4 At the confirmation prompt, click **OK**.

5 If the Network Element is a blade system, proceed to Configuring Blade System Blades.

If the Network Element is a server group, proceed to Configuring Servers in a Group.

Viewing Network Elements

Note: *To view a network element, you must have the Topology > Element Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a network element:

1 Right-click the network element and click **View Element**.

Acuitas displays the **View Network Element** window, listing the parameters for the network element.

2 Click **Close** to close the window.

Modifying Network Elements

Note: *To modify a network element, you must have the Topology > Element Details > Modify Element security group permission. For instructions, see Specifying Permissions by Security Group.*

To modify a network element:

1 Right-click the network element and click **Edit Element**.

Acuitas displays the **Edit Network Element** window, listing the parameters for the network element.

2 Make the necessary changes:

Table 2-2 Edit Network Element Parameters

Parameter	Description
General Details	
IP Version	*Read Only:* IPv4 or IPv6.

Table 2-2 Edit Network Element Parameters

Parameter	Description
IP Address	The value you enter depends on the device type: ■ MCC or SCEF: Enter the Management Configuration Module (MCM) IP address. ■ c7000 blade system: Enter the IP address of the chassis, such as the blade system's enclosure iLO IP address. ■ MME: Enter the IP address of the MME ■ HP ProLiant DL380 virtual node: Enter the server iLO IP address (which is the IP address for which Acuitas should collect traps). ■ vCenter VIM: Enter the IP address of the vCenter server. ■ vCloud Director VIM: Enter the IP address of the vCloud Director server. ■ OpenStack VIM: Enter the IP address of the OpenStack controller. ■ SSF: Enter the IP address of the SSF ■ Siemens SPCRF: Enter the IP address of the Siemens SPCRF EMS ■ HPE HSS: Enter the IP address of the HPE HSS ■ Device Gateway: Enter the IP address of the Device Gateway ■ MSF: Enter the IP address of the MSF ■ Vertica: Enter the IP address of the VERTICA database
Name	Enter the display name of the network element. For MCC, MME, and SSF, the maximum allowed characters is 50 with no blank spaces allowed.
Description	Enter the description of the network element.
File Server	*(Applies to HPE HSS, MCC, MME, Siemens SPCRF, SSF, VIMs and MSFs only)* Select the file server.
VIM Protocol Details (Applies to VIMs only)	
Type	*Read Only:* VIM type
User Name	Enter the username. In the case of vCloud Director, enter the vCloud Director Organization login name
Password/Confirm Password	Enter the password for the user. Acuitas allows upper and lower case letters, numbers, and the following special characters for the CLI/NETCONF password: ([!@#$%^&*]) ***Note:*** *If you change the password on the network element, you must also change that account information here.*

Table 2-2 Edit Network Element Parameters

Parameter	Description
FQDN *(Applies to vCenter only)*	If the vCenter certificate was generated based on a Fully Qualified Domain Name, you must enter it so that Acuitas can access the vCenter server. If the certificate was generated based on an IP address, you must leave the field blank.
Connection URL*(Applies to vCloud Director only)*	Set the parameter to match the vCloud Director connection URL. For example, https://172.18.255.204
Organization Name *(Applies to vCloud Director only)*	Enter the vCloud Director organization name.
Admin User Name *(Applies to vCloud Director only)*	Enter the user name for the vCloud Director account with vCloud Director system administration privileges. This account is used by the VNF Manager to correlate hosting relationships between VMs and hosts. ***Note:*** *Without the Admin User Name and Admin Password, VNF Manager cannot correlate hosting relationships between VMs and hosts.*
Admin Password/Confirm Password *(Applies to vCloud Director only)*	Enter the password for the vCloud Director account with vCloud Director system administration privileges. ***Note:*** *Without the Admin User Name and Admin Password, VNF Manager cannot correlate hosting relationships between VMs and hosts.*
Identity Service Endpoint *(Applies to OpenStack only)*	Enter the Identity Service Endpoint, such as http://127.0.0.1:5000/v2.0 for REST API v2, or https://identity.affirmed.com:443/identity/v3 for REST API v3
Project/Tenant Name *(Applies to OpenStack only)*	Enter the OpenStack tenant (project) *Required for REST API v2 and optional for REST API v3.*
Domain Name *(Applies to OpenStack only)*	Enter the Domain name. *Required for REST API v3.*
CLI & NETCONF (Applies to MCC, MME, SSF, MSF, and Vertica only)	
User Name	For an MCC, enter `emsadmin`. For an MME, enter `ems`. For an SSF, enter `admin`. For an MSF and Vertica, enter `root`.

Table 2-2 Edit Network Element Parameters

Parameter	Description
Password/Confirm Password	Enter the password for the user. Acuitas allows upper and lower case letters, numbers, and the following special characters for the CLI/NETCONF password: ([!@#$%^&*]) ***Note:*** *If the MCC is configured to use pki (public key infrastructure) for ssh access, and the ssh key is protected by a passphrase, enter the passphrase.* ***Note:*** *If you change the password on the network element, you must also change that account information here.*
Port	For an MCC, enter port 2022. For an MME and SSF, enter port 830. For MSF and Vertica, enter port 22.
CLI Time Out	Leave as default value.
SFTP (Applies to MCC, MME, SSF, and MSF only)	
User Name	For an MCC and Vertica, enter `emsadmin`. For an MME and SSF, enter `ems`. For an MSF, enter `root`.
Password	Enter the password for the user. ***Note:*** *If the MCC is configured to use pki (public key infrastructure) for ssh access, and the ssh key is protected by a passphrase, enter the passphrase.*
Port	For an MCC and Vertica, enter port 2222. For an MME and SSF, enter port 22. For MSF, enter port 21.
SNMP	
SNMP Community	The Community string used for sending SNMP requests for data collection from the device. This value must match the value on the network element. The default community string is **affirmed**. For the c7000, Acuitas allows special characters.
Location Details Enter the Address of the network element.	

3 Click **Save**.

4 At the confirmation prompt, click **OK**.

5 If the Network Element is a blade system, proceed to Configuring Blade System Blades.

If the Network Element is a server group, proceed to Configuring Servers in a Group.

Configuring Blade System Blades

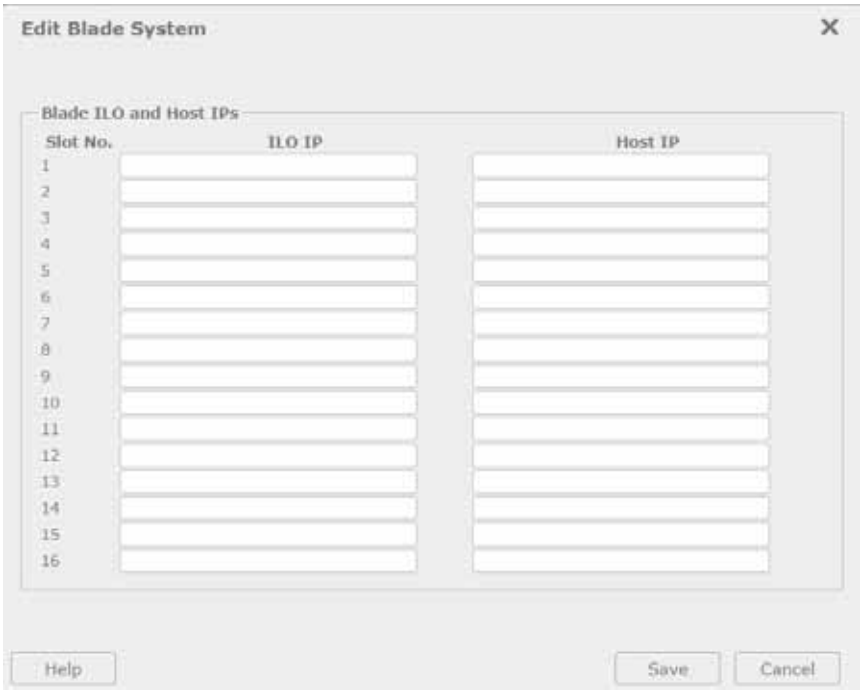
For an NE that is blade system, you need to configure each blade with an IP address for which Acuitas should collect traps.

To configure blades:

1 Use the following method to configure the blades:

Pop-up menu: Right-click the blade system and click **Configure Blades**.

Figure 2-2 Configure Blades Screen



2 For each slot, enter the blade iLO IP address and the Host IP address to which Acuitas should collect traps.

3 Click **Save**.

Note: *In addition to this procedure, you need to configure the Acuitas server IP address as an SNMP trap destination on the blade system management system.*

Configuring Servers in a Group

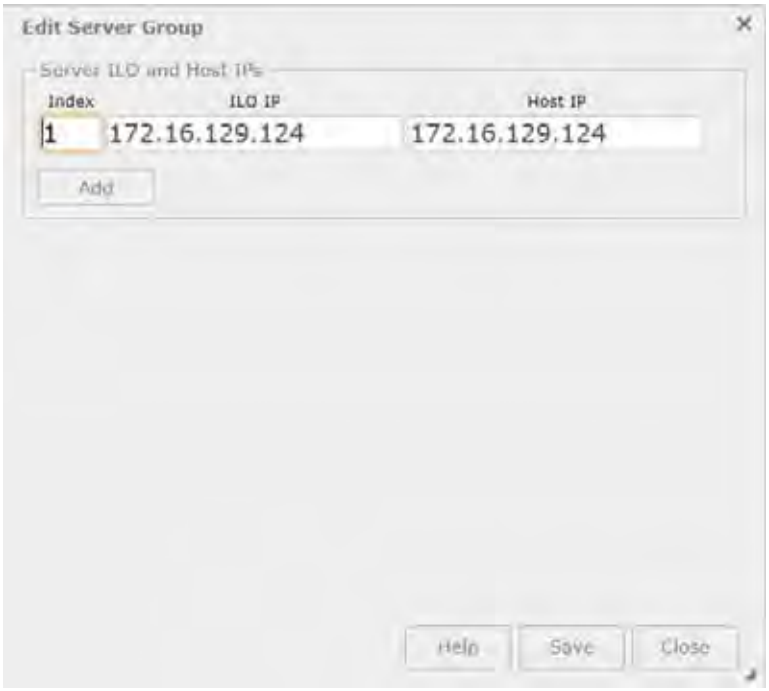
For an NE that is a server group, you need to configure each server's IP address for which Acuitas should collect traps.

To configure servers in a group:

1 Use the following method to configure the servers in a group:

Pop-up menu: Right-click the server group and click **Configure Server**.

Figure 2-3 Configure Server Screen



2 For each server in the group, enter the index, the iLO IP address, and the Host IP address to which Acuitas should collect traps and click **Add**.

In the case of OpenStack, issue the following commands on OpenStack CLI to identify the Hypervisor IP Addresses:

a Issue the following command to list the Hypervisor hostnames:

```
nova hypervisor-list
```

b Issue the following command to find the host IP for a Hypervisor:

```
nova hypervisor-show <hypervisor hostname>
```

3 Click **Save**.

Note: *In addition to this procedure, you need to configure the Acuitas server IP address as an SNMP trap destination on each server in the group.*

Adding Network Element Remarks

You can add remarks or notes to network elements. Remarks could provide information on usage of the network element, key observations, special configuration, and so on.

Note: *To add remarks to a network element, you must have the Topology > Element Details > Add NE Remarks security group permission. For instructions, see Specifying Permissions by Security Group.*

To add remarks to a network element:

1. Right-click a network element and click **NE Remarks**.

   Acuitas displays the **NE Notes** window, listing existing remarks.

2. Click **Add Note**.
3. Enter the notes. Acuitas automatically adds other details, including name of the user providing the remark, NE for which the remark is made, and the date and time of the remark.
4. Click **Apply**.
5. Click **Close** to close the window.

Deleting Network Elements

When you delete a network element from Acuitas, all associated configuration, historical statistics, and alarms are permanently deleted.

If you do not want to permanently delete the network element, but want to temporarily render it unaccessible by Acuitas, unmanage it instead. See Managing/Unmanaging Network Elements.

Note: *To delete a network element, you must have the Topology > Element Details > Delete Element security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete a network element:

1. Right-click a network element and click **Delete**.
2. At the confirmation prompt, click **OK**.

Managing/Unmanaging Network Elements

By default, a network element is in the Managed state (is accessible by Acuitas).

When a network element is in the Unmanaged state, is it not accessible by Acuitas. As a result, the following operations take place:

- Associated Template schedules are disabled.
- Associated Software schedules are disabled.
- Associated Performance Task schedules are disabled.
- Deep discovery is stopped.
- No traps are received.
- New Schedules cannot be created.
- Schedules cannot be quick run/force started.
- Schedules cannot be enabled.

When you Unmanage a Virtualized Infrastructure Manager (VIM), the VNF Manager rejects all communications to the VIM, including all lifecycle management commands and auto-discovery of the VIM configuration. For more information on the VNF Manager, see VNF Manager.

Note: *To manage/unmanage a network element, you must have the Topology > Group Details > Edit Group security group permission. For instructions, see Specifying Permissions by Security Group.*

To manage/unmanage a network element:

1. Right-click a network element and click **Manage/Unmanage**.
2. At the confirmation prompt, click **OK**.

Audit Trail

Audit Trail logs the Acuitas activities/events performed by the user. Audit trail is automatically enabled.

For instructions on how to view Audit Trail at the application level, see Audit Trail.

For instructions on how to stream Audit Trails and Alarms to the syslog Server, see Streaming Acuitas Audit Trails and Alarms to syslog.

Configuring Audit Trail Purge Settings

Note: *To configure Audit Trail purge settings, you must have the Topology > System Configuration > Configure Audit Trails Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure Audit Trail purge settings:

1. Click the **Settings** icon on the toolbar and select **Topology => Application Settings => Audit Trail Purge Settings**.
2. Select **Enable** and specify how many days (1 - 365) you want the Audit Trail saved.
3. Click **Save**.

Viewing the Topology Audit Trail

Note: *To view the Topology Audit Trail, you must have the Configuration > Config Audit Trails > View Config Audit Trails security group permission. For instructions, see Specifying Permissions by Security Group.*

Topology Audit Trail logs topology operation details.

To view the Topology Audit Trail:

1. Click the **Settings** icon on the toolbar and select **Topology => Audit Trail**.

   Acuitas displays the **Topology Audit Trail** window, listing the topology operations.
2. From the **Topology Audit Trail** window, use any of the following methods to view topology operation details:

   Toolbar: Select the operation and click the **View** icon.

Pop-up menu: Right-click the operation and click **View**.

Acuitas displays the **Audit Trail View** window, listing the following information:

- Resource Name
- Description
- User Name
- Date/Time
- Status

3 Click **Close** to close the window.

Exporting Topology Audit Trail

You can export the Topology Audit Trail to a CSV/PDF/XLS/XML/HTML file.

Note: *To export the Topology Audit Trail, you must have the Configuration > Config Audit Trails > Export Config Audit Trails security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To export the Topology Audit Trail:

1 Click the **Settings** icon on the toolbar and select **Topology => Audit Trail**.

2 If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.

3 Click the **Export** icon.

Acuitas displays the **Configure Export Parameters** window.

4 Configure the parameters as follows:

- **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
- **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
- **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
- **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.

5 Click **Apply**.

Acuitas displays the **Download Files** window.

6 Click **Download Exported File**.

7 From the **Download File**s window, click **Close**.

Streaming Acuitas Audit Trails and Alarms to syslog

You can configure Acuitas to stream the following entities to a remote syslog server:

- Configuration audit trails
- Topology audit trails
- Security audit trails
- Alarms

The syslog file is written in /var/log/affirmed.log.

To configure syslog on Acuitas:

1. Shutdown Acuitas server:

```
cd /opt/Affirmed/NMS/bin
./emsstop
```

2. Copy the existing version of the following file:

   /opt/Affirmed/NMS/server/ems/conf/ems-jboss-standalone.xml

   For example:

```
cp /opt/Affirmed/NMS/server/ems/conf/ems-jboss-standalone.xml
/opt/Affirmed/NMS/server/ems/conf/ems-jboss-standalone.xml.no_rsyslog
```

3. Edit the following file:

   /opt/Affirmed/NMS/server/ems/conf/ems-jboss-standalone.xml

4. Make the following changes.

   a. Add the following custom-handler under xml path:

```
"/server/profile/ <subsystem
xmlns="urn:jboss:domain:logging:2.0">" just before handler for
<size-rotating-file-handler name="SERVER_FILE">
       <custom-handler name="SYSLOG"
class="org.apache.log4j.net.SyslogAppender"
module="org.apache.log4j">
          <level name="INFO"/>
          <formatter>
             <pattern-formatter pattern="%d %-5p [%c] %x - %m%n"/>
          </formatter>
          <properties>
             <property name="Facility" value="LOCAL1"/>
             <property name="SyslogHost" value="localhost:51400"/>
          </properties>
        </custom-handler>
```

b Add the following logger under xml path:

```
"/server/profile/ <subsystem
xmlns="urn:jboss:domain:logging:2.0">" just after logger using
<handler name="SERVER_FILE"/> in <logger category="org.jboss"
use-parent-handlers="false">
       <logger category="syslogOutput"
use-parent-handlers="false">
          <level name="INFO"/>
          <handlers>
             <handler name="SYSLOG"/>
          </handlers>
       </logger>
```

c The syslogOutput includes only audit trail and alarms. If you need to stream any output in vm.log or other Acuitas log files to syslog, add the SYSLOG handler to those loggers.

5 Save the file.

6 Start the Acuitas server:

```
cd /opt/Affirmed/NMS/bin
./starttems.sh
```

Using rsyslog Server

This section describes how to configure the rsyslog server.

To install and configure rsyslog on Acuitas:

1 Complete this step if you need to install rsyslog on the server. Otherwise, skip to step 2.

a Obtain the rsyslog.repo file available at the following web site and place it in the /etc/yum.repos.d/ directory:

http://rpms.adiscon.com

b Issue the following command to add the package:

```
yum update rsyslog
Loaded plugins: product-id, security, subscription-manager
This system is not registered to Red Hat Subscription Management.
You can use subscription-manager to register.
rsyslog_v5 | 2.5 kB     00:00
rsyslog_v5/primary_db |  24 kB     00:00
Setting up Update Process
Package(s) rsyslog available, but not installed.
No Packages marked for Update
```

c Issue the following command to install the package:

```
yum install rsyslog
```

2 Edit the following file:

/etc/rsyslog.conf

3 Uncomment the following section to receive UPD syslog messages. Set the UDPServerRun parameter to the appropriate port. **Note:** The firewall must allow UDP on this port.

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 51400
```

In some versions of the file, you may have to uncomment following configuration to enable UDP syslog. **Note:** Only required once.

```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="5140")
```

4 Add the following line to print the sender IP Address in the log. **Note:** Enter the entire string on a single line.

```
#### GLOBAL DIRECTIVES ####
$template EmsFileFormat,"%TIMESTAMP% [%FROMHOST%] %syslogtag%%msg:::
sp-if-no-1st-sp%%msg:::drop-last-lf%\n"
```

5 Add the following line to log into the desired log file using the template specified in step 4. You can specify any path and filename:

```
LOCAL1.*  /var/log/affirmed.log;EmsFileFormat
```

6 Save the /etc/rsyslog.conf file.

7 Issue the following command to restart the rsyslog service:

```
service rsyslog restart
Shutting down system logger:       [  OK  ]
Starting system logger:            [  OK  ]
```

Configuring the Mail Server

You can set the parameters that specify how the application sends messages to the mail server, including SMTP access and authentication settings. If you configure alarm e-mail notification, Acuitas forwards alarms as e-mail to the mail server.

Note: *To configure the mail server, you must have the Topology > System Configuration > Configure Mail Server Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure the mail server:

1. Click the **Settings** icon on the toolbar and select **Topology => Application Settings => Mail Server**.

   Acuitas displays the **Mail Server** window.

2. Configure the parameters as follows:
   - **Primary SMTP Host Name** – Host name of the Simple Mail Transfer Protocol (SMTP) server.
   - **Secondary SMTP Host Name** – Another host name of the SMTP server, used in case of any failure in the Primary SMTP Host name.
   - **SMTP Port** – Port ID for the SMTP.
   - **SMTP User** – User name of the SMTP server.
   - **SMTP Password**– Password of the SMTP server.
   - **Confirm Password**– Confirmation of the entered password.
   - **Sender Name** – User name used for sending e-mail by the Acuitas server.
   - **Sender Mail ID** – Mail ID used for sending e-mail by the Acuitas server.
3. Click **Save**.

Configuring SNMP Settings

SNMP parameters are used as global SNMP settings.

Note: *These settings are not generally required for configuration.*

Note: *To configure SNMP settings, you must have the Topology > System Configuration > Configure SNMP Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure SNMP Settings:

1 Click the **Settings** icon on the toolbar and select **Topology => Application Settings => SNMP Settings**.

Acuitas displays the **SNMP Configuration** window.

2 To modify the default configuration, click the **Edit** icon.

3 Configure the parameters as follows:

Southbound SNMP Parameters:

- **No. of Retries** – Number of retries to send SNMP requests to a device.
- **Port** – Port number to which the SNMP request is sent for a device.
- **Timeout** – Timeout in milliseconds after an SNMP request to get a response from the device.

Northbound SNMP Parameters:

- **SNMP Version** – SNMPv2c or SNMPv3
- **Trap Community** – (SNMPv2c) Trap Community string used to forward alarms to trap receivers.
- **User Name** – (SNMPv3) Security name
- **Authentication Protocol** – (SNMPv3) MD5 or SHA
- **Authentication Password** – (SNMPv3) Secret key
- **Privacy Protocol** – (SNMPv3) DES or AES
- **Privacy Password** – (SNMPv3) Privacy key
- **Security Level** – (SNMPv3) noAuthNoPriv, authNoPriv, authPriv

4 Click **Save**.

Configuring Message Prompt on Locked User Accounts

The Administrator can configure the email ID to be included in the system-level message prompt to any user attempting to log into a locked or expired account. For example:

```
Please contact J.Doe@XYZCorp with your account request
```

Note: *To configure the email ID, you must have the Topology > System Configuration > Configure Admin Contact Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure the email ID:

1. Click the **Settings** icon on the toolbar and select **Topology => Application Settings => Administrator Settings**.

   Acuitas displays the **Administrator Details** window.

2. Configure the parameter as follows:

   - **Email ID** – Mail ID to be included in the system-level message prompt to any user attempting to log into a locked or expired account.

3. Click **Save**.

Chapter 3

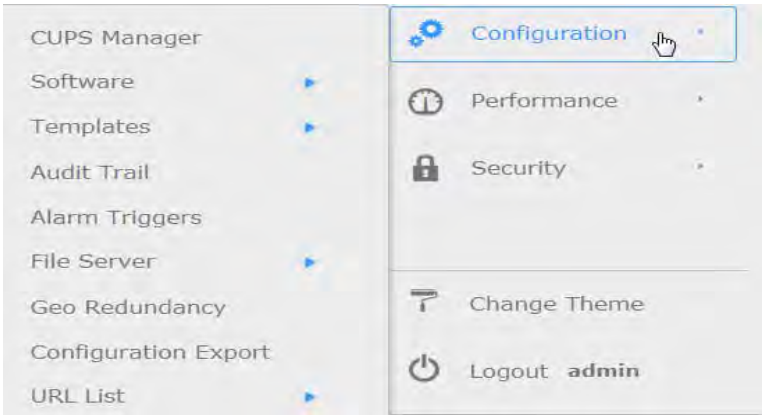
Configuration

The following topics describe how to access and use the Configuration applications:

- CUPS Manager
- Software Releases
- Software Schedules
- Software Rollback
- Configuration Templates
- Template Schedules
- Alarm Triggered Configurations
- Audit Trail
- File Servers
- Geographic Redundancy Manager
- Configuration Export Manager
- URL List Management

To access these applications, select the applicable option from the **Settings** icon on the toolbar.

Figure 3-1 Accessing Configuration Applications



CUPS Manager

The CUPS Manager supports managing Control and User Plane Separation (CUPS) in MCC devices. CUPS separates the Control Plane and the User Plane Function.

Note: *The Control Plane is also known as the Control Plane Function (CPF). The User Plane is also known as the User Plane Function (UPF).*

You can use the CUPS Manager to:

- Configure the required Sx interfaces and Packet Forwarding Control Protocol (PFCP) objects on the Control Plane and User Plane.
- Configure geo-redundant Control Planes in a Geographic Redundancy group:
  - Use the Geographic Redundancy Manager to set up the Geographic Redundancy group of Control Planes. Specify the primary Control Plane and secondary Control Plane. See Geographic Redundancy Manager.
  - Use the CUPS Manager to configure the primary Control Plane to Sxa/Sxb endpoints. See Configuring a CUPS Group. Use the Geographic Redundancy Manager to replicate this configuration to the secondary Control Plane. See Geographic Redundancy Manager.
  - In the Geographic Redundancy group, only the active Control Plane can communicate with the User Plane. If both Control Planes have active state, only the primary Control Plane can communicate with the User Plane.
- View the grouping for single or geo-redundant Control Plane(s) and associated User Plane(s).

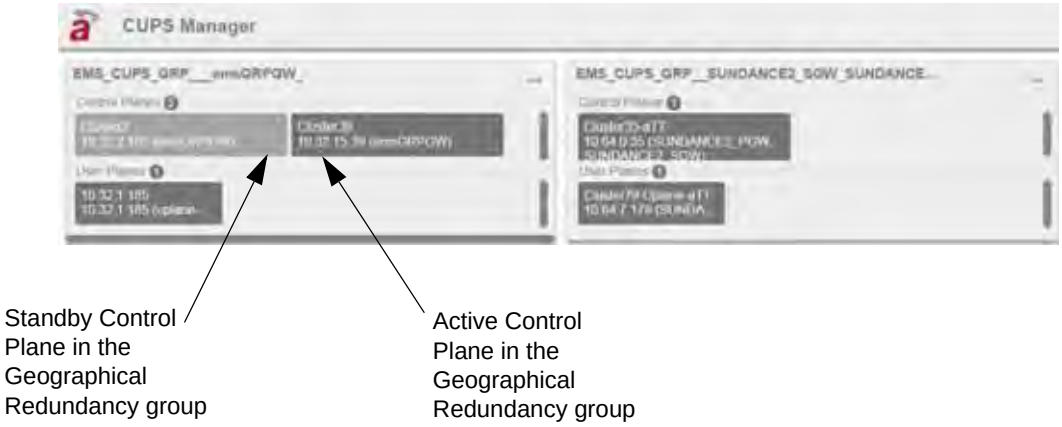
- Perform an audit report to identify configuration differences between the single Control Plane (or active Control Plane in the Geographic Redundancy group) and the User Plane.
- Replicate common configuration from the single Control Plane (or active Control Plane in the Geographic Redundancy group) to the User Plane.

To access the CUPS Manager application, click the **Settings** icon on the toolbar and select the **Configuration => CUPS Manager** option.

Note: *To access the CUPS Manager application, you must have the Configuration > CUPS Manager >Configuration security group permissions. For instructions, see Specifying Permissions by Security Group.*

Acuitas displays the **CUPS Manager** window showing the grouping of each Control Plane and associated User Plane(s), including those autodiscovered by the CUPS Manager and those explicitly configured with the CUPS Manager. The group name is autogenerated with the syntax EMS_CUPS_GRP_<*SGW Name*>_<*PGW Name*>.

Figure 3-2 CUPS Manager Window



In the case of geo-redundant Control Planes, the **CUPS Manager** window shows the grouping for the geo-redundant Control Planes and associated User Plane(s). The active Control Plane is displayed in dark grey; the standby Control Plane is displayed in light grey.

To expand a CUPS group to the full screen, click the **Menu Items** icon and select **Toggle Full Screen**.

To collapse the CUPS group, click the **Menu Items** icon and select **Toggle Full Screen** again.

To view the description of a CUPS group, click the **Menu Items** icon and select **Description**.

In the case of geo-redundant Control Planes, to view the associated Geographical Redundancy Group, click the **Menu Items** icon and select **Geo Redundancy**.

Using the Main Menu

To change the screen background color (dark or light):

1 Click the **Main Menu** icon on the toolbar and select **Change Theme**.

To access online Help:

1 Click the **Main Menu** icon on the toolbar and select **Help**.

Acuitas displays Help in a separate window, showing the context-sensitive help for Acuitas.

Configuring a CUPS Group

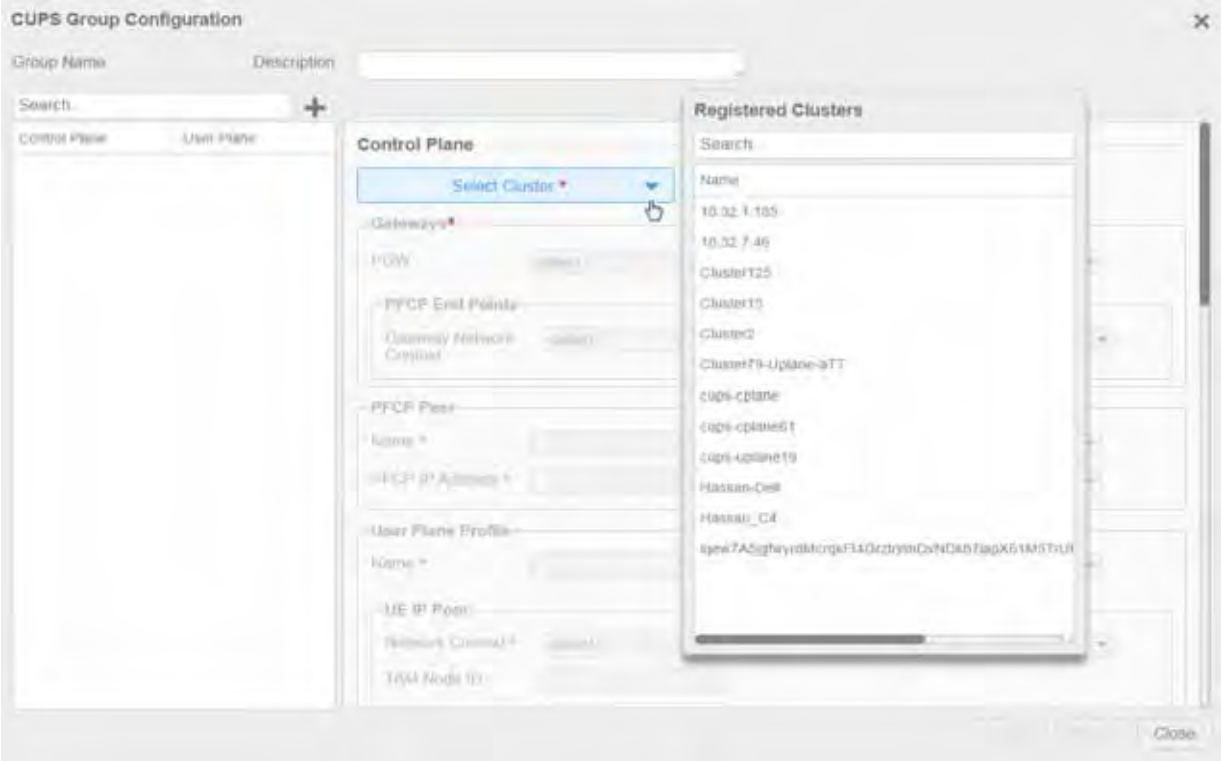
A CUPS group is the grouping of a Control Plane and its associated User Plane(s).

To configure a new CUPS group:

1 From the **CUPS Manager** window, click the **Create CUPS Group** icon in the right pane.

Acuitas displays the **CUPS Group Configuration** screen.

Figure 3-3 Selecting a Registered Cluster



2 Configure the parameters as follows:

Table 3-1 CUPS Group Configuration Parameters

Parameter	Description
Group Name	Read Only autogenerated name (when you save the group).
Description	Enter a description for the group.
Control Plane	
Select Cluster	Select a cluster for the Control Plane.
Gateways	

Table 3-1 CUPS Group Configuration Parameters

Parameter	Description
PGW	Select a PGW.
SGW	Select an SGW.
PFCP Endpoints	
Gateway Network Context	Select a network context (SX) on which this endpoint is anchored
Gateway Loopback IP	Select the primary loopback IP address.
PFCP Peer: Configure the PFCP Peer that the Gateway services point to.	
Name	Select or enter a name.
Network Context	Select the network context associated with this peer. The Control Plane and User Plane use different network contexts.
PFCP IP Address	Enter a PFCP IP Address of this peer.
PFCP Version	Select a PFCP version on the interface shared with this peer: ■ v1
User Plane Profile	
Name	Enter a name for this profile. Each User Plane requires a unique User Plane Profile.
State	Select the Admin state of this profile: ■ enabled ■ disabled
UE IP Pool	
Network Context	Select the network context associated with this profile.
IP Sub Pool	Select the IP Sub-pool associated with this profile. On the Control Plane, the IP Sub-pools are not advertised. On the User Plane, the IP Sub-pools are local to a specific User Plane.
TAM Node ID	Enter the Traffic Anchoring Mode (TAM) node ID associated with this IP Sub-pool in the User Plane. TAM mode is used to anchor the loopbacks and IP sub-pools on a specific node for Sx sessions.
User Plane	
Select Cluster	Select a cluster for the User Plane.

Table 3-1 CUPS Group Configuration Parameters

Parameter	Description
Network Profile 1 - 4 The User Plane requires at least one network profile configuration for each of the following interface types: ■ S1-U - GTP-U ■ S5-S8 - GTP-U SGW ■ S5-S8 - GTP-U PGW ■ S5-S8 - Lawful Intercept (LI) This enables Operators to choose the network contexts for the various User Plane network interfaces.	
Name	Select or enter a network profile associated with this service.
Interface Type	Select an interface type: ■ s1u-gtpu ■ s5s8-gtpu-sgw ■ s5s8-gtpu-pgw ■ lawful-intercept
Network Context	Select a network context.
PFCP Peer 1 - 2: Configure the PFCP Peer(s) that the user plane service points to.	
Name	Select or enter a name.
Network Context	Select the network context associated with this peer. The Control Plane and User Plane use different network contexts.
PFCP IP Address	Enter a PFCP IP Address of this peer.
PFCP Version	Select a PFCP version on the interface shared with this peer: ■ v1
User Plane Service	
Name	Enter a service name
Admin State	Select the Admin state of this service: ■ enabled ■ disabled

Table 3-1 CUPS Group Configuration Parameters

Parameter	Description
PFCP Link Down Queue Messages	Select whether to buffer data usage messages on the User Plane when the Packet Forwarding Control Protocol (PFCP) link is down between the User Plane and the Control Plane. ■ enabled ■ disabled When enabled, the UPF transmits the buffered data usage messages (as Sx Session Report messages) when the PFCP link is restored. This feature allows the CPF to more accurately report data usage for CDRs and offline interfaces even with intermittent PFCP link failures.
PFCP Endpoints	
Network Context	Select a network context (SX) on which this endpoint is anchored
Loopback IP	Select the primary loopback IP address.
Common *PFCP Profile:* Configure the common settings for both the Control Plane and the User Plane.	
Name	Select or enter the name of the profile
Association Retry Interval	Enter the amount of time in milliseconds the PGW/SGW User Plane waits before re-initiating an Sx association if the association is down.
Node Response Timeout	Enter the amount of time in milliseconds the PGW/SGW User Plane waits for the peer to respond. If it does not receive a response, the message is retransmitted based on the Node Restransmit Count value.
Node Retransmit Count	Enter the number of message retransmissions to send before declaring a path down.
Periodic Interval	Enter the amount of time in milliseconds to wait before retransmitting a heartbeat request.
Guard Time Interval	Enter the amount of time in milliseconds to wait before tearing down the Sx association.
Session Keep Alive Time Interval	Enter the amount of time in minutes to wait before sending monitor messages to a peer. Value 0 disables monitoring (even when Clear on Session Monitor Failure is enabled) ***Note:*** *This parameter only sends the monitor message if it does not receive any session-level messages during the configured interval.*

Table 3-1 CUPS Group Configuration Parameters

Parameter	Description
Clear on Session Monitor Failure	Select whether to clear a session upon monitor timeout or link failure. ■ enabled ■ disabled If disabled, sessions are cleared only if PFCP_CTXT_NOT_FOUND is received.

3 Click **Save**.

The CUPS Manager adds the Control Plane/User Plane pair to the left pane.

4 To close the screen, click **Close**.

Adding Another User Plane to the Control Plane

To add another User Plane to the Control Plane:

1 From the **CUPS Manager** window, on the group, click the **Menu Items** icon

and select **Edit CUPS Group**.

2 In the left pane, click the **Add New Control Plane/User Plane Pair** icon. .

3 Enter new parameter values for the new User Plane (see Table 3-1).

4 Click **Save**.

The CUPS Manager adds the new Control Plane/User Plane pair to the left pane.

5 To close the screen, click **Close**.

Removing a User Plane from the Control Plane

To remove a User Plane from the Control Plane:

1 From the **CUPS Manager** window, on the group, click the **Menu Items** icon

and select **Edit CUPS Group**.

2 In the left pane, select a Control Plane/User Plane pair (Use the **Search** text box in the left pane to search for a particular pair).

3 Click the **Delete** icon to remove the User Plane from the Control Plane.

Figure 3-4 Removing a User Plane from the Control Plane

4 At the confirmation prompt, type **Yes** and click **Yes**.

Note: *Removing the last User Plane from the Control Plane deletes the entire group. To avoid this situation, add another User Plane to the Control Plane before removing the desired User Plane.*

Viewing the Details of a Control Plane/User Plane Pair

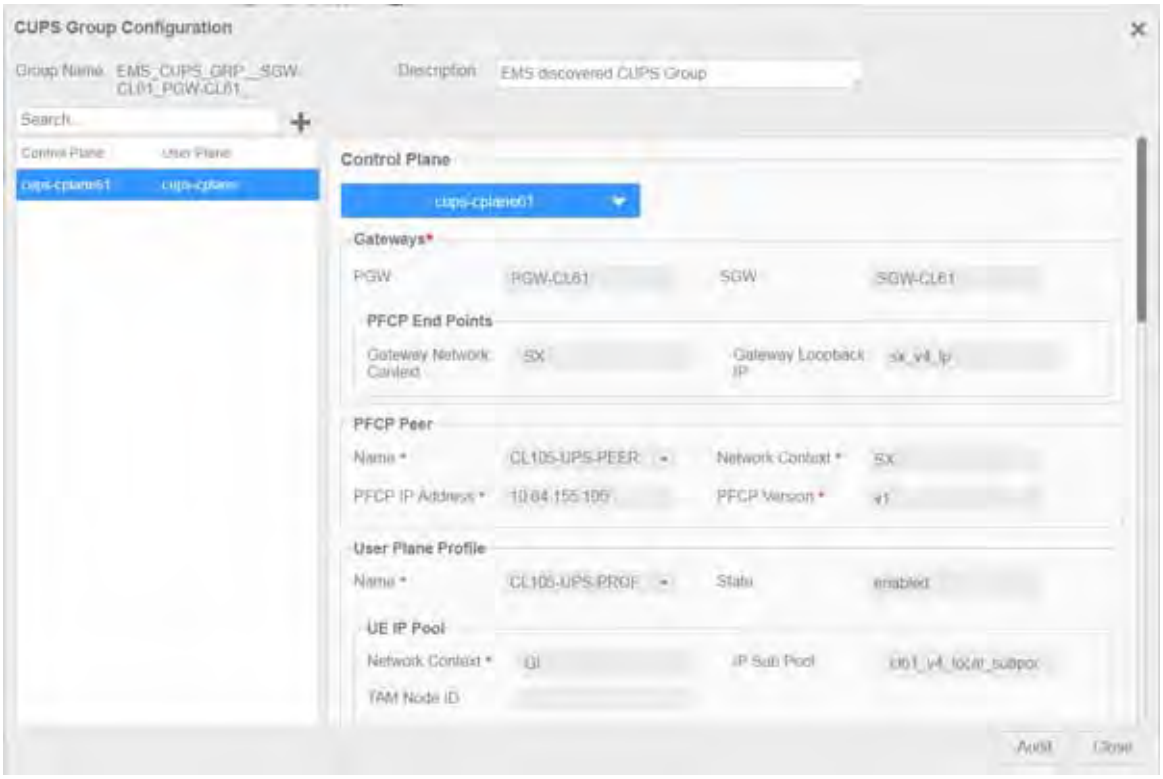
To view the details of a pair of single Control Plane (or active Control Plane in the Geographic Redundancy group) and the User Plane, click one of the entities in the CUPS group.

Figure 3-5 Selecting an Entity in the CUPS Group

In the left pane, select a Control Plane/User Plane pair (Use the **Search** text box in the left pane to search for a particular pair).

Acuitas displays the **CUPS Group Configuration** screen for the pair. The fields are Read Only.

Figure 3-6 Viewing a Control Plane/User Plane Pair



To close the screen, click **Close**.

Auditing and Replicating Configuration

You can perform an audit report to identify configuration differences between a single Control Plane (or active Control Plane in the Geographic Redundancy group) and the User Plane. And, you can replicate (synchronize) common configuration from the single Control Plane (or active Control Plane in the Geographic Redundancy group) to the User Plane.

To audit and replicate configuration:

1. From the **CUPS Manager** window, on the group, click the **Menu Items** icon

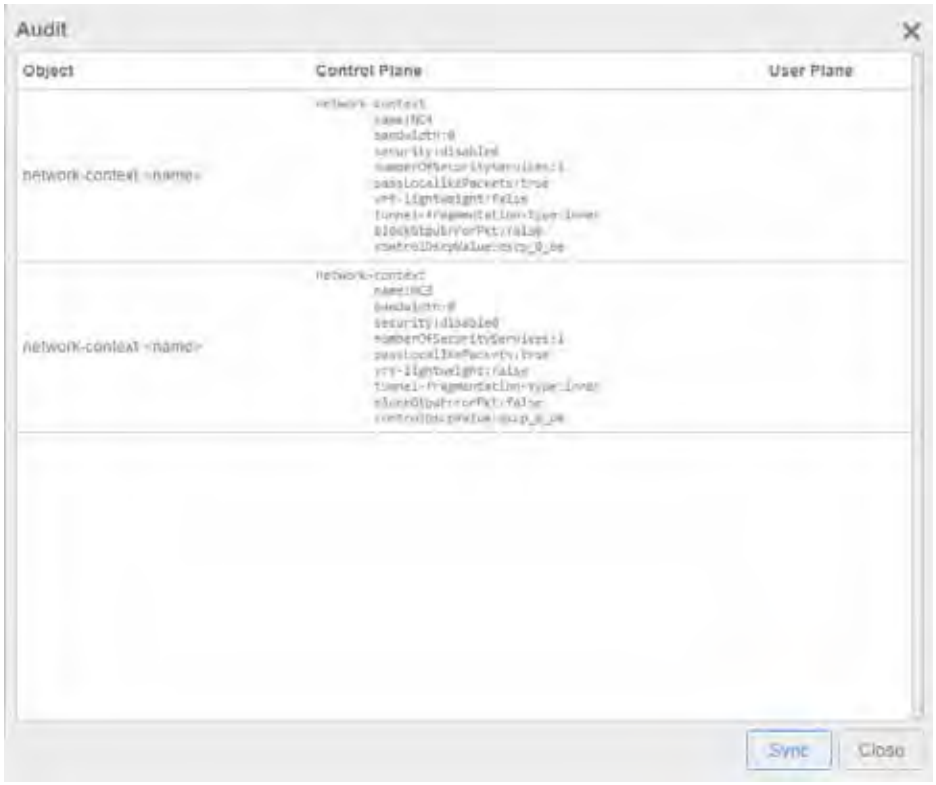
   and select **Edit CUPS Group**.

2. In the left pane, select a Control Plane/User Plane pair (Use the **Search** text box in the left pane to search for a particular pair).

3. Click **Audit**.

   Acuitas displays the **Audit** window, listing configuration differences between the Control Plane and associated User Plane.

Figure 3-7 Audit Window



4 To replicate the configuration from the Control Plane to the User Plane in the pair, click **Sync**.

5 At the confirmation prompt, type **Yes** and click **Yes**.

6 Click **Close**.

Entities Replicated

For an entity to be replicated, you must have Write or Admin security group permissions to that entity. For example, a user with the Configuration > MCC Configuration > Workflow Provisioning > Write or Admin security group permissions can replicate the Workflow Data Profile.

If you do not have a specific role assigned, the objects with those roles *are not* replicated.

For instructions, see Specifying Permissions by Security Group.

The following tables list the configuration objects on the Control Plane that are replicated on the User Plane during the replication process.

Table 3-2 Common Service-Construct Configuration

Command
service-construct advice-of-charge <*name*>
service-construct advice-of-charge <*name*> charging-notification-list <mscc-result-code>
service-construct aoc-hardware-id-format <*name*>
service-construct application-rule-group
service-construct ca-certificate-list <*name*>
service-construct ca-certificate-list <*name*> ca-certificate <*name*>
service-construct content-insertion content-insertion-profile
service-construct content-insertion insertion-object-list
service-construct data-record-template http-proxy http-transaction
service-construct diffserv-profile dscp-mapping <*code*>
service-construct domain-rule-group <*name*>
service-construct edr-flow-network-stats-profile <*name*>
service-construct edr-interface-profile <*name*>
service-construct edr-interface-profile <*name*> edr-service-profile <*name*>
service-construct edr-server-profile <*name*>
service-construct edr-session-data-stats-profile <*name*>
service-construct host-list
service-construct host-list ip-address
service-construct http-header-enrichment
service-construct http-rule-group <*name*>
service-construct http-url-rewrite <*name*>
service-construct ip-list
service-construct ldap profile
service-construct mms mmsc-group
service-construct packet-filter
service-construct pdngw-list
service-construct protocol-application-rule-group <*name*>
service-construct quality-of-service <*name*>

Table 3-2 Common Service-Construct Configuration

Command
service-construct service-rule
service-construct session-rule-group
service-construct session-rule-group rule
service-construct service-rule packet-filter
service-construct sms smsc-group
service-construct static-dns-map
service-construct static-dns-map host
service-construct tcp-optimization-profile
service-construct time-of-day-rule-group rule
service-construct tls-rule-group <*name*>
service-construct tls-rule-group <*name*> rule <*name*>
service-construct ua-profile <*name*>
service-construct url-list

Table 3-3 Common Services Configuration

Command
services affirmed-apps fair-bandwidth-usage-service-profile
services charging billing-plan
services charging charging-instance
services charging rating-group
services content-cache
services content-cache instance <*name*>
services content-filter instance
services crbn-profile <*name*>
services dns-proxy
services dns-proxy dns-ip-flow
services dns-proxy dns-policy
services dns-proxy instance

Table 3-3 Common Services Configuration

Command
services dns-proxy static-dns-map
services dns-proxy tunnel-detection-profile
services http-proxy
services http-proxy abr-optimization-profile
services http-proxy encryption-profile
services http-proxy explicit-proxy-profile
services http-proxy http-ip-flow
services http-proxy http-request-policy
services http-proxy http-response-policy
services http-proxy https-profile
services http-proxy http-transaction-record-profile
services http-proxy instance
services http-proxy fraud-detection-profile
services http-proxy sps-attribute
services http-proxy sps-profile
services http-proxy steering-group
services http-proxy tcp-splicing-policy
services http-proxy tcp-splicing-profile
services http-proxy toll-free-profile
services http-proxy web-image-optimization profile
services http-server instance
services metering geo-redundant-group
services metering metering-instance
services quality-of-service qos-flow
services quality-of-service qos-policy
services sip-proxy instance
services steering steering-flow
services steering steering-policy

Table 3-3 Common Services Configuration

Command
services subscriber-firewall subscriber-firewall-policy
services video-adaptation instance
services wap-gateway instance

Table 3-4 Common Network-Context Configuration

Command
network-context <*name*>

Table 3-5 Common Workflow Configuration

Command
workflow data-profile <*name*>
workflow data-profile <*name*> geo-redundant-group <*name*>
workflow data-profile <*name*> metering-service <*name*>

Table 3-6 Common Zone Configuration

Command
zone <*name*> gateway apn <*name*>
zone <*name*> gateway apn <*name*> associated-ue-pool <*name*>
zone <*name*> gateway apn <*name*> charging <*name*>
zone <*name*> gateway enhanced-features-list <*name*>
zone <*name*> gateway filter-id-pco-action-association-table <*name*>
zone <*name*> gateway pcscf-table <*name*>
zone <*name*> gateway profile qci-profile <*name*>
zone <*name*> gateway service-rule-pco-action-association-table <*name*>

Table 3-7 Other Configuration

Command
flow-idle-timeout-profile <*name*>
geographic-redundancy group <*name*>
infrastructure file-management profile <*type*> <*prefix*>
networking-profiles neighbor-discovery-profile <*name*>

Use Cases

The following use cases demonstrate how to use the CUPS Manager to configure CUPS groups.

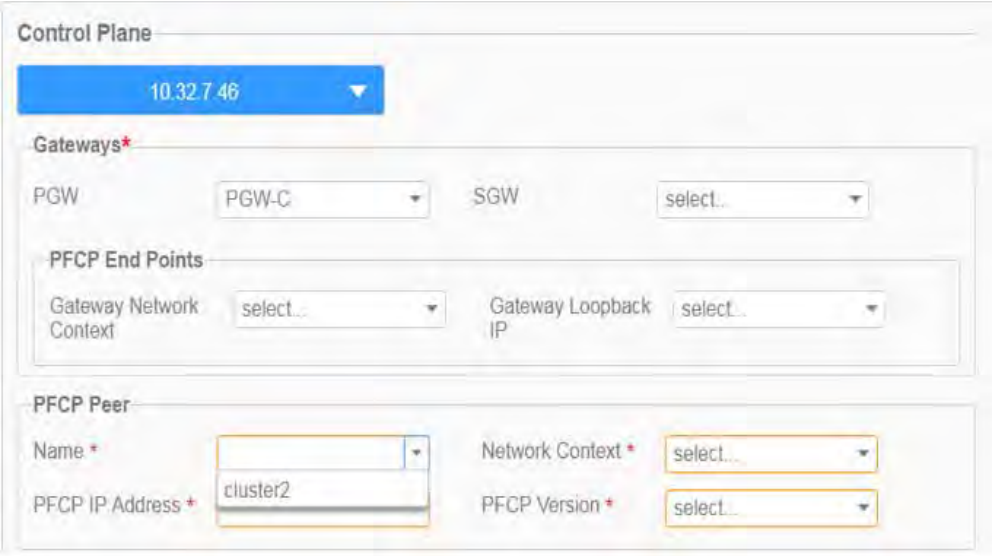
Configuring a PGW-based CUPS Group

To configure a PGW-based CUPS Group:

1. Configure a new PGW using either the CLI or the Configuration Navigator. For an existing PGW, skip this step.
2. From the **CUPS Manager** window, click the **Create CUPS Group** icon in the right pane.

   Acuitas displays the **CUPS Group Configuration** screen.
3. Under **Gateways**, in the **PGW** field, select the PGW.
4. Under **PFCP Endpoints**, select the PFCP endpoints for the PGW:
   - Gateway Network Context — Select a network context (SX) on which the endpoint is anchored.
   - Gateway Loopback IP — Select the primary loopback IP address.
5. Under **PFCP Peer**, specify the PFCP Peer that the PGW points to. Either configure the Peer:
   - Name — Select or enter a name.
   - Network Context — Select the network context associated with this peer.
   - PFCP IP Address — Enter a PFCP IP Address of this peer.
   - PFCP Version — Select a PFCP version on the interface shared with this peer

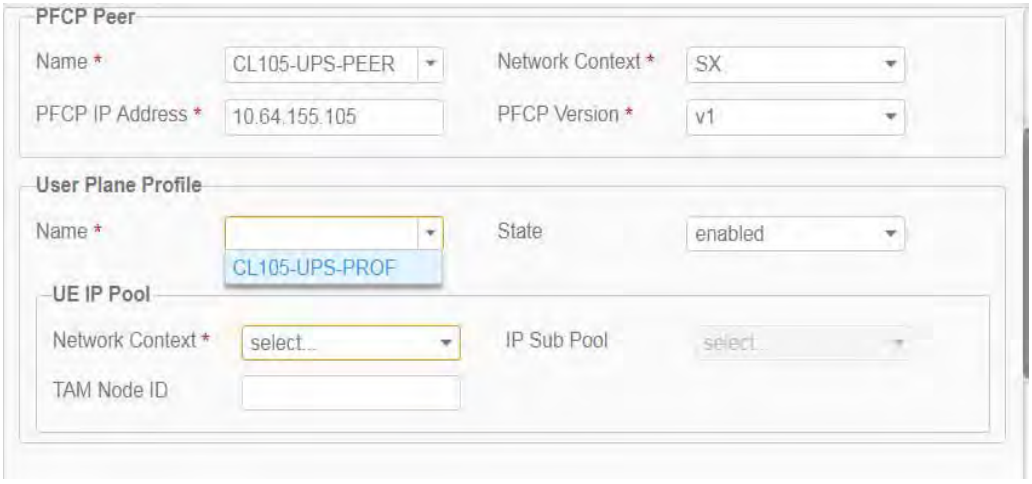
   Or select an existing Peer, as shown in the following figure:



6 Under **User Plane Profile**, specify the User Plane Profile to associate with the PFCP Peer. Either configure the User Plane Profile:

- Name — Enter a name for this profile.
- State — Select the Admin state of this profile:
- Network Context — Select the network context associated with this profile.
- IP Sub Pool — Select the IP Sub-pool associated with this profile.
- TAM Node ID — Enter the Traffic Anchoring Mode (TAM) node ID associated with this IP Sub-pool in the User Plane.

Or select an existing User Plane Profile as shown in the following figure:



7 Configure the remaining fields of the **CUPS Group Configuration** screen (see CUPS Group Configuration Parameters) and click **Save**.

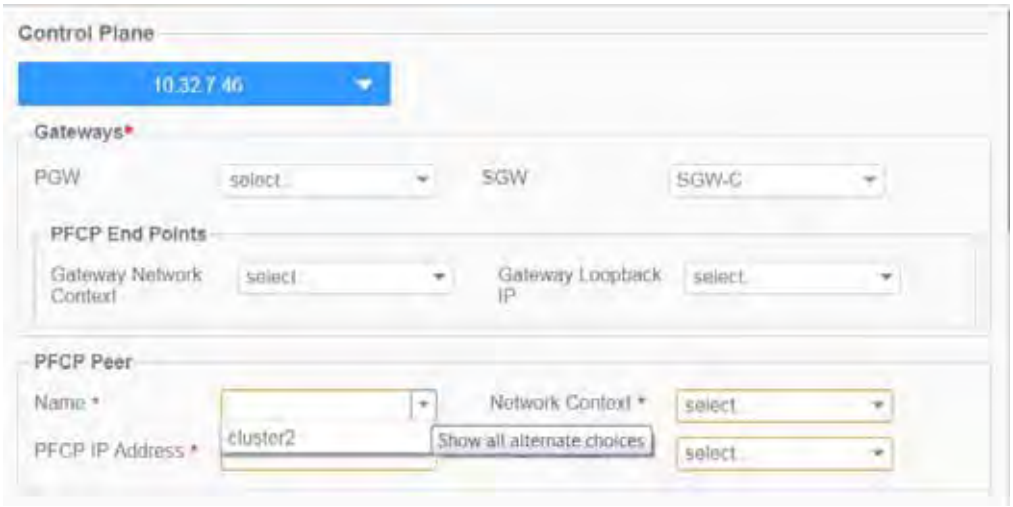
Configuring a SGW-based CUPS Group

To configure a SGW-based CUPS Group:

1. Configure a new SGW using either the CLI or the Configuration Navigator. For an existing SGW, skip this step.
2. From the **CUPS Manager** window, click the **Create CUPS Group** icon in the right pane.

   Acuitas displays the **CUPS Group Configuration** screen.
3. Under **Gateways**, in the **SGW** field, select the SGW.
4. Under **PFCP Endpoints**, select the PFCP endpoints for the SGW:
   - Gateway Network Context — Select a network context (SX) on which the endpoint is anchored.
   - Gateway Loopback IP — Select the primary loopback IP address.
5. Under **PFCP Peer**, specify the PFCP Peer that the SGW points to. Either configure the Peer:
   - Name — Select or enter a name.
   - Network Context — Select the network context associated with this peer.
   - PFCP IP Address — Enter a PFCP IP Address of this peer.
   - PFCP Version — Select a PFCP version on the interface shared with this peer

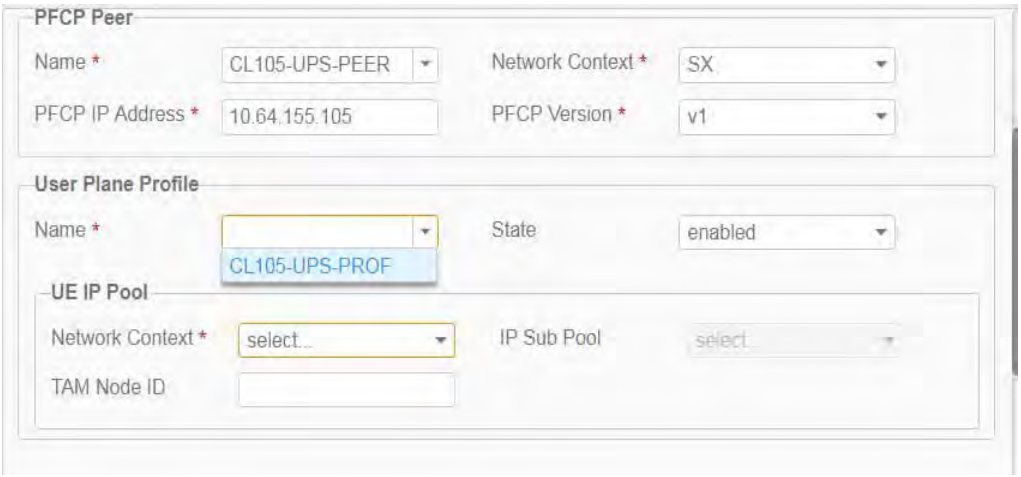
   Or select an existing Peer, as shown in the following figure:



6. Under **User Plane Profile**, specify the User Plane Profile to associate with the PFCP Peer. Either configure the User Plane Profile:
   - Name — Enter a name for this profile.
   - State — Select the Admin state of this profile:

- Network Context — Select the network context associated with this profile.
- IP Sub Pool — Select the IP Sub-pool associated with this profile.
- TAM Node ID — Enter the Traffic Anchoring Mode (TAM) node ID associated with this IP Sub-pool in the User Plane.

Or select an existing User Plane Profile as shown in the following figure:



7 Configure the remaining fields of the **CUPS Group Configuration** screen (see CUPS Group Configuration Parameters) and click **Save**.

Configuring a PGW- and SGW-based CUPS Group

To configure a PGW- and SGW-based CUPS Group:

1 Configure a new PGW and new SGW using either the CLI or the Configuration Navigator. For existing PGW and SGW, skip this step.

2 From the **CUPS Manager** window, click the **Create CUPS Group** icon in the right pane.

Acuitas displays the **CUPS Group Configuration** screen.

3 Under **Gateways:**

- In the **PGW** field, select the PGW.
- In the **SGW** field, select the SGW.

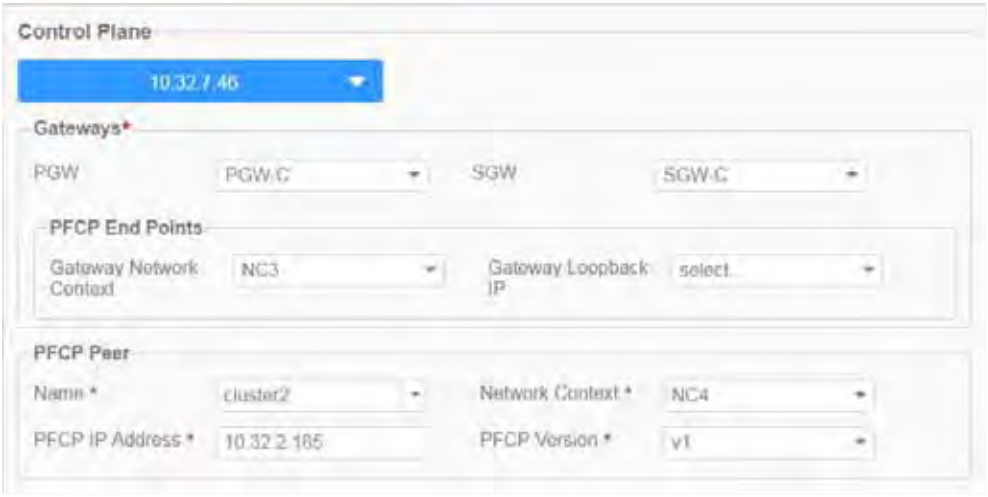
4 Under **PFCP Endpoints**, select the PFCP endpoints to associate with both the PGW and the SGW:

- Gateway Network Context — Select a network context (SX) on which the endpoint is anchored.
- Gateway Loopback IP — Select the primary loopback IP address.

5 Under **PFCP Peer**, specify the PFCP Peer associated to the SGW/PGW Peer List. Either configure the Peer:

- Name — Select or enter a name.
- Network Context — Select the network context associated with this peer.
- PFCP IP Address — Enter a PFCP IP Address of this peer.
- PFCP Version — Select a PFCP version on the interface shared with this peer

Or select an existing Peer, as shown in the following figure:



6 Configure the remaining fields of the **CUPS Group Configuration** screen (see CUPS Group Configuration Parameters) and click **Save**.

Software Releases

Acuitas allows you to manage the software releases and DPI signature files loaded on the different network elements in the network.

For sample instructions for managing MME software updates for a standalone MME, see Acuitas Support for Managing MME Software Updates.

Adding Software Releases

To add a software release:

Note: *To add a software release, you must have the Configuration > Software Configuration > Software Details > Add Software Details security group permission. For instructions, see Specifying Permissions by Security Group.*

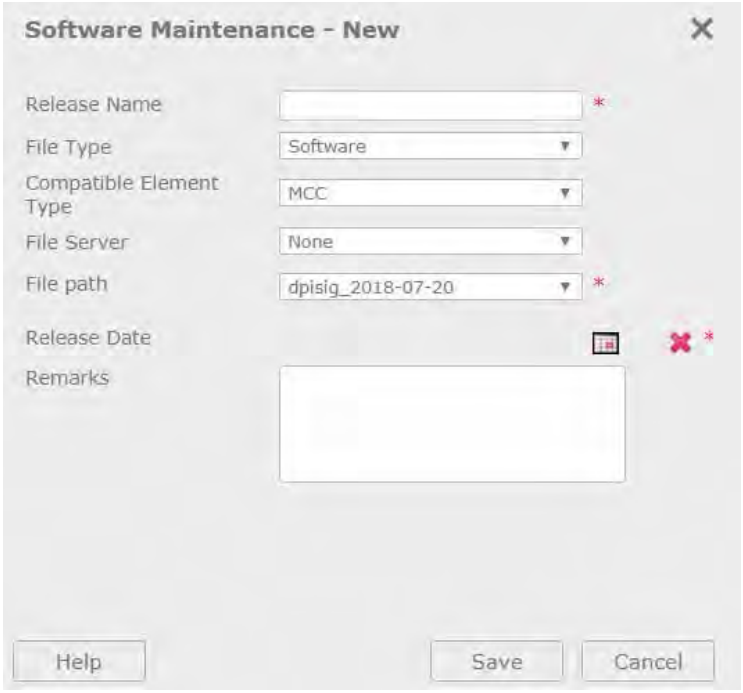
---

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Maintenance**.

Acuitas displays the **Software Maintenance** window, listing the software releases and DPI signature files maintained by the network elements in the system.

2 Click the **New** icon.

Figure 3-8 New Software Maintenance Window



3 Configure the parameters as follows:

- **Release Name** – Enter a release name
- **File Type** – Select **Software** to download a software release.
  Select **DPI signature** to download a DPI signature file (supported for MCC only).
- **Compatible Element Type** – MCC or MME.
- **File Server** – Select the file server from which to download the software release or DPI signature.
- **File Path** – Select the software image or DPI signature.
  For MCC, a maximum of three software images are listed. For MME, a maximum of three software images are listed.
- **Release Date** – Click the **Calendar** icon and select a date.
- **Remarks** – Enter any remarks.

4 Click **Save**.

Acuitas checks connectivity to the file server and availability of the specified image or DPI signature and downloads it.

5 To close the **New Software Maintenance** window, click the **Close** icon.

Viewing Software Releases

You can view the current set of software releases and DPI signature files maintained by the network elements.

Note: *To view a software release, you must have the Configuration > Software Configuration > Software Details > View Software Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a software release:

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Maintenance**.

Acuitas displays the **Software Maintenance** window, listing the software releases and DPI signature files maintained by the network elements in the system.

2 From the **Software Maintenance** window, use any of the following methods to view release details:

Toolbar: Select the release and click the **View** icon.

Pop-up menu: Right-click the release and click **View**.

Acuitas displays the **Software Maintenance View** window, listing the following information:

- Release Name
- File Type
- Compatible Element Type
- File Server
- File Name: software image or DPI signature name
- Release Date
- Software Status
- File Availability Status
- Remarks

3 Click **Close** to close the window.

Modifying Software Releases

You can modify a software release or DPI signature file only if it is not currently in use and has not been set obsolete.

Note: *To modify a software release, you must have the Configuration > Software Configuration > Software Details > Modify Software Details security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To modify a software release:

1. Click the **Settings** icon on the toolbar and select **Configuration => Software => Maintenance**.

   Acuitas displays the **Software Maintenance** window, listing the software releases and DPI signature files maintained by the network elements in the system.

2. Use any of the following methods to edit the release:

   Toolbar: Select the release and click the **Edit** icon.

   Pop-up menu: Right-click the release and click **Edit**.

3. Make the necessary changes:

   - **Release Name** – Enter a release name
   - **File Type** – Select **Software** to download a software release.
     Select **DPI signature** to download a DPI signature file (supported for MCC only).
   - **Compatible Element Type** – MCC or MME.
   - **File Server** – Select the file server from which to download the software release or DPI signature.
   - **File Path** – Select the software image or DPI signature.
     For MCC, a maximum of three software images are listed. For MME, a maximum of three software images are listed.
   - **File Availability Status** – *Read Only*
   - **Release Date** – Click the **Calendar** icon and select a date.
   - **Remarks** – Enter any remarks.

4. Click **Save**.

   Acuitas checks connectivity to the file server and availability of the specified software image or DPI signature file and downloads it.

Setting Software Releases Obsolete

You can set a software release or DPI signature file obsolete to indicate that it can no longer be used for upgrading any device. Once the release is marked as obsolete as part of any Schedule, it cannot be put to any further use.

Note: *To set a software release obsolete, you must have the Configuration > Software Configuration > Software Details > Obsolete Software Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To set a software release obsolete:

1. Click the **Settings** icon on the toolbar and select **Configuration =>**

   Software => Maintenance.

   Acuitas displays the **Software Maintenance** window, listing the software releases and DPI signature file maintained by the network elements in the system.

2. Use any of the following methods to set the release obsolete:

   Toolbar: Select the release and click the **Obsolete** icon.

   Pop-up menu: Right-click the release and click **Obsolete**.

3. At the confirmation prompt, click **OK**.

Deleting Software Releases

You can delete a software release or DPI signature file only if it is not used as part of any active or completed software schedule.

Note: *To delete a software release, you must have the Configuration > Software Configuration > Software Details > Delete Software Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete a software release:

1. Click the **Settings** icon on the toolbar and select **Configuration =>**

   Software => Maintenance.

   Acuitas displays the **Software Maintenance** window, listing the software releases and DPI signature files maintained by the network elements in the system.

2 Use any of the following methods to delete the release:

Toolbar: Select the release and click the **Delete** icon.

Pop-up menu: Right-click the release and click **Delete**.

3 At the confirmation prompt, click **OK**.

Acuitas Support for Managing MME Software Updates

This section provides sample instructions for managing MME software updates for a standalone MME. For additional instructions and for instructions for managing MME software updates for an MME cluster, see *Software Update* in the *Affirmed Networks MCC C-SGN/MME Operator Guide*.

For this release, the procedure is partially automated. It prepares the MME for manual update.

This feature requires the MME to be running version 10.1.0.0 or higher. For versions lower than 10.1.x.x, you must use CLI commands to perform the software update.

To manage MME software updates:

1 Manually copy the target MME tar ball (for example, epc-10.2.02.tar) to the following directory on the Acuitas server:

/opt/Affirmed/NMS/server/ems/data/staging-device-sw/

Do not copy more than three MME images to this directory and do not change the filenames.

2 Create a software release that can be scheduled to run later.

Click the **Settings** icon on the toolbar and select **Configuration** => **Software** => **Maintenance**.

Acuitas displays the **Software Maintenance** window, listing the software releases maintained by the network elements in the system.

3 Click the **New** icon.

4 In the **New Software Maintenance** window, configure the parameters as follows:

- **Release Name** – Enter a release name
- **File Type** – Select **Software** to download a software release.
- **Compatible Element Type** – MME.
- **File Server** – Select the file server from which to download the software release.
- **File Path** – Select the software image. A maximum of six images are listed. MME image file names have the epc- prefix and the .tar extension removed.

- **Release Date** – Click the **Calendar** icon and select a date.
- **Remarks** – Enter any remarks.

5 Click **Save**.

6 Create a software schedule to run the software update.

Click the **Settings** icon on the toolbar and select **Configuration =>**

Software => Schedule.

Acuitas displays the **Software Schedule** window, listing the software schedules.

7 Click the **New** icon.

8 In the **New Software Schedule** window, configure the parameters as follows:

- **Schedule Name** – Enter a schedule name.
- **File Type** – Select **Software** to download a software release.
- **Software Release** – Select the software release. Software releases have the epc- prefix and the .tar extension removed.
- **Upgrade Process Type** – Select the software upgrade type **Upload Only**, where, at the scheduled time, selected software file is uploaded to the selected list of devices
- **Select Elements** – Select the target MMEs by highlighting and clicking the right-arrow.
- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time** – Click the **Calendar** icon and select a date and time.

9 Click **Save**.

When the software scheduled task is run, Acuitas performs the following steps to prepare the MME for software update:

a Validates that MME is reachable, then copies the specified MME tarball to directory /usr/local/epc/software on the target MME.

b Uses NETCONF to execute the MME command **`system software select file <MME_tarball>`**, where **`<MME_tarball>`** is the target MME tar file (for example, epc-10.2.02.tar).

You can verify that this step completed by issuing the following command from the MME:

```
show system software
FILE               VERSION    STATE     KEEP
-----------------------------------------------
epc-10.0.19.4.tar  10.0.19.4  -         no
epc-10.1.02.tar    10.1.02    -         no
epc-10.2.08.tar    10.2.08    -         no
epc-10.3.04.tar    10.3.04    selected  no
epc-9.1.18.2.tar   9.1.18.2   -         yes
epc-9.1.19.1.tar   9.1.19.1   -         no
```

c Uses NETCONF to execute the MME command **`set system software auto-update disable`**. This command prevents the MGMT VM from automatically updating any VM running the non-selected software version whenever the VM registers with MGMT VM.

You can verify that this step completed by issuing the following command from the MME:

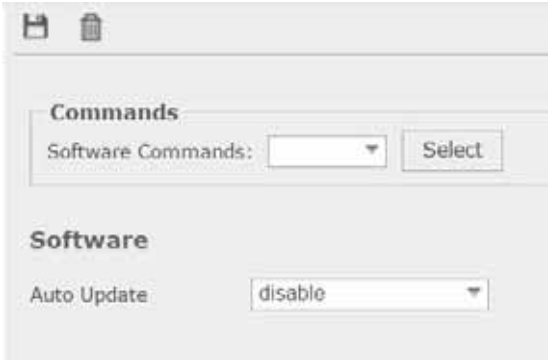
```
show full-configuration system software auto-update
system software auto-update disable
```

10 In the Configuration Navigator:

a Expand **System** in the tree.

b Click **Software**.

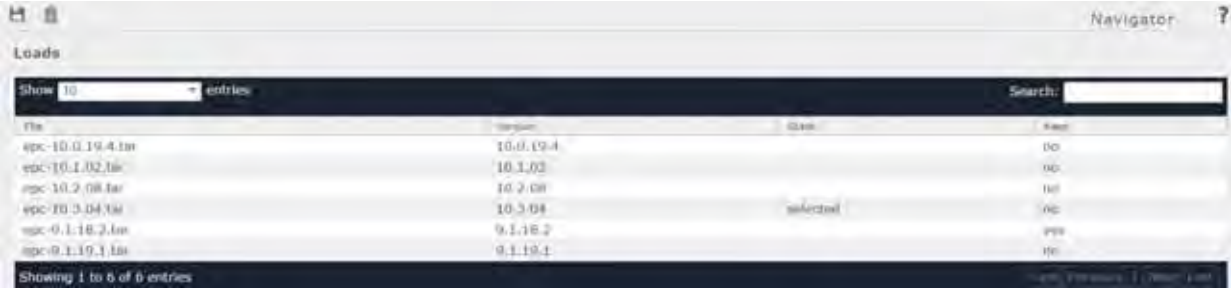
c Verify that the **Auto Update** field is set to **disable**.



d Expand **Software**.

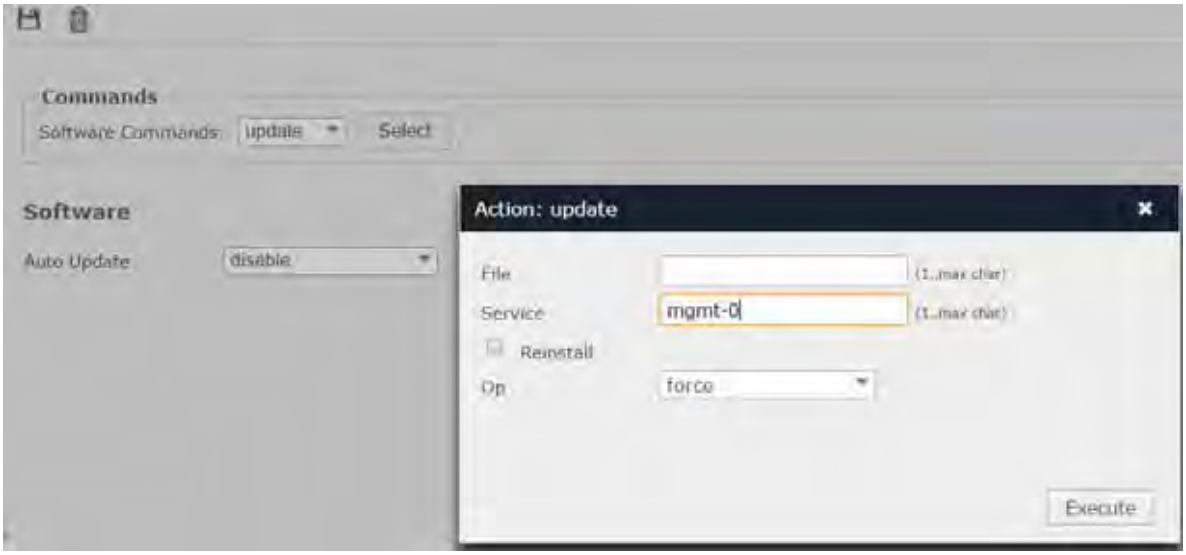
e Click **Loads**.

f Verify that the target image has the State column status set to **selected**.



11 In the Configuration Navigator, perform the software update. Update the MGMT VM first. This action gracefully dries up the service, updates the software, reboots the MME, and restores it to the previous admin state.

- **a** Expand **System** in the tree.
- **b** Click **Software**.
- **c** In the **Software Command** field, select **update** and click **Select**.
- **d** Leave the **File** field blank to use the selected target image.
- **e** In the **Service** field, enter the service name, such as mgmt-0.
- **f** In the **Op** field, select **force**.
- **g** Click **Execute**.



12 In the Configuration Navigator, click **Vm** in the tree. Monitor the Vm screen until the Procedural column status changes to **sw-update**.

When the update completes, MGMT VM reboot/switchover occur.

13 Once the MME restarts and becomes reachable from Acuitas, repeat step 10 through step 12 to perform the software update on the remaining VMs, one at a time.

Software Schedules

Acuitas allows you to manage the schedules for upgrading the software or DPI signature files of a single or multiple elements. For example, you can schedule a software upgrade for a set of Network Elements as part of a typical maintenance cycle. Acuitas can be configured to execute it automatically.

Adding Software Schedules

Note: *To add a software schedule, you must have the Configuration > Software Configuration > Software Schedule > Add Software Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

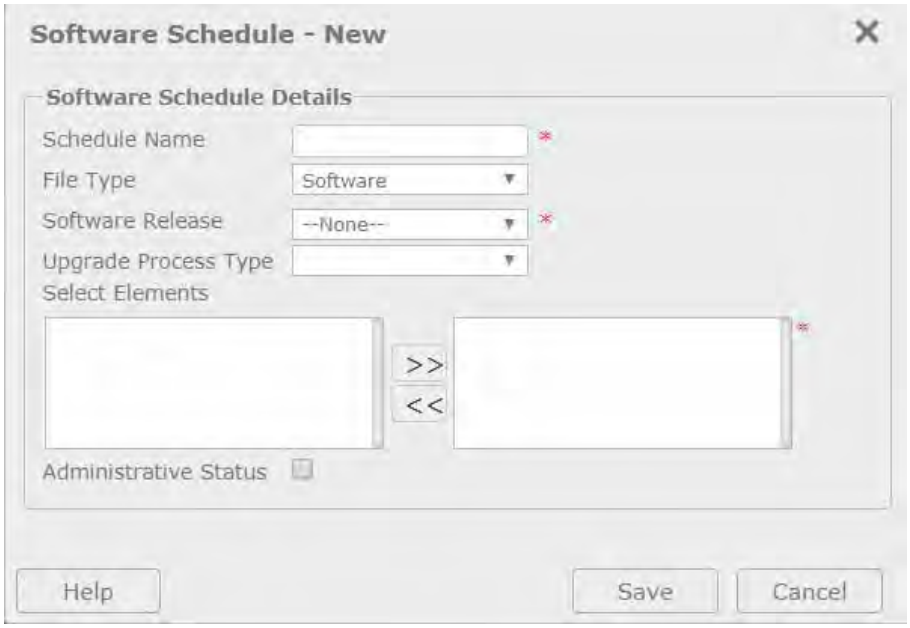
To add a software schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration =>** **Software => Schedule**.

Acuitas displays the **Software Schedule** window, listing the software schedules.

2 Click the **New** icon.

Figure 3-9 New Software Schedule Window



3 Configure the parameters as follows:

- **Schedule Name** – Enter a schedule name.
- **File Type** – Select **Software** to download a software release.
  Select **DPI signature** to download a DPI signature file (supported for MCC only).
- **Software Release** – Select the software release or DPI signature file.
- **Upgrade Process Type** – Select the software or DPI signature files upgrade type:
  - **Upload and Upgrade** (supported for MCC only):

    Both upload and upgrade are performed as a single task. At the scheduled time, selected software or DPI signature file is uploaded to the selected list of devices and then upgraded.
  - **Upload Only**: At the scheduled time, either:

    Selected software file is uploaded to the selected list of devices (supported for MCC and MME).

    Selected DPI signature file is uploaded to selected list of devices (supported for MCC only).
  - **Upgrade Only** (supported for MCC only):

    At the scheduled time, previously uploaded software or DPI signature file is upgraded to the selected list of devices.
- **Select Elements** – Select the elements by highlighting and clicking the right-arrow.
- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time** – Click the **Calendar** icon and select a date and time.

4 Click **Save**.

Viewing Software Schedules

Note: *To view a software schedule, you must have the Configuration > Software Configuration > Software Schedule > View Software Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a software schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Software => Schedule.

Acuitas displays the **Software Schedule** window, listing the software schedules.

2 From the **Software Schedule** window, use any of the following methods to view schedule details:

Toolbar: Select the schedule and click the **View** icon.

Pop-up menu: Right-click the schedule and click **View**.

Acuitas displays the **Software Schedule View** window, listing the following information:

- Schedule Name
- File Type
- Software Release
- Upgrade Process Type
- Element Name
- Last Execution Time
- Next Execution Time
- Operational Status
- Administrative Status

3 Click **Close** to close the window.

Viewing Software Schedule Subtask Status

When multiple Network Elements use a particular software schedule, Acuitas creates a separate subtask to run the schedule on each node. You can view the status of a each subtask.

Note: *To view software schedule subtask status, you must have the Configuration > Software Configuration > Software Schedule > View Sub Task security group permission. For instructions, see Specifying Permissions by Security Group.*

To view software schedule subtask status:

1. Click the **Settings** icon on the toolbar and select **Configuration** => **Software** => **Schedule**.

   Acuitas displays the **Software Schedule** window, listing the software schedules.

2. From the **Software Schedule** window, use any of the following methods to view subtasks:

   Toolbar: Select the schedule and click the **View Sub Tasks** icon.

   Pop-up menu: Right-click the schedule and click **View Sub Tasks**.

   Acuitas displays the **Sub Tasks Details** window, listing the following information:

   - Element Name
   - Schedule Name
   - Software Release
   - Order of Execution
   - Status
   - Last Attempted Time
   - Operational Status

3. To view software schedule status of a subtask, select the subtask and click the **View Status** icon.

4. Acuitas displays the **Software Schedule View Status** window, listing the software schedule progress status report.

5. Click **Close** to close the window.

6. To close the **Sub Tasks Details** window, click the **Close** icon.

Copying Software Schedules

You can make a copy of an existing software schedule and then modify and save it with a new name.

Note: *To copy a software schedule, you must have the Configuration > Software Configuration > Software Schedule > Copy Software Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To copy a software schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration => Software => Schedule**.

   Acuitas displays the **Software Schedule** window, listing the software schedules.

2. To copy a schedule, select the software schedule and click the **Copy** icon.
3. Make the necessary changes:
   - **Schedule Name** – Enter a schedule name.
   - **File Type** – Select **Software** to download a software release.
     Select **DPI signature** to download a DPI signature file (supported for MCC only).
   - **Software Release** – Select the software release or DPI signature file.
   - **Upgrade Process Type** – Select the software or DPI signature files upgrade type:
     - **Upload and Upgrade** (supported for MCC only):

       Both upload and upgrade are performed as a single task. At the scheduled time, selected software or DPI signature file is uploaded to the selected list of devices and then upgraded.
     - **Upload Only**: At the scheduled time, either:

       Selected software file is uploaded to the selected list of devices (supported for MCC and MME).

       Selected DPI signature file is uploaded to selected list of devices (supported for MCC only).
     - **Upgrade Only** (supported for MCC only):

       At the scheduled time, previously uploaded software or DPI signature file is upgraded to the selected list of devices.
   - **Select Elements** – Select the elements by highlighting and clicking the right-arrow.
   - **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.

- **Schedule Time** – Click the **Calendar** icon and select a date and time.

4 Click **Save**.

Enabling/Disabling Software Schedules

Note: *To enable a software schedule, you must have the Configuration > Software Configuration > Software Schedule > Start Software Schedule security group permission. To disable a software schedule, you must have the Configuration > Software Configuration > Software Schedule > Stop Software Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To enable/disable a software schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Schedule**.

Acuitas displays the **Software Schedule** window, listing the software schedules.

2 Use any of the following methods to enable a schedule:

Toolbar: Select the schedule and click the **Enable Schedule** icon.

Pop-up menu: Right-click the schedule and select **Enable Schedule**.

Use any of the following methods to disable a schedule:

Toolbar: Select the schedule and click the **Disable Schedule** icon.

Pop-up menu: Right-click the schedule and select **Disable Schedule**.

3 At the confirmation prompt, click **OK**.

The Administrative Status of the schedule changes to Enabled or Disabled.

Quick Start Software Schedules

Note: *To Quick Start a software schedule, you must have the Configuration > Software Configuration > Software Schedule > Start Software Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To Quick Start (instantly execute) a software schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Schedule**.

Acuitas displays the **Software Schedule** window, listing the software schedules.

2 Use any of the following methods to Quick Start a software schedule:

Toolbar: Select the schedule and click the **Quick Start** icon.

Pop-up menu: Right-click the schedule and select **Quick Start**.

Modifying Software Schedules

Note: *To modify a software schedule, you must have the Configuration > Software Configuration > Software Schedule > Modify Software Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To modify a software schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Schedule**.

Acuitas displays the **Software Schedule** window, listing the software schedules.

2 Use any of the following methods to modify a schedule:

Toolbar: Select the schedule and click the **Edit** icon.

Pop-up menu: Right-click the schedule and select **Edit**.

3 Make the necessary changes:

- **Schedule Name** – Enter a schedule name

- **File Type** – Select **Software** to download a software release.
  Select **DPI signature** to download a DPI signature file (supported for MCC only).
- **Software Release** – Select the software release or DPI signature files.
- **Upgrade Process Type** – Select the software or DPI signature files upgrade type:
  - **Upload and Upgrade** (supported for MCC only):

    Both upload and upgrade are performed as a single task. At the scheduled time, selected software or DPI signature file is uploaded to the selected list of devices and then upgraded.
  - **Upload Only**: At the scheduled time, either:

    Selected software file is uploaded to the selected list of devices (supported for MCC and MME).

    Selected DPI signature file is uploaded to selected list of devices (supported for MCC only).
  - **Upgrade Only** (supported for MCC only):

    At the scheduled time, previously uploaded software or DPI signature file is upgraded to the selected list of devices.
- **Element Name** – *Read-only*.
- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time** – Click the **Calendar** icon and select a date and time.

4 Click **Save**.

Deleting Software Schedules

You can delete a software schedule only if it has the Operational state Scheduled, Success, or Failure.

Note: *To delete a software schedule, you must have the Configuration > Software Configuration > Software Schedule > Delete Software Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To delete a software schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Schedule**.

Acuitas displays the **Software Schedule** window, listing the software schedules.

2 Use any of the following methods to delete a software schedule:

Toolbar: Select the schedule and click the **Delete** icon.

Pop-up menu: Right-click the schedule and select **Delete**.

3 At the confirmation prompt, click **OK**.

Software Rollback

Acuitas allows you to rollback the software or a DPI signature file of a network element to the previous version.

Performing Software Rollback

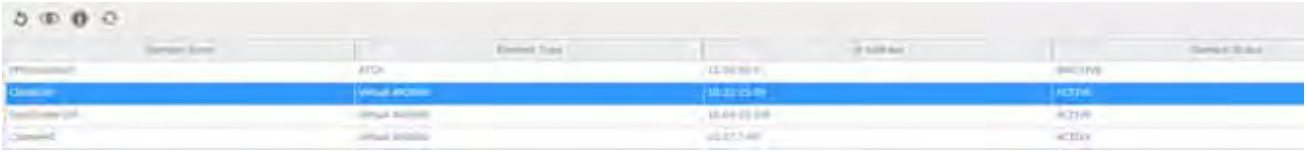
Note: *To perform a software rollback, you must have the Configuration > Software Configuration > Software Rollback > Run Software Rollback security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To perform a software rollback:

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Rollback**.

Acuitas displays the **Software Rollback** window, listing the network elements.

Figure 3-10 Software Rollback Window



2 Click the **Refresh** icon to refresh the list of devices.

3 Click the **Element Name** column to sort the devices alphabetically by name in ascending or descending order.

The sort is dynamic: Acuitas re-sorts the order every time you refresh the screen.

4 Select the network element to rollback.

5 To perform a software rollback, click the **Rollback** icon and select the **Software Rollback**.

To perform a DPI signature rollback, click the **Rollback** icon and select **DPI Rollback**.

6 At the confirmation prompt, click **Yes**.

Acuitas verifies that the following conditions are true:

- The `rollback version` is available.
- The activation-status is in `Idle` state.

If both are true, Acuitas activates the previous release and reboots the Network Element.

Viewing Software Rollback Progress

Note: *To view software rollback process, you must have the Configuration > Software Configuration > Software Rollback > View Software Rollback security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To view software rollback progress:

1 Click the **Settings** icon on the toolbar and select **Configuration => Software => Rollback**.

Acuitas displays the **Software Rollback** window, listing the network elements.

2 Click the **Refresh** icon to refresh the list of devices.

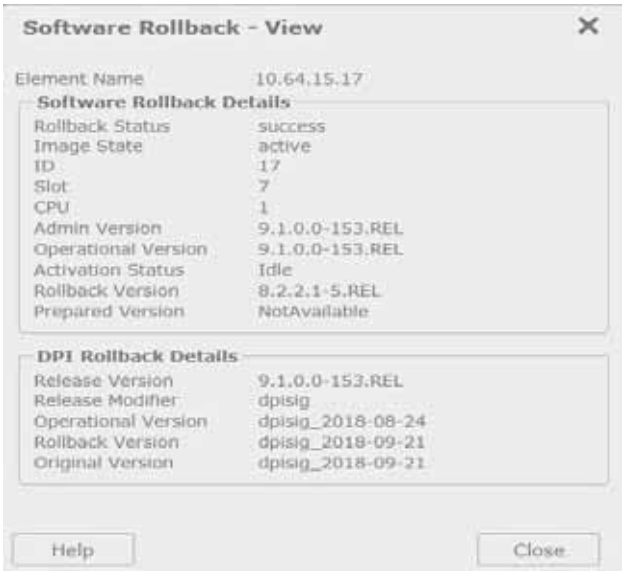
3 Click the **Element Name** column to sort the devices alphabetically by name in ascending or descending order.

The sort is dynamic: Acuitas re-sorts the order every time you refresh the screen.

4 Select the network element and click the **View** icon.

Acuitas displays the **Software Rollback View** window, listing the **Software Rollback Details** and the **DPI Rollback Details** for the network element.

Figure 3-11 Software Rollback View Window



5 Click **Close** to close the window.

Viewing Software Rollback Status

Note: *To view software rollback status, you must have the Configuration > Software Configuration > Software Rollback > View Software Rollback security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To view software rollback status:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Software => Rollback.

Acuitas displays the **Software Rollback** window, listing the network elements.

2 Click the **Refresh** icon to refresh the list of devices.

3 Click the **Element Name** column to sort the devices alphabetically by name in ascending or descending order.

The sort is dynamic: Acuitas re-sorts the order every time you refresh the screen.

4 Select the network element and click the **View Rollback Status** icon.

Acuitas displays the **Software Rollback View Status** window, listing the software rollback status.

Figure 3-12 View Status Window for a Software Rollback

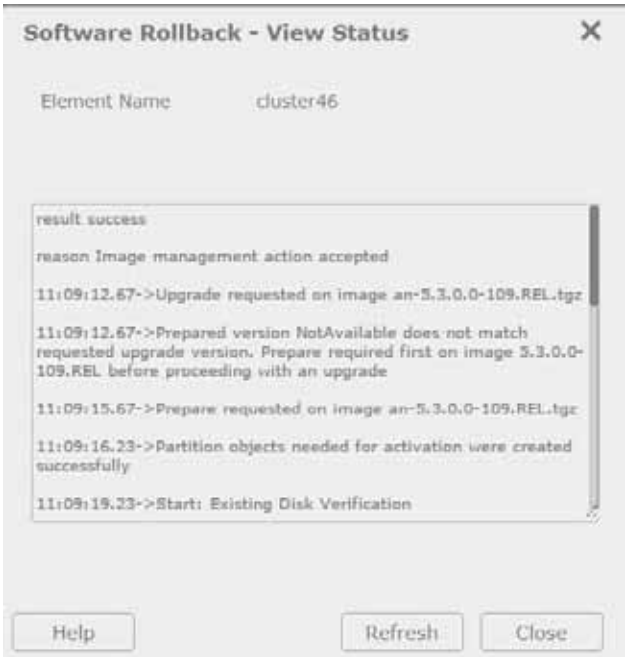


Figure 3-13 View Status Window for a DPI Signature Rollback

5 To refresh the status, click **Refresh**.

6 Click **Close** to close the window.

Configuration Templates

Configuration templates allow you to apply similar configurations to multiple elements while significantly reducing time consuming manual work. You schedule templates to be periodically executed.

Adding Configuration Templates

Note: *To add a configuration template, you must have the Configuration > Configuration Template > Template Maintenance > Add Configuration Template security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To add a configuration template:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Maintenance**.

   Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2. Click the **New** icon.
3. Configure the parameters as follows:
   - **Template Name** – Enter a template name
   - **Protocol Type** – CLI
   - **Template Type**:
     - Configuration – Used to configure an element
     - Alarm Triggered – Used to configure an element based on the alarm of the element
   - **Applicable Element Type** – MCC or MME
4. Click **Next**.
5. In the Configuration Command list, enter the sequence of commands to be executed on the device. Enter each command on a separate line. The command list can contain a maximum of 1000 lines (including empty lines). Each line can contain a maximum of 1200 characters.

   Use the **`$UserInput$`** syntax to specify a user input token, the value of which you specify when you schedule the Configuration Template. For example, the following command uses the user input token **Cluster** and the user input token **Slot**.

   ```
   show cluster $UserInput$Cluster statistics $UserInput$Slot
   ```

Note: *The Alarm Triggered Configuration Template does not support the use of variables in CLI scripts that are triggered by alarms.*

6 Click **Save**.

To schedule the execution of the template, see Template Schedules.

To apply the template to elements based on alarm triggers, see Alarm Triggered Configurations.

Viewing Configuration Templates

Note: *To view a configuration template, you must have the Configuration > Configuration Template > Template Maintenance > View Configuration Template security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a configuration template:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Templates => Maintenance.

Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2 From the **Template Maintenance** window, use any of the following methods to view configuration template details:

Toolbar: Select the template and click the **View** icon.

Pop-up menu: Right-click the template and click **View**.

Acuitas displays the **Template Maintenance View** window, listing the following information:

- Template Name
- Template Type
- Protocol Type
- Status
- Applicable Element Type
- Configuration Command List

3 Click **Close** to close the window.

Copying Configuration Templates

You can make a copy of an existing configuration template and then modify and save it with a new name.

Note: *To copy a configuration template, you must have the Configuration > Configuration Template > Template Maintenance > Copy Configuration Template security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To copy a configuration template:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Maintenance**.

   Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2. Use any of the following methods to copy a configuration template:

   Toolbar: Select the configuration template and click the **Copy** icon.

   Pop-up menu: Right-click the configuration template and select **Copy**.

3. Make the necessary changes:
   - **Template Name** – Enter a template name
   - **Protocol Type** – CLI
   - **Template Type**:
     - Configuration – Used to configure an element
     - Alarm Triggered – Used to configure an element based on the alarm of the element
   - **Applicable Element Type** – MCC or MME
4. Click **Next**.
5. In the Configuration Command list, enter the sequence of commands to be executed on the device. Enter each command on a separate line. The command list can contain a maximum of 1000 lines (including empty lines). Each line can contain a maximum of 1200 characters.

   Use the **`$UserInput$`** syntax to specify a user input token, the value of which you specify when you schedule the Configuration Template.

Note: *The Alarm Triggered Configuration Template does not support the use of variables in CLI scripts that are triggered by alarms.*

6 Click **Save**.

To schedule the execution of the template, see Template Schedules.

Modifying Configuration Templates

You can modify a configuration template only if it is not used as part of any active schedule and is not obsolete.

Note: *To modify a configuration template, you must have the Configuration > Configuration Template > Template Maintenance > Modify Configuration Template security group permission. For instructions, see Specifying Permissions by Security Group.*

To modify a configuration template:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Templates => Maintenance.

Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2 From the **Template Maintenance** window, use any of the following methods to modify a configuration template:

Toolbar: Select the template and click the **Edit** icon.

Pop-up menu: Right-click the template and click **Edit**.

3 Make the necessary changes:

- Template Name
- Template Type
- Protocol Type
- Applicable Element Type

4 Click **Next**.

5 In the Configuration Command list, enter the sequence of commands to be executed on the device. Enter each command on a separate line. The command list can contain a maximum of 1000 lines (including empty lines). Each line can contain a maximum of 1200 characters.

Use the **`$UserInput$`** syntax to specify a user input token, the value of which you specify when you schedule the Configuration Template.

Note: *The Alarm Triggered Configuration Template does not support the use of variables in CLI scripts that are triggered by alarms.*

---

6 Click **Save**.

To schedule the execution of the template, see Template Schedules.

Setting Configuration Templates Obsolete

You can set a configuration template obsolete only if it is not used as part of any active schedule. Once you set it obsolete, you indicate that it can no longer be used.

Note: *To set a configuration template obsolete, you must have the Configuration > Configuration Template > Template Maintenance > Obsolete Configuration Template security group permission. For instructions, see Specifying Permissions by Security Group.*

To set a configuration template obsolete:

1 Click the **Settings** icon on the toolbar and select **Configuration => Templates => Maintenance**.

Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2 Use any of the following methods to set the configuration template obsolete:

Toolbar: Select the configuration template and click the **Obsolete** icon.

Pop-up menu: Right-click the configuration template and click **Obsolete**.

3 At the confirmation prompt, click **OK**.

The Status of the configuration template changes from Active to Inactive indicating that the template is excluded from future use.

Deleting Configuration Templates

Before you can delete a configuration template, delete any template schedules that use it. See Deleting Software Schedules.

Note: *To delete a configuration template, you must have the Configuration > Configuration Template > Template Maintenance > Delete Configuration Template security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete a configuration template:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Maintenance**.

   Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2. Use any of the following methods to delete a configuration template:

   Toolbar: Select the configuration template and click the **Delete** icon.

   Pop-up menu: Right-click the configuration template and select **Delete**.

3. At the confirmation prompt, click **OK**.

Exporting Configuration Templates

You can export a configuration template to a CSV/PDF/XLS/XML/HTML file.

Note: *To export a configuration template, you must have the Configuration > Configuration Template > Template Maintenance > Export Configuration Template security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To export a configuration template:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Maintenance**.

   Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2. If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.

3. Click the **Export** icon.

   Acuitas displays the **Configure Export Parameters** window.

4. Configure the parameters as follows:

   - **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
   - **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
   - **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
   - **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.

5. Click **Apply**.

   Acuitas displays the **Download Files** window.

6. Click **Download Exported File**.

7. From the **Download File**s window, click **Close**.

Importing Configuration Templates

You can import a configuration template from an XML file.

Note: *To import a configuration template, you must have the Configuration > Configuration Template > Template Maintenance > Import Configuration Template security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To import a configuration template:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Maintenance**.

   Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2. Click the **Import** icon.

   Acuitas displays the **Import Template** window.

3. Click **Browse** and select the template file (supported file format is .xml).
4. Click **Import**.

Template Schedules

You can schedule templates to be periodically executed.

Note: *If a template executes a large number of CLI commands, the session may timeout before the commands commit. To avoid a timeout, increase the milliseconds value of the CLI Time Out parameter at the Edit Network Element window.*

Adding Template Schedules

Note: *To add a template schedule, you must have the Configuration > Configuration Template > Template Schedule > Add Template Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To add a template schedule:

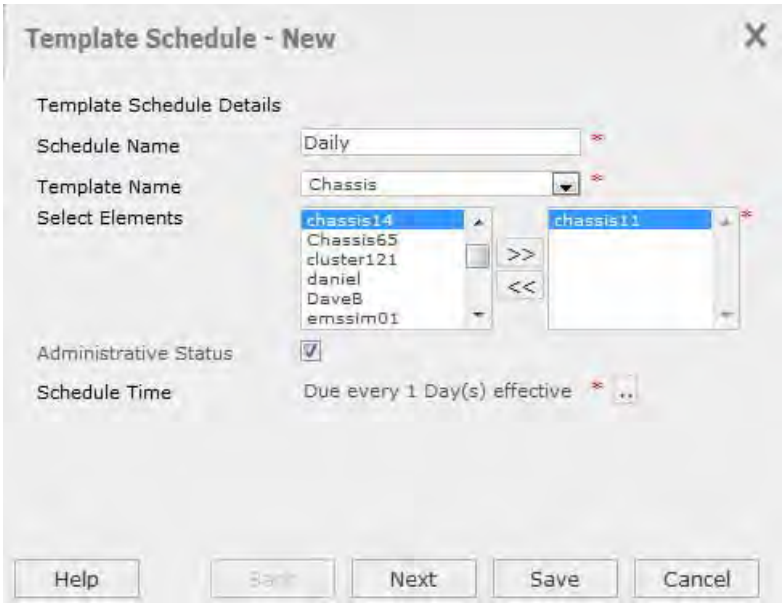
1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Templates => Schedule.

Acuitas displays the **Template Schedule** window, listing the template schedules.

2 Click the **New** icon.

Figure 3-14 New Template Schedule Window

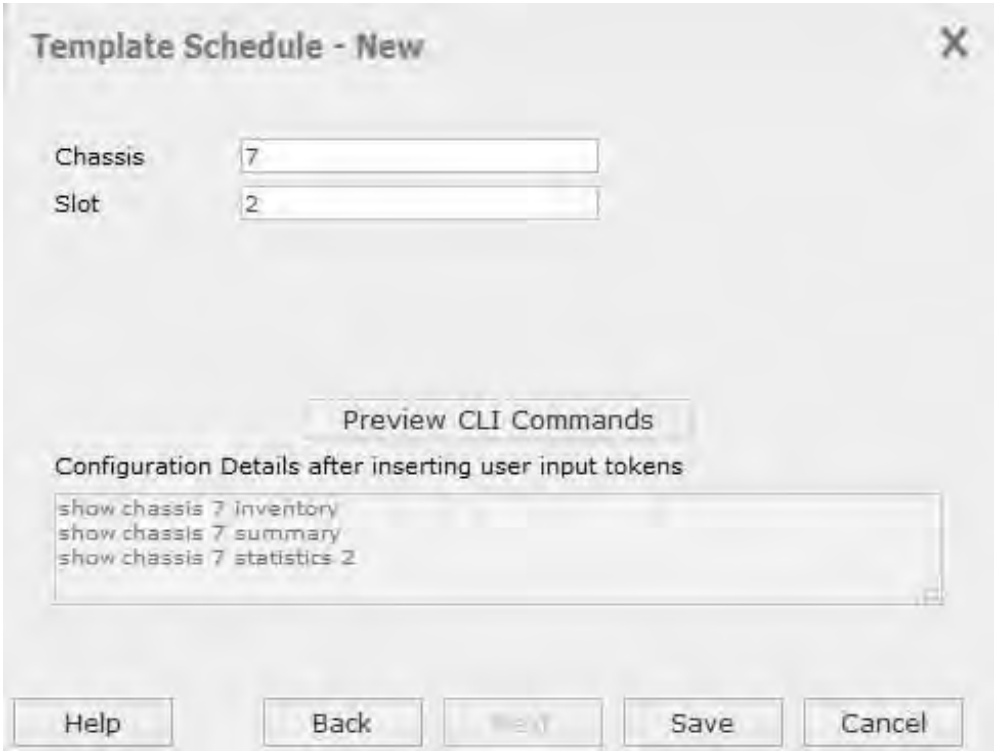


3 Configure the parameters as follows:

- **Schedule Name** – Enter a schedule name
- **Template Name** – Select the configuration template.
- **Select Elements** – Select the elements by highlighting and clicking the right-arrow.
- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time**:
  - Click **Recurrence Pattern** icon.
  - Specify the recurrence details and click **Schedule**.

4 Click **Next**.

Figure 3-15 Configuration Command List



5 If the specified configuration template contains user input token(s), specify the value(s) in the **Token Details** field. In the example above, the value of the Chassis token is specified as 7 and the value of the Slot token is specified as 2.

6 Click **Preview CLI Commands** to see the preview of the CLI command(s) that were provided in the Configuration Command List of the specified configuration template. If the configuration template contained user input token(s), the specified values are inserted in the CLI command(s).

7 Click **Save**.

To view the results of the template execution, see Viewing Template Schedule Execution Status.

Copying Template Schedules

You can make a copy of an existing template schedule and then modify and save it with a new name.

Note: *To copy a template schedule, you must have the Configuration > Configuration Template > Template Schedule > Copy Template Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To copy a template schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Schedule**.

   Acuitas displays the **Template Schedule** window, listing the template schedules.

2. Use any of the following methods to copy a template schedule:

   Toolbar: Select the template schedule and click the **Copy** icon.

   Pop-up menu: Right-click the template schedule and select **Copy**.

3. Make the necessary changes:
   - **Schedule Name** – Enter a schedule name
   - **Template Name** – Select the configuration template.
   - **Select Elements** – Select the elements by highlighting and clicking the right-arrow.
   - **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
   - **Schedule Time**:
     - Click the **Recurrence Pattern** icon.
     - Specify the recurrence details and click **Schedule**.
4. Click **Next**.
5. If the specified configuration template contains user input token(s), specify the value(s) in the **Token Details** field.
6. Click **Preview CLI Commands** to see the preview of the CLI command(s) that were provided in the Configuration Command List of the specified configuration template. If the configuration template contained user input token(s), the specified values are inserted in the CLI command(s).
7. Click **Save**.

To view the results of the template execution, see Viewing Template Schedule Execution Status.

Viewing Template Schedules

Note: *To view a template schedule, you must have the Configuration > Configuration Template > Template Schedule > View Template Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a template schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Schedule**.

   Acuitas displays the **Template Schedule** window, listing the template schedules.

2. From the **Template Schedule** window, use any of the following methods to view template schedule details:

   Toolbar: Select the template schedule and click the **View** icon.

   Pop-up menu: Right-click the template schedule and click **View**.

   Acuitas displays the **Template Schedule View** window, listing the following information:

   - Schedule Name
   - Template Name
   - Element Name
   - Last Execution Time
   - Next Execution Time
   - Schedule Interval
   - Operational Status
   - Administrative Status
   - Configuration Command List

3. Click **Close** to close window.

   To view the results of the template execution, see Viewing Template Schedule Execution Status.

Viewing Template Schedule Execution Status

Note: *To view a template schedule execution status, you must have the Configuration > Configuration Template > Template Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a template schedule execution status:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Schedule**.

   Acuitas displays the **Template Schedule** window, listing the template schedules.

2. Right-click the template schedule and click **Execution Status**.

   Acuitas displays the **Template Execution Status View** window, listing the various execution times for the previous 24 hours.

3. Select an execution time to view the details:
   - Schedule Name
   - Element
   - Execution Status
   - Commands executed for this schedule:
     - Type
     - Command
     - Response
     - Status

4. Click **Close** to close window.

Enabling/Disabling Template Schedules

You can enable/disable template schedules.

Note: *To enable a template schedule, you must have the Configuration > Configuration Template > Template Schedule > Start Template Schedule security group permission. To disable a software schedule, you must have the Configuration > Configuration Template > Template Schedule > Stop Software Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To enable/disable a template schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Schedule**.

   Acuitas displays the **Template Schedule** window, listing the template schedules.

2. Use any of the following methods to enable a template schedule:

   Toolbar: Select the template schedule and click the **Enable Schedule** icon.

   Pop-up menu: Right-click the template schedule and select **Enable Schedule**.

   Use any of the following methods to disable a template schedule:

   Toolbar: Select the template schedule and click the **Disable Schedule** icon.

   Pop-up menu: Right-click the template schedule and select **Disable Schedule**.

3. At the confirmation prompt, click **OK**.

   The Administrative Status of the template schedule changes to Enabled or Disabled.

Quick Start Template Schedules

Note: *To Quick Start a template schedule, you must have the Configuration > Configuration Template > Template Schedule > Start Template Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To Quick Start (instantly execute) a template schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Schedule**.

   Acuitas displays the **Software Schedule** window, listing the template schedules.

2. Use any of the following methods to Quick Start a template schedule:

   Toolbar: Select the template schedule and click the **Quick Start** icon.

   Pop-up menu: Right-click the template schedule and select **Quick Start**.

   To view the results of the template execution, see Viewing Template Schedule Execution Status.

Modifying Template Schedules

Note: *To modify a template schedule, you must have the Configuration > Configuration Template > Template Schedule > Modify Template Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To modify a template schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration => Templates => Schedule**.

   Acuitas displays the **Template Schedule** window, listing the template schedules.

2. Use any of the following methods to modify a template schedule:

   Toolbar: Select the template schedule and click the **Edit** icon.

   Pop-up menu: Right-click the template schedule and select **Edit**.

3. Make the necessary changes:

- **Schedule Name** – Enter a schedule name
- **Template Name** – Select the configuration template.
- **Select Elements** – Select the elements by highlighting and clicking the right-arrow.
- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time**:
  - Click the **Recurrence Pattern** icon.
  - Specify the recurrence details and click **Schedule**.

4 Click **Next**.

5 If the specified configuration template contains user input token(s), specify the value(s) in the **Token Details** field.

6 Click **Preview CLI Commands** to see the preview of the CLI command(s) that were provided in the Configuration Command List of the specified configuration template. If the configuration template contained user input token(s), the specified values are inserted in the CLI command(s).

7 Click **Save**.

To view the results of the template execution, see Viewing Template Schedule Execution Status.

Deleting Template Schedules

You can delete a template schedule only if its operational status is Completed or its administrative status is Disabled.

Note: *To delete a template schedule, you must have the Configuration > Configuration Template > Template Schedule > Delete Template Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group*.

To delete a template schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration => Templates => Schedule**.

Acuitas displays the **Template Schedule** window, listing the template schedules.

2 Use any of the following methods to delete a template schedule:

Toolbar: Select the template schedule and click the **Delete** icon.

Pop-up menu: Right-click the template schedule and select **Delete**.

3 At the confirmation prompt, click **OK**.

Alarm Triggered Configurations

Alarm Triggered Configuration Templates allow you to apply configurations to elements based on alarm triggers. Configuration Templates designated as type Alarm Triggered can be specified to be executed when the alarm is received. For instructions on creating Alarm Triggered Configuration Templates, see Adding Configuration Templates.

Adding Alarm Triggered Configuration

Note: *To add an Alarm Triggered Configuration, you must have the Configuration > Alarm Triggered Configuration > Add Alarm Triggered Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

To add an alarm triggered configuration:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Alarm Triggers.

Acuitas displays the **Alarm Triggered Configuration** window.

The left pane lists the configured Alarm Triggered configurations. The right pane lists the alarm filters.

2 Click the **New** icon.

3 Configure the parameters as follows:

- **Configuration Name** – Enter a configuration name.
- **Template Name** – Select an Alarm Triggered Configuration Template.
- **Run as** – By default, Acuitas executes the configuration using the credentials of the default CLI user. To use a different credential in the device or to run it as a different user, mark this checkbox and provide the necessary credentials to run this configuration task:
- **User Name**
- **Password**
- **Confirm Password**

4 Click **Save**. The newly created Alarm Triggered Configuration is listed in the **Alarm Triggered Configuration** window.

5 To associate the configuration with alarm filters, select the configuration in the left pane and mark the required check boxes in the right pane.

Note: *It is not recommended that you mark the All checkbox, because it associates the template with any alarm (which could be a large number of alarms).*

---

6 Click **OK** to associate the configuration with alarm filters.

Modifying Alarm Triggered Configurations

Note: *To modify an Alarm Triggered Configuration, you must have the Configuration > Alarm Triggered Configuration > Modify Alarm Triggered Configuration security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To modify an Alarm Triggered Configuration:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Alarm Triggers.

Acuitas displays the **Alarm Triggered Configuration** window, listing the Alarm Triggered configurations.

2 Use any of the following methods to modify an Alarm Triggered Configuration:

Toolbar: Select the Alarm Triggered Configuration and click the **Edit** icon.

Pop-up menu: Right-click the Alarm Triggered Configuration and click **Edit**.

Acuitas displays the **Edit Alarm Triggered Configuration** window.

3 Make the necessary changes:

- **Configuration Name** – Enter a configuration name.
- **Template Name** – Select an Alarm Triggered Configuration Template.
- **Run as** – By default, Acuitas executes the configuration using the credentials of the default CLI user. To use a different credential in the device or to run it as a different user, mark this checkbox and provide the necessary credentials to run this configuration task:
- **User Name**

- **Password**
- **Confirm Password**

4 Click **Save**. The modified Alarm Triggered Configuration is listed in the **Alarm Triggered Configuration** window.

5 To associate the configuration with alarm filters, select the configuration in the left pane and mark the required check boxes in the right pane.

Note: *It is not recommended that you mark the All checkbox, because it associates the template with any alarm (which could be a large number of alarms).*

---

6 Click **OK** to associate the configuration with alarm filters.

Deleting Alarm Triggered Configurations

Note: *To delete an Alarm Triggered Configuration, you must have the Configuration > Alarm Triggered Configuration > Delete Alarm Triggered Configuration security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To delete an Alarm Triggered Configuration:

1 Click the **Settings** icon on the toolbar and select **Configuration =>** **Alarm Triggers**.

Acuitas displays the **Alarm Triggered Configuration** window, listing the Alarm Triggered configurations.

2 Use any of the following methods to delete a Alarm Triggered Configuration:

Toolbar: Select the Alarm Triggered Configuration and click the **Delete** icon.

Pop-up menu: Right-click the Alarm Triggered Configuration and select **Delete**.

3 At the confirmation prompt, click **OK**.

Use Case: Alarm Triggered Configuration

This use case demonstrates how to use an alarm triggered configuration to disable transcoding in the event of widespread transcoding failures. The following tasks are described:

- Create an Configuration Maintenance Template
- Create a decreasing threshold of 80%
- Create an alarm filter for the decreasing threshold
- Set up Alarm Triggered Configuration with filter
- Modify the MCC's schedule to add the threshold alarm to the specific KPI
- View execution status

Create an Configuration Maintenance Template

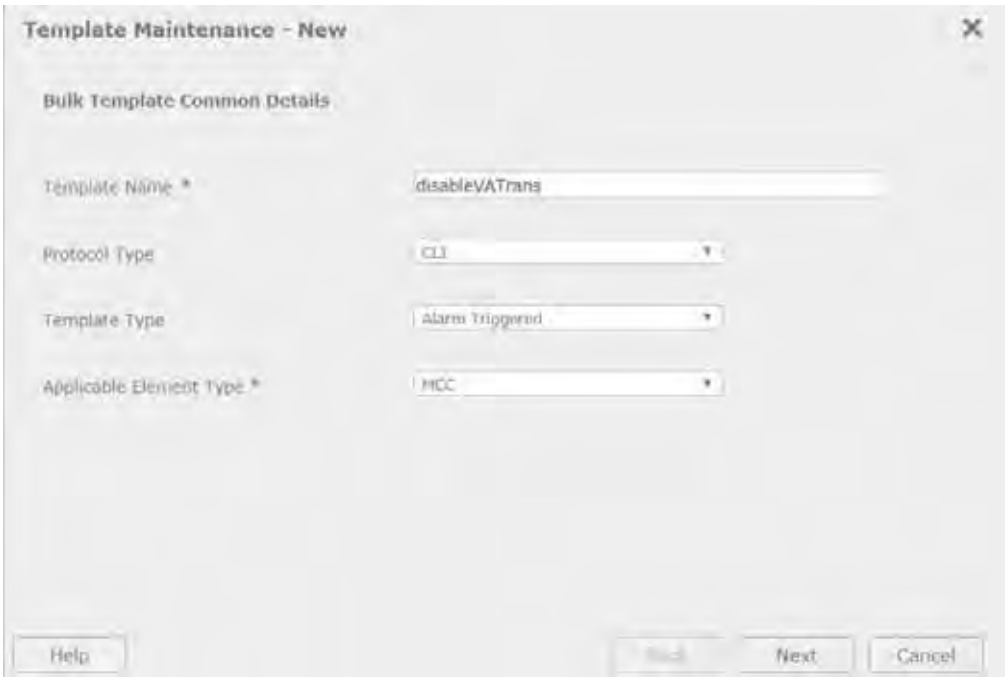
To add a configuration template:

1. Click the **Settings** icon on the toolbar and select **Configuration =>** **Templates => Maintenance**.

   Acuitas displays the **Template Maintenance** window, listing the configuration templates.

2. Click the **New** icon.
3. Configure the parameters as follows:
   - **Template Name** – Enter a template name
   - **Protocol Type** – CLI
   - **Template Type** – Select Alarm Triggered, which configures an element based on the alarm of the element
   - **Applicable Element Type** – MCC or MME

Figure 3-16 Template Maintenance Window



4 Click **Next**.

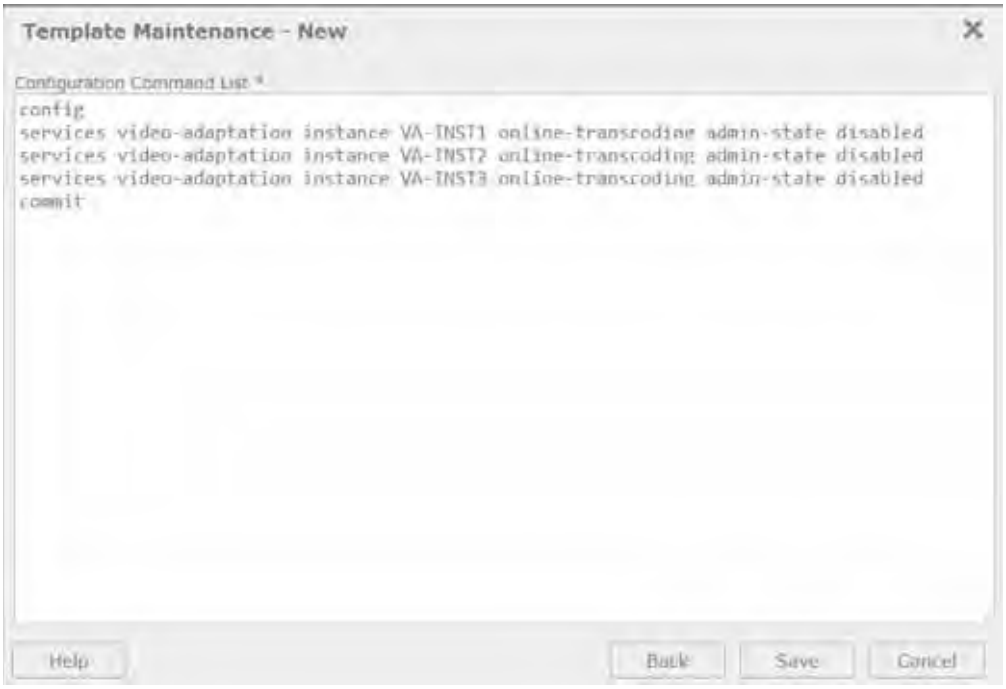
5 In the Configuration Command list, enter the sequence of commands to be executed on the device. Enter each command on a separate line. The command list can contain a maximum of 1000 lines (including empty lines). Each line can contain a maximum of 1200 characters.

Use the following commands:

```
config
services video-adaptation instance [Video Adaptation Instance]
online-transcoding admin-state disabled
commit
```

Enter a separate command for each [***Video Adaptation Instance***]. In this example, the MCC has three video adaptation instances; each requires its own command to disable the instance. Keep in mind that if changes are later made to the MCC's video adaptation instances, you need to adjust this command list to reflect the changes.

Figure 3-17 Template Maintenance Window



6 Click **Save**.

7 Close the **Template Maintenance** window.

Create a Decreasing Threshold of 80%

To add a threshold:

1 Click the **Settings** icon on the toolbar and select **Performance =>** **Configure Thresholds**.

2 Acuitas displays the **Threshold Configuration** window.

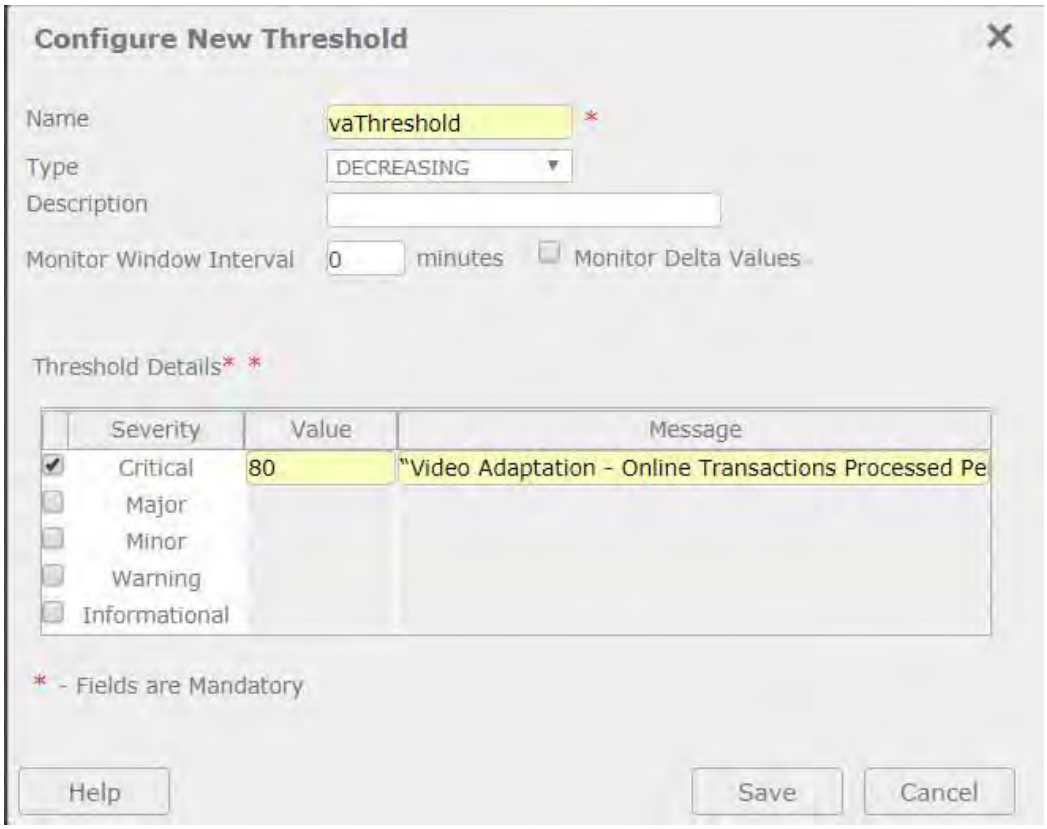
3 Click the **Add New Threshold** icon.

4 Complete the fields as follows:

- **Name** – Enter the threshold name.
- **Type** – Specify Decreasing (the threshold applies when a data point falls below the specified level).
- **Description** – Enter a threshold description.
- **Monitor Window Interval** – Leave the value 0.
- **Monitor Delta Values** – Leave the checkbox unmarked.
- **Threshold Details:**
  - Mark the **Critical** checkbox.
  - Enter the **Value** 80.
  - Enter the following **Message**: "Video Adaptation - Online Transactions Processed Percentage" has reached below 80%.

    When a threshold event is raised, this message is displayed in Alarms/Event Logs tab.

Figure 3-18 Configure New Threshold Window



5 Click **Save** to commit the data.

6 Click **Close** to close the **Threshold Configuration** window.

Create an Alarm Filter for the Decreasing Threshold

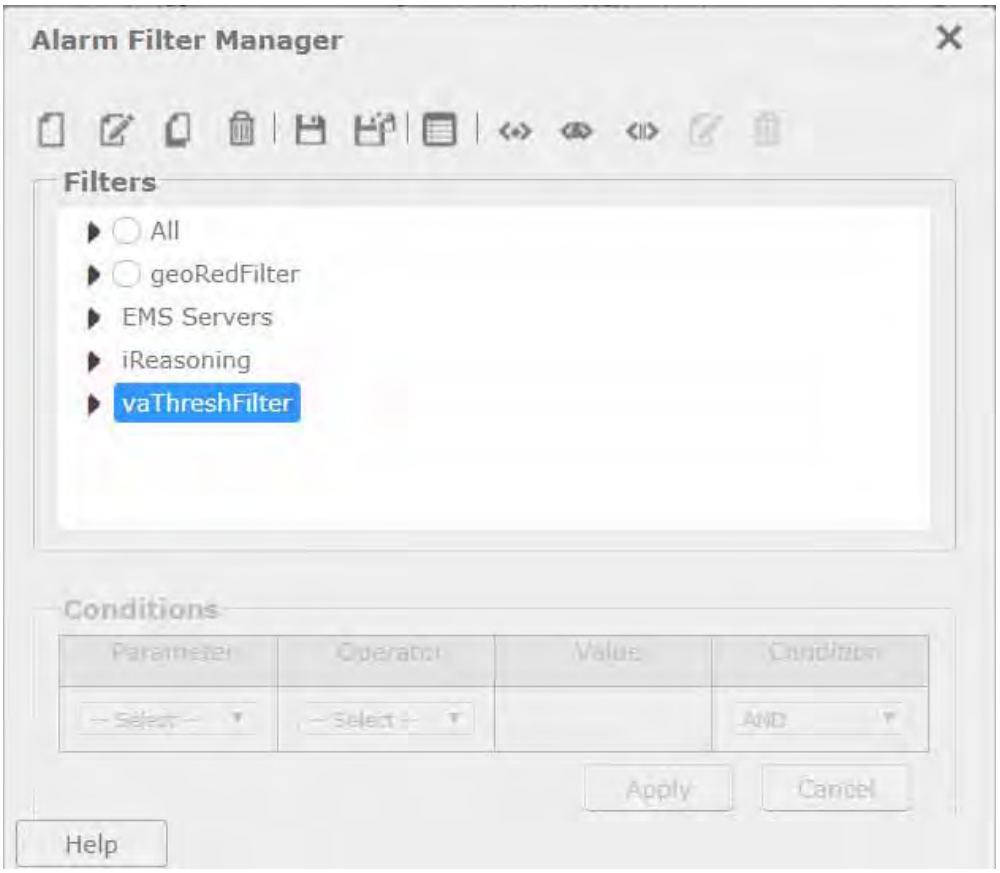
To create a filter:

1. From the Alarms tab, click the **Filter** icon.

   Acuitas displays the **Filter Manager**.

2. Click the **New Filter** icon.
3. In the **Add Filter** dialog, enter the Filter Name and click **Add**. A filter with that name is created.

Figure 3-19 Filter Manager



4 In the **Filter Manager**, select the filter and click the **Add Condition** icon:

a Complete the Conditions fields.

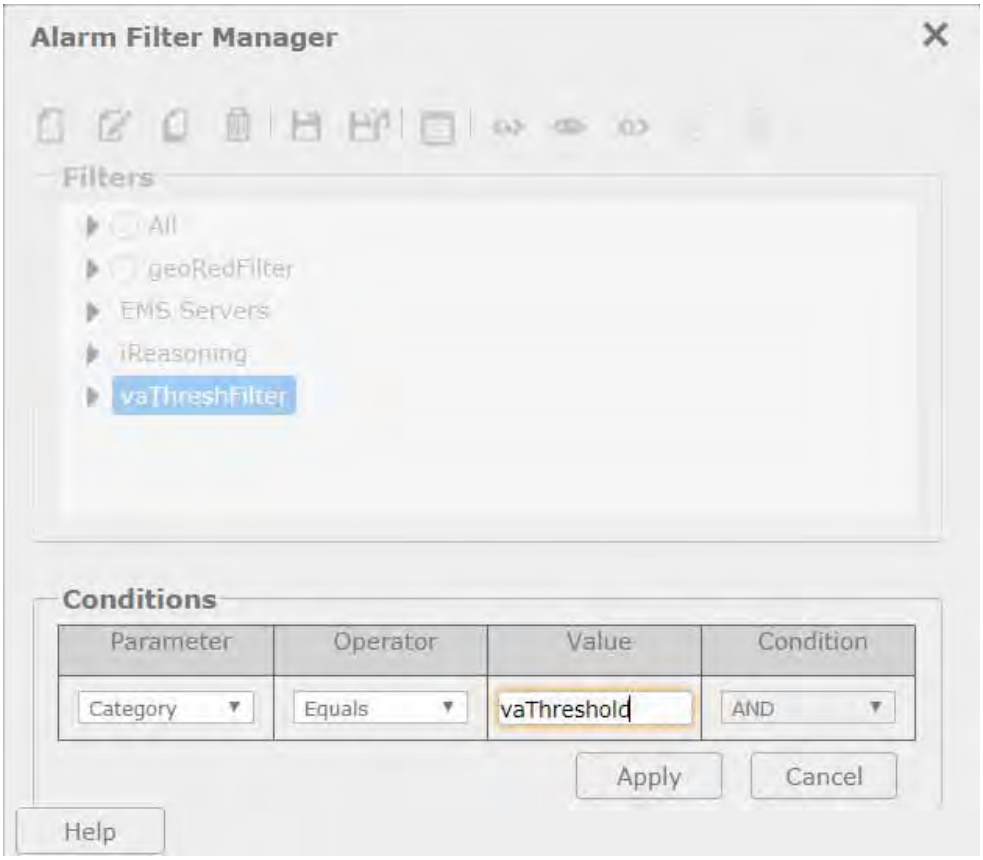
– In the **Parameter** field, select **Category**.

– In the **Operator** field, select **Equals**.

– In the **Value** field, enter the name of the threshold created in Create a Decreasing Threshold of 80%.

b Click **Apply**.

Figure 3-20 Filter Manager



5 Click the **Save Filter** icon.

6 Close the **Alarm Filter Manager**.

Create an Alarm Triggered Configuration

To create an alarm triggered configuration:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Alarm Triggers.

Acuitas displays the **Alarm Triggered Configuration** window.

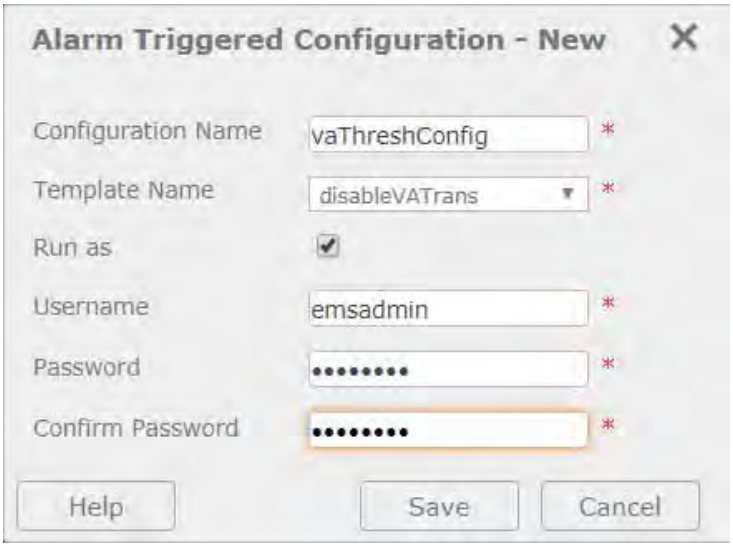
The left pane lists the configured Alarm Triggered configurations. The right pane lists the alarm filters.

2 Click the **New** icon.

3 Configure the parameters as follows:

- **Configuration Name** – Enter a configuration name.
- **Template Name** – Select the Alarm Triggered Configuration Template created in Create an Configuration Maintenance Template.
- **Run as** – Mark this checkbox and provide the necessary credentials to run this configuration task:
- **User Name**
- **Password**
- **Confirm Password**

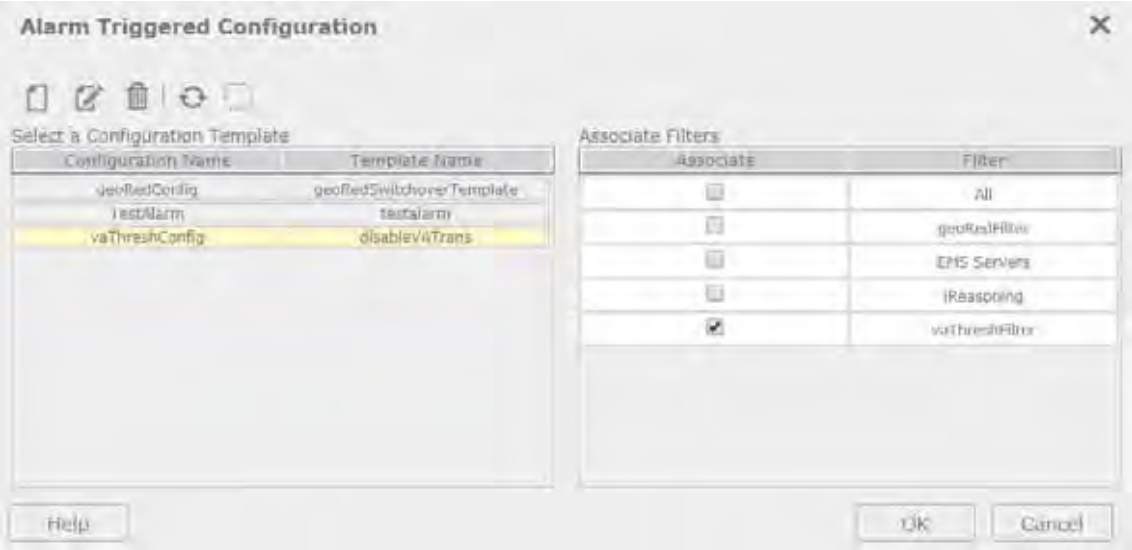
Figure 3-21 Alarm Triggered Configuration



4 Click **Save**. The newly created Alarm Triggered Configuration is listed in the **Alarm Triggered Configuration** window.

5 To associate the configuration with the alarm filter, select the configuration in the left pane and mark the check box in the right pane for the alarm filter created in Create an Alarm Filter for the Decreasing Threshold.

Figure 3-22 Alarm Triggered Configuration



6 Click **OK** to associate the configuration with alarm filter.

Modify the Performance Schedule to Add the Threshold Alarm to the Specific KPI

To modify a User Tasks Scheduler:

1 Click the **Settings** icon on the toolbar and select **Performance** => **User Tasks** => **Schedule**.

2 Select the MCC collection schedule to monitor the Online Transcoding. The scheduler name is <*MCC name*>_MCC_PM_COLLECTION.

3 Click the **Edit User Task Scheduler** icon.

4 When the schedule is fully loaded, scroll through the entire Performance Object table and expand the **derivedmetrics** list.

Figure 3-23 Edit Task Scheduler

5 Scroll through the **derivedmetrics** list and select the Performance Object videoAdaptationOnlineTranscodingProcessedPercentage.

6 In the **Threshold** field, select the threshold that was created in Create a Decreasing Threshold of 80%.

Figure 3-24 Edit Task Scheduler

7 Click **Save**.

View Execution Status

View Triggered Alarm

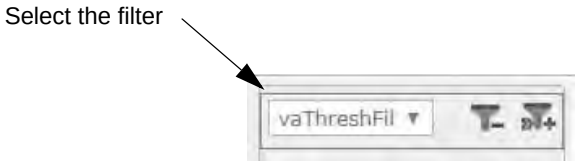
If a threshold alarm has triggered, you can view it.

To view alarms:

1 Click the **Alarms** tab.

2 To filter the alarms list to only the threshold alarms, select the filter created in Create an Alarm Filter for the Decreasing Threshold from the filter list to apply it.

Figure 3-25 Select the Filter



3 Use any of the following methods to view/edit an alarm's details:

Toolbar: Select the alarm and click the **Alarm Details** icon.

Pop-up menu: Right-click the alarm and click **Alarm Details**.

Or: Double-click the alarm.

Acuitas displays the **Alarm Details** window.

View Triggered Configuration Execution Status

Once the alarm has triggered, you can view the Alarm Triggered Configuration execution status.

To view an alarm triggered configuration execution status:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

Alarm Triggers.

Acuitas displays the **Alarm Triggered Configuration** window.

2 Select the alarm triggered configuration created for the threshold and click the

Execution Status icon.

3 Select an Execution Time to view the CLI response from the MCC. The correct response should be as shown in this example.

Figure 3-26 Template Execution Status

Verify the Video Adaptation Instances were Disabled

On the MCC, you can verify whether the video adaptation instances were disabled.

To verify video adaptation instances admin-state:

1 Issue the following CLI command on the MCC:

```
show running-config services video-adaptation instance
online-transcoding
```

The output should show that the admin-state for each instance is disabled:

```
an3000-mcm-slot7cpu1# show running-config services video-adaptation
instance online-transcoding
services video-adaptation instance [Video Adaptation Instance]
online transcoding admin-state disabled
```

Re-enable the Video Adaptation Instances

Once the admin-state for each instance is disabled, the instances remain in that state until you explicitly re-enable them.

To re-enable video adaptation instances admin-state:

1 Issue the following CLI commands on the MCC for each video adaptation instance. Each instance requires its own command to enable the instance:

```
config
services video-adaptation instance [Video Adaptation Instance]
online-transcoding admin-state enabled
commit
exit
```

For example:

```
an3000-mcm-slot7cpu1# config
an3000-mcm-slot7cpu1(config)# services video-adaptation instance
OTF_AND_OFFLINE online-transcoding admin-state enabled
an3000-mcm-slot7cpu1(config-instance-OTF_AND_OFFLINE)# commit
Commit complete.
an3000-mcm-slot7cpu1(config-instance-OTF_AND_OFFLINE)# exit
an3000-mcm-slot7cpu1(config)# services video-adaptation instance
VA_ONLINE online-transcoding admin-state enabled
an3000-mcm-slot7cpu1(config-instance-VA_ONLINE)# commit
Commit complete.
an3000-mcm-slot7cpu1(config-instance-VA_ONLINE)# exit
an3000-mcm-slot7cpu1(config)# exit
```

Audit Trail

The application level Audit Trail records all configuration operations and activities.

For information on Topology Audit Trail, see Audit Trail.

For information on Device Audit Trail, see Device Audit Trail.

Viewing the Audit Trail

Note: *To view the Audit Trail, you must have the Configuration > Config Audit Trails > View Config Audit Trails security group permission. For instructions, see Specifying Permissions by Security Group.*

To view the Audit Trail:

1. Click the **Settings** icon on the toolbar and select **Configuration =>** **Audit Trail**.

   Acuitas displays the **Audit Trail** window, listing the configuration operations.

2. From the **Audit Trail** window, use any of the following methods to view configuration operation details:

   Toolbar: Select the operation and click the **View** icon.

   Pop-up menu: Right-click the operation and click **View**.

   Acuitas displays the **Audit Trail View** window, listing the following information:

   - Resource Name
   - Description
   - User Name
   - Date/Time
   - Status
   - Operation
   - CLI Execution status

3. Click **Close** to close the window.

Exporting Audit Trail

You can export the Audit Trail to a CSV/PDF/XLS/XML/HTML file.

Note: *To export the Audit Trail, you must have the Configuration > Config Audit Trails > Export Config Audit Trails security group permission. For instructions, see Specifying Permissions by Security Group.*

To export the Audit Trail:

1. Click the **Settings** icon on the toolbar and select **Configuration => Audit Trail**.
2. If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.
3. Click the **Export** icon.

   Acuitas displays the **Configure Export Parameters** window.
4. Configure the parameters as follows:
   - **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
   - **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
   - **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
   - **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.
5. Click **Apply**.

   Acuitas displays the **Download Files** window.
6. Click **Download Exported File**.
7. From the **Download File**s window, click **Close**.

File Servers

You can use File Servers across a location to maintain network element database backups and network element software.

Adding File Servers

Note: *To add a File Server, you must have the Configuration > FTP Server Details > Add FTP Server Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To add a file server:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

File Server => Settings.

Acuitas displays the **File Server Settings** window, listing the file servers.

2 Click the **New** icon.

3 Configure the parameters as follows:

- **File Server Type** – Select SFTP.
- **File Server Name**
- **IP Version** – Select IPv4 or IPv6.
- **IP Address**
- **Port**
- **User Name**
- **Password**
- **Confirm Password**
- **Save File Server, if inactive** – Leave the checkbox unmarked if you want the IP Address validated with the given credentials.

4 Click **Save**.

Viewing File Servers

Note: *To view a File Server, you must have the Configuration > FTP Server Details > View FTP Server Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a file server:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

File Server => Settings.

Acuitas displays the **File Server Settings** window, listing the file servers.

2 From the **File Server** window, use any of the following methods to view file server details:

Toolbar: Select the file server and click the **View** icon.

Pop-up menu: Right-click the file server and click **View**.

Acuitas displays the **File Server Details** window, listing the following information:

- File Server Type
- File Server Name
- IP Address
- User Name

3 Click **Close** to close the window.

Modifying File Servers

Note: *To modify a File Server, you must have the Configuration > FTP Server Details > Modify FTP Server Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To modify a file server:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

File Server => Settings.

Acuitas displays the **File Server Settings** window, listing the file servers.

2 Use any of the following methods to modify a file server:

Toolbar: Select the file server and click the **Edit** icon.

Pop-up menu: Right-click the file server and click **Edit**.

Acuitas displays the **Edit Network Element** window.

3 Make the necessary changes:

- **File Server Name**
- **Port**
- **User Name**
- **Password**
- **Confirm Password**
- **Save File Server, if inactive** – Leave the checkbox unmarked if you want the IP Address validated with the given credentials.

4 Click **Save**.

Deleting File Servers

You cannot delete the default file server.

Note: *To delete a File Server, you must have the Configuration > FTP Server Details > Delete FTP Server Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete a file server:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

File Server.

Acuitas displays the **File Server** window, listing the file servers.

2 Use any of the following methods to delete a file server:

Toolbar: Select the file server and click the **Delete** icon.

Pop-up menu: Right-click the file server and select **Delete**.

3 At the confirmation prompt, click **OK**.

Geographic Redundancy Manager

The Acuitas Geographic Redundancy solution is based on a collaborative system of two geographically-separated network elements functioning as standby partners for each other. A Geographic Redundancy group has a designated primary and a designated secondary system. Each group represents a set of services with an active representation on the primary node and a standby representation on the secondary node. If the active node goes out of commission, the services on the standby node can be enabled so these services can resume.

The redundancy group supports the following HA modes:

- **warm-manual** — No session synchronization occurs between nodes. Failovers are Operator controlled.
- **hot-auto** — Synchronization of per-session data occurs between nodes. Failovers are automatically triggered based on network health monitoring results. In addition, failovers can be Operator controlled.
- **hot-manual** — Synchronization of per-session data occurs between nodes. Failovers are Operator controlled.

A Geographic Redundancy group configured as either hot-auto or hot-manual allows for synchronization of session states between the NE pair. The active node synchronizes session data associated with the Geographic Redundancy group with that of its peer. The primary node is the Operator's intended active module based on network design. When the primary node is active, it advertises lower-cost routes compared to the secondary, thus causing control and data traffic to flow towards the primary node under normal networking conditions. In hot-auto mode, the secondary node independently determines whether the network is directing traffic towards it, and fails over to the active state only when external servers are available. The surrounding NEs select the lower cost routes, thus directing traffic to the primary node under normal conditions. In the event of a network outage, some or all of the surrounding NEs may lose routes to the primary node and thus begin forwarding traffic to the secondary node.

When the secondary node detects network reachability on some or all of its shared IP interfaces, it implies a partial or full outage of either the primary node or a network fault. In this scenario, the active node is not functional. In a hot-auto redundancy group, the primary node fails over to standby and the secondary node fails over to active. The primary node withdraws its routes from the network and later re-advertises using a high cost metric (as it becomes standby). The secondary node (now active) advertises lower cost routes, achieves connectivity with its neighboring NEs (if the nature of the network outage allows for it), and resumes processing using the data synchronized with the former primary node.

In hot-auto mode, an automatic failback can occur from the secondary active node to the primary active node under similar circumstances (network fault or secondary node failure). The Operator can also trigger a failback to the primary active node (using switchover).

In hot-manual mode, the operator can monitor for Geographic Redundancy alarms and manually control the failover.

To activate/deactivate a GR group, set the Manual HA State to active on either the primary or secondary node (not both). A GR group in hot-auto mode cannot be manually activated/deactivated.

The Acuitas Geographic Redundancy Manager is the mediator and facilitator of the Geographic Redundancy solution. Acuitas mediates the collaboration between nodes and performs user-initiated actions such as replication and switchover.

Use the Acuitas Geographic Redundancy Manager application to manage and monitor Geographic Redundancy groups:

- Configure Geographic Redundancy group instances and specify what entities you want placed in the Geographic Redundancy group:

Network Context Entities:
Loopback IP ***Note:*** *In either hot-auto or hot-manual mode, the Loopback IP reserved for inter-node communication between the peers cannot be assigned to any Geographic Redundancy group.*
NAT Pool
UE Pool
External Interface Entities:
AAA Interface Group > Diameter > Node Admin Net Health Report Enabled: Specifies whether to monitor network health towards the AAA interface Link Type: Indicates whether the link used to monitor neighboring network elements is a shared link among the primary and secondary NE's or a private (local) link
AAA Interface Group > GTPP > Node Admin
AAA Interface Group > Radius Client > Server Group Net Health Report Enabled: Specifies whether to monitor network health towards the AAA interface Link Type: Specifies whether the link used to monitor neighboring network elements is a shared link among the primary and secondary NE's or a private (local) link
Gateway Entities:
GGSN
PGW
SGW
ePDG
WAG

Service Function Entities:
Charging Instance
Content Filter Instance
QoS Policy: Replicates a QoS Policy and the following associated entities: Services > Rate Limiting Subscriber Group Service Construct > Subscriber Group and associated subscriber ID file
Workflow Entities:
Data Profile
Subscriber Analyzer ***Note:*** *A different Subscriber Analyzer must be used for each Geographic Redundancy group.*

The user can replicate these entities and their associated configuration data from the active node to the standby node. In addition to these entities, the Acuitas Geographic Redundancy Manager replicates Filter Category/Public Key/User Agent files for Content Services.

- Compare configuration data between the active and standby nodes of a selected Geographic Redundancy group.
- Replicate configuration data from the active to the standby node for a selected Geographic Redundancy group.
- Monitor the health of Geographic Redundancy groups.
- Perform a switchover so the standby node takes over service from the previously active node.

Viewing Geographic Redundancy Groups

Note: *To view Geographic Redundancy groups, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To view Geographic Redundancy Groups:

1 Use either of the following methods to view a Geographic Redundancy group:

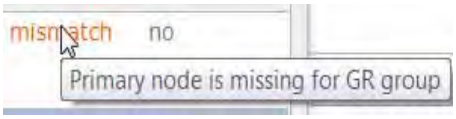
Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager, listing the following information:

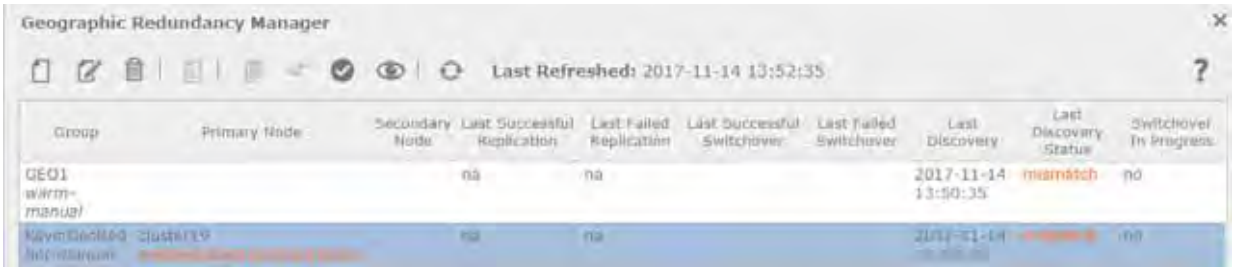
- Group name
- Status for Primary Node and Secondary Node:
  - Name
  - Admin State
  - Operational status
  - Runtime HA state — Specifies the current runtime state of the redundancy group. In manual mode, this value always reflects the manually configured HA state. In hot-auto mode, the HA state can change based on faults or failures in network connectivity.
  - Sync Records — Number of records in queue to be synchronized from active (record source) to standby (record sink).
  - Geo-Link state — Reflects the state of the connection between primary and secondary NEs.
- Switchover in Progress — yes or NA
- Date and time of Last Successful Replication
- Date and time of Last Failed Replication
- Date and time of Last Successful Switchover
- Date and time of Last Failed Switchover
- Date and time of Last Discovery

- Status of Last Discovery:
  - Success — GR group is successfully discovered and found to be consistent across Acuitas, the primary node, and the secondary node.
  - Mismatch — GR group has mismatch(es). To view the mismatch condition, point the cursor at the mismatch status for a tooltip of the mismatch:



For more information on mismatch conditions, see Last Discovery Status is Mismatch.

Figure 3-27 Geographic Redundancy Manager



2 To close the Geographic Redundancy Manager, click the **Close** icon.

Adding Geographic Redundancy Groups

Note: *To add a Geographic Redundancy group, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

Prerequisites

Before setting up a Geographic Redundancy group:

- Verify that the system time between the two nodes is synchronized.
- Disable the Admin State of the Peer objects in the external interface entities you want placed in the Geographic Redundancy group:
  - AAA Interface Group > Diameter > Node Admin > Peer > Admin State > disabled
  - AAA Interface Group > GTPP > Node Admin > Peer > Admin State > disabled

– AAA Interface Group > Radius Client > Server Group > Peer > Admin State > disabled

To add a Geographic Redundancy Group:

1 Use either of the following methods to add a Geographic Redundancy group:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Click the **Create Group** icon.

3 Configure the parameters as follows. The required fields depend on the HA mode you select:

Table 3-8 Geographic Redundancy Group Parameters

Parameter	Description
Common:	
Name	Specify a Geographic Redundancy group name that is unique across the network. The name should not exceed 16 characters. If it does not, Acuitas logs the error during discovery and fails to store the name in the database.
HA Mode	The instance configured HA mode: ■ warm-manual - no synchronization of sessions occurs between nodes. Failovers are operator controlled. ■ hot-auto - synchronization of per-session data occurs between nodes. Failovers are automatically triggered based on network health monitoring outcomes. ■ hot-manual - synchronization of per-session data occurs between nodes. Failovers are operator controlled. Requires that one of the following parameters be set to enabled: – Monitor AAA – Monitor OCS – Monitor PCRF – Monitor S6B – Monitor STA – Monitor SWM

Table 3-8 Geographic Redundancy Group Parameters

Parameter	Description
Route Metric Offset	Route metric offset or cost difference between routes advertised between primary, secondary, active, and standby servers. Specifies the offset value used to form a metric for loopback address routes advertised by the NE associated with a Geographic Redundancy group. Based on the current runtime state, the primary and secondary NE apply a different multiplier to the configured offset when forming a route metric such that the active NE advertises more favorable routes than the standby to the neighboring servers
Route Convergence Interval	Number of seconds for changes in route metrics to propagate between neighboring network elements
Failover Soak Interval	Number of seconds to pause after a failover before considering another failover
Link Timeout	Number of seconds of missed keep-alive packets from the peer before declaring the Geographic Redundancy link down
DSCP Value	DiffServ Code Point value with which to mark all georedundant packets
Group ID	Unique identifier for the group. Once specified, this value cannot be modified. To change a Group ID, the group must first be deleted.
Monitor AAA	Set to enabled to monitor Accounting Authentication Authorization interface to govern fault detection and automatic failover: ■ disabled ■ enabled
Monitor OCS	Set to enabled to monitor OCS to govern fault detection and automatic failover: ■ disabled ■ enabled
Monitor PCRF	Set to enabled to monitor PCRF to govern fault detection and automatic failover: ■ disabled ■ enabled
Monitor S6B	Set to enabled to monitor S6B to govern fault detection and automatic failover: ■ disabled ■ enabled

Table 3-8 Geographic Redundancy Group Parameters

Parameter	Description
Monitor STA	Set to enabled to monitor STA to govern fault detection and automatic failover: ■ disabled ■ enabled
Monitor SWM	Set to enabled to monitor SWM to govern fault detection and automatic failover: ■ disabled ■ enabled
Primary Node:	
Node Name	Select an NE to serve as the primary node in the group
Admin State	Admin State of the primary node: ■ disabled ■ enabled
Manual HA State	Operator's current desired state for the primary node: ■ active ■ standby To activate/deactivate a GR group, set to active on either the primary or secondary node (not both). A GR group in hot-auto mode cannot be manually activated/deactivated.
Network Context	Network context containing this Geographic Redundancy Server service endpoint ***Note:*** *Only one Geographic Redundancy group is allowed per Network Context that has security firewall operations enabled.*
Loopback IP Name	Local node address used for communication between primary and secondary nodes
Loopback IP Address	Local node address used for communication between primary and secondary nodes
Service Endpoint	Service Endpoint for this Geographic Redundancy Server service. The Service Endpoint must already exists. Create it at Network Context > *name* > Service Endpoint
Local Port Range Base	Base UDP port number used for communication between primary and secondary nodes. Must be the initial value of a contiguous block of UDP ports.
Local Number of Ports	Size of the contiguous block of ports
Secondary Node:	Select an NE to serve as the secondary node in the group
Node Name	Select an NE to serve as the primary node in the group

Table 3-8 Geographic Redundancy Group Parameters

Parameter	Description
Admin State	Admin State of the secondary node: ■ disabled ■ enabled
Manual HA State	The manually configured HA state of the secondary node (the operator current desired state): ■ active ■ standby To activate/deactivate a GR group, set to active on either the primary or secondary node (not both). A GR group in hot-auto mode cannot be manually activated/deactivated.
Network Context	Network context containing this Geographic Redundancy Server service endpoint. ***Note:*** *Only one Geographic Redundancy group is allowed per Network Context that has security firewall operations enabled.*
Loopback IP Name	Local node address used for communication between primary and secondary nodes
Loopback IP Address	Local node address used for communication between primary and secondary nodes
Service Endpoint	Service Endpoint for this Geographic Redundancy Server service. The Service Endpoint must already exists. Create it at Network Context > *name* > Service Endpoint
Local Port Range Base	Base UDP port number used for communication between primary and secondary nodes. Must be the initial value of a contiguous block of UDP ports.
Local Number of Ports	Size of the contiguous block of ports.

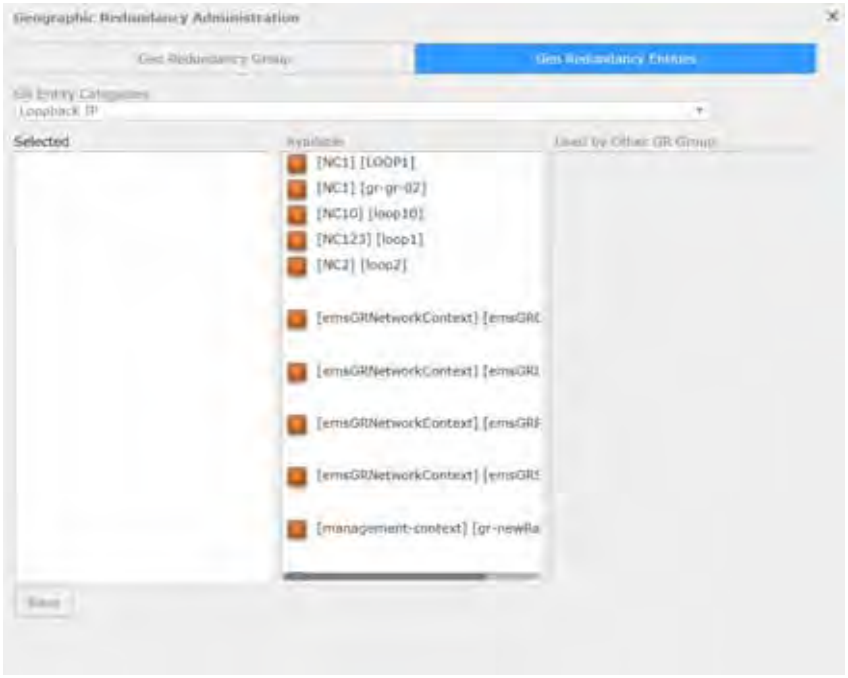
Acuitas propagates the common parameters across both the primary and secondary nodes. In addition, Acuitas ensures that the peer information is configured for both the primary node and secondary node as follows:

- The primary node's local loopback IP address and port range base are used to configure the secondary node's remote IP address and remote base port, respectively.
- The secondary node's local loopback IP address and port range base are used to configure the primary node's remote IP address and remote base port, respectively.

Once the process completes, Acuitas adds the **Geo Redundancy Group** icon to the primary and secondary nodes in the Network View tab, indicating they are members of a Geographic Redundancy group.

4 In the **Geo Redundancy Entities** tab, select an entity category you want to place in the Geographic Redundancy group.

The Geographic Redundancy Manager lists available instances and instances used by another Geographic Redundancy group.



5 To add an entity instance, drag and drop it from the Available list to the Selected list.

If the entity has associated data (indicated with a star icon), Acuitas opens a pop-up configuration window. Configure the parameters in the pop-up window and click **Apply**.

6 Click **Save**.

7 Repeat step 4 through step 6 to add as many entities as needed.

Modifying Geographic Redundancy Groups

Note: *To modify a Geographic Redundancy group, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see* *Specifying Permissions by Security Group**.*

To modify a Geographic Redundancy Group:

1 Use either of the following methods to modify a Geographic Redundancy group:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Select a Geographic Redundancy group.

3 Click the **Modify Group** icon.

4 Configure the parameters as follows. The fields you can change depend on the HA mode:

Table 3-9 Geographic Redundancy Group Parameters

Parameter	Description
Common:	
Name	*Read Only:* Specify a Geographic Redundancy group name that is unique across the network.

Table 3-9 Geographic Redundancy Group Parameters

Parameter	Description
HA Mode	The instance configured HA mode: ■ warm-manual - no synchronization of sessions occurs between nodes. Failovers are operator controlled. ■ hot-auto - synchronization of per-session data occurs between nodes. Failovers are automatically triggered based on network health monitoring outcomes. ■ hot-manual - synchronization of per-session data occurs between nodes. Failovers are operator controlled. Requires that one of the following parameters be set to enabled: – Monitor AAA – Monitor OCS – Monitor PCRF – Monitor S6B – Monitor STA – Monitor SWM You can change HA mode from hot-manual to hot-auto or hot-auto to hot-manual. You cannot change HA mode to or from warm-manual.
Route Metric Offset	Route metric offset or cost difference between routes advertised between primary, secondary, active, and standby servers. Specifies the offset value used to form a metric for loopback address routes advertised by the NE associated with a Geographic Redundancy group. Based on the current runtime state, the primary and secondary NE apply a different multiplier to the configured offset when forming a route metric such that the active NE advertises more favorable routes than the standby to the neighboring servers
Route Convergence Interval	Number of seconds for changes in route metrics to propagate between neighboring network elements
Failover Soak Interval	Number of seconds to pause after a failover before considering another failover
Group ID	*Read Only:* Unique identifier for the group. Once specified, this value cannot be modified. To change a Group ID, the group must first be deleted.
Link Timeout	Number of seconds of missed keep-alive packets from the peer before declaring Geographic Redundancy link down
DSCP Value	DiffServ Code Point value with which to mark all georedundant packets

Table 3-9 Geographic Redundancy Group Parameters

Parameter	Description
Monitor AAA	Whether to monitor Accounting Authentication Authorization interface to govern fault detection and automatic failover: ■ disabled ■ enabled ***Note:*** *Read Only for warm-manual HA mode.*
Monitor OCS	Whether to monitor OCS to govern fault detection and automatic failover: ■ disabled ■ enabled ***Note:*** *Read Only for warm-manual HA mode.*
Monitor PCRF	Whether to monitor PCRF to govern fault detection and automatic failover: ■ disabled ■ enabled ***Note:*** *Read Only for warm-manual HA mode.*
Monitor S6B	Set to enabled to monitor S6B to govern fault detection and automatic failover: ■ disabled ■ enabled
Monitor STA	Set to enabled to monitor STA to govern fault detection and automatic failover: ■ disabled ■ enabled
Monitor SWM	Set to enabled to monitor SWM to govern fault detection and automatic failover: ■ disabled ■ enabled
Primary Node:	
Node Name	*Read Only:* NE to serve as the primary node in the group
Admin State	*Read Only:* Admin State of the primary node: ■ disabled ■ enabled

Table 3-9 Geographic Redundancy Group Parameters

Parameter	Description
Manual HA State	The manually configured HA state of the primary node (the operator current desired state): ■ active ■ standby To activate/deactivate a GR group, set to active on either the primary or secondary node (not both). A GR group in hot-auto mode cannot be manually activated/deactivated
Network Context	Network context containing this Geographic Redundancy Server service endpoint. ***Note:*** *Only one Geographic Redundancy group is allowed per Network Context that has security firewall operations enabled.*
Loopback IP Name	local node address used for communication between primary and secondary nodes
Loopback IP Address	local node address used for communication between primary and secondary nodes
Service Endpoint	Service Endpoint for this Geographic Redundancy Server service. The Service Endpoint must already exists. Create it at Network Context > *name* > Service Endpoint
Local Port Range Base	Base UDP port number used for communication between primary and secondary nodes. Must be the initial value of a contiguous block of UDP ports.
Local Number of Ports	Size of the contiguous block of ports
Secondary Node:	
Node Name	*Read Only:* NE to serve as the secondary node in the group
Admin State	*Read Only:* Admin State of the secondary node: ■ disabled ■ enabled
Manual HA State	The manually configured HA state of the secondary node (the operator current desired state): ■ active ■ standby To activate/deactivate a GR group, set to active on either the primary or secondary node (not both). A GR group in hot-auto mode cannot be manually activated/deactivated
Network Context	Network context containing this Geographic Redundancy Server service endpoint. ***Note:*** *Only one Geographic Redundancy group is allowed per Network Context that has security firewall operations enabled.*

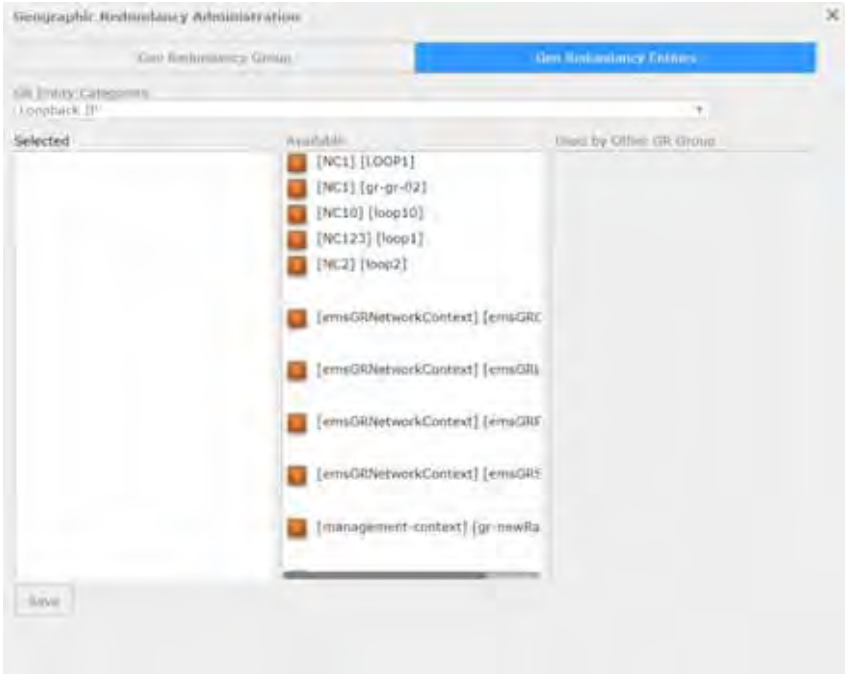
Table 3-9 Geographic Redundancy Group Parameters

Parameter	Description
Loopback IP Name	local node address used for communication between primary and secondary nodes
Loopback IP Address	local node address used for communication between primary and secondary nodes
Service Endpoint	Service Endpoint for this Geographic Redundancy Server service. The Service Endpoint must already exists. Create it at Network Context > *name* > Service Endpoint
Local Port Range Base	Base UDP port number used for communication between primary and secondary nodes. Must be the initial value of a contiguous block of UDP ports.
Local Number of Ports	Size of the contiguous block of ports

5 To toggle the Admin State on the primary node, click **Toggle Primary Admin State**. To toggle the Admin State on the secondary node, click **Toggle Secondary Admin State**. To shut down the Geographic Redundancy group completely, disable the Admin State of both the primary and secondary nodes.

6 In the **Geo Redundancy Entities** tab, select an entity category you want to place in the Geographic Redundancy group.

The Geographic Redundancy Manager lists available instances and instances used by another Geographic Redundancy group.



7 To add an entity instance, drag and drop it from the Available list to the Selected list.

If the entity has associated data (indicated with a star icon), Acuitas opens a pop-up configuration window. Configure the parameters in the pop-up window and click **Apply**.

8 Click **Save**.

9 Repeat step 6 through step 8 to add as many entities as needed.

Comparing Configurations

Use this tool to compare configuration data on the active and standby nodes of a Geographic Redundancy group.

You should use the compare tool to identify any configurations changes that occurred since the last time the configuration was replicated between the active and standby nodes. Do so before replicating (as described in Replicating Configurations.)

Note: *To compare Geographic Redundancy group configurations, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To compare configurations:

1 Use either of the following methods to compare configurations:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Select a Geographic Redundancy group.

3 Click the **Compare** icon.

4 At the confirmation prompt, click **OK**.

Acuitas displays the Configuration Comparison report for the group.

Colored markers indicate where mismatches exist.

Figure 3-28 Configuration Comparison Report

5 Scroll down to the colored markers to view the mismatch.

Figure 3-29 Configuration Mismatch

6 To close the report, click **Close**.

If the Configuration Comparison report lists mismatches, replicate the configuration from the active to the standby node (see Replicating Configurations).

Replicating Configurations

Use this tool to replicate configurations from the active to the standby node of a Geographic Redundancy group. Do so to ensure that the configuration on the standby node is up-to-date relative to the active node.

Note: *The replication action can be service affecting.*

Before replicating, you can use the compare tool to identify configurations mismatches. See Comparing Configurations.

Entities Not Replicated

The following entities are not replicated during the replication process because they are not shared among the MCC clusters for geo-redundancy:

- nsinfo
- alarms available-alarms
- infrastructure logging-filter-parameters
- performance-statistics-management
- service-construct plugin
- personalities
- test
- chassis
- cluster
- service-construct geo-redundancy-server
- ip-protocols
- zone system congestion-control
- zone content congestion-control
- zone gateway congestion-control

- security
- Child entities of network-context except ip-sub-pool
- Entities of service-construct interface aaa-interface-group diameter (when link-type is private)
- Entities of service-construct interface aaa-interface-group radius-client (when link-type is private)

The following attributes are not replicated:

- For all entities: autoIndex
- For zone:
  - content threshold
  - gateway connectivity-check
  - gateway session-load-balancer
  - gateway threshold
  - resource-control
  - system threshold
- For network-context:
  - security
  - number-of-security-services

Note: *To replicate Geographic Redundancy group configurations, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see* *Specifying Permissions by Security Group**.*

To replicate configurations:

1 Use either of the following methods to replicate configurations:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

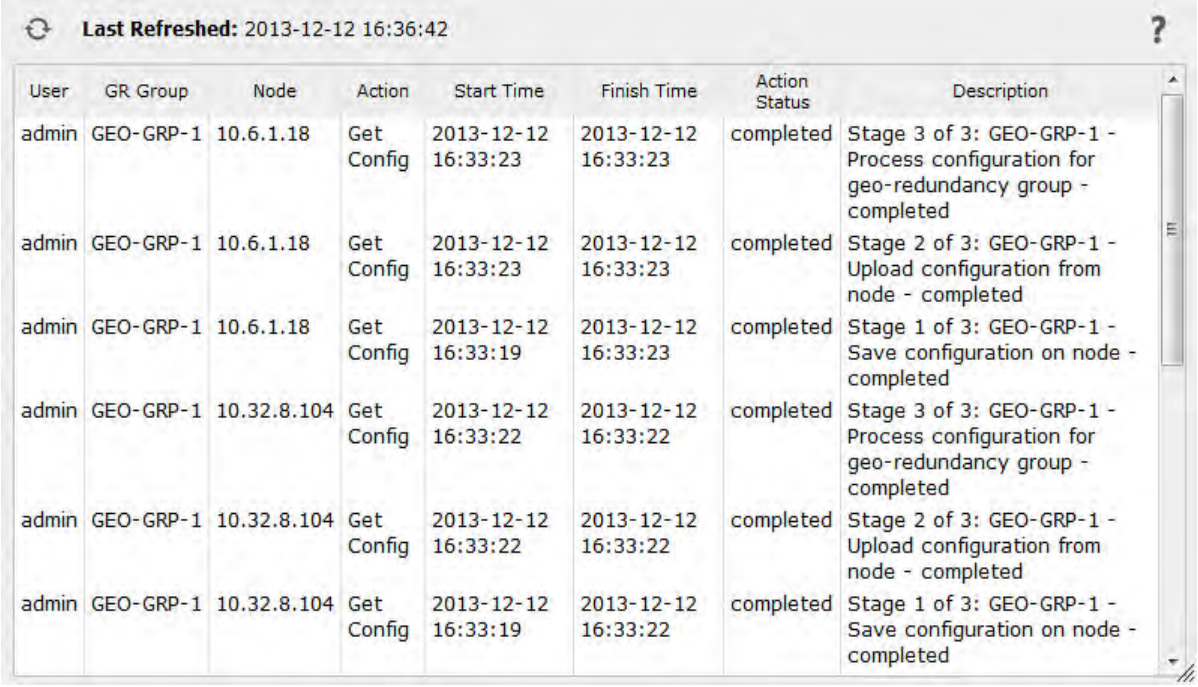
2 Select a Geographic Redundancy group.

3 Click the **Replicate** icon.

4 At the confirmation prompt, click **OK**.

Acuitas displays the Recent Activities report for the group showing the replication process.

Figure 3-30 Replication Activities Report



User	GR Group	Node	Action	Start Time	Finish Time	Action Status	Description
admin	GEO-GRP-1	10.6.1.18	Get Config	2013-12-12 16:33:23	2013-12-12 16:33:23	completed	Stage 3 of 3: GEO-GRP-1 - Process configuration for geo-redundancy group - completed
admin	GEO-GRP-1	10.6.1.18	Get Config	2013-12-12 16:33:23	2013-12-12 16:33:23	completed	Stage 2 of 3: GEO-GRP-1 - Upload configuration from node - completed
admin	GEO-GRP-1	10.6.1.18	Get Config	2013-12-12 16:33:19	2013-12-12 16:33:23	completed	Stage 1 of 3: GEO-GRP-1 - Save configuration on node - completed
admin	GEO-GRP-1	10.32.8.104	Get Config	2013-12-12 16:33:22	2013-12-12 16:33:22	completed	Stage 3 of 3: GEO-GRP-1 - Process configuration for geo-redundancy group - completed
admin	GEO-GRP-1	10.32.8.104	Get Config	2013-12-12 16:33:22	2013-12-12 16:33:22	completed	Stage 2 of 3: GEO-GRP-1 - Upload configuration from node - completed
admin	GEO-GRP-1	10.32.8.104	Get Config	2013-12-12 16:33:19	2013-12-12 16:33:22	completed	Stage 1 of 3: GEO-GRP-1 - Save configuration on node - completed

If Acuitas encounters an error during the configuration loading stage of replication, you can view the details of the actual commands executed on the standby node. Acuitas sources a CLI file for configuration replication on the standby node in the directory:

/home/users/admin/ems.rpl.cli.<Geographic Redundancy Group name>

For details, see Troubleshooting Problems with Geographic Redundancy Groups.

5 To close the report, click the **Close** icon.

Switching Over to the Standby Node

Use this tool to perform a switchover so the standby node takes over service from the previously active node.

In the case of GR group in hot-auto mode, switchover is a one-directional switchover that reverts the primary node from standby to active. Switchover is available only when the following conditions are met:

- Primary node is standby and operationally up
- Standby node is active
- Admin State is enabled on both the primary and secondary node.

To perform a switchover without these restrictions, modify the GR group from hot-auto mode to hot-manual mode. Then, perform the switchover.

Note: *The switchover action can be service affecting.*

Note: *To switchover to the Geographic Redundancy group standby node, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see* *Specifying Permissions by Security Group**.*

To switchover to the standby node:

1 Use either of the following methods to switchover to the standby node:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Select a Geographic Redundancy group.

3 Click the **Switchover** icon.

4 At the confirmation prompt, click **OK**.

Acuitas displays the Recent Activities report for the group showing the switchover process.

5 To close the report, click the **Close** icon.

Viewing Recent Activities

Use this tool to view recent Geographic Redundancy activities.

Note: *To view recent Geographic Redundancy group activities, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To view recent activities:

1 Use either of the following methods to view recent activities:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

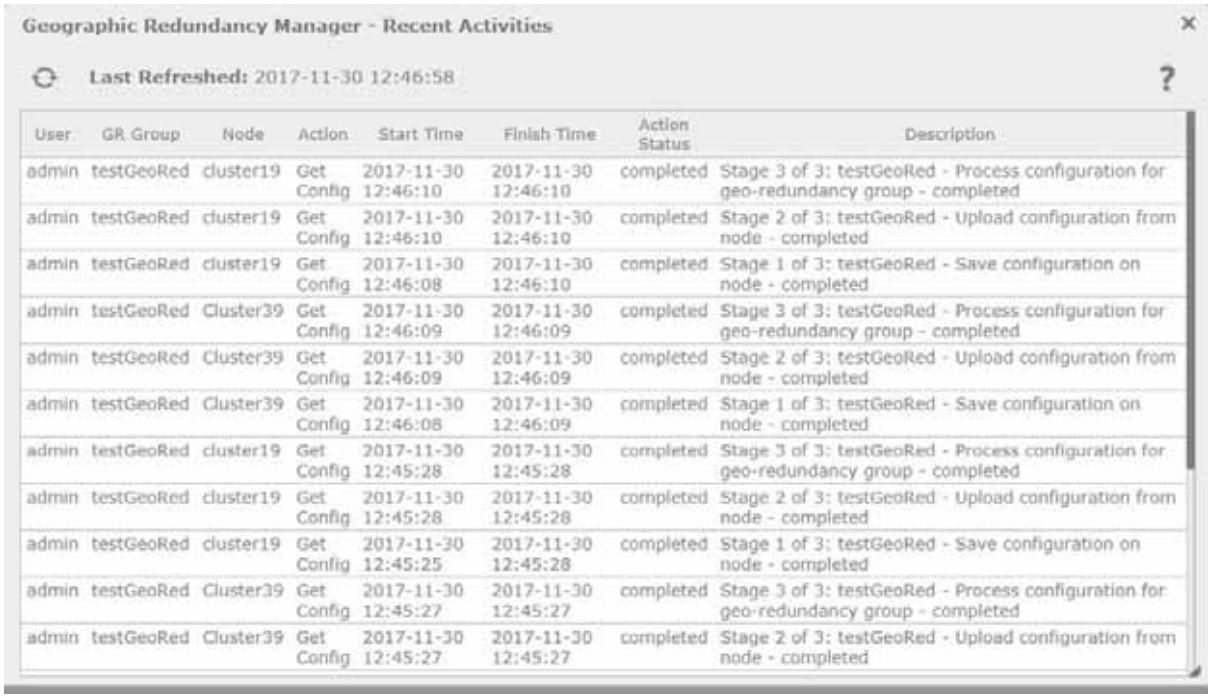
Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Click the **View Recent Activities** icon.

Acuitas displays the Recent Activities report for the group.

Figure 3-31 Recent Activities Report



User	GR Group	Node	Action	Start Time	Finish Time	Action Status	Description
admin	testGeoRed	cluster19	Get Config	2017-11-30 12:46:10	2017-11-30 12:46:10	completed	Stage 3 of 3: testGeoRed - Process configuration for geo-redundancy group - completed
admin	testGeoRed	cluster19	Get Config	2017-11-30 12:46:10	2017-11-30 12:46:10	completed	Stage 2 of 3: testGeoRed - Upload configuration from node - completed
admin	testGeoRed	cluster19	Get Config	2017-11-30 12:46:08	2017-11-30 12:46:10	completed	Stage 1 of 3: testGeoRed - Save configuration on node - completed
admin	testGeoRed	Cluster39	Get Config	2017-11-30 12:46:09	2017-11-30 12:46:09	completed	Stage 3 of 3: testGeoRed - Process configuration for geo-redundancy group - completed
admin	testGeoRed	Cluster39	Get Config	2017-11-30 12:46:09	2017-11-30 12:46:09	completed	Stage 2 of 3: testGeoRed - Upload configuration from node - completed
admin	testGeoRed	Cluster39	Get Config	2017-11-30 12:46:08	2017-11-30 12:46:09	completed	Stage 1 of 3: testGeoRed - Save configuration on node - completed
admin	testGeoRed	cluster19	Get Config	2017-11-30 12:45:28	2017-11-30 12:45:28	completed	Stage 3 of 3: testGeoRed - Process configuration for geo-redundancy group - completed
admin	testGeoRed	cluster19	Get Config	2017-11-30 12:45:28	2017-11-30 12:45:28	completed	Stage 2 of 3: testGeoRed - Upload configuration from node - completed
admin	testGeoRed	cluster19	Get Config	2017-11-30 12:45:25	2017-11-30 12:45:28	completed	Stage 1 of 3: testGeoRed - Save configuration on node - completed
admin	testGeoRed	Cluster39	Get Config	2017-11-30 12:45:27	2017-11-30 12:45:27	completed	Stage 3 of 3: testGeoRed - Process configuration for geo-redundancy group - completed
admin	testGeoRed	Cluster39	Get Config	2017-11-30 12:45:27	2017-11-30 12:45:27	completed	Stage 2 of 3: testGeoRed - Upload configuration from node - completed

3 To refresh the report, click the **Refresh** icon.

4 To close the report, click the **Close** icon.

Viewing Chronological Switchover Log of Geo Redundancy Groups

Use this tool to view the chronological log of switchover events of an individual Geographic Redundancy group.

Note: *To view the chronological switchover log of a Geo Redundancy Group, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To view the chronological switchover log:

1 Use either of the following methods to view the chronological switchover log:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

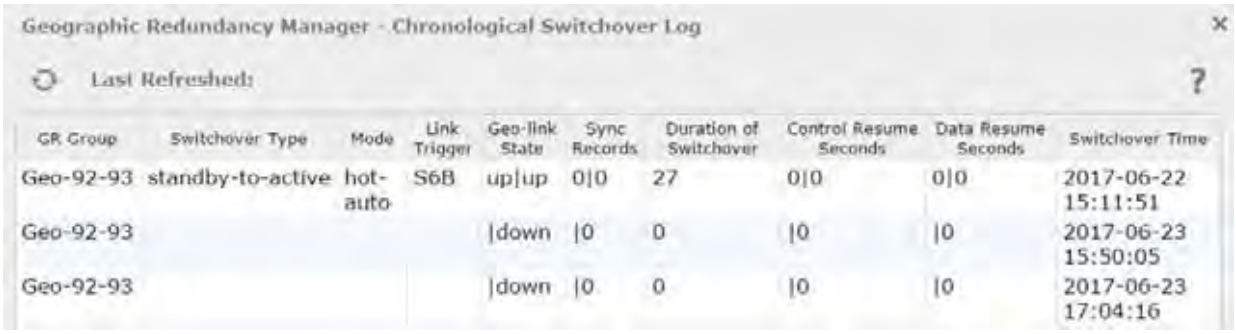
2 Select a Geographic Redundancy group that has had a switchover.

3 Click the **View Chronological Switchover Log** icon.

Acuitas displays the chronological log of the switchover events of the Geographic Redundancy group, including

- GR Group – Name of the Geographic Redundancy group
- Switchover Type – active-to-standby or standby-to-active
- Mode – warm-manual|hot-auto|hot-manual|
- Link Trigger – The link failure that caused the switchover (none|AAA|PCRF|OCS|S6B|STA|SWM|)
- Geo-link State – The geo-link state of both primary and secondary nodes (up|down|partially-up|maint|dryup|congested|)
- Sync Records – Total number of records to sync with the peer node
- Duration of Switchover – Switchover duration, in seconds
- Control Resume Seconds – First control packet received after the switchover, in seconds
- Data Resume Seconds – First data packet received after the switchover, in seconds
- Switchover Time – Timestamp of switchover

Figure 3-32 Chronological Switchover Log



GR Group	Switchover Type	Mode	Link Trigger	Geo-link State	Sync Records	Duration of Switchover	Control Resume Seconds	Data Resume Seconds	Switchover Time
Geo-92-93	standby-to-active	hot-auto	S6B	up|up	0|0	27	0|0	0|0	2017-06-22 15:11:51
Geo-92-93				|down	|0	0	|0	|0	2017-06-23 15:50:05
Geo-92-93				|down	|0	0	|0	|0	2017-06-23 17:04:16

4 To refresh the report, click the **Refresh** icon.

5 To close the report, click the **Close** icon.

Deleting Geographic Redundancy Groups

Deleting a Geographic Redundancy group requires you to make changes using the Configuration Navigator as well as use the Geographic Redundancy Manager.

Note: *To delete Geographic Redundancy groups, you must have Configuration > MCC Configuration > Network Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To delete a Geographic Redundancy Group:

1 Use the Configuration Navigator to disable the Admin State of all the gateway instances that are part of the Geographic Redundancy group on both active and standby node:

Note: *Disabling the Admin State of a gateway can be service affecting.*

---

a Click the gateway instance (For example, Zone > *name* > Gateway > PGW > *name*).

b Set the Admin State to disabled.

c Click the **Save** icon.

d Repeat step a through step c to disable as all the gateway instances included in the Geographic Redundancy group.

2 Use the Geographic Redundancy Manager to disassociate all the entities from the primary node in the Geographic Redundancy group:

a Use either of the following methods to access the Geographic Redundancy Manager:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

b Select the Geographic Redundancy group.

c Click the **Modify Group** icon.

d In the **Geo Redundancy Entities** tab, select an entity category included in the Geographic Redundancy group.

e To remove the entity instance, drag and drop it from the Selected list to the Available list.

f Click **Save**.

g Repeat step d through step f to remove all the entities included in the Geographic Redundancy group.

3 Use the Geographic Redundancy Manager to replicate the Geographic Redundancy configuration for the Geographic Redundancy group:

a Click the **Replicate** icon.

b At the confirmation prompt, click **OK**.

Acuitas displays the Recent Activities report for the group showing the replication process.

c To close the report, click the **Close** icon.

4 Use the Configuration Navigator to delete Loopback IP, NAT Pool, and UE Pool instances that are part of the Geographic Redundancy group on the standby node:

   a Click the object instance (For example, Network Context > *name* > Loopback IP > *name*).

   b Click the **Delete** icon.

   c At the confirmation prompt, click **OK**.

   d Repeat step a through step c to disable as all the Loopback IP, NAT Pool, and UE Pool instances included in the Geographic Redundancy group.

5 Use Geographic Redundancy Manager to delete the Geographic Redundancy group:

   a Use either of the following methods to access the Geographic Redundancy Manager:

   Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

   Network View tab: Click the **Geo Redundancy Group** icon on the device.

   Acuitas displays the Geographic Redundancy Manager.

   b Select the Geographic Redundancy group.

   c Click the **Delete Group** icon.

6 At the confirmation prompt, click **OK**.

Configuration when Primary System is Out of Service

If a situation or disaster places the active system out of service, use one of the following procedures to minimize the scenario where, when the primary system comes back up, both systems are serving as active.

Scenario 1: Active System is Manageable Prior to Going Out of Service

Use this procedure prior to the active system going out of service:

1 Perform a switchover of the Geographic Redundancy group.

Use this procedure once the disaster situation has been resolved:

1 On the secondary (now active) system, disable the Geographic Redundancy group Admin State.

2 On the primary system, enable the Geographic Redundancy group Admin State.

Scenario 2: Active System *is not* Manageable Prior to Going Out of Service

Use this procedure once the Active System is out of service:

1. On the secondary system, enable the Geographic Redundancy group Admin State.

Use this procedure once the disaster situation has been resolved:

1. On the secondary (now active) system, disable the Geographic Redundancy group Admin State.
2. On the primary system, disable the Geographic Redundancy group Admin State to clear any calls that came up while the primary and secondary were concurrently enabled.
3. On the primary system, enable the Geographic Redundancy group Admin State.

Scenario 3: Active System *is not* Manageable Prior to Going Out of Service and is Manually Disconnected from the Network

Use this procedure once the Active System is out of service:

1. Disconnect the primary system from the network.
2. On the secondary system, enable the Geographic Redundancy group Admin State.

Use this procedure once the disaster situation has been resolved:

1. On the secondary (now active) system, disable the Geographic Redundancy group Admin State.
2. Connect the primary system to the network.

Troubleshooting Problems with Geographic Redundancy Groups

Use the solutions in this topic to help troubleshoot Geographic Redundancy group problems.

Geographic Redundancy Group Icon Not Visible

Problem

The Geographic Redundancy group icon is not visible on the device.

Solution

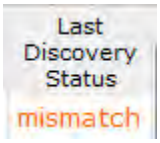
In the Network View tab, the **Geo Redundancy Group** icon appears on the device when you have Configuration > MCC Configuration > Network Configuration > Admin security group permissions.

Ask your System Administrator to grant you those permissions.

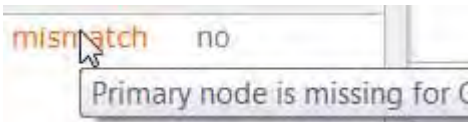
Last Discovery Status is Mismatch

Problem

Following configuration of a Geographic Redundancy group on both the primary and secondary nodes, the Geographic Redundancy Manager lists `mismatch` for the Last Discovery Status.



To view information on the mismatch condition, point the cursor at the mismatch status. Acuitas displays a tooltip of the mismatch:



Discovery mismatch conditions are listed in the following table:

Table 3-10 Discovery Mismatch Conditions

Condition	Description
GR group is not found on primary node	Acuitas failed to find the GR group on the primary node.
GR group is not found on secondary node	Acuitas failed to find the GR group on the secondary node.
Primary node is missing for GR group	Acuitas failed to find the primary node for the GR group.
Secondary node is missing for GR group	Acuitas failed to find the secondary node for the GR group.
Primary node is missing from database	Primary node is missing from the database. Acuitas will resolve it by adding it automatically.
Secondary node is missing from database	Secondary node is missing from the database. Acuitas will resolve it by adding it automatically.
HA mode mismatches on primary node	HA mode of the GR group at the primary node does not match with what is maintained by Acuitas.
HA mode mismatches on secondary node	HA mode of the GR group at the secondary node does not match with that maintained by Acuitas.
Group ID mismatches on primary node	Group ID of the GR group at the primary node does not match with what is maintained by Acuitas.
Group ID mismatches on secondary node	Group ID of the GR group at the secondary node does not match with what is maintained by Acuitas.
HA role mismatches on primary node	HA role mode of the GR group at the primary node does not match with what is maintained by Acuitas.
HA role mismatches on secondary node	HA role of the GR group at the secondary node does not match with that maintained by Acuitas.
GR group has attribute mismatch(es)	Acuitas found discrepanc(ies) for the GR group attributes: ■ For common attribute values between the primary node, secondary node, and Acuitas ■ For peer information for primary or secondary node (for example, the local loopback IP address and local port range base of a GR group on one node must be the same as remote loopback IP address and remote port range base of its peer) The mismatched attribute names are included in of the description.
Primary node is unreachable	Primary node is unreachable and cannot be discovered.
Secondary node is unreachable	Secondary node is unreachable and cannot be discovered.
Both primary and secondary nodes are active	GR groups on both the primary and secondary are operationally active. This is a critical situation that needs to be resolved to avoid service disruptions.

Solution

Acuitas sends alarms when the Geographic Redundancy group is discovered to be in mismatch state. For additional information on the mismatch situation, view the details associated with the corresponding alarms.

Synchronize the Geographic Redundancy configuration:

1 Use either of the following methods to synchronize Geographic Redundancy configuration:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Select the Geographic Redundancy group.

3 Click the **Modify Group** icon.

4 Click **Save**.

Acuitas attempts to synchronize Geographic Redundancy configuration for the group.

How to Enable/Disable a Geographic Redundancy Group on a Node

Problem

How to enable/disable a Geographic Redundancy group on a node.

Solution

To enable/disable a Geographic Redundancy Group on a node:

1 Use either of the following methods to enable/disable a Geographic Redundancy group:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Select the Geographic Redundancy group.

3 Click the **Modify Group** icon.

4 Toggle the Admin State for the node you want to change. To do so, click either **Toggle Primary Admin State** or **Toggle Secondary Admin State**.

To shut down the Geographic Redundancy group completely, disable the Admin State of both the primary and secondary nodes.

Geographic Redundancy Group is Operationally Up on Primary and Secondary Nodes

Problem

The Geographic Redundancy group is operationally up on both the primary and secondary nodes.

Solution

Immediately disable the Admin State of one of the nodes:

1 Use either of the following methods to disable a Geographic Redundancy group:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Select the Geographic Redundancy group.

3 Click the **Modify Group** icon.

4 Toggle the Admin State for the node you want to change. To do so, click either **Toggle Primary Admin State** or **Toggle Secondary Admin State**.

Configuration Comparison Report Lists Differences

Problem

The Configuration Comparison report for primary and standby nodes in a Geographic Redundancy group lists differences.

Solution

Replicate the Geographic Redundancy configuration for the Geographic Redundancy group:

1 Use either of the following methods to replicate the Geographic Redundancy group configuration:

Settings icon on the toolbar: Select **Configuration** => **Geo Redundancy**.

Network View tab: Click the **Geo Redundancy Group** icon on the device.

Acuitas displays the Geographic Redundancy Manager.

2 Select the Geographic Redundancy group.

3 Click the **Replicate** icon.

4 At the confirmation prompt, click **OK**.

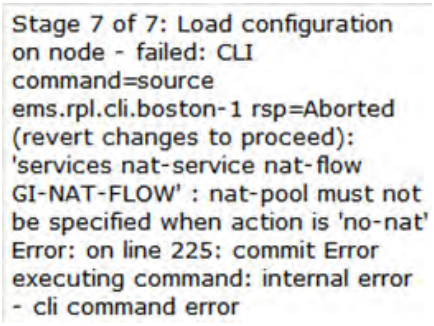
5 To close the report, click the **Close** icon.

If replication does not resolve the configuration differences, you must use the Configuration Navigator to manually resolve them.

Error When Replicating Configuration

Problem

Acuitas encounters an error when replicating the Geographic Redundancy group configuration and reports it in the Recent Activities report.



Solution

Acuitas sources a configuration replication CLI file on the standby node in the directory:

/home/users/admin/ems.rpl.cli.<Geographic Redundancy Group name>

To resolve the error:

1. View the configuration replication CLI file on the standby node.
2. Locate the line that contains the error (line 225 in this example).
3. Use the Configuration Navigator to resolve the configuration error.
4. Issue the following command:

   `source ems.rpl.cli.<Geographic Redundancy Group name>`

Failure Due to Unchangeable Entities

Problem

Following configuration of a Geographic Redundancy group, the Recent Activities report lists failure because entities were unchangeable.

```
Stage 1 of 1: Assign entities
to GR Group - failed: Error:
zone[default] PGW[ch8pgw]
unchangeable
```

Solution

To resolve the failure:

1 Use the Configuration Navigator to disable the Admin State of the object (Zone > *name* > Gateway > PGW in this example).

Note: *Disabling the Admin State of a configuration entity can be service affecting.*

Configuration Export Manager

Use the Configuration Export Manager to save an NE's configuration to raw CLI output. You can provision an NE and save its configuration as a "golden" configuration to be input into a configuration template and applied to other NEs.

For instructions on creating configuration templates, see Configuration Templates.

You can store up to three configuration files for an NE.

Acuitas also supports backing up configuration data for each of the reachable managed NEs to individual files. For details, see Network Configuration Backup.

Viewing Configuration Files

Note: *To view configuration files, you must have Configuration > MCC Configuration > System Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To view configuration files:

1 Click the **Settings** icon on the toolbar and select **Configuration => Configuration Export**.

Acuitas displays the Configuration Export Manager, listing all configuration files. The filename is <*timestamp*>.<*version*>cgf.cli, where *timestamp* is the date and time when the file was saved and *version* is the software version running on the NE.

In the case of a large number of files, Acuitas displays them over multiple pages.

To specify how many files you want displayed per page, select the value in the Show Entries box. Use the page navigational icons at the bottom of the window to page through the entries.

Use the **Search** text box at the top on the window to search for a particular file based on its node name, filename, or size.

Click **Refresh** to refresh the list.

Viewing Configuration Details

You can view a configuration file's details.

To view a configuration file's details:

1 Select the file and click **View**.

Acuitas displays the CLI commands in the configuration file.

Printing Configuration File

You can print a configuration file.

To print a configuration file:

1. Select the file and click **View**.

   Acuitas displays the CLI commands in the configuration file.
2. Click **Print**.
3. Select the desired printer.
4. Click **OK**.

Saving Configuration Files

You can save an active and manageable NE's current configuration to a file. You can save up to three configuration files for an NE. If three configuration files already exist for the NE, Acuitas prompts you to delete one before proceeding.

Note: *To save configuration files, you must have Configuration > MCC Configuration > System Configuration > Admin security group permissions. For instructions, see* *Specifying Permissions by Security Group**.*

To save a configuration file:

1. Click the **Settings** icon on the toolbar and select **Configuration =>** **Configuration Export**.

   Acuitas displays the Configuration Export Manager, listing all configuration files.
2. Select the NE for which you want to save the configuration.
3. Click the **Save** icon.

   The configuration file is added to the list. You may have to page through the entries to view it.

Downloading Configuration Files

You can download a configuration file.

Note: *To download configuration files, you must have Configuration > MCC Configuration > System Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To download a configuration file:

1. Click the **Settings** icon on the toolbar and select **Configuration => Configuration Export**.

   Acuitas displays the Configuration Export Manager, listing all configuration files.
2. Select the file and click **Download**.
3. At the Firefox prompt, click **Save File**.
4. Click **OK**.

Comparing Configuration Files

You can compare two configuration files. For example, you can use the compare tool to identify any configurations changes that occurred between the times the configuration file was saved for a particular node.

Note: *To compare configuration files, you must have Configuration > MCC Configuration > System Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To compare configuration files:

1. Click the **Settings** icon on the toolbar and select **Configuration =>** **Configuration Export**.

   Acuitas displays the Configuration Export Manager, listing all configuration files.
2. Select the first file you want to compare and click **Compare**.
3. At the selection prompt, select the second file to compare and click **Compare**.

   Acuitas displays the Configuration Comparison report for the files.

   Colored markers indicate where mismatches exist.

Figure 3-33 Configuration Comparison Report

4. Scroll down to the colored markers to view the mismatch.
5. To close the report, click **Close**.

Deleting Configuration Files

Note: *To delete configuration files, you must have Configuration > MCC Configuration > System Configuration > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To delete a configuration file:

1. Click the **Settings** icon on the toolbar and select **Configuration => Configuration Export**.

   Acuitas displays the Configuration Export Manager, listing all configuration files.
2. Select the file you want to delete and click **Delete**.
3. At the confirmation prompt, click **OK**.

URL List Management

Use URL List Management to manage files of URLs and avoid input errors. A single URL file can contain a maximum of 5 million individual URLs.

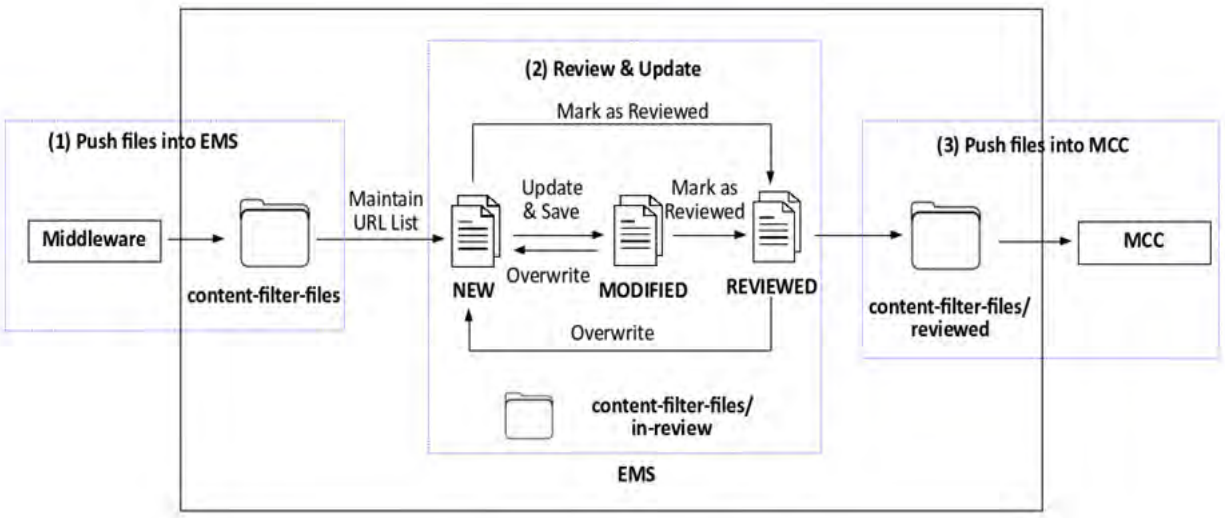
You can use URL List Management to:

- View URL file contents
- Edit URL file contents
- Import contents from a local URL file
- Compare current to previous URL file contents
- Push the URL file onto single or multiple network elements

Note: *To manage URL lists, you must have the Configuration > URL List Management security group permission. For instructions, see Specifying Permissions by Security Group.*

The following figure illustrates the directory structure and lifecycle management of URL files in the /opt/Affirmed/NMS/server/ems/data/content-filter-files directory.

Figure 3-34 URL List File Lifecycle Management



Viewing URL List Files

You can view the current set of URL list files in the /opt/Affirmed/NMS/server/ems/data/content-filter-files directory.

To view URL list files:

1 Click the **Settings** icon on the toolbar and select **Configuration =>** **URL List => Maintenance**.

Acuitas displays the **URL List Maintenance** window, listing the URL list files.

Figure 3-35 URL List Maintenance Window

The window lists the following information:

- URL File Name
- File Type
- File Size
- State: NEW, MODIFIED, REVIEWED
- Last Reviewed Time
- Auto Push: checkbox to automatically push a clear-text file to destination network elements.

- Operations:
  - Review and Edit
  - Overwrite
  - Mark As Reviewed
  - Compare

These Operations are described in the following sections.

Specifying to Auto-Push File to Destination Network Elements

You can enable Auto-Push to automatically push a clear-text file to destination network elements. By default, Auto-Push pushes the files to all managed network elements every hour. The existing files on the network elements are overwritten with each Auto-Push.

To enable Auto-Push for a file:

1. From the **URL List Maintenance** window, mark the **Auto Push** checkbox for the URL List.

2. At the confirmation prompt, click **OK**.

   When Auto-Push is enabled, the other operations (Review and Edit, Overwrite, Mark As Reviewed, and Compare) are disabled for the file.

   You must explicitly enable the Auto-Push schedule.

To enable the Auto-Push schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration =>**

   URL List => Schedule.

   Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

   The pre-defined AUTO-PUSH-HASHED schedule pushes all hashed files to destination network elements. The pre-defined AUTO-PUSH-CLEAR-TEXT schedule pushes specified clear-text files to destination network elements.
2. Use any of the following methods to enable the pre-defined AUTO-PUSH-HASHED or AUTO-PUSH-CLEAR-TEXT schedule:

   Toolbar: Select the URL list schedule and click the **Enable Schedule** icon.

   Pop-up menu: Right-click the URL list schedule and select **Enable Schedule**.

Specifying Auto-Push Settings

You can modify the default Auto-Push settings, including push frequency and destination network elements.

To modify Auto-Push settings:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

URL List => Schedule.

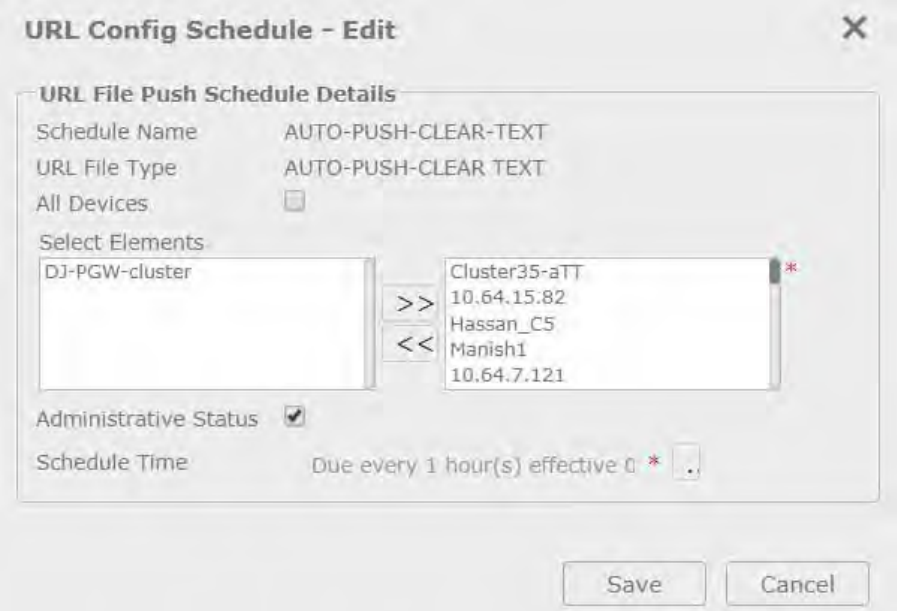
Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2 Use any of the following methods to modify the pre-defined AUTO-PUSH-HASHED or AUTO-PUSH-CLEAR-TEXT schedule:

Toolbar: Select the URL list schedule and click the **Edit** icon.

Pop-up menu: Right-click the URL list schedule and select **Edit**.

Figure 3-36 Edit URL List Schedule Window



3 Make the necessary changes:

- **Schedule Name** – *Read-only.*
- **URL File Type** – *Read-only*.
- **All Devices** – Mark the checkbox to push the files to all destination network elements. Unmark the checkbox to specify the destination network elements.
- **Select Elements** – Select the network elements by highlighting and clicking the right-arrow.

- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time**:
  - Click **Recurrence Pattern** icon.
  - Specify the recurrence details and click **Schedule**.

4 Click **Save**.

Review and Edit

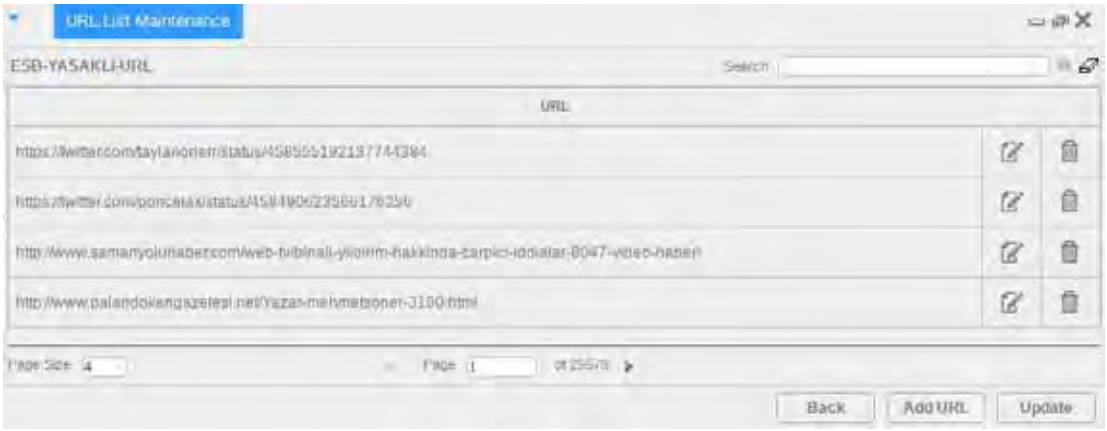
You can review and edit URLs in a clear-text URL file.

To edit URLs in a file:

1 From the **URL List Maintenance** window, click the **Review and Edit** icon of the URL list you want to review.

Acuitas lists the URLs in the file.

Figure 3-37 URLs in the File



2 Use the **Search** text box to search for URL instance(s) by string. Enter the string (minimum 5 characters) contained in the URL and click the **Search** icon. For example, enter twitter to list all URLs containing twitter.

Editing a Single URL

To edit a single URL in a file:

1 Click the **Edit** icon of the URL you want to modify.

2 Change the URL string in the text box. When you have finished, click the **OK** icon

The URL is highlighted in yellow to indicate it has been changed.

To undo the change, click the **Undo** icon.

3 You can make up to 50 edit and deletion changes to a file during a single update session. To save all changes for this update session, click **Update**. The state changes to MODIFIED.

If you attempt to make more than 50 changes, the system prompts you to save the current set of changes. Click **OK**.

4 To return to the **URL List Maintenance** window, click **Back**.

Deleting a Single URL

To delete a single URL in a file:

1 Click the **Delete** icon of the URL you want to delete.

The URL is highlighted in red to indicate it is deleted.

To undo the change, click the **Undo** icon.

2 You can make up to 50 edit and deletion changes to a file during a single update session. To save all changes for this update session, click **Update**. The state changes to MODIFIED.

If you attempt to make more than 50 changes, the system prompts you to save the current set of changes. Click **OK**.

3 To return to the **URL List Maintenance** window, click **Back**.

Adding URL(s) to a File

You can add URL(s) to a file either by:

- Entering them as text: Maximum of 50 changes to a file during a single update session
- Uploading a text file: Maximum uploaded file size: 9 MB.

To add URL(s) to a file:

1. Click **Add URL**.
2. In the **Type** field, select **Text** or **File**.
   - If you select **Text**, enter the URL(s) in the text box, each on its own line.
   - If you select **File**, click **Choose File** to upload a text file of URLs. Select the text file and click **Upload**.
3. Click **Add**.

   The added URL(s) are appended to the end of the URL file. The file state changes to MODIFIED.
4. To return to the **URL List Maintenance** window, click **Back**.

Overwrite

You can overwrite a clear-text URL file that is in the MODIFIED or REVIEWED state, as long as it contains the same content in both the /opt/Affirmed/NMS/server/ems/data/content-filter-files/ directory and the /opt/Affirmed/NMS/server/ems/data/content-filter-files/in-reviewed directory. When you do so, the file in the /in-review directory is overwritten by the file in the content-filter-files/ directory.

To overwrite a file:

1. From the **URL List Maintenance** window, click the **Overwrite** icon of the URL list you want to overwrite.

Mark As Reviewed

You can mark a clear-text URL file that is in the MODIFIED state as reviewed.

To mark a file as reviewed:

1 From the **URL List Maintenance** window, click the **Mark As Reviewed** icon of the URL list.

The file is copied from the /opt/Affirmed/NMS/server/ems/data/content-filter-files/in-review directory to the /opt/Affirmed/NMS/server/ems/data/content-filter-files/reviewed directory. The state changes to REVIEWED.

Compare

You can compare a clear-text URL file's current contents to its earlier file contents to identify any URLs added or removed since the last time the file was marked as reviewed. The operation compares the current version of file in /opt/Affirmed/NMS/server/ems/data/content-filter-files/in-review to its previous reviewed version of file in /opt/Affirmed/NMS/server/ems/.data/content-filter-files/reviewed.

To perform the Compare operation, the system copies and separately maintains the current available file from the /reviewed and /in-review directories until the operation completes. Any subsequent changes made by Review and Edit, Overwrite, or Mark As Reviewed are not taken into account in the comparison. The resulting Comparison file lists the timestamps from the file versions from the /reviewed and /in-review folders.

You can perform only one Compare operation at a time.

To compare a file:

1 From the **URL List Maintenance** window, click the **Compare** icon of the URL list you want to compare.

2 If the files are identical, click **OK** at the confirmation prompt.

3 If the files differ, the **Compare** icon changes to a **Comparison File** icon.

4 Click the icon to view the changes.

5 In the **Diff** field, select **Added URLs** or **Removed URLs** to view the list.

Figure 3-38 Comparison File

6 You cannot perform another comparison on these files until the comparison file is deleted. To delete it, click the **Delete** icon.

7 To return to the **URL List Maintenance** window, click **Back**.

URL List Schedules

Acuitas allows you to manage the schedules to push a clear-text URL list onto a single or multiple network elements. For example, you can schedule to upload a URL list for a set of Network Elements as part of a typical maintenance cycle. The operation to push a URL list to a network element is logged to the Audit Trail.

As an alternative, you can enable Auto-Push, which automatically pushes a clear-text file to destination network elements. See Specifying to Auto-Push File to Destination Network Elements.

Adding URL List Schedules

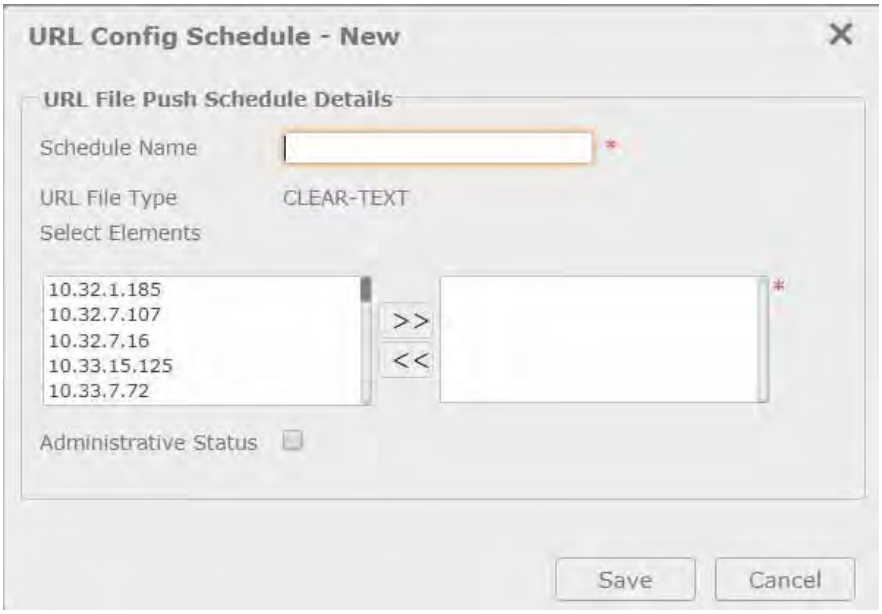
To add a URL list schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration** => **URL List** => **Schedule**.

Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2 Click the **New** icon.

Figure 3-39 New URL List Schedule Window



3 Configure the parameters as follows:

- **Schedule Name** – Enter a schedule name.
- **Select Elements** – Select the elements by highlighting and clicking the right-arrow.

- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.

- **Schedule Time** – Click the **Calendar** icon and select a date and time.

4 Click **Save**.

Viewing URL List Schedules

To view a software schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

URL List => Schedule.

Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2 From the **URL Config Schedule** window, use any of the following methods to view software schedule details:

Toolbar: Select the URL list schedule and click the **View** icon.

Pop-up menu: Right-click the URL list schedule and click **View**.

Acuitas displays the **URL Config Schedule View** window, listing the following information:

- Schedule Name
- URL List Name
- Element Name(s)
- Last Execution Time
- Operational Status
- Administrative Status

3 Click **Close** to close the window.

Viewing URL List Schedule Subtask Status

When multiple Network Elements use a particular URL list schedule, Acuitas creates a separate subtask to run the schedule on each node. You can view the status of a each subtask.

To view URL list schedule subtask status:

1. Click the **Settings** icon on the toolbar and select **Configuration => URL List => Schedule**.

   Acuitas displays the **URL List Config Schedule** window, listing the URL list schedules.

2. From the **URL List Config Schedule** window, use any of the following methods to view subtasks:

   Toolbar: Select the URL list schedule and click the **View Sub Tasks** icon.

   Pop-up menu: Right-click the URL list schedule and click **View Sub Tasks**.

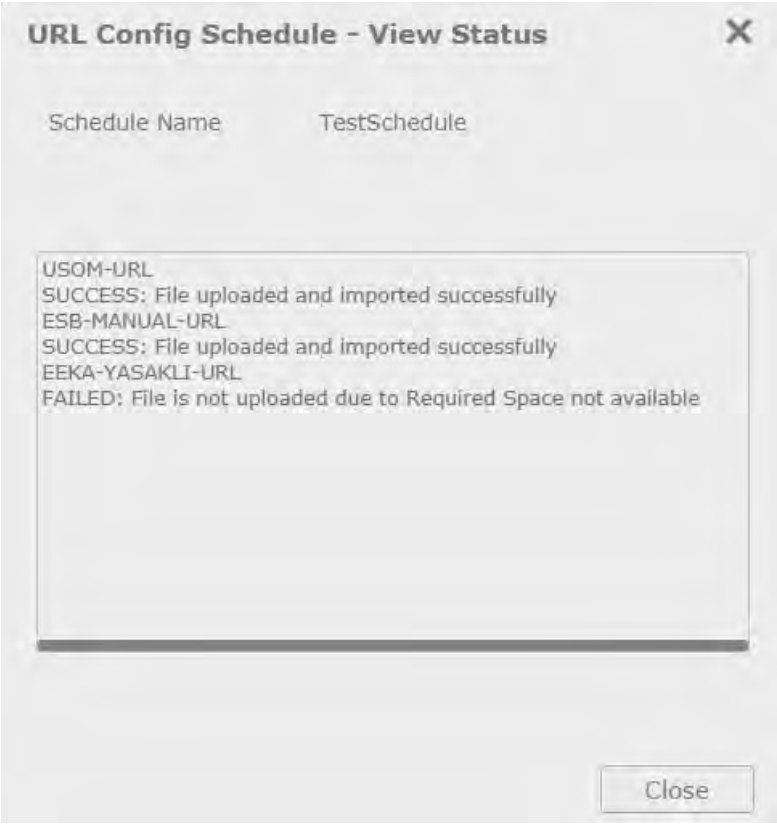
   Acuitas displays the **Sub Tasks Details** window, listing the following information:

   - Element Name
   - Schedule Name
   - URL File Type
   - Order of Execution
   - Status
   - Last Attempted Time
   - Operational Status

3. To view software schedule status of a subtask, select the subtask and click the **View Status** icon.

4. Acuitas displays the **URL Config Schedule View Status** window, listing the URL list schedule progress status report.

Figure 3-40 URL Config Schedule View Status Window



5 Click **Close** to close the window.

6 To close the **Sub Tasks Details** window, click the **Close** icon.

Copying URL List Schedules

You can make a copy of an existing URL list schedule and then modify and save it with a new name. You cannot copy the pre-defined AUTO-PUSH-HASHED and AUTO-PUSH-CLEAR-TEXT schedules.

To copy a URL list schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

URL List => Schedule.

Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2 To copy a URL list schedule, select the URL list schedule and click the **Copy** icon.

3 Make the necessary changes:

- **Schedule Name** – Enter a schedule name.
- **Select Elements** – Select the elements by highlighting and clicking the right-arrow.
- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time** – Click the **Calendar** icon and select a date and time.

4 Click **Save**.

Enabling/Disabling URL List Schedules

To enable/disable a URL list schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

URL List => Schedule.

Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2 Use any of the following methods to enable a URL list schedule:

Toolbar: Select the URL list schedule and click the **Enable Schedule** icon.

Pop-up menu: Right-click the URL list schedule and select **Enable Schedule**.

Use any of the following methods to disable a URL list schedule:

Toolbar: Select the URL list schedule and click the **Disable Schedule** icon.

Pop-up menu: Right-click the URL list schedule and select **Disable Schedule**.

3 At the confirmation prompt, click **OK**.

The Administrative Status of the URL list schedule changes to Enabled or Disabled.

Quick Start Software Schedules

To Quick Start (instantly execute) a URL list schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

URL List => Schedule.

Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2 Use any of the following methods to Quick Start a URL list schedule:

Toolbar: Select the URL list schedule and click the **Quick Start** icon.

Pop-up menu: Right-click the URL list schedule and select **Quick Start**.

Modifying URL List Schedules

To modify a URL list schedule:

1 Click the **Settings** icon on the toolbar and select **Configuration =>**

URL List => Schedule.

Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2 Use any of the following methods to modify a URL list schedule:

Toolbar: Select the URL list schedule and click the **Edit** icon.

Pop-up menu: Right-click the URL list schedule and select **Edit**.

3 Make the necessary changes:

- **Schedule Name** – *Read-only.*
- **URL File Type** – *Read-only*.
- **All Devices** – For the pre-defined AUTO-PUSH-HASHED and AUTO-PUSH-CLEAR-TEXT schedules, mark the checkbox to push the files to all destination network elements. Unmark the checkbox to specify the destination network elements.
- **Select Elements** – Select the elements by highlighting and clicking the right-arrow.
- **Administrative Status** – Mark the checkbox to set the Admin Status of the schedule to Enabled.
- **Schedule Time**:
  - Click **Recurrence Pattern** icon.
  - Specify the recurrence details and click **Schedule**.

4 Click **Save**.

Deleting URL List Schedules

You can delete a URL list schedule only if it has the Operational state Scheduled, Success, or Failure. You cannot delete the pre-defined AUTO-PUSH-HASHED and AUTO-PUSH-CLEAR-TEXT schedules.

To delete a URL list schedule:

1. Click the **Settings** icon on the toolbar and select **Configuration => URL List => Schedule**.

   Acuitas displays the **URL Config Schedule** window, listing the URL list schedules.

2. Use any of the following methods to delete a URL list schedule:

   Toolbar: Select the URL list schedule and click the **Delete** icon.

   Pop-up menu: Right-click the URL list schedule and select **Delete**.

3. At the confirmation prompt, click **OK**.

Chapter 4

Fault

Acuitas allows you to:

- Identify network elements with alarms
- View alarms and events

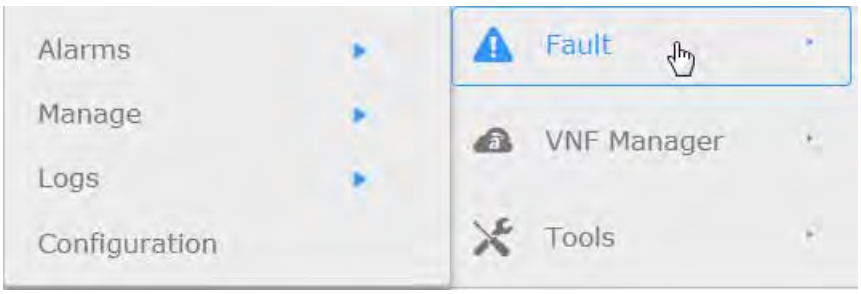
In addition, Acuitas allows you to configure the Fault Management functions that:

- Detect and isolate malfunctions in a network
- Maintain logs of traps received from the system for Operators to examine for any network fault
- Acknowledge and act on error detection notifications
- Trace and identify faults associated with network elements or the Acuitas system.

Note: *For fault information for the MCC MME, see the Affirmed Networks MCC MME Fault Management Reference Guide.*

To access Fault applications, select the applicable option from the **Settings** icon on the toolbar.

Figure 4-1 Accessing Fault Applications



Alarms

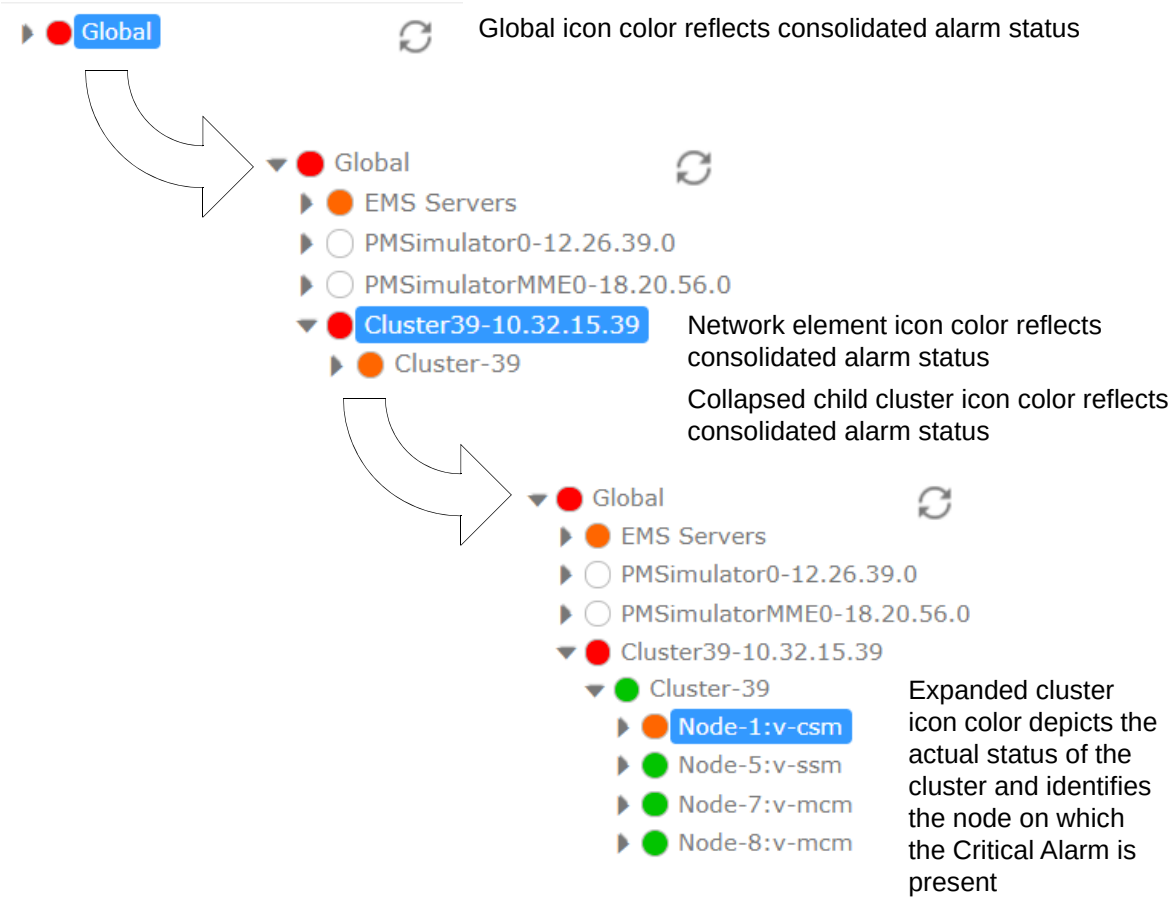
Identifying Network Elements with Alarms

Acuitas dynamically updates the tree display with current alarm information. As alarms are generated, the tree node icon changes color to represent the highest severity of alarms. Alarm color is propagated from the particular component for which the alarm was generated to the parent of the component. Specifically, when the parent component is collapsed in the tree, its icon color reflects the consolidated alarm status. When the parent component is expanded in the tree, its icon color depicts the actual status of the node.

Note: *Alarm severity color is configurable. For instructions, see Configuring Alarm Severity Color Settings.*

Alarm Propagation depicts how a user drills down to the actual problem after observing an alarm propagated to the Global level.

Figure 4-2 Alarm Propagation



Managing Network Element Fault Management State

When a network element is added to Acuitas, its Managed Fault management state is set to Active so that Acuitas automatically configures itself as a trap destination and can process traps from the network element.

There are scenarios where Acuitas can resolve Fault Management problems in production systems. For example:

- If a managed network element is not properly configured or setup, it can send a high rate of traps to Acuitas. If it overflows the Acuitas traps staging buffer, many incoming traps to Acuitas can be dropped. And, when encountering a trap storm, Acuitas can consume a lot of resources to process the incoming traps and purge traps-related database tables, resulting in a significant negative impact on the Acuitas performance and operations. In this scenario, the administrator can set the network element's Managed Fault management state to unmanaged so that Acuitas removes itself as trap destination and no longer receives new traps from the network element. Once the issues are resolved, the administrator must set the network element's Managed Fault management state to managed.

- If, during the course of network element operation, the Acuitas trap destination is inadvertently deleted from the network element, Acuitas shows no notification or warning that the trap destination is deleted. As a result, Acuitas no longer receives any traps from the network element. If this scenario arises, Acuitas can automatically configure itself as a trap destination.

- Some network elements support a fixed number of trap destinations. If, when adding the element to Acuitas for management, the maximum number is reached, Acuitas cannot configure itself as a trap destination. If this scenario arises, Acuitas can notify the user and periodically retry to configure itself as a trap destination.

Changing Managed Fault management state to unmanaged is an infrequent operation performed only when Acuitas is overwhelmed by a trap storm. The action required by the administrator is to change the Managed Fault management state to unmanaged and rectify the situation. Then, when the issues have been corrected, the administrator must change the Managed Fault management state back to managed.

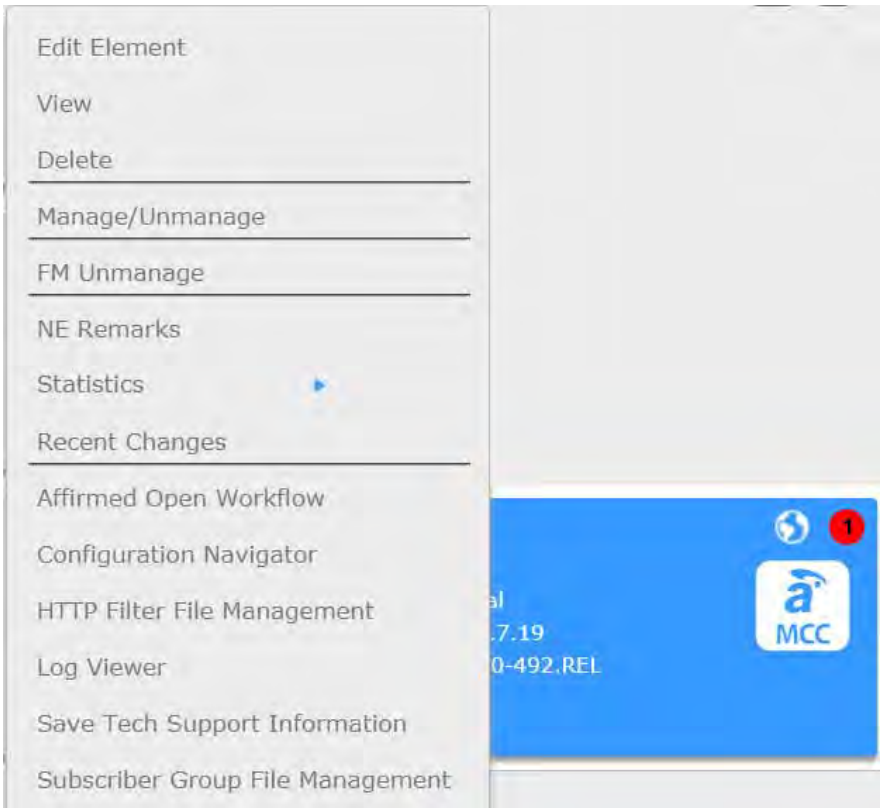
Note: *To manage/unmanage Fault Management state of a network element, you must have the Topology > Group Details > Edit Group security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To manage/unmanage the Managed Fault management state of a network element, the network element must be in the Managed state (is accessible by Acuitas).

To manage/unmanage the Managed Fault management state of a network element:

1 Right-click a network element and click **FM Manage** or **FM Unmanage**.

Figure 4-3 FM Manage/Unmanage



2 At the confirmation prompt, click **OK**.

When the network element is in Managed state (is accessible by Acuitas), the device icon in the Network View tab includes a status icon for Managed Fault management state and trap destination state indicating that administrator attention is required:

- When the Managed Fault management state is set to Managed but Acuitas is not configured as a trap destination of the network element, the state icon is red.

  To determine the cause of the state icon, point the cursor at the icon. Acuitas opens a pop-up window that lists the cause.

To determine the cause of the bad trap destination state, click the state icon. Acuitas opens a pop-up Alert window that lists the cause.

If this scenario arises, Acuitas periodically retries to configure itself as a trap destination.

- When the Managed Fault management state is set to Unmanaged, the device lists the Status as FM Unmanaged and the state icon is grey.

  To determine the cause of the state icon, point the cursor at the icon. Acuitas opens a pop-up window that lists the cause..

  If this scenario arises, the administrator can set the Managed Fault management state to Managed.

During normal operation, when the network element Managed Fault management state is set to Managed and Acuitas is configured as a trap destination, no state icon is shown on the device icon because no user attention is required.

When the network element is in Managed state (is accessible by Acuitas), its Managed Fault management state is set to Managed (Active) and Acuitas automatically configures itself as a trap destination.

If the administrator unmanages the network element (is inaccessible by Acuitas), Acuitas sets the Managed Fault management state to unmanaged (Inactive) and removes the Acuitas trap destination from the network element.

Configuring Trap OID Display Length

By default, Acuitas displays the complete trap OID in the Trap OID field in the following areas of Acuitas:

- Alarms and Event Logs tabs
- Host System Alarms tab
- Alarm Details window
- Event Logs View window
- Alarm Filter Conditions (under Parameter)

For example:

.1.3.6.1.4.1.116.6.41.1.1.1.1.1.1.65536002

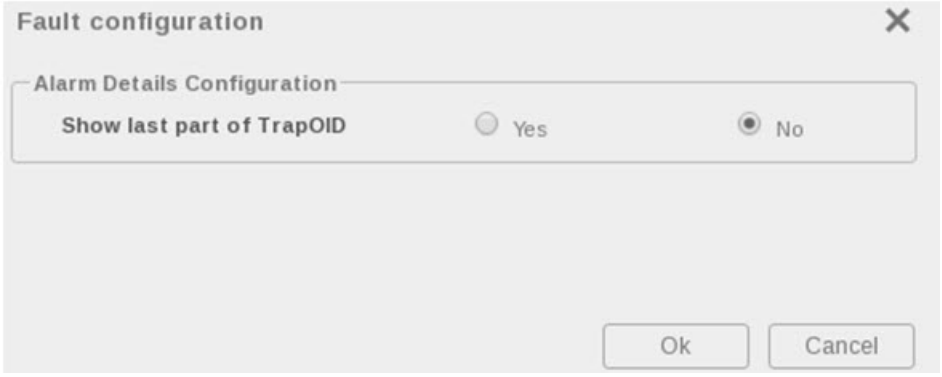
You can configure Acuitas to display only the last part of the full OID. For example:

65536002

Note: *To configure trap OID display length, you must have the Fault > Configuration security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To configure the Trap OID display length:

1. Click the **Settings** icon on the toolbar and select **Fault => Configure**.
2. In the **Show last part of TrapOID** field, mark the **Yes** box and click **OK**.



Viewing Alarms

The Alarm Browser provides a summary of the Alarms currently active for the selected group or network element in the tree. It displays the Alarm specific details in a tabular view indicating information on network element, affected component, reason for the alarm, severity of the alarm, and similar parameters.

For information about viewing alarms generated by host system components, such as iLO and VMware alarms associated with a virtual node, see Viewing Host System Alarms.

Note: *To view alarms, you must have the Fault > Alarms > View Alarms security group permission. For instructions, see Specifying Permissions by Security Group.*

To view alarms:

1. Select the object in the tree for which you want to view alarms:
   - To view alarms from all NEs, select **Global** in the tree.
   - To view alarms from NEs in a particular group, select the group in the tree.
   - To view alarms for a particular NE, select the NE in the tree.
2. To view NE alarms, click the **Alarms** tab.

Figure 4-4 Alarms tab

Alarms are listed with the following information:

- **Alarm ID** – Unique ID of the alarm
- **Severity** – Problem severity
- **Host Name** – Network element reporting the problem
- **Group** – Group having the fault
- **Source** – Network element component having the fault
- **Message** – Message/fault description obtained from the network element
- **Date Updated** – Date and time of last update of the alarm
- **Ack. Status** – Indicates whether or not the alarm is acknowledged
- **Owner** – Alarm owner
- **Category** – Alarm category, such as Temperature Threshold, CPU Threshold
- **Event Type** – (network element alarm/status poll/data collection)
- **Date Created** – Date and time when the alarm was raised
- **Age** – Numbers of days, hours, minutes, seconds, and milliseconds since the alarm was raised
- **Date Ack.** – Date and time the alarm was acknowledged, if applicable
- **Cleared Time** – Date and time the alarm was cleared, if applicable
- **Remedy** – Problem remedy suggested by the administrator
- **Additional Info** – Lists more information about the alarm
- **NE Alarm SeqNo** – NE Alarm Sequence Number
- **NE Alarm Idx** – NE Alarm Index
- **Trap OID** – Unique identifier for the device alarm type. Is listed as **N/A** for EMS Server alarms. To configure trap OID display length, see Configuring Trap OID Display Length.

Viewing Host System Alarms

For virtual nodes and clusters, you can view alarms generated by host system components, such as iLO and VMware alarms associated with a virtual node.

For Acuitas to collect traps for the blade system, the following configuration is required:

- In Acuitas, configure each blade with the blade iLO IP address and the Host IP address for which Acuitas should collect traps.
- On the blade system management system, configure the Acuitas server IP address as an SNMP trap destination.

- In Acuitas, configure the rack, shelf, blade, and Enclosure Onboard Administrator IP address where the virtual node is located.

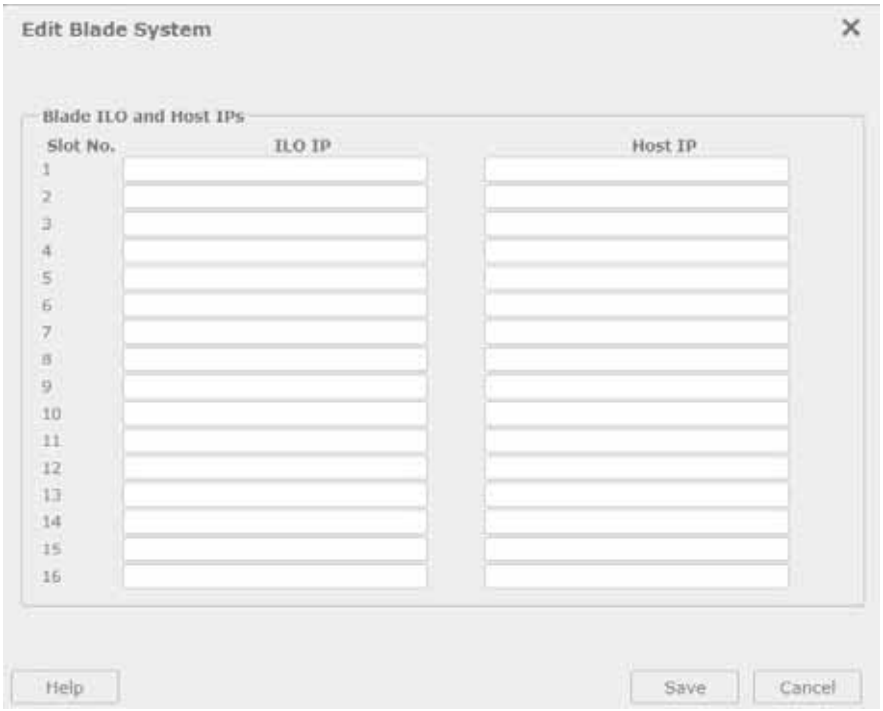
Instructions for these requirements are described in the following topics.

Configure Blades

To configure blades:

1 In Acuitas, right-click the blade system and click **Configure Blades**.

Figure 4-5 Configure Blades Screen



2 For each slot, enter the Blade iLO IP address and the Host IP address to which Acuitas should collect traps.

3 Click **Save**.

Configure the Acuitas Server IP Address as an SNMP Trap Destination

For instructions, see *Configuring SNMP* in the *Mobile Content Cloud Deployment Guide for VMware ESXi*.

Configure the Rack, Shelf, Blade, and IP Address of the Virtual Node

To configure the rack, shelf, blade, and IP address where the virtual node is located:

1 In Acuitas, right-click the virtual node and click **Configuration Navigator**.

2 Expand **Cluster** in the tree.

3 Expand a Cluster ID.

4 Expand **Node**.

5 Click a Node ID.

6 Configure the parameters as follows:

- **Rack** – Enter the physical rack in the blade system where the virtual node is located.
- **Shelf** – Enter the shelf in the blade system where the virtual node is located.
- **Blade** – Enter the blade index where the hardware is hosted, such as the slot number of the blade within the blade system.
- **IP Address** – Enter the Management IP address of the hardware, such as the enclosure Onboard Administrator IP of the blade system.

7 Click the **Save** icon.

Once these configuration requirements are met, you can view alarms generated by blade system components.

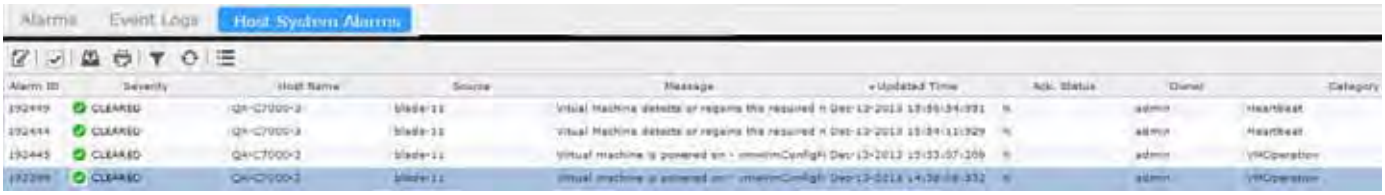
To view host system alarms:

1 Select the object in the tree for which you want to view alarms:

- To view alarms from all nodes in a cluster, select the cluster in the tree.
- To view alarms for a particular node, select the node in the tree.

2 Click the **Host System Alarms** tab.

Figure 4-6 Host System Alarms tab



Alarms are listed with the following information:

- **Alarm ID** – Unique ID of the alarm
- **Severity** – Problem severity
- **Host Name** – Network element reporting the problem
- **Source** – Network element component having the fault
- **Message** – Message/fault description obtained from the network element
- **Date Updated** – Date and time of last update of the alarm
- **Ack. Status** – Indicates whether or not the alarm is acknowledged

- **Owner** – Alarm owner
- **Category** – Alarm category, such as Server Power, VM Operation
- **Date Created** – Date and time when the alarm was raised
- **Date Ack.** – Date and time the alarm was acknowledged, if applicable
- **Cleared Time** – Date and time the alarm was cleared, if applicable
- **Event Type** (network element alarm/status poll/data collection)
- **Remedy** – Problem remedy suggested by the administrator
- **Additional Info** – Lists more information about the alarm
- **NE Alarm SeqNo** – NE Alarm Sequence Number
- **NE Alarm Idx** – NE Alarm Index
- **Trap OID** – Unique identifier for the device alarm type. Is listed as **N/A** for EMS Server alarms. To configure trap OID display length, see Configuring Trap OID Display Length.

Filtering Alarms

Severity Filter

You can filter alarms based on alarm severity.

The alarm filter icons on the toolbar indicate the global alarm counts. They indicate the numbers and severity of all alarms on the network.

Click the alarm filter icon to view alarms of that severity.

Acuitas lists **Alarms Details** for the severity you chose.

Figure 4-7 Filtered Alarms - Critical Severity

Alarm Details

Custom Filter

You can configure a specific Alarm Filter to view alarms based on filter conditions.

For instructions, see Creating Filters.

Quick Filter

You can use the Quick Filter to view alarms based on a specific parameter and value.

For instructions, see Using Quick Filters.

Viewing/Editing Alarm Details

You can view and edit an alarm's details. You can:

- Check the alarm's associated event logs for the detailed history of an alarm, such as how many times the same alarm has been raised.
- Change the owner for the alarm
- Acknowledge the alarm (if you are the alarm owner)
- Annotate the alarm by providing comments

Acuitas saves these changes to maintain a history of changes.

Note: *To modify alarm details, you must have the Fault > Alarms > Modify Alarm Details security group permission. To annotate an alarm, you must have the Fault > Alarms > Annotate Alarm security group permission. For instructions, see Specifying Permissions by Security Group.*

To view/edit alarm details:

1. Click the **Alarms** tab.
2. Use any of the following methods to view/edit an alarm's details:

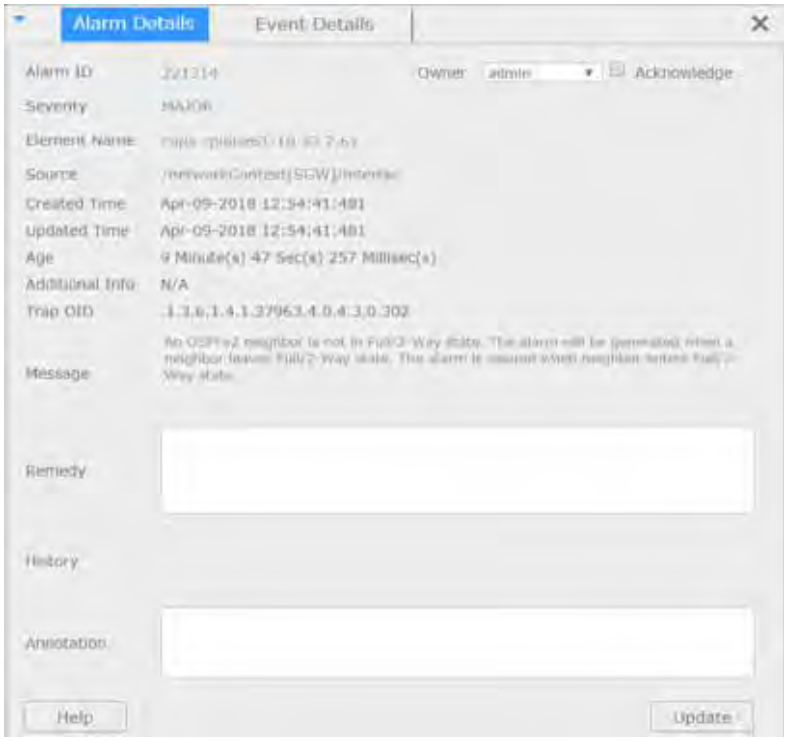
Toolbar: Select the alarm and click the **Alarm Details** icon.

Pop-up menu: Right-click the alarm and click **Alarm Details**.

Or: Double-click the alarm.

Acuitas displays the **Alarm Details** window.

Figure 4-8 Alarm Details Window



3 To edit the alarm, make the necessary changes and click **Update**.

- **Owner** – You can change the field to assign the alarm to a new owner.
- **Acknowledge** – If you are the alarm owner and the alarm has not been cleared, you can mark this checkbox to acknowledge the alarm. By acknowledging an alarm, you notify other Operators that someone has seen the alarm. Such information helps other Operators know what network issues are being addressed.
- **Remedy** – You can enter a remedy
- **Annotation** – You can enter an annotation. (Requires Fault > Alarms > Annotate Alarm security group permission.)

Acuitas updates the alarm information accordingly, including the **Owner**, **Ack. Status**, **Ack. Time**, **Remedy**, and/or **Annotation** fields.

4 Click the **Event Details** tab to view the Events of the alarm. By default, this tab lists event logs raised 15 minutes before and after the occurrence of each alarm log. It can help to debug the root cause of the alarm.

Assigning Alarm Owners

If you have sufficient privileges, you can assign an alarm. By assigning an alarm, you notify the Operator of the network issue to be addressed.

Note: *To assign an alarm owner, you must have the Fault > Alarms > Assign Owner security group permission. For instructions, see Specifying Permissions by Security Group.*

To assign an alarm:

1. Click the **Alarms** tab.
2. Use any of the following methods to assign an alarm:

   Toolbar: Select the alarm and click the **Assign** icon.

   Pop-up menu: Right-click the alarm and click **Assign**.
3. In the **Assign To** field, select the required owner.
4. Click **Assign**.

   Acuitas updates the **Owner** field accordingly.

Acknowledging Alarms

If you are the alarm owner, you can acknowledge an alarm. By acknowledging an alarm, you notify other Operators that someone has seen the alarm. Such information helps other Operators know what network issues are being addressed.

Note: *You cannot acknowledge an alarm that is cleared.*

Note: *To acknowledge an alarm, you must have the Fault > Alarms > Acknowledge Alarms security group permission. For instructions, see Specifying Permissions by Security Group.*

To acknowledge an alarm:

1. Click the **Alarms** tab.
2. Use any of the following methods to acknowledge an alarm:

   Toolbar: Select the alarm and click the **Acknowledge** icon.

Pop-up menu: Right-click the alarm and click **Acknowledge**.

Acuitas updates the alarm information accordingly, including the **Ack. Status** and **Ack. Time** fields.

Clearing Alarms

If you have sufficient privileges, you can clear alarms that have been acknowledged:

- When you clear an alarm generated by the Acuitas server, it is automatically cleared.
- When you clear an NE alarm, Acuitas forwards the clear request to the network element. If the alarm is cleared by network element, Acuitas receives the clear trap that clears the alarm.
- Once an alarm is cleared, the clear event is added to the event log and the alarm is updated to show the cleared state.

Note: *To clear an alarm, you must have the Fault > Alarms > Clear Alarms security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To clear an alarm:

1. Click the **Alarms** tab.
2. Use any of the following methods to clear an alarm:

   Toolbar: Select the alarm and click the **Clear** icon.

   Pop-up menu: Right-click the alarm and click **Clear**.
3. At the confirmation prompt, click **OK**.

   In the **Annotation** window, enter the reason for clearing the alarm (required). This annotation is sent to the MCC for inclusion in the actual clear trap.
4. Click **Save**.

   Acuitas updates the alarm **Severity** to Cleared and the severity color to green.

   Acuitas saves any annotation messages to maintain a history of changes. They are listed in the History section of the **Alarm Details** window.

   Use any of the following methods to access the **Alarm Details** window:

   Toolbar: Select the alarm and click the **Alarm Details** icon.

   Pop-up menu: Right-click the alarm and click **Alarm Details**.

Or: Double-click the alarm.

Showing/Hiding Cleared Alarms

You can show or hide all the cleared alarms.

To hide cleared alarms:

1. Click the **Alarms** tab.
2. Click the **Hide Cleared Alarms** icon.

   Acuitas updates the list of alarms (Cleared alarms are no longer shown).

To show cleared alarms:

1. Click the **Alarms** tab.
2. Click the **Show Cleared Alarms** icon.

   Acuitas updates the list of alarms (Cleared alarms are shown).

Purging Cleared Alarms

You can purge all the cleared alarms and any event logs associated with the alarms. The purge action removes the alarms and associated events from database tables and archives them on the Acuitas server in the following directory:

/opt/Affirmed/NMS/server/ems/archive

Note: *To purge alarms, you must have the Fault > Alarms > Purge Alarms security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To purge cleared alarms:

1. Click the **Alarms** tab.
2. Click the **Purge Now** icon.

   Acuitas updates the list of alarms (Cleared alarms are no longer shown).

   To purge event logs that *are not* associated with alarms, purge the event logs. For instructions, see Purging Event Logs.

Deleting Alarms

If you have sufficient privileges, you can delete alarms generated by the Acuitas server that have been cleared. You cannot delete alarms generated by a network element until it has been removed from the network.

Note: *To delete an alarm, you must have the Fault > Alarms > Delete Alarms security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To delete an alarm:

1. Click the **Alarms** tab.
2. Use any of the following methods to delete an alarm:

   Toolbar: Select the alarm and click the **Delete** icon.

   Pop-up menu: Right-click the alarm and click **Delete**.
3. At the confirmation prompt, click **OK**.

   Acuitas updates the list of alarms (Deleted alarms are no longer shown).

Forwarding Alarms

You can forward alarms to a trap listener or to an e-mail listener.

For more information about the format of traps sent to northbound interfaces, such as to OSS systems, see Appendix A, Interfacing with Northbound Interfaces.

Note: *To forward an alarm, you must have the Fault > Alarms > Forward Alarms security group permission. For instructions, see Specifying Permissions by Security Group.*

To forward an alarm:

1. Click the **Alarms** tab.
2. Use any of the following methods to forward an alarm:

   Toolbar: Select the alarm and click the **Alarm Forwarding** icon.

   Pop-up menu: Right-click the alarm and click **Alarm Forwarding**.

   Acuitas displays the **Alarm Forwarding** window.
3. To forward the alarm to a trap listener:
   a. Click the **Trap** tab.
   b. Select a trap listener from the list.

Note: *To add a trap listener, click **Trap Config**. See Configuring SNMP Alarm Forwarding for instructions.*

To forward the alarm to an e-mail listener:

a. Click the **Email** tab.
b. Select an e-mail listener from the list.

Note: *To add an e-mail listener, click **Email Config**. See Configuring Alarm E-mail Notification for instructions.*

---

4. Click **Send**.

Streaming Alarms to syslog

You can configure Acuitas to stream alarms to a remote syslog server.

The syslog file is written in /var/log/affirmed.log.

To configure syslog on Acuitas:

1. Shutdown Acuitas server:

```
cd /opt/Affirmed/NMS/bin
./emsstop
```

2. Edit the following file:

   /opt/Affirmed/NMS/server/ems/conf/ems-jboss-standalone.xml

3. Make the following changes.

   a. Add the following custom-handler under xml path:

```
"/server/profile/ <subsystem
xmlns="urn:jboss:domain:logging:2.0">" just before handler for
<size-rotating-file-handler name="SERVER_FILE">
       <custom-handler name="SYSLOG"
class="org.apache.log4j.net.SyslogAppender"
module="org.apache.log4j">
          <level name="INFO"/>
          <formatter>
             <pattern-formatter pattern="%d %-5p [%c] %x - %m%n"/>
          </formatter>
          <properties>
             <property name="Facility" value="LOCAL1"/>
             <property name="SyslogHost" value="localhost:5140"/>
          </properties>
        </custom-handler>
```

   b. Add the following logger:

```
"/server/profile/ <subsystem
xmlns="urn:jboss:domain:logging:2.0">" just after logger using
<handler name="SERVER_FILE"/> in <logger category="org.jboss"
use-parent-handlers="false">
       <logger category="syslogOutput"
use-parent-handlers="false">
          <level name="INFO"/>
          <handlers>
             <handler name="SYSLOG"/>
          </handlers>
       </logger>
```

   c. The syslogOutput includes only audit trail and alarms. If you need to stream any output in vm.log or other Acuitas log files to syslog, add the SYSLOG handler to those loggers.

4 Save the file.

5 Start the Acuitas server:

```
cd /opt/Affirmed/NMS/bin
./starttems.sh
```

Using rsyslog Server

This section describes how to install and use the rsyslog server.

To install and configure rsyslog on Acuitas:

1 Obtain the rsyslog.repo file available at the following web site and place it in the /etc/yum.repos.d/ directory:

http://rpms.adiscon.com

2 Issue the following command to add the package:

```
yum update rsyslog
Loaded plugins: product-id, security, subscription-manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager to register.
rsyslog_v5 | 2.5 kB     00:00
rsyslog_v5/primary_db |  24 kB     00:00
Setting up Update Process
Package(s) rsyslog available, but not installed.
No Packages marked for Update
```

3 Issue the following command to install the package:

```
yum install rsyslog
```

4 When the installation completes, edit the following file:

/etc/rsyslog.conf

5 Uncomment the following section to receive UPD syslog messages. Set the UDPServerRun parameter to the appropriate port. **Note:** The firewall must allow UDP on this port.

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 5140
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="5140")
```

6 Add the following line to print the sender IP Address in the log. **Note:** Enter the entire string on a single line.

```
#### GLOBAL DIRECTIVES ####

$template EmsFileFormat,"%TIMESTAMP% [%FROMHOST%] %syslogtag%%msg:::
sp-if-no-1st-sp%%msg:::drop-last-lf%\n"
```

7 Add the following line to log into the desired log file using the template specified in step 6. You can specify any path and filename:

```
LOCAL1.*    /var/log/affirmed.log;EmsFileFormat
```

8 Save the rsyslog,conf file.

9 Issue the following command to restart the rsyslog service:

```
service rsyslog restart

Shutting down system logger:       [  OK  ]

Starting system logger:            [  OK  ]
```

Viewing Alarm Statistics

Acuitas provides pie charts of the alarm statistics for a specified time period. The charts show percentage of alarms by:

- Severity
- Acknowledged/Unacknowledged
- Owner
- Network Element

Note: *To view alarm statistics, you must have the Fault > Alarms > View Alarms security group permission. For instructions, see Specifying Permissions by Security Group.*

To view alarm statistics:

1 Click the **Alarms** tab.

2 Click the **Alarm Stats** icon.

Acuitas displays the pie charts of alarm statistics.

3 If desired, change the data time period.

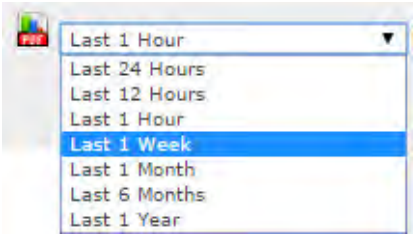
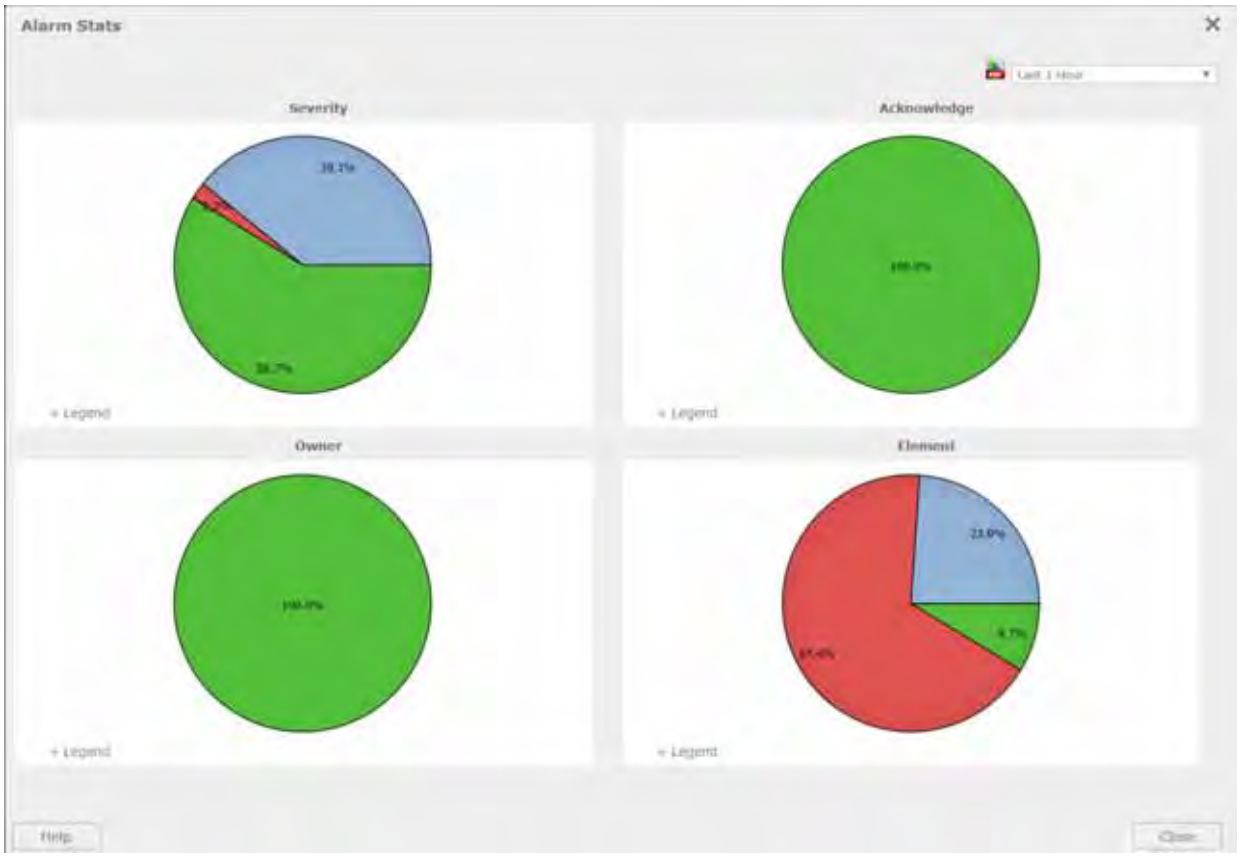
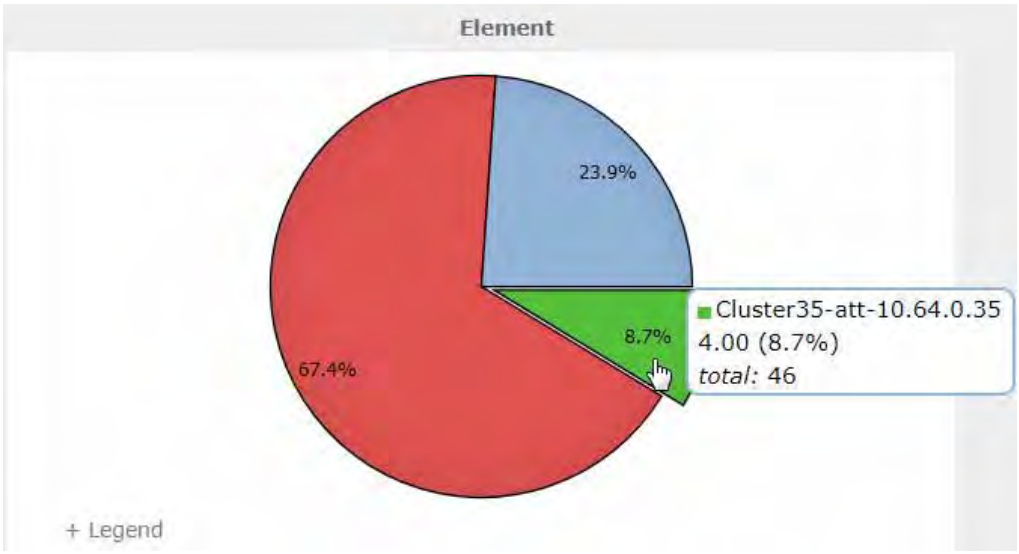


Figure 4-9 Alarm Stats



4 To view the chart legend, click the **Legends** icon. + Legends If necessary, use the scrollbar to display the legend.

5 To view a single point in the graph, point the cursor at a point. Acuitas opens a pop-up window that lists the data for that point.



6 To export the charts, click the **Export as PDF** icon.

Acuitas displays the **Download Files** window.

7 Right-click **Download PDF File** and select **Save Link As**.

8 Specify where you want the file saved and click **Save**.

To close the window, click the **Close** icon.

Exporting Alarms

You can export alarms to a CSV/PDF/XLS/XML/HTML file.

Note: *To export alarms, you must have the Fault > Alarms > Export Alarms security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To export alarms:

1. Click the **Alarms** tab.
2. If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.
3. Select the record(s) to be exported. To select multiple records, Shift-click or Control-click the records in the list. To export the Whole Data or Current View, do not select any records.
4. Click the **Export Alarms** icon.

   Acuitas displays the Configure Export Parameters window.
5. Configure the parameters as follows:
   - **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
   - **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
   - **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
   - **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.
6. Click **Apply**.

   Acuitas displays the **Download Files** window.
7. Click **Download Exported File**.
8. From the **Download File**s window, click **Close**.

Printing Alarms

You can print alarms.

Note: *To print alarms, you must have the Fault > Alarms > Print Alarms security group permission. For instructions, see Specifying Permissions by Security Group.*

To print alarms:

1. Click the **Alarms** tab.
2. From the **Alarms** tab, click the **Print Alarms** icon.

   Acuitas displays the **Print Preview** window.
3. Click **Print**.
4. Select the desired printer.
5. Click **Print**.

Generating an Alarm Report

Note: *To generate an alarm report, you must have the Fault > Alarms > Generate Alarm Report security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To generate an alarm report:

1. Click the **Settings** icon on the toolbar and select **Fault => Alarms => Generate Reports**.

   Acuitas displays the **Alarm Report Generator**.

2. To generate specific conditions for the report:

   a. Click the **New Filter** icon.

   b. Enter the Filter Name and click **Add**.

   c. Select the filter and click the **Add Condition** icon.

   d. Complete the Conditions fields by selecting appropriate values for **Parameter**, **Operator**, **Value**, and **Condition**.

   e. Click **Apply**.

3. If the report needs a combination of AND and OR conditions to achieve the desired result:

   a. Click the **Create AND group** icon (or **Create OR Group** icon).

   b. Click the **Add Condition** icon and complete the Conditions for the group.

   c. Click **Apply**.

4. Click **Download Report** to download the report.

   Acuitas displays the **Download Alarm Report File** window.

5. Click **Download Exported File**.

6. From the **Download Alarm Report File** window, click **Close**.

7. From the **Alarm Report Generator** window, click **Cancel**.

Configuring Alarm Purge Settings

Acuitas periodically purges cleared alarms and any event logs associated with the alarms. You can specify the following purge settings:

- **Maximum Number of Alarms to Retain**: When the number of cleared alarms increases beyond a specified limit (default 10,000 alarms), Acuitas purges alarms every 30 minutes.
- **Purge Alarms Older Than**: Acuitas purges cleared alarms older than a specified number of days (default 10 days).

Because logs are archived periodically, Acuitas does not archive the cleared alarms when they are purged.

In addition to these settings, you can manually trigger alarm purging. For details, see Purging Cleared Alarms.

Note: *To configure alarm purge settings, you must have the Fault > Alarms > Configure Alarm Purge Interval security group permission. For instructions, see Specifying Permissions by Security Group.*

To specify purge settings:

1. Click the **Settings** icon on the toolbar and select **Fault => Alarms => Purge Settings**.
2. To purge alarms based on the maximum number to retain, mark the **Maximum no. of Alarms to retain** checkbox and specify the maximum number.

   To purge alarms based on age, mark the **Purge alarms older than** checkbox and specify the number of days.
3. Click **OK**.

To purge event logs that *are not* associated with alarms, purge the event logs. For instructions, see Purging Event Logs.

Configuring SNMP Alarm Forwarding

Acuitas supports forwarding alarms to other specific management systems as either SNMP TRAPs or as SNMP INFORMs.

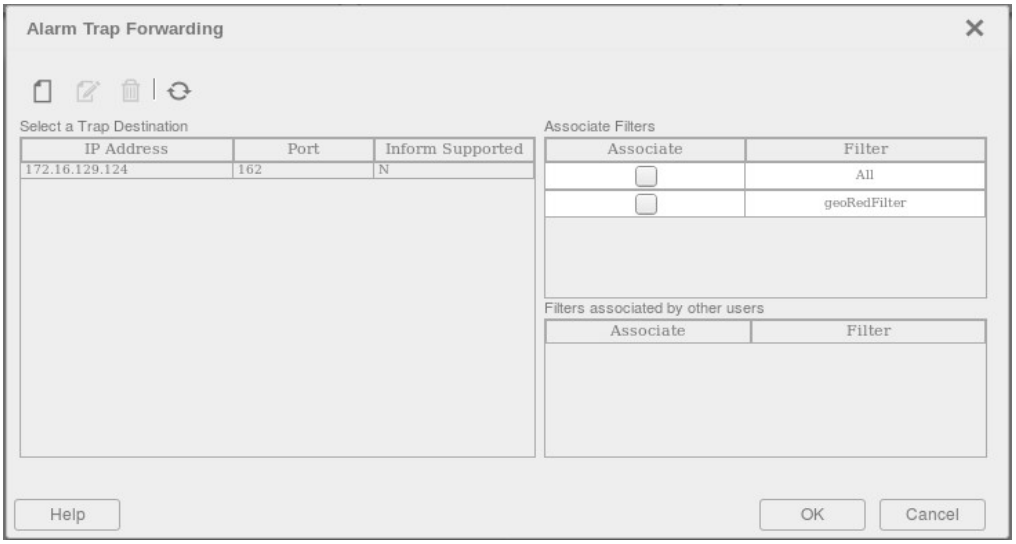
Note: *To configure SNMP alarm forwarding, you must have the Fault > Alarms > Manage > Manage Alarm Trap Forwarding security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure SNMP alarm forwarding:

1 Click the **Settings** icon on the toolbar and select **Fault => Manage => Trap Forwarding**.

Acuitas displays the **Alarm Trap Forwarding** window. The left pane lists the destination addresses and their ports for which the alarm needs to be sent and lists whether the destination supports INFORMs. The right pane lists the alarm filters.

Figure 4-10 Alarm Trap Forwarding



Note: *The Inform Supported column is shown only when the global flag inform.enable=true is set in the NorthboundTrapConfig.properties file. See NorthboundTrapConfig.properties File.*

---

2 To add a SNMP Listener, click the **Add** icon. (Requires Fault > Alarms > Manage > Manage Alarm Trap Forwarding > Add SNMP Publisher security group permission.)

Acuitas displays the **Create New SNMP Listener** window.

Figure 4-11 Create New SNMP Listener

a Specify the **IP Version**, **IP Address**, and **Port**.

b To forward alarms as SNMP INFORMs, mark the **Inform Supported** checkbox.

Note: *The Inform Supported field is shown only when the global flag inform.enable=true is set in the NorthboundTrapConfig.properties file. See NorthboundTrapConfig.properties File.*

---

c Specify the **Trap Forward Type** – SNMPv2 or SNMPv3.

If you specify SNMPv3, specify the following parameters:

- **User Name** – Security name
- **Authentication Protocol** – MD5 or SHA
- **Authentication Password** – Secret key
- **Privacy Protocol** – DES or AES
- **Privacy Password** – Privacy key
- **Security Level** – noAuthNoPriv, authNoPriv, authPriv

d Click **OK** to commit the data. The newly created SNMP Listener is listed in the Alarm Trap Forwarding window. Only one Trap Destination at a time can have the **Inform Supported** checkbox marked.

Figure 4-12 Alarm Trap Forwarding

3 To associate the trap listener with alarm filters, select the Trap Destination in the left pane and mark the required check boxes in the right pane. (Requires Fault > Alarms > Manage > Manage Alarm Trap Forwarding > Assign Filter for SNMP Publisher security group permission.)

4 Click **OK** to associate the trap listener with alarm filters.

NorthboundTrapConfig.properties File

The NorthboundTrapConfig.properties file contains configurable attributes to control handling of SNMP INFORMs. If you change any property value, restart the Acuitas server for the new value to take effect.

NorthboundTrapConfig.properties is in the directory:

/opt/Affirmed/NMS/server/ems/resources

The configurable attributes are as follows:

inform.enable=true

Global flag that enables INFORM support, including:

- Sending INFORM heartbeat to northbound systems
- Sending SNMP INFORMs
- Configuring INFORM for trap destination in Acuitas

inform.timeout=10000

SNMP INFORM timeout. Default:10 seconds.

inform.noOfRetries=3

SNMP INFORM number of retries. Default: 3.

inform.queueSize=500

SNMP INFORM queue size. The maximum limit of queue size is based on the JVM Heap Memory (any value configured greater than this value is overridden).

heartBeat.isSupported=true

Global flag that enables heartbeat mechanism that checks the availability of both Acuitas and the northbound system.

heartBeat.timeInterval=30000

Heartbeat polling time interval to update server cache used for INFORM queue processing Default: 30 seconds

NMSSNMPAgent.properties File

The NorthboundTrapConfig.properties file contains configurable attributes to control SNMP Agent details.

NMSSNMPAgent.properties is in the directory:

/opt/Affirmed/NMS/server/ems/resources

The SNMP Agent port can be configured in the following field in the NMSSNMPAgent.properties file.

SNMP_AGENT_UDPPORT=1161

Default: 1161

Make sure that the port is open for external northbound access in the firewall configuration.

Configuring Alarm E-mail Notification

If an alarm requires generation of an e-mail alert, you can configure an e-mail server for alarm e-mail notification.

Acuitas can be configured to either send all the alarms or alarms that match pre-defined match criteria. To be notified for only specific cases, first create an alarm filter with the match criteria and use it for configuring the e-mail notification. For example, create a filter with the match criteria of owner=<user ID> to forward all the alarms assigned to that user's e-mail. For instructions on creating an alarm filter, see Filter Management.

The following alarm details are sent as part of the e-mail sent to the user:

- Alarm ID
- NE
- Source (shelf/slot/card/port)
- Severity
- Alarm Raised by (generated by NE/by Acuitas)
- Created time
- Last updated time
- Owner assigned
- Acknowledgment status
- Acknowledged time (if acknowledged)
- Alarm description
- Remedy (If available)

Note: *To configure alarm e-mail forwarding, you must have the Fault > Alarms > Manage > Manage Alarm Email Forwarding security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure E-mail Notification:

1 Click the **Settings** icon on the toolbar and select **Fault => Manage => Email Notification**.

2 If the mail server is not already configured:

   a At the confirmation prompt asking if you want to configure the Mail server, click **OK**.

   b Configure the Mail Server details:

      – **Primary SMTP Host Name** – Host name of the Simple Mail Transfer Protocol (SMTP) server.

      – **Secondary SMTP Host Name** – Another host name of the SMTP server, used in case of any failure in the Primary SMTP Host name.

      – **SMTP Port** – Port ID for the SMTP.

      – **SMTP User** – User name of the SMTP server.

      – **SMTP Password** – Password of the SMTP server.

      – **Confirm Password** – Confirmation of the entered password.

      – **Sender Name** – User name used for sending e-mail by the Acuitas server.

      – **Sender Mail ID** – Mail ID used for sending e-mail by the Acuitas server.

   c Click **Save**.

3 To add an E-mail Listener, click the **Add** icon. (Requires Fault > Alarms > Manage > Manage Alarm Email Forwarding > Add Email Publisher security group permission.)

   To modify an existing E-mail Listener, select the E-mail Listener you want to modify and click the **Edit** icon. (Requires Fault > Alarms > Manage > Manage Alarm Email Forwarding > Modify Email Publisher security group permission.)

   Acuitas displays the **Add** (or **Modify**) **Email Listener** window.

   a Specify the **Email address** and **Details**.

   b Click **OK** to commit the data. The newly created Email Recipient is listed in the Alarm Email Notification window.

4 To associate the Email Recipient with alarm filters, select the Email Recipient in the left pane.

5 To select the filters that need to be associated with the Email Recipient, select the required check boxes in the right pane. (Requires Fault > Alarms > Manage > Manage Alarm Email Forwarding > Assign Filter for Email Publisher security group permission.)

6 Click **OK** to associate the Email Recipient with alarm filters.

Events

Viewing Event Logs

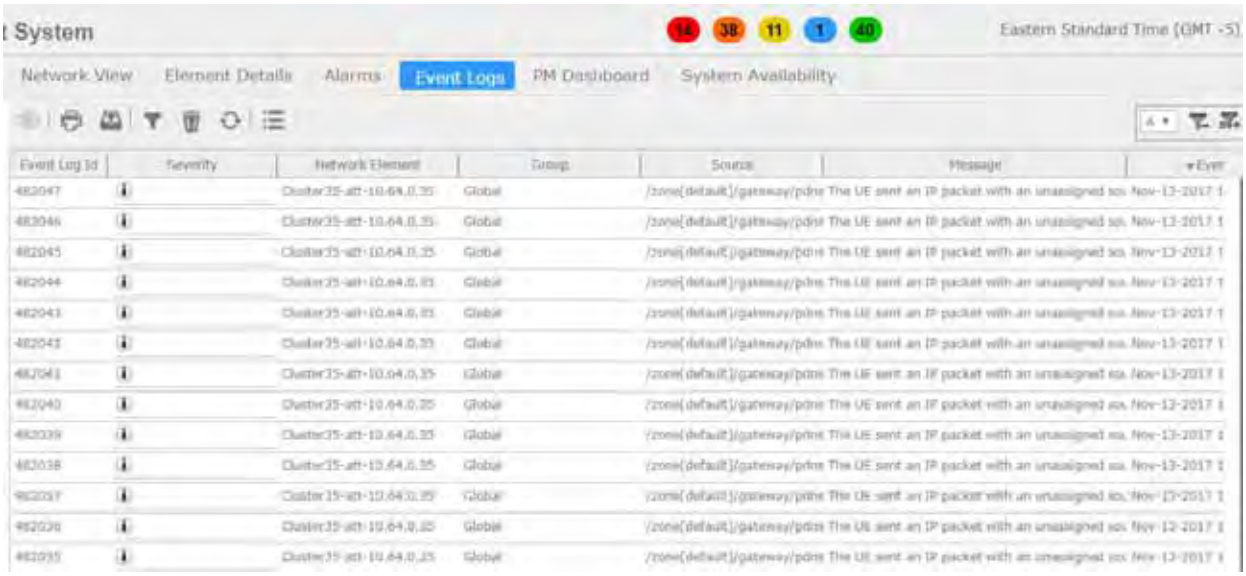
When a trap is generated as a consequence of a fault, by default an Event Log is generated, which is then consolidated to an alarm. Event Logs can be viewed, printed, exported and purged.

Note: *To view event logs, you must have the Fault > Logs > View Logs security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To view Event Logs:

1. Select the object in the tree for which you want to view events:
   - To view events from all NEs, select **Global** in the tree.
   - To view events for a particular NE, select the NE in the tree.
2. Click the **Event Logs** tab.

Figure 4-13 Event Logs tab



Events are listed with the following information:

- **Event Log ID** – Unique across all the network elements
- **Severity** - Informational for events and specific severity for alarms generated by the NE and Acuitas
- **Network Element**
- **Group** – Group having the event
- **Source** – Source having the event
- **Message** – Message/fault description obtained from the network element
- **Event Time** – Date and time of the event
- **Age** – Numbers of days, hours, minutes, seconds, and milliseconds since the event occurred
- **Category** – Event category
- **Event Type** – Category of event, such as data collection based
- **Remedy** – Remedy for the event, if available
- **Additional Info** – Lists more information about the event
- **Trap OID** – Unique identifier for each device alarm type.Is listed as **N/A** for EMS Server events. To configure trap OID display length, see Configuring Trap OID Display Length.

In the case of a large number of log entries, use the page navigational bar at the bottom of the window to page through the entries.

Viewing Event Details

You can view an event's details.

To view event details:

1. Click the **Event Logs** tab.
2. Use any of the following methods to view an event's details:

   Toolbar: Select the event and click the **View** icon.

   Pop-up menu: Right-click the event and click **View**.

   Acuitas displays the **Event Logs View** window.
3. Click **Close** to close the window.

Printing Event Logs

You can print event logs.

Note: *To print event logs, you must have the Fault > Logs > Print Logs security group permission. For instructions, see Specifying Permissions by Security Group.*

To print event logs:

1. Click the **Event Logs** tab.
2. From the **Event Log** tab, click the **Print Event Log** icon. .

   Acuitas displays the **Print Preview** window.
3. Click **Print**.
4. Select the desired printer.
5. Click **Print**.

Exporting Event Logs

You can export event logs to a CSV/PDF/XLS/XML/HTML file.

Note: *To export event logs, you must have the Fault > Logs > Export Logs security group permission. For instructions, see Specifying Permissions by Security Group.*

To export event logs:

1. Click the **Event Logs** tab.
2. If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.
3. Select the record(s) to be exported. To select multiple records, Shift-click or Control-click the records in the list. To export the Whole Data or Current View, do not select any records.
4. Click the **Export Event Logs** icon.

   Acuitas displays the **Configure Export Parameters** window.
5. Configure the parameters as follows:
   - **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
   - **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
   - **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
   - **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.
6. Click **Apply**.

   Acuitas displays the **Download Files** window.
7. Click **Download Exported File**.
8. From the **Download Files** window, click **Close**.

Purging Event Logs

Acuitas supports an archive and purge mechanism whereby administrators can configure the Purge Interval for purging event logs that *are not* associated with alarms (such as informational event). Acuitas archives the logs to be purged before purging them from the database.

By default, event logs older than 30 days or event logs exceeding 250,000 logs are purged.

You can specify the following purge settings:

- **Maximum Number of Events to Retain**: When the number of events increases beyond a specified limit (default 40,000 events), Acuitas purges logs.

  Note: This purge setting applies only to event logs that *are not* associated with alarms. Keep in mind that the list of event logs can greatly exceed 40,000 logs because the list includes those that are associated with alarms and those that are not.

- **Purge Event Older Than**: Acuitas can purge events older than a specified number of days.

In addition to these settings, you can manually trigger event purging.

For details, see Configuring Purge Interval for Event Logs.

To purge event logs that are associated with cleared alarms, purge alarms. For instructions, see Purging Cleared Alarms.

Note: *To purge event logs, you must have the Fault > Logs > Purge Logs security group permission. For instructions, see Specifying Permissions by Security Group.*

Configuring Purge Interval for Event Logs

Note: *To configure the purge interval for event logs, you must have the Fault > Logs > Configure Log Purge Interval security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure purge interval:

1 Click the **Settings** icon on the toolbar and selectt **Fault => Logs =>**

Purge Settings.

2 To purge logs based on the maximum number to retain, mark the **Maximum no. of logs to retain** checkbox and specify the maximum number.

To purge logs based on age, mark the **Purge logs older than** checkbox and specify the number of days.

3 Click **OK**.

Purging a Specific Log

To purge a specific event log:

1 Click the **Event Logs** tab.

2 Select the event to be purged.

3 Click the **Purge Now** icon.

Purging All Event Logs

To purge all event logs:

1 Click the **Settings** icon on the toolbar and select **Fault => Logs =>**

Purge Now.

2 At the confirmation prompt, click **OK**.

Chapter 5

Performance

Acuitas contains Performance Management tools that allow you to recognize current or impending performance issues that can cause problems for network users. Activities include the monitoring and maintenance of acceptable network performance, and the collection and analysis of statistics critical to network performance.

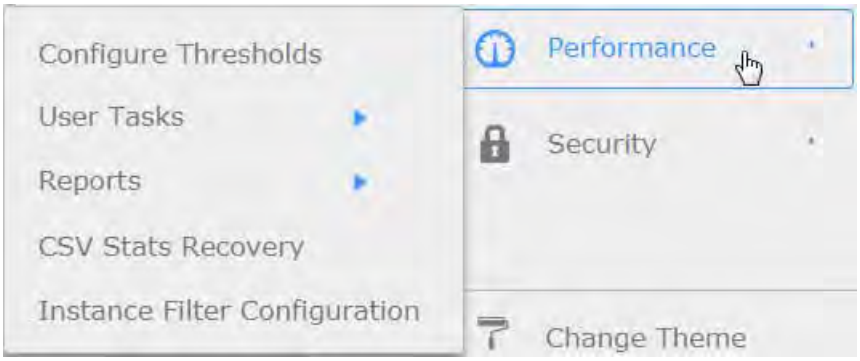
Note: *For performance information for the MCC MME, see the Affirmed Networks MCC MME Performance Management Reference Guide.*

The following topics describe how to access and use the Performance applications:

- Enabling/Disabling Performance Collections
- Performance Reports
- Thresholds
- User Tasks Templates
- Users Tasks Scheduler
- CSV Stats Recovery

To access Performance management applications, select the applicable option from the **Settings** icon on the toolbar.

Figure 5-1 Accessing Performance Applications



In addition to the Performance management applications, Acuitas contains an application to view Key Performance Indicators (KPIs) collected during the previous 24 hours (default time period). For details, see Viewing Key Performance Indicators.

Exporting Performance Management Data

Acuitas supports the following methods for exporting Performance Management data:

- Raw Performance Management data:
  - Acuitas periodically exports Performance Management data to comma-separated values (CSV) files on the Acuitas server. For details, see Exported Performance Management Data.
  - You can configure Performance Management reports to be exported to CSV files. For details, see Configuring Export Reports.
  - You can export a historical Performance Management report as textual data or graphical data in various formats, including .csv, .pdf, .xml, .xls, .html. For details, see Exporting Historical Statistics Reports.
- KPI data:
  - Acuitas periodically exports KPIs to comma-separated values (CSV) files on the Acuitas server. For details, see Exported Performance Management Data.
  - You can export KPIs as a daily report. For details, see Configuring the Dashboard.
  - You can export a KPI report as textual data or graphical data in a .pdf file. For details, see Exporting KPI Data from the Dashboard.

Enabling/Disabling Performance Collections

You can enable/disable performance collections using the Task Scheduler.

Note: *To enable/disable a performance collection, you must have the Performance > User Tasks > Task Schedule > Start/Stop Task Schedule security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To enable/disable a performance collection:

1 Click the **Settings** icon on the toolbar and select **Performance => User Tasks => Schedule**.

Acuitas displays the **Task Scheduler**, listing performance management collections and other scheduled data collections.

In the **Task Scheduler**, the MCC_PM_COLLECTION schedule is the performance stats collection task.

2 Use any of the following methods to enable a performance management collection:

Toolbar: Select the performance management collection and click the **Enable Schedule** icon.

Pop-up menu: Right-click the performance management collection and select **Enable Schedule**.

Use any of the following methods to disable a performance management collection:

Toolbar: Select the performance management collection and click the **Disable Schedule** icon.

Pop-up menu: Right-click the performance management collection and select **Disable Schedule**.

3 At the confirmation prompt, click **OK**.

The Admin Status of the performance management collection changes to Enabled or Disabled.

Performance Reports

Acuitas provides reports on:

- Historical – Report on the data collected for a specified period. It is a view of the historical data for the performance statistic attributes configured in the data collection tasks for devices.
- Real Time – Live data collected report. It is a graphical view of the current data for the performance statistic attributes configured as a part of the data collection task.
- Outage Report – Report on the outage of network elements.

For a list of performance statistics, see *Acuitas Performance Statistics*.

Configuring Data Type and Unit Conversion at the Global Level

The Administrator can configure the statistic data type at the global level. Acuitas applies the configured data type to Historical Reports and KPIs (displayed in Dashboard charts):

- Delta Value — Statistic values are plotted based on the following formula:

  Delta value = current counter value - previous counter value

- Rate Value — Statistic values are plotted based on the following formula:

  Rate value = Delta value / collection time interval in seconds

  By default, the Rate Value is applied.

The Administrator can configure the unit conversion at the global level. Acuitas applies the configured unit conversion when formulating derived metrics KPIs (displayed in Dashboard charts):

- Base-2
- Base-10

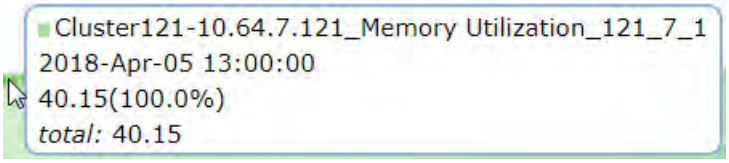
Understanding Delta Value and Rate Value Effects on Charts

The decision to display charts as Delta Value or Rate Value depends on whether you are interested in *summation* values or *average* values in a collection period:

- Delta value for Global Statistic sets each data point to represent the summation of the collected values in that collection period.

- Rate value for Global Statistic sets each data point to represent the average of the collected values in that collection period.

In the chart, collection time interval plays a major role in the charted results. To determine the collection time interval for the chart, point the cursor at a particular data point. Acuitas opens a pop-up window that lists the node name, timestamp, and value for that data point.



Point the cursor at an adjacent data point to see its timestamp.

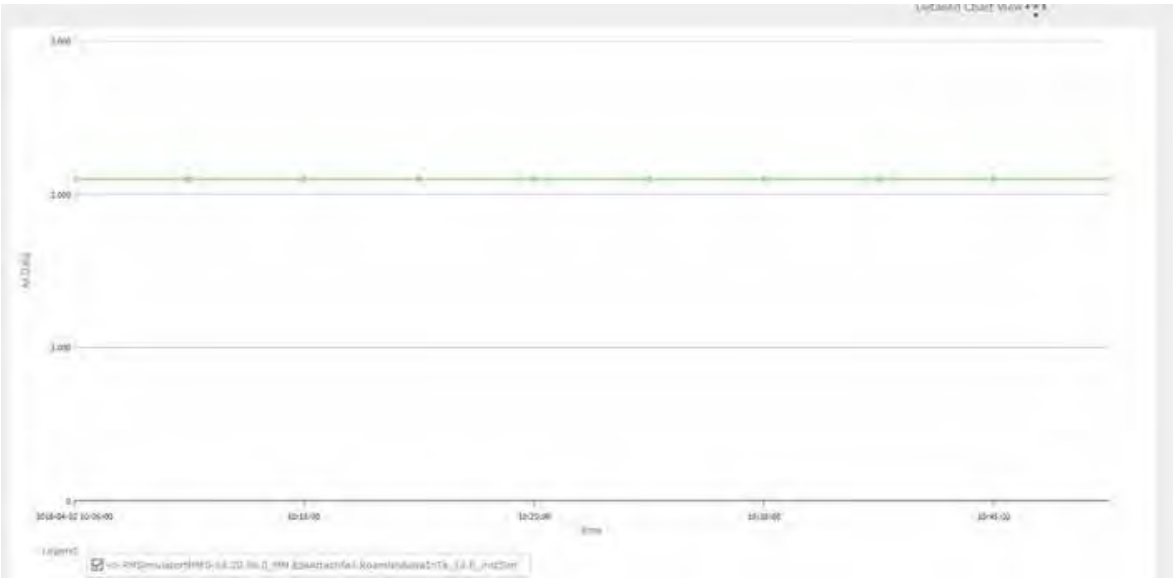
The collection time interval is the ending timestamp minus the beginning timestamp.

The following examples demonstrate the difference between Delta and Rate value using the following data. Acuitas collects data from the node every 5 minutes. Data is collected between 10:00 to 11:00 am.

Time of Collection	Collected Value
10:00	2100
10:05	2100
10:10	2100
10:15	2100
10:20	2100
10:25	2100
10:30	2100
10:35	2100
10:40	2100
10:45	2100
10:50	2100
10:55	2100

In a **Delta** chart plotting 1 hour of data, each data point represents 5 minutes of data. In this example, each data point shows the value 2100 collected from node.

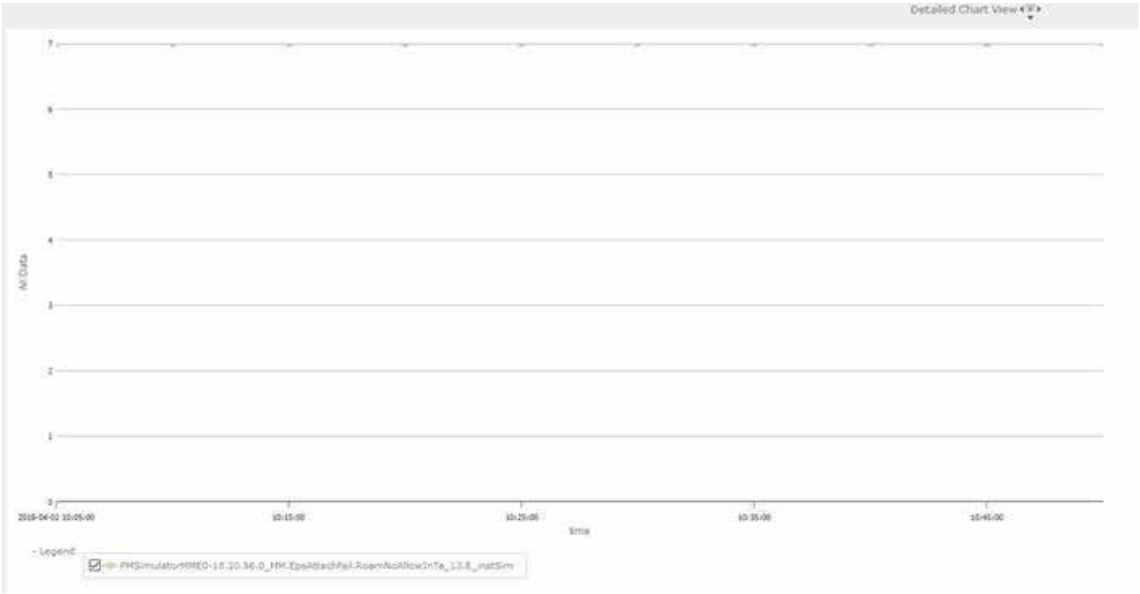
Figure 5-2 Delta Chart with Collection Time Period 1 Hour



In the **Rate** chart plotting 1 hour of data, each data point represents Delta value / collection time interval in seconds or:

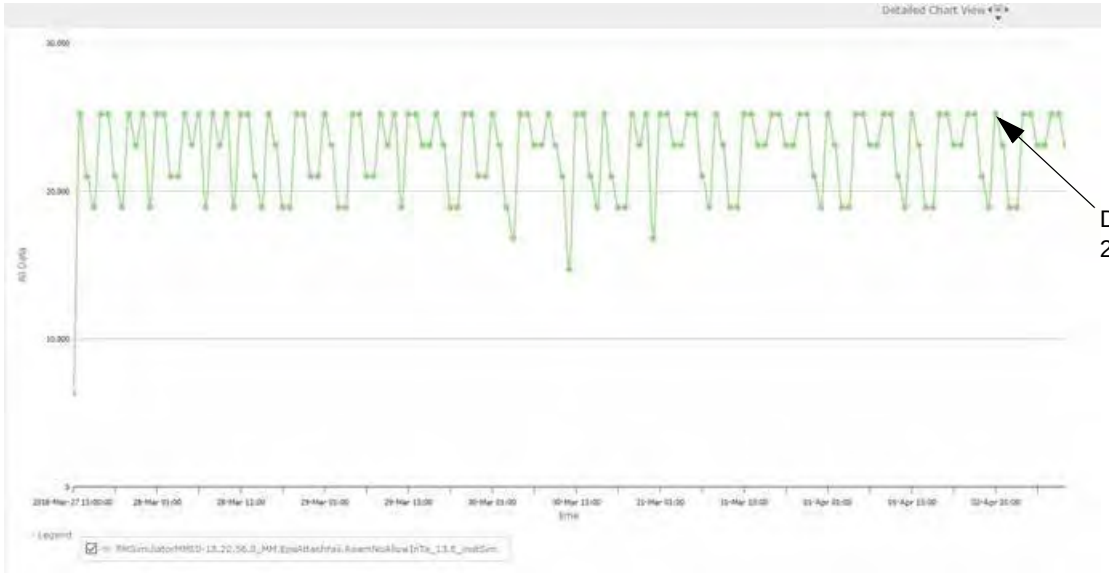
(2100 / 300 seconds) = 7

Figure 5-3 Rate Chart with Collection Time Period 1 Hour



In a **Delta** chart plotting 7 days of data, each data point represents 1 hour of data. At 10:00 on April 2, the Delta value is 25200, which is the summation of collected values from 10:00 to 10:55.

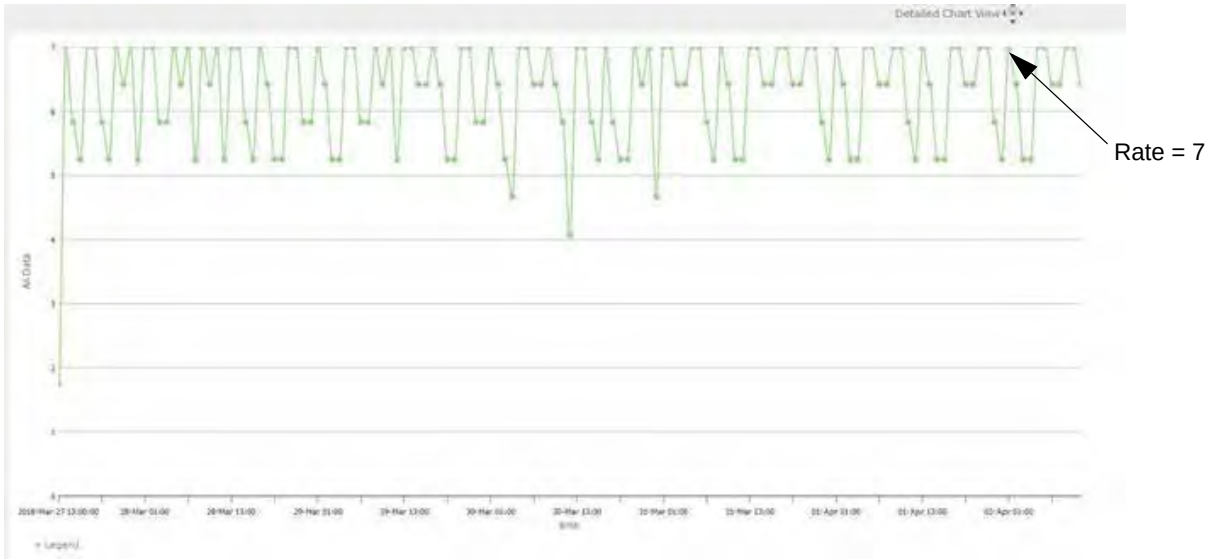
Figure 5-4 Delta Chart with Collection Time Period 7 Days



In a **Rate** chart plotting 7 days of data, each data point represents 1 hour of data. At 10:00 on April 2, the Rate value is the Delta value / collection time interval in seconds or:

(the summation of collected values from 10:00 to 10:55 / 3600 seconds) = 7

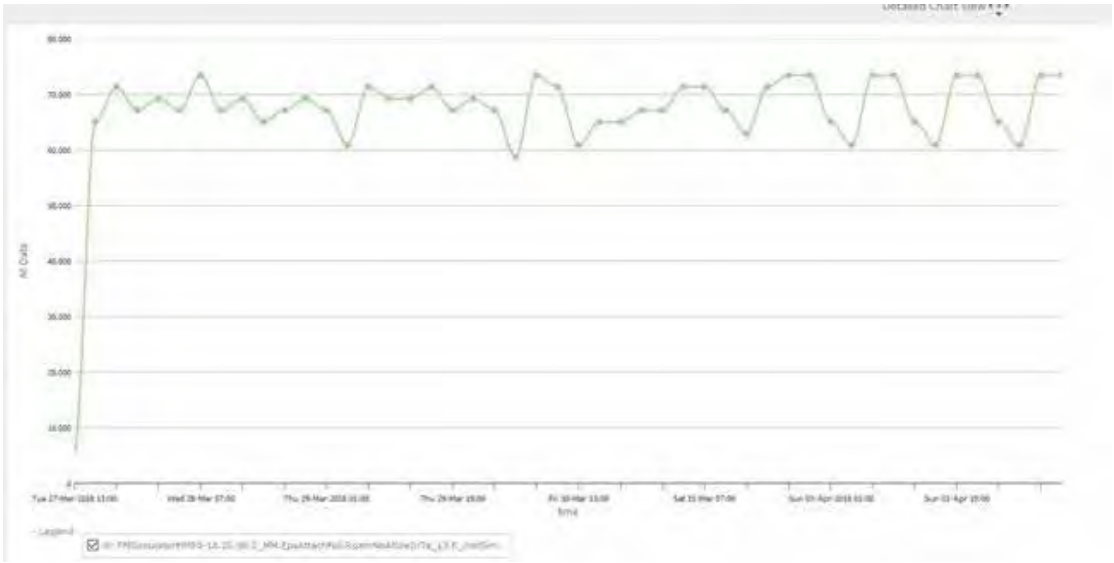
Figure 5-5 Rate Chart with Collection Time Period 7 Days



In a chart plotting more than 7 days of data, each data point represents 3 hours of data. This example illustrates that the collected data are not constant during this 3-hour period.

In a **Delta** chart, each data point represents the summation of 3 hours collected data.

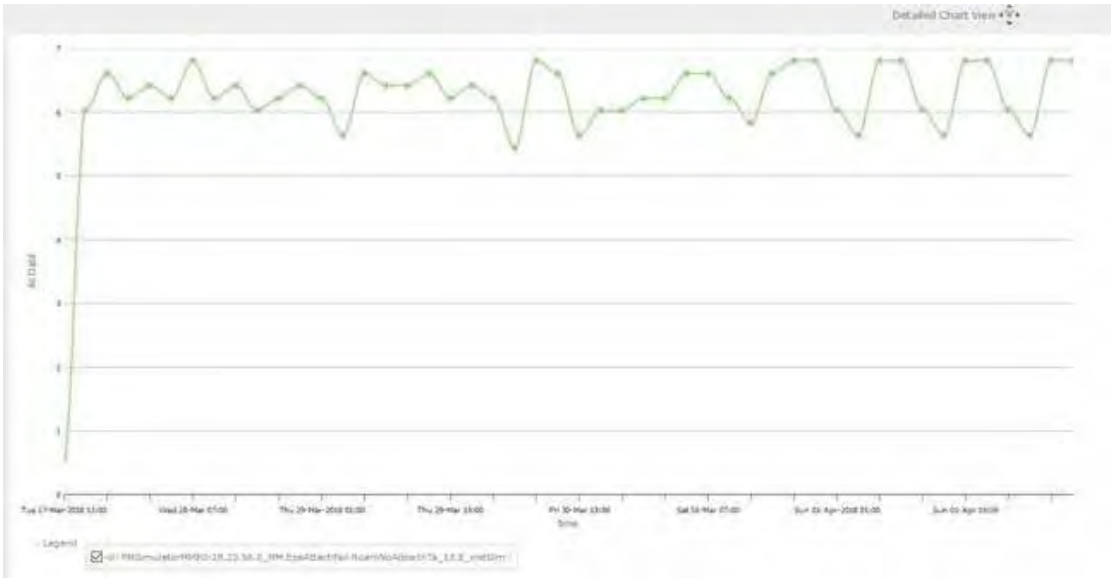
Figure 5-6 Delta Chart with Collection Time Period > 7 Days



In a **Rate** chart, each data point represents Delta value / collection time interval in seconds or:

(the summation of 3 hours collected data / 10800 seconds)

Figure 5-7 Rate Chart with Collection Time Period > 7 Days



Configuring Data Type and Unit Conversion

Note: *To configure the statistics data type and unit conversion, you must have the Performance > View Report > Statistics Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure Data Type at the global level:

1. Click the **Settings** icon on the toolbar and select **Performance => Reports => Statistics Configuration**.
2. Mark the data type to be configured (Rate Value or Delta Value).
3. Click **OK**.

To configure Unit Conversion at the global level:

1. Click the **Settings** icon on the toolbar and select **Performance => Reports => Statistics Configuration**.
2. Mark the unit conversion to be configured (Base-2 or Base-10).
3. Click **OK**.

Viewing Historical Statistics

Acuitas provides the user a view of the historical data of performance statistic attributes for a specified period.

For each interval:

- Counter statistics are displayed as per-second average values. The data is aggregated over the reporting interval. For example, for an hourly reporting interval, data is presented as average values per second over the hour.
- Gauge and average statistics are displayed as average values.
- Minimum and maximum statistics are displayed as actual values.

Configuring Historical Report Data Purging

Acuitas uses a pre-defined range of Purging Interval and a default Purging Interval for each type of historical statistics table. The Purging Interval is the time interval for which the data is retained in the table, with older data being purged.

Historical Table Type	Data Granularity	Purging Interval Range	Purging Interval Default
BASE	5-minute	6 – 48 hours	24 hours †
HOURLY	15-minute	1 – 6 day(s)	3 days †
DAILY	Hourly	1 – 3 week(s)	2 weeks †
WEEKLY	3-hour	4 – 8 weeks	6 weeks
MONTHLY	Daily	6 – 18 months	~12 months (360 days)
YEARLY	Weekly	2 – 5 years	3 years

† Represents a changed default purging interval in Acuitas 9.1.1 and higher. For more information, see Purge Interval Considerations.

You can configure the purging interval for each type of statistics table.

To configure a Purging Interval:

1 Issue the following commands at the command prompt:

```
cd /opt/Affirmed/NMS/bin
configureserver.sh
```

Acuitas displays the **Configure Server Details** menu.

```
Configure Server Details
------------------------

1.DatabaseDetails

2.PortDetails

3.Authentication

4.ProtocolDetails

5.PurgeConfigurationDetails
```

```
6.Exit


Please select your option from (1 | 2 | 3 | 4 | 5 |6) [1] :
```

2 To view the current purge settings, enter **5**.

```
Purge Configuration Details
-----------------------------------
            Table Type       Current Interval      Default Interval
1)          BASE             5 hours               24 hours
2)          HOURLY           3 days                5 days
3)          DAILY            Default               2 weeks
4)          WEEKLY           4 weeks               6 weeks
5)          MONTHLY          6 months              12 months
6)          YEARLY           2 years               3 years
Please select table type from (1 | 2 | 3  | 4 | 5 | 6 | 7 - EXIT ) [7]:
```

3 To manage a purging interval, enter the table number.

```
1) Reset to Default
2) Configure
3) Back
Please select your option from (1 | 2 | 3) [3]:
```

- To reset the purging interval to the default purging interval setting, enter **1**.

  For example:

  ```
  WEEKLY Table purge interval set to default value 12 months
  ```

- To set a new purging interval, enter **2**.

  For example:

  ```
  WEEKLY Table (4 – 8 weeks) [4]: 6
  WEEKLY Table purge interval set to 6week(s)
  ```

```
Please select table type from (1 | 2 | 3  | 4 | 5 | 6 | 7 - EXIT ) [7]:
```

4 To exit, enter **7**.

```
Configured Purge Interval Details:
BASE Table: 24 hours
WEEKLY Table: 6 weeks
HOURLY Table: 4 days
```

Any changes you make take affect when the purging schedule next runs.

Purge Interval Considerations

In Acuitas 9.1.1 and later, the default purge interval has changed for the following tables:

Table 5-1 Changed Default Purging Interval

Table Type	Data Granularity	Pre-9.1.1 Default Purging Interval	9.1.1 Default Purging Interval
BASE	5-minute	4 hours	24 hours
HOURLY	15-minute	1 day	3 days
DAILY	1-hour	1 week	2 weeks

These changes affect the behavior of the Dashboard Reports and the Historical Reports:

Table 5-2 Changed Dashboard Reports

Selected Interval	Pre-9.1.1 Table Type	Pre-9.1.1 Data Granularity	9.1.1 Table Type	9.1.1 Data Granularity
Last 12 hours	HOURLY	15-minute	BASE	5-minute
Last 24 hours	HOURLY	15-minute	BASE	5-minute

Table 5-3 Changed Historical Reports

Selected Interval	Pre-9.1.1 Data Granularity	9.1.1 Data Granularity
Last 24 hours	15-minute	5-minute
Last 3 days	1-hour	15-minute
Last 2 weeks	3-hour	1-hour

Note: *To view Historical Statistics, you must have the Performance > View Report > View Historical Statistics security group permission. For instructions, see Specifying Permissions by Security Group.*

To view Historical Statistics:

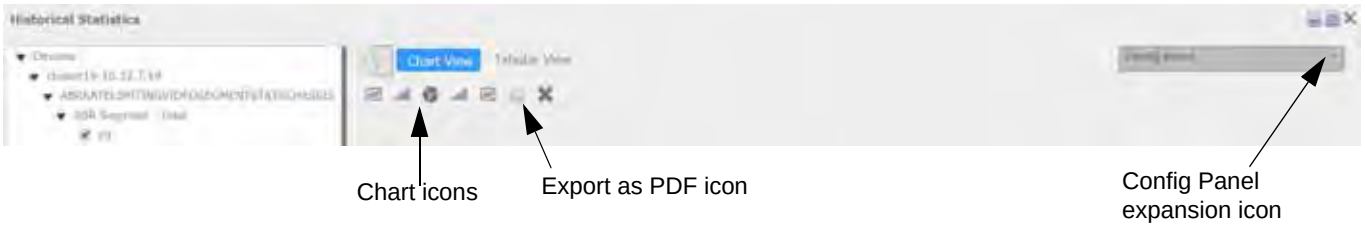
1 Use any of the following methods to view Historical Statistics:

Settings icon on the toolbar: Select **Performance => Reports => Historical**.

Pop-up menu: Right-click the Network Element and click **Statistics => Historical**.

Acuitas displays the Historical Statistics screen. The left pane lists all the NEs managed (or the Network Element you right-clicked) and the metrics. The Chart View tab is selected by default.

Figure 5-8 Historical Statistics



2 In the left panel, expand the device and metrics and mark the instances you want to view. You are limited to 10 or fewer instances.

3 To view the description of a metric:

a Point the cursor at the metric name.

b Click the detail icon.

Acuitas opens a pop-up window that displays the description of the statistic.

The window remains open until you close it or click another detail icon.

4 Click the **Config Panel** expansion icon to specify:

- **Period From** – Select the start time
- **Period To** – Select the end time
- **X Axis** – Collected Time to appear on the X axis
- **Show** All – Show statistics for all instances (such as multiple stats slots)
- **Show** Top *x* – Show highest statistics for specified number of instances
- **Show** Bottom *x* – Show lowest statistics for specified number of instances
- **Group All** – Mark this checkbox to group the charts for different selected metrics in a single chart. Unmark this checkbox for individual charts for each metric.

5 To view as a graphical chart (Chart View):

a Select the **Chart View** tab from the Historical Statistics window.

b Click the specific chart icons to view the data in the required graphical format.

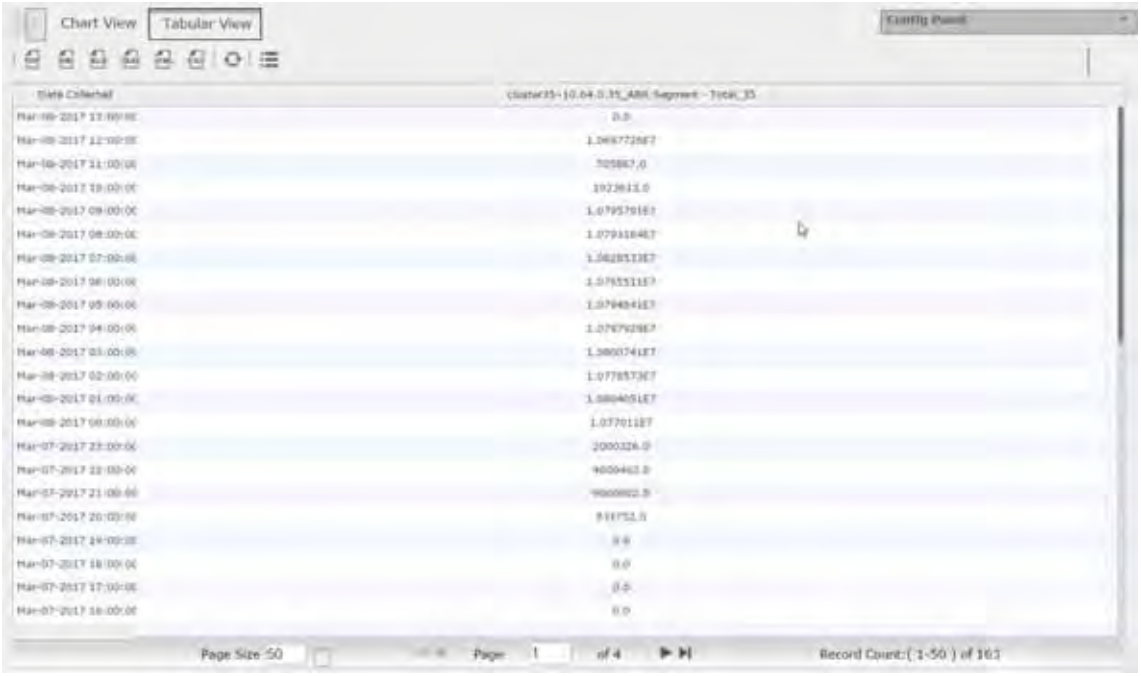
6 To view as a table of data (Tabular View):

a Select the **Tabular View** tab from the Historical Statistics window.

Acuitas retrieves data from the Acuitas database and displays a chart or textual report of the values.

The following example shows a Tabular View.

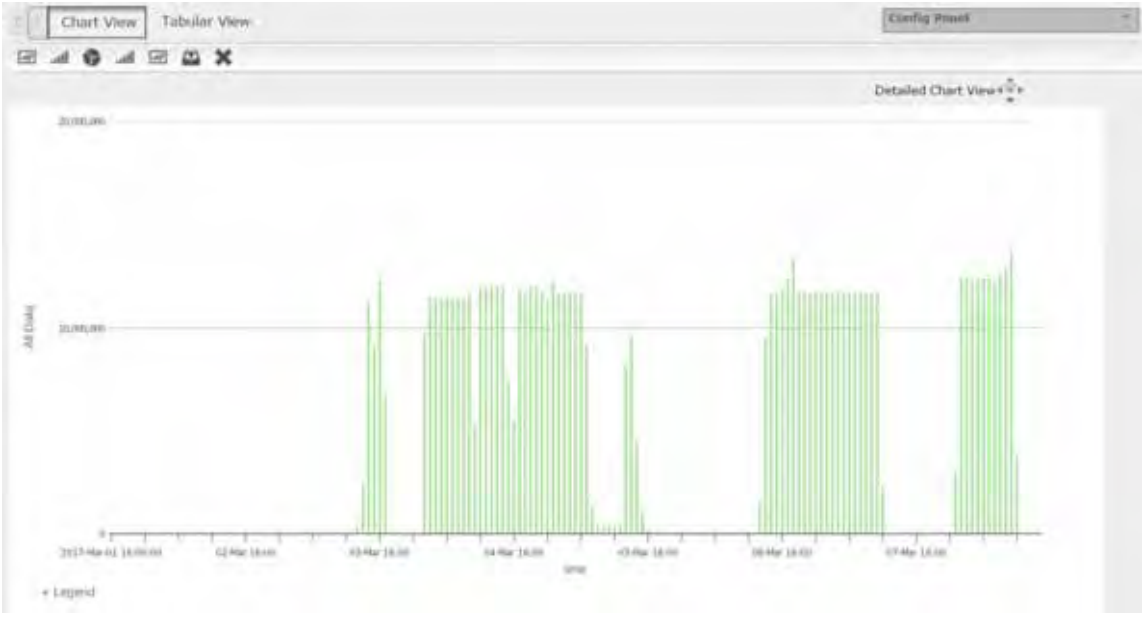
Figure 5-9 Example Tabular View



The collection time interval is indicated in the Date Collected column.

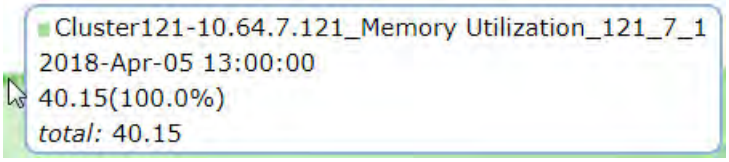
The following example shows a Chart View.

Figure 5-10 Example Chart View



To view the chart legend, click the **Legends** icon. + Legends If necessary, use the scrollbar to display the legend.

To determine the collection time interval for the chart, point the cursor at a particular data point. Acuitas opens a pop-up window that lists the node name, timestamp, and value for that data point.



Point the cursor at an adjacent data point to see its timestamp.

The collection time interval is the ending timestamp minus the beginning timestamp.

To clear the displayed chart, click the **Clear** icon. ✖

Exporting Historical Statistics Reports

You can save the graphical chart as a .pdf file. You can save the textual historical report in various formats, including .csv, .pdf, .xml, .xls, .html.

To save a graphical chart (Chart View):

1. Select the **Chart View** tab from the Historical Statistics window.
2. Click the **Export as PDF** icon on the tool bar of Chart view.

   Acuitas displays the **Download Files** window.
3. Right-click **Download PDF File** and select **Save Link As**.
4. Specify where you want the file saved and click **Save**.
5. From the **Download File**s window, click **Close**.

To save as a grid of data (Tabular View):

1. Select the **Tabular View** tab from the Historical Statistics window.
2. Click the icon of the required file format.

.pdf .xlm .xls .html .csv

   Acuitas displays the **Download Files** window.
3. Click **Download Exported File**.
4. From the **Download File**s window, click **Cancel**.

Viewing Real Time Statistics

Acuitas provides the user a quick graphical view of the current values of performance statistic attributes. The data collected as a part of the Real Time Stats is not persisted. Users with sufficient privilege can start an on-demand polling to monitor few performance metrics.

Note: *To view Real Time Statistics, you must have the Performance > View Report > View Real Statistics security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To view Real Time Statistics:

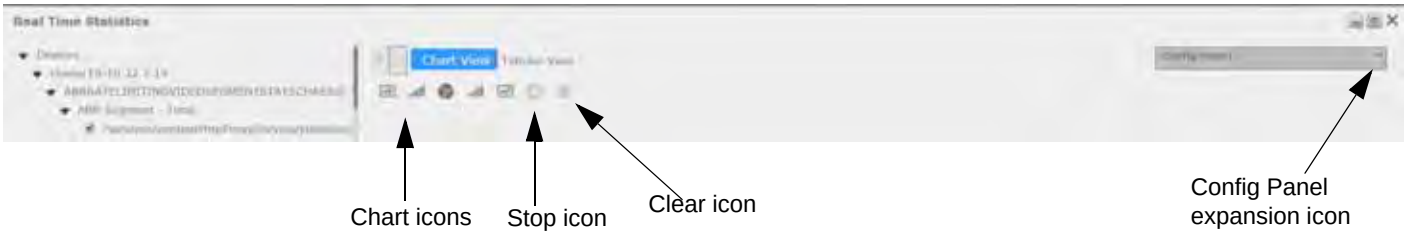
1 Use any of the following methods to view Real Time Statistics:

Settings icon on the toolbar: Select **Performance => Reports => Real Time**.

Pop-up menu: Right-click the Network Element and click **Statistics => Real Time**.

Acuitas displays the **Real Time Statistics** screen. The left pane lists all the NEs managed (or the Network Element you right-clicked) and the metrics.

Figure 5-11 Real Time Statistics



2 In the left panel, expand the device and metrics and mark the instances you want to view. You are limited to 10 or fewer instances.

3 To view the description of a metric:

a Point the cursor at the metric name.

b Click the detail icon.

Acuitas opens a pop-up window that displays the description of the statistic.

The window remains open until you close it or click another detail icon.

4 Click the **Config Panel** expansion icon to specify:

- **X Axis** – Collected Time to appear on the X axis
- **Server Polling** – Enter the number of seconds for the polling period (frequency of chart to be plotted). Range: 10 seconds to 120 seconds.
- **Configure Points** – Enter the number of data points to be plotted in the graph.
- **Group All** – Mark this checkbox to group the charts for different selected metrics in a single chart. Unmark this checkbox for individual charts for each metric.

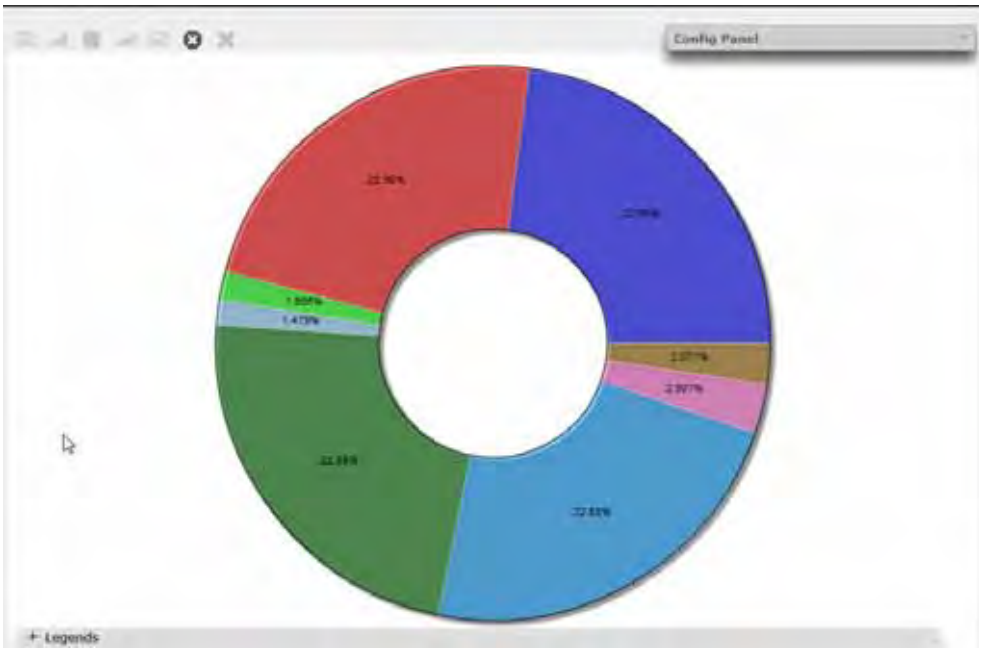
5 Click the specific chart icons to view the data in the required graphical format.

Line Chart | Bar Chart | Pie Chart | Stacked Bar Chart | Stacked Area Chart

Acuitas retrieves the data from the Acuitas database and displays the selected chart in the chart area. The chart is refreshed and redrawn whenever new data is collected based on the server polling interval.

The following example shows a Pie Chart.

Figure 5-12 Example Pie Chart



6 To view the chart legend, click the **Legends** icon. + Legends If necessary, use the scrollbar to display the legend.

7 To clear the displayed chart, click the **Clear** icon.

8 Click the **Stop** icon after viewing the Real Time Statistics.

Viewing Outage Reports

An outage refers to the time during which a network element is unreachable. Acuitas tracks the availability of each network element it manages by recording the start and end time for each unreachable window. This report determines the device Lost Time and Regained Time for each NE being managed.

Note: *To view an Outage Report, you must have the Performance > View Report > View Outage Report security group permission. For instructions, see Specifying Permissions by Security Group.*

To view an Outage Report:

1 Use any of the following methods to view an Outage Report:

Settings icon on the toolbar: Select **Performance => Reports => Outage**.

Pop-up menu: Right-click the Network Element and click **Statistics => Outage Report**.

Acuitas lists the outage details of the devices.

Configuring Export Reports

You can configure Performance Management reports to be exported to CSV files.

Note: *To configure an Export Report, you must have the Performance > View Report > Export Report Config security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure an Export Report:

1 Use the following method to configure an Export Report:

Settings icon on the toolbar: Select **Performance => Reports => Export Report Config**.

Acuitas displays the **Export Report Editor** window, listing the available elements.

2 Select the elements for the historical report by highlighting and clicking the right-arrow.

3 Click **Next**.

4 Expand the metrics tables and mark the metrics you want reported.

5 Click **Save**.

Acuitas exports the metrics to individual files by metric table every midnight, with the exported CSV files containing the last 24 hours data.

For daily Performance Management reports, the export filename is Historical_<*Entity Name*>_<*Table Name*>_<*Date*>.csv. The file is exported to the Acuitas server, in the directory */opt/Affirmed/NMS/server/ems/archive/<Date>/*.

By default, Acuitas purges any file older than 30 days. To configure a different purge interval, see Configuring Export Purge Interval.

Triggering Report Export on Demand

You can trigger the export of Performance Management reports to CSV files on demand.

Note: *To export reports on demand, you must have the Performance > View Report > Export Reports Now security group permission. For instructions, see Specifying Permissions by Security Group.*

To trigger report export:

1 Click the **Settings** icon on the toolbar and select **Performance => Reports => Export Now**.

2 At the confirmation prompt, click **OK**.

Acuitas exports the metrics to individual files by metric table, with the exported CSV file containing the data from 00:00 to the current time.

The files are exported to the Acuitas server, in the directory */opt/Affirmed/NMS/server/ems/archive/reports_export_now.*

For daily Performance Management reports, the export filename is Historical_<*Entity Name*>_<*Table Name*>_<*Date*>.csv.

For daily dashboard reports, the export filename is <*Entity Name*>_<*Dashboard Title*>_<*Report Title*>_<*Date*>.csv.

By default, Acuitas purges any file older than 30 days. To configure a different purge interval, see Configuring Export Purge Interval.

Configuring Export Purge Interval

You can configure the purge interval of exported CSV files.

Note: *To configure the Purge Interval, you must have the Performance > View Report > Purge Export Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure the Purge Interval:

1 Use the following method to configure the purge interval:

Settings icon on the toolbar: Select **Performance => Reports => Purge Export Configuration**.

2 Specify the number of days after which the system purges the exported CSV files.

3 Click **OK**.

Thresholds

You can define Thresholds with various severity levels for a performance statistic attribute or a Key Performance Indicator (KPI). When the data collected for an attribute or KPI crosses the threshold level defined, a threshold event is generated with the specified severity.

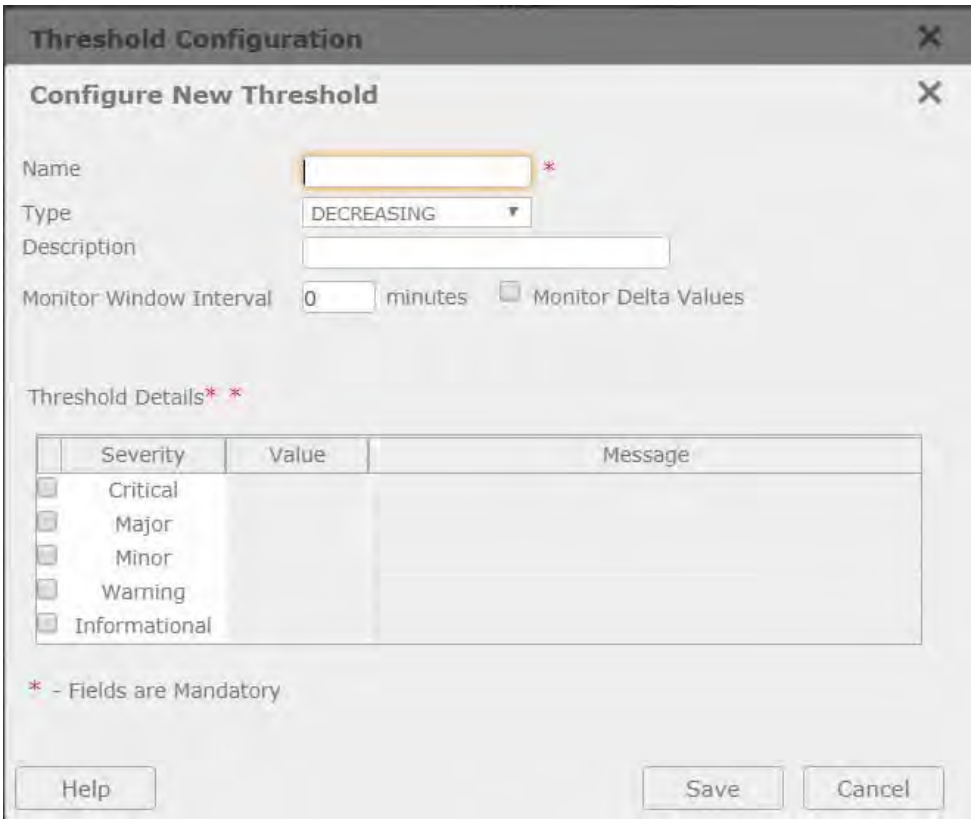
Adding Thresholds

Note: *To add a threshold, you must have the Performance > Configure Threshold > Add Threshold security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To add a threshold:

1. Click the **Settings** icon on the toolbar and select **Performance => Configure Thresholds**.
2. Acuitas displays the **Threshold Configuration** window.
3. Click the **Add New Threshold** icon.

Figure 5-13 Configure New Threshold



4 Complete the fields as follows:

- **Name** – Enter the threshold name.
- **Type** – Specify whether the threshold applies when a data point exceeds (Increasing) or falls below (Decreasing) the specified level.
- **Description** – Enter a threshold description.
- **Monitor Window Interval** – Enter how many minutes must transpire once the threshold has occurred before raising the alarm.
- **Monitor Delta Values** – Mark the checkbox to have Acuitas monitor the delta value between the previous and current interval counter values.
- **Threshold Details:**
  - Specify the **Value** for the threshold for configured severity categories.
  - Enter a corresponding **Message** for each configured category. When a threshold event is raised, the configured message is displayed in Alarms/Event Logs tab.

5 Click **Save** to commit the data.

6 Click **Close** to close the **Threshold Configuration** window.

7 You need to associate the threshold with a PM collection task. For instructions, see Associating a Threshold with a PM Collection Task. For the appropriate performance statistic attribute or Key Performance Indicator, select the new threshold from the **Threshold** field.

Viewing Thresholds

Note: *To view a threshold, you must have the Performance > Configure Threshold > View Threshold security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a threshold:

1 Click the **Settings** icon on the toolbar and select **Performance => Configure Thresholds**.

2 Acuitas displays the **Threshold Configuration** window, listing the following fields.

- **Threshold Name**
- **Type** – Specifies whether the threshold applies when a data point exceeds (Increasing) or falls below (Decreasing) the specified level.
- **Description**

3 Select a threshold to view its threshold details:

- **Severity** – Critical, Major, Minor, Warning, Informational
- **Value** – Value for the threshold
- **Message** – The configured message to display in Alarms/Event Logs tab when the threshold event is raised.

4 Click **Close** to close **Threshold Configuration** window.

Modifying Thresholds

Note: *To modify a threshold, you must have the Performance > Configure Threshold > Modify Threshold security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To modify a threshold:

1. Click the **Settings** icon on the toolbar and select **Performance =>** **Configure Thresholds**.
2. Acuitas displays the **Threshold Configuration** window.
3. Select a threshold to view and click **Edit Threshold Details** icon.
4. Make the necessary changes:
   - **Name** – Enter the threshold name.
   - **Type** – Specify whether the threshold applies when a data point exceeds (Increasing) or falls below (Decreasing) the specified value.
   - **Description** – Enter a threshold description.
   - **Monitor Window Interval** – Enter how many minutes must transpire once the threshold has occurred before raising the alarm.
   - **Monitor Delta Values** – Mark the checkbox to have Acuitas monitor the delta value between the previous and current interval counter values.
   - **Threshold Details:**
     - Specify the **Value** for the threshold for configured severity categories.
     - Enter a corresponding **Message** for each configured category. When a threshold event is raised, the configured message is displayed in Alarms/Event Logs tab.
5. Click **Save** to commit the data.
6. Click **Close** to close **Threshold Configuration** window.

User Tasks Templates

The User Tasks template specifies the metrics to be collected for performance statistics:

Note: *By default, Acuitas is configured to collect all the appropriate metrics. It is not essential for the administrator to change user task templates.*

Note: *To manage user task templates, you must have the Performance > User Tasks > Task Template security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

Viewing User Tasks Templates

To view a User Tasks Template:

1 Click the **Settings** icon on the toolbar and select **Performance =>**

User Tasks => Templates.

Acuitas displays the **Task Template**, listing the user tasks templates.

Select a template to view the performance metrics it collects.

Modifying User Tasks Templates

You can modify a data collection task, as long as it is not currently in use by the Task Scheduler.

To Modify a User Tasks Template:

1 Click the **Settings** icon on the toolbar and select **Performance =>**

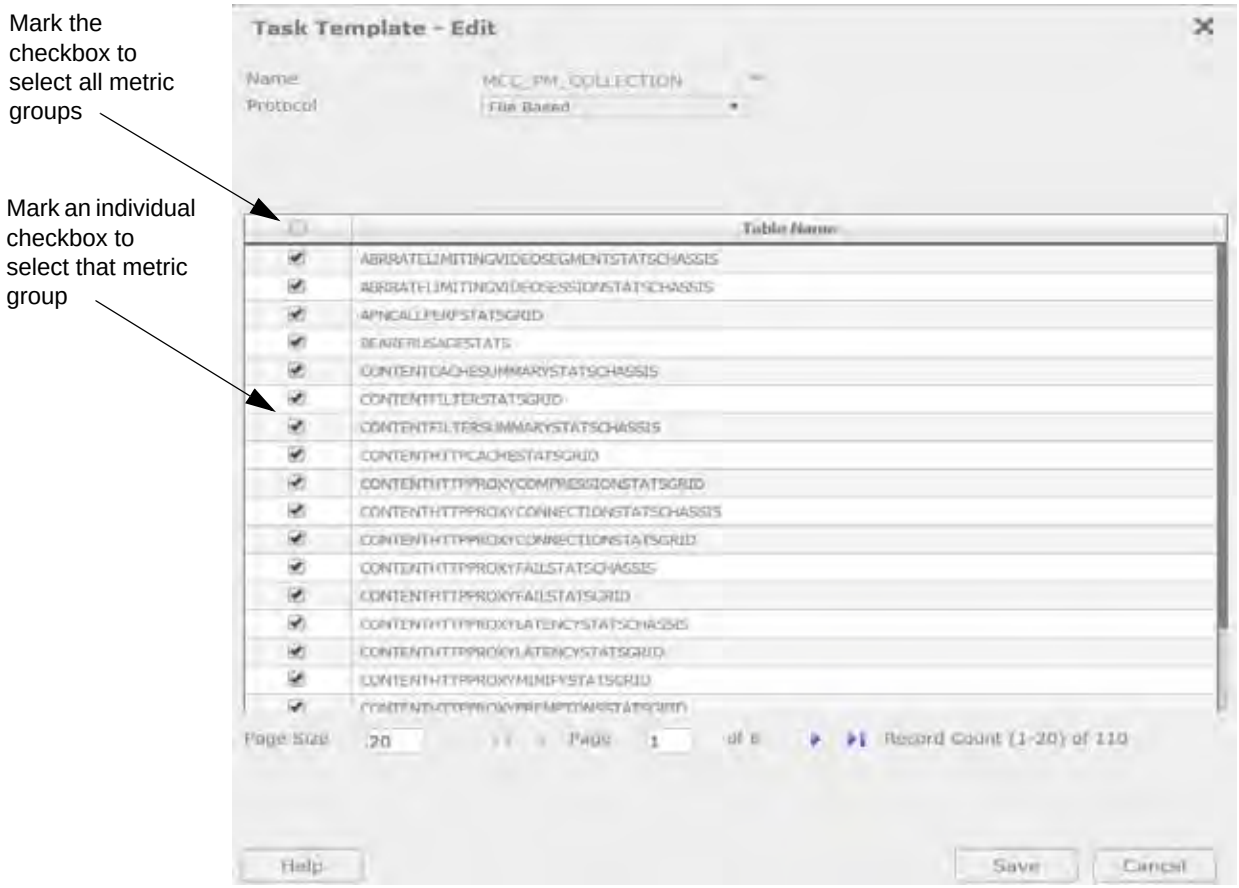
User Tasks => Templates.

Acuitas displays the **Task Template**, listing the user tasks templates.

2 Select a template and click the **Edit User Task Template** icon.

3 For a template with **Task Type** set to File Based, you can configure the data to be collected. Mark the checkboxes to select the metrics groups you want collected. To select all metrics groups, mark the checkbox at the top of the column.

Figure 5-14 User Task Template Details Edit



4 Click **Save** to commit the data.

5 At the confirmation prompt, click **OK**.

6 Click **Close** to close **Task Template** window.

Users Tasks Scheduler

A user tasks scheduler triggers data collection tasks based on task templates to be periodically executed.

Viewing User Tasks Scheduler

Note: *To view a user task schedule, you must have the Performance > User Tasks > Task Schedule > View Task Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To view the User Tasks Scheduler:

1. Click the **Settings** icon on the toolbar and select **Performance => User Tasks => Schedule**.
2. Use any of the following methods to view a user tasks schedule:

   Toolbar: Select the user tasks schedule and click the **View** icon.

   Pop-up menu: Right-click the user tasks schedule and select **View**.
3. Click **Close** to close the window.

Enabling/Disabling User Tasks Schedules

You can enable/disable user tasks schedules using the Task Scheduler.

Note: *To enable/disable a user task, you must have the Performance > User Tasks > Task Schedule > Start/Stop Task Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To enable/disable a user tasks schedule:

1. Click the **Settings** icon on the toolbar and select **Performance => User Tasks => Schedule**.

   Acuitas displays the **Task Scheduler**, listing performance management collections and other scheduled data collections.
2. Use any of the following methods to enable a user tasks schedule:

   Toolbar: Select the user tasks schedule and click the **Enable Schedule** icon.

Pop-up menu: Right-click the user tasks schedule and select **Enable Schedule**.

Use any of the following methods to disable a user tasks schedule:

Toolbar: Select the user tasks schedule and click the **Disable Schedule** icon.

Pop-up menu: Right-click the user tasks schedule and select **Disable Schedule**.

3 At the confirmation prompt, click **OK**.

The Admin Status of the user tasks schedule changes to Enabled or Disabled.

Associating a Threshold with a PM Collection Task

For a particular performance statistic attribute or Key Performance Indicator, you associate it with either a metric-based threshold or an instance-based threshold.

For a metric, data is always collected as a list of (instance,value) pairs. Each (instance,value) pair is first matched with a defined instance-based threshold, then a metric-based threshold. When no instance-based threshold exists, only the metric-level threshold is matched. When the data collected for a metric crosses the defined instance-based or metric-based threshold level, a threshold event is generated with the specified severity.

To associate a threshold with a PM collection task, modify a user tasks schedule.

Note: *To modify a user task schedule, you must have the Performance > User Tasks > Task Schedule > Modify Task Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

Prerequisite to Configure a Metric-based Threshold

To associate a particular performance statistic attribute or Key Performance Indicator with a metric-based threshold, you first need to create a threshold. For instructions, see Thresholds.

Prerequisites to Configure an Instance-based Threshold

To associate a particular performance statistic attribute or Key Performance Indicator with an instance-based threshold, you first need to create the following entities:

- Threshold. For instructions, see Thresholds.
- Instance filter.

The instance filter can contain a single index value or a set of index values. For example, a single index can be a specified value for the index zone_name, apn_name, or so on. A set of index values can be a specified value for multiple indices. When you configure the instance filter, include the indices, each separated by a period, in the order to match the target metric.

Note: *To create an instance filter, you must have the Performance > Instance Filter Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

To create an instance filter:

1 Click the **Settings** icon on the toolbar and select **Performance =>**

Instance Filter Configuration.

Acuitas displays the **Instance Filter Configuration**.

2 Click the **New Filter** icon.

In the **Add Filter** dialog, enter the Filter Name. In the case of multiple indices, include the indices values in the name, each separated by a period, in the order to match the target metric. Click **Add**.

A filter with that name is created.

3 In the **Filter Manager**, select the filter and click the **Add Condition** icon:

a Complete the Conditions fields by selecting Instance Name for **Parameter** and appropriate values for **Operator**, **Value**, and **Condition**.

For example, to configure an instance filter for the metric NumCurrentSessions for which data is collected for each zone and apn, specify the following set of indices:

– The index zone_name with the value `default`.

– The index apn_name with the value `am.truphone.com`.

Specify the **Operator** and **Value**. For this filter, the **Value** you enter must include the multiple indices values, each separated by a period, in the order to match (that is, zone_name first and apn_name second):

```
default.am.truphone.com
```

For example, specify any of the following settings:

– **Starts with** `default`

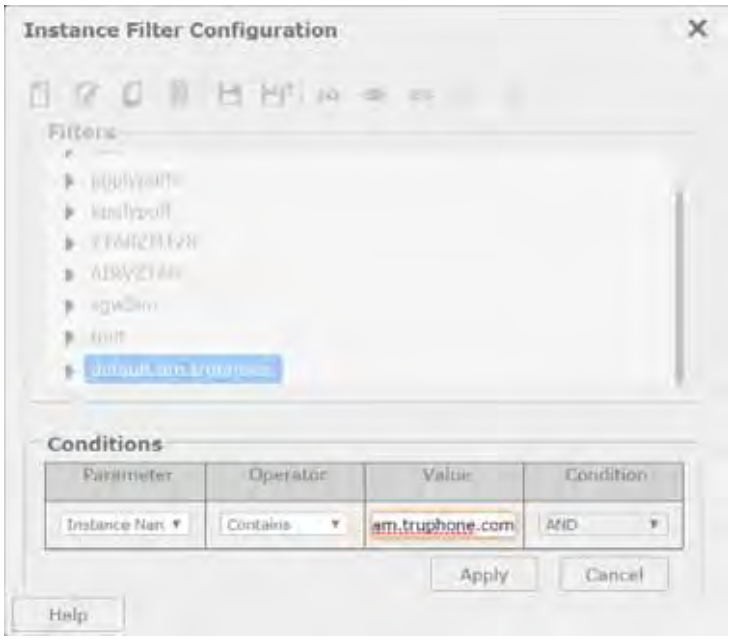
– **Ends with** `truphone.com` or `am.truphone.com`

– **Equals** `default.am.truphone.com`

– **Not Equals** `default.bm.truphone.com`

– **Contains** `default` or `am.truphone.com`

Table 5-4 Instance Filter Configuration



b Click **Apply**.

4 To add additional Conditions, repeat step 3. Specify **Condition** = AND or OR.

5 If the filter needs a combination of AND and OR conditions to achieve the desired result:

a In the **Filter Manager**, select the filter and click the **Create AND group** icon (or **Create OR Group** icon).

b In the **Filter Manager**, select the AND... (or OR...) group and click the **Add Condition** icon and complete the Conditions for the group.

c Click **Apply**.

6 Click the **Save Filter** icon.

Modifying User Tasks Scheduler

To modify a User Tasks Scheduler:

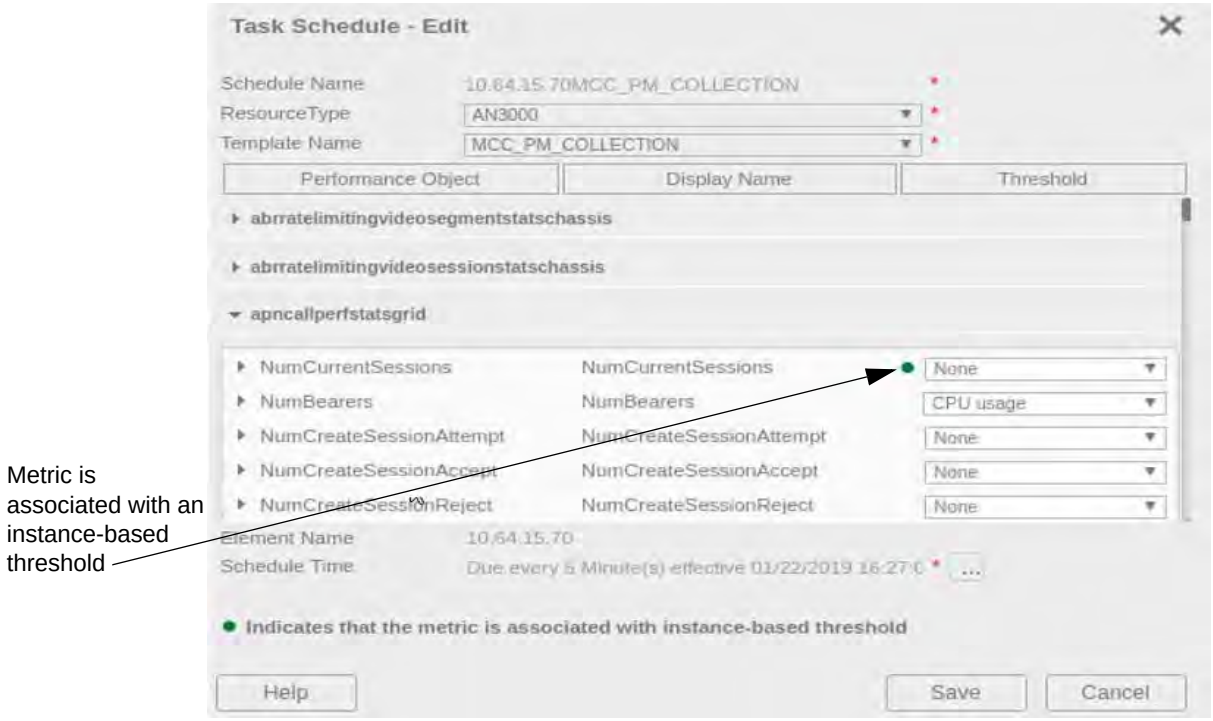
1 Click the **Settings** icon on the toolbar and select **Performance** => **User Tasks** => **Schedule**.

2 Use any of the following methods to modify a user tasks schedule:

Toolbar: Select the user tasks schedule and click the **Edit User Task Scheduler** icon.

Pop-up menu: Right-click the user tasks schedule and select **Edit**.

Figure 5-15 Task Schedule Edit

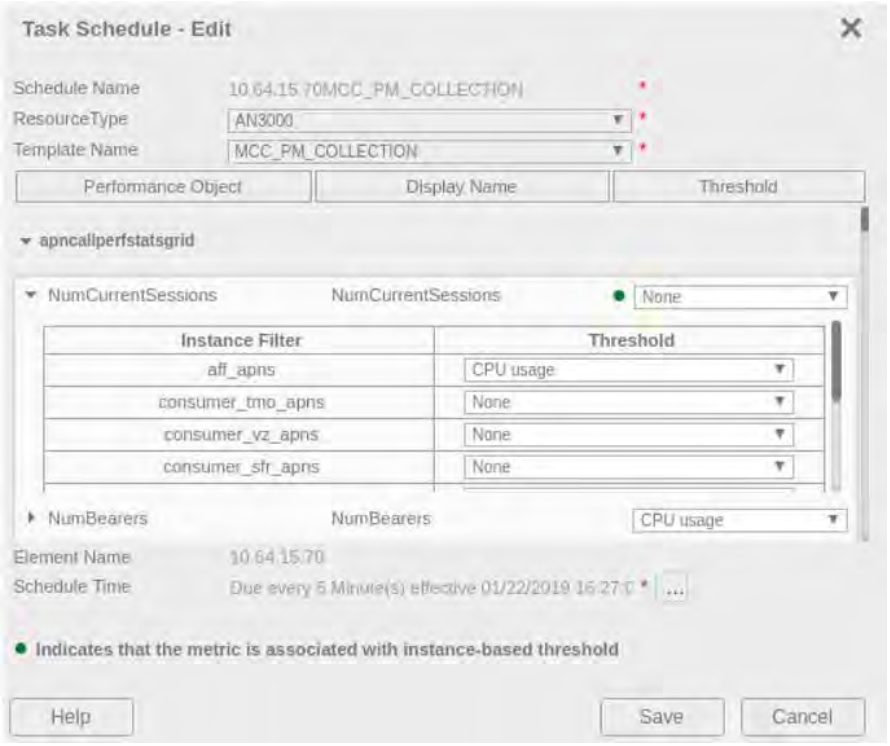


3 Make the necessary changes:

- **Schedule Name** – Enter the schedule name.
- **Performance Object** – Expand the Performance object name to list the metrics.

  An icon in the Threshold column indicates that the metric is associated with an instance-based threshold. To list the instance-based thresholds, expand the metric.

Figure 5-16 Task Schedule Edit with Expanded Metric



- **Threshold** – Select a threshold to be associated with each performance statistic attribute or Key Performance Indicator.

Note: *Reachability task schedules (resourcereachability Performance object) cannot be associated with an instance-based threshold.*

---

4 In the Scheduled Time field, click the **Recurrence Pattern** icon to configure Recurrence Details.

5 Specify the recurrence details and click **Schedule**.

6 Click **Save**.

Acuitas matches each instance-level value in the collected data with its associated threshold value and based on the results, raises a threshold event.

Quick Start Data Collection

Note: *To Quick Start a data collection task, you must have the Performance > User Tasks > Task Schedule > Start/Stop Task Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To Quick Start (instantly execute) a data collection task:

1 Click the **Settings** icon on the toolbar and select **Performance => User Tasks => Schedule**.

Acuitas displays the **Task Scheduler**, listing performance management collections and other scheduled data collections.

2 Use any of the following methods to Quick Start a data collection tasks:

Toolbar: Select the data collection tasks and click the **Quick Start** icon.

Pop-up menu: Right-click the data collection tasks and select **Quick Start**.

Exporting User Tasks Scheduler

You can export a list of user tasks scheduler instances to a CSV file.

Note: *To export user tasks scheduler instances, you must have the Performance > User Tasks > Task Schedule > View Task Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To export user tasks schedules:

1 Click the **Settings** icon on the toolbar and select **Performance => User Tasks => Schedule**.

Acuitas displays the **Task Scheduler**, listing performance management collections and other scheduled data collections.

2 If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.

3 Click the **Export** icon.

Acuitas displays the **Configure Export Parameters** window.

4 Configure the parameters as follows:

- **File Type**: Select the required file format (CSV).
- **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
- **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
- **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.

5 Click **Apply**.

Acuitas displays the **Download Files** window.

6 Click **Download Exported File**.

7 From the **Download File**s window, click **Close**.

CSV Stats Recovery

Acuitas allows you to perform on-demand statistics recovery in MCC and SCEF devices. For example, in case of an Acuitas server outage or a device is unreachable for more than 30 minutes, performance data in the Acuitas database may be missing, which would result in gaps in the performance reports. You can launch a statistics recovery operation to save the 5-minute interval CSV files for the specified device(s).

Acuitas exports the recovered CSV files to the export directory:

/opt/Affirmed/NMS/server/ems/data/pm/<node name>

The export filename is *<PM stats table name>-<interval timestamp>*.csv, where *interval timestamp* represents the starting timestamp of the export interval.

Launching a CSV Stats Recovery

Only a single CSV stats recovery can be launched at a time. The Launch option is disabled if another recovery is running.

Note: *To launch a CSV stats recovery, you must have the Performance > Stats Recovery security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To launch a CSV statistics recovery:

1. Click the **Settings** icon on the toolbar and select **Performance =>** **CSV Stats Recovery**.

   Acuitas displays the **CSV Stats Recovery** window, listing the statistics recovery schedules.

2. Click the **Refresh** icon to refresh the list of schedules.

3. To perform a new on-demand statistics recovery, click the **Launch** icon.

   Acuitas displays the CSV Stats Recovery Launch screen.

Figure 5-17 CSV Stats Recovery Launch Screen

4 Configure the parameters as follows:

- **Recovery Name** – Enter the recovery name.
- **From Time** – Click the **Calendar** icon and select a start date and 5-minute interval time (24-hour, based on GMT timezone) for the statistics. Click **Save**.
- **To Time** – Click the **Calendar** icon and select a end date and 5-minute interval time (24-hour, based on GMT timezone) for the statistics. Click **Save**.

  The maximum recovery range is 14 days.
- **All Devices** – Mark the checkbox to recover the statistics from all managed devices. Unmark the checkbox to specify the managed devices.
- **Assigned List** – Select the MCCs by highlighting and clicking the right-arrow.

5 Click **Save**.

Acuitas adds the recovery schedule to the **CSV Stats Recovery** window and runs the recovery. If files already exist in the export directory for a particular collection period, the operation *does not* overwrite them.

Viewing Statistics Recovery Schedule Details

Note: *To view CSV stats recovery schedule details, you must have the Performance > Stats Recovery security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a statistics recovery schedule details:

1 Click the **Settings** icon on the toolbar and select **Performance =>**

CSV Stats Recovery.

Acuitas displays the **CSV Stats Recovery** window, listing the statistics recovery schedules:

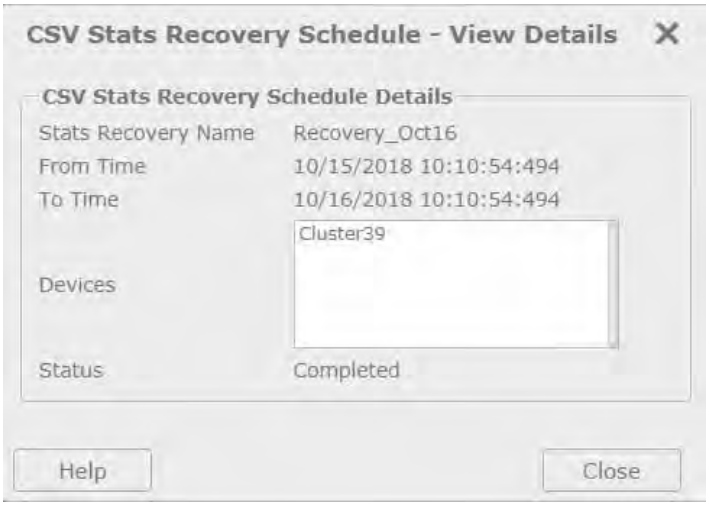
- Stats Recovery Name
- From Time
- To Time
- Status (Scheduled, Running, Completed)

2 From the **CSV Stats Recovery** window, use any of the following methods to view schedule details:

Toolbar: Select the schedule and click the **View Details** icon.

Pop-up menu: Right-click the schedule and click **View Details**.

Acuitas displays the **View Details** window.



3 Click **Close** to close the window.

Viewing Statistics Recovery Schedule Status

When multiple Network Elements use a particular statistics recovery schedule, Acuitas runs the schedule on each node. You can view the status of a recovery schedule on a per-device basis.

Note: *To view CSV stats recovery schedule status, you must have the Performance > Stats Recovery security group permission. For instructions, see Specifying Permissions by Security Group.*

To view Statistics Recovery Schedule status:

1. Click the **Settings** icon on the toolbar and select **Performance =>** **CSV Stats Recovery**.

   Acuitas displays the **CSV Stats Recovery** window, listing the statistics recovery schedules:

   - Stats Recovery Name
   - From Time
   - To Time
   - Status (Scheduled, Running, Completed)

2. From the **CSV Stats Recovery** window, use any of the following methods to view schedule details:

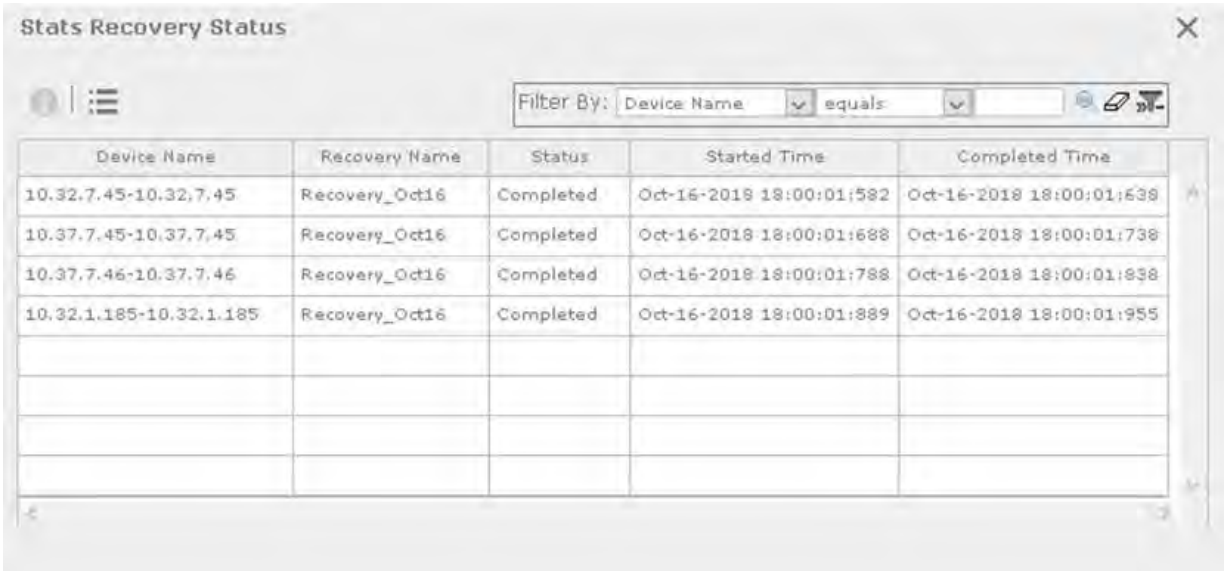
   Toolbar: Select the schedule and click the **View Status** icon.

   Pop-up menu: Right-click the schedule and click **View Status**.

   Acuitas displays the **Stats Recovery Status** window, listing the following information:

   - Device Name
   - Recovery Name
   - Software Release
   - Status (Scheduled, Running, Completed)
   - Started Time
   - Completed Time

Figure 5-18 Stats Recovery Status Screen



3 To view status of a recovery on a per-device basis, select the device and click the **View Status** icon.

4 Acuitas displays the **Stats Recovery View Status** window, listing the recovery status report for the selected device.

Possible scenarios for recovery of a statistics CSV file include:

- No statistics CSV file was recovered because of a connection failure to an MCC. A status message indicates the failure.
- Partial statistics CSV file was recovered because some data intervals were unavailable on the MCC. A status message lists which intervals were not recovered.
- Complete statistics CSV file was recovered with all requested intervals. A status message indicates recovery success.

5 Click **Close** to close the **Stats Recovery View Status** window.

6 To close the **Stats Recovery Status** window, click the **Close** icon.

Deleting Statistics Recovery Schedules

You can delete a statistics recovery schedule only if it has the Status Scheduled or Completed.

Note: *To delete a statistics recovery schedule, you must have the Performance > Stats Recovery security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete a statistics recovery schedule:

1 Click the **Settings** icon on the toolbar and select **Performance =>**

CSV Stats Recovery.

Acuitas displays the **CSV Stats Recovery** window, listing the statistics recovery schedules:

- Stats Recovery Name
- From Time
- To Time
- Status (Scheduled, Running, Completed)

2 Use any of the following methods to delete a statistics recovery schedule:

Toolbar: Select the schedule and click the **Delete** icon.

Pop-up menu: Right-click the schedule and select **Delete**.

3 At the confirmation prompt, click **OK**.

Viewing Key Performance Indicators

Acuitas contains an application to view Key Performance Indicators (KPIs).

The Administrator can configure the statistic data type of KPIs displayed in the Dashboard charts at the global level:

- Delta Value — Statistic values are plotted based on the following formula:

  Delta value = current counter value - previous counter value

- Rate Value — Statistic values are plotted based on the following formula:

  Rate value = Delta value / collection time interval in seconds

  By default, the Rate Value is applied.

For instructions, see Configuring Data Type and Unit Conversion at the Global Level.

KPI metrics are described in Appendix B, Key Performance Indicators (KPIs) Metrics.

Note: *To view Key Performance Indicators, you must have the Performance > PM Stats > View Dashboard security group permission. For instructions, see Specifying Permissions by Security Group.*

To view Key Performance Indicators:

1. Select a network element or Acuitas server.
2. Click the **PM Dashboard** tab.
   - For the Acuitas server, Acuitas graphically displays the **EMS PM Stats Dashboard**:
     - CPU Usage (%) - Last 24 Hours
     - Memory Usage (%) - Last 24 Hours
     - Disk Usage (%) - Last 24 Hours
   - For a network element, Acuitas lists preconfigured dashboards in the toolbar of the dashboard.
3. For a network element, select the dashboard you want to view from the toolbar of the dashboard:
   - **System KPIs Dashboard**:
     - CPU Utilization - Last 24 Hours (Top 5 Instance(s))
     - Memory Utilization - Last 24 Hours (Top 5 Instance(s))

- **SGW KPIs Dashboard:**
  - EPS Attach Success Rate - Last 24 Hours (Bottom 5 Instance(s))
  - Mobility Update Success Rate with SGW Relocation - Last 24 Hours (Bottom 5 Instance(s))
  - Mobility Update Success Rate without SGW Relocation - Last 24 Hours (Bottom 5 Instance(s))
- **PGW KPIs Dashboard:**
  - EPS Attach Success Rate - Last 24 Hours (Bottom 5 Instance(s))
  - Network Initiated Dedicated Bearer Creation Success Rate - Last 24 Hours (Bottom 5 Instance(s))
  - UE Initiated Dedicated Bearer Creation Success Rate - Last 24 Hours (Bottom 5 Instance(s))
- **GGSN KPIs Dashboard:**
  - UMTS PDP Context Activation Success Rate - Last 24 Hours (Bottom 5 Instance(s))
- **Content Service KPIs Dashboard:**
  - Cache Object Hit Ratio - Last 24 Hours (All Instance(s))
  - Cache Byte Hit Ratio - Last 24 Hours (All Instance(s))
  - HTTP Proxy Transactions Success Rate - Last 24 Hours (All Instance(s))
  - HTTP Proxy Average Service Time - Last 24 Hours (All Instance(s))
- **MME LTE Usage KPIs Dashboard:**
  - LTE - Total eNodeB Connected - Last 24 Hours (All Instance(s))
  - LTE - Total Simultaneous Attached Subscribers (SAU) - Last 24 Hours (All Instance(s))
  - LTE - Peak Number of Active Default Bearers - Last 24 Hours (All Instance(s))
  - LTE - Peak Number of Active Dedicated Bearers - Last 24 Hours (All Instance(s))
- **MME VM CPU and MEM KPIs Dashboard:**
  - VM - Busiest CPU Usage - Last 24 Hours (All Instance(s))
  - VM - Memory Usage - Last 24 Hours (All Instance(s))
- **MME LTE KPIs Dashboard:**
  - LTE - Attach Success Rate Nodal - Last 24 Hours (All Instance(s))
  - LTE - Percentage of SAU in ECM-CONNECTED - Last 24 Hours (All Instance(s))
  - LTE - Session Activation Success Rate Nodal - Last 24 Hours (All Instance(s))

– LTE - Bearer Activation Success Rate Nodal - Last 24 Hours (All Instance(s))

Acuitas graphically displays the metrics.

4 For some derived metrics, you can change the data unit of the displayed metrics. Click the unit at the top of the chart (such as bps, Kbps, Mbps, Gbps, Tbps) to regraph the metrics based on the selected unit. The derived graphics that support changing data units are listed with a dagger (†) in Derived Metrics.

You can save the data based on the selected unit as textual data or graphical data in a .pdf file. For instructions, see Exporting KPI Data from the Dashboard.

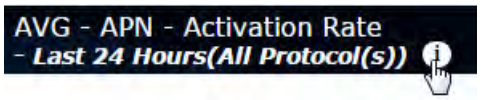
5 To view the chart legend, click the **Legends** icon. + Legends If necessary, use the scrollbar to display the legend.

6 To refresh the metrics, click the **Refresh** icon.

7 To view a KPI formula:

a Point the cursor at the KPI name.

b Click the detail icon.



Acuitas opens a pop-up window that displays the KPI formula.

The window remains open until you close it or click another detail icon.

8 To view other KPIs, select the dashboard you want to view.

The above reports can be filtered to show top-*n* or bottom-*n* values and can be aggregated into hourly, daily, weekly, monthly, or annual values. This information can be useful to illustrate long-term trends. For example, you could generate a report showing the top-*n* VOIP protocols used in the last hours, weeks, months, or year. To do so, or to add a new dashboard and specify the KPI data you want to view, follow the instructions in Configuring the Dashboard.

Configuring the Dashboard

You can configure the Dashboard to display multiple charts with different KPIs. The appropriate statistics to monitor depend on how the system is deployed. And, you can configure to periodically export the Dashboard as a report.

A single Dashboard report supports up to four graphs.

Note: *To add a new dashboard, you must have the Performance > PM Stats > Add Dashboard security group permission. To modify a dashboard, you must have the Performance > PM Stats > Modify Dashboard security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure the Dashboard:

1. Click the **PM Dashboard** tab.
2. To open the tree display, click the **Toggle Resource Selection View** icon (next to the **Settings** icon) to expand the left pane.
3. Select the Global Group, Group, or device for which you want to display KPIs.
4. Add a new dashboard or modify an existing dashboard:
   - To add a new dashboard, click the **New Dashboard** icon on the tool bar of the Dashboard.
   - To modify an existing dashboard, select the dashboard you want to modify from the toolbar of the Dashboard. Then, click the **Edit Dashboard** icon on the tool bar of the Dashboard.

   Acuitas displays the **Dashboard Editor** window.
5. Configure the parameters as follows:

Table 5-5 Dashboard Parameters

Parameter	Description
Title	Enter a name for the dashboard.
Statistics Type	Select the statistics type: ■ Historical ■ Realtime
Filter	Click the Filter icon to set up conditions to filter records. For details, see Using the Dashboard Filter Manager to Filter Records.
Set as default	Mark the checkbox to set this dashboard as the default.

Table 5-5 Dashboard Parameters

Parameter	Description
Layout Type	Select the screen layout for the data.
Properties when Statistics Type is set to Realtime:	
Metrics	Click the Metric Configuration icon. to specify the metric to display. In the Metric Configurator screen: **1** In **Metric Table Name**, select the data collection group name that contains the metrics you want to display. For details, see Derived Metrics and Raw Metrics. **2** If desired, enter a value in the **Filter** field and click the **Search** icon. **3** In **Metric Name**, select the metric. **4** Click **Apply**.
Chart	Select the chart type: ■ Pie ■ Bar ■ Line
Refresh Interval	Select the time interval at which the chart is to be refreshed, in seconds.
Properties when Statistics Type is set to Historical:	
Metrics	Click the Metric Configuration icon. to specify the metric to display. In the Metric Configurator screen: **1** In **Metric Table Name**, select the data collection group name that contains the metrics you want to display. For details, see Derived Metrics and Raw Metrics. **2** If desired, enter a value in the **Filter** field and click the **Search** icon. **3** In **Metric Name**, select the metric. **4** Click **Apply**.
Chart	Select the chart type: ■ Pie ■ Bar ■ Line
Interval	Select the historical time interval you want for the chart.

Table 5-5 Dashboard Parameters

Parameter	Description
Show	Specify how many devices you want to include: ■ **Show** All – Shows statistics for all devices (up to 50 instances) ■ **Show** Top *x* – Shows statistics for the highest specified number of devices (up to 20 instances) ■ **Show** Bottom *x* – Shows lowest statistics for the lowest specified number of devices (up to 20 instances)
Aggregate Type	Select the data aggregate type to control the aggregation function used to aggregate data over Resource or Resource Groups: ■ **Avg** – Uses average function to aggregate for the resource or resource group ■ **Min** – Uses minimum function to aggregate for the resource or resource group ■ **Max** – Uses maximum function to aggregate for the resource or resource group ■ **Sum** – Uses the sum function to aggregate for the resource or resource group
Filter By	Select the filter to filter the data displayed. ■ **All** – Shows all statistics ■ **All Gateway** (for QCI/ARP statistics only) – Show all gateway statistics ■ **All PGW** (for QCI/ARP statistics only) – Shows statistics for gateway type PGW ■ **All SGW** (for QCI/ARP statistics only) – Shows statistics for gateway type SGW

Table 5-5 Dashboard Parameters

Parameter	Description
Group By	Select the grouping: ■ Subgroup ■ Resource ■ Instance ■ Category (use for the following metrics:) – DPI - % Protocol Network Usage – DPI - Protocol Network Usage (Mbps) ■ Application (use for the following metrics:) – DPI - % Application Network Usage – DPI - Application Network Usage (Mbps) ■ Protocol (use for the following metrics:) – DPI - % Protocol Network Usage – DPI - Protocol Network Usage (Mbps) ■ Operating System (use for the following metrics:) – DPI - % OS Network Usage – DPI - OS Network Usage (Mbps) ■ Gateway (use for the following metrics:) – QCI/ARP - Downlink Throughput(Mbps) – QCI/ARP - Uplink Throughput(Mbps) – QCI/ARP - Bearer Drop Rate – QCI/ARP - Handover Success Rate – QCI/ARP - Bearer Retainability Rate ■ Apn (use for the following metrics:) – QCI/ARP APN - Downlink Throughput(Mbps) – QCI/ARP APN - Uplink Throughput(Mbps) – QCI/ARP APN - Bearer Drop Rate – QCI/ARP APN - Handover Success Rate – QCI/ARP APN - Bearer Retainability Rate ■ QciArp (use for the following metrics:) – QCI/ARP - Downlink Throughput(Mbps) – QCI/ARP - Uplink Throughput(Mbps) – QCI/ARP - Bearer Drop Rate – QCI/ARP - Handover Success Rate – QCI/ARP - Bearer Retainability Rate – QCI/ARP APN - Downlink Throughput(Mbps) – QCI/ARP APN - Uplink Throughput(Mbps) – QCI/ARP APN - Bearer Drop Rate – QCI/ARP APN - Handover Success Rate – QCI/ARP APN - Bearer Retainability Rate

Table 5-5 Dashboard Parameters

Parameter	Description
Enable Export Configuration	**1** Mark the checkbox if you want to export the Dashboard as a daily report. **2** Click **Next**. **3** Enter a report title.
Apply this Export Configuration for	Specify to apply the Export configuration for NEs: ■ To apply the export to all available NEs, select **All**. ■ To apply the export for the NE for which the dashboard is displayed, select **Selected**. ■ To select a set of NE for which the export is applied, select **Associate**.: **1** Click **Next**. **2** To select an NE, highlight it in the **Available List** and click the right-arrow to move it to the **Assigned List**. To remove a selected NE, highlight it in the **Assigned List** and click the left-arrow to move it to the **Available List**.

6 Click **Save**.

By default, Acuitas purges any file older than 30 days. To configure a different purge interval, see Configuring Export Purge Interval.

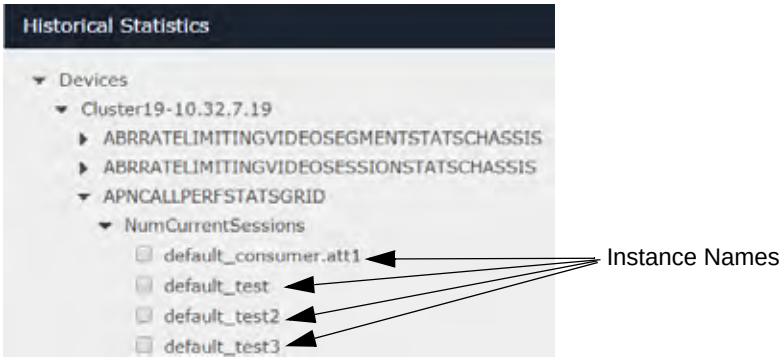
If you marked the **Enable Export Configuration** checkbox to export the dashboard, the export filename is *<Entity Name>_<Dashboard Title>_<Report Title>_<Date>*.csv. The file is exported to the Acuitas server, in the directory */opt/Affirmed/NMS/server/ems/archive/<Date>/*.

Keep in mind that if the dashboard you export has the **Show** setting set to Top x or Bottom x, the highest or lowest devices in the CSV file may differ from the devices shown when you run the dashboard in real time. The difference results because the exported files contain data from the previous full day whereas the real time data uses data from the previous 24 hours. Depending on the actual time at which you view the real time dashboard, the highest or lowest devices may differ between the export data and the real time dashboard display.

Using the Dashboard Filter Manager to Filter Records

You can use the Dashboard Filter Manager to create a filter based on specific parameters, values, and conditions.

For example, you can create a filter of particular object instance(s), such as APN instances. The object instance name is the string displayed in the Historical Statistics screen. In the left panel, expand the device, statistics table name, and metric to view the instances names.



To create a Dashboard filter:

1. In the **Dashboard Editor** window, click the Filter icon.

   Acuitas displays the Dashboard Filter Manager screen.

2. Click the **New Filter** icon.
3. In the **Add Filter** dialog, enter the Filter Name and click **Add**. A filter with that name is created.
4. In the **Filter Manager**, select the filter and click the **Add Condition** icon:
5. Complete the Conditions fields by selecting appropriate values for **Parameter**, **Operator**, and **Value**. In the Value field, you can use the % character as a wildcard symbol in any position and multiple times, *except* when using the Equals or Not Equals Operators. Value matching *is not* case sensitive.

   For example, to create a filter of particular object instance(s), select **Parameter** = Instance, **Operator** = Equals, Not Equals, Contains, Starts with, or Ends with, and **Value** = a string in the object instance name(s).

   - **Operator** = Equals and **Value** = a string. The filter matches any instance with the values in the specified order.
   - **Operator** = Not Equals and **Value** = a string. The filter excludes any instance with the values in the specified order.
   - **Operator** = Contains and **Value** = a string. The filter matches any instance containing the specified values.

- **Operator** = Starts with and **Value** = a string. The filter matches any instance with the values starting with the values in the specified order.
- **Operator** = Ends with and **Value** = a string. The filter matches any instance with the values ending with the values in the specified order.

6 Click **Apply**.

7 To add additional Conditions, repeat step 4 through step 6. Specify **Condition** = AND or OR.

8 If the filter needs a combination of AND and OR conditions to achieve the desired result:

a In the **Filter Manager**, select the filter and click the **Create AND group** icon (or **Create OR Group** icon).

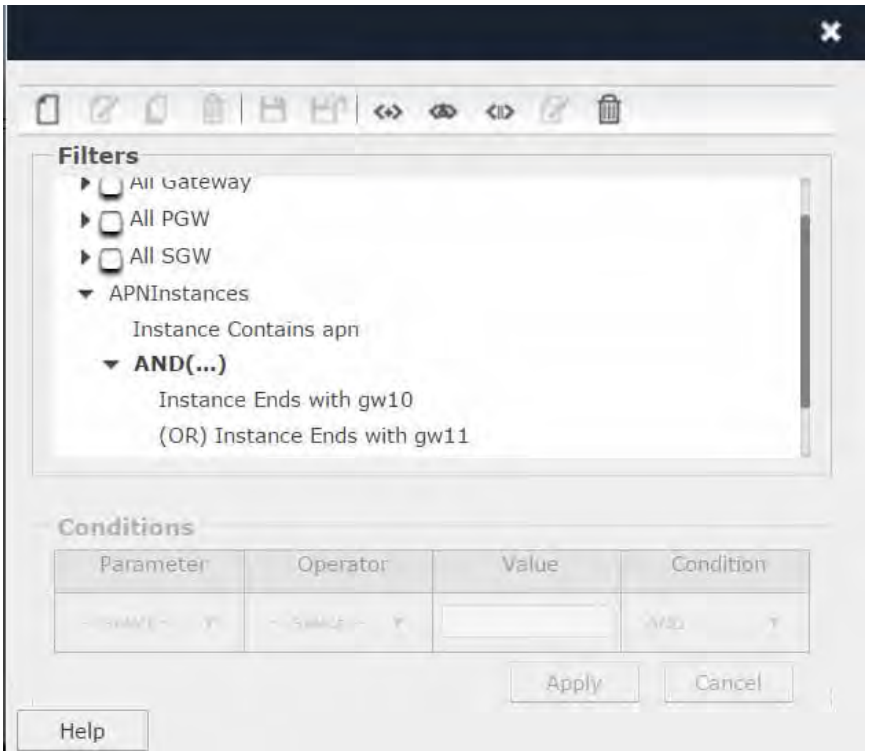
b In the **Filter Manager**, select the AND... (or OR...) group and click the **Add Condition** icon and complete the Conditions for the group.

c Click **Apply**.

9 Click the **Save Filter** icon.

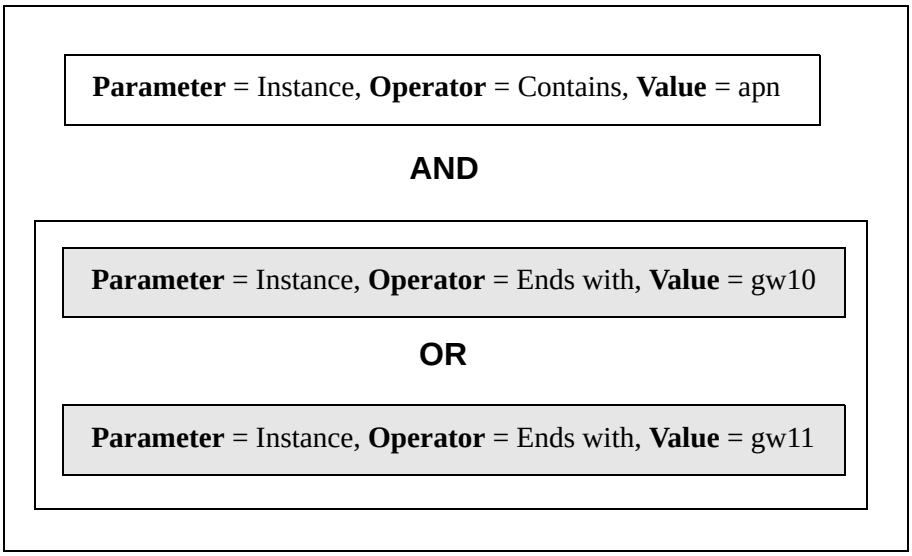
The following example creates a filter of APN instances (filter name **APNInstances**).

Figure 5-19 Dashboard Filter Manager



The Conditions are as follows:

Figure 5-20 Filter Conditions



This filter would filter on the highlighted instances in the following list:

default_apn_gw10

default_apn_gw11

default_apn_gw12

default_pgw_gw10

default_pgw_gw11

default_pgw_gw12

Example Dashboards

The following examples illustrate how to use the Dashboard configuration fields.

Example 1: Top 5 Protocols for Protocol Network Usage (Mbps)

Configure the Dashboard parameters as follows:

- **Metrics**: Select **DPI - Protocol Network Usage (Mbps)**.
- **Chart**: Select the chart type (Pie, Bar, or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **Top 5**.
- **Filter By**: Select **All**.
- **Group By**: Select **Protocol**.

Example 2: Top 5 Protocols Categories for % Protocol Network Usage

Configure the Dashboard parameters as follows:

- **Metrics**: Select **DPI - % Protocol Network Usage**.
- **Chart**: Select the chart type (Bar or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **Top 5**.
- **Filter By**: Select **All**.
- **Group By**: Select **Category**.

Example 3: Top 5 Protocols for a Specific Category for % Protocol Network Usage

Configure the Dashboard parameters as follows:

- **Metrics**: Select **DPI - % Protocol Network Usage**.
- **Chart**: Select the chart type (Bar or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **Top 5**.
- **Filter By**: Select a pre-configured filter with the conditions Category Equals <***Specific Category***>
- **Group By**: Select **Protocol**.

Example 4: Top 10 Applications for % Application Network Usage

Configure the Dashboard parameters as follows:

- **Metrics**: Select **DPI - % Application Network Usage**.
- **Chart**: Select the chart type (Bar or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **Top 10**.
- **Filter By**: Select **All**.
- **Group By**: Select **Application**.

Example 5: Top 10 Applications for Application Network Usage (Mbps)

Configure the Dashboard parameters as follows:

- **Metrics**: Select **DPI - Application Network Usage (Mbps)**.
- **Chart**: Select the chart type (Pie, Bar, or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **Top 10**.
- **Filter By**: Select **All**.
- **Group By**: Select **Application**.

Example 6: Individual QCI/ARP Statistics at the Cluster-level

Configure the Dashboard parameters as follows:

- **Metrics**:
  - For raw statistics, select metric table name **EMSGWAPNQCIARPSTATS** or **EMSGWQCIARPSTATS**.

    Select the individual metric you want to view.
  - For derived statistics, select metric table name **DERIVEDSTATS**.

    In the Filter field, enter **qci/arp** and click the **Search** icon.

    Select the individual metric you want to view.
- **Chart**: Select the chart type (Pie, Bar, or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **All**.
- **Aggregate Type**: Select **Avg**.
- **Filter By**: Select **All Gateway** to show statistics for all gateway types.
- **Group By**: Select **QCI/ARP**.

Example 7: Individual APN Statistics at the Cluster-level

Configure the Dashboard parameters as follows:

- **Metrics**:
  - For raw statistics, select metric table name **EMSGWAPNQCIARPSTATS** or **EMSGWQCIARPSTATS**.

    Select the individual metric you want to view.
  - For derived statistics, select metric table name **DERIVEDSTATS**.

    In the Filter field, enter **qci/arp** and click the **Search** icon.

    Select the individual metric you want to view.
- **Chart**: Select the chart type (Pie, Bar, or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **All**.
- **Aggregate Type**: Select **Avg**.
- **Filter By**: Select **All Gateway** to show statistics for all gateway types.
- **Group By**: Select **APN**.

Example 8: Individual PGW Statistics at the Cluster-level

Configure the Dashboard parameters as follows:

- **Metrics**:
  - For raw statistics, select metric table name **EMSGWAPNQCIARPSTATS** or **EMSGWQCIARPSTATS**.

    Select the individual metric you want to view.
  - For derived statistics, select metric table name **DERIVEDSTATS**.

    In the Filter field, enter **qci/arp** and click the **Search** icon.

    Select the individual metric you want to view.
- **Chart**: Select the chart type (Pie, Bar, or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **All**.
- **Aggregate Type**: Select **Avg**.
- **Filter By**: Select **All PGW**.
- **Group By**: Select **Gateway**.

Example 9: Aggregated PGW Statistics at the Cluster-level

Configure the Dashboard parameters as follows:

- **Metrics**:
  - For raw statistics, select metric table name **EMSGWAPNQCIARPSTATS** or **EMSGWQCIARPSTATS**.

    Select the individual metric you want to view.
  - For derived statistics, select metric table name **DERIVEDSTATS**.

    In the Filter field, enter **qci/arp** and click the **Search** icon.

    Select the individual metric you want to view.
- **Chart**: Select the chart type (Pie, Bar, or Line).
- **Interval**: Select the historical time interval you want for the chart.
- **Show**: Select **All**.
- **Aggregate Type**: Select **Avg**.
- **Filter By**: Select **All PGW**.
- **Group By**: Select **Resource**.

Exporting KPI Data from the Dashboard

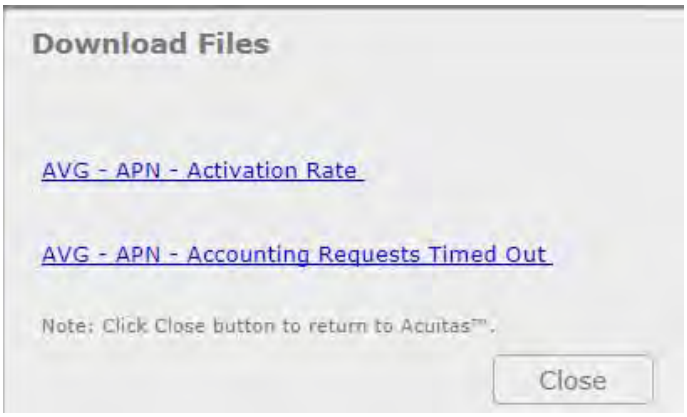
You can save KPI data as textual data or graphical data.

Note: *To export KPI data from the dashboard, you must have the Performance > PM Stats > View Dashboard security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To save KPI data as textual data:

1. Click the **PM Dashboard** tab.
2. On the tool bar of the Dashboard, click the icon of the required file format:
   - **Export as Table PDF** icon
   - **Export as Table CSV** icon

   Acuitas displays the **Download Files** window listing the individual data files.



3. Right-click in the open file and select **Save Link As**.
4. Specify where you want the file saved and click **Save**.
5. From the **Download File**s window, click **Close**.

To save KPI data as graphical data:

1. Click the **PM Dashboard** tab.
2. Click the **Export as Chart PDF** icon on the tool bar of the Dashboard.
3. Acuitas displays the **Download Files** window.
4. Click **Download PDF File**.

5 Right-click in the open file and select **Save Link As**.

6 Specify where you want the file saved and click **Save**.

7 From the **Download File**s window, click **Close**.

Chapter 6

VNF Manager

The Virtual Network Function (VNF) Manager allows you to perform full life-cycle management of clusters. You can use the VNF Manager to:

Commission Clusters:

- **MCC Clusters:** Automate deployment of MCC clusters in the following systems:
  - HP BladeSystem c7000 multi-chassis, 16-blade/32-VM deployment (two VMs per blade)
  - HP ProLiant DL380 Gen9 Server

  MCC cluster commissioning interoperates with VMware vCenter, vCloud Director, or OpenStack to perform the following function:
  - Upload software images
  - Instantiate MCC cluster
  - Configure MCC cluster for service
- **MCC MME Clusters:** Automate deployment of MCC MME clusters.

  MCC MME cluster commissioning interoperates with OpenStack to perform the following function:
  - Upload software images
  - Instantiate MCC MME cluster
  - Configure MCC MME cluster for service

Monitor Clusters:

- Monitor capacity utilization of MCC clusters (*MCC Clusters Only*)
- Report on network elasticity for:
  - Life-cycle management events, including cluster instantiation, scale out/scale in, and termination.
  - Conditions leading to dynamic scale out/scale in events

- Report on network inventory for:
  - Clusters and their nodes
  - Blade Systems and their blades
  - Server Groups and their servers
  - Hosting relationships between nodes and blades

Scale Out/Scale In Clusters:

- Scale out/scale in network capacity by creating and removing virtual machines (VMs) within a cluster. This process can be performed in the following ways:
  - Manually when initiated by an Operator
  - Dynamically when the capacity is overloaded/underloaded as determined by an associated policy (*MCC Clusters Only*)
  - Programmatically through the VNF Manager and Provisioning API, which is a representational state transfer (REST)-based API

Prerequisites

Prior to using the Virtual Network Function (VNF) Manager, perform these prerequisites.

vCenter Requirements

If you use vCenter, perform the prerequisites in this section.

Install Acuitas Packages for VMware

To install Acuitas packages for VMware:

1. Log into the Acuitas server as `root`.
2. Issue the following commands to untar the package tarball:

```
cd /opt/Affirmed/NMS/ctool
tar -zxvf ./acuitas-commission-tool.tar.gz
```

3. Issue the following commands to install the package:

```
cd acuitas-commission-tool
./install.sh
```

4. Accept the VMware license agreement.
5. When prompted to install the RedHat pre-built packages, enter **yes**.
6. Issue the following command to remove the acuitas-commission-tool directory created by the tar command:

```
cd ..; rm –rf acuitas-commission-tool
```

Adding Host Resolution Information in /etc/hosts

When hosts are identified by their names in vCenter, the VNF Manager must be able to resolve the host names to their IP addresses. The solution is to add IP address and hostname to the Acuitas /etc/hosts file.

Importing the vCenter Certificate

For Acuitas to communicate with vCenter, follow this procedure to import the vCenter Certificate prior to starting the Acuitas server. This procedure exports the vCenter certificate from a Firefox Browser and imports the same certificate into Acuitas.

To import the vCenter certificate into the keystore:

1. Log into the vCenter web interface at the vCenter IP address with the Firefox browser.
2. Download the vCenter certificate from the Certificate Manager of your browser. For example, if you are using Firefox, select **Options** > **Advanced** > **Certificates** > **View Certificate**.
3. Place the downloaded certificate in */opt/Affirmed/NMS/jre/bin* on the Acuitas machine.
4. Issue the following commands to import the certificate (in this case, 10.10.10.10.crt).

   ```
   cd /opt/Affirmed/NMS/jre/bin
   ```

   ```
   ./keytool -import -noprompt -trustcacerts -alias <vCenter IP address>
   -file 10.10.10.10.crt -keystore
   /opt/Affirmed/NMS/server/ems/resources/.keystore -storepass <keystore
   password>
   ```

   Contact the Affirmed Networks Technical Assistance Center (TAC) for the keystore password.
5. Issue the following command to verify that the certificate is installed:

   ```
   ./keytool -storetype JCEKS -storepass <keystore password> -keystore
   /opt/Affirmed/NMS/server/ems/resources/.keystore  -list
   ```

Adding the vCenter Network Element

To add a vCenter network element:

1. Use any of the following methods to add a vCenter network element:

   Settings icon on the toolbar: Select **Topology => Add Element**.

   Pop-up menu: Right-click an object in the tree and click **Add Element**.

   Acuitas displays the **Add Network Element** window.
2. Configure the parameters as follows:

Table 6-1 Add Network Element Parameters

Parameter	Description
Device Type	Select the device type: ■ VIM
General Details	

Table 6-1 Add Network Element Parameters

Parameter	Description
IP Version	Select IPv4 or IPv6.
IP Address	Enter the IP address of the vCenter server.
Name	Enter the display name of the network element.
Description	Enter the description of the network element.
File Server	Select the file server.
VIM Protocol Details	
Type	Select the VIM type: ■ vCenter
User Name	Enter the username. Such as, administrator@vsphere.local.
Password/Confirm Password	Enter the password for the user.
FQDN	The vCenter certificate is generated based on a Fully Qualified Domain Name. You must enter it so that Acuitas can access the vCenter server.
Location Details Enter the Address of the network element.	

3 Click **Save**.

4 At the confirmation prompt, click **OK**.

Note: *You cannot delete a vCenter Network Element if hosts from it are managed by VNF Manager. For instructions on unmanaging the hosts, see* *vCenter Only: Unmanaging a Host**.*

Requirement to Install ovatools to Enable Features

For VNF Manager to support various features for vCenter deployment of MCC 8.1 and later releases, a separate administrative step must be performed to install ovatools. The features and the required ovatools versions are:

Feature	MCC Version	ovatools Version
General	All	ovatools-1.3.1
Base Routability and EW L3 Connectivity	MCC 8.1 and later	ovatools-1.3.3
Automatic SCSI Configuration Base Routability and EW L3 Connectivity	MCC 8.4	ovatools-1.3.4

To install ovatools:

1 As `root`, issue the following commands:

```
cd /opt/Affirmed/NMS/ctool/acuitas-commission-tool
./install ovatools-<version>
```

vCloud Director Requirements

If you use vCloud Director, perform the prerequisites in this section.

Importing the vCloud Director Certificate

For Acuitas to communicate with vCloud Director, follow this procedure to import the vCloud Director Certificate.

To import the vCloud Director certificate into the keystore:

1. Log into the vCloud Director web interface at the vCloud Director IP address with the Firefox browser.
2. Download the vCloud certificate from the Certificate Manager of your browser. For example, if you are using Firefox, select **Options** > **Advanced** > **Certificates** > **View Certificate**.
3. Place the downloaded certificate in */opt/Affirmed/NMS/jre/bin* on the Acuitas machine.
4. Issue the following commands to import the certificate (in this case, 10.10.10.10.crt).

   ```
   cd /opt/Affirmed/NMS/jre/bin
   ```

   ```
   ./keytool -import -noprompt -trustcacerts -alias <vCloud Director IP address> -file 10.10.10.10.crt -keystore /opt/Affirmed/NMS/server/ems/resources/.keystore -storepass <keystore password>
   ```

   Contact the Affirmed Networks Technical Assistance Center (TAC) for the keystore password.
5. Issue the following command to verify that the certificate is installed:

   ```
   ./keytool -storetype JCEKS -storepass <keystore password> -keystore /opt/Affirmed/NMS/server/ems/resources/.keystore  -list
   ```

Adding the vCloud Director Network Element

To add a vCloud Director network element:

1. Use any of the following methods to add a vCloud Director network element:

   Settings icon on the toolbar: Select **Topology => Add Element**.

   Pop-up menu: Right-click an object in the tree and click **Add Element**.

   Acuitas displays the **Add Network Element** window.
2. Configure the parameters as follows:

Table 6-2 Add Network Element Parameters

Parameter	Description
Device Type	Select the device type: ■ VIM
General Details	
IP Version	Select IPv4 or IPv6.
IP Address	Enter the IP address of the vCloud Director server.
Name	Enter the display name of the network element.
Description	Enter the description of the network element.
File Server	Select the file server.
VIM Protocol Details	
Type	Select the VIM type: ■ vCloudDirector
Connection URL	Set the parameter to match the vCloud Director connection URL. For example, https://172.18.255.204
Organization Name	Enter the vCloud Director organization name.
User Name	Enter the vCloud Director Organization login name.
Password/Confirm Password	Enter the password for the user.
Admin User Name	Enter the user name for the vCloud Director account with vCloud Director system administration privileges. This account is used by the VNF Manager to retrieve host information for the instantiated VMs.
Admin Password/Confirm Password	Enter the password for the vCloud Director account with vCloud Director system administration privileges.
Location Details Enter the Address of the network element.	

3 Click **Save**.

4 At the confirmation prompt, click **OK**.

Note: *You cannot delete a vCloud Network Element if Organization vDCs from it are managed by VNF Manager. For instructions on unmanaging the Organization vDCs, see vCloud Director Only: Managing Organization vDCs.*

VNF Manager Support for Managing Anti-affinity Rule

VNF Manager automatically manages anti-affinity rules in vCloud Director during the life-cycle management of the MCC cluster. The anti-affinity rules instruct vCloud Director to not co-host the same type (mcm, csm, or ssm) of MCC node.

The anti-affinity rules are named as follows:

`<vApp Name>-<VM Type>-anti-affinity`

where <*VM Type*> is mcm, csm, or ssm.

For example:

mcc-16-mcm-anti-affinity

OpenStack Requirements

If you use OpenStack as your Virtual Infrastructure Manager, perform the prerequisites in this section. The Acuitas VNF Manager supports the following OpenStack versions:

- RedHat: Kilo, Liberty, Mitaka, Newton
- Ubuntu: Liberty

Preconfiguration Requirements for OpenStack

The following items must be previously configured by OpenStack administrator as prerequisites:

VNF Manager Access

Grant the VNF Manager access to the OpenStack platform via the OpenStack REST APIs.

Required Images

Upload required images:

- For MCC, you must upload both controller and payload images for a specific version with the following file naming convention:

  an-<*version*>-<*point*>.REL-<controller | payload>

  For example:

  an-6.1.2.0-110.REL-controller

  an-6.1.2.0-110.REL-payload

- For MCC MME, it is recommended that you upload its image with the following naming convention:

  an-mme-<*version*>

nova Flavor Instances

Create the nova Flavor instances for each VM personality/type:

- For MCC, it is recommended that you use the following flavor naming convention:

  AN-<*personality*>-<*additional information*>

  where <*personality*> is one of ASM | CCM | CPM | DCM | IOM | MCM | SSM | WSM | ISM | IWM.

  For example:

  AN-CCM-20g

- For MCC MME, you use the following flavor naming conventions:

  AN-<*type*>-<*additional information*>

  where <*type*> is one of MGMT | RM | CALLP | SIG | LB | DATA | EDP.

  For example:

  AN-MGMT-Generic

Required Networks

Create Management, Base, East/West and North/South networks. It is recommended that you use the following network naming convention:

AN<*additional information*>

For example:

AN-MGMT

AN-Base1

nova Scheduling

Enable ServerGroupAntiAffinityFilter for nova scheduling. To do so, add `ServerGroupAntiAffinityFilter` to the `scheduler_default_filters` line in `/etc/nova/nova.conf` on the host that runs the `nova-scheduler`.

For example:

```
scheduler_default_filters=RetryFilter,AvailabilityZoneFilter,RamFilter
,ComputeFilter,ComputeCapabilitiesFilter,ImagePropertiesFilter,CoreFil
ter,ServerGroupAntiAffinityFilter
```

Server Groups

Create server groups with an anti-affinity policy if needed:

```
nova server-group-create --policy anti-affinity
an-mcc-ssm-anti-affinity
```

It is recommended that you use the following server group naming convention:

an-<*additional information*>

For example:

an-mcc-ssm-anti-affinity

Typically MCM, SSM, and CSM server groups are created as such for MCC.

Security Group Instance

Create Security Group instance

Availability Zone Instances

Create Availability Zone instances according to network deployment needs.

Importing the SSL Certificate

For Acuitas to communicate with Identity Service REST API v3 over HTTPS, follow this procedure to import the SSL Certificate.

To import the SSL certificate into the keystore:

1. Log into the OpenStack Horizon web interface at the Identity Service IP address with the Firefox browser.
2. Download the SSL certificate from the Certificate Manager of the Firefox browser by selecting **Options** > **Advanced** > **Certificates** > **View Certificate**.
3. Place the downloaded certificate in */opt/Affirmed/NMS/jre/bin* on the Acuitas machine.
4. Issue the following commands to import the certificate (in this case, 10.10.10.10.crt).

   ```
   cd /opt/Affirmed/NMS/jre/bin
   ```

   ```
   ./keytool -import -noprompt -trustcacerts -alias <Identity Service IP address> -file 10.10.10.10.crt -keystore /opt/Affirmed/NMS/server/ems/resources/.keystore -storepass <keystore password>
   ```

   Contact the Affirmed Networks Technical Assistance Center (TAC) for the keystore password.
5. Issue the following command to verify that the certificate is installed:

   ```
   ./keytool -storetype JCEKS -storepass <keystore password> -keystore /opt/Affirmed/NMS/server/ems/resources/.keystore  -list
   ```

Adding the OpenStack Network Element

To add an OpenStack network element:

1. Use any of the following methods to add an OpenStack network element:

   Settings icon on the toolbar: Select **Topology => Add Element**.

   Pop-up menu: Right-click an object in the tree and click **Add Element**.

   Acuitas displays the **Add Network Element** window.
2. Configure the parameters as follows:

Table 6-3 Add Network Element Parameters

Parameter	Description
Device Type	Select the device type: ■ VIM
General Details	
IP Version	Select IPv4 or IPv6.
IP Address	Enter the IP address of the OpenStack controller.
Name	Enter the display name of the network element.
Description	Enter the description of the network element.
File Server	Select the file server.
VIM Protocol Details	
Type	Select the VIM type: ■ OpenStack
User Name	Enter the username.
Password/Confirm Password	Enter the password for the user.
Identity Service Endpoint	Enter the Identity Service Endpoint, such as http://127.0.0.1:5000/v2.0 for REST API v2, or https://identity.affirmed.com:443/identity/v3 for REST API v3
Project/Tenant Name	Enter the OpenStack tenant (project)
Domain Name	Enter the Domain name. *Required for REST API v3.*
Location Details Enter the Address of the network element.	

3 Click **Save**.

4 At the confirmation prompt, click **OK**.

Note: *You cannot delete an OpenStack Network Element if Availability Zones from it are managed by VNF Manager. For instructions on unmanaging the Availability Zones, see* *OpenStack Only: Managing Availability Zones**.*

Configuring Hosts

Perform the appropriate steps for your scenario:

- **If the cluster is a server group:** Configure the servers in the group (configure each server's IP address for which Acuitas should collect traps). See Configuring Servers in a Group.
- **If the cluster is a blade system:** Configure each blade with an IP address for which Acuitas should collect traps. See Configuring Blade IP Addresses.

Configuring Servers in a Group

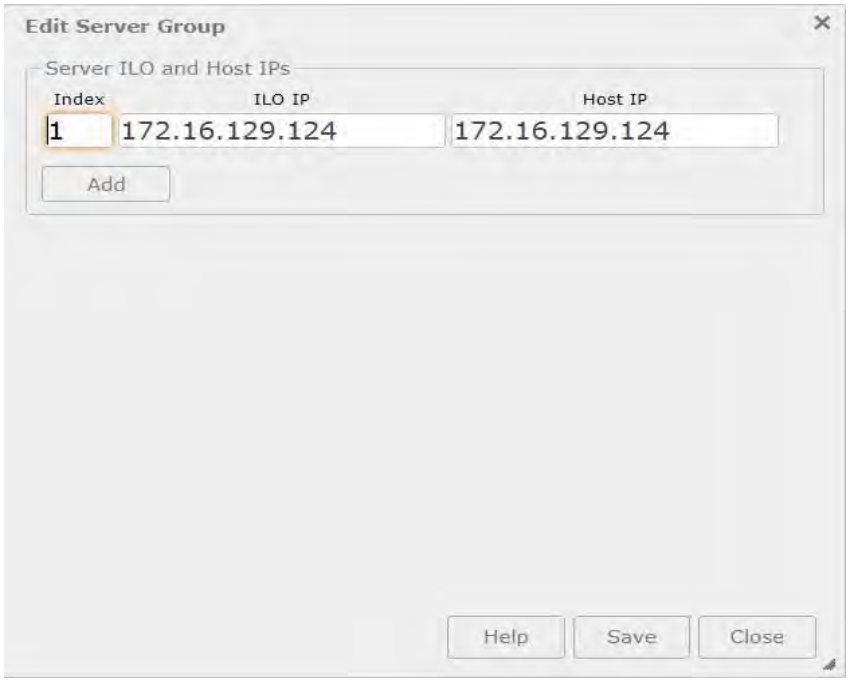
For an NE that is a server group, you need to configure each server's IP address for which Acuitas should collect traps.

To configure servers in a group:

1 Use the following method to configure the servers in a group:

Pop-up menu: Right-click the server group and click **Configure Server**.

Figure 6-1 Configure Server Screen



2 For each server in the group, enter the index, the iLO IP address, and the Host IP address to which Acuitas should collect traps and click **Add**.

In the case of OpenStack, issue the following commands on the OpenStack CLI to find the Hypervisor IP Addresses:

a Issue the following command to list the Hypervisor hostnames:

```
nova hypervisor-list
```

b Issue the following command to find the host IP for a Hypervisor:

```
nova hypervisor-show <hypervisor hostname>
```

3 Click **Save**.

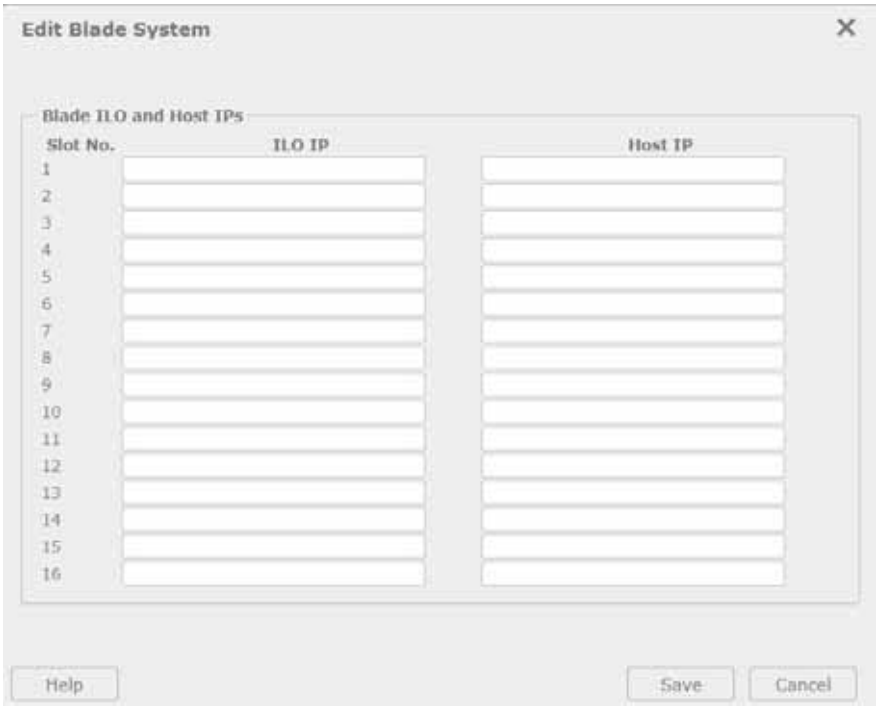
Note: *In addition to this procedure, you need to configure the Acuitas server IP address as an SNMP trap destination on each server in the group.*

Configuring Blade IP Addresses

For a cluster that is a blade system, you need to configure each blade with an IP address for which Acuitas should collect traps.

To configure blade IP addresses:

1 In the Network View, right-click the blade system and click **Configure Blades**.



2 For each slot, enter the blade iLO IP address and the Host IP address to which Acuitas should collect traps.

3 Click **Save**.

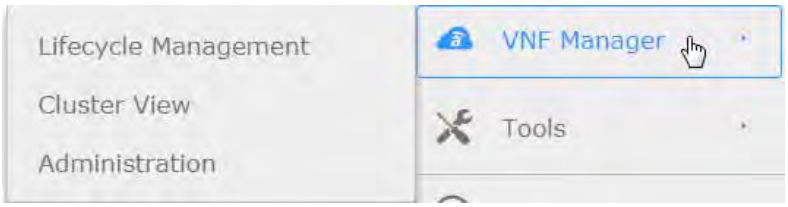
Administering the VNF Manager

To use the Virtual Network Function (VNF) Manager to scale out/scale in a cluster to dynamically adapt to needs of network capacity and throughput, you first need to administer the system.

To access VNF Manager administration, select the applicable VNF Manager option from the **Settings** icon on the toolbar.

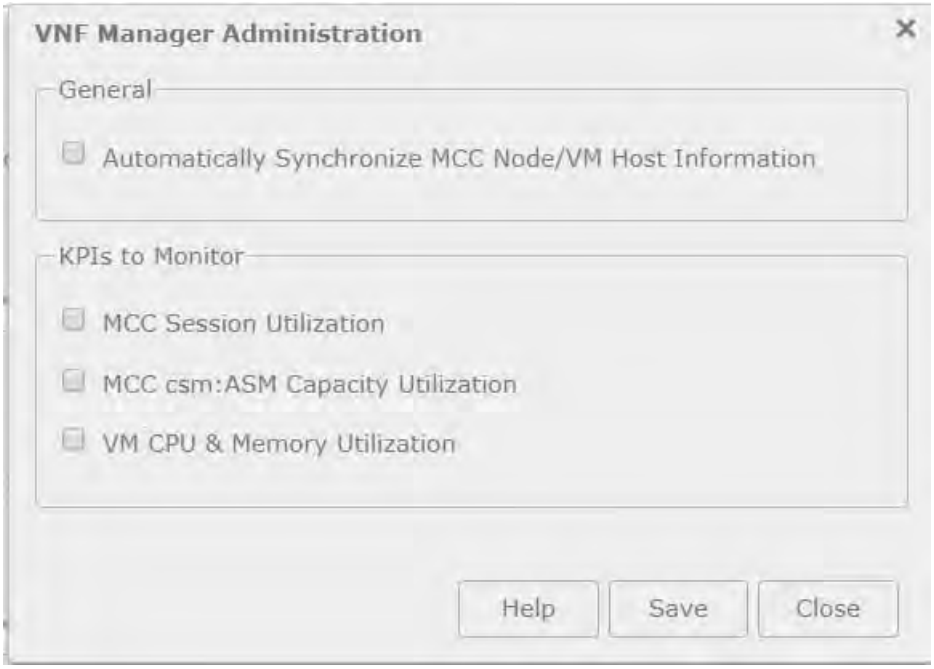
Note: *To access the VNF Manager administration, you must have the EMS Management > VNF Manager > Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

Figure 6-2 Accessing VNF Manager Application



The VNF Manager displays the **VNF Manager Administration** window, listing the configuration settings.

Figure 6-3 VNF Manager Administration



1 Configure the parameters as follows:

Table 6-4 VNF Manager Administration Parameters

Parameter	Description
Automatically Synchronize MCC Node/VM Host Information	Mark the checkbox to enable automatically synchronizing of MCC node hosting information (the Blade, IP Address, VM IP Address, and VM Name fields on MCC's node object). When enabled, VNF Manager performs synchronization only when it can locate the VM hosting information in its database. If VNF Manager fails to obtain the VM hosting information from its database, no configuration is made in Blade and IP Address fields.
KPIs to Monitor	Mark the checkboxes for the Key Performance Indicators you want monitored for an MCC cluster. For details, see Viewing Key Performance Indicators.

2 Click **Save**.

Commissioning Clusters

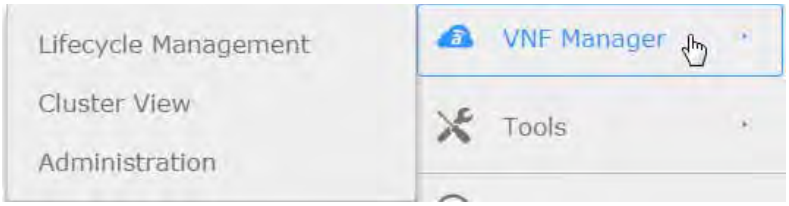
You can use the VNF Manager to commission MCC clusters and MCC MME clusters. Each cluster is defined either by:

- Inputing required information into the VNF Manager graphical user interface.
- Importing a CSV file containing the required information into the VNF Manager.

To use the Virtual Network Function (VNF) Manager to commission a cluster, select the **VNF Manager** > **Lifecycle Management** option from the **Settings** icon on the toolbar.

Note: *To access the VNF Manager application, you must have the EMS Management > VNF Manager > Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

Figure 6-4 Accessing VNF Manager Application



The VNF Manager displays the **Cluster** window.

To change the screen background color (dark or light):

1 Click the **Settings** icon on the toolbar and select **Change Theme**.

To commission a cluster, perform these tasks in the following order:

- vCenter Only: Uploading Open Virtualization Archive (OVA) Packages
- vCenter Only: Discovering and Configuring Hosts
- OpenStack Only: Managing Availability Zones
- vCloud Director Only: Managing Organization vDCs
- Configuring a Cluster with a CSV File (*skip if you intend to input the required information into the VNF Manager graphical user interface instead of from a imported CSV file*)
- Cluster-Level Configuration (*this procedure is not required if you intend to import a CSV file containing the configuration information*)
- Configuring Nodes in the Cluster
- Validating Cluster Configuration
- Instantiating the Cluster

vCenter Only: Uploading Open Virtualization Archive (OVA) Packages

You can upload OVA packages and apply them to a cluster.

To upload OVA packages:

1. Copy the OVA files for MCM, CSM, and SSM to /data/ova. You must use the OVA file naming convention:

   an-<*version*>-<*point*>.REL_<*VM Type*>-<*additional information*>.ova

   For example:

   an-7.3.3.0-353.REL_CSM-C8.M32768.ova

2. From the **Cluster** window, select a Virtualized Infrastructure Manager (VIM) in the right pane.

3. Click the **Manage Templates** icon in the right pane .

   The VNF Manager lists the OVA files in data/ova.

4. In the **Manage OVA Template** screen, click the **Add OVA Template** icon.
5. Select the OVA template you want to upload.
6. Click **Add**.

Once the OVA is uploaded, VNF Manager injects property metadata into the OVA so that it can be used by vCenter. VNF Manager renames the file and places it in /opt/Affirmed/NMS/ova. The name of the modified OVA is:

an-<*version*>-<*point*>.REL_<*VM Type*>-<*additional information*>props.ova

For example:

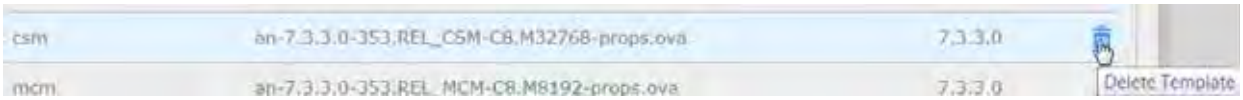
an-7.3.3.0-353.REL_CSM-C8.M32768.props.ova

You can specify the OVA when commissioning the cluster.

Deleting an Uploaded OVA package

To delete an uploaded OVA package:

1. From the **Cluster** window, select a Virtualized Infrastructure Manager (VIM) in the right pane.
2. Click the **Manage Templates** icon in the right pane .
3. In the **Manage OVA Template** screen, select the instance and click the **Delete Template** icon.



4. At the confirmation prompt, click **Yes**.

   VNF Manager removes the OVA file from storage.
5. In the **Manage OVA Template** screen, click **Close**.

OpenStack and vCloud Director Only: Viewing VIM Configuration

To view VIM configuration:

1. From the **Cluster** window, select an OpenStack or vCloud Director Virtualized Infrastructure Manager (VIM) in the right pane.
2. Click the **View VIM Configuration** icon in the right pane .

   VNF Manager lists the VIM configuration prerequisites.
3. To close the **Configuration Prerequisites** screen, click **Close**.

OpenStack Only: Managing Availability Zones

You configure OpenStack Availability Zones to be managed by a Virtualized Infrastructure Manager (VIM).

To manage Availability Zones:

1. From the **Cluster** window, select an OpenStack Virtualized Infrastructure Manager (VIM) in the right pane.
2. Expand **Availability Zones** in the right pane.
3. Click the **Add Managed Availability Zones** icon in the right pane.

   In the **Managed Availability Zones** screen, the VNF Manager lists the Availability Zones.
4. Mark the **Is Managed** checkbox for each Availability Zone you want to be managed by the Virtualized Infrastructure Manager (VIM).
5. Click **Save**.

   VNF Manager lists the Availability Zones in the right pane.

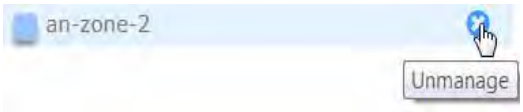
   Once an Availability Zone is configured to be managed by the VNF Manager, you can apply it to a cluster.

To unmanage an Availability Zone:

Note: *You must unmanage the Availability Zones managed by a VIM before you can delete that OpenStack Network Element.*

---

1. From the **Cluster** window, select an OpenStack Virtualized Infrastructure Manager (VIM) in the right pane.
2. Expand **Availability Zones** in the right pane.
3. In the **Availability Zone** list, select the instance and click the **Unmanage** icon.



4. At the confirmation prompt, click **Yes**.

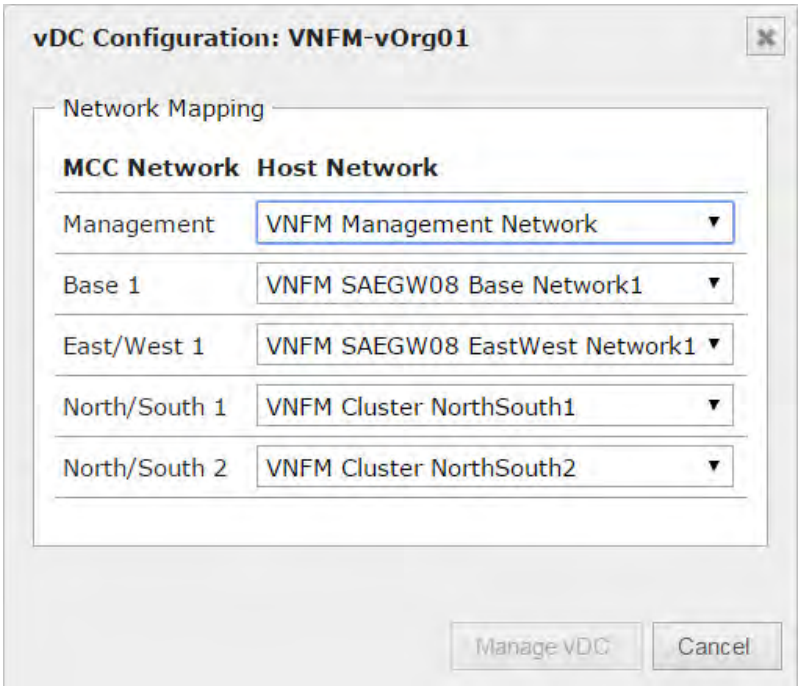
vCloud Director Only: Managing Organization vDCs

You configure vCloud Director Organization Virtual Data Centers to be managed by a Virtualized Infrastructure Manager (VIM).

To manage Organization vDCs:

1. From the **Cluster** window, select a vCloud Director Virtualized Infrastructure Manager (VIM) in the right pane.
2. Expand **Organization vDCs** in the right pane.
3. Click the **Add Organization vDCs** icon in the right pane.

   In the **Managed vDCs** screen, the VNF Manager lists the Organization vDCs.
4. Click the Organization vDC you want to be managed by the Virtualized Infrastructure Manager (VIM).
5. Make any changes to the Network Mapping of the Organization vDC.



6. Click **Manage vDC**.

   VNF Manager lists the Organization vDC in the right pane.

   Once an Organization vDC is configured to be managed by the VNF Manager, it can be used to deploy VMs for clusters.

To unmanage an Organization vDC:

Note: *You must unmanage the Organization vDC managed by a VIM before you can delete that vCloud Director Network Element.*

---

1. From the **Cluster** window, select a vCloud Director Virtualized Infrastructure Manager (VIM) in the right pane.
2. Expand **Organization vDCs** in the right pane.
3. In the **Organization vDCs** list, select the instance and click the **Unmanage** icon.

4. At the confirmation prompt, click **Yes**.

vCenter Only: Discovering and Configuring Hosts

You discover vCenter hosts managed by a Virtualized Infrastructure Manager (VIM) and configure them so that VNF Manager can place Virtual Machine (VM) on them.

To discover and configure hosts:

1. From the **Cluster** window, select a vCenter Virtualized Infrastructure Manager (VIM) in the right pane.
2. Expand **Hosts** in the right pane.

   VNF Manager lists the discovered hosts.

vCenter Only: Adding a Managed Host

To add a vCenter managed host:

1. To add a vCenter managed host, click the **Add Managed Hosts** icon in the right pane.
2. In the **Manage Hosts** screen, select a Datacenter.
3. To limit the search, either:
   - Mark the Name/IP button and enter the host name(s) or IP address(es). Separate each with a comma.
   - Mark the Folder Name button and enter a single Folder name.

   Click the **Search Hosts** icon.

   Or, leave the fields blank to search for all available hosts.

   VNF Manager lists the available Hosts.
4. Click a host in the list to configure it.
5. Configure the parameters as follows:

Table 6-5 Manage Host Parameters

Parameter	Description
Host Username	For root user access to the host, enter `root`. For non-root user access to the host, enter the username. You must also provide the Host Password. VNF Manager uses the username and password during cluster deployment.
Host Password	For root user access to the host, the Host Password is optional. For non-root user access to the host, the Host Password is required. VNF Manager uses the username and password during cluster deployment.

Table 6-5 Manage Host Parameters

Parameter	Description
Storage > Reserve Storage for VM	Mark the button for the datastore you want to reserve to create the VM.
Network Mapping	For each host network, select from the list of network types: ■ Management ■ Base 1 ■ Base 2 ■ East/West 1 ■ East/West 2 ■ North/South 1 ■ North/South 2

6 Click **Manage Host**.

7 In the **Manage Hosts** screen, click **Close**.

Once a host is successfully discovered and configured to be managed by the VNF Manager, you can apply it to a cluster.

vCenter Only: Viewing Host Configuration

To view host configuration:

1 From the **Cluster** window, select a Virtualized Infrastructure Manager (VIM) in the right pane.

2 Expand **Hosts** in the right pane.

VNF Manager lists those managed by the VNF Manager.

3 To view a managed host's configuration, click the host's **View Details** icon.

VNF Manager displays the **Hosts Configuration** screen listing the details.

4 In the **Host Configuration** screen, click **Close**.

vCenter Only: Modifying Host Configuration

You can modify host configuration, as long as it *has not* been added to a cluster that is already commissioned and running.

Exception: Host Username and Host Password can always be modified.

To modify host configuration, repeat the procedure in vCenter Only: Discovering and Configuring Hosts. In step 4, select the managed host you want to change.

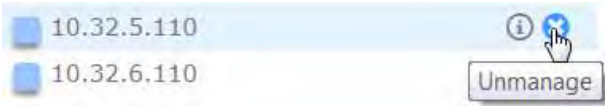
vCenter Only: Unmanaging a Host

You can unmanage a host, as long as it *has not* been added to a cluster that is already commissioned and running.

To unmange a host:

1. From the **Cluster** window, select a Virtualized Infrastructure Manager (VIM) in the right pane.
2. Expand **Hosts** in the right pane.

   VNF Manager lists the Hosts managed by the VNF Manager.
3. To unmanage a host, click the host's **Unmanage** icon.



4. At the confirmation prompt, click **Yes**.

Configuring a Cluster with a CSV File

You can import a CSV file containing the cluster configuration information.

Import can be used to import a new cluster or to add additional nodes to an existing cluster.

Note: *Skip this procedure if you intend to input the required information into the VNF Manager graphical user interface instead of from a imported CSV file.*

Creating the CSV File

The following tables list all the required information you need to enter into the CSV file. The following rules apply:

- Enter the settings in the exact column order indicated in the table.
- Any field *not* marked as Required is Optional. Leave blanks for settings that do not apply to your system.
- Do not modify the header line (the line containing the column names)
- Enter the settings in the case indicated in the table

vCenter Initialization Worksheet

Table 6-6 vCenter Initialization Worksheet

Column	Input	Description	Data
1	Cluster Id	Enter the cluster ID (common to all VMs in a cluster). Valid range is 1 to 127.	
2	Node Id	Node ID for each VM Range: 1-128 MCMs must be 7 or 8. CSM cannot be 7 or 8. SSM cannot be 7 or 8. ***Note:*** *Setting SSM Node ID to 1 is not recommended because it can result in dropped proxy traffic for some sessions by the Linux Kernel on the CSM.* *To disallow setting SSM Node ID to 1:* *1. Edit /opt/Affirmed/NMS/server/ems/resources/cloud.properties and set the following property: cloud.ssm.nonode1.enabled=true* *2. Restart the Acuitas server*	
3	Instantiation Order	VM instantiation order to be applied during cluster instantiation. If no instantiation order specified, VNF Manager instantiates VMS by ascending node type ID: mcm (1), ssm (2), csm (3), mgmt (10), rm (11), callp (12), sig (13), lb (14), data (15), edp (16), mrm (17), msm (18) If some VMs in a cluster have instantiation order specified, VNF Manager first instantiates those VMs according to instantiation order, then instantiates the other VMs according to ascending node type ID. In the case of mgmt/mrm of MCC MME, mgmt-0/mrm-0 are always be instantiated first and mgmt-1/mrm-1 are always instantiated last, regardless of specified instantiation order.	
4	Node Type	■ MCM ■ CSM ■ SSM	

Table 6-6 vCenter Initialization Worksheet

Column	Input	Description	Data
5	Node Personality	Leave this field blank if deploying MCC with compact building block strategy. ■ MCM - vMCM ■ CSM: – ASM (Advanced Services Module) – CCM (Centralized Control Module) – DCM (Distributed Control Module) ■ SSM: – IOM (I/O Module) – WSM (Workflow Services Module) – ISM (Integrated Services Module: Content and Subscriber Services) – IWM (Integrated Workflow Module	
6	Host IP	IP Address of ESXi host where the VM is to be instantiated. In vCenter, if the host is configured using the hostname instead of IP address, enter the hostname for this setting. vCenter must be able to reach this host. For SR-IOV, a single host cannot support: ■ More than 2 VMs ■ More than 1 SSM For non-SR-IOV, a single host cannot support: ■ More than 2 VMs	
7	VM Name	Name format: Type-MCC ID - Node. Can contain only alphanumeric characters, _, and -. Example: vMCM-44-7	
8	Reserved	Whether the VM is reserved for expansion: ■ True ■ False ***Note:*** *For an MCC cluster with a single MCM, it is recommended that its cluster configuration* ***not have*** *the other MCM set to reserved. Otherwise the VNF Manager marks that MCM as instantiated due to its existence in the MCC configuration.*	

Table 6-6 vCenter Initialization Worksheet

Column	Input	Description	Data
9	Building Block Strategy	Strategy to use to create node personality: ■ compact — For traditional MCM, CSM, and SSM nodes. ■ specialized — Optimized for large clusters (more than 12 nodes). ■ advanced-services-separation — Used to separate advanced services ■ control-services-separation — Used to separate control services ■ integrated-services — Centralizes the execution of data forwarding services (workflow and I/O) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM and Call-Control Management services (PGW, SGW, and GGSN) in another VM ■ integrated-workflow — Centralizes the execution of data forwarding services (workflow) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM, Call-Control Management services (PGW, SGW, and GGSN) in another VM, and I/O services in another VM.	
10	Cluster Logical IP	Cluster Logical Management IP Address Enter the IP Address to be used by the active MCM. Cannot be defined for CSM or SSM. Example: 10.32.10.75	
11	NTP IP	NTP IP Address Enter the IP Address for the NTP Server. Must be valid for MCM. Cannot be defined for CSM or SSM. Example: 10.32.0.254	
12	SR-IOV Configuration	Specify the networks supporting SR-IOV: ■ none ■ ew-ns	
13	EW Redundant	Indicates if EW Redundancy is enabled: ■ True ■ False Required for MCM. Cannot be defined for CSM or SSM.	

Table 6-6 vCenter Initialization Worksheet

Column	Input	Description	Data
14	Enable root SSH Access	Applies to the root_ssh_access parameter: ■ True ■ False Required for MCM. Cannot be defined for CSM or SSM.	
15	Enable Multiple Sessions	Applies to the multi-session parameter: ■ True ■ False Required for MCM. Cannot be defined for CSM or SSM.	
16	Disk Format	■ thin ■ eagerZeroedThick	
17	CPU	CPU value Range: 1-100 Not required for non-SR-IOV systems.	
18	CPU Affinity	CPU Affinity range Required for create and add operations to deploy MCC with specialized building block strategy. For SSM, VNF Manager is hardcoded to take half of the CPUs from the host without considering user input.	
19	Memory	Memory value, in MB Not required for non-SR-IOV systems.	
20	MGMT	AN Management Network Label Required.	
21	Management IP	Management IP Address Enter the IP Address for the VM to be used to access (ssh) the VM. Example: 10.32.7.75	
22	Management Gateway IP	Management Gateway IP Address Enter the Gateway IP address for Management IP. Example: 10.32.0.1	
23	Management Netmask Length	Netmask Length for Management IP Enter the netmask length for Management IP address. Range: 0 - 32	

Table 6-6 vCenter Initialization Worksheet

Column	Input	Description	Data
24	Management VLAN	Management VLAN ID Enter the Management VLAN ID to be used for the Management IP addresses. Range: 0-4095	
25	BASE1	AN Base 1 Network Label Required.	
26	BASE2	AN Base 2 Network Label Required for SR-IOV systems and non-SR-IOV systems with East-West redundancy.	
27	Base VLAN A	Base: VLAN ID A Enter VLAN ID for Base interconnect. Range: 0-4095	
28	Base VLAN B	Base: VLAN ID B Enter VLAN ID for redundant Base interconnect. Range: 0-4095	
29	Enable Base Routability	Whether to enable base routability for the cluster: ■ True ■ False When enabled, VNF Manager allows configuration of Base Master IP address (per cluster) and Base IP Address, and Base Netmask length (per node) ***Note:*** *To enable Base Routability, you must perform a special administrative step to install an-mod-ova version 1.3.3. For instructions, see Requirement to Install ovatools to Enable Features.*	
30	Base Master IP	Base Master IP is a floating IP address. It is held by the active MCM node.	
31	BASE IP	IP address for Base network	
32	BASE Netmask Length	Netmask length for Base network	
33	EW1	AN East-West 1 Network Label Required for CSM and SSM. Cannot be defined for MCM.	
34	EW2	AN East-West 2 Network Label Required for CSM and SSM of SR-IOV systems and non-SR-IOV systems with East-West redundancy. Cannot be defined for MCM.	

Table 6-6 vCenter Initialization Worksheet

Column	Input	Description	Data
35	EW VLAN A	East-West: VLAN ID A Enter VLAN ID for East-West. Range: 0-4095	
36	EW VLAN B	East-West: VLAN ID B Enter VLAN ID for redundant East-West. Range: 0-4095	
37	Enable EW L3	Whether to enable EW L3 for the cluster: ■ True ■ False When enabled, VNF Manager allows configuration of IP address(es) and netmask length(es) for EW networks. ***Note:*** *To enable EW L3, you must perform a special administrative step to install an-mod-ova version 1.3.3. For instructions, see Requirement to Install ovatools to Enable Features.*	
38	EW1 IP	IP address of EW 1 network	
39	EW1 Netmask Length	Netmask length of EW 1 network	
40	EW2 IP	IP address of EW 2 network	
41	EW2 Netmask Length	Netmask length of EW 2 network	
42	NS1	AN North-South 1 Network Label Required for SSM. Cannot be defined for MCM or CSM.	
43	NS2	AN North-South 2 Network Label Required for SSM. Cannot be defined for MCM or CSM.	

Sample vCenter CSV File

############## Acuitas VNFM Cluster Configuration for VCenter ##

Cluster Id: 0-127

Instantiation Order: unique positive integer

Node Type: mcm|csm|ssm

Node Personality: ASM|CCM|DCM|IOM|WSM|ISM|IWM|(empty for mcm)

VM Name: alphanumeric, _ or - only

Reserved: True|False,

Disk Format: thin|eagerZeroedThick

CPU Affinity: use '-' for ranges and '|' to separate values, e.g. 0|2|4-7 means processors 0,2,4,5, 6 and 7

Memory: in MB

Cluster Logical IP,NTP IP,Enable root SSH Access,Enable Multiple Sessions: MCM only

MCM Only information must be consistent between the 2 MCM's

Network Information (BASE1, ...,NS2 Physical Function): Consistent for VM's hosted by the same host

Enable root SSH Access,Enable Password Aging,Enable Multiple Sessions,Enable Telnet Access: True|False

Building Block Strategy: compact|specialized|advanced-services-separation|control-services-separation|integrated-services|integrated-workflow default is specialized,

SR-IOV Configuration,EW Redundant,Enable Base Routability,Enable EW L3: True|False

###

!!!!

125,13,ssm,WSM,10.64.5.236,WSM-125-13,none,,,,,,,,16,0-15,56320,AN Management Network,10.64.13.125,10.64.0.1,20,0,AN Base 1 Network,AN Base 2 Network,,,,,168.254.1.13,16,AN East-West 1 Network,AN East-Westh 2 Network,,,,165.254.100.13,24,166.254.100.13,24,AN North-South 1 Network,AN North-South 2 Network

vCloud Director Initialization Worksheet

Table 6-7 vCloud Director Initialization Worksheet

Column	Input	Description	Data
1	Cluster Id	Enter the cluster ID (common to all VMs in a cluster). Valid range is 1 to 127.	
2	Node Id	Node ID for each VM Range: 1-128 MCMs must be 7 or 8. CSM cannot be 7 or 8. SSM cannot be 7 or 8. ***Note:*** *Setting SSM Node ID to 1 is not recommended because it can result in dropped proxy traffic for some sessions by the Linux Kernel on the CSM.* *To disallow setting SSM Node ID to 1:* *1. Edit /opt/Affirmed/NMS/server/ems/resources/cloud.properties and set the following property: cloud.ssm.nonode1.enabled=true* *2. Restart the Acuitas server*	
3	Node Type	■ MCM ■ CSM ■ SSM	
4	Node Personality	Leave this field blank if deploying MCC with compact building block strategy. ■ MCM - vMCM ■ CSM: – ASM (Advanced Services Module) – CCM (Centralized Control Module) – DCM (Distributed Control Module) ■ SSM: – IOM (I/O Module) – WSM (Workflow Services Module) – ISM (Integrated Services Module: Content and Subscriber Services) – IWM (Integrated Workflow Module	
5	VM Name	Name format: Type-MCC ID - Node. Can contain only alphanumeric characters, _, and -. Example: vMCM-44-7	

Table 6-7 vCloud Director Initialization Worksheet

Column	Input	Description	Data
6	Reserved	Whether the VM is reserved for expansion: ■ True ■ False ***Note:*** *For an MCC cluster with a single MCM, it is recommended that its cluster configuration* ***not have*** *the other MCM set to reserved. Otherwise the VNF Manager marks that MCM as instantiated due to its existence in the MCC configuration.*	
7	vApp Name	vApp name	
8	vDC Name	Virtual Data Center name	
9	Building Block Strategy	Strategy to use to create node personality: ■ compact — For traditional MCM, CSM, and SSM nodes. ■ specialized — Optimized for large clusters (more than 12 nodes). ■ advanced-services-separation — Used to separate advanced services ■ control-services-separation — Used to separate control services ■ integrated-services — Centralizes the execution of data forwarding services (workflow and I/O) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM and Call-Control Management services (PGW, SGW, and GGSN) in another VM ■ integrated-workflow — Centralizes the execution of data forwarding services (workflow) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM, Call-Control Management services (PGW, SGW, and GGSN) in another VM, and I/O services in another VM.	
10	Cluster Logical IP	Cluster Logical Management IP Address Enter the IP Address to be used by the active MCM. Cannot be defined for CSM or SSM. Example: 10.32.10.75	
11	NTP IP	NTP IP Address Enter the IP Address for the NTP Server. Must be valid for MCM. Cannot be defined for CSM or SSM. Example: 10.32.0.254	
12	mcm vApp Template	Name of the MCM vApp Template	

Table 6-7 vCloud Director Initialization Worksheet

Column	Input	Description	Data
13	csm vApp Template	Name of the CSM vApp Template	
14	ssm vApp Template	Name of the SSM vApp Template	
15	Enable root SSH Access	Applies to the root_ssh_access parameter: ■ True ■ False Required for MCM. Cannot be defined for CSM or SSM.	
16	Enable Multiple Sessions	Applies to the multi-session parameter: ■ True ■ False Required for MCM. Cannot be defined for CSM or SSM.	
17	Secondary Disk	Secondary Disk (SCSI type only), in MB	
18	Management IP	Management IP Address Enter the IP Address for the VM to be used to access (ssh) the VM. Example: 10.32.7.75	
19	Management Gateway IP	Management Gateway IP Address Enter the Gateway IP address for Management IP. Example: 10.32.0.1	
20	Management Netmask Length	Netmask Length for Management IP Enter the netmask length for Management IP address. Range: 0 - 32	
21	Management VLAN	Management VLAN ID Enter the Management VLAN ID to be used for the Management IP addresses. Range: 0-4095	
22	BASE IP	IP address for Base network	
23	BASE Netmask Length	Netmask length for Base network	
24	Base VLAN A	Base: VLAN ID A Enter VLAN ID for Base interconnect. Range: 0-4095	

Table 6-7 vCloud Director Initialization Worksheet

Column	Input	Description	Data
25	Enable Base Routability	Whether to enable base routability for the cluster: ■ True ■ False When enabled, VNF Manager allows configuration of Base Master IP address, Base IP Address, and Base Netmask length for each node	
26	Base Master IP	Base Master IP is a floating IP address. It is held by the active MCM node.	
27	EW VLAN A	East-West: VLAN ID A Enter VLAN ID for East-West. Range: 0-4095	
28	Enable EW L3	Whether to enable EW L3 for the cluster: ■ True ■ False When enabled, VNF Manager allows configuration of IP address(es) and netmask length(es) for EW networks	
29	EW1 IP	IP address of EW 1 network	
30	EW1 Netmask Length	Netmask length of EW 1 network	

Sample vCloud Director CSV File

```
############## Acuitas VNFM Cluster Configuration for vCloud Director ##########################################
# Cluster Id: 1-127
# Node Type: mcm|csm|ssm
# Node Personality: ASM|CCM|DCM|IOM|WSM|ISM|IWM(empty for mcm)
# VM Name: alphanumeric, _ or - only
# Reserved: True|False
# Secondary Disk: in MB
# Building Block Strategy: compact|specialized|advanced-services-separation|control-services-separation|
integrated-services|integrated-workflow
# Enable root SSH Access,Enable Multiple Sessions: True|False
# Enable Base Routability,Enable EW L3: True|False
# The following are for MCM only (information must be consistent between the 2 MCM's):,
#    Base VLAN A,EW VLAN A,Cluster Logical IP,NTP IP,Enable root SSH Access,Enable Multiple Sessions
#    Building Block Strategy,mcm vApp Template,csm vApp Template,ssm vApp Template
#    Enable Base Routability,Base Master IP,Enable EW L3
#################################################################################################################
# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!    DO NOT CHANGE HEADER LINE       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
#################################################################################################################
Cluster Id,Node Id,Node Type,Node Personality,VM Name,Reserved,vApp Name,VDC Name,Building Block
Strategy,Cluster Logical IP,NTP IP,mcm vApp Template,csm vApp Template,ssm vApp Template,Enable root SSH
Access,Enable Multiple Sessions,Secondary Disk,Management IP,Management Gateway IP,Management Netmask
Length,Management VLAN,BASE IP,BASE Netmask Length,Base VLAN A,Enable Base Routability,Base Master IP,EW VLAN
A,Enable EW L3,EW1 IP,EW1 Netmask Length
16,7,mcm,,MCM-16-7,FALSE,an-mcc-16,Acton EMS-VNFM
QADev,compact,10.168.200.227,172.16.239.2,MCM-8.0.0.0-688,CSM-8.0.0.0-688,SSM-8.0.0.0-688,TRUE,TRUE,,10.168.200
.221,10.168.200.1,24,0,168.254.1.7,16,0,TRUE,168.254.1.200,0,TRUE,,
16,8,mcm,,MCM-16-8,FALSE,an-mcc-16,Acton EMS-VNFM
QADev,compact,10.168.200.227,172.16.239.2,MCM-8.0.0.0-688,CSM-8.0.0.0-688,SSM-8.0.0.0-688,TRUE,TRUE,,10.168.200
.222,10.168.200.1,24,0,168.254.1.8,16,0,TRUE,168.254.1.200,0,TRUE,,
16,1,csm,,CSM-16-1,FALSE,an-mcc-16,Acton EMS-VNFM
QADev,,,,MCM-8.0.0.0-688,CSM-8.0.0.0-688,SSM-8.0.0.0-688,,,,10.168.200.223,10.168.200.1,24,0,168.254.1.1,16,,,,
,,165.254.100.1,24
16,2,ssm,,SSM-16-2,FALSE,an-mcc-16,Acton EMS-VNFM
QADev,,,,MCM-8.0.0.0-688,CSM-8.0.0.0-688,SSM-8.0.0.0-688,,,16,10.168.200.225,10.168.200.1,24,0,165.254.1.2,16,,
,,,,165.254.100.2,24
```

OpenStack Initialization Worksheet for MCC

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
1	Cluster Id	Enter the cluster ID (common to all VMs in a cluster). Valid range is 1 to 127.	
2	Availability Zone	Enter the Availability Zone configured at OpenStack within which the VM is placed.	
3	Node Id	Node ID for each VM Range: 1-128 MCMs must be 7 or 8. CSM cannot be 7 or 8. SSM cannot be 7 or 8. ***Note:*** *Setting SSM Node ID to 1 is not recommended because it can result in dropped proxy traffic for some sessions by the Linux Kernel on the CSM.* *To disallow setting SSM Node ID to 1:* *1. Edit /opt/Affirmed/NMS/server/ems/resources/cloud.properties and set the following property: cloud.ssm.nonode1.enabled=true* *2. Restart the Acuitas server*	
4	Instantiation Order	VM instantiation order to be applied during cluster instantiation. If no instantiation order specified, VNF Manager instantiates VMS by ascending node type ID: mcm (1), ssm (2), csm (3), mgmt (10), rm (11), callp (12), sig (13), lb (14), data (15), edp (16), mrm (17), msm (18) If some VMs in a cluster have instantiation order specified, VNF Manager first instantiates those VMs according to instantiation order, then instantiates the other VMs according to ascending node type ID. In the case of mgmt/mrm of MCC MME, mgmt-0/mrm-0 are always be instantiated first and mgmt-1/mrm-1 are always instantiated last, regardless of specified instantiation order.	
5	Node Type	■ MCM ■ CSM ■ SSM	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
6	Node Personality	Leave this field blank if deploying MCC with compact building block strategy. ■ MCM - vMCM ■ CSM: – ASM (Advanced Services Module) – CCM (Centralized Control Module) – DCM (Distributed Control Module) ■ SSM: – IOM (I/O Module) – WSM (Workflow Services Module) – ISM (Integrated Services Module: Content and Subscriber Services) – IWM (Integrated Workflow Module	
7	VM Name	Name format: Type-MCC ID - Node. Can contain only alphanumeric characters, _, and -. Example: vMCM-44-7	
8	Reserved	Whether the VM is reserved for expansion: ■ True ■ False ***Note:*** *For an MCC cluster with a single MCM, it is recommended that its cluster configuration* ***not have*** *the other MCM set to reserved. Otherwise the VNF Manager marks that MCM as instantiated due to its existence in the MCC configuration.*	
9	Flavor	The server flavor configured at OpenStack, used by the VM.	
10	Server Group	The Serve Group this VM belongs to. Is used to apply anti-affinity rules.	
11	Security Group	Security Group: ■ When a security group is configured, the VNF Manager creates all ports associated with the security group. ■ When no security group is configured, VNF Manager creates all ports with port security disabled. ***Note:*** *This behavior is a fundamental change from the prior functionality where (when no security group was configured) the cluster was deployed with the default security group.*	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
12	Building Block Strategy	Strategy to use to create node personality: ■ compact — For traditional MCM, CSM, and SSM nodes. ■ specialized — Optimized for large clusters (more than 12 nodes). ■ advanced-services-separation — Used to separate advanced services ■ control-services-separation — Used to separate control services ■ integrated-services — Centralizes the execution of data forwarding services (workflow and I/O) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM and Call-Control Management services (PGW, SGW, and GGSN) in another VM ■ integrated-workflow — Centralizes the execution of data forwarding services (workflow) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM, Call-Control Management services (PGW, SGW, and GGSN) in another VM, and I/O services in another VM.	
13	Cluster Logical IP	Cluster Logical Management IP Address Enter the IP Address to be used by the active MCM. Cannot be defined for CSM or SSM. Example: 10.32.10.75	
14	NTP IP	NTP IP Address Enter the IP Address for the NTP Server. Must be valid for MCM. Cannot be defined for CSM or SSM. Example: 10.32.0.254	
15	SR-IOV Configuration	Specify the networks supporting SR-IOV: ■ none ■ ew-ns ■ ew-ns-base-mgmt	
16	EW Redundant	Whether to configure the cluster with redundant East-West: ■ True ■ False	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
17	Enable VLAN Stripping	Whether to enable VLAN stripping: ■ True ■ False Set to True for OpenStack deployments that do not allow Flat Networks and instead manage VLAN tagged traffic before the traffic arrives at the MCC. In these cases, network interfaces within the MCC must be configured as untagged. Untagged packets sent from the MCC are tagged by the OpenStack controller.	
18	Controller Image	Controller image name configured at OpenStack Used for MCM nodes	
19	Payload Image	Payload image configured at OpenStack Used for CSM and SSM nodes	
20	Cinder Enabled	Whether the VM is cinder enabled: ■ True ■ False	
21	Controller Boot Size	Cinder volume in GB for the Controller boot image Example: 112	
22	Payload Boot Size	Cinder volume in GB for the Payload boot image Example: 50	
23	Enable root SSH Access	Applies to the root_ssh_access parameter: ■ True ■ False Required for MCM. Cannot be defined for CSM or SSM.	
24	Enable Multiple Sessions	Applies to the multi-session parameter: ■ True ■ False Required for MCM. Cannot be defined for CSM or SSM.	
25	MGMT	AN Management Network Label Required.	
26	Management IP	Management IP Address Enter the IP Address for the VM to be used to access (ssh) the VM. Example: 10.32.7.75	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
27	Management Gateway IP	Management Gateway IP Address Enter the Gateway IP address for Management IP. Example: 10.32.0.1	
28	Management Netmask Length	Netmask Length for Management IP Enter the netmask length for Management IP address. Range: 0 - 32	
29	Management VLAN	Management VLAN ID Enter the Management VLAN ID to be used for the Management IP addresses. Range: 0-4095	
30	BASE1	AN Base 1 Network Label Required.	
31	BASE2	AN Base 2 Network Label Required for East-West redundancy.	
32	Base VLAN A	VLAN ID for Base interconnect.	
33	Base VLAN B	VLAN ID for redundant Base interconnect (only for East-West Redundancy support).	
34	Enable Base Routability	Whether to enable base routability for the cluster: ■ True ■ False When enabled, VNF Manager allows configuration of Base Master IP address, Base IP Address, and Base Netmask length for each node	
35	Base Master IP	Base Master IP is a floating IP address. It is held by the active MCM node.	
36	BASE IP	IP address for Base network	
37	BASE Netmask Length	Netmask length for Base network	
38	EW1	AN East-West 1 Network Label Used for CSM and SSM nodes Example: AN EW 1 Network	
39	EW2	AN East-West 2 Network Label Required for East-West redundancy Used for CSM and SSM nodes. Example: AN EW 2 Network	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
40	EW VLAN A	East-West: VLAN ID A Enter VLAN ID for East-West. Range: 0-4095	
41	EW VLAN B	East-West: VLAN ID B Enter VLAN ID for redundant East-West. Range: 0-4095	
42	Enable EW L3	Whether to enable EW L3 for the cluster: ■ True ■ False When enabled, VNF Manager allows configuration of IP address(es) and netmask length(es) for EW networks	
43	EW1 IP	IP address of EW 1 network	
44	EW1 Netmask Length	Netmask length of EW 1 network	
45	EW2 IP	IP address of EW 2 network	
46	EW2 Netmask Length	Netmask length of EW 2 network	
47	NS1	AN North-South 1 Network Label Used by SSM nodes. Example: AN NS 1 Network	
48	NS1 IP	AN North-South 1 IP Address	
49	NS2	AN North-South 2 Network Label Used by SSM nodes. Example: AN NS 2 Network	
50	NS2 IP	AN North-South 2 IP Address	
51	NS3 ***Note:*** *In the remaining columns, you can specify the North-South Network Labels and IP Addresses for additional North/South networks. You must configured the networks consecutively without gaps. Configured North/South networks at the SSM node level take precedence over values configured at the MCM level.*	AN North-South 3 Network Label Used by SSM nodes. Example: AN NS 3 Network	
52	NS3 IP	AN North-South 3 IP Address	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
53	NS4	AN North-South 4 Network Label Used by SSM nodes. Example: AN NS 4 Network	
54	NS4 IP	AN North-South 4 IP Address	
55	NS5	AN North-South 5 Network Label Used by SSM nodes. Example: AN NS 5 Network	
56	NS5 IP	AN North-South 5 IP Address	
57	NS6	AN North-South 6 Network Label Used by SSM nodes. Example: AN NS 6 Network	
58	NS6 IP	AN North-South 6 IP Address	
59	NS7	AN North-South 7 Network Label Used by SSM nodes. Example: AN NS 7 Network	
60	NS7 IP	AN North-South 7 IP Address	
61	NS8	AN North-South 8 Network Label Used by SSM nodes. Example: AN NS 8 Network	
62	NS8 IP	AN North-South 8 IP Address	
63	NS9	AN North-South 9 Network Label Used by SSM nodes. Example: AN NS 9 Network	
64	NS9 IP	AN North-South 9 IP Address	
65	NS10	AN North-South 10 Network Label Used by SSM nodes. Example: AN NS 10 Network	
66	NS10 IP	AN North-South 10 IP Address	
67	NS11	AN North-South 11 Network Label Used by SSM nodes. Example: AN NS 11 Network	
68	NS11 IP	AN North-South 11 IP Address	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
69	NS12	AN North-South 12 Network Label Used by SSM nodes. Example: AN NS 12 Network	
70	NS12 IP	AN North-South 12 IP Address	
71	NS13	AN North-South 13 Network Label Used by SSM nodes. Example: AN NS 13 Network	
72	NS13 IP	AN North-South 13 IP Address	
73	NS14	AN North-South 14 Network Label Used by SSM nodes. Example: AN NS 14 Network	
74	NS14 IP	AN North-South 14 IP Address	
75	NS15	AN North-South 15 Network Label Used by SSM nodes. Example: AN NS 15 Network	
76	NS15 IP	AN North-South 15 IP Address	
77	NS16	AN North-South 16 Network Label Used by SSM nodes. Example: AN NS 16 Network	
78	NS16 IP	AN North-South 16 IP Address	
79	NS17	AN North-South 17 Network Label Used by SSM nodes. Example: AN NS 17 Network	
80	NS17 IP	AN North-South 17 IP Address	
81	NS18	AN North-South 18 Network Label Used by SSM nodes. Example: AN NS 18 Network	
82	NS18 IP	AN North-South 18 IP Address	
83	NS19	AN North-South 19 Network Label Used by SSM nodes. Example: AN NS 19 Network	
84	NS19 IP	AN North-South 19 IP Address	

Table 6-8 OpenStack Initialization Worksheet for MCC

Column	Input	Description	Data
85	NS20	AN North-South 20 Network Label Used by SSM nodes. Example: AN NS 20 Network	
86	NS20 IP	AN North-South 20 IP Address	
87	NS21	AN North-South 21 Network Label Used by SSM nodes. Example: AN NS 21 Network	
88	NS21 IP	AN North-South 21 IP Address	
89	NS22	AN North-South 22 Network Label Used by SSM nodes. Example: AN NS 22 Network	
90	NS22 IP	AN North-South 22 IP Address	
91	NS23	AN North-South 23 Network Label Used by SSM nodes. Example: AN NS 23 Network	
92	NS23 IP	AN North-South 23 IP Address	
93	NS24	AN North-South 24 Network Label Used by SSM nodes. Example: AN NS 24 Network	
94	NS24 IP	AN North-South 24 IP Address	

Sample OpenStack CSV File for MCC

```
############# Acuitas VNFM Cluster Configuration for OpenStack ##############################################
# Cluster Id: 1-127
# Instantiation Order: unique positive integer
# Node Type: mcm|csm|ssm
# Node Personality: ASM|CCM|DCM|IOM|WSM|ISM|IWM|(empty for mcm)
# VM Name: alphanumeric, _ or - only
# Reserved, Cinder Enabled: True|False
# The following are for MCM only (information must be consistent between the 2 MCM's):
#    Building Block Strategy,Security Group,Controller Image,Payload Image,Controller Boot Size,Payload Boot
Size
#    SR-IOV Configuration,EW Redundant,Enable VLAN Stripping,Cluster Logical IP,NTP IP,Enable root SSH
Access,Enable Multiple Sessions
#    MGMT,BASE1,BASE2,Base VLAN A,Base VLAN B,EW1,EW2,EW VLAN A,EW VLAN B
#    Enable Base Routability,Base Master IP,Enable EW L3
# The following cluster configurations are taken from MCM (information must be consistent between the 2 MCM's):
#
NS1,NS2,NS3,NS4,NS5,NS6,NS7,NS8,NS9,NS10,NS11,NS12,NS13,NS14,NS15,NS16,NS17,NS18,NS19,NS20,NS21,NS22,NS23,NS24,
,
# Building Block Strategy:
compact|specialized|advanced-services-separation|control-services-separation|integrated-services|integrated-wor
kflow
# SR-IOV Configuration,EW Redundant,Enable VLAN Stripping,Enable Base Routability,Enable EW L3: True|False
# Enable root SSH Access,Enable Multiple Sessions: True|False
##########################################################################################################################
##################
# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!    DO NOT CHANGE HEADER LINE       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
##########################################################################################################################
##################
Cluster Id,Availability Zone,Node Id,Instantiation Order,Node Type,Node Personality,VM
Name,Reserved,Flavor,Server Group,Security Group,Building Block Strategy,Cluster Logical IP,NTP IP,SR-IOV
Configuration,EW Redundant,Enable VLAN Stripping,Controller Image,Payload Image,Cinder Enabled,Controller Boot
Size,Payload Boot Size,Enable root SSH Access,Enable Multiple Sessions,MGMT,Management IP,Management Gateway
IP,Management Netmask Length,Management VLAN,BASE1,BASE2,Base VLAN A,Base VLAN B,Enable Base Routability,Base
Master IP,BASE IP,BASE Netmask Length,EW1,EW2,EW VLAN A,EW VLAN B,Enable EW L3,EW1 IP,EW1 Netmask Length,EW2
IP,EW2 Netmask Length,NS1,NS 1 IP,NS2,NS 2 IP,NS3,NS 3 IP,NS4,NS 4 IP,NS5,NS 5 IP,NS6,NS 6 IP,NS7,NS 7
IP,NS8,NS 8 IP,NS9,NS 9 IP,NS10,NS 10 IP,NS11,NS 11 IP,NS12,NS 12 IP,NS13,NS 13 IP,NS14,NS 14 IP,NS15,NS 15
IP,NS16,NS 16 IP,NS17,NS 17 IP,NS18,NS 18 IP,NS19,NS 19 IP,NS20,NS 20 IP,NS21,NS 21 IP,NS22,NS 22 IP,NS23,NS 23
IP,NS24,NS 24 IP
15,zone-15,7,1,mcm,,MCM-15-7,FALSE,AN-MCM,mcm-anti-affinity-group,default,compact,2001:470:8865:4001:10:64:0:21
5,2001:470:8865:21:10:2:1:98,ew-ns,TRUE,FALSE,an-controller-an-9.0.0.0-549.REL,an-payload-an-9.0.0.0-549.REL,FA
LSE,0,0,TRUE,TRUE,AN-MGMT,2001:470:8865:4001:10:64:7:215,2001:470:8865:4001::1,64,2200,AN-BASE1,AN-BASE2,0,0,FA
LSE,,168.254.15.7,16,AN-EW1-PF,AN-EW2-PF,50,51,FALSE,,,,,AN-NS1-PF,,AN-NS2-PF
15,zone-15-2,8,2,mcm,,MCM-15-8,FALSE,AN-MCM,mcm-anti-affinity-group,default,compact,2001:470:8865:4001:10:64:0:
215,2001:470:8865:21:10:2:1:98,ew-ns,TRUE,FALSE,an-controller-an-9.0.0.0-549.REL,an-payload-an-9.0.0.0-549.REL,
FALSE,0,0,TRUE,TRUE,AN-MGMT,2001:470:8865:4001:10:64:8:215,2001:470:8865:4001::1,64,2200,AN-BASE1,AN-BASE2,0,0,
FALSE,,168.254.15.8,16,AN-EW1-PF,AN-EW2-PF,50,51,FALSE,,,,,AN-NS1-PF,,AN-NS2-PF
15,zone-15,1,3,csm,,CSM-15-1,FALSE,AN-CSM,csm-anti-affinity-group,,,,,,,,,,,,,,,2001:470:8865:4001:10:64:1:215
,2001:470:8865:4001::1,64,2200,,,,,,,168.254.15.1,16,,,,,,160.254.15.1,16,161.254.15.1,16,AN-NS1-PF,,AN-NS2-PF
15,zone-15-2,2,4,csm,,CSM-15-2,FALSE,AN-CSM,csm-anti-affinity-group,,,,,,,,,,,,,,,2001:470:8865:4001:10:64:2:2
15,2001:470:8865:4001::1,64,2200,,,,,,,168.254.15.2,16,,,,,,160.254.15.2,16,161.254.15.2,16,AN-NS1-PF,,AN-NS2-P
F
15,zone-15,3,5,ssm,,SSM-15-3,FALSE,AN-SSM,ssm-anti-affinity-group,,,,,,,,,,,,,,,2001:470:8865:4001:10:64:3:215
,2001:470:8865:4001::1,64,2200,,,,,,,168.254.15.3,16,,,,,,160.254.15.3,16,161.254.15.3,16,AN-NS1-PF,10.80.1.11,
AN-NS2-PF,10.81.1.11
15,zone-15-2,4,6,ssm,,SSM-15-4,FALSE,AN-SSM,ssm-anti-affinity-group,,,,,,,,,,,,,,,2001:470:8865:4001:10:64:4:2
15,2001:470:8865:4001::1,64,2200,,,,,,,168.254.15.4,16,,,,,,160.254.15.4,16,160.254.15.4,16
```

OpenStack Initialization Worksheet for MCC MME

Table 6-9 OpenStack Initialization Worksheet for MCC MME

Column	Input	Description	Data
1	Cluster Name	Enter the cluster name Can contain only alphanumeric characters, _, and -.	
2	Cluster Id	Enter the cluster ID (common to all VMs in a cluster). Valid range is 1 to 127.	
3	VM Name	Enter the VM name. Can contain only alphanumeric characters, _, and -. Example: vMCM-44-7	
4	Instantiation Order	VM instantiation order to be applied during cluster instantiation. If no instantiation order specified, VNF Manager instantiates VMs by ascending node type ID: mcm (1), ssm (2), csm (3), mgmt (10), rm (11), callp (12), sig (13), lb (14), data (15), edp (16), mrm (17), msm (18) If some VMs in a cluster have instantiation order specified, VNF Manager first instantiates those VMs according to instantiation order, then instantiates the other VMs according to ascending node type ID. In the case of mgmt/mrm of MCC MME, mgmt-0/mrm-0 are always be instantiated first and mgmt-1/mrm-1 are always instantiated last, regardless of specified instantiation order.	
5	Service Role	Service Role: ■ mgmt-N (N=0-1) ■ |rm-N (N=0-1) ■ sig-N (N=0-19) ■ callpN-M (N=0-15, M=0-1) ■ lb-N (N=0-7) ■ data-N (N=0-15) ■ edp-N (N=0-15)	
6	Reserved	Whether the VM is reserved for expansion: ■ True ■ False	

Table 6-9 OpenStack Initialization Worksheet for MCC MME

Column	Input	Description	Data
7	Building Block Strategy	Strategy to use to create node personality: ■ compact (corresponds to 2-VM Model): – mrm – msm ■ specialized (corresponds to 5/6/7-VM Model): – mgmt – rm – callp – sig – lb – data – edp	
8	Cluster Logical IP	Cluster Logical Management IP Address	
9	NTP IP	NTP IP Address Enter the IP Address for the NTP Server.	
10	Security Group	Security Group: ■ When a security group is configured, the VNF Manager creates all ports associated with the security group. ■ When no security group is configured, VNF Manager creates all ports with port security disabled. ***Note:*** *This behavior is a fundamental change from the prior functionality where (when no security group was configured) the cluster was deployed with the default security group.*	
11	Image	Controller image name configured at OpenStack	
12	Flavor	The server flavor configured at OpenStack, used by the VM.	
13	Availability Zone	Enter the Availability Zone configured at OpenStack within which the VM is placed.	
14	Server Group	The Serve Group this VM belongs to. Is used to apply anti-affinity rules.	
15	Cinder Enabled	Whether the VM is cinder enabled: ■ True ■ False	
16	Boot Size	Cinder volume in GB for the Controller boot image	
17	mgmt Ephemeral Size	Cinder volume in GB for the mgmt Ephemeral	

Table 6-9 OpenStack Initialization Worksheet for MCC MME

Column	Input	Description	Data
18	non-mgmt Ephemeral Size	Cinder volume in GB for the non-mgmt Ephemeral	
19	MGMT	AN Management Network Label Required.	
20	MGMT2	The management network for non-mgmt nodes/VMs	
21	Management IP	Management IP Address Enter the IP Address for the VM to be used to access (ssh) the VM. Example: 10.32.7.75	
22	Management Gateway IP	Management Gateway IP Address Enter the Gateway IP address for Management IP. Example: 10.32.0.1	
23	Management Netmask Length	Netmask Length for Management IP Enter the netmask length for Management IP address. Range: 0 - 32	
24	Management VLAN	Management VLAN ID Enter the Management VLAN ID to be used for the Management IP addresses. Range: 0-4095	
25	BASE1	AN Base 1 Network Label Required.	
26	EW1	AN East-West 1 Network Label Example: AN EW 1 Network	
27	EDP EW1	East/West 1 network name for EDP VMs/nodes	
28	EDP EW2	East/West 2 network name for EDP VMs/nodes	
29	Base VLAN	VLAN ID for Base network	
30	EW VLAN	VLAN ID for East/West network for non-EDP VMs/nodes	
31	EDP EW VLAN A	VLAN ID for East/West 1 network for EDP VMs/nodes	
32	EDP EW VLAN B	VLAN ID for East/West 2 network for EDP VMs/nodes	
33	NS1	AN North-South 1 Network Label Example: AN NS 1 Network	
34	NS1 IP	AN North-South 1 IP Address	

Table 6-9 OpenStack Initialization Worksheet for MCC MME

Column	Input	Description	Data
35	NS2	AN North-South 2 Network Label Example: AN NS 2 Network	
36	NS2 IP	AN North-South 2 IP Address	
37	NS3 ***Note:*** *In the remaining columns, you can specify the North-South Network Labels and IP Addresses for additional North/South networks. You must configured the networks consecutively without gaps. Configured North/South networks at the node level take precedence over respective values configured at the cluster level.*	AN North-South 3 Network Label Example: AN NS 3 Network	
38	NS3 IP	AN North-South 3 IP Address	
39	NS4	AN North-South 4 Network Label Example: AN NS 4 Network	
40	NS4 IP	AN North-South 4 IP Address	
41	NS5	AN North-South 5 Network Label Example: AN NS 5 Network	
42	NS5 IP	AN North-South 5 IP Address	
43	NS6	AN North-South 6 Network Label Example: AN NS 6 Network	
44	NS6 IP	AN North-South 6 IP Address	
45	NS7	AN North-South 7 Network Label Example: AN NS 7 Network	
46	NS7 IP	AN North-South 7 IP Address	
47	NS8	AN North-South 8 Network Label Example: AN NS 8 Network	
48	NS8 IP	AN North-South 8 IP Address	
49	NS9	AN North-South 9 Network Label Example: AN NS 9 Network	
50	NS9 IP	AN North-South 9 IP Address	

Table 6-9 OpenStack Initialization Worksheet for MCC MME

Column	Input	Description	Data
51	NS10	AN North-South 10 Network Label Example: AN NS 10 Network	
52	NS10 IP	AN North-South 10 IP Address	
53	NS11	AN North-South 11 Network Label Example: AN NS 11 Network	
54	NS11 IP	AN North-South 11 IP Address	
55	NS12	AN North-South 12 Network Label Example: AN NS 12 Network	
56	NS12 IP	AN North-South 12 IP Address	
57	NS13	AN North-South 13 Network Label Example: AN NS 13 Network	
58	NS13 IP	AN North-South 13 IP Address	
59	NS14	AN North-South 14 Network Label Example: AN NS 14 Network	
60	NS14 IP	AN North-South 14 IP Address	
61	NS15	AN North-South 15 Network Label Example: AN NS 15 Network	
62	NS15 IP	AN North-South 15 IP Address	
63	NS16	AN North-South 16 Network Label Example: AN NS 16 Network	
64	NS16 IP	AN North-South 16 IP Address	
65	NS17	AN North-South 17 Network Label Example: AN NS 17 Network	
66	NS17 IP	AN North-South 17 IP Address	
67	NS18	AN North-South 18 Network Label Example: AN NS 18 Network	
68	NS18 IP	AN North-South 18 IP Address	
69	NS19	AN North-South 19 Network Label Example: AN NS 19 Network	
70	NS19 IP	AN North-South 19 IP Address	

Table 6-9 OpenStack Initialization Worksheet for MCC MME

Column	Input	Description	Data
71	NS20	AN North-South 20 Network Label Example: AN NS 20 Network	
72	NS20 IP	AN North-South 20 IP Address	
73	NS21	AN North-South 21 Network Label Example: AN NS 21 Network	
74	NS21 IP	AN North-South 21 IP Address	
75	NS22	AN North-South 22 Network Label Example: AN NS 22 Network	
76	NS22 IP	AN North-South 22 IP Address	
77	NS23	AN North-South 23 Network Label Example: AN NS 23 Network	
78	NS23 IP	AN North-South 23 IP Address	
79	NS24	AN North-South 24 Network Label Example: AN NS 24 Network	
80	NS24 IP	AN North-South 24 IP Address	

Sample OpenStack CSV File for MCC MME

```
############## Acuitas VNFM Cluster Configuration of MCC MME for OpenStack ####################################

# Cluster Name, VM Name: alphanumeric, _ or - only

# Instantiation Order: unique positive integer

# Cluster Id: 0-255

# Service Role: mgmt-N (N=0-1)|rm-N (N=0-1)|sig-N (N=0-19)|callpN-M (N=0-15, M=0-1)|lb-N (N=0-7)|data-N
(N=0-15)|edp-N (N=0-15) |mrm-N (N=0-1) |msmN-M (N=0-3, M=0-1)

# Building Block Strategy: compact|specialized

# Reserved, Cinder Enabled: True|False

# The unit for Cinder volumes (Boot Size, mgmt Ephemeral Size and non-mgmt Ephemeral Size), when used, is in GB

#    The headers apply to both mgmt and mrm configuration

# The following configuration are taken from mgmt-0 and mrm-0:

#    Cluster Logical IP,NTP IP,Image,Security Group,Cinder Enabled,Boot Size,mgmt Ephemeral Size,non-mgmt
Ephemeral Size,MGMT,MGMT2,BASE1,EW1

# The following configurations on cluster level are taken from mgmt-0 node/VM:

#    NS1,NS2,...,NS24

# MGMT2, if configured, is the management network for non-mgmt nodes/VMs

# The NS1,NS2,...,NS24 from lb/data nodes/VMs, if configured, overrides their respective configuration on
cluster level
```

```
# EDP, if configured, the following North/South IPs and networks are taken from edp nodes/VMs directly:

#    NS1,NS 1 IP,NS2,NS 2 IP,...,NS24,NS 24 IP

#########################################################################################################################

# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!    DO NOT CHANGE HEADER LINE       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

#########################################################################################################################

Cluster Name,Cluster Id,VM Name,Instantiation Order,Service Role,Reserved,Building Block Strategy,Cluster
Logical IP,NTP IP,Security Group,Image,Flavor,Availability Zone,Server Group,Cinder Enabled,Boot Size,mgmt
Ephemeral Size,non-mgmt Ephemeral Size,MGMT,MGMT2,Management IP,Management Gateway IP,Management Netmask
Length,Management VLAN,BASE1,EW1,EDP EW1,EDP EW2,Base VLAN,EW VLAN,EDP EW VLAN A,EDP EW VLAN B,NS1,NS 1
IP,NS2,NS 2 IP,NS3,NS 3 IP,NS4,NS 4 IP,NS5,NS 5 IP,NS6,NS 6 IP,NS7,NS 7 IP,NS8,NS 8 IP,NS9,NS 9 IP,NS10,NS 10
IP,NS11,NS 11 IP,NS12,NS 12 IP,NS13,NS 13 IP,NS14,NS 14 IP,NS15,NS 15 IP,NS16,NS 16 IP,NS17,NS 17 IP,NS18,NS 18
IP,NS19,NS 19 IP,NS20,NS 20 IP,NS21,NS 21 IP,NS22,NS 22 IP,NS23,NS 23 IP,NS24,NS 24 IP
vmme081,81,vmme081-mgmt-0,3,mgmt-0,172.18.4.2,172.16.239.2,FALSE,,epc-11.0.18,MGMT,vmc081ZoneA,,FALSE,0,0,0,epc
-oam-vlan360,vmc081-mgmtprv,172.18.4.3,172.18.4.1,24,vmc081-base,vmc081-eastwest,,,
```

```
# The NS1,NS2,...,NS24 from lb/data/edp nodes/VMs, if configured, overrides their respective configuration on
cluster level

#########################################################################################################################

# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!    DO NOT CHANGE HEADER LINE       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

#########################################################################################################################

Cluster Name,Cluster Id,VM Name,Instantiation Order,Service Role,Building Block Strategy,Cluster Logical IP,NTP
IP,Reserved,Security Group,Image,Flavor,Availability Zone,Server Group,Cinder Enabled,Boot Size,mgmt Ephemeral
Size,non-mgmt Ephemeral Size,MGMT,MGMT2,Management IP,Management Gateway IP,Management Netmask
Length,BASE1,EW1,NS1,NS 1 IP,NS2,NS 2 IP,NS3,NS 3 IP,NS4,NS 4 IP,NS5,NS 5 IP,NS6,NS 6 IP,NS7,NS 7 IP,NS8,NS 8
IP,NS9,NS 9 IP,NS10,NS 10 IP,NS11,NS 11 IP,NS12,NS 12 IP,NS13,NS 13 IP,NS14,NS 14 IP,NS15,NS 15 IP,NS16,NS 16
IP,NS17,NS 17 IP,NS18,NS 18 IP,NS19,NS 19 IP,NS20,NS 20 IP,NS21,NS 21 IP,NS22,NS 22 IP,NS23,NS 23 IP,NS24,NS 24
IP

mme-test,100,vmc090-mrm-0,mrm-0,1,compact,10.168.200.70,172.162.39.2,False,vmc090SecGroup,epc-11.0.09-fixes,mrm
-vmc090,srvr741,,False,0,0,0,epc-oam-vlan361,vmc090-mgmtprv,10.168.200.71,10.168.200.1,24,vmc090-base,vmc090-ea
stwest,epc-access-vlan305,,epc-core-vlan325,,,
```

Importing the CSV File

To import a CSV file into the cluster:

1. Expand **Clusters** in the right pane.
2. Click the **Import Cluster Configuration** icon in the right pane.
3. Specify the cluster name to which to apply the CSV file.
4. Click **Choose File** and choose the CSV file.
5. Click **Import**.
6. *vCenter Only*:
   a. Click the cluster in the right pane.
   b. On the cluster in the left pan, click the **View Cluster Configuration** icon.
   c. Configure the parameters as follows:

Table 6-10 Cluster Configuration Parameters

Parameter	Description
MCM template	MCM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in VNF Manager. For details, see vCenter Only: Uploading Open Virtualization Archive (OVA) Packages.
CSM template	CSM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in VNF Manager. For details, see vCenter Only: Uploading Open Virtualization Archive (OVA) Packages.
SSM template	SSM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in VNF Manager. For details, see vCenter Only: Uploading Open Virtualization Archive (OVA) Packages.

   d. Click **Save**.

Validating Cluster Configuration

You can execute validation checks on the cluster configuration:

- If the cluster *has not* yet been deployed, the operation validates the entire cluster hosts/VMs. You could perform this operation to verify the cluster before actually instantiating the cluster (as instantiation might require a maintenance window).
- If the cluster has already been deployed, the operation validates only the additional host/VMs that are not reserved for expansion.

Validation performs the following checks:

- Validates VM name's uniqueness (no duplicate names) per vCenter.
- Validates Datastore name for space and/or parenthesis per host.
- Validates vSwitch SR-IOV-enable status against cluster level SR-IOV-enable and EW-Redundancy setting for the following networks:
  - East-West 1 Network
  - East-West 2 Network
  - North-South 1 Network
  - North-South 2 Network
- Validates communication/connectivity between vCenter and host.

To validate cluster configuration:

1. Click the **Cluster Operations** icon and click **Validate Cluster Configuration**.
2. At the confirmation prompt, click **Yes**.

Cluster-Level Configuration

Note: *This procedure is not required if you import a CSV file containing the configuration information.*

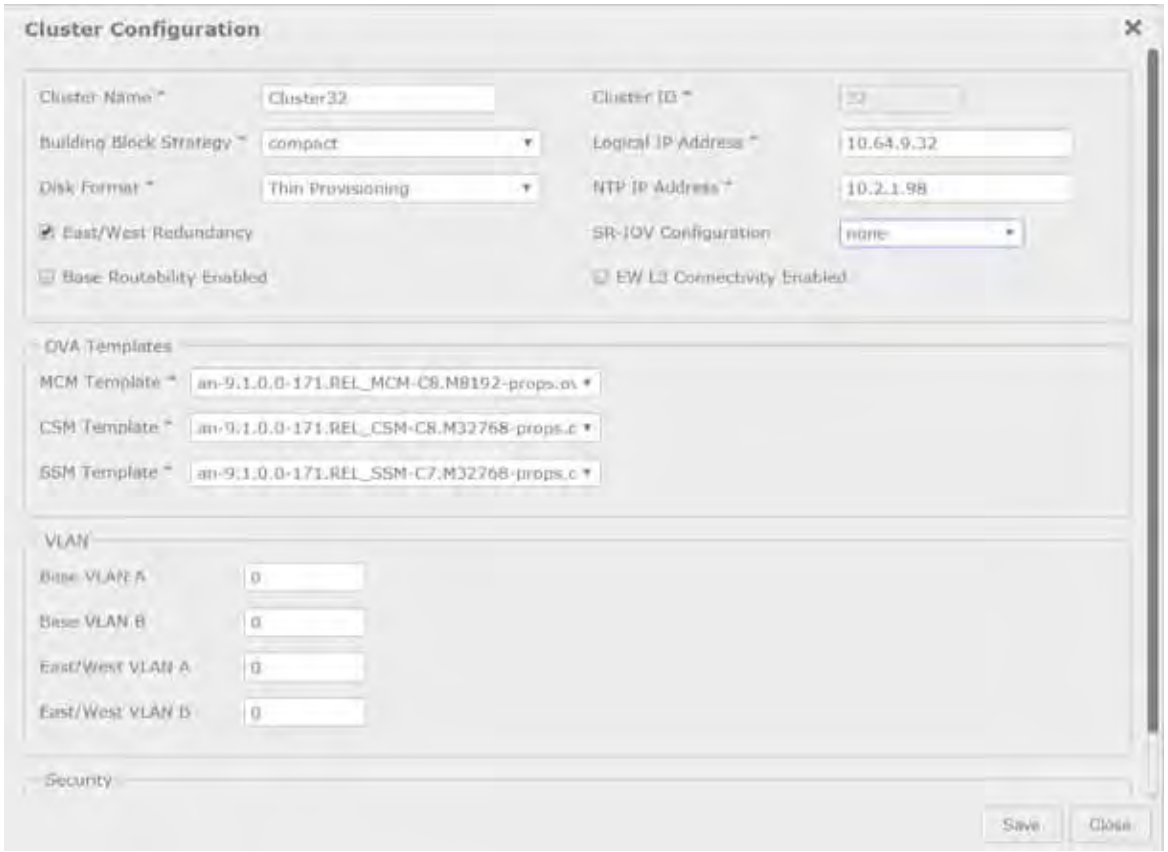
To configure a new cluster:

1. From the **Cluster** window, select a Virtualized Infrastructure Manager (VIM) in the right pane.
2. Click the **Create New Cluster** icon in the right pane.

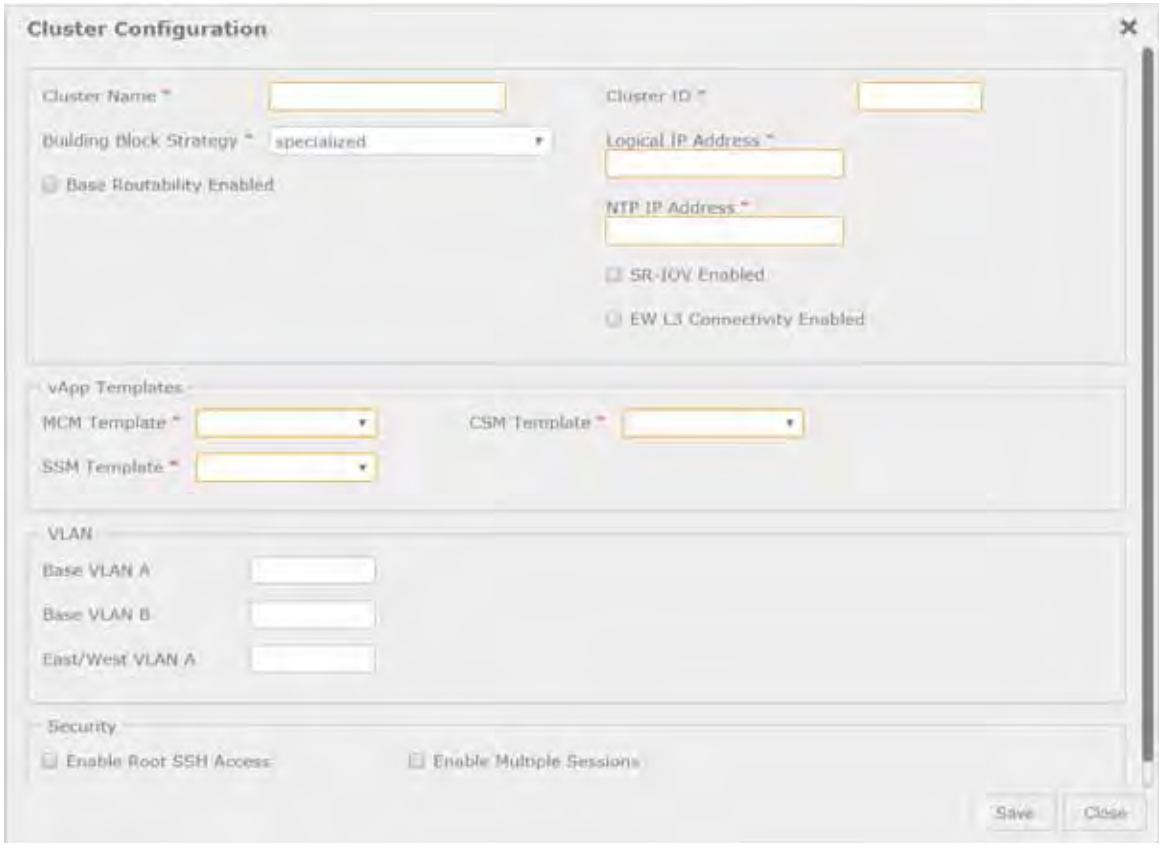
   Acuitas displays the **Cluster Configuration** screen.

Figure 6-5 Cluster Configuration Screens

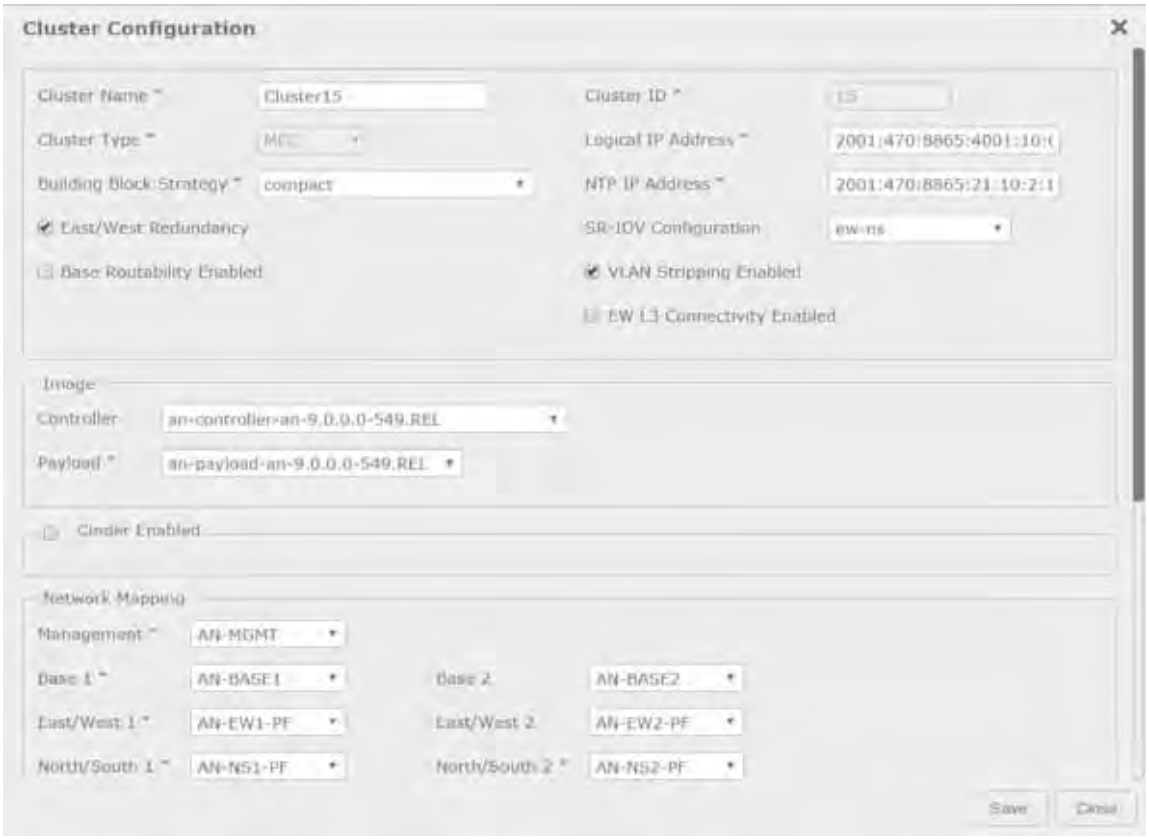
vCenter Screen (MCC Only):



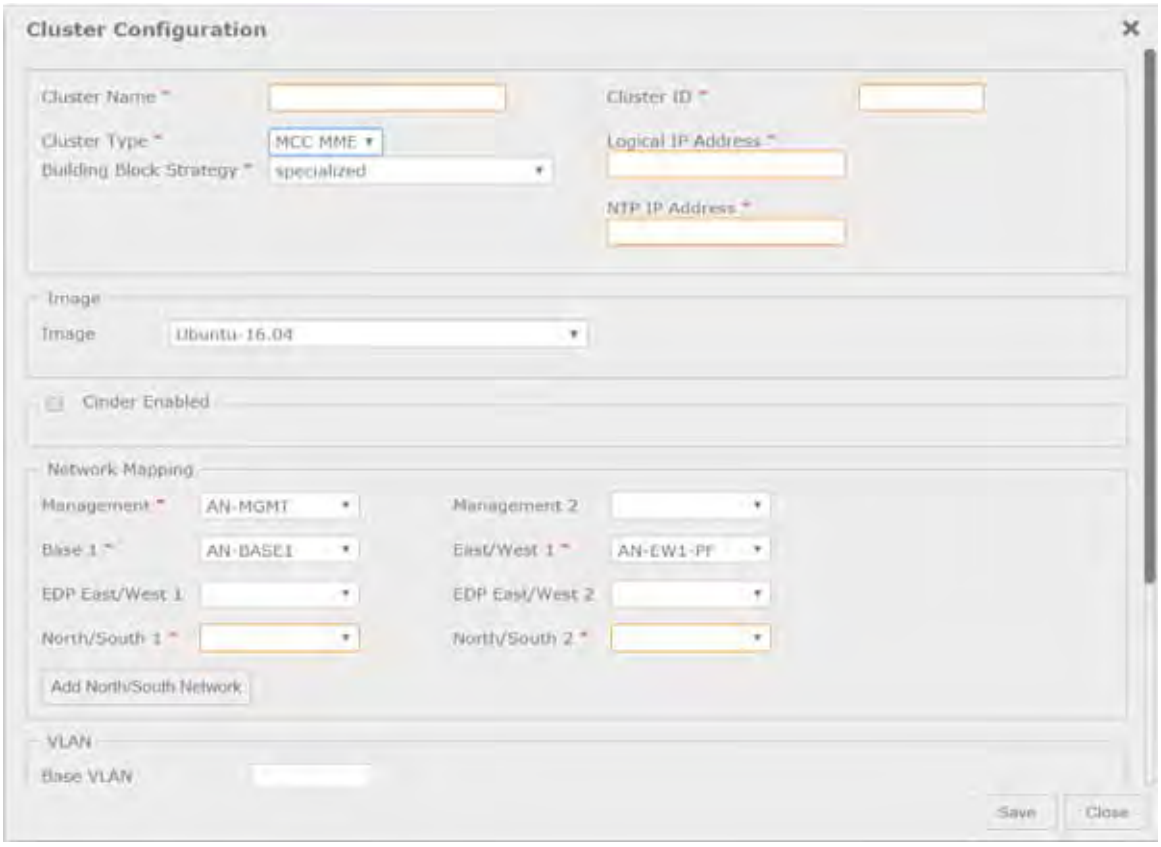
vCloud Director Screen (MCC Only):



OpenStack Screen for MCC:



OpenStack Screen for MCC MME:



3 Configure the parameters as follows:

Table 6-11 Cluster Configuration Parameters

Parameter	Applies to	Description
Cluster Name	*All*	Cluster name
Cluster Type	*OpenStack Only*	Specifies the cluster type: ■ MCC ■ MCC MME
Cluster ID	*All*	Cluster ID (common to all VMs in a cluster). Valid range is 1 to 127.

Table 6-11 Cluster Configuration Parameters

Parameter	Applies to	Description
Building Block Strategy	*All*	Specifies the supported combinations of node types/personalities to build the cluster **For MCC:** ■ advanced-services-separation: – MCM – CSM: ASM, CPM – SSM (without personality) ■ control-services-separation — MCM, ASM, SSM, CCM, DCM ■ compact — MCM, CSM, SSM ■ specialized — ASM, CCM, DCM, IOM, MCM, WSM ■ integrated-services – MCM – CSM: CPM – SSM: ISM (Integrated Services Module: Content and Subscriber Services) ■ integrated-workflow: – MCM – CSM: CPM – SSM: IOM – SSM: IWM (Integrated Workflow Module) **For MCC MME:** ■ compact (corresponds to 2-VM Model): – mrm – msm ■ specialized (corresponds to 5/6/7-VM Model): – mgmt – rm – callp – sig – lb – data – edp The personalities available for the cluster are filtered based on the Building Block Strategy.
Logical IP Address	*All*	IP Address to be used by the active MCM.
NTP IP Address	*All*	IP address of the NTP server
Disk Format	*vCenter Only*	■ Thin Provision ■ Thick Provision Eager Zeroed

Table 6-11 Cluster Configuration Parameters

Parameter	Applies to	Description
SR-IOV Configuration	*MCC Cluster Only*	This setting defines the required networks for the nodes: ■ none ■ ew-ns ■ ew-ns-base-mgmt (OpenStack only)
East-West Redundancy	*MCC Cluster Only*	Mark the checkbox to support East-West Redundancy for the cluster.
Base Routability Enabled	*OpenStack, vCenter, vCloud Director Only*	Mark the checkbox to enable base routability: When enabled, VNF Manager allows configuration of Base Master IP address (per cluster) and Base IP Address, and Base Netmask length (per node)
Master Base IP Address	*OpenStack, vCenter, vCloud Director Only*	***Note:*** *Applies when Base Routability is enabled.* Base Master IP is a floating IP address. It is held by the active MCM node.
VLAN Stripping Enabled	*OpenStack Only* *MCC Cluster Only*	Mark the checkbox to enable VLAN stripping: Enable VLAN stripping for OpenStack deployments that do not allow Flat Networks and instead manage VLAN tagged traffic before the traffic arrives at the MCC. In these cases, network interfaces within the MCC must be configured as untagged. Untagged packets sent from the MCC are tagged by the OpenStack controller.
EW L3 Connectivity Enabled	*OpenStack, vCenter, vCloud Director Only*	Mark the checkbox to enable EW L3 for the cluster: When enabled, VNF Manager allows configuration of IP address(es) and netmask length(es) for EW networks
Image	*OpenStack Only*	
Controller	*MCC Cluster Only*	Controller image
Payload	*MCC Cluster Only*	Payload image
Image	*MCC MME Cluster Only*	Image for MCC MME
Cinder Enabled		Mark the checkbox to enable boot and ephemeral Cinder block volumes.
Controller Boot Size	*MCC Cluster Only*	Cinder volume in GB for the Controller boot images Example: 112 Required only when Cinder is enabled.
Payload Boot Size	*MCC Cluster Only*	Cinder volume in GB for the Payload boot images Example: 50 Required only when Cinder is enabled.
Boot Size		The Cinder boot volume in GB for all nodes/VMs. Required only when Cinder is enabled.

Table 6-11 Cluster Configuration Parameters

Parameter	Applies to	Description
(MGMT&RM) or MRM Ephemeral Size	*MCC MME Cluster Only*	The Cinder ephemeral volume in GB for mgmt and rm nodes/VMs. The default is 200. Required only when Cinder is enabled.
Other Ephemeral Size	*MCC MME Cluster Only*	The Cinder ephemeral volume in GB for nodes/VMs other than mgmt and rm. Required only when Cinder is enabled.
OVA Templates	*vCenter Only*	
MCM template		MCM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in VNF Manager. For details, see vCenter Only: Uploading Open Virtualization Archive (OVA) Packages.
CSM template		CSM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in VNF Manager. For details, see vCenter Only: Uploading Open Virtualization Archive (OVA) Packages.
SSM template		SSM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in VNF Manager. For details, see vCenter Only: Uploading Open Virtualization Archive (OVA) Packages.
vApp Templates	*vCloud Director Only*	
MCM template		MCM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in vCloud Director Catalog as a vAppTemplate.
CSM template		CSM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in vCloud Director Catalog as a vAppTemplate.
SSM template		SSM Open Virtualization Archive (OVA) package template. The template must have already been uploaded in vCloud Director Catalog as a vAppTemplate.
Network Mapping	*OpenStack Only*	
Management		AN Management Network Label Required.
Management 2	*MCC MME Cluster Only*	AN Management Network Label Required.
Base 1		AN Base 1 Network Label Required.
Base 2	*MCC Cluster Only*	AN Base 2 Network Label Required for cluster with East/West redundancy.

Table 6-11 Cluster Configuration Parameters

Parameter	Applies to	Description
East/West 1		East-West 1 Network Label Used by CSM and SSM nodes.
East/West 2	*MCC Cluster Only*	East-West 2 Network Label Required for cluster with East/West redundancy for CSM and SSM nodes.
North/South 1		North-South 1 Network Label Used by SSM nodes.
North/South 2		North-South 2 Network Label Used by SSM nodes.
Add North/South Network		Click **Add North/South Network** to configure additional North/South networks (up to 24 total). Specify the North-South Network Label for each North/South network. You must configure the networks consecutively without gaps. As an alternative, you can configure North/South networks at the node level (see Configuring Nodes in the Cluster). In that case, VNF Manager *does not* use the North/South networks configured at the cluster level.
North/South 3		North-South 3 Network Label Used by SSM nodes.
North/South 4		North-South 4 Network Label Used by SSM nodes.
North/South 5		North-South 5 Network Label Used by SSM nodes.
North/South 6		North-South 6 Network Label Used by SSM nodes.
North/South 7		North-South 7 Network Label Used by SSM nodes.
North/South 8		North-South 8 Network Label Used by SSM nodes.
North/South 9		North-South 9 Network Label Used by SSM nodes.
North/South 10		North-South 10 Network Label Used by SSM nodes.
North/South 11		North-South 11 Network Label Used by SSM nodes.

Table 6-11 Cluster Configuration Parameters

Parameter	Applies to	Description
North/South 12		North-South 12 Network Label Used by SSM nodes.
North/South 13		North-South 13 Network Label Used by SSM nodes.
North/South 14		North-South 14 Network Label Used by SSM nodes.
North/South 15		North-South 15 Network Label Used by SSM nodes.
North/South 16		North-South 16 Network Label Used by SSM nodes.
North/South 17		North-South 17 Network Label Used by SSM nodes.
North/South 18		North-South 18 Network Label Used by SSM nodes.
North/South 19		North-South 19 Network Label Used by SSM nodes.
North/South 20		North-South 20 Network Label Used by SSM nodes.
North/South 21		North-South 21 Network Label Used by SSM nodes.
North/South 22		North-South 22 Network Label Used by SSM nodes.
North/South 23		North-South 23 Network Label Used by SSM nodes.
North/South 24		North-South 24 Network Label Used by SSM nodes.
VLAN		
Base VLAN A		VLAN ID for Base interconnect.
Base VLAN B		VLAN ID for redundant Base interconnect. (only for East-West Redundancy support).
East West VLAN A		VLAN ID for East-West.
East West VLAN B		VLAN ID for redundant East-West. (only for East-West Redundancy support).

Table 6-11 Cluster Configuration Parameters

Parameter	Applies to	Description
Security		
Enable Root SSH Access	*MCC Cluster Only*	Mark the checkbox to enable user SSH access (strongly recommended to unmark).
Enable Multiple Sessions	*MCC Cluster Only*	Mark the checkbox to enable multiple simultaneous logins per username.
Security Group		Security Group: ■ When a security group is configured, the VNF Manager creates all ports associated with the security group. ■ When no security group is configured, VNF Manager creates all ports with port security disabled. ***Note:*** *This behavior is a fundamental change from the prior functionality where (when no security group was configured) the cluster was deployed with the default security group.*

4 Click **Save**.

Once the cluster configuration is completed, you can add nodes to the cluster.

Modifying Cluster Configuration

You can modify a cluster configuration, as long as the cluster *is not* already commissioned and running.

To modify cluster configuration:

1 From the **Cluster** window, select a Virtualized Infrastructure Manager (VIM) in the right pane.

2 Click the cluster you want to modify in the right pane.

VNF Manager lists the Hosts/Availability Zones managed by the VNF Manager.

3 On the cluster in the left pan, click the **View Cluster Configuration** icon.

VNF Manager displays the **Cluster Configuration** screen listing the details.

4 Make the changes and click **Save**.

5 In the **Cluster Configuration** screen, click **Close**.

Configuring Nodes in the Cluster

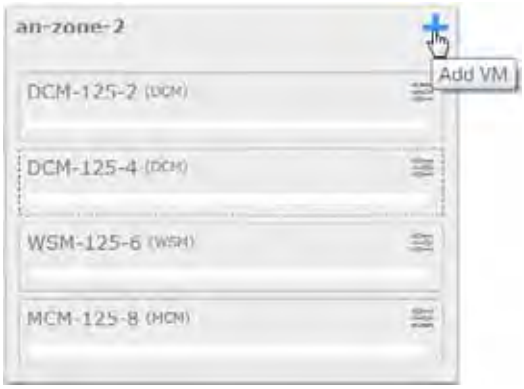
Note: *The procedure is not required if you import a CSV file containing all the configuration information. However, you can use this procedure to make additional changes to the cluster.*

Rules:

- Each cluster must have at least the MCM-7 VM defined.
- Each host can support only one of VM type SSM.

To configure a node to the cluster:

1. To add a VM to the cluster, expand the appropriate item in the right pane:
   - *vCenter:* **Hosts**
   - *vCloud Director:* **Organization vDC**
   - *OpenStack:* **Availability Zones**
2. Drag and drop a host/organization vDC/availability zone to the cluster.
3. To configure the VM, click the host/organization vDC/availability zone's **Add VM** icon.



Acuitas displays the **VM Configuration** screen.

Figure 6-6 vCenter VM Configuration Screen

vCenter Screen:

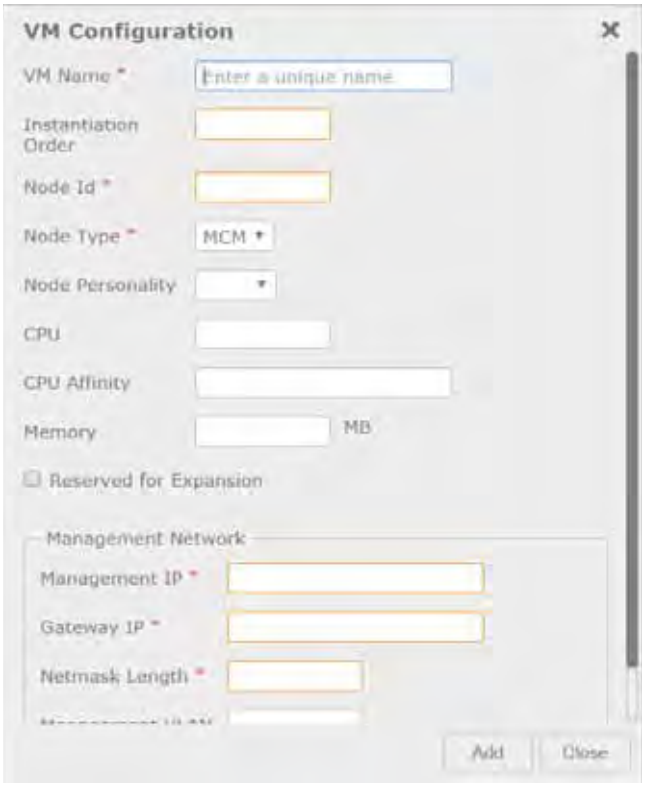


Figure 6-7 vCloud Director VM Configuration Screen

vCloud Director Screen:

Figure 6-8 OpenStack VM Configuration Screen for MCC

OpenStack for MCC Screen:

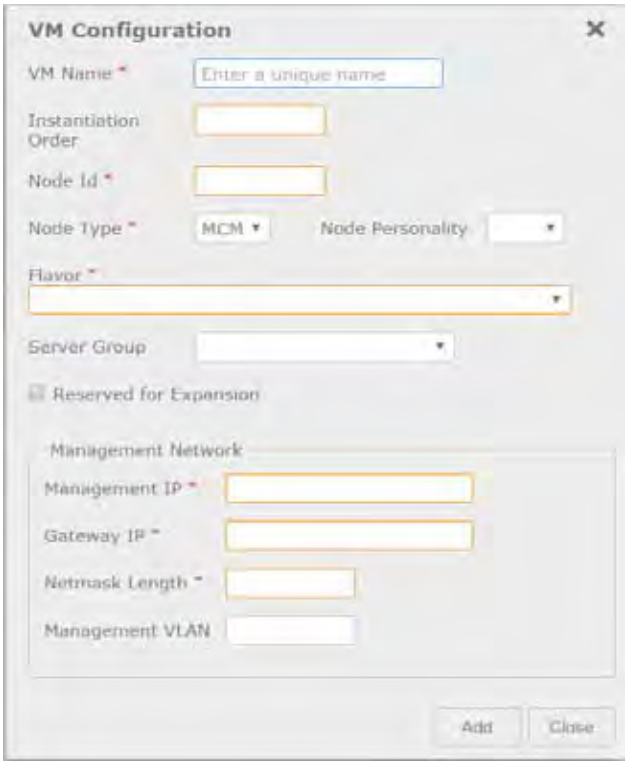
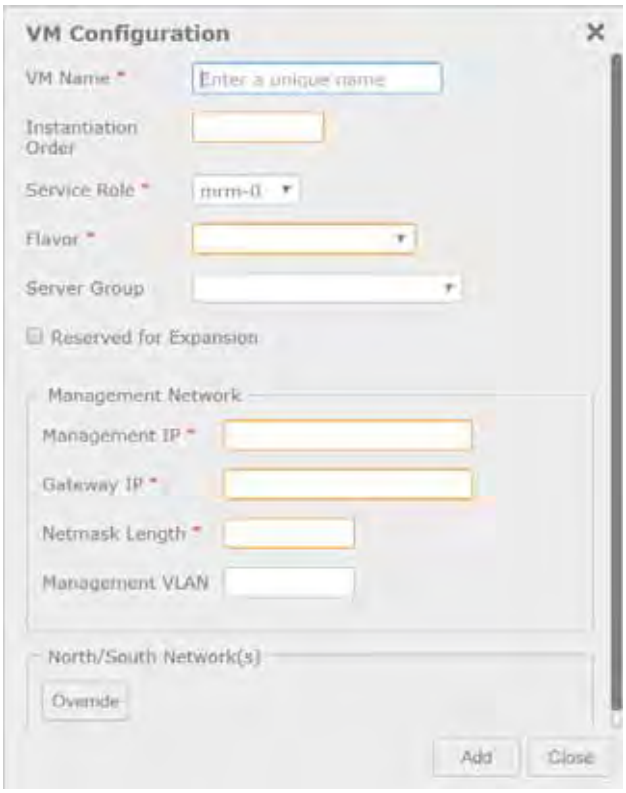


Figure 6-9 OpenStack VM Configuration Screen for MCC MME

OpenStack for MCC MME Screen:



4 Configure the parameters as follows:

Table 6-12 VM Configuration Parameters

Parameter	Applies to	Description
VM Name	*All*	VM name. Default name is <*Node Type*>-<*Cluster ID*>-<*Node ID*>
Instantiation Order	*vCenter and OpenStack Only*	VM instantiation order to be applied during cluster instantiation. If no instantiation order specified, VNF Manager instantiates VMS by ascending node type ID: mcm (1), ssm (2), csm (3), mgmt (10), rm (11), callp (12), sig (13), lb (14), data (15), edp (16), mrm (17), msm (18) If some VMs in a cluster have instantiation order specified, VNF Manager first instantiates those VMs according to instantiation order, then instantiates the other VMs according to ascending node type ID. In the case of mgmt/mrm of MCC MME, mgmt-0/mrm-0 are always be instantiated first and mgmt-1/mrm-1 are always instantiated last, regardless of specified instantiation order.

Table 6-12 VM Configuration Parameters

Parameter	Applies to	Description
Service Role	*MCC MME Cluster Only*	Server role the VM performs: ■ mgmt-N (N=0-1) ■ rm-N (N=0-1) ■ sig-N (N=0-19) ■ callpN-M (N=0-15, M=0-1) ■ lb-N (N=0-7) ■ data-N (N=0-15) ■ edp-N (N=0-15)
Node ID	*MCC Cluster Only*	For MCM VM: ■ Range: 7 or 8 For CSM VM: ■ Range: 1-128. ■ Cannot be 7 or 8. For SSM VM: ■ Range: 1-128. ■ Cannot be 7 or 8. ***Note:*** *Setting SSM Node ID to 1 is not recommended because it can result in dropped proxy traffic for some sessions by the Linux Kernel on the CSM. To disallow setting SSM Node ID to 1:* *1. Edit /opt/Affirmed/NMS/server/ems/resources/cloud.properties and set the following property: cloud.ssm.nonode1.enabled=true* *2. Restart the Acuitas server*
Node Type	*MCC Cluster Only*	VM Type: ■ MCM ■ CSM ■ SSM

Table 6-12 VM Configuration Parameters

Parameter	Applies to	Description
Node Personality	*MCC Cluster Only*	For MCM VM, leave this field blank. MCM is required for all Building Block Strategies. For CSM VM, the personalities available are filtered based on the Building Block Strategy ■ compact: – Leave blank ■ advanced-services-separation: – ASM: Advanced Services Module – CPM: Control Plane Module ■ control-services-separation: – ASM (Advanced Services Module – Content services) – CCM: Centralized Control Module – DCM: Distributed Control Module ■ specialized: – ASM: Advanced Services Module – CCM: Centralized Control Module – DCM: Distributed Control Module ■ integrated-services – CSM: CPM ■ integrated-workflow: – CSM: CPM For SSM VM, the personalities available are filtered based on the Building Block Strategy ■ compact: – Leave blank ■ advanced-services-separation: – Leave blank ■ specialized: – IOM: I/O Module – WSM: Workflow Services Module ■ control-services-separation: – SSM (leave personality blank) ■ integrated-services – SSM: ISM (Integrated Services Module: Content and Subscriber Services) ■ integrated-workflow: – SSM: IOM – SSM: IWM (Integrated Workflow Module)

Table 6-12 VM Configuration Parameters

Parameter	Applies to	Description
CPU	*vCenter Only*	CPU value For MCM VM: ■ Default: 8 For CSM VM: ■ Range: 8-18 ■ Default: 8 For SSM VM: ■ Range: 8-20 ■ Default: 20 Not required for non-SR-IOV systems.
CPU Affinity	*vCenter Only*	CPU Affinity range. Required for systems with specialized building block strategy.
Memory	*vCenter Only*	Memory value, in MB For MCM VM: ■ Range: 8-16 ■ Default: 16 For CSM VM and SSM VM: ■ Range: 32-64 ■ Default: 64 Not required for non-SR-IOV systems.
Secondary Disk	*vCloud Director Only*	Secondary Disk (SCSI type only), in MB
vApp Name	*vCloud Director Only*	vApp Name
Flavor	*OpenStack Only*	OpenStack Flavor
Server Group	*OpenStack Only*	OpenStack server group
North/South Network IP Addresses	*OpenStack Only*	Configure North/South 1 IP address and North/South 2 IP address for the following VM types: ■ MCC SSM VM ■ MCC MME LB | DATA | EDP VM Click **Additional North/South IP(s)** to configure additional North/South IP addresses.

Table 6-12 VM Configuration Parameters

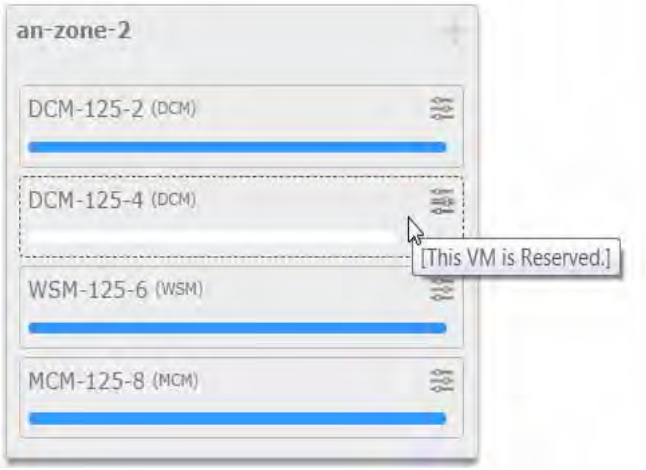
Parameter	Applies to	Description
Override North/South Network(s)	*OpenStack Only*	Click **Override** to configure North/South networks for the following VM types: ■ MCC SSM VM ■ MCC MME LB | DATA | EDP VM Specify the North-South Network Label for up to 24 North/South networks. You must configured the networks consecutively without gaps. If you *do not* configure North/South networks at the node level, VNF Manager uses the North/South networks configured at the cluster level (see Cluster-Level Configuration).
Reserved for Expansion	*All VM Types*	Mark the checkbox to reserve the VM for capacity management rather than create the VM at the time of commissioning. Later, once a cluster expansion/contraction policy is associated with the cluster, the pool of VMs is used for the required elasticity of the cluster when the thresholds for creating/removing VMs are reached. Only VMs reserved for capacity management can be dynamically or manually added. ***Note:*** *For an MCC cluster with a single MCM, it is recommended that its cluster configuration* ***not have*** *the other MCM set to reserved. Otherwise the VNF Manager marks that MCM as instantiated due to its existence in the MCC configuration.*
Management IP	*All VM Types*	IP Address for the VM to be used to access (ssh) the VM.
Gateway IP	*All VM Types*	Gateway IP address for Management IP. ***Note:*** *MCC MME can be deployed with a private network for non-mgmt nodes/VMs. In this scenario, the VNF Manager still requires you to input Gateway IP and Netmask Length for the non-mgmt nodes/VMs even though they are not used by the nodes/VMs. You can input the same Gateway IP and Netmask Length as those configured for the mgmt nodes/VMs.*
Netmask Length	*All VM Types*	Netmask length for Management IP address. Range: 0 - 32 ***Note:*** *MCC MME can be deployed with a private network for non-mgmt nodes/VMs. In this scenario, the VNF Manager still requires you to input Gateway IP and Netmask Length for the non-mgmt nodes/VMs even though they are not used by the nodes/VMs. You can input the same Gateway IP and Netmask Length as those configured for the mgmt nodes/VMs.*
Management VLAN	*All VM Types*	Management VLAN ID to be used for the Management IP addresses. Range: 0-4095
Base IP	*OpenStack, vCenter, vCloud Director Only*	***Note:*** *Applies when Base Routability is enabled.* IP address for Base network
Base Netmask Length	*OpenStack, vCenter, vCloud Director Only*	***Note:*** *Applies when Base Routability is enabled.* Netmask length for Base network

Table 6-12 VM Configuration Parameters

Parameter	Applies to	Description
East/West 1 IP	*OpenStack, vCenter, vCloud Director Only*	***Note:*** *Applies when Base Routability is enabled.* IP address of EW 1 network
East/West 1 Netmask Length	*OpenStack, vCenter, vCloud Director Only*	***Note:*** *Applies when East-West Redundancy is enabled.* Netmask length of EW 1 network
East/West 2 IP	*OpenStack, vCenter Only*	***Note:*** *Applies when East-West Redundancy is enabled.* IP address of EW 2 network
East/West 2 Netmask Length	*OpenStack, vCenter Only*	***Note:*** *Applies when East-West Redundancy is enabled.* Netmask length of EW 2 network

5 Click **Add**.

The VM is added to the cluster. If the VM is reserved for capacity management, it has a dotted outline.



Modifying VM Configuration

You can modify VM configuration, as long as the cluster *is not* already instantiated.

To modify VM configuration:

1 On the VM in the node, click the **Virtual Machine Operations** icon and select **View Configuration Details**.

VNF Manager displays the **VM Configuration** screen listing the details.

2 Make the changes and click **Save**.

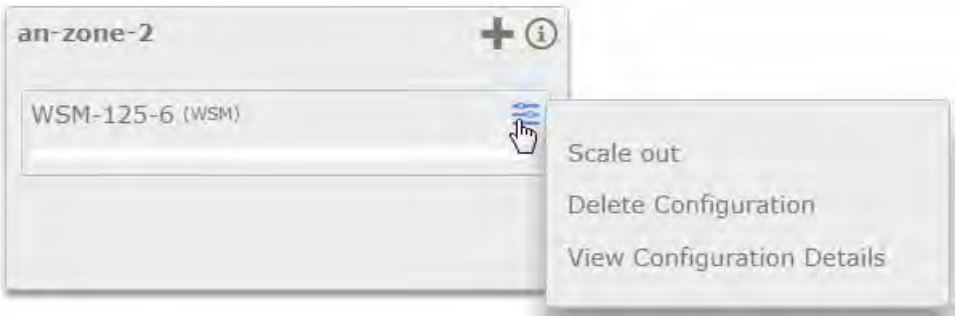
3 In the **VM Configuration** screen, click **Close**.

Deleting a VM

You can delete a VM, as long as the cluster *is not* already instantiated.

To delete VM configuration:

1 On the VM in the node, click the **Virtual Machine Operations** icon and select **Delete Configuration**.



2 At the confirmation prompt, click **Yes**.

Validating Cluster Configuration

You can execute validation checks on the cluster configuration:

- If the cluster *has not* yet been deployed, the operation validates the entire cluster hosts/VMs. You could perform this operation to verify the cluster before actually instantiating the cluster (as instantiation might require a maintenance window).
- If cluster has already been deployed, the operation validates only the additional host/VMs that are not reserved for expansion.

Validation performs the following checks:

- Validates VM name's uniqueness (no duplicate names) per vCenter.
- Validates Datastore name for space and/or parenthesis per host.
- Validates vSwitch SR-IOV-enable status against cluster level SR-IOV-enable and EW-Redundancy setting for the following networks:
  - East-West 1 Network
  - East-West 2 Network
  - North-South 1 Network
  - North-South 2 Network
- Validates communication/connectivity between vCenter and host.

To validate cluster configuration:

1. Click the **Cluster Operations** icon and click **Validate Cluster Configuration**.
2. At the confirmation prompt, click **Yes**.

Instantiating the Cluster

Once a cluster and its VMs have been successfully configured, you can instantiate the cluster. You do so by invoking the **Instantiate Cluster** command, which performs a sequence of commands to the VIM and network element, including:

- Validates cluster configuration
- Deploys the OVAs to the VIM
- Configures the VMs
- Powers on the VMs
- Configures the cluster
- Manages the cluster in the Network View

If a VM was reserved for capacity management (the **Reserved for Expansion** checkbox was checked), the VM is not created at the time of commissioning. Instead, once a cluster expansion/contraction policy is associated with the cluster, the pool of VMs is used for the required elasticity of the cluster when the thresholds for creating/removing VMs are reached. Only VMs reserved for capacity management are dynamically or manually added.

To instantiate the cluster:

1. Click the **Cluster Operations** icon and click **Instantiate Cluster**.
2. At the confirmation prompt, click **Yes**.

Checking Operation Progress

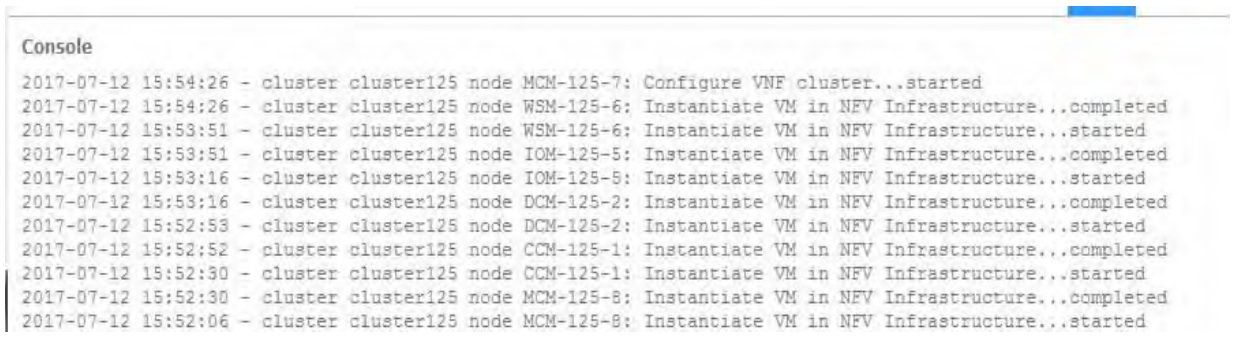
During instantiation, you can check operation progress.

To check operation progress:

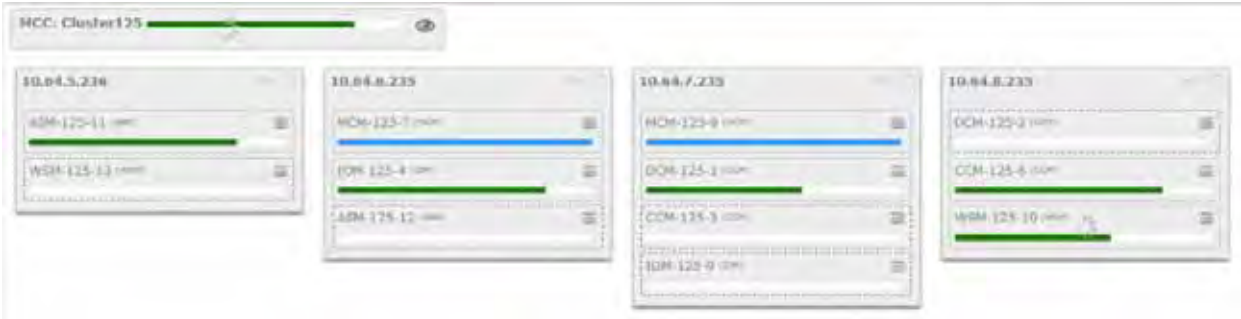
1. Expand **Clusters** in the right pane.
2. Click the cluster in the right pane.

The VNF Manager displays the **Console** window, listing the detailed steps of the process.

Figure 6-10 Console Window



During instantiation, the VNF Manager displays the cluster in the **Cluster** window, showing the progress of instantiating the nodes and VMs.



Scaling In Cluster to Remove Nodes in an Inconsistent State

When an error is encountered during instantiation, that node is ignored and cluster expansion continues. You can scale in the cluster to remove any nodes with errors that left them in an inconsistent state.

To scale in a cluster:

1. Click the **Cluster Operations** icon and click **Scale In Cluster**.
2. For an MCC cluster, enter the **Scale In Node IDs** that you want to remove. Separate multiple IDs with a comma.

   For an MCM node, you can scale in only one at a time. You *cannot* scale in an MCM with other nodes.

   For an MCC MME cluster, enter the **Node Service Roles** that you want to remove. Separate multiple roles with a comma.

For MCC MME MGMT/RM/MRM nodes, you can scale in only one at a time. You *cannot* scale in these nodes with other nodes.

3 Click **OK**.

Scaling Out Cluster to Instantiate Nodes

Scale out handles node creation errors. When an error is encountered, that node is ignored and cluster expansion continues.

After you have scaled in any failed nodes and fixed the underlying issues, you can scale out those nodes.

You *cannot* scale out an unreserved MCM. Instead, scale out an unreserved MCM using the procedure Scaling Out Nodes.

To scale out a cluster:

1 Click the **Cluster Operations** icon and click **Scale Out Cluster**.

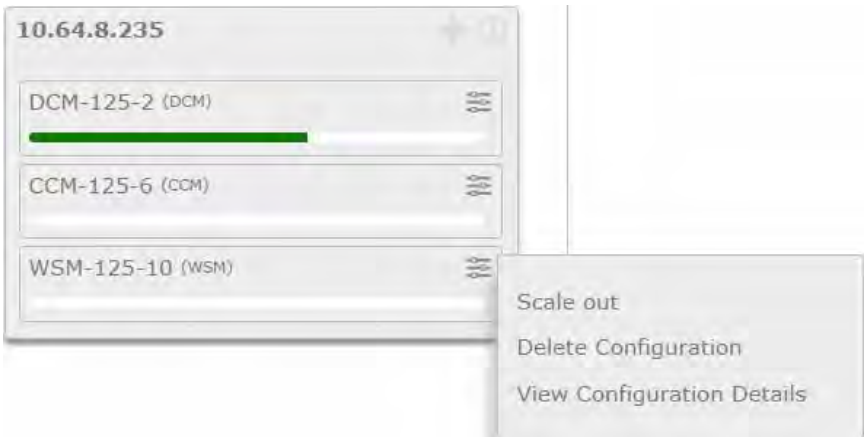
2 At the confirmation prompt, click **Yes**.

Scaling Out Nodes

The VNF Manager supports manual creation of all node types for both MCC and MCC MME. Manual scale out adds one VM to a cluster, as long as the VM *is not* already instantiated.

To manually scale out a node:

1 On the VM in the node, click the **Virtual Machine Operations** icon and select **Scale Out**.



2 At the confirmation prompt, click **Yes**.

Manual Scale Out Considerations

Keep in mind that if you manually scale out a cluster that has an associated scale-in policy, the policy may remove the node you added. If the VNF Manager detects that the cluster is in an underload condition specified by the scale-in policy, it immediately removes the node you added. To avoid this situation, before you manually add a node, either:

- Disable the policy — Modify the associated policy, mark the **Disable Policy** checkbox, and click **Save**. For details, see Modifying a Policy. This method disables the policy for all clusters associated with it.
- Disassociate the cluster from the policy — Modify the associated policy, click the **X** icon of the cluster in the **Clusters Using This Policy** field, and click **OK**. For details, see Disassociating a Policy from a Cluster. This method only disables the policy for this cluster.

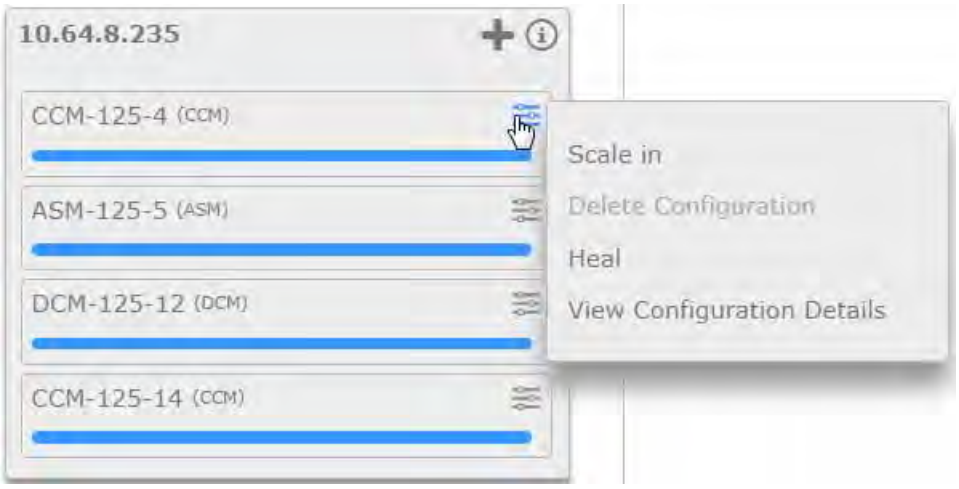
Scaling In Nodes

The VNF Manager supports manual removal of all node types for both MCC and MCC MME. The scale in is launched for an instantiated node/VM.

In the case of management nodes/VMs, you can perform scale in only on the current standby node. If you select the active node, you are prompted to first perform a manual switchover to the standby node (to do so, issue the mcmswitchover command at the Cluster <*ID*>).

To manually scale in a node:

1 On the VM in the node, click the **Virtual Machine Operations** icon and select **Scale In**.



2 At the confirmation prompt, click **Yes**.

Manual Scale In Considerations

Keep in mind that if you manually scale in a cluster that has an associated scale-out policy, the policy may add the node you removed. If the VNF Manager detects that the cluster is in an overload condition specified by the scale-out policy, it immediately adds back the node you removed. To avoid this situation, either:

- Disable the policy — Modify the associated policy, mark the **Disable Policy** checkbox, and click **Save**. For details, see Modifying a Policy. This method disables the policy for all clusters associated with it.
- Disassociate the cluster from the policy — Modify the associated policy, click the **X** icon of the cluster in the **Clusters Using This Policy** field, and click **OK**. For details, see Disassociating a Policy from a Cluster. This method only disables the policy for this cluster.

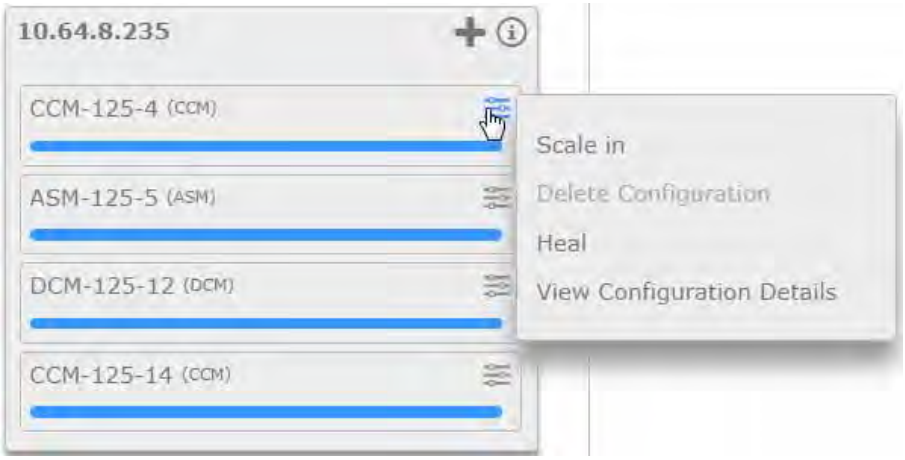
Healing Nodes

The VNF Manager supports healing a failed MCC node or MCC MME node when manually initiated by an Operator. VNF Manager performs healing operations by removing the failed node and instantiating it to either the same host or a new host. Healing operations ensure that the node configuration remains intact to avoid impacting services.

- For MCC nodes, healing is supported in OpenStack and vCenter deployments. To support healing of MCMs, the MCC must be deployed with two MCM nodes.
- For MCC MME nodes, healing is supported in OpenStack deployments. To support healing of mcms, the MCC MME must be deployed with two mgmt nodes.
- Healing is supported for standby MCC MCM, MME MGMT/RM/MRM node and other nodes. Active MCC MCM, MME MGMT/RM/MRM node cannot be healed.

To heal a node:

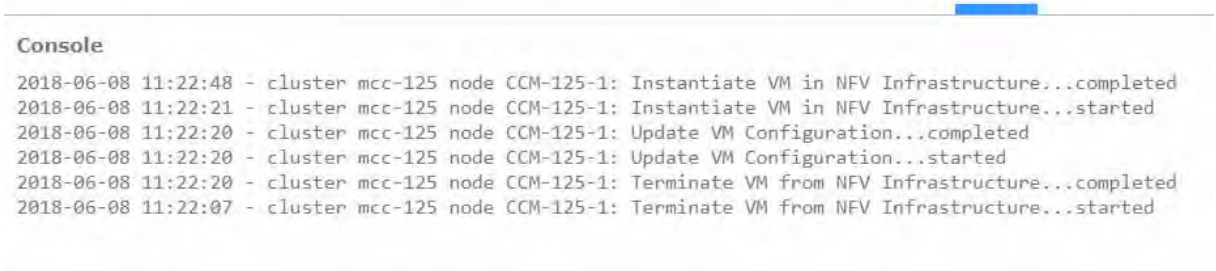
1. On the VM in the node, click the **Virtual Machine Operations** icon and select **Heal**.



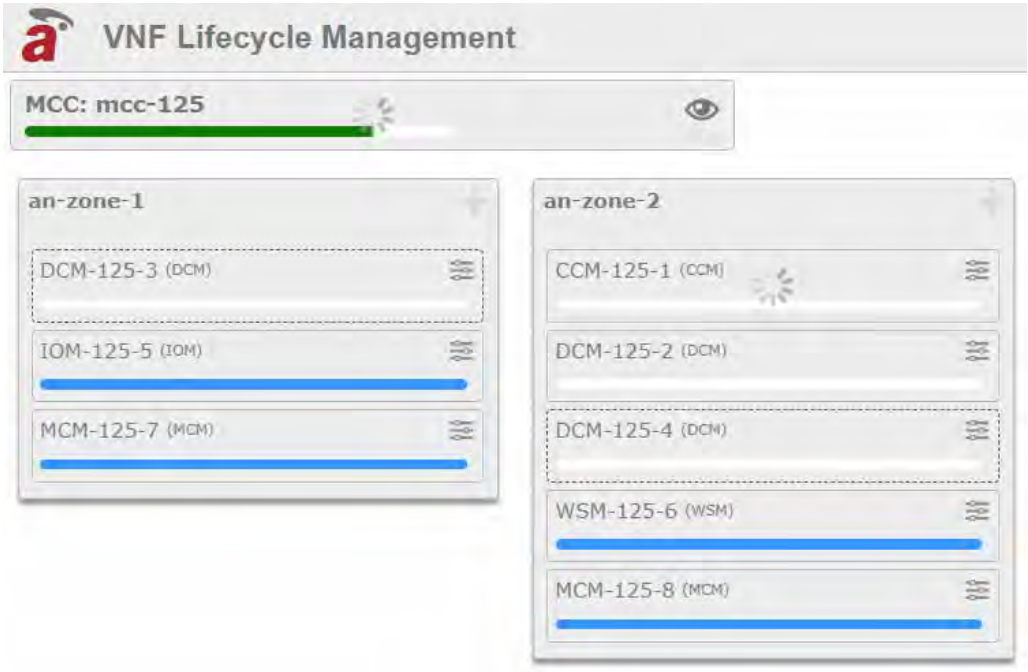
2 Select the Target Availability Zone (OpenStack) or Target Host (vCenter) and click **OK**.

3 At the confirmation prompt, click **Yes**.

The VNF Manager lists the detailed steps of the process in the **Console** window including listing the update to the target Availability Zone or Host.



During healing, the VNF Manager displays the cluster in the **Cluster** window, showing the progress of instantiating the node.



Healing Considerations

In some cases, the VNF Manager cannot remove the failed node. For example, if the host for the node is down, the VIM (OpenStack or vCenter) may not allow the VNF Manager to un-deploy the node. In this case, the VNF Manager returns an error. The OpenStack or vCenter administrator must perform appropriate tasks, for example, remove the host from inventory to allow for the un-deployment of the node. Then, the Operator can retry the Heal operation.

The VNF Manager does not alter any configuration on the MCC or MCC MME. If incorrect configuration exists, the operator must correct the issue on the MCC.

vCenter Only: Do not heal VMs that have overlapping CPU Affinity ranges to the same host. For example, do not heal a VM with CPU Affinity range 0-8 to a host with another VM in that range. Before performing the Heal operation, verify that the CPU Affinity ranges of the VMs do not overlap.

Terminating the Cluster

You can terminate the cluster. Terminating a cluster is a non-recoverable procedure. It terminates all services performed by the cluster.

To terminate a cluster, invoke the **Terminate Cluster** command, which kicks off the sequence of commands to the VIM and network element, including:

- Powers off the VMs
- Removes the VMs from the host
- Unmanages the cluster from the Network View

To terminate the cluster:

1. To terminate the cluster, click the **Cluster Operations** icon and click **Terminate Cluster**.
2. At both confirmation prompts, click **Yes**.

Aborting Cluster Operation

You can abort an ongoing cluster operation (intantiation/scaleout/termination). The **Abort Operation** command submits a request to stop the ongoing operation in the next logical step.

To abort the cluster operation:

1. To abort the cluster operation, click the **Cluster Operations** icon and click **Abort Operation**.
2. At the confirmation prompt, click **Yes**.

Downloading Cluster Configuration

You can download the cluster configuration to a CSV file.

To download the cluster configuration:

1. To download the cluster configuration, click the **Cluster Operations** icon and click **Download Cluster Configuration**.
2. At the confirmation prompt, click **Yes**.

Using Cluster View

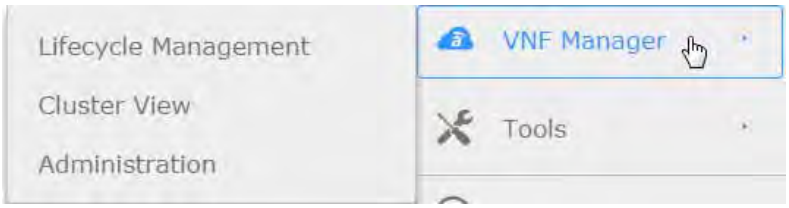
You use Cluster View to:

- View cluster alarms
- View cluster details
- View physical and logical topology
- View Key Performance Indicators
- View cluster reports
- Configure dynamic cluster scale out/ scale in

To use the Cluster View, select the **VNF Manager** > **Cluster View** option from the **Settings** icon on the toolbar.

Note: *To access the VNF Manager application, you must have the EMS Management > VNF Manager > Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

Figure 6-11 Accessing VNF Manager Application



The VNF Manager displays the **Cluster View** window, showing the clusters.

Note: *The Cluster View shows only MCC clusters, not MCC MME clusters.*

Figure 6-12 Cluster View

Each cluster lists the following information:

- Cluster name
- Status
- IP address
- Version number
- Resource Type
- Policy icon for the policy associated with the cluster
- Alarm icon with color and count representing the highest severity alarms on the cluster
- Cluster icon
- Graphical representation of usage statistics for the cluster, including number of active sessions, CPU utilization, and memory utilization

To view a single data point, point the cursor at a graph. The VNF Manager displays the data value.

- If the cluster is unreachable or unmanaged, the cluster lists the Status as Not Reachable, Unmanaged, or both.

The cluster includes a status icon indicating whether it is:

  - Unreachable
  - Unmanaged
  - Both

- If the cluster is in the process of scaling in/scaling out, the cluster includes the scale indication icon:

  - Scale In icon:
  - Scale Out icon:

To change the screen background color (dark or light):

1 From the **Settings** icon on the toolbar select **Change Theme**.

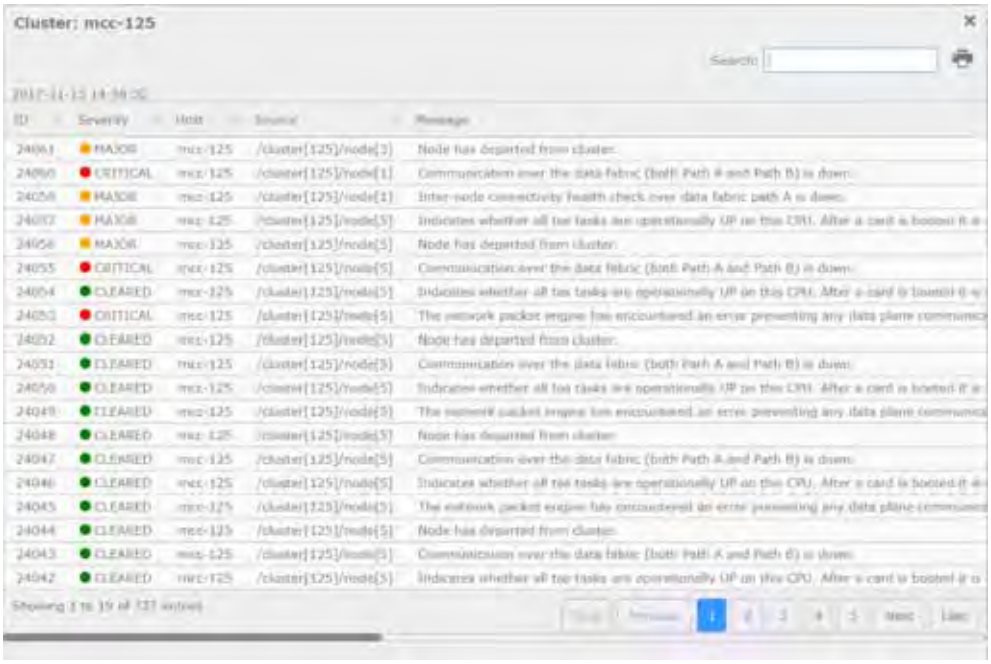
Viewing Cluster Alarms

To view cluster alarms, click the cluster's alarm icon.

The cluster's alarms are listed with the following information:

- **Alarm ID** – Unique ID of the alarm
- **Severity** – Problem severity
- **Host** – Network element reporting the problem
- **Source** – Network element component having the fault
- **Message** – Message/fault description obtained from the network element
- **Updated** – Date and time of last update of the alarm
- **Ack. Status** – Indicates whether or not the alarm is acknowledged
- **Owner** – Alarm owner
- **Category** – Alarm category, such as Temperature Threshold, CPU Threshold

Figure 6-13 Cluster Alarms



Use the Search text box on the toolbar to search for instances of an alarm.

In the case of a large number of alarms, use the page navigational bar at the bottom of the window to page through the entries.

To print the alarms, click the **Print** icon. Select the printer and click **Print**.

Click the Close icon to close the Cluster Alarm window.

Viewing Cluster Details

To view details for a cluster, click the cluster in the **Cluster View** window. The VNF Manager displays the **Cluster Details** window.

Viewing Physical and Logical Topology

To present the topology mapping relationships, the VNF Manager requires that you configure the following IP addresses:

- HP Blade System: Configure the chassis and each blade with an IP address. For instructions, see Adding a Network Element and Configuring Blade System Blades.
- Server Group: Configure each server's IP address. For instructions, see Adding a Network Element and Configuring Servers in a Group.

To view the physical and logical topology for a cluster, click **Physical View** in the **Cluster Details** window.

Figure 6-14 Physical View of a Blade System

Figure 6-15 Physical View of a Server Group

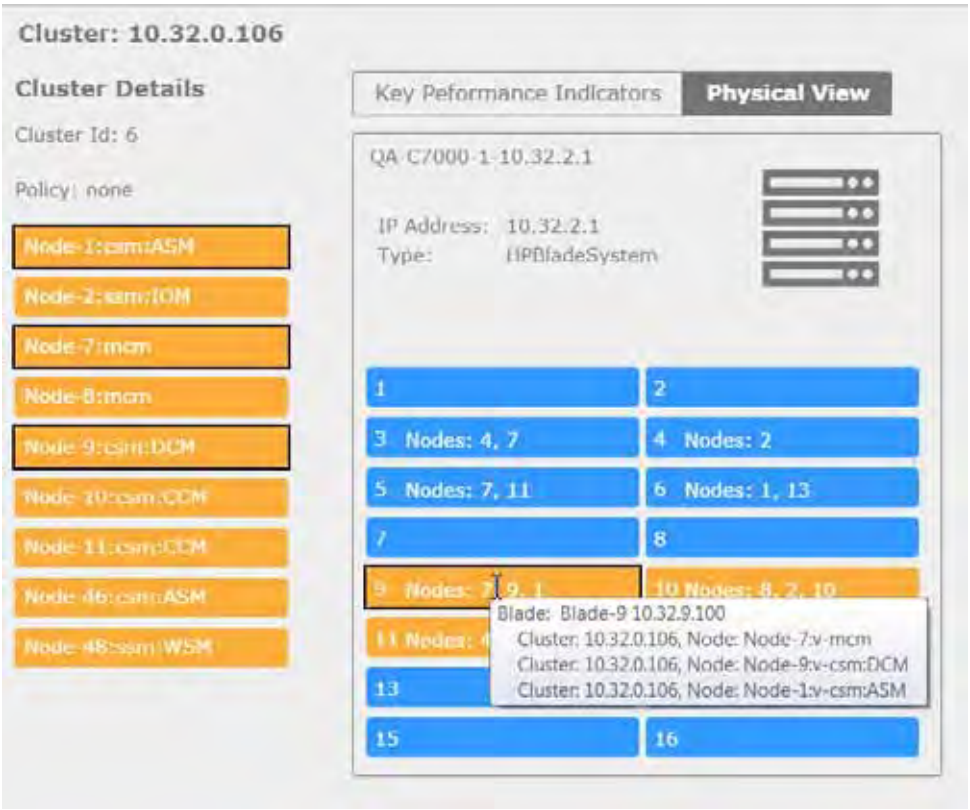
The Physical View displays the nodes in the cluster and indicates where they reside in the hosting blade system(s) or in the Server Group.

Nodes with a dotted outline are ones that the VNF Manager does not have enough information on to display physical and logical topology.

To view a node's location, point the cursor at a node in the list. The VNF Manager highlights the location in the host blade system or in the Server Group.

To view a blade's details, point the cursor at a node. The VNF Manager opens a pop-up window that lists the details of the nodes on that blade or Server Group.

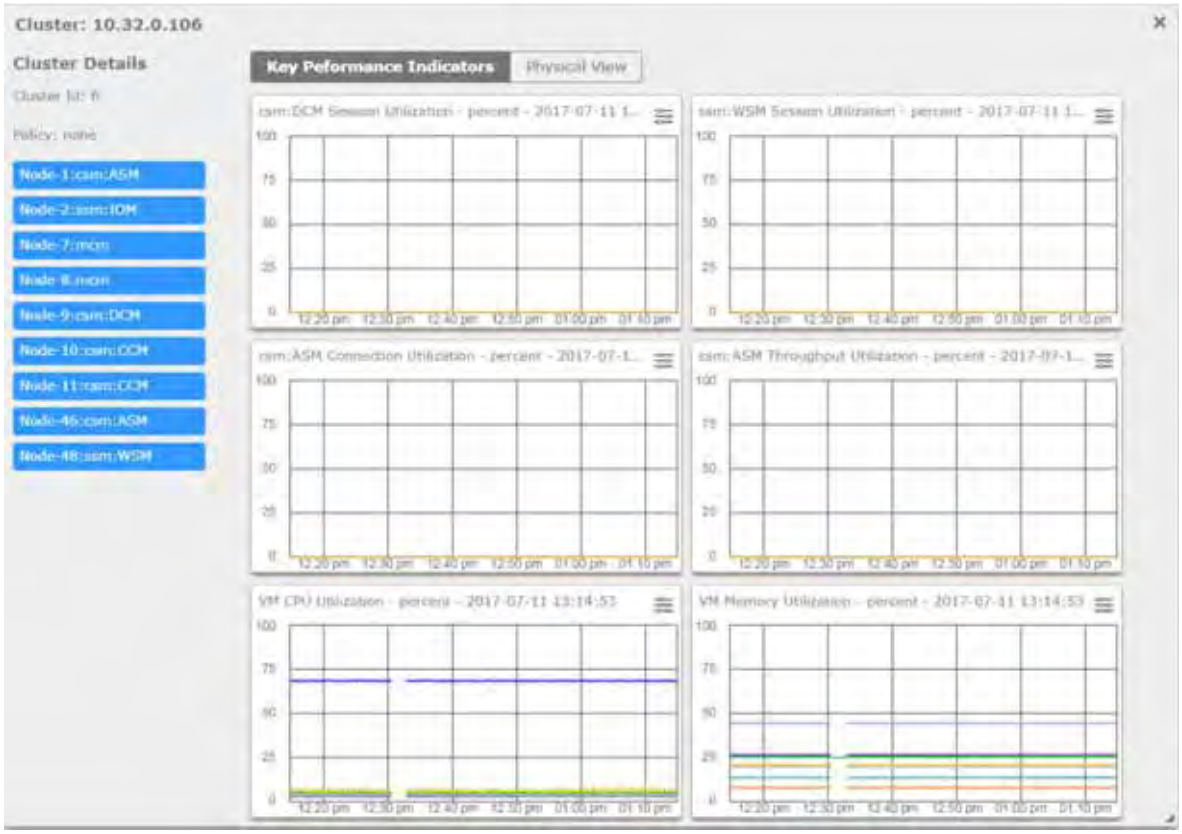
Figure 6-16 Blade Details



Viewing Key Performance Indicators

To view the Key Performance Indicators for a cluster, click **Key Performance Indicators** in the **Cluster Details** window.

Figure 6-17 Key Performance Indicators



The Key Performance Indicators View displays the cluster KPIs, updating the graphs every 10 seconds. The VNF Manager retains the collected KPIs for 60 minutes.

To toggle a graph to full screen, click the **Graph Settings** icon and select **Toggle Fullscreen**.

The cluster KPIs are listed in the following table.

Table 6-13 Cluster KPIs

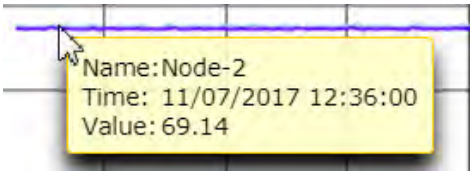
KPIs	Description
DCM Session Capacity Utilization	Is calculated as: 100 * <*number of active DCM sessions*> / <*number of designed DCM sessions for cluster*> The <*number of active DCM sessions*> is the subscriber count, which is the number of attached subscriber sessions. The <*number of designed DCM sessions for cluster*> is the aggregate maximum number of designed DCM sessions for all the v-CSM and DCM modules combined. **For specialized building block strategy, is calculated as:** (number of DCM * <*DCM Node Session Capacity*>) where <*DCM Node Session Capacity*> is configured at Infrastructure > Dynamic Scale > DCM > Node Session Capacity.
WSM Session Capacity Utilization	Is calculated as: 100 * <*number of active WSM sessions*> / <*number of designed WSM sessions for cluster*> The <*number of active WSM sessions*> is the subscriber count, which is the number of attached subscriber sessions The <*number of designed WSM sessions for cluster*> is the aggregate maximum number of designed WSM sessions for all the v-SSM and WSM modules combined. **For specialized building block strategy, is calculated as:** (number of WSM * <*WSM Node Session Capacity*>) where <*WSM Node Session Capacity*> is configured at Infrastructure > Dynamic Scale > WSM > Node Session Capacity.
ASM Connection Capacity Utilization	Is calculated as: 100 * <*number of active ASM connections*> / <*number of designed ASM connections for cluster*> The <*number of active ASM connections*> is the num_current_client_connections, a gauge on the cluster level. The <*number of designed ASM connections for cluster*> is the aggregate maximum number of designed ASM connections for all the v-CSM and ASM modules combined. **For specialized building block strategy, is calculated as:** (number of ASM * <*ASM Node Connection Capacity*>) where <*ASM Node Connection Capacity*> is configured at Infrastructure > Dynamic Scale > ASM > Node Connection Capacity.

Table 6-13 Cluster KPIs

KPIs	Description
ASM Throughput Capacity Utilization	Is calculated as: 100 * <*ASM throughput*> / <*designed ASM throughput for cluster*> <*ASM throughput*> is the rateOf (num_bytes_client_response) + rateOf (num_bytes_client_request) on the cluster level The <*designed ASM throughput for cluster*> is the aggregation of designed ASM throughput for all the v-CSM and ASM modules combined. **For specialized building block strategy, is calculated as:** (number of ASM * <*ASM Node Throughput Capacity*>) where <*ASM Node Throughput Capacity*> is configured at Infrastructure > Dynamic Scale > ASM > Node Throughput Capacity.
VMs CPU Utilization	CPU Utilization (%)
VMs Memory Utilization	Memory Utilization (MB)

To view a single data point, point the cursor at a graph.

The VNF Manager opens a pop-up window that lists the node name, timestamp, and data value.



Click the **Close** icon to close the **Cluster Details** window.

Viewing Cluster Reports (*MCC Clusters and MCC MME Clusters*)

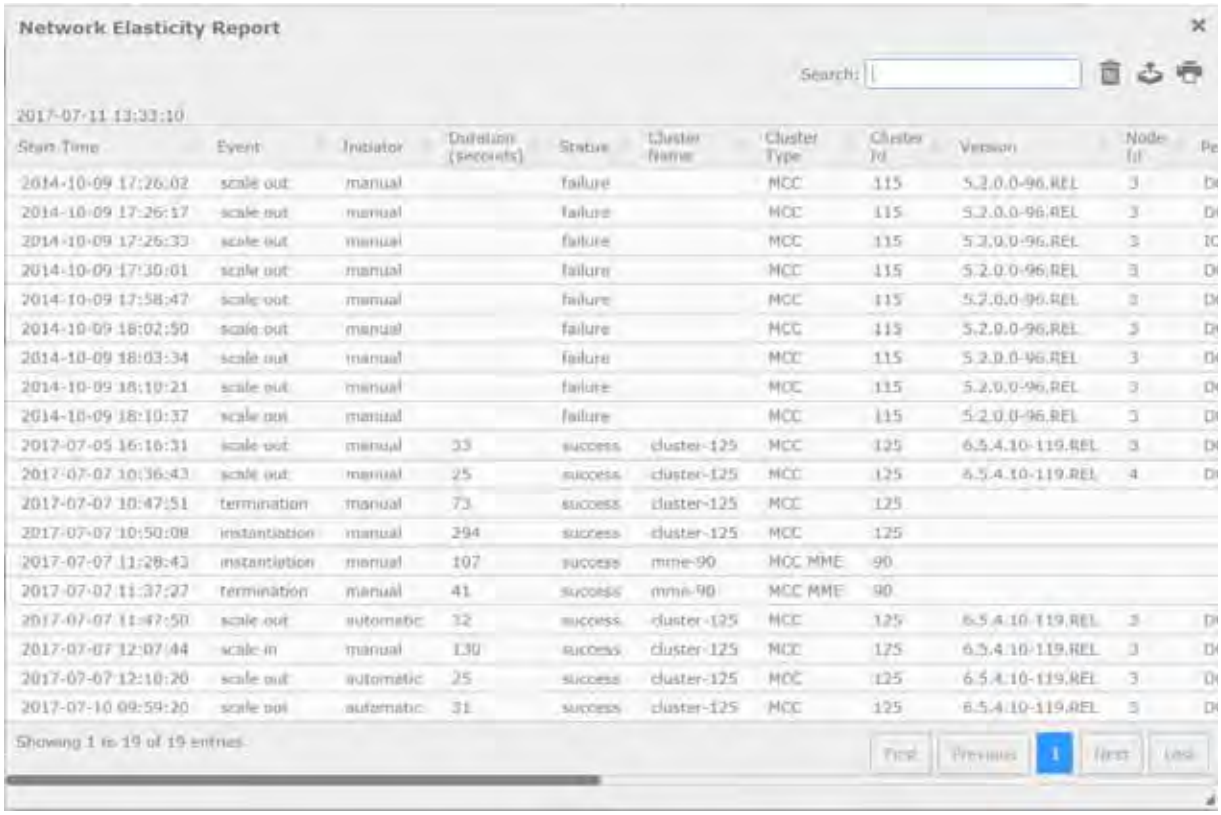
The VNF Manager provides reports on:

- Network Elasticity – Historical records on the following cluster activities and the conditions leading to dynamic scale out/scale in events:
  - Instantiation
  - Scale out
  - Scale in
  - Termination
- Network Inventory – Report on:
  - Clusters and their nodes
  - Blade Systems and their blades
  - Server Groups and their servers
  - Hosting relationships between nodes and blades

Network Elasticity Report

To view the Network Elasticity Report, click the **Reports** icon and select **Network Elasticity**.

Figure 6-18 Network Elasticity Report



The Network Elasticity Report fields are described in the following table.

Table 6-14 Network Elasticity Report Fields

Field	Description
Start Time	Time when the scale out/scale in was initiated
Event	Event activity: ■ instantiation ■ scale out ■ scale in ■ termination
Initiator	Event activity initiator: ■ manual ■ automatic

Table 6-14 Network Elasticity Report Fields

Field	Description
Duration (seconds)	Time duration of the activity, in seconds
Status	Event activity status: ■ success ■ failure
Cluster Name	Cluster Name
Cluster Type	Cluster Type: ■ MCC ■ MCC MME
Cluster ID	Cluster ID
Version	Cluster version. For example: MCC: 7.2.4.3-133.REL MCC MME: 11.0.09
Node ID	Node ID
Personality	Node Personality: ■ N/A ■ DCM ■ ASM ■ WSM ■ CCM ■ IOM ■ ISM ■ IWM
Count	Number of nodes after the event
Threshold	***Note:*** *Applies for automatic initiator only.* Threshold Name: ■ DCM Session Utilization ■ WSM Session Utilization ■ ASM Connection Utilization ■ ASM Throughput Utilization
Threshold Value %	***Note:*** *Applies for automatic initiator only.* Threshold value, in percentage

Table 6-14 Network Elasticity Report Fields

Field	Description
Threshold Crossing Duration (seconds)	***Note:*** *Applies for automatic initiator only.* Time duration (in seconds) after the threshold is crossed and remains crossed until the scale out/scale in is automatically initiated by the VNF Manager
Additional Information	Additional information for the event in failure

To view a summary of a particular row in the report, click the row. The VNF Manager opens a window that lists the fields in the row. Click the **Close** icon to close the Table Row Summary.

Use the Search text box on the toolbar to search for instances of an activity.

In the case of a large number of activities, use the page navigational bar at the bottom of the window to page through the entries.

To purge report data, click the **Purge Data** icon. Specify the number of days after which to purge data and click **OK**.

To export the report to a CSV file, click the **Export to CSV** icon.

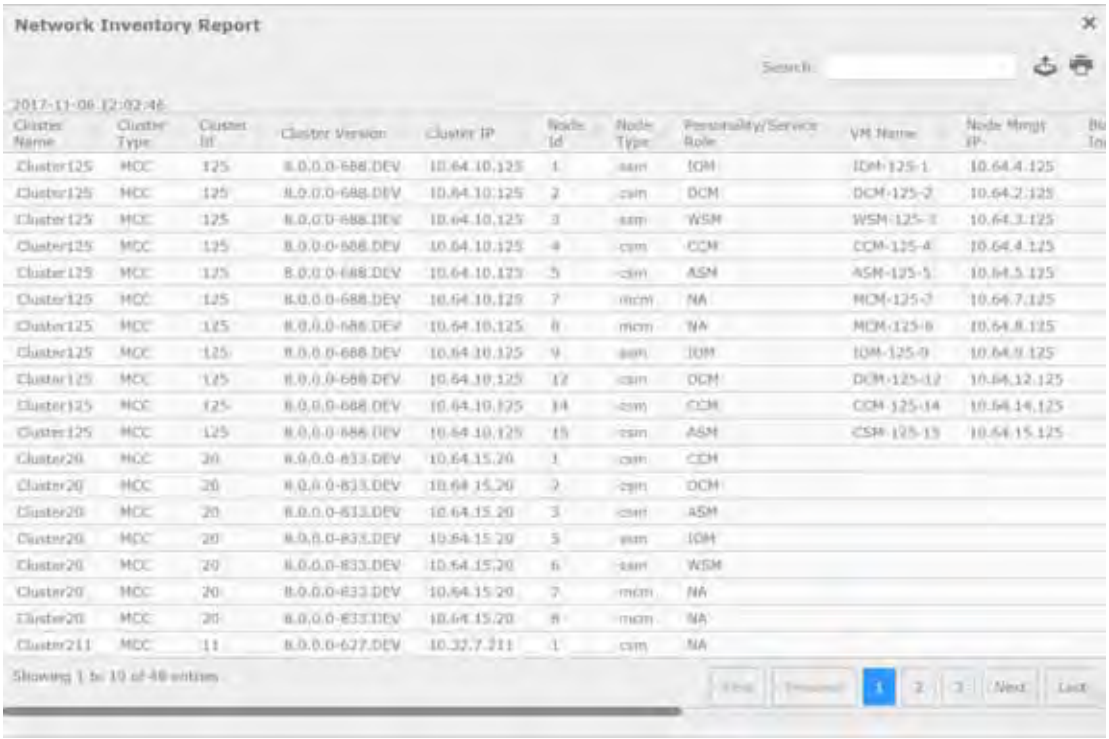
To print the report, click the **Print** icon. Select the printer and click **Print**.

Click the **Close** icon to close the Network Elasticity Report. ✕

Network Inventory Report

To view the Network Inventory Report, click the **Reports** icon and select **Network Inventory**.

Figure 6-19 Network Inventory Report



The Network Inventory Report fields are described in the following table.

Table 6-15 Network Inventory Report Fields

Field	Description
Cluster Name	Cluster Name
Cluster Type	MCC or MCC MME
Cluster ID	Cluster ID
Cluster Version	Cluster version For example: MCC: 7.2.4.3-133.REL MCC MME: 11.0.09
Cluster IP	Cluster management IP address
Node ID	Node ID

Table 6-15 Network Inventory Report Fields

Field	Description
Node Type	Node type **For MCC:** ■ MCM ■ CSM ■ SSM **For MCC MME:** ■ mgmt ■ |rm ■ sig ■ callp ■ lb ■ data ■ edp
Personality/Service Role	MCC Node Personality: ■ N/A ■ DCM ■ ASM ■ WSM ■ CCM ■ IOM ■ ISM ■ IWM MCC MME Service Role: ■ mgmt-N (N=0-1) ■ |rm-N (N=0-1) ■ sig-N (N=0-19) ■ callpN-M (N=0-15, M=0-1) ■ lb-N (N=0-7) ■ data-N (N=0-15) ■ edp-N (N=0-15)
VM Name	Name of the VM host
Node Mgmt IP	Management IP Address of the VM host
Blade/Server Index	Index of the bladed hosting the node
Blade/Server ILO IP	Management IP address of the blade
Blade/Server Host IP	Host IP address of the blade
Blade System/Server Group Name	Blade System/Server Group Name

Table 6-15 Network Inventory Report Fields

Field	Description
Blade System IP	Management IP address of the blade system

If a node in the cluster is hosted by a blade in the Blade System registered with Acuitas, all the Network Inventory Report fields are present for the node. If a node in the cluster *is not* hosted by any blade registered with Acuitas, data for blade information is missing for the node. If a blade in a Blade System does not host any node, data for node information is missing for the blade.

To view a summary of a particular row in the report, click the row. The VNF Manager opens a window that lists the fields in the row. Click the **Close** icon to close the Table Row Summary.

Use the Search text box on the toolbar to search for instances of an inventory.

In the case of a large number of activities, use the page navigational bar at the bottom of the window to page through the entries.

To export the report to a CSV file, click the **Export to CSV** icon.

To print the report, click the **Print** icon. Select the printer and click **Print**.

Click the **Close** icon to close the Network Inventory Report.

Network Inventory Report Export

Acuitas supports exporting the network inventory report daily to a CSV file. To use this feature, you schedule a backup of configuration data. For instructions, see Network Configuration Backup.

Configuring Dynamic Scale Out/Scale In

You can configure a cluster to dynamically scale out/scale in out when the capacity is underloaded/overloaded as determined by an associated scaling policy. The policy specifies the actions to take in response to capacity overload or underload conditions. A cluster is assigned a single scaling policy. A policy can be assigned to multiple clusters.

Overload Condition occurs when both of the following are true:

- Any policy KPI rises above the overload threshold
- The KPI remains above its configured overload threshold over the configured time duration

Underload Condition occurs when both of the following are true:

- All policy KPIs fall below the underload thresholds
- All policy KPIs remains below their respectively configured underload thresholds over their configured time durations

Actions for Overload Condition:

- Send overload notification
- Create a new DCM, WSM, or ASM

Actions for Underload Condition:

- Send underload notification
- Remove an existing DCM, WSM, or ASM

Scale out handles node creation errors. When an error is encountered, that node is ignored and cluster expansion continues.

Prerequisite When a Cluster was not Instantiated by VNF Manager

To allow scaling-out of a cluster that was not instantiated by VNF Manager, perform this prerequisite procedure:

Import the existing cluster into VNF Manager:

1. Start the Acuitas server and log into Acuitas.
2. Add the vCenter Network Element (*skip this step if vCenter is already managed by Acuitas*):
   a. Use any of the following methods to add a vCenter network element:

      Settings icon on the toolbar: Select **Topology** => **Add Element**.

Pop-up menu: Right-click an object in the tree and click **Add Element**.

Acuitas displays the **Add Network Element** window.

b Configure the parameters as follows:

Table 6-16 Add Network Element Parameters

Parameter	Description
Device Type	Select the device type: ■ VIM
General Details	
IP Version	Select IPv4 or IPv6.
IP Address	Enter the IP address of the vCenter server.
Name	Enter the display name of the network element.
Description	Enter the description of the network element.
File Server	Select the file server.
VIM Protocol Details	
Type	Select the VIM type: ■ vCenter
User Name	Enter the username. Such as, administrator@vsphere.local.
Password	Enter the password for the user.
FQDN	If the vCenter certificate was generated based on a Fully Qualified Domain Name, you must enter it so that Acuitas can access the vCenter server. If the certificate was generated based on an IP address, you must leave the field blank.
Location Details Enter the Address of the network element.	

c Click **Save**.

d At the confirmation prompt, click **OK**.

3 Add the existing MCC cluster. Be sure to specify the MCC cluster name and IP address of the existing cluster:

a Use any of the following methods to add the MCC cluster:

Settings icon on the toolbar: Select **Topology => Add Element**.

Pop-up menu: Right-click an object in the tree and click **Add Element**.

Acuitas displays the **Add Network Element** window.

b Configure the parameters as follows:

Table 6-17 Add Network Element Parameters

Parameter	Description
Device Type	Select the device type: ■ MCC ■ c7000 blade system ■ MME ■ Server Group of virtual nodes ■ VIM
General Details	
IP Version	Select IPv4 or IPv6.
IP Address	IP Address: ■ MCC: Enter the Management Configuration Module (MCM) IP address.
Name	Enter the display name of the MCC cluster.
Description	Enter the description of the MCC cluster.
File Server	Select the file server.
Password/Confirm Password	Enter the password for the user. Acuitas allows upper and lower case letters, numbers, and the following special characters for the CLI/NETCONF password: ([!@#$%^&*]) ***Note:*** *If you change the password on the network element, you must also change that account information here.*
FQDN	If the vCenter certificate was generated based on a Fully Qualified Domain Name, you must enter it so that Acuitas can access the vCenter server. If the certificate was generated based on an IP address, you must leave the field blank.
CLI & NETCONF	
User Name	Enter `emsadmin`.
Password/Confirm Password	Enter the password for the user. Acuitas allows upper and lower case letters, numbers, and the following special characters for the CLI/NETCONF password: ([!@#$%^&*]) ***Note:*** *If you change the password on the network element, you must also change that account information here.*
Port	Enter 2022.
CLI Time Out	Leave as default value.
SFTP	

Table 6-17 Add Network Element Parameters

Parameter	Description
User Name	For an MCC, enter `emsadmin`.
Password	Enter the password for the user.
Port	For an MCC, enter port 2222.
SNMP	
SNMP Community	The Community string used for sending SNMP requests for data collection from the device. This value must match the value on the network element. The default community string is **affirmed**. For the c7000, Acuitas allows special characters.
Location Details Enter the Address of the network element.	

c. Click **Save**.

d. At the confirmation prompt, click **OK**.

4. In VNF Manager, upload the OVA packages:

a. Copy the OVA files for MCM, CSM, and SSM to /data/ova.

b. From the **Cluster** window, select a Virtualized Infrastructure Manager (VIM) in the right pane.

c. Click the **Manage Templates** icon in the right pane .

The VNF Manager lists the OVA files in data/ova.

d. In the **Manage OVA Template** screen, click the **Add OVA Template** icon.

e. Select the OVA template you want to upload.

f. Click **Add**.

5. In VNF Manager, discover and configure the hosts:

a. From the **Cluster** window, select the vCenter Virtualized Infrastructure Manager (VIM) in the right pane.

b. Expand **Hosts** in the right pane.

VNF Manager lists the discovered hosts.

c. In VNF Manager, click the **Add Managed Hosts** icon in the right pane.

d. In the **Manage Hosts** screen, select a Datacenter.

VNF Manager lists the available Hosts.

e Click a host in the list to configure it.

f Configure the parameters as follows:

Table 6-18 Manage Host Parameters

Parameter	Description
Host Username	For root user access to the host, enter `root`. For non-root user access to the host, enter the username. You must also provide the Host Password. VNF Manager uses the username and password during cluster deployment.
Host Password	For root user access to the host, the Host Password is optional. For non-root user access to the host, the Host Password is required. VNF Manager uses the username and password during cluster deployment.
Storage > Reserve Storage for VM	Mark the button for the datastore you want to reserve to create the VM
Network Mapping	For each host network, select from the list of network types: ■ Management ■ Base 1 ■ Base 2 ■ East/West 1 ■ East/West 2 ■ North/South 1 ■ North/South 2

g Click **Manage Host**.

h In the **Manage Hosts** screen, click **Close**.

6 Import the existing cluster configuration CSV file into the cluster:

a Expand **Clusters** in the right pane.

b Click the **Import Cluster Configuration** icon in the right pane.

c Specify the cluster name to which to apply the CSV file. The cluster name must match the name specified in step 3.

d Click **Browse** and choose the CSV file.

e Click **Import**.

f Click the cluster in the right pane.

g On the cluster in the left pan, click the **View Cluster Configuration** icon.

h Configure the parameters as follows:

Table 6-19 Cluster Configuration Parameters

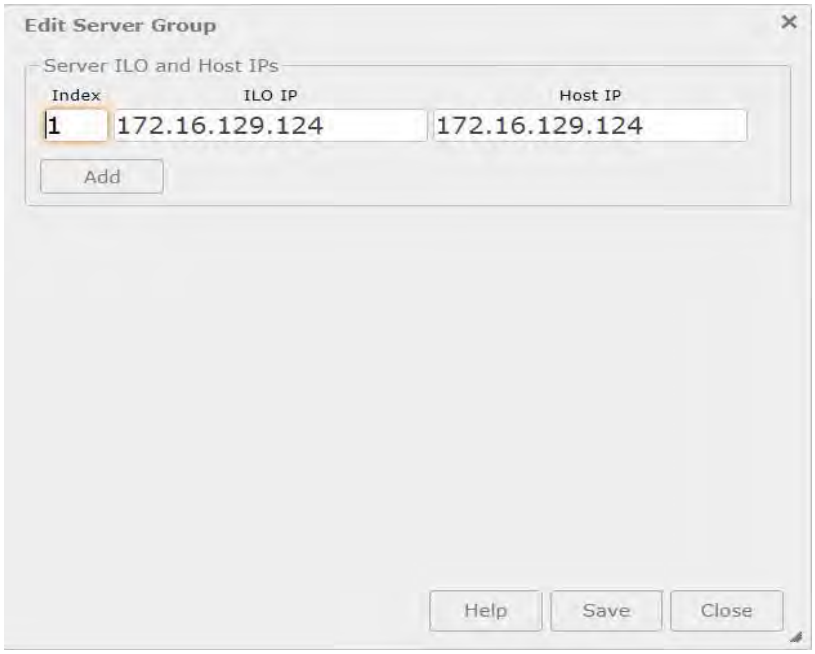
Parameter	Description
SR-IOV Configuration	This setting defines the required networks for the nodes: ■ none ■ ew-ns ■ ew-ns-base-mgmt (OpenStack only)
East-West Redundancy	By default, supports East-West Redundancy for the cluster.
MCM template	MCM Open Virtualization Archive (OVA) package template.
CSM template	CSM Open Virtualization Archive (OVA) package template.
SSM template	SSM Open Virtualization Archive (OVA) package template.

i Click **Save**.

7 Perform the appropriate steps for your scenario:

If the cluster is a server group: Configure the servers in the group (configure each server's IP address for which Acuitas should collect traps):

a In the Network View, right-click the server group and click **Configure Server**.

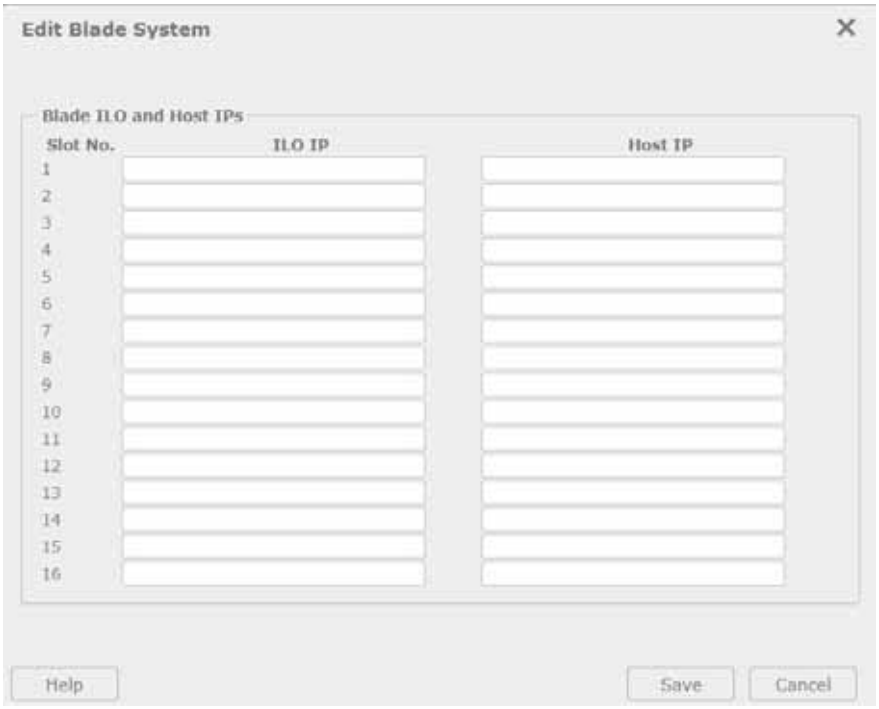


b For each server in the group, enter the index, the iLO IP address, and the Host IP address to which Acuitas should collect traps and click **Add**.

c Click **Save**.

If the cluster is a blade system: Configure each blade with an IP address for which Acuitas should collect traps.

a In the Network View, right-click the blade system and click **Configure Blades**.



b For each slot, enter the blade iLO IP address and the Host IP address to which Acuitas should collect traps.

c Click **Save**.

8 Use the Configuration Navigator to verify the cluster/node information is correct. The information *must match* the existing/pre-deployed cluster configuration. For each node, if any of the following information is missing, add it:

- Blade ID
- IP Address
- VM IP Address
- VM Name

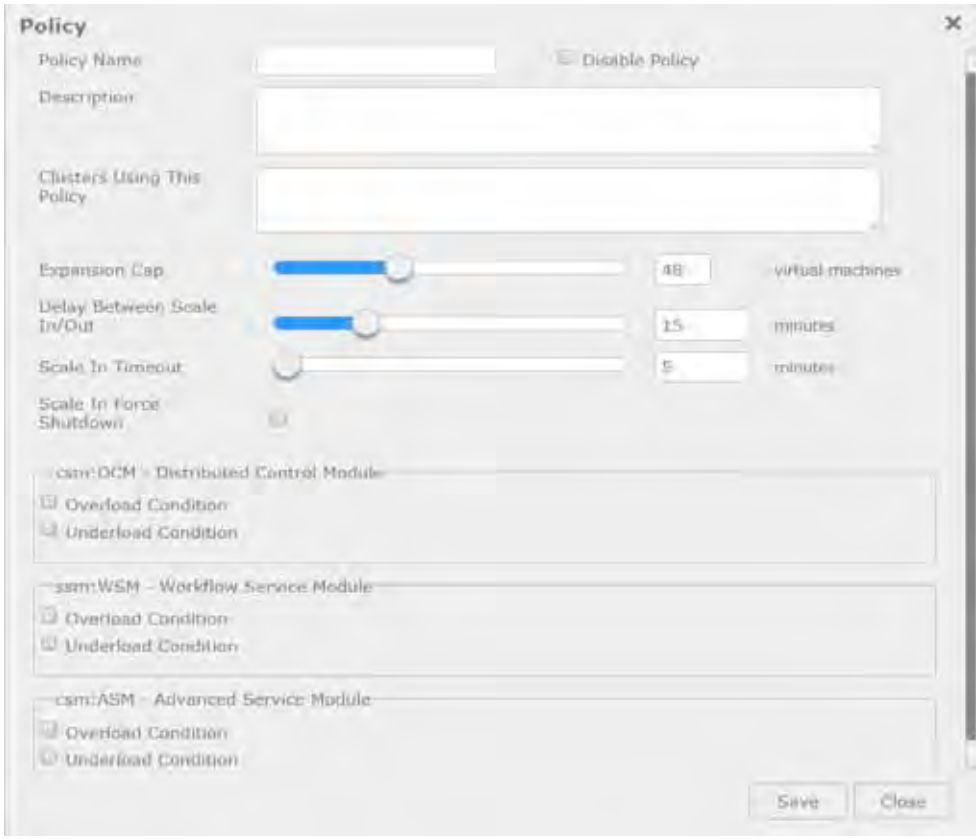
The VNF Manager can now scale-out the cluster, as specified by the imported CSV file. Proceed to Configuring Scaling Policy.

Configuring Scaling Policy

To add a scaling policy:

1 From the **Cluster View** window, click the **Policy Management** icon on the toolbar.

2 Click the **Add Policy** icon.



3 Configure the policy parameters as follows:

Table 6-20 Policy Parameters

Parameter	Description
Policy Name	Card ID
Disable Policy	Mark the checkbox to disable the policy.
Description	Description (up to1024 characters)
Clusters Using this Policy	List of clusters assigned this policy. To disassociate a cluster from this policy, click the X icon.
Expansion Cap	Drag the slider to set the maximum number of virtual machines in the cluster

Table 6-20 Policy Parameters

Parameter	Description
Delay Between Scale In/Out	Drag the slider to set the time (in minutes) that the system must wait between scale in or scale out operations for a cluster.
Scale In Timeout	Drag the slider to set the time out (in minutes) that the system waits for the end of dry up when scaling in.
Scale In Force Shutdown	Mark the checkbox to force a shutdown when scaling in, if dry up is not finished for the given Scale In Timeout value.

4 Specify the Overload and/or Underload threshold and action to take for each applicable node type.

Note: *If you assign a policy to a Server Group, when the Overload or Underload threshold is met, only an alarm is sent out.*

Table 6-21 Threshold and Action Parameters

Parameter		Description
DCM Distributed Control Module:		
Overload Condition Mark the checkbox to specify the overload condition.	DCM Session Threshold	Drag the slider to set the threshold value for the DCM Session Capacity Utilization KPI For description, see DCM Session Capacity Utilization
	Duration	Drag the slider to set the threshold crossing duration, in seconds
	Create a DCM for Overload condition and send alarm	Mark the checkbox to create a DCM and send an alarm when the overload condition is met
	Send alarm only	Mark the checkbox to only send an alarm when the overload condition is met

Table 6-21 Threshold and Action Parameters

	Parameter	Description
Underload Condition Mark the checkbox to specify the underload condition.	DCM Session Threshold	Drag the slider to set the threshold value for the DCM Session Capacity Utilization KPI For description, see DCM Session Capacity Utilization
	Duration	Drag the slider to set the threshold crossing duration, in seconds
	Create a DCM for Underload condition and send alarm	Mark the checkbox to create a DCM and send an alarm when the underload condition is met
	Send alarm only	Mark the checkbox to only send an alarm when the underload condition is met
WSM Workflow Service Module:		
Overload Condition Mark the checkbox to specify the overload condition.	WSM Session Threshold	Drag the slider to set the threshold value for the WSM Session Capacity Utilization KPI For description, see WSM Session Capacity Utilization
	Duration	Drag the slider to set the threshold crossing duration, in seconds.
	Create a WSM for Overload condition and send alarm	Mark the checkbox to create a WSM and send an alarm when the overload condition is met
	Send alarm only	Mark the checkbox to only send an alarm when the overload condition is met
Underload Condition Mark the checkbox to specify the underload condition.	WSM Session Threshold	Drag the slider to set the threshold value for the WSM Session Capacity Utilization KPI For description, see WSM Session Capacity Utilization
	Duration	Drag the slider to set the threshold crossing duration, in seconds
	Create a WSM for Underload condition and send alarm	Mark the checkbox to create a WSM and send an alarm when the underload condition is met
	Send alarm only	Mark the checkbox to only send an alarm when the underload condition is met

Table 6-21 Threshold and Action Parameters

Parameter		Description
ASM Advanced Service Module		
Overload Condition Mark the checkbox to specify the overload condition.	ASM Connection Threshold	Drag the slider to set the threshold value for the ASM Connection Capacity Utilization KPI For description, see ASM Connection Capacity Utilization
	ASM Throughput Threshold	Drag the slider to set the threshold value for the ASM Throughput Capacity Utilization KPI For description, see ASM Throughput Capacity Utilization
	Duration	Drag the slider to set the threshold crossing duration, in seconds.
	Create a ASM for Overload condition and send alarm	Mark the checkbox to create a ASM and send an alarm when the overload condition is met
	Send alarm only	Mark the checkbox to only send an alarm when the overload condition is met
Underload Condition Mark the checkbox to specify the underload condition.	ASM Connection Threshold	Drag the slider to set the threshold value for the ASM Connection Capacity Utilization KPI For description, see ASM Connection Capacity Utilization
	ASM Throughput Threshold	Drag the slider to set the threshold value for the ASM Throughput Capacity Utilization KPI For description, see ASM Throughput Capacity Utilization
	Duration	Drag the slider to set the threshold crossing duration, in seconds.
	Create an ASM for Underload condition and send alarm	Mark the checkbox to create an ASM and send an alarm when the underload condition is met
	Send alarm only	Mark the checkbox to only send an alarm when the underload condition is met

5 Click **Save**.

6 To close the Policy Management window, click the **Policy Management** icon on the toolbar again.

Scale Out Restrictions

The VNF Manager can add a node to a cluster, with the following restrictions:

- Total number of VMs in the cluster cannot exceed 128
- Total number of VMs for the cluster cannot exceed the **Expansion Cap** configured in the cluster policy
- Time lapse between the completion of the previous VM creation/deletion and the current time must be at least the **Delay Between Scale In/Out** configured in the cluster policy
- Total number of ASMs in the cluster cannot exceed the configured Cluster > Max ASMs value

Scale In Restrictions

The VNF Manager can remove a node from a cluster, with the following restrictions:

- Node *cannot* contain less than the following number of VM types:
  - Optional configuration is for specialized building block strategy: Must contain at least 2 MCM, 2 CCM, 2 DCM, 2 WSM, 2 IOM, and 1 ASM
- No outstanding node creations or deletions
- Time lapse between the completion of the previous VM creation/deletion and the current time must be at least the **Delay Between Scale In/Out** configured in the cluster policy.

Modifying a Policy

You can modify an existing policy.

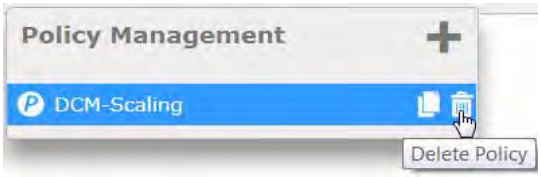
To modify a policy:

1. From the **Cluster View** window, click the **Policy Management** icon on the toolbar.
2. Click the policy in the list.
3. Modify the policy parameters.
4. Click **Save**.
5. To close the Policy Management window, click the **Policy Management** icon on the toolbar again.

Deleting a Policy

To delete a policy:

1. From the **Cluster View** window, click the **Policy Management** icon on the toolbar.
2. To delete a policy from the list, click the **Delete Policy** icon.



3. At the confirmation prompt, click **OK**.
4. To close the Policy Management window, click the **Policy Management** icon on the toolbar again.

Copying a Policy

You can make a copy of an existing policy and then modify and save it with a new name.

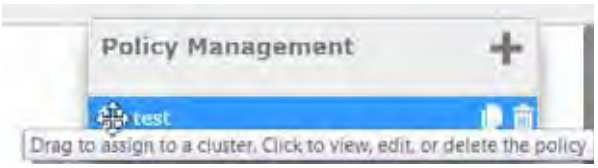
To copy a policy:

1. From the **Cluster View** window, click the **Policy Management** icon on the toolbar.
2. Click the **Copy Policy** icon.
3. Configure the policy parameters using a different policy name.
4. Click **Save**.
5. To close the Policy Management window, click the **Policy Management** icon on the toolbar again.

Assigning a Policy to a Cluster

To assign a policy to a cluster:

1. From the **Cluster View** window, click the **Policy Management** icon on the toolbar.
2. Drag and drop the policy's **P** icon from the policy list to the cluster.



The Policy icon is added to the cluster

3 To close the Policy Management window, click the **Policy Management** icon on the toolbar again.

Disassociating a Policy from a Cluster

To disassociate a policy from a cluster:

1 From the **Cluster View** window, click the **Policy Management** icon on the toolbar.

2 Click the policy associated with the cluster.

3 In the **Clusters Using This Policy** field, click the **X** icon of the cluster you want to disassociate from the policy.

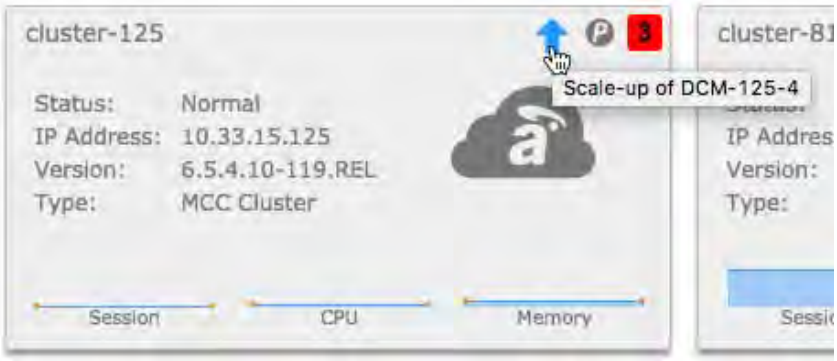
4 At the confirmation prompt, click **OK**.

5 To close the Policy Management window, click the **Policy Management** icon on the toolbar again.

Monitoring Dynamic Scale Out/Scale In

When a cluster is in the process of scaling out/scaling in, the VNF Manager adds the scale indication icon to the cluster.

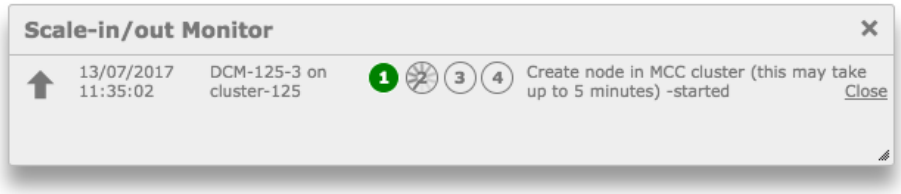
To view the scale out/scale in activity, point the cursor at the scale indication icon. The VNF Manager displays the activity.



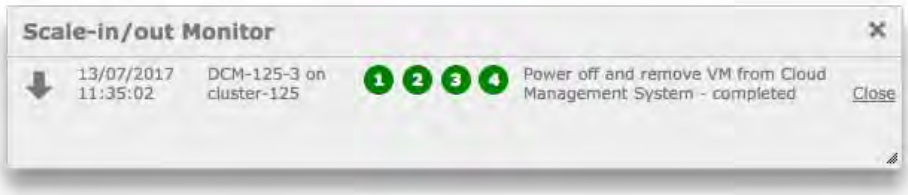
During scale out/scale in, the VNF Manager displays the **Scale-in/out Monitor** window, listing the detailed steps of the process, and indicating whether the scale-in/scale out succeeded.

Figure 6-20 Scale-in/out Monitor Examples

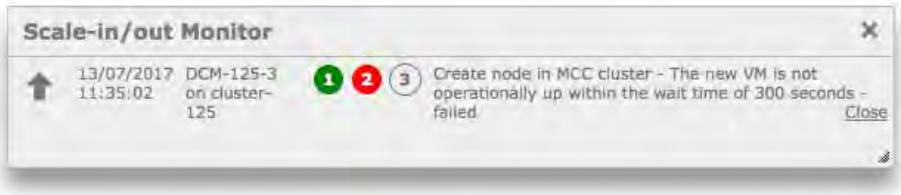
Starting a Scale-out:



Completing a Scale-in:



Error During Scale-out:



Click the **Close** icon to close the **Scale-in/out Monitor** window.

Alarm Notifications

Overload/Underload Conditions

The VNF Manager sends alarm notifications for overload/underload conditions, for both approaching and crossing conditions, for the following KPIs:

- DCM Session Capacity Utilization
- WSM Session Capacity Utilization
- ASM Connection Capacity Utilization
- ASM Throughput Capacity Utilization

The alarms are listed in the following table.

Table 6-22 Overload/Underload Alarms

Alarm Name	Severity	Description
vnfScaleKpiMon	MAJOR	The listed KPI is transitioned to one of the following states: ■ Underload threshold crossed for 80% of the duration ■ Overload threshold crossed for 80% of the duration
	CRITICAL	The listed KPI is transitioned to one of the following states: ■ Underload condition ■ Overload condition
	CLEARED	The listed KPI is transitioned to normal condition (neither underload or overload condition)

Scale Out/Scale In Faults

The VNF Manager sends configuration alarm notifications when failing to scale in or scale out a cluster.

The alarms are listed in the following table.

Table 6-23 Scale Out/Scale In Alarms

Alarm Name	Severity	Description
vnfScaleOut	CRITICAL	Failed to create VM
vnfScaleIn	CRITICAL	Failed to delete VM

Using the VNF Manager and Provisioning API

The VNF Manager and Provisioning API provides a northbound Application Programming Interface (API) for use by Network Function Virtualization Orchestrator (VFVO) to control and monitor virtualized MCC and MCC MME clusters in real-time. The API:

- Exposes necessary VIM information for constructing cluster configurations
- Manages cluster configurations as the basis for cluster lifecycle management
- Provides lifecycle management of MCC and MCC MME clusters
- Supports dynamic scaling of MCC and MCC MME clusters
- Supports MCC and MCC MME configuration

The VNF Manager and Provisioning API is a representational state transfer (REST)-based API over HTTPS. For details, see VNF Manager and Provisioning REST API.

Note: *To use the VNF Manager Provisioning API, you must have the Tools > Northbound API security group permission. For instructions, see Specifying Permissions by Security Group.*

VNF Manager and Provisioning API Audit Logs

Each VNF Manager and Provisioning API operation is logged to the following file:

/opt/Affirmed/NMS/server/ems/log/nbapi.log

Each API operation that causes change to Acuitas or MCC clusters is logged in the Acuitas configuration audit log.

Troubleshooting Problems with OpenStack Cluster Commissioning

Use the solutions in this topic to help troubleshoot OpenStack cluster commissioning problems.

Host has Multiple SSM Nodes Instantiated

Problem

A host has more than one SSM nodes instantiated. The anti-affinity rule for SSM was not applied.

Cause

Either the an-mcc-ssm-anti-affinity policy server group was not created or the ServerGroupAntiAffinityFilter was not enabled for nova scheduler.

Solution

- Create *an-mcc-ssm-anti-affinity* policy server group with an anti-affinity policy:

  ```
  nova server-group-create --policy anti-affinity
  an-mcc-ssm-anti-affinity
  ```

- Enable ServerGroupAntiAffinityFilter for nova scheduling. To do so, add `ServerGroupAntiAffinityFilter` to the following line in `/etc/nova/nova.conf` on the host that runs the `nova-scheduler`:

  ```
  scheduler_default_filters=RetryFilter,AvailabilityZoneFilter,RamFi
  lter,ComputeFilter,ComputeCapabilitiesFilter,ImagePropertiesFilter
  ,CoreFilter,ServerGroupAntiAffinityFilter
  ```

VNF Manager Fails to Show VIM Configuration

Problem

The following problems can occur from the **Cluster** window:

- Selecting a VIM in the right pane and clicking the **View VIM Configuration** icon fails to list the referenced entities.
- Selecting a VIM in the right pane, expanding **Availability Zones**, and clicking the **Add Managed Availability Zones** icon returns the following error:

```
Exception while trying to get the lists of zones:
ConnectionException{message=<host> …)
```

Cause

VNF Manager relies on the Acuitas server to resolve the OpenStack controller hostname. If the hostname cannot be resolved, Acuitas fails to list the Availability Zones and logs a java.net.UnknownHostException to the vm.log.

Solution

Either add the OpenStack controller hostname to the DNS configuration or add the OpenStack controller IP address and hostname to the Acuitas /etc/hosts file.

Chapter 7

Security

Security management allows you to control and monitor user access to the network and associated network management information. Specifically, you control user authentication, user authorization, and user privileges.

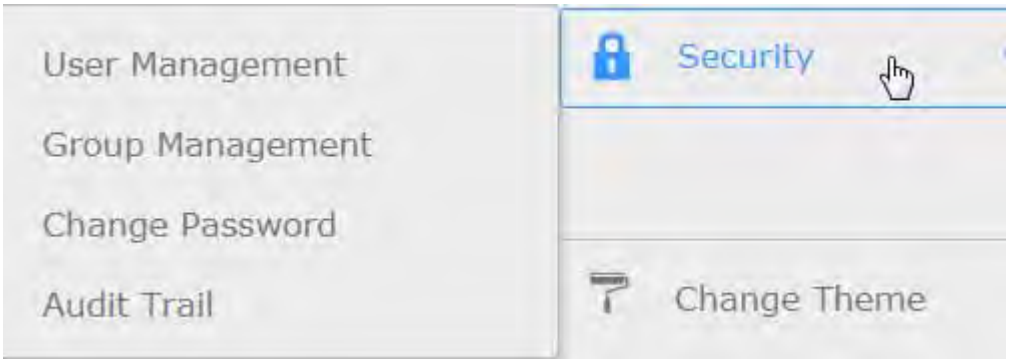
Administrators use Security applications to:

- Add users and security groups dynamically.
- Assign which managed elements can be accessed by a security group
- Assign users pre-defined privileges based on user role, such as Administrator, Provisioning, and Maintenance.
- Assign permissions on a granular basis, such as permission to view alarms and assign alarms. Acuitas supports a list of pre-defined permissions.
- Track user activities via Audit Trails.

Note: *When you use the Security applications to add or change groups and/or users, the change takes 1 minute to take effect.*

To access Security applications, select the applicable option from the **Settings** icon on the toolbar.

Figure 7-1 Accessing Security Applications



Security Groups

Security groups logically group users based on user role and define the operations users can perform. For example, members of a customer support organization could be assigned to the Administrator group with administrative privileges.

Acuitas uses security group permissions to control group members access to specific types of objects and control the actions the members can perform on those objects:

- Only those management functions granted to the Operator are visible in menu selections.
- Only those managed elements accessible to a member are visible in Network View, Alarms, and PM Dashboard.
- Only those objects accessible to a member are visible in the Configuration Navigator.

For instructions on setting security group permissions, see Specifying Permissions by Security Group.

Acuitas supports the following default security groups:

- **Administrator** – Has administrator privileges and can view managed objects and operations.

  Administrator includes the following permissions under Configuration > MCC Configuration:

  – System Configuration > Admin

  – Network Configuration > Admin

  – Service Rule Provisioning > Admin

  – Service Provisioning – Charging > Admin

  – Service Provisioning – QoS > Admin

  – Service Provisioning – Subscriber Firewall > Admin

  – Service Provisioning – Content > Admin

  – Service Provisioning – FBWU > Admin

  – VNF Manager > Configuration > Admin

  – Workflow Provisioning > Admin

  In addition, Administrator includes the following permissions under Configuration > MME Configuration:

  – Read

  – Read/Write

  – Admin

  In addition, Administrator includes the following permissions under Configuration > SSF Configuration:

  – Read

  – Read/Write

  – Admin

  Acuitas supports multiple active sessions for this user name.

- **Operator** – Has viewing privileges only.

  Operator includes the following permissions under Configuration > MCC Configuration:

  – System Configuration > Read

  – Network Configuration > Read

  – Service Rule Provisioning > Read

  – Service Provisioning – Charging > Read

  – Service Provisioning – QoS > Read

  – Service Provisioning – Subscriber Firewall > Read

- Service Provisioning – Content > Read
- Service Provisioning – FBWU > Read
- VNF Manager > Configuration > Read
- Workflow Provisioning > Read

In addition, Operator includes the following permissions under Configuration > MME Configuration:

- Read

In addition, Operator includes the following permissions under Configuration > SSF Configuration:

- Read

Adding Security Groups

An administrator can add security groups.

Note: *To add a security group, you must have the Security Manager > Security Group Details > Add Group security group permission. To modify security group permissions, you must have Security Manager > Security Group Details > Modify Group > Modify Functional Access. For instructions, see Specifying Permissions by Security Group.*

To add a security group:

1. Click the **Settings** icon on the toolbar and select **Security =>**

   Group Management.

   Acuitas displays the **Security Group** window, listing the security groups in the system.

2. Click the **Add** icon.
3. Configure the parameters as follows:
   - **Name** – Enter the group name.
   - **Description** – Enter the group description.
   - **Permissions** – Mark the checkboxes to allow the group members to access the functional areas of Acuitas (Topology, Fault, Configuration, Performance, Security Manager, Tools, VNF Manager). Click the expansion icons to open and close function objects in the tree display.

     For details on security permissions, see Specifying Permissions by Security Group.
4. Click **Save**.

Associating Resources with Security Groups

You can select which managed elements can be accessed by a security group.

Note: *To associate resources with a security group, you must have the Security Manager > Security Group Details > Associate Resources security group permission. For instructions, see Specifying Permissions by Security Group.*

To associate resources with a security group:

1. Click the **Settings** icon on the toolbar and select **Security =>** **Group Management**.

   Acuitas displays the **Security Group** window, listing the security groups in the system.

2. From the **Security Group** window, use any of the following methods to associate resources with a security group:

   Toolbar: Select the group and click the **Associate Resources** icon.

   Pop-up menu: Right-click the group and click **Associate Resources**.

   Acuitas displays the Associate Resources window.

3. Specify the NEs that the group can access:

   - To select individual NEs, highlight each one in the **Available List** and click the right-arrow to move it to the **Assigned List**. To remove a selected NE, highlight it in the **Assigned List** and click the left-arrow to move it to the **Available List**.
   - To specify all NEs, mark the **Associate All Resources** checkbox.

4. Click **Save**.

   Now, when a user of the security group logs in, only those managed elements accessible to the member are visible in Network View, Alarms, and PM Dashboard.

Viewing Security Groups

Note: *To view a security group, you must have the Security Manager > Security Group Details > View Group security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a security group:

1. Click the **Settings** icon on the toolbar and select **Security =>**

   Group Management.

   Acuitas displays the **Security Group** window, listing the security groups in the system.

2. From the **Security Group** window, use any of the following methods to view a groups's details:

   Toolbar: Select the group and click the **View** icon.

   Pop-up menu: Right-click the group and click **View**.

   Acuitas displays the View window, listing the following information:

   - Functional Access tab – Lists security group Name, Description, and Permissions to access the functional areas of Acuitas (Topology, Fault, Configuration, Performance, Security Manager, Tools, VNF Manager).
   - Group Members tab – Lists members of the security group.

3. Click **Close** to close the window.

Copying Security Groups

An administrator can make a copy of an existing security group and then modify and save it with a new name.

Note: *To copy a security group, you must have the Security Manager > Security Group Details > Copy Group security group permission. For instructions, see* *Specifying Permissions by Security Group*.

To copy a security group:

1. Click the **Settings** icon on the toolbar and select **Security =>** **Group Management**.

   Acuitas displays the **Security Group** window, listing the security groups in the system.

2. Use any of the following methods to copy a security group:

   Toolbar: Select the security group and click the **Copy** icon.

   Pop-up menu: Right-click the security group and select **Copy**.

3. Make the necessary changes:

   - **Name** – Enter the group name.
   - **Description** – Enter the group description.
   - **Permissions** – Mark the checkboxes to allow the group members to access the functional areas of Acuitas (Topology, Fault, Configuration, Performance, Security Manager, Tools, VNF Manager). Click the expansion icons to open and close function objects in the tree display.

4. Click **Save**.

Exporting Security Groups

You can export a list of security groups to a CSV file.

Note: *To export a list of security groups, you must have the Security Manager > Security Group Details > View Group security group permission. For instructions, see Specifying Permissions by Security Group.*

To export security groups:

1. Click the **Settings** icon on the toolbar and select **Security => Group Management**.

   Acuitas displays the **Security Group** window, listing the security groups in the system.

2. If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.

3. Click the **Export** icon.

   Acuitas displays the **Configure Export Parameters** window.

4. Configure the parameters as follows:
   - **File Type**: Select the required file format (CSV).
   - **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
   - **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
   - **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.

5. Click **Apply**.

   Acuitas displays the **Download Files** window.

6. Click **Download Exported File**.

7. From the **Download File**s window, click **Close**.

Modifying Security Groups

An administrator can modify security groups.

Note: *To modify a security group, you must have the Security Manager > Security Group Details > Modify Group security group permission. To modify security group permissions, you must have Security Manager > Security Group Details > Modify Group > Functional Group Access. For instructions, see Specifying Permissions by Security Group.*

To modify a security group:

1. Click the **Settings** icon on the toolbar and select **Security =>**

   Group Management.

   Acuitas displays the **Security Group** window, listing the security groups in the system.

2. Use any of the following methods to edit the security group:

   Toolbar: Select the security group and click the **Edit** icon.

   Pop-up menu: Right-click the security group and click **Edit**.

   Acuitas displays the Edit Group Details window, listing the settings for the user.

3. Make the necessary changes:

   - **Name** – Enter the group name.
   - **Description** – Enter the group description.
   - **Permissions** – Mark the checkboxes to allow the group members to access the functional areas of Acuitas (Topology, Fault, Configuration, Performance, Security Manager, Tools, VNF Manager). Click the expansion icons to open and close function objects in the tree display.

     For details on permissions, see Specifying Permissions by Security Group.

4. Click **Apply**.

Deleting Security Groups

An administrator can delete security groups.

When you delete a security group, all users assigned to that group are also deleted. If a user is assigned to multiple groups, the user sessions are terminated.

Note: *To delete a security group, you must have the Security Manager > Security Group Details > Delete Group security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To delete a security group:

1. Click the **Settings** icon on the toolbar and select **Security =>**

   Group Management.

   Acuitas displays the **Security Group** window, listing the security groups in the system.

   Toolbar: Select the security group and click the **Delete** icon.

   Pop-up menu: Right-click the security group and click **Delete**.

2. At the confirmation prompt, click **OK**.

Specifying Permissions by Security Group

Use group permissions to specify which management functions members can access in menu selections. For example, you can specify that the group can view Historical statistics.

For configuration functions, you can specify which managed objects group members can view in the Configuration Navigator. For example, you can specify that a particular group can view Workflow objects. And, you can specify which management functions members can access in menu selections. For example, you can specify that the group can access Workflow and HTTP Filter File Management applications.

To configure permissions by a security group:

1. Access the Security Group window. In the **Permissions** field, expand **EMS Management**.
2. Expand the specific function (Topology, Fault, Configuration, Performance, Security Manager, Tools, VNF Manager).
3. Expand the sub function, such as MCC Configuration.
4. Mark the checkboxes for the permissions you want members to have.

Figure 7-2 Setting Permissions for Group Members

5 Click **Save**.

The following table lists the roles and associated managed objects, management functions, and actions that each role can access.

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration	
Configuration > FTP Server Reassign	Reassign an FTP Server
Configuration > Alarm Triggered Configuration > Add Alarm Triggered Configuration	Add Alarm Triggered Configuration
Configuration > Alarm Triggered Configuration > Modify Alarm Triggered Configuration	Modify Alarm Triggered Configuration
Configuration > Alarm Triggered Configuration > Delete Alarm Triggered Configuration	Delete Alarm Triggered Configuration
Configuration > Alarm Triggered Configuration > View Alarm Triggered Configuration	View Alarm Triggered Configuration

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > Alarm Triggered Configuration > Execution Status	View Alarm Triggered Configuration Execution Status
Configuration > MCC Configuration > System Configuration > Read (Read-Only access) Configuration > MCC Configuration > System Configuration > Write (Write access)	**Configuration Navigator:** ■ Alarms ■ Cluster ■ Fault Management ■ Image Management ■ Infrastructure ■ Performance Statistics Management ■ Security ■ User Access **Management Functions:** ■ Log Viewer

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > MCC Configuration > System Configuration > Admin (Administrative access)	**Configuration Navigator:** ■ Alarms ■ Cluster ■ Fault Management ■ Image Management ■ Infrastructure ■ Performance Statistics Management ■ Security ■ User Access **Management Functions:** ■ Log Viewer ■ Configuration Export **Actions:** ■ Cluster *id* > Card *id* reboot ■ Image Management removeAdminVersion ■ Image Management upgrade ■ Image Management onlineupgrade ■ Image Management prepare ■ Image Management rollback ■ Image Management reset ■ Image Management firmwareupgrade ■ Image Management displayAvailableAdminVersions ■ Image Management displayActivationProgress ■ Image Management onlineupgradeplan ■ Image Management displayLastActivationResult ■ Infrastructure > Filemgmt > Profile *profile* trigger_file_transfer

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > MCC Configuration > Network Configuration > Read (Read-Only access)	**Configuration Navigator:** ■ Geo Redundancy ■ Network Context ■ IP Protocols ■ Security ■ User Access ■ Service Construct > DiffServ Profile ■ Service Construct > DiffServ Profile > Class Mapping ■ Service Construct > DiffServ Profile > DSCP Mapping ■ Service Construct > Interface ■ Service Construct > Loopback IP List ■ Service Construct > MMS ■ Service Construct > SMS ■ Service Construct > UA Profile ■ Service Construct > Geo Redundancy Server ■ Service Construct > Host List ■ Service Construct > IP List ■ Service Construct > LDAP ■ Service Construct > PLMNID List ■ Service Construct > REALM List ■ Service Construct > Interface Trigger Template ■ Service Construct > Quality of Service ■ Service Construct > Static DNS Map ■ Services > Metering ■ Workflow > Control Profile ■ Workflow > APN Mapping List ■ Zone **Workflow:** ■ Host List ■ LDAP ■ MMS ■ QoS ■ SMS ■ UA Profile ■ Workflow > Control Profile ■ Workflow > APN Mapping List

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > MCC Configuration > Network Configuration > Write (Write access)	**Configuration Navigator:** ■ Geo Redundancy ■ IP Protocols ■ Network Context ■ Security ■ User AccessService Construct > DiffServ Profile ■ Service Construct > DiffServ Profile > Class Mapping ■ Service Construct > DiffServ Profile > DSCP Mapping ■ Service Construct > Interface ■ Service Construct > MMS ■ Service Construct > SMS ■ Service Construct > UA Profile ■ Service Construct > Geo Redundancy Server ■ Service Construct > Host List ■ Service Construct > IP List ■ Service Construct > LDAP ■ Service Construct > Loopback IP List ■ Service Construct > PLMNID List ■ Service Construct > REALM List ■ Service Construct > Interface Trigger Template ■ Service Construct > Quality of Service ■ Service Construct > Static DNS Map ■ Services > Metering ■ Workflow > Control Profile ■ Workflow > APN Mapping List ■ Zone **Actions:** ■ Zone *name* > Gateway > Subscriber imsiTable ■ Zone *name* > Gateway > Subscriber > Clear > Imsi range ■ Zone *name* > Gateway > Subscriber > Clear > Imsi apn ■ Zone *name* > Gateway > Subscriber > Clear > Imsi all ■ Zone *name* > Gateway > Subscriber > Clear > Imsi home ■ Zone *name* > Gateway > Subscriber > Clear > Imsi visiting ■ Zone *name* > Gateway > Subscriber > Clear > Imsi active ■ Zone *name* > Gateway > Subscriber > Clear > Imsi idle ■ Zone *name* > Gateway > Subscriber > Count > Imsi range ■ Zone *name* > Gateway > Subscriber > Count > Imsi apn

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
(Continued)	■ Zone *name* > Gateway > Subscriber > Count > Imsi all ■ Zone *name* > Gateway > Subscriber > Count > Imsi home ■ Zone *name* > Gateway > Subscriber > Count > Imsi visiting ■ Zone *name* > Gateway > Subscriber > Count > Imsi active ■ Zone *name* > Gateway > Subscriber > Count > Imsi idle **Workflow:** ■ Host List ■ LDAP ■ MMS ■ QoS ■ SMS ■ UA Profile ■ Workflow > Control Profile ■ Workflow > APN Mapping List

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > MCC Configuration > Network Configuration > Admin (Administrative access)	**Configuration Navigator:** ■ Geo Redundancy ■ IP Protocols ■ Network Context ■ Service Construct > DiffServ Profile ■ Service Construct > DiffServ Profile > Class Mapping ■ Service Construct > DiffServ Profile > DSCP Mapping ■ Service Construct > Interface ■ Service Construct > MMS ■ Service Construct > SMS ■ Service Construct > UA Profile ■ Service Construct > Geo Redundancy Server ■ Service Construct > Host List ■ Service Construct > LDAP ■ Service Construct > Loopback IP List ■ Service Construct > PLMNID List ■ Service Construct > REALM List ■ Service Construct > Interface Trigger Template ■ Service Construct > Quality of Service ■ Service Construct > Static DNS Map ■ Services > Metering ■ Workflow > Control Profile ■ Workflow > APN Mapping List ■ Zone **Management Functions:** ■ Geographic Redundancy Manager

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
(Continued)	**Actions:** ■ Network Context *name* > ping ■ Network Context *name* > clearospf ■ Network Context *name* > restartospf ■ Network Context *name* > debugospflog all ■ Network Context *name* > debugospflog none ■ Network Context *name* > debugospflog events ■ Network Context *name* > debugospflog ifsm ■ Network Context *name* > debugospflog lsa ■ Network Context *name* > debugospflog nfsm ■ Network Context *name* > debugospflog nsm ■ Network Context *name* > debugospflog packet ■ Network Context *name* > debugospflog route ■ Zone *name* > Gateway > Subscriber imsiTable ■ Zone *name* > Gateway > Subscriber > Clear > Imsi range ■ Zone *name* > Gateway > Subscriber > Clear > Imsi apn ■ Zone *name* > Gateway > Subscriber > Clear > Imsi all ■ Zone *name* > Gateway > Subscriber > Clear > Imsi home ■ Zone *name* > Gateway > Subscriber > Clear > Imsi visiting ■ Zone *name* > Gateway > Subscriber > Clear > Imsi active ■ Zone *name* > Gateway > Subscriber > Clear > Imsi idle ■ Zone *name* > Gateway > Subscriber > Count > Imsi range ■ Zone *name* > Gateway > Subscriber > Count > Imsi apn ■ Zone *name* > Gateway > Subscriber > Count > Imsi all ■ Zone *name* > Gateway > Subscriber > Count > Imsi home ■ Zone *name* > Gateway > Subscriber > Count > Imsi visiting ■ Zone *name* > Gateway > Subscriber > Count > Imsi active ■ Zone *name* > Gateway > Subscriber > Count > Imsi idle **Workflow:** ■ Host List ■ LDAP ■ MMS ■ QoS ■ SMS ■ UA Profile ■ Workflow > Control Profile ■ Workflow > APN Mapping List

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > MCC Configuration > Service Rule Provisioning > Read (Read-Only access) Configuration > MCC Configuration > Service Rule Provisioning > Write (Write access) Configuration > MCC Configuration > Service Rule Provisioning > Admin (Administrative access)	**Configuration Navigator and Workflow:** ■ Service Construct > Protocol Application Rule Group ■ Service Construct > HTTP Rule Group ■ Service Construct > Packet Filter ■ Service Construct > Service Rule ■ Service Construct > Time of Day Rule Group
Configuration > MCC Configuration > Service Provisioning – Steering > Read (Read-Only access) Configuration > MCC Configuration > Service Provisioning – Steering >Write (Write access) Configuration > MCC Configuration > Service Provisioning – Steering >Admin (Administrative access)	**Configuration Navigator and Workflow:** ■ Services > Steering > Steering Flow ■ Services > Steering > Steering Policy ■ Services > Steering > Service Data Flow
Configuration > MCC Configuration > Service Provisioning – Charging > Read (Read-Only access) Configuration > MCC Configuration > Service Provisioning – Charging > Write (Write access)	**Configuration Navigator and Workflow:** ■ Service Construct > Advice of Charge ■ Services > Charging ■ Services > Charging > Service Data Flow
Configuration > MCC Configuration > Service Provisioning – Charging > Admin (Administrative access)	**Configuration Navigator:** ■ Service Construct > Advice of Charge ■ Service Construct > Data Record Template ■ Services > Charging ■ Services > Charging > Service Data Flow **Workflow:** ■ Advice of Charge ■ Charging
Configuration > MCC Configuration > Service Provisioning – QoS > Read (Read-Only access) Configuration > MCC Configuration > Service Provisioning – QoS > Write (Write access) Configuration > MCC Configuration > Service Provisioning – QoS > Admin (Administrative access)	**Configuration Navigator and Workflow:** ■ Services > Quality of Service ■ Services > Quality of Service > Service Data Flow
Configuration > MCC Configuration > Service Provisioning – Subscriber Firewall > Read (Read-Only access) Configuration > MCC Configuration > Service Provisioning – Subscriber Firewall > Write (Write access) Configuration > MCC Configuration > Service Provisioning – Subscriber Firewall > Admin (Administrative access)	**Configuration Navigator and Workflow:** ■ Services > Subscriber Firewall ■ Services > Subscriber Firewall > Service Data Flow

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > MCC Configuration > Service Provisioning – Content > Read (Read-Only access) Configuration > MCC Configuration > Service Provisioning – Content > Write (Write access)	**Configuration Navigator only:** ■ vTap **Configuration Navigator and Workflow:** ■ Service Construct > CA Certificate List ■ Service Construct > Control Service Profile > DHCP Service Profile ■ Service Construct > Header Enrichment ■ Service Construct > TLS Termination Policy ■ Service Construct > URL Rewrite Profile ■ Services > Content Cache > Instance ■ Services > Content Filter > Instance ■ Services > DNS Proxy Service > DNS Proxy Instance ■ Services > DNS Proxy Service > DNS Policy ■ Services > DNS Proxy Service > DNS IP Flow ■ Services > Multi Protocol Proxy > Encryption Profile ■ Services > Multi Protocol Proxy > Explicit Proxy Profile ■ Services > Multi Protocol Proxy > Fraud Detection Profile ■ Services > Multi Protocol Proxy > Http Ip Flow ■ Services > Multi Protocol Proxy > Http Request Policy ■ Services > Multi Protocol Proxy > Http Response Policy ■ Services > Multi Protocol Proxy > HTTPS Profile ■ Services > Multi Protocol Proxy > Instance ■ Services > Multi Protocol Proxy > Minify ■ Services > Multi Protocol Proxy > Preemptive DNS ■ Services > Multi Protocol Proxy > Server Connection ■ Services > Multi Protocol Proxy > Service Data Flow ■ Services > Multi Protocol Proxy > SPS Attribute ■ Services > Multi Protocol Proxy > SPS Profile ■ Services > Multi Protocol Proxy > Steering Group ■ Services > Multi Protocol Proxy > TCP Splicing Policy ■ Services > Multi Protocol Proxy > TCP Splicing Profile ■ Services > Multi Protocol Proxy > Web Image Optimization ■ Services > Http Server > Instance ■ Services > SMTP Proxy > Instance ■ Services > Video Adaptation ■ Services > Video Adaptation > Instance ■ Services > Video Adaptation > Offline Serving Policy ■ Services > Video Adaptation > Offline Transcoding Policy ■ Services > Video Adaptation > Online Transcoding Policy

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
(Continued)	■ Services > Video Adaptation > Target Media Profile ■ Services > Video Adaptation > Transcoding Rule ■ Services > WAP Gateway > Instance ■ Services > WAP Gateway > WAP IP Flow ■ Services > WAP Gateway > Service Data Flow
Configuration > MCC Configuration > Service Provisioning – Content > Admin (Administrative access)	**Configuration Navigator:** ■ vTap ■ Service Construct > CA Certificate List ■ Service Construct > Control Service Profile > DHCP Service Profile ■ Service Construct > Deep Packet Inspection ■ Service Construct > File Download Profile ■ Service Construct > Header Enrichment ■ Service Construct > TCP Optimization Profile ■ Service Construct > TLS Termination Policy ■ Service Construct > URL List ■ Service Construct > URL List Stats ■ Service Construct > URL Rewrite Profile ■ Services > Content Cache > Instance ■ Services > Content Cache > Eviction Threshold Disk ■ Services > Content Cache > Eviction Threshold Memory ■ Services > Content Filter > Category Source ■ Services > Content Filter > Global ■ Services > Content Filter > Instance ■ Services > DNS Proxy Service > DNS Proxy Instance ■ Services > DNS Proxy Service > DNS Policy ■ Services > DNS Proxy Service > DNS IP Flow ■ Services > Multi Protocol Proxy > Back End Forwarding ■ Services > Multi Protocol Proxy > Encryption Profile ■ Services > Multi Protocol Proxy > Http Ip Flow ■ Services > Multi Protocol Proxy > Http Request Policy ■ Services > Multi Protocol Proxy > Http Response Policy ■ Services > Multi Protocol Proxy > HTTPS Profile ■ Services > Multi Protocol Proxy > Instance ■ Services > Multi Protocol Proxy > LTMI ■ Services > Multi Protocol Proxy > Non HTTPS Profile ■ Services > Multi Protocol Proxy > Preemptive DNS

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
(Continued)	■ Services > Multi Protocol Proxy > Server Connections ■ Services > Multi Protocol Proxy > Minify ■ Services > Multi Protocol Proxy > SPS Attribute ■ Services > Multi Protocol Proxy > SPS Profile ■ Services > Multi Protocol Proxy > Service Data Flow ■ Services > Multi Protocol Proxy > Steering Group ■ Services > Multi Protocol Proxy > Web Image Optimization ■ Services > Multi Protocol Proxy > Fraud Detection Profile ■ Services > Multi Protocol Proxy > HTTPS Profile ■ Services > Http Server > Instance ■ Services > SMTP Proxy > Instance ■ Services > Video Adaptation ■ Services > Video Adaptation > Instance ■ Services > Video Adaptation > Offline Serving Policy ■ Services > Video Adaptation > Offline Transcoding Policy ■ Services > Video Adaptation > Online Transcoding Policy ■ Services > Video Adaptation > Target Media Profile ■ Services > Video Adaptation > Transcoding Rule ■ Services > WAP Gateway > Instance ■ Services > WAP Gateway > WAP IP Flow ■ Services > WAP Gateway > Service Data Flow **Actions:** ■ Service Construct > URL List *name* import **Workflow:** ■ Service Construct > Header Enrichment ■ Service Construct > File Download Profile ■ Service Construct > TCP Optimization Profile ■ Service Construct > URL List ■ Service Construct > Control Service Profile > DHCP Service Profile ■ Services > Content Cache > Instance ■ Services > Content Filter > Instance ■ Services > Multi Protocol Proxy > Encryption Profile ■ Services > Multi Protocol Proxy > Http Ip Flow ■ Services > Multi Protocol Proxy > Http Request Policy ■ Services > Multi Protocol Proxy > Http Response Policy ■ Services > Multi Protocol Proxy > Instance ■ Services > SMTP Proxy > Instance ■ Services > Video Adaptation

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
(Continued)	■ Services > WAP Gateway > Instance ■ Services > WAP Gateway > WAP IP Flow **Management Functions:** ■ HTTP Filter File Management ■ Subscriber Group File Management
Configuration > MCC Configuration > Service Provisioning – FBWU > Read (Read-Only access) Configuration > MCC Configuration > Service Provisioning – FBWU > Write (Write access) Configuration > MCC Configuration > Service Provisioning – FBWU > Admin (Administrative access)	**Configuration Navigator and Workflow:** ■ Services > Affirmed Apps > Fair Bandwidth Usage Service Profile
Configuration > MCC Configuration > Workflow Provisioning > Read (Read-Only access) Configuration > MCC Configuration > Workflow Provisioning > Write (Write access) Configuration > MCC Configuration > Workflow Provisioning > Admin (Administrative access) ***Note:*** *Provides Read-Only access to all other provisioning entities in the Affirmed Open Workflow application.*	**Configuration Navigator and Workflow:** ■ Workflow > Data Profile ■ Workflow > Subscriber Analyzer **Management Functions:** ■ Workflow Provisioning ■ Service Evaluation
Configuration > MME Configuration > Read	**Configuration Navigator:** ■ Read objects
Configuration > MME Configuration > Read/Write	**Configuration Navigator:** ■ Read/Write objects
Configuration > MME Configuration > Admin	**Configuration Navigator:** ■ Administer objects
Configuration > Software Configuration > Software Details > Add Software Details	Add a software release
Configuration > Software Configuration > Software Details > Modify Software Details	Modify a software release
Configuration > Software Configuration > Software Details > Delete Software Details	Delete a software release
Configuration > Software Configuration > Software Details > View Software Details	View a software release
Configuration > Software Configuration > Software Details > Obsolete Software Details	Set a software release obsolete
Configuration > Software Configuration > Software Schedule > Add Software Schedule	Add a software schedule

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > Software Configuration > Software Schedule > Modify Software Schedule	Modify a software schedule
Configuration > Software Configuration > Software Schedule > Copy Software Schedule	Copy a software schedule
Configuration > Software Configuration > Software Schedule > Delete Software Schedule	Delete a software schedule
Configuration > Software Configuration > Software Schedule > View Software Schedule	View a software schedule
Configuration > Software Configuration > Software Schedule > Start Software Schedule	Enable a software schedule QuickStart a software schedule
Configuration > Software Configuration > Software Schedule > Stop Software Schedule	Disable a software schedule
Configuration > Software Configuration > Software Schedule > View Sub Tasks	View software schedule subtasks
Configuration > Software Configuration > Software Schedule > View Software Schedule	View software schedule status
Configuration > Software Configuration > Software Rollback > Run Software Rollback	Perform a software rollback
Configuration > Software Configuration > Software Rollback > View Software Rollback	View software rollback process
Configuration > Configuration Template > Template Maintenance > Add Configuration Template	Add a configuration template
Configuration > Configuration Template > Template Maintenance > Modify Configuration Template	Modify a configuration template
Configuration > Configuration Template > Template Maintenance > Copy Configuration Template	Copy a configuration template
Configuration > Configuration Template > Template Maintenance > Delete Configuration Template	Delete a configuration template
Configuration > Configuration Template > Template Maintenance > Obsolete Configuration Template	Set a configuration template obsolete
Configuration > Configuration Template > Template Maintenance > Export Configuration Template	Export a configuration template
Configuration > Configuration Template > Template Maintenance > Import Configuration Template	Import a configuration template
Configuration > Configuration Template > Template Maintenance > View Configuration Template	View a configuration template

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > Configuration Template > Template Schedule > Add Template Schedule	Add a template schedule
Configuration > Configuration Template > Template Schedule > Modify Template Schedule	Modify a template schedule
Configuration > Configuration Template > Template Schedule > Copy Template Schedule	Copy a template schedule
Configuration > Configuration Template > Template Schedule > Delete Template Schedule	Delete a template schedule
Configuration > Configuration Template > Template Schedule > Start Template Schedule	Enable a template schedule
Configuration > Configuration Template > Template Schedule > Stop Template Schedule	Disable a template schedule
Configuration > Configuration Template > Template Schedule > Execute Template	Execute a template schedule QuickStart a template schedule
Configuration > Configuration Template > Template Schedule > View Template Schedule	View a template schedule
Configuration > SSF Configuration > Read	**Configuration Navigator:** Access read SSF objects
Configuration > SSF Configuration > Read/Write	**Configuration Navigator:** Access read and configure SSF objects
Configuration > SSF Configuration > Admin	**Configuration Navigator:** Access configure SSF objects
Configuration > FTP Server Details > Add FTP Server Details	Add a file server
Configuration > FTP Server Details > Modify FTP Server Details	Modify a file server
Configuration > FTP Server Details > Delete FTP Server Details	Delete a file server
Configuration > FTP Server Details > View FTP Server Details	View a file server
Configuration > Config Audit Trails > View Config Audit Trails	View the Audit Trail
Configuration > Config Audit Trails > Export Config Audit Trails	Export the Audit Trail
Configuration > URL List Management	Manage URL lists
Configuration > CUPS Manager > Configuration > Read	**Management Functions:** ■ List all the C-Plane, U-Plane groups ■ Audit the common configuration on the C-Plane and U-Plane

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Configuration > CUPS Manager > Configuration > Read/Write	**Management Functions:** ■ List all the C-Plane, U-Plane groups ■ Audit the common configuration on the C-Plane and U-Plane ■ Migrate existing clusters to C-Plane/U-Plane ■ Sync the common configuration from the C-Plane to the U-Plane
Configuration > CUPS Manager > Configuration > Admin	**Management Functions:** ■ List all the C-Plane, U-Plane groups ■ Migrate existing clusters to C-Plane/U-Plane ■ Audit the common configuration on the C-Plane and U-Plane ■ Sync the common configuration from the C-Plane to the U-Plane
Fault	
Fault > Alarms > View Alarms	View alarms
Fault > Alarms > Delete Alarms	Delete alarm
Fault > Alarms > Acknowledge Alarms	Acknowledge alarm
Fault > Alarms > Clear Alarms	Clear alarm
Fault > Alarms > Assign Owner	Assign alarm owner
Fault > Alarms > Annotate Alarm	Annotate alarm
Fault > Alarms > Export Alarms	Export alarms
Fault > Alarms > Print Alarms	Print alarms
Fault > Alarms > Forward Alarms	Forward alarm
Fault > Alarms > Alarm Summary	View alarm summary
Fault > Alarms > View Alarm Purge Interval	View the alarm purge interval
Fault > Alarms > Configure Alarm Purge Interval	Configure alarm purge interval
Fault > Alarms > Purge Alarms	Purge alarm
Fault > Alarms > Generate Alarm Report	Generate an alarm report
Fault > Alarms > Modify Alarm Details	Modify alarm details
Fault > Alarms > Alarm Archive	View alarm archive
Fault > Alarms > Alarm Archive > Alarm Archive From Local	View alarm archive from local file

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Fault > Alarms > Alarm Archive > Alarm Archive From Server	View alarm archive from server file
Fault > Alarms > Alarm Archive > Delete Alarm Archive	
Fault > Alarms > Manage > Manage Alarm Trap Forwarding	Configure SNMP alarm forwarding
Fault > Alarms > Manage > Manage Alarm Trap Forwarding > Add SNMP Publisher	Add an SNMP Listener
Fault > Alarms > Manage > Manage Alarm Trap Forwarding > Modify SNMP Publisher	Modify an SNMP Listener
Fault > Alarms > Manage > Manage Alarm Trap Forwarding > Delete SNMP Publisher	Delete an SNMP Listener
Fault > Alarms > Manage > Manage Alarm Trap Forwarding > Assign Filter for SNMP Publisher	Associate the trap listener with alarm filters
Fault > Alarms > Manage > Manage Alarm Email Forwarding	Configure alarm e-mail forwarding
Fault > Alarms > Manage > Manage Alarm Email Forwarding > Add Email Publisher	Add an E-mail Listener
Fault > Alarms > Manage > Manage Alarm Email Forwarding > Modify Email Publisher	Modify an E-mail Listener
Fault > Alarms > Manage > Manage Alarm Email Forwarding > Delete Email Publisher	Delete an E-mail Listener
Fault > Alarms > Manage > Manage Alarm Email Forwarding > Assign Filter for Email Publisher	Associate the Email Publisher with alarm filters
Fault > Configuration	Configure Trap OID Display Length
Fault > Logs > View Logs	View Event Logs
Fault > Logs > Export Logs	Export Event Logs
Fault > Logs > Print Logs	Print Event Logs
Fault > Logs > View Log Purge Interval	View the purge interval for event logs
Fault > Logs > Configure Log Purge Interval	Configure the purge interval for event logs
Fault > Logs > Purge Logs	Purge event log
Fault > Logs > Logs Archive	To view an event log archive
Fault > Logs > Logs Archive > Logs Archive From Local	View logs archive from local file
Fault > Logs > Logs Archive > Logs Archive From Server	View logs archive from server file

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Performance	
Performance > Configure Threshold > Add Threshold	Add a threshold
Performance > Configure Threshold > Modify Threshold	Modify a threshold
Performance > Configure Threshold > Delete Threshold	Delete a threshold
Performance > Configure Threshold > View Threshold	View a threshold
Performance > View Report > View Real Statistics	View Real Time Statistics
Performance > View Report > Export Reports Now	Export Reports Now
Performance > View Report > View Historical Statistics	View Historical Statistics
Performance > View Report > View Outage Report	View Outage Report
Performance > View Report > Export Report Config	Configure Export Report
Performance > View Report > Purge Export Configuration	Configure Export Purge Interval
Performance > View Report > Export Outage Report	Export Outage Report
Performance > View Report > Report Configuration	Configure a performance report
Performance > User Tasks > Task Schedule > View Task Schedule	View a user task schedule Export a list of user task schedules
Performance > User Tasks > Task Schedule > Modify Task Schedule	Modify a user task schedule
Performance > User Tasks > Task Schedule > Delete Task Schedule	Delete a user task schedule
Performance > User Tasks > Task Schedule > Start/Enable Task Schedule	Start/Enable/disable a user task schedule Quick Start a user task schedule
Performance > User Tasks > Task Schedule > Disable Task Schedule	Disable a user task schedule
Performance > User Tasks > Task Template > Add Task Template	Add a user task template
Performance > User Tasks > Task Template > Modify Task Template	Modify a user task template
Performance > User Tasks > Task Template > Delete Task Template	Delete a user task template
Performance > User Tasks > Task Template > View Task Template	View a user task template
Performance > PM Stats > Add Dashboard	Add a new dashboard
Performance > PM Stats > Modify Dashboard	Modify a dashboard

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Performance > PM Stats > Delete Dashboard	Delete a dashboard
Performance > PM Stats > View Dashboard	View Key Performance Indicators Export list of dashboards
Performance > System Reachability	View system availability
Performance > Instance Filter Configuration	Configure an Instance Filter
Performance > Stats Recovery	Manage statistics recovery schedules
Security	
Security Manager > Security Group Details > Add Group	Add Security Group
Security Manager > Security Group Details > Modify Group	Modify Security Group
Security Manager > Security Group Details > Modify Group > Modify Functional Access	Modify Security Group Permissions
Security Manager > Security Group Details > Delete Group	Delete Security Group
Security Manager > Security Group Details > View Group	View Security Group Export list of Security Groups
Security Manager > Security Group Details > Copy Group	Copy Security Group
Security Manager > Security Group Details > Associate Resources	Associate Resources with a Security Group
Security Manager > Security User Details > Add User	Add User
Security Manager > Security User Details > Modify User Details	Modify User Unlock User
Security Manager > Security User Details > Modify User Details > Admin Details	Modify Admin User Details
Security Manager > Security User Details > Modify User Details > General Details	Modify General User Details
Security Manager > Security User Details > Delete User	Delete User
Security Manager > Security User Details > View Audit Trails	View a user’s audit trail
Security Manager > Security User Details > View User Details	View user Export list of users
Security Manager > Security User Details > Kill User	Terminate a user’s session
Security Manager > Security User Details > Change Password	Change user password
Security Manager > Security User Details > View Active Users List	View active users list

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Security Manager > Security User Details > View Resource Audit Trails	View Resource Audit Trails
Security Manager > Security User Details > Export Resource Audit Trails	Export Resource Audit Trails
Security Manager > Change Password	Change password
Tools	
Tools > Color Settings > View Severity Color Configuration	View alarm severity color settings
Tools > Color Settings > Edit Severity Color Configuration	Configure alarm severity color settings
Tools > Northbound API	Use the Northbound API
Tools > Network Configuration Backup	Configure or trigger a backup of NE configuration data
Tools > Database Administration > Backup > Schedule Backup	Schedule a database backup
Tools > Database Administration > Backup > View Backup	View a triggered database backup
Tools > Database Administration > Backup > View Backup Schedule	View a scheduled database backup
Tools > Database Administration > Backup > Delete Backup	Delete a database backup
Tools > Database Administration > Backup > User Triggered Backup	Add a user triggered database backup
Tools > Database Administration > Restore	Restore the database from a backup
Tools > NE Config Backup	Schedule or trigger a backup of NE configuration data
Tools > NE Config Backup > User Triggered NE Config Backup	Trigger a backup of NE configuration data
Tools > NE Config Backup > NE Config Backup View	View NE configuration backup details
Tools > NE Config Backup > NE Config Backup Delete	Delete a backup of NE configuration data
Tools > NE Config Backup > NE Config Backup Restore	Restore an NE configuration backup file
Tools > NE Config Backup > NE Config Backup Download	Download a backup of NE configuration data
Tools > NE Config Backup > NE Config Backup Purge	Purge NE configuration data backup files
Tools > NE Config Backup > Scheduled NE Backup > Add	Schedule a backup of NE configuration data
Tools > NE Config Backup > Scheduled NE Backup > View	View scheduled NE configuration backup details
Tools > NE Config Backup > Scheduled NE Backup > Modify	Modify a scheduled NE configuration backup
Tools > NE Config Backup > Scheduled NE Backup > Start	Enable NE configuration backup schedule

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
Tools > NE Config Backup > Scheduled NE Backup > Stop	Disable NE configuration backup schedule
Tools > NE Config Backup > Scheduled NE Backup > Force Start	Quick Start (instantly execute) an NE configuration backup schedule
Tools > NE Config Backup > Scheduled NE Backup > Export	Export NE configuration backup schedule
Tools > NE Config Backup > Scheduled NE Backup > Delete	Delete an NE configuration backup schedule
Topology	
Topology > Element Details > Add Element	Add Network Element
Topology > Element Details > Modify Element	Modify Network Element
Topology > Element Details > Delete Element	Delete Network Element
Topology > Element Details > View NE Remarks	View remarks for a network element
Topology > Element Details > Add NE Remarks	Add remarks to a network element
Topology > Element Details > View Element	View Network Element
Topology > Manage/Unmanage	Manage/unmanage a network element
Topology > Group Details > Add Group	Add Group
Topology > Group Details > Edit Group	Modify Group
Topology > Group Details > Delete Group	Delete Group
Topology > System Configuration > View Mail Server Details	View the mail server
Topology > System Configuration > Configure Mail Server Details	Configure the mail server
Topology > System Configuration > View SNMP Details	View SNMP settings
Topology > System Configuration > Configure SNMP Details	Configure SNMP settings
Topology > System Configuration > View Audit Trails Details	View Audit Trail
Topology > System Configuration > Configure Audit Trails Details	Configure Audit Trail purge settings
Topology > System Configuration > Configure Admin Contact Details	Configure the email ID to be included in the system-level message prompt to any user attempting to log into a locked or expired account
Topology > Edit Protocols > Edit SNMPv2c	

Table 7-1 Group Permissions

Group Permission	Management Functions, Managed Objects, and Actions
VNF Manager	
VNF Manager > Configuration > Read	**Management Functions:** ■ In VNF Manager > Cluster View: – View information
VNF Manager > Configuration > Read/Write	**Management Functions:** ■ In VNF Manager > Cluster View: – View information – Assign policies – Manually create and remove nodes
VNF Manager > Configuration > Admin	**Management Functions:** ■ In VNF Manager > Cluster View: – View information – Create/Modify/Assign/Delete policies – Manually create and remove nodes

Users

Adding Users

An administrator can add users.

Note: *To add a user, you must have the Security Manager > Security User Details > Add User security group permission. For instructions, see Specifying Permissions by Security Group.*

To add a user:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

2 Click the **Add** icon.

3 Configure the parameters as follows:

- **User Name** – User account name
- **Password** – User account password
- **Confirm Password** – User account password
- **Idle Timeout** – Number of minutes of idle time after which the user is logged out. Value 0 indicates the client session does not expire.
- **Maximum Password Age** – Number of days from the first login after which the password expires. A value of 0 indicates that the password does not expire.
- **Maximum Account Age** – Number of days from the first login after which the user account expires. A value of 0 indicates that the account does not expire.
- **Description** – User account description
- **Status** – User account status:
  - Active: User is active and can log in.
  - Inactive: User is inactive and cannot log in
  - Blocked: User is blocked from logging in
  - Password Expired: Maximum password age has expired
  - Account Expired: Maximum Account Age has expired
  - Account Locked: User had consecutive failed logon attempts (default 6), so the user account is disabled and must be activated by the administrator.
  - Change Password on Login: User is forced to change password on next login

  - Dormancy Period Exceeded: User is locked out because the dormancy time was exceeded
- **Supervisor** – Supervisor account (to terminate the user's session, change the user's password, controlling the user's status)
- **Assign Group** – Groups to which the user account belongs. Select a group and click the right-arrow to assign the user to it.
- **Pager** – User account pager address, specified as <PAGERNUMBER>@<SERVICEPROVIDERDOMAIN>.
- **E-mail Address** – User account e-mail address
- **Mobile** – User account phone number
- **Password Change on re-Login** – Mark the checkbox to force the user to change password on next login.

4 Click **Save**.

Viewing Users

Note: *To view a user, you must have the Security Manager > Security User Details > View User Details security group permission. For instructions, see Specifying Permissions by Security Group.*

To view users:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

Users are listed with the following information:

- **User Name** – User account name
- **Assigned Group(s)** – Groups to which the user account belongs
- **Description** – User account description
- **Status** – User account status:
  - Active: User is active and can log in.
  - Inactive: User is inactive and cannot log in
  - Blocked: User is blocked from logging in
  - Password Expired: Maximum password age has expired
  - Account Expired: Maximum Account Age has expired

  - Account Locked: User had consecutive failed logon attempts (default 6), so the user account is disabled and must be activated by the administrator.
  - Change Password on Login: User is forced to change password on next login
  - Dormancy Period Exceeded: User is locked out because the dormancy time was exceeded
- **E-mail Address** – User account e-mail address
- **Updated Time** – Date and time of last update of the account
- **Account Expiry** – Date and time when the account will expire

2 From the **Security User** window, use any of the following methods to view a user's details:

Toolbar: Select the user and click the **View** icon.

Pop-up menu: Right-click the user and click **View**.

Acuitas displays the User Profile window, listing the settings for the user:

- **Name** – User account name
- **Idle Timeout** – Number of minutes of idle time after which the user is logged out. Value 0 indicates the client session does not expire.
- **Maximum Password Age** – Number of days from the first login after which the password expires. A value of 0 indicates that the password does not expire.
- **Maximum Account Age** – Number of days from the first login after which the user account expires. A value of 0 indicates that the account does not expire.
- **Assign Group** – Groups to which the user account belongs.
- **Pager** – User account pager address, specified as <PAGERNUMBER>@<SERVICEPROVIDERDOMAIN>.
- **E-mail** – User account e-mail address.
- **Mobile** – User account phone number.
- **Supervisor** – Supervisor account (used to terminate the user's session, change the user's password, and control the user's status).
- **Password Change on re-Login** – Whether to force the user to change password on next login.

3 Click **Close** to close the window.

Modifying Users

An administrator can modify users.

Note: *To modify a user, you must have the Security Manager > Security User Details > Modify User Details security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To modify a user:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

2 Use any of the following methods to edit the user:

Toolbar: Select the user and click the **Edit** icon.

Pop-up menu: Right-click the user and click **Edit**.

Acuitas displays the Edit User window, listing the settings for the user.

3 Configure the parameters as follows:

- **User Name** – User account name
- **Idle Timeout** – Number of minutes of idle time after which the user is logged out. Value 0 indicates the client session does not expire.
- **Maximum Password Age** – Number of days from the first login after which the password expires. A value of 0 indicates that the password does not expire.

  Cannot be modified for admin user.
- **Maximum Account Age** – Number of days from the first login after which the user account expires. A value of 0 indicates that the account does not expire.

  Cannot be modified for admin user.
- **Description** – User account description
- **Status** – User account status:
  - Active: User is active and can log in.
  - Inactive: User is inactive and cannot log in
  - Blocked: User is blocked from logging in
  - Password Expired: Maximum password age has expired
  - Account Expired: Maximum Account Age has expired

  - Account Locked: User had consecutive failed logon attempts (default 6), so the user account is disabled and must be activated by the administrator.
  - Change Password on Login: User is forced to change password on next login
  - Dormancy Period Exceeded: User is locked out because the dormancy time was exceeded

- **Supervisor** – Supervisor account (used to terminate the user's session, change the user's password, and control the user's status)
- **New Password** – User account password
- **Confirm Password** – User account password
- **Send Mail Notification** – Mark the checkbox to notify the user of a password change by e-mail.
- **Assign Group** – Groups to which the user account belongs. Select a group and click the right-arrow to assign the user to it.
- **Pager** – User account pager address, specified as <PAGERNUMBER>@<SERVICEPROVIDERDOMAIN>.
- **E-mail** – User account e-mail address
- **Mobile** – User account phone number
- **Password Change on re-Login** – Mark the checkbox to force the user to change password on next login.

4 Click **Save**.

Exporting Users

You can export a list of users to a CSV file.

Note: *To export a list of users, you must have the Security Manager > Security Users Details > View User Details permission. For instructions, see* *Specifying Permissions by Security Group*.

To export users:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

2 If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.

3 Click the **Export** icon.

Acuitas displays the **Configure Export Parameters** window.

4 Configure the parameters as follows:

- **File Type**: Select the required file format (CSV).
- **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
- **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
- **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.

5 Click **Apply**.

Acuitas displays the **Download Files** window.

6 Click **Download Exported File**.

7 From the **Download File**s window, click **Close**.

Changing User Password

An administrator can change a user's password.

Note: *To change a user's password, you must have the Security Manager > Security User Details > Change Password security group permission. For instructions, see Specifying Permissions by Security Group.*

To change a user password:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

2 Use any of the following methods to edit the user:

Toolbar: Select the user and click the **Edit** icon.

Pop-up menu: Right-click the user and click **Edit**.

Acuitas displays the Edit User window, listing the settings for the user.

3 Enter the new password in the **New Password** and **Confirm Password** fields.

4 To notify the user of the password change by e-mail, mark the **Send mail notification** checkbox.

5 Click **Save**.

Viewing User Audit Trail

The security Audit Trail is a record of users' Acuitas operations/activities. The following table lists the operation to the Acuitas system and the corresponding message logged to the audit trail:

Table 7-2 Audit Trail Operations

Category	Event	Logged Message
Authentication	User attempts to log into Acuitas	Login
	User attempts to log into Acuitas using the credentials of the blocked account	Login: User Blocked
	User tries to login into Acuitas using the credentials of account present in inactive status.	Login: User Inactive
	User tries to login into Acuitas using the credentials of the account present in temporary locked status.	Login: User Locked
	User tries to login into Acuitas using the wrong password for more than 3 times.	Login: Maximum failed login count exceeded. ***Note:*** *Also raises a Critical alarm*
	User tries to login into Acuitas using credentials of expired account.	Login: User Account Expired
	User tries to login into Acuitas using expired password	Login: Password Expired
	User tries to logout of Acuitas	Logout

Table 7-2 Audit Trail Operations

Category	Event	Logged Message
User Security Profile Update ***Note:*** *In the case of multiple updates to the user profile, a single message listing all changes is logged to the Audit Trail*	Modified Idle time out	Update: *username*'s idle time out period
	Update minimum Password Age	Update: *username*'s minimum password age
	Update maximum Password Age	Update: *username*'s maximum password age
	Update the account description	Update: *username*'s description
	Update the user account status	Update: *username*'s account status
	Update the account's supervisor	Update: *username*'s supervisor
	Assign or remove group associated with user	Update: *username*'s group assignment
	Update personal information email, pager	Update: *username*'s personal information email, pager

Table 7-2 Audit Trail Operations

Category	Event	Logged Message
Security Configuration Operations	Create a user account: **1** **Security => User Management** **2** Click the **Add** icon and create the user.	Add User: *username*
	Terminate a user session: **1** **Security => User Management** **2** Click the **Active User List** icon. **3** Mark the checkbox for the user and click the **Terminate User Session(s)** icon.	Terminate User Session: *username*
	Delete a user account: **1** **Security => User Management** **2** Select the user and click the **Delete** icon.	Delete User: *username* deleted
	Change a user password: **1** **Security => User Management** **2** Select the user and click the **Edit** icon. **3** Enter the new password in the New Password and Confirm Password fields.	Update: *username* changed the password
	Create a security group: **1** **Security => Group Management** **2** Click the **Add** icon and create the group.	Create group: *group name*
	Delete a security group: **1** **Security => User Management** **2** Select the security group and click the **Delete** icon.	Delete group: *group name*
	Modify a security group: **1** **Security => User Management** **2** Select the security group and click the **Edit** icon.	Update group: *group name*

Table 7-2 Audit Trail Operations

Category	Event	Logged Message
User Account Changes made by Acuitas	Password expired: When the user's maximum password age exceeds the number of days after first login, the Acuitas system updates the status of user profile to 'password expired.'	System: User *username*'s password expired ***Note:*** *Also raises a Major alarm*
	Enable User: Enable user to active status from the 'account blocked' status after waiting for the lockout time. Current lockout time is 30 minutes.	System: User *username* activated from blocked state
	Account expired: When the user's maximum account age exceeds the number of days after first login, the Acuitas system updates the status of user profile to 'Account expired.'	System: User *username*'s account expired ***Note:*** *Also raises a Major alarm*
	Dormancy period: Acuitas system marks the user's account status as 'Dormancy period exceeded' when either of following events takes place: ■ User attempts to login for first time, but the number of days between the account creation and the attempted login is greater than the dormancy period. ■ User attempts to login, but the number of days between the last successful login and the current login is greater than system's dormancy period. Existing dormancy period is configured as 30 days.	System: User *username* moved to dormant state ***Note:*** *Also raises a Major alarm*

Note: *To view an audit trail, you must have the Security Manager > Security User Details > View Audit Trails security group permission. For instructions, see Specifying Permissions by Security Group.*

To view the Audit Trail for all users:

1 Click the **Settings** icon on the toolbar and select **Security => Audit Trail**.

Acuitas displays the Audit Trail window, listing the Security Audit Trail, with the following details:

- Date and time of the event
- User name of the user that performed the operation
- IP address of the host performing the event.
- Module on which the operation was performed
- Operation description
- Element name
- Status of the event indicating the success or failure of that event.

2 To view all Audit Trails (Configuration, Fault, Performance, Platform, Security, and Topology), in the Filter Manager, select **All Modules**. If desired, use the Quick Filter to filter the data displayed in the window.

You can export the Audit Trail to a CSV/PDF/XLS/XML/HTML file.

To view the Audit Trail for a particular user:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

2 Select the user and click the **Audit Trail** icon.

Acuitas displays the Audit Trail window, listing the activities for the user, with the following details:

- Module on which the operation was performed
- Description of the operation
- User name of the user that performed the operation
- IP address of the host performing the event.
- Date and time of the event
- Status of the event indicating the success or failure of that event.

3 If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.

You can export the Audit Trail to a CSV/PDF/XLS/XML/HTML file.

To export the Audit Trail:

1. From the **Audit Trail** window, click the **Export** icon.

   Acuitas displays the **Configure Export Parameters** window.

2. Configure the parameters as follows:
   - **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
   - **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
   - **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
   - **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.
3. Click **Apply**.

   Acuitas displays the **Download Files** window.

4. Click **Download Exported File**.
5. From the **Download File**s window, click **Cancel**.

Managing Active User Sessions

An administrator can view the list of users who are currently logged in and terminate one or more user session(s).

Note: *To terminate a user's session, you must have the Security Manager > Security User Details > Kill User security group permission. For instructions, see Specifying Permissions by Security Group.*

To manage active user sessions:

1. Click the **Settings** icon on the toolbar and select **Security => User Management**.

   Acuitas displays the **Security User** window, listing the users in the system.

2. Click the **Active User List** icon.

   Acuitas displays the Active User Listing window, listing users currently logged in.

3. To terminate any user sessions, mark the checkboxes for the user(s) and click the **Terminate User Session(s)** icon.

4. At the confirmation prompt, click **Yes**.

   Acuitas forces the termination of the current session of the specified user(s) and takes the user(s) to the login prompt.

5. Click **Close** to close the window.

Unlocking Users

An administrator can unlock a user whose account is locked because the user tried to login with the wrong password six consecutive times (or the number of times specified in the securityconfiguration.properties file).

Note: *To unlock a user, you must have the Security Manager > Security User Details > Modify User Details security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To unlock a user:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

2 Select the user and click the **Unlock User** icon.

3 At the confirmation prompt, click **OK**.

Acuitas unlocks the account so that the user can log in.

Deleting Users

An administrator can delete users.

A currently logged-in user cannot be deleted. The default user admin cannot be deleted.

Note: *To delete a user, you must have the Security Manager > Security User Details > Modify User Details > Delete User security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To delete a user:

1 Click the **Settings** icon on the toolbar and select **Security =>**

User Management.

Acuitas displays the **Security User** window, listing the users in the system.

Toolbar: Select the user and click the **Delete** icon.

Pop-up menu: Right-click the user and click **Delete**.

2 At the confirmation prompt, click **OK**.

Chapter 8

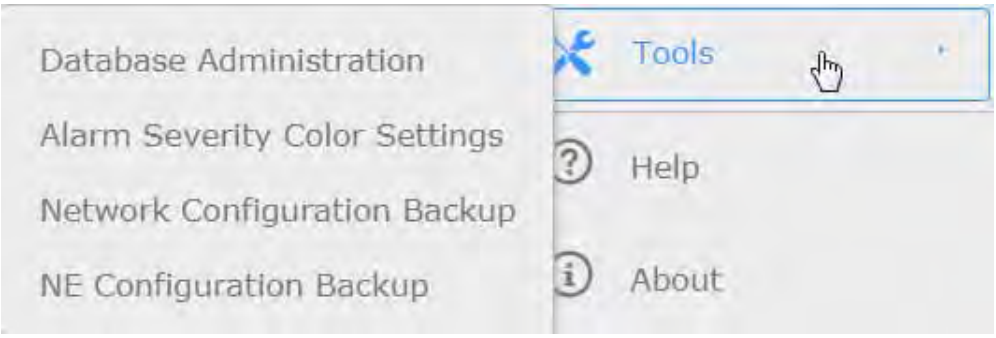
Tools

The following topics describe how to access and use the Tools applications:

- Database Administration
- Configuring Alarm Severity Color Settings
- Network Configuration Backup
- NE Configuration Backup and Restore

To access Tools applications, select the applicable option from the **Settings** icon on the toolbar.

Figure 8-1 Accessing Tools Applications



Database Administration

You can schedule a database backup for automatic execution and can trigger a backup manually on demand. The backup can also be used to restore a database from an earlier date and time.

Adding User Triggered Database Backup

You can trigger a backup on demand.

Note: *To add a user triggered database backup, you must have the Tools > Database Administration > Backup > User Triggered Backup security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure a user triggered database backup:

1. Click the **Settings** icon on the toolbar and select **Tools =>** **Database Administration**.

   Acuitas displays the **Database Backup and Restore** window.

2. Click the **User Triggered DB-Backup** icon.
3. Configure the parameters as follows:
   - **Backup Files Prefix Name** – Specify the prefix you want for the backup file, such as DB_backup.
   - **File Server** – Specify whether you want the backup stored on the local or remote server. It is recommended that you store the backup on the remote server, as a local backup will not be available if the system becomes out of service.
   - **Relative Path in File Server** – If you select to have the backup stored on remote server, specify the path where you want it stored. If you select to have the backup stored on the local server, it is stored at: */opt/Affirmed/NMS/server/databaseBackup*
   - **Full Backup** – Mark this checkbox to trigger a full backup.
4. Click **Save**.
5. At the confirmation prompt, click **OK**.
6. Click **Close**.

   Acuitas displays the backup in the **Database Backup and Restore** window.

Viewing Database Backup Details

You can view database backups details.

Note: *To view a triggered database backup, you must have the Tools > Database Administration > Backup > View Backup security group permission. For instructions, see Specifying Permissions by Security Group.*

To view database backup details:

1 Click the **Settings** icon on the toolbar and select **Tools => Database Administration**.

Acuitas displays the **Database Backup and Restore** window.

2 Use any of the following methods to view an backup's details:

Toolbar: Select the backup and click the **View DB Backup** icon.

Pop-up menu: Right-click the backup and click **View DB Backup**.

Acuitas displays the **View Database Backup** window.

3 Click **Close** to close the window.

Scheduling Database Backup

You can configure the Acuitas server to backup its database based on a pre-configured schedule. *Do not* schedule backups more than twice a day, as it can impact on system performance (backups cause pauses in Acuitas system and affect performance/scalability of the system).

Note: *To schedule a database backup, you must have the Tools > Database Administration > Backup > Schedule Backup security group permission. For instructions, see Specifying Permissions by Security Group.*

To schedule a database backup:

1 Click the **Settings** icon on the toolbar and select **Tools => Database Administration**.

Acuitas displays the **Database Backup and Restore** window.

2 Click the **Scheduled DB-Backup** icon.

3 Configure the parameters as follows:

- **Backup Files Prefix Name** – Specify the prefix you want for the backup file, such as DB_backup.
- **File Server** – Specify whether you want the backup stored on the local or remote server. It is recommended that you store the backup on the remote server, as a local backup will not be available if the system becomes out of service.
- **Relative Path in File Server** – If you select to have the backup stored on remote server, specify the path where you want it stored. If you select to have the backup stored on the local server, it is stored at: */opt/Affirmed/NMS/server/databaseBackup*
- **Full Backup** – Mark this checkbox to trigger a full backup.
- **Recurrence** – Mark this checkbox to specify a backup recurrence. *Do not* schedule more than twice a day, as it can impact system performance:
  - Click the **Recurrence Pattern** icon and configure Recurrence Details.
  - Click the **Recurrence**.
- **Purge Backup** – Mark this checkbox to specify how many backups to retain.

4 Click **Save**.

Viewing Scheduled Database Backup

You can view a scheduled database backup.

Note: *To view a scheduled database backup, you must have the Tools > Database Administration > Backup > View Backup Schedule security group permission. For instructions, see Specifying Permissions by Security Group.*

To view a scheduled database backup:

1 Click the **Settings** icon on the toolbar and select **Tools => Database Administration**.

Acuitas displays the **Database Backup and Restore** window.

2 Click the **Scheduled DB-Backup View** icon.

3 Click **Close** to close the window.

Deleting Database Backup

You can delete a database backup.

Note: *To delete a database backup, you must have the Tools > Database Administration > Backup > Delete Backup security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete a database backup:

1. Click the **Settings** icon on the toolbar and select **Tools => Database Administration**.

   Acuitas displays the **Database Backup and Restore** window.

2. Use any of the following methods to delete a backup:

   Toolbar: Select the backup and click the **Delete DB Backup** icon.

   Pop-up menu: Right-click the backup and click **Delete DB Backup**.

   Acuitas displays the View Database Backup window.

3. Click **Close** to close the window.
4. At the confirmation prompt, click **OK**.
5. Click **Close** to close the window.

   Acuitas removes the backup from the **Database Backup and Restore** window.

Restoring Database from Backup

You can restore the Acuitas database to a successful backed up version.

Use the appropriate method to restore the database:

- Standalone Acuitas Server
- Acuitas Server Cluster (HA or HA + DR)

CAUTION: Database restore is service affecting. During the process, the Acuitas server is brought down.

Note: *To restore the database from a backup, you must have the Tools > Database Administration > Restore security group permission. For instructions, see Specifying Permissions by Security Group.*

Standalone Acuitas Server

To restore the database from a backup:

1 Click the **Settings** icon on the toolbar and select **Tools =>**

Database Administration.

Acuitas displays the **Database Backup and Restore** window.

2 Use any of the following methods to restore the database to a backup:

Toolbar: Select the backup and click the **Restore Database** icon.

Pop-up menu: Right-click the backup and click **Restore Database**.

3 At the confirmation prompt, click **OK**.

4 Click **Close** to close the window.

Note: *If the restore operation fails, Acuitas displays the Database Restore Operation window. Click Yes to restore the database from the local machine. Click No to restore an existing database.*

5 Determine whether the restoration process has finished. To do so, issue the following command from the /opt/Affirmed/NMS/dbrestore directory:

```
[root@qahpems02 dbrestore]# ls -lrt
```

If the command output indicates that the directory contains the sql file, the process *is not* complete.

In the following sample command output, the sql file is shown in red text.

```
total 135096
-rw-r--r-- 1 root root       600 Oct  5 14:19 log4j.xml
drwxr-xr-x 2 root root      4096 Oct 11 10:47 bin
drwxr-xr-x 2 root root      4096 Oct 11 10:47 lib
-rw-r--r-- 1 root root       103 Oct 11 15:41 restore.txt
-rw-r--r-- 1 root root 138315816 Oct 11 16:31
http3_10-11-2012-16-30-03.sql
-rw-r--r-- 1 root root      2038 Oct 11 16:31 restore.log
```

If the command output indicates that the directory no longer contains the sql file and contains the restore.txt file and the restore.log file, the restore is successful.

In the following sample command output, the restore.txt and the restore.log files are shown in red text.

```
total 20
-rw-r--r-- 1 root root  600 Oct  5 14:19 log4j.xml
drwxr-xr-x 2 root root 4096 Oct 11 10:47 bin
drwxr-xr-x 2 root root 4096 Oct 11 10:47 lib
-rw-r--r-- 1 root root  103 Oct 11 16:38 restore.txt
-rw-r--r-- 1 root root 2194 Oct 11 16:38 restore.log
```

6 Once the restoration process has finished, you must manually start the server using starttems.sh with the -u option.

Acuitas Server Cluster (HA or HA + DR)

Use the configure_ha script to restore a database from backup. For configure_ha command syntax, see Acuitas High Availability Configuration.

To restore the database from a backup:

1 On the HA server, issue the following commands to restore the database:

```
cd /opt/Affirmed/NMS/bin
```

```
./configure_ha [--virtualhostname virtual hostname] [--virtualip
virtual IP address] [--primaryhostname primary hostname] [--primaryip
primary IP address] [--secondaryhostname secondary hostname]
[--secondaryip secondary IP address] [--multicastip multicast IP
address] [--backupfile file_path] [--restore]
```

```
Please double check the following configuration options:
{
  virtualhostname => 'virtual_hostname',
  virtualip => ' virtual_IP_address',
  primaryhostname => 'primary_hostname',
  primaryip => 'primary_IP_address',
  secondaryhostname => 'secondary_hostname',
  secondaryip => 'secondary_IP_address',
  primaryslaveid => 'primary_slave_ID',
  secondaryslaveid => 'secondary_slave_ID',
  primaryipinterface => 'primary_IP_interface',
  secondaryipinterface => 'secondary_IP_interface',
  ipinterface => 'IP_interface',
  multicastip => 'multicast_IP_address'
}
Are you sure you want to continue with this configuration? (y/n):
```

2 Enter **y** to continue with this configuration.

```
Are you sure you want to use the backup file file_path to restore the
database? (Y/N):
```

3 Enter **y** to restore the database.

Configuring Alarm Severity Color Settings

You can configure alarm severity colors settings. And, you can restore alarm severity colors settings to the system default settings.

Note: *To configure alarm severity color settings, you must have the Tools > Color Settings > Edit Severity Color Configuration security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure alarm severity color settings:

1. Click the **Settings** icon on the toolbar and select **Tools => Alarm Severity Color Settings**.

   Acuitas displays the **Color Configuration** window.
2. Click the color to be changed. Choose any color from the RGB or Color Slider tab.
3. Click **Apply**.
4. At the confirmation prompt, click **OK**.

To restore alarm severity colors to the system default settings:

1. Click the **Settings** icon on the toolbar and select **Tools => Alarm Severity Color Settings**.

   Acuitas displays the **Color Configuration** window.
2. Click **Restore to Defaults**.
3. Click **Apply**.

Network Configuration Backup

Acuitas supports backing up configuration data for each of the reachable managed NEs. You can:

- Schedule a backup of NE configuration data for automatic daily execution
- Trigger a backup manually on demand

The backup is saved as ASCII output that can be used to compare a configuration against one from another date and time to identify any configurations changes that occurred.

Network Configuration Backup files are retained for a maximum of 90 days.

In addition to backing up configuration data, Acuitas backs up the Virtual Network Function (VNF) Manager network inventory report to a CSV file. For details on the network inventory report, see Network Inventory Report.

Configuration Data Backup — Acuitas backs up the configuration data for each of the reachable managed NEs to individual files. The file is exported to the Acuitas server, in the directory */opt/Affirmed/NMS/server/ems/data/config/<NE name>*. The backup filename is *yyyy_mm_dd_hh_mm_ss*.cfg.

Note: *The configuration backup files **are not** replicated between nodes in High Availability and/or Disaster Recover Systems.*

Network Inventory Report Backup — Acuitas backs up the network inventory report to a CSV file. The file is exported to the Acuitas server, in the directory */opt/Affirmed/NMS/server/ems/data/report/nir*. The export filename is *yyyy_mm_dd_hh_mm_ss*.csv where *yyyy_mm_dd_hh_mm_ss* represents the timestamp of the report generation, for example 2014_11_05_15_26_49.csv.

Note: *To configure or trigger a backup, you must have the Tools > Configuration Backup security group permission. For instructions, see Specifying Permissions by Security Group.*

Triggering Configuration Backup on Demand

To trigger a configuration backup:

1. Click the **Settings** icon on the toolbar and select **Tools =>**

   Network Configuration Backup.

   Acuitas displays the **Network Configuration Backup** window.
2. Click **Backup Now**.
3. Click **Close**.

The configuration data and network inventory report backups are performed immediately and are retained for the configured retention period before being purged.

Scheduling Configuration Backup

To configure a configuration backup:

1. Click the **Settings** icon on the toolbar and select **Tools =>**

   Network Configuration Backup.

Acuitas displays the **Network Configuration Backup** window.

2 Configure the parameters as follows:

- **Enable Daily Backup** – Mark the checkbox to configure an automatic daily configuration data backup.
- **Task Execution Time** – Specify the time (24-hour) you want the backup to start.
- **Backup Retention Period** – Specify the number of days you want the backup stored before being purged.

3 Click **Save**.

4 Click **Close**.

The configuration data and network inventory report backups are performed daily at the configured execution time and are retained for the configured retention period before being purged.

NE Configuration Backup and Restore

From Acuitas, you can backup and restore NE configuration data:

- Backup – You can perform a backup of the NE configuration and store it on the local Acuitas server or a remote server. The backup is available to restore the configuration to a previous known state in the event of lost or incorrect configuration.

  You can:

  – Trigger a backup manually on demand

  – Schedule a backup of automatic daily execution

  NE Configuration Backup files are retained for a maximum of 90 days.

  Acuitas also supports backing up configuration data and network inventory reports for each of the reachable managed NEs to individual files. For details, see Network Configuration Backup.

- Restore – You can select a successful backed up configuration file and restore it on the NE. The result would be the NE configured exactly as the backup configuration.

Note: *To backup and restore NE configuration, you must have the Tools > NE Config Backup group permissions. For instructions, see Specifying Permissions by Security Group.*

Adding User Triggered NE Configuration Backup

You can trigger an NE backup on demand.

Note: *To add a user triggered NE configuration backup, you must have the Tools > NE Config Backup > User Triggered NE Config Backup security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure a user triggered NE backup:

1 Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

Acuitas displays the **NE Backup and Restore** window.

2 Click the **User Triggered NE-Backup** icon.

3 Configure the parameters as follows:

- **Backup Files Prefix Name** – Specify the prefix you want for the backup file, such as NE_backup.
- **File Server** – Specify the file server on which you want the backup stored.
- **Relative Path in File Server** – If you select to have the backup stored on a remote server, specify the path where you want the backup stored. If you select to have the backup stored on the EMS server, it is stored at: *JBOSSHOME/server/ems/data/nebackups.*
- **Select Elements**– Select the elements by highlighting and clicking the right-arrow.

4 Click **Save**.

5 At the confirmation prompt, click **OK**.

6 Click **Close**.

Acuitas initiates the NE configuration backup on each of the selected nodes. The backups of the individual nodes are stored on the configured file server location in separate folders labeled <*MCC Display Name*>. The details of the backup are logged in the configuration Audit Trail on success/failure.

Viewing NE Configuration Backup Details

You can view NE configuration backup details.

Note: *To view NE configuration backup details, you must have the Tools > NE Config Backup > NE Config Backup View security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To view NE configuration backup details:

1 Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

Acuitas displays the **NE Backup and Restore** window.

2 Use any of the following methods to view a backup's details:

Toolbar: Select the backup and click the **View** icon.

Pop-up menu: Right-click the backup and click **View**.

Acuitas displays the **View NE Backup** window.

3 Click **Close** to close the window.

Purging NE Configuration Backup Files

You can specify the purging mechanism to retain only the last number of backup files per MCC.

Note: *To purge NE configuration backup files, you must have the Tools > NE Config Backup > NE Config Backup Purge security group permission. For instructions, see Specifying Permissions by Security Group.*

To purge NE configuration backup files:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Click the **Purge** icon.
3. Mark the **Purge Backup** checkbox and specify how many backups to retain.
4. Click **Save**.

Downloading NE Configuration Backup File

You can download an NE configuration backup file only if its status is Success.

Note: *To download an NE configuration backup file, you must have the Tools > NE Config Backup > NE Config Backup Download security group permission. For instructions, see Specifying Permissions by Security Group.*

To download an NE configuration backup file:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Select the NE Configuration backup filename and click the **Download** icon.
3. At the confirmation prompt, click **OK**.

Restoring NE Configuration Backup File

You can restore an NE configuration backup file only if its status is Success.

Note: *To restore an NE configuration backup file, you must have the Tools > NE Config Backup > NE Config Backup Restore security group permission. For instructions, see Specifying Permissions by Security Group.*

To restore an NE configuration backup file:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Select the NE Configuration backup filename and click the **Restore** icon.

   Acuitas initiates NE configuration restore process on the specific MCC.

Deleting NE Configuration Backup

You can delete an NE configuration backup.

Note: *To delete an NE configuration backup, you must have the Tools > NE Config Backup > NE Config Backup Delete security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete an NE configuration backup:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Use any of the following methods to delete an NE configuration backup:

   Toolbar: Select the backup and click the **Delete** icon.

   Pop-up menu: Right-click the backup and select **Delete**.

3. At the confirmation prompt, click **OK**.

Scheduling NE Configuration Backup

You can configure the Acuitas server to backup NE configuration based on a pre-configured schedule.

Note: *To schedule an NE configuration backup, you must have the Tools > NE Config Backup > Scheduled NE Backup >Add security group permission. For instructions, see Specifying Permissions by Security Group.*

To schedule an NE configuration backup:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Click the **Scheduled NE-Backup** icon.

3. Click the **New** icon.

4. Configure the parameters as follows:

   - **NE Backup Schedule Name** – Specify the schedule name.
   - **Recurrence** – Mark this checkbox to specify a backup recurrence. By default, the scheduler will be scheduled to execute once every 12 hours. If you leave the checkbox unmarked, the schedule is saved in the disabled state:
     - Click the **Recurrence Pattern** icon . and configure the Recurrence Details.
     - Click **Reschedule**.
   - **Backup Files Prefix Name** – Specify the prefix you want for the backup file, such as NE_backup.
   - **File Server** – Specify the file server on which you want the backup stored.
   - **Relative Path in File Server** – If you select to have the backup stored on a remote server, specify the path where you want the backup stored. If you select to have the backup stored on the EMS server, it is stored at: *JBOSSHOME/server/ems/data/nebackups.*
   - **Select Elements**– Select the elements by highlighting and clicking the right-arrow.

5. Click **Save**.

Acuitas performs the NE configuration backup to execute once in every configured interval. By default, the scheduler executes the backup once in every 12 hours (the minimum interval).

The backups of the individual nodes are stored on the configured file server location in separate folders labeled <*MCC Display Name*>.

The details of the backup are logged in the configuration Audit Trail on success/failure.

Viewing Scheduled NE Configuration Backup Details

You can view scheduled NE configuration backup details.

Note: *To view a scheduled NE configuration backup details, you must have the Tools > NE Config Backup > Scheduled NE Backup > View security group permission. For instructions, see Specifying Permissions by Security Group.*

To view NE configuration backup details:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Click the **Scheduled NE-Backup** icon.
3. Use any of the following methods to view a backup's details:

   Toolbar: Select the backup and click the **View** icon.

   Pop-up menu: Right-click the backup and click **View**.

   Acuitas displays the **View NE Backup** window.
4. Click **Cancel** to close the window.

Modifying Scheduled NE Configuration Backup

You can modify a scheduled NE configuration backup only if it does not have the status Complete.

Note: *To modify a scheduled NE configuration backup, you must have the Tools > NE Config Backup > Scheduled NE Backup > Modify security group permission. For instructions, see Specifying Permissions by Security Group.*

To modify a scheduled NE configuration backup:

1 Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

Acuitas displays the **NE Backup and Restore** window.

2 Click the **Scheduled NE-Backup** icon.

3 Select the schedule and click the **Edit** icon.

4 Configure the parameters as follows:

- **NE Backup Schedule Name** – Specify the schedule name.
- **Recurrence** – Mark this checkbox to specify a backup recurrence. By default, the scheduler will be schedule to execute once in every 12 hours. If you leave the checkbox unmarked, the schedule is saved in the disabled state:
  - Click the **Recurrence Pattern** icon and configure Recurrence Details.
  - Click the **Recurrence**.
- **Backup Files Prefix Name** – Specify the prefix you want for the backup file, such as NE_backup.
- **File Server** – Specify the file server on which you want the backup stored.
- **Relative Path in File Server** – If you select to have the backup stored on a remote server, specify the path where you want the backup stored. If you select to have the backup stored on the EMS server, it is stored at: *JBOSSHOME/server/ems/data/nebackups.*
- **Select Elements**– Select the elements by highlighting and clicking the right-arrow.

5 Click **Save**.

Acuitas performs the NE configuration backup to execute once in every configured interval. By default, the scheduler executes the backup once in every 12 hours (the minimum interval).

The details of the backup are logged in the configuration Audit Trail on success/failure.

Enabling/Disabling NE Configuration Backup Schedules

You can enable/disable NE configuration backup schedules.

Note: *To enable an NE configuration schedule, you must have the Tools > NE Config Backup > Scheduled NE Backup > Start security group permission. To disable an NE configuration schedule, you must have the Tools > NE Config Backup > Scheduled NE Backup > Stop security group permission. For instructions, see Specifying Permissions by Security Group.*

To enable/disable an NE backup schedule:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Click the **Scheduled NE-Backup** icon.
3. Use any of the following methods to enable a schedule:

   Toolbar: Select the schedule and click the **Enable** icon.

   Pop-up menu: Right-click the schedule and select **Start**.

   Use any of the following methods to disable a schedule:

   Toolbar: Select the schedule and click the **Disable** icon.

   Pop-up menu: Right-click the schedule and select **Stop**.
4. At the confirmation prompt, click **OK**.

   The Administrative Status of the schedule changes to Enabled or Disabled.

Quick Start NE Configuration Backup Schedules

Note: *To Quick Start an NE configuration backup schedule, you must have the Tools > NE Config Backup > Scheduled NE Backup > Force Start security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To Quick Start (instantly execute) an NE configuration backup schedule:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Click the **Scheduled NE-Backup** icon.
3. Use any of the following methods to Quick Start a schedule:

   Toolbar: Select the schedule and click the **Quick Start** icon.

   Pop-up menu: Right-click the schedule and select **Quick Start**.

Exporting NE Configuration Backup Schedules

You can export an NE configuration backup schedule.

To export an NE configuration backup schedules:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Click the **Scheduled NE-Backup** icon.
3. If desired, use the Filter Manager to filter the data displayed in the window.
4. Select the schedule(s) to be exported. To select multiple schedules, Shift-click or Control-click the schedules in the list. To export the Whole Data or Current View, do not select any schedule.
5. Click the **Export** icon.

   Acuitas displays the **Configure Export Parameters** window.
6. Configure the parameters as follows:
   - **File Type**: Select the required file format (CSV).
   - **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
   - **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
   - **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.
7. Click **Apply**.

   Acuitas displays the **Download Files** window.
8. Click **Download Exported File**.
9. From the **Download File**s window, click **Close**.

Deleting NE Configuration Backup Schedules

You can delete an NE configuration backup schedule only if its administrative status is Disabled.

Note: *To delete an NE configuration backup schedule, you must have the Tools > NE Config Backup > Scheduled NE Backup > Delete security group permission. For instructions, see Specifying Permissions by Security Group.*

To delete an NE configuration backup schedule:

1. Click the **Settings** icon on the toolbar and select **Tools => NE Configuration Backup**.

   Acuitas displays the **NE Backup and Restore** window.

2. Click the **Scheduled NE-Backup** icon.
3. Use any of the following methods to delete a backup schedule:

   Toolbar: Select the schedule and click the **Delete** icon.

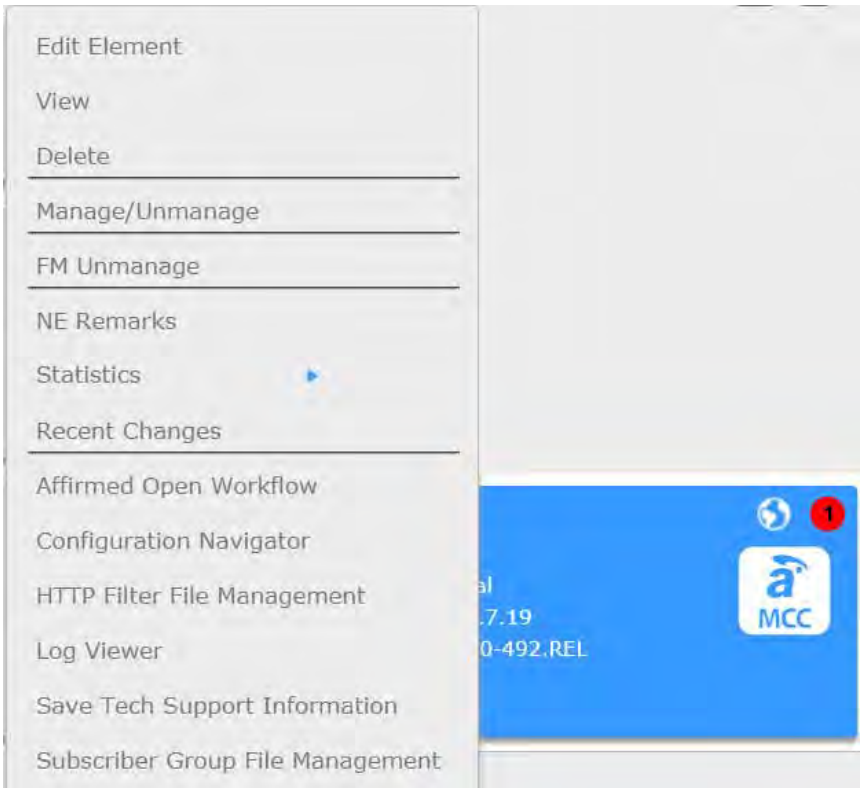
   Pop-up menu: Right-click the schedule and select **Delete**.
4. At the confirmation prompt, click **OK**.

Chapter 9

Affirmed Open Workflow

The Affirmed Open Workflow application runs on the system. It defines the treatment of a service flow across various services resident on the system. To access the application, right-click an NE and select **Affirmed Open Workflow**.

Figure 9-1 Accessing the Affirmed Open Workflow Application



Workflow also uses the HTTP Filter File Management application to define control lists to either allow or deny content requests to a specific list of domains or URLs. To access the HTTP Filter File Management application, right-click an NE and select **HTTP Filter File Management**. For details, see HTTP Filter File Management.

Overview

Workflow is an application running on the system that defines the treatment of a service flow across various services resident on the system. Workflow allows the Operator to customize a subscriber's packet treatment across various services.

Workflow binds a single or set of subscribers to a set of services and/or a control profile:

- The *set of services* specifies the services to provide for the PDN session. When the workflow is established, each associated subscriber's traffic flow is steered to the collection of associated services. Different subscriber flows can be given different treatment to provide end-to-end service(s).
- The *control profile* specifies the back-end interfaces to use for PCRF, authentication, accounting, and charging systems. As an alternative, the control profile allows the Operator to configure subscriber profiles statically rather than using these interfaces. The profile also specifies the mechanism to dynamically obtain the services that have been programmed on the system.

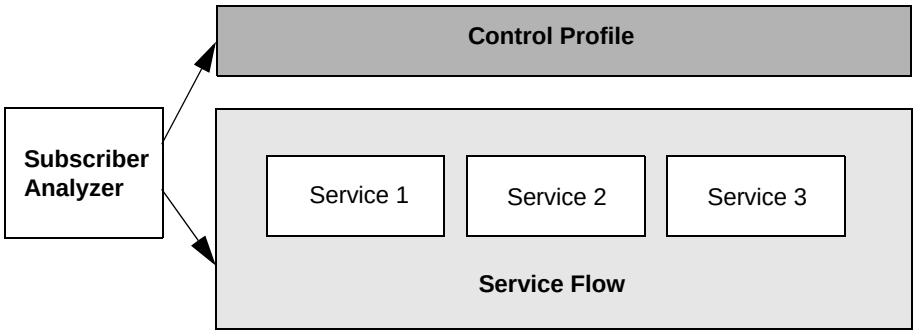
Bound to a workflow is a *subscriber analyzer*, which identifies subscribers whose traffic is subject to the workflow. The analyzer specifies which subscriber attributes to match to identify subscribers:

- **Static association** – An Operator binds a subscriber analyzer to a set of services by explicitly specifying the service flow to use.
- **Dynamic association** – An Operator binds a subscriber analyzer to a control profile that identifies the external entity to provide the set of services. The system can dynamically obtain the service flow using the specified interface (PCRF or RADIUS/Diameter) based on the subscriber policy.

The workflow specifies whether the bearer setup event should trigger this binding.

The following figure illustrates the various components that make up a workflow.

Figure 9-2 Workflow Components



You can use any of the following methods to configure workflow:

- Build a Workflow – You can build a workflow in a top-down manner, by creating the workflow and configuring the service functions (building blocks) and services the workflow will use.
- Build Out Functions – You can create the service functions and the services and later specify them for use when you build a workflow.

In addition, you can clone an existing workflow, service, or service function by selecting it, giving it a new name or identifier, and modifying necessary parameters.

Functions and services are listed in the following table.

Table 9-1 Functions and Services

Category	Name	Description
Constructs	ACL List	Defines the action to take when and an unknown IP address attempts to access the NE.
	Advice of Charge	Defines the action to take after online quota is exhausted, such as to return a notification message or redirect subsequent HTTP traffic to a configured URL.
	Apn Mapping List	Provides additional granularity to APN mapping. It contains a list of APN values to be mapped to, based upon user-specific criteria.
	Ca Certification List	Configures a list of TLS CA-Certificates.
	Content Insertion Profile	Defines a Content Insertion Profile that supports: ■ Insertion of local or remote hosted images or videos (such as, advertisements) ■ Insertion of externally hosted content on ad server via URL links ■ Banners located at the top/bottom of the page or centrally located overlays
	Default Policy Cause Code List	Configures the Diameter credit control failover behavior on the Gx/Gy interfaces based on the result code received in the CCA error message.
	DHCP Local Server Profile	Defines DHCP local server profile.
	DHCP Service Profile	Enables DHCP-enabled UE IP allocation.
	Diffserv Profile Class Mapping	Defines parameters for priority queuing.
	Diffserv Profile DSCP Mapping	Configures the mapping of DSCP codes to queue priorities
	EDR Server Profile	Configures the EDR (Event Data Record) server Profile (maximum 8) to generate EDRs
	Encryption Profile	Defines an Encryption Profile.

Table 9-1 Functions and Services

Category	Name	Description
(Continued)	File Download Profile	Defines parameters for importing lists from a file server.
	Filter Hash List	Defines a hashed database containing URLs to be blocked
	Host List	Serves as a whitelist used by the Fraud Detection Profile. It contains the IP addresses that represent legitimate proxies.
	HTTP Header Enrichment	Defines the HTTP headers/cookies that an HTTP Policy adds, removes, or replaces in the HTTP request or response header.
	HTTP Rule Group	Defines a set of rules for matching header attributes in HTTP request and response headers.
	HTTP URL Rewrite	Defines a set of rewrite-rules used in HTTP Policy for URL substitution.
	IMSI Range	Defines an IMSI range used to generate SGW CDRs based on a list of configured IMSI ranges
	IMSI Range List	Defines an list of IMSI ranges used to generate SGW CDRs based on the configured IMSI ranges
	Insertion Object List	Defines an Insertion Object List
	IP List	Defines an IP Address List
	LDAP Feature Group	Configures an LDAP Feature Group
	LDAP Profile	Configures an LDAP Profile
	LDAP Server	Configures an LDAP Server
	Loopback IP List	Configures a Loopback IP List
	Multimedia Messaging Service Blacklist	Configures a Multimedia Messaging Service destination address blacklist
	Multimedia Messaging Service Center Error Responses	Configures error response status and text in case of rejected Multimedia Messaging requests.
	Multimedia Messaging Service MM3 Profile	Configures a Multimedia Messaging Service MM3 Profile
	Multimedia Messaging Service Center	Configures a Multimedia Messaging Service Center
	Multimedia Messaging Service Center Group	Configures a group of Multimedia Messaging Service Centers
	Multimedia Messaging Service STI Profile	Configures a Multimedia Messaging Service Standard Transcoder Interface Profile

Table 9-1 Functions and Services

Category	Name	Description
(Continued)	Packet Filter	Defines a 5-tuple or Service Data Flow filter.
	Protocol Application Rule Group	Defines layer 7 applications, protocols, and subprotocols for Signature Analysis by detecting deterministic and/or heuristic patterns in bidirectional packet flow. Signature Analysis is the key technology that enables Workflow to control application of advanced services on subscriber traffic (such as charging, per-application filtering, QoS, and so on).
	QoS	Configures default and network Quality of Service characteristics associated with subscribers.
	Realm List	Configures the Realm/Username@realm list.
	Service Rule	Combination of a packet filter, HTTP (Deep Packet Inspection), and/or Time of Day rule.
	Session Rule Group	Configures a list of rule groups that can be configured for RAT type, MBR matching, or both.
	Short Message Service Center Profile	Configures a Short Message Service Center Profile
	Short Message Service Center Group	Configures a group of SMSCs
	Short Message Service Notification	Configures SMS notification text messages
	TCP Optimization Profile	Specifies changes to the TCP/IP stack targeted to improve throughput and user experience in the mobile network
	Time of Day Rule Group	Defines a group of rules used to provide time-of-day filtering
	TLS Rule Group	Defines a set of rules for matching on SNI (Server Name Indication) and Server certificate CN (Common Name) fields of a TLS handshake
	TLS Termination Policy	Configures policies for terminating TLS connections
	UA Profile	Defines a User Agent Profile
	URL List	Defines a WAP IP Flow
Charging	Charging Instance	Binds one or more billing plans.
	Billing Plan	Defines the charging method to be applied to list of Rating Groups.
	Rating Group	Defines the basis for charging service data flows.

Table 9-1 Functions and Services

Category	Name	Description
DNS Proxy	DNS Proxy > DNS IP Flow	Configures a DNS Proxy IP Flow
	DNS Proxy > DNS Policy	Defines DNS Policy
	DNS Proxy > Instance	Configures DNS Proxy Service instance
	DNS Proxy > DNS Proxy Service	Configures a DNS Proxy Service
	DNS Proxy > Static DNS Map	Configures a static DNS map for DNS lookups in HTTP Proxy
Metering Service	Metering Instance	Defines the Metering Service instance to operate in parallel to the charging service to convey the usage counts to the gateway
Multi Protocol Proxy	ABR Optimization Profile	Configures an ABR rate limiting optimization profile
	ACR Encryption Profile	Configures an Anonymous Customer Reference (ACR) encryption profile
	Explicit Proxy Profile	Defines Explicit Proxy Address Profile
	Fraud Detection Profile	Defines Fraud Detection Profile
	Global Multi Protocol Proxy Service	Defines Global Multi Protocol Proxy Service
	HTTP IP Flow	Defines HTTP IP Layer 3 service flow
	HTTPS Profile	Defines profile for handling HTTPS traffic
	HTTP Proxy Instance	Defines HTTP Proxy Service instance
	HTTP Request Policy	Defines HTTP Request Policy
	HTTP Response Policy	Defines HTTP Response Policy
	HTTP Transaction Record Profile	Defines HTTPS Transaction Record Profile
	Steering GW Group	Configures group of steering destinations
	TCP Splicing Policy	Defines TCP Splicing Policy
	TCP Splicing Profile	Defines profile for handling splicing traffic
	Web Image Optimization Profile	Configures an HTTP Web Image Optimization Profile

Table 9-1 Functions and Services

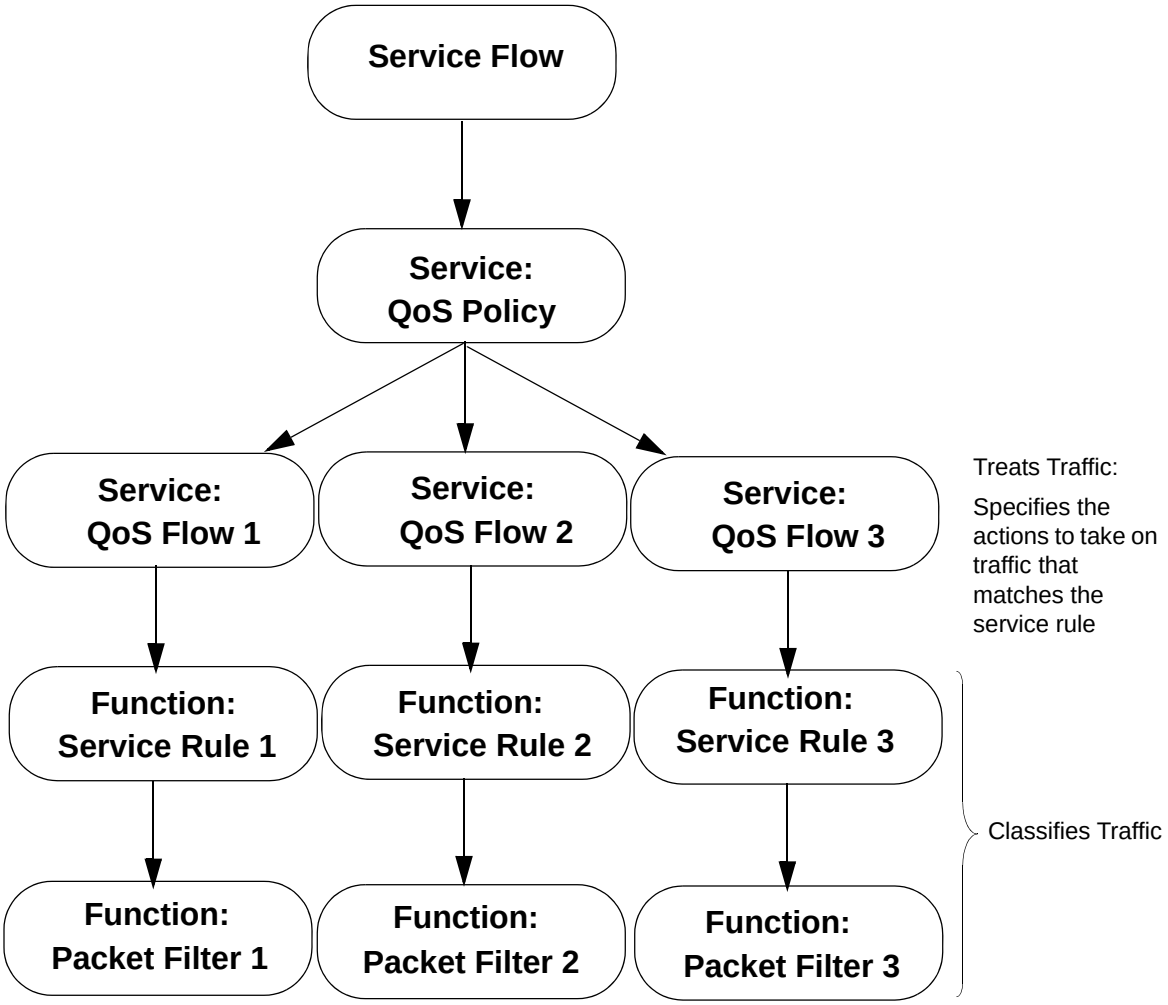
Category	Name	Description
Quality of Service	Fair Bandwidth Usage	Normalizes bandwidth use then monthly subscription levels are breached.
	QoS Flow	Allows for service data flow-level rate enforcement.
	QoS Policy	Defines the QoS to be given to a list of QoS Flows.
Steering	Steering Flow	Configures a Layer 3 steering flow
	Steering Policy	Configures a Layer 3 steering policy
Subscriber Firewall	Subscriber Firewall Flow	Defines Network Address and Port Translation treatment of multiple classified traffic flows.
	Subscriber Firewall Policy	Binds one or more (prioritized) Subscriber Firewall Flows and defines the NAT treatment to be applied when associated with a service flow.

Table 9-1 Functions and Services

Category	Name	Description
Content and Video	Content Cache	Defines the behavior of the web and video cache.
	Content Filter	Defines the filtering capability for a subscriber workflow.
	Content Filter Blacklist File	Configures a Black List used by a global content filter to deny content requests to a specific list of domains or URLs.
	Content HTTP Server Instance	Configures an HTTP Server Instance
	Global Content Cache Service	Configures the behavior of the web and video cache on the system.
	Global Content Filter Service	Configures a global content filter service
	Global Video Adaptation Service	Configures a global video adaptation service
	HTTP Server Entitlement Service	Configures an Entitlement Service mapping
	HTTP Server Policy	Configures an HTTP Server Policy
	Malware Category	Configures a Malware Category
	Offline Serving Policy	Configures offline serving policy
	Offline Transaction Policy	Configures offline transcoding policy
	Oneline Category Group	Configures an Online Category
	Online Transcoding Policy	Configures online transcoding policy
	SMTP Proxy	Configures a Simple Mail Transfer Protocol Proxy instance
	Static Category	Configures a static Category
	Transcoding Map	Configures a list of source > target map entries to be used in the online transcoding policy
	Transcoding Rule	Configures rule to be eligible for transcoding
	Video Adaptation	Configures video adaptation services.
	WAP Gateway	Configures a Wireless Application Protocol Gateway Service Instance

The following figure illustrates the building blocks of a sample service flow, in which traffic is classified and treated according to the components.

Figure 9-3 Sample Service Flow



For a configured workflow, you can use the following workflow tools:

- Validating Workflow – Use the workflow validation report to identify potential configuration issues, such as a classification match that can never occur because of the priorities of the various workflow objects.
- Workflow Service Evaluation – Use the workflow service evaluation report to identify what services are evoked from a simulated flow from a system.
- Workflow Tracing – Use the workflow trace report to graphs the PDN session for a subscriber.
- Comparing/Synchronizing a Workflow on Separate Devices – Use the Network Provisioning tool to provision workflow across multiple devices.

Service Flow Switching

The system supports switching service flows, whereby any services can be switched to a new service.

For example, in the following scenarios, the system switches the service flow to match the corresponding new plan dynamically without terminating the subscriber:

- When a subscriber's plan quota runs out
- When a subscriber purchases optional plan packages
- When a subscriber upgrades/downgrades a package
- When a policy changes in the network

When service flow switching occurs, the system reclassifies traffic and applies all referenced services supported by the new service flow:

- Some services (such as charging instance and QoS Policy) immediately take effect for the next packet. Existing connections may be mapped to different QoS flows or rating groups, based on the new service flow.
- Other services (such as Multi Protocol Proxy and steering service) take effect only for new transactions. Current transactions continue to use the previous service flow.

When switching to a new charging instance, all referenced rating groups present in both the previous and new service flow are reauthorized for grants from the OCS server. Rating groups present in the previous service flow but not in the new service flow are closed by sending the FINAL reporting reason to the OCS server with current usage information. These rating groups are deleted from the subscriber and the subscriber data traffic is reclassified and assigned to the new rating groups.

Permissions Required for Workflow Access

To use the Affirmed Open Workflow application, you must have Configuration > MCC Configuration > Workflow Provisioning > Write or Admin security group permissions. To manage specific workflow functions and services, you need additional permissions. For example, a user who is assigned the Write role for Content Service and the Read-Only role for Workflow Provisioning can modify Content Service entities in Workflow and can view other entities in Workflow.

For instructions on setting permissions, see Specifying Permissions by Security Group.

Build Out Functions

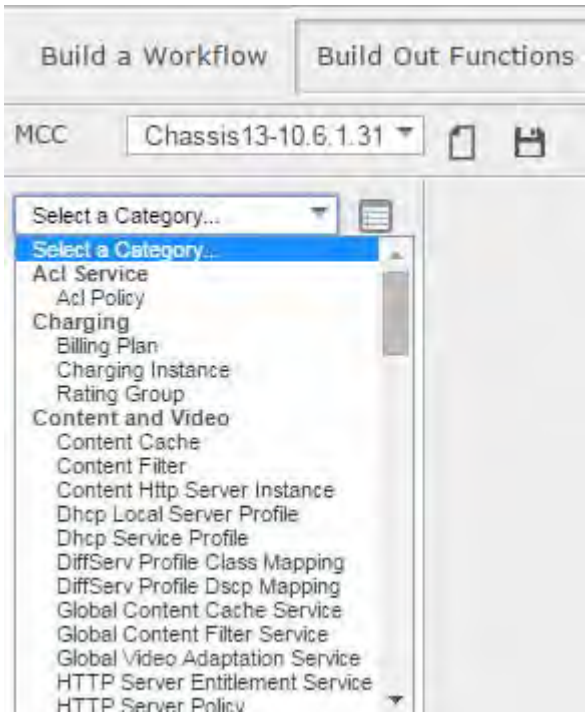
You can create the service functions and the services independent of any workflow. Later, you can specify them for use when you build a workflow.

To build out functions:

1. Right-click an NE and select **Affirmed Open Workflow**.
2. Click the **Build Out Functions** tab.
3. If desired, select a different NE from the dropdown list.

   At the confirmation prompt, click **OK**.
4. Expand **Select a Category** in the left pane.

Figure 9-4 Select a Category



5. Click the name of the service function or service you want to create, inspect, or modify.

   Acuitas restricts display of large numbers of object instances to the first 50 instances. Use the Search box to page through and filter configuration object instances based on instance name to list the object instances you want.

Figure 9-5 Search Box

Use the Search text box to search for object instance(s) by instance name. Enter the string contained in the name and click the **Search** icon. For example, enter SR- to list all object instances with names containing SR-.

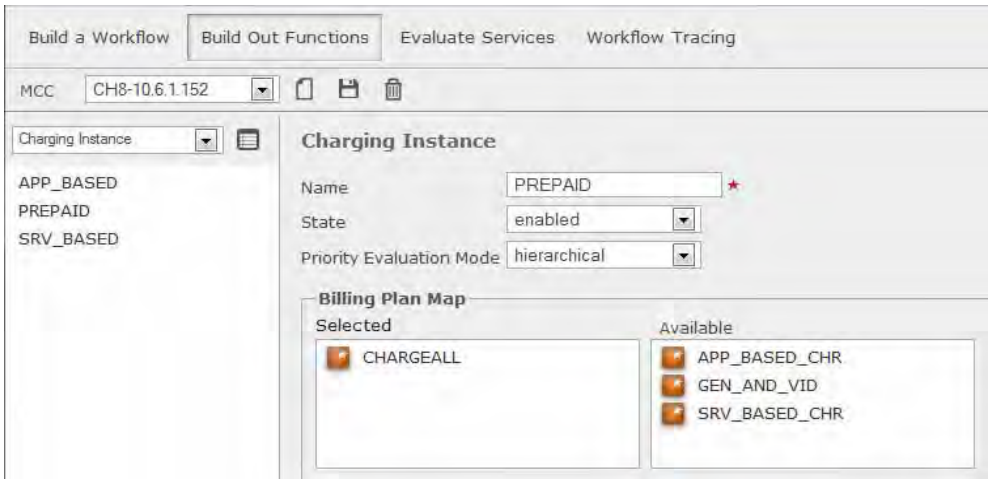
Use the icons to navigate over multiple groups of results:

- Previous Group
- Next Group
- First Group
- Last Group

6 To view an overview of all instances of that type, click the **Overview** icon.

7 To create a new instance, click the **Create** icon.

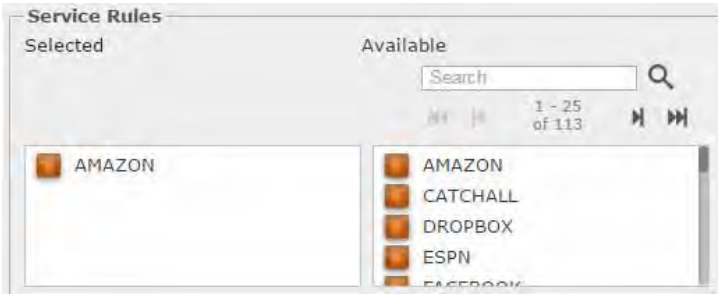
To modify an existing service function or service, click the instance. In the following example, the Charging Instance PREPAID is selected.



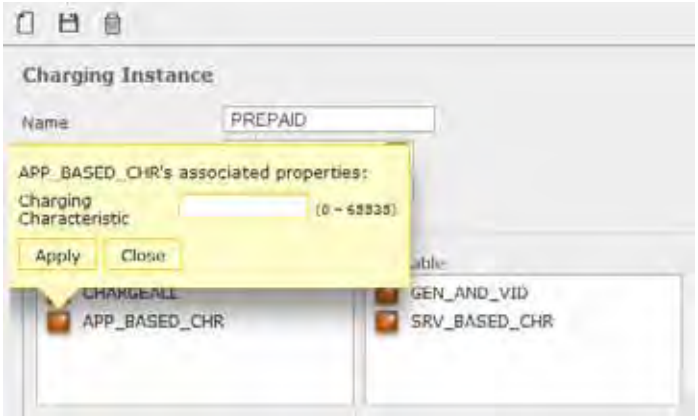
8 Configure the parameters in the configuration window. You can add or remove referenced constructs, such as the Billing Plan map in this example:

- To add an existing referenced construct, drag and drop it from the Available list to the Selected list.

  Acuitas restricts display of large numbers of object instances to the first 25 instances. Use the Search box to page through and filter configuration object instances based on instance name to list the referenced construct you want.



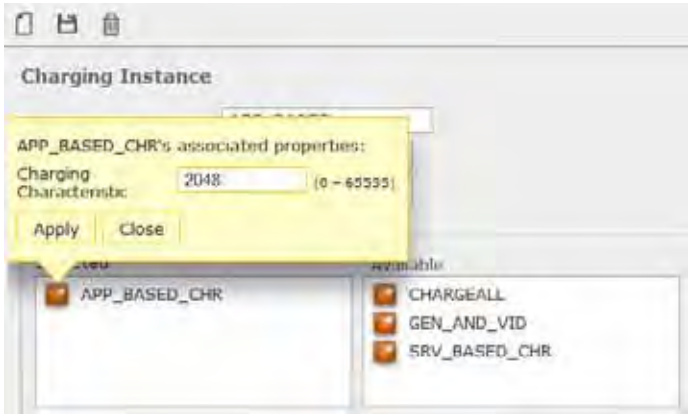
  If the referenced construct has associated data (indicated with a star icon), Acuitas opens a pop-up configuration window.



  Configure the parameters in the pop-up window and click **Apply**.

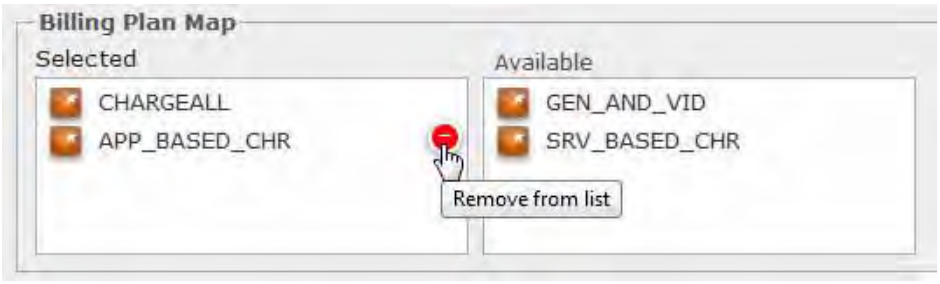
- To view/modify an existing referenced construct that has associated data (indicated with a star icon), click the instance.

  Acuitas opens a pop-up configuration window.



Configure the parameters in the pop-up window and click **Apply**.

- To remove a referenced construct from the list, click the **Remove** icon.



9 Click the **Save** icon.

Once you have created the service functions and the services, you can specify them for use when you build a workflow. For details, see Build a Workflow.

Build a Workflow

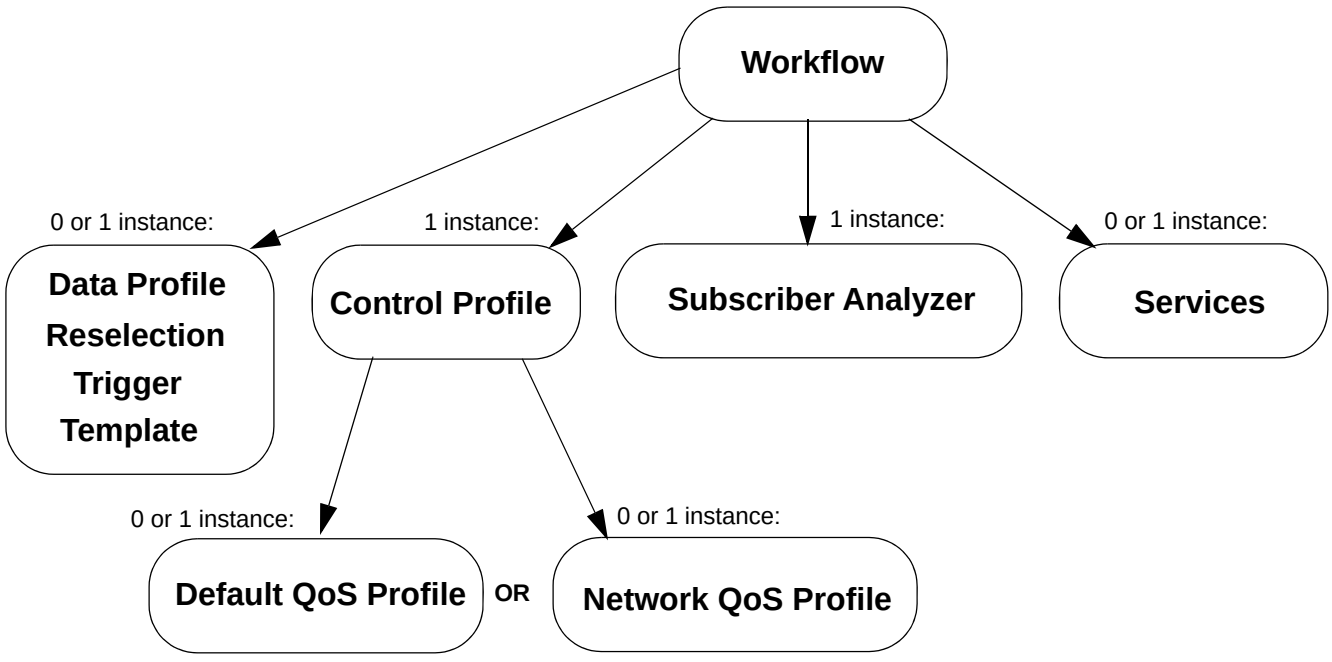
You can build a workflow in a top-down manner, by creating the workflow and configuring the service functions (building blocks) and services the workflow will use. You can specify to use existing service functions and services, or you can create new ones to use.

When you build a workflow, you create or specify to use an existing:

- Subscriber analyzer to define the rules that dictate whether to apply a specific service flow to a subscriber.
- Control profile to specify the back-end interfaces for charging, PCRF, authentication, and accounting to be used for the workflow.
- Data profile reselection trigger template that triggers a data profile switch and associates the template from the control profile. MCC switches the data profile by applying the subscriber analyzer selection based on RAT type. This feature supports switching of a data profile with and without PCRF on RAT change: This feature also supports 3GPP to non-3GPP handover and vice versa.
- Services to provide for the PDN session and controls resource utilization by the session.

The following figure illustrates the components of workflow.

Figure 9-6 Workflow Components



To build a workflow:

1. Right-click an NE and select **Affirmed Open Workflow**.
2. Click the **Build a Workflow** tab.
   - To select an existing workflow, select it from the Workflows list in the right pane.

     You can clone an existing workflow by giving it a new name, and modifying necessary parameters.

   - To create a new workflow, click the **Create** icon.

3. Configure the parameters as follows:
   - **MCC** – If desired, select a different NE from the dropdown list.
   - **Workflow Name** – Enter the Workflow name.
   - **Priority** – Enter the Priority.

Control Profile

The Control Profile specifies the back-end interfaces for charging, PCRF, authentication, and accounting to be used for the workflow.

1. In the **Control Profile** field, specify the Control Profile to use:
   - To select an existing Control Profile, select it from the dropdown list.
   - To view the details of the selected Control Profile, click the **View Control Profile** icon.
   - To create a new Control Profile, click **New Control Profile** in the Control Profiles list in the right pane.

     Configure the parameters in the following table and click the **Save** icon.
   - To modify an existing Control Profile, click it the Control Profiles list in the right pane.

     Configure the parameters in the following table and click the **Save** icon.

Table 9-2 Control Profile Parameters

Parameter	Description
Name	Control Profile name
Default Accounting Interface	Default accounting interface (RADIUS/Diameter)
Default Offline Interface 1	Default Offline Interface 1 (local/diameter)
Default Offline Interface 2	Default Offline Interface 2 (local/diameter)
Default Online Interface	Default Online Interface (local/diameter)
Default Auth Interface	Default Authorization interface.
Default PCRF Interface	Default Policy and Charging and Rules Function interface.
Mapped APN Name	Mapped Access Point Name. Use this parameter to map the generic APN to a specified APN so that external entities like policy and charging servers can provide differentiated treatments. The mapped APN to use. The APN must already exist. Create it at Zone > *name* > Gateway > APN.
Default Home Post Paid Charging Svc	Default postpaid charging service for the home PLMN. This charging instance must already exist. See Charging Instance. ***Note:*** *Dynamic selection of a Charging Instance via a RADIUS interface takes precedence over this Charging Instance.*
Default Roaming Post Paid Charging Svc	Default postpaid charging service for the visited PLMN. This charging instance must already exist. See Charging Instance. ***Note:*** *Dynamic selection of a Charging Instance via a RADIUS interface takes precedence over this Charging Instance.*
Default Roaming Pre Paid Charging Svc	Default prepaid charging service for the visited PLMN. This charging instance must already exist. See Charging Instance. ***Note:*** *Dynamic selection of a Charging Instance via a RADIUS interface takes precedence over this Charging Instance.*
Default Home Pre Paid Charging Svc	Default prepaid charging service for the home PLMN. This charging instance must already exist. See Charging Instance. ***Note:*** *Dynamic selection of a Charging Instance via a RADIUS interface takes precedence over this Charging Instance.*

Table 9-2 Control Profile Parameters

Parameter	Description
Charging Characteristics	Charging characteristic per subscriber. This number could be one provisioned in each user's subscription data, per-APN, or for the entire profile at HSS. It is significant inside the user's home network. It can be used by the Operator to specify data as CDF address, OCS address, interim reporting interval/volume for on-line charging, tariff times, and so on.
OCS Enabled	Online charging enabled per subscriber: ■ true ■ false
UE IP Allocation Mode	UE IP Allocation Mode: ■ Local-ue-ip-allocation – The UE IP assignment is managed locally on the system using local pools. ■ Radius-ue-ip-allocation – The UE IP allocation is managed from an external server (for both Framed IP behavior as well as for pool name based assignment) ■ Dhcp-relay-ue-ip-allocation – The UE IP is assigned/managed using a DHCP relay, with the UE acting as the DHCP client and the system learning the IP that the UE finally selects. The system manages a 'remote' UE pool to keep track of the DHCP assigned UE addresses. ■ Dhcp-client-ue-ip-allocation – The UE IP is assigned by the external DHCP server, however the system acts as a DHCP client and performs the DHCP negotiation on behalf of the UE. ■ Lns-ip-allocation – The UE IP is assigned by LNS (L2TP Network Server) ■ S6-3gpp-aaa-ue-ip-allocation UE IP address allocation is managed as Framed-Pool, Framed-Ipv6-Pool, or Served-Party-Ip-Address allocation
Dhcp Local Server Admin Mode	DHCP local server admin mode (applies when **UE IP Allocation Mode** is set to local-ue-ip-allocation): ■ enabled ■ disabled
Dhcp Local Server Profile	DHCP local server to use (applies when **UE IP Allocation Mode** is set to local-ue-ip-allocation). The DHCP local Server Profile must already exist. See DHCP Local Server Profile.

Table 9-2 Control Profile Parameters

Parameter	Description
Remote IP Alloc Fallback Option	Fallback Option to use if the RADIUS server does not allocate an IP address to a user requesting access (applies when **UE IP Allocation Mode** specifies to use RADIUS). ■ alloc-none ■ alloc-local-pool – Allocates a UE IP address locally from the local UE pool ■ alloc-remote-pool – Allocates a UE IP address locally from the remote UE pool The system rejects the request if the GGSN/PGW allocates an IP address from the remote UE Pool and later the RADIUS server requests to reserve the same IP address.
Dhcp Service Profile	External DHCP server(s) to use (applies when **UE IP Allocation Mode** specifies to use a DHCP Relay Agent, DHCP client, or DHCP proxy).
APN Reporting	APN to use when reporting APN to external devices: ■ original — Initial APN ■ mapped — Final / current APN ■ prior-mapped — APN mapped prior to the mapped (final / current) APN. This setting allows APN Reporting to continue to be based on the previously-mapped APN (even following a remap to a final APN) ■ custom — Customized Access Point Name (APN) reported on external interfaces. The customized APN is used in the Called-Station-ID AVP in messages in the external interfaces
Custom Reporting APN Name	Customized APN sent in Called-Station-ID AVP in the external interfaces. Applies only when **APN Reporting** is set to custom.
Allow Dedicated Bearers	Specifies whether subscribers can have dedicated bearers or secondary PDP contexts: ■ true ■ false
Default Tunnel Configuration	Default Tunnel configuration to use to bypass routing of egress traffic and force upstream packet into a pre-configured GRE tunnel referenced by a tunnel interface. The APN must already exist. Create it at Network Context > *name* > Tunnel.
Ldap Interface Profile	LDAP Interface Profile to use. The LDAP Interface Profile must already exist. See LDAP Profile.
APN Mapping List	List of mappings to APNs. The APN List must already exist. See APN Mapping List.

Table 9-2 Control Profile Parameters

Parameter	Description
APN Mapping Control	Control for mapping APN: ■ none – No APN mapping. ■ explicit – Map to the APN specified by the **Mapped APN Name** field. ■ PAP username exclusive – Map APN using the Password Authentication Protocol (PAP) username and **Apn Mapping List**. ■ PAP username or explicit – Map APN using the Password Authentication Protocol (PAP) username and **Apn Mapping List**, if possible. Default to APN specified by the **Mapped APN Name** field. ■ External – Map APN using value received from external source.
APN Mapping Failure Behavior	GW behavior if APN remapping fails: ■ Use original – Allow the call using the original APN value ■ Reject – Reject the call
Default Advice of Charge	Default Advice of Charge to use. The Advice of Charge must already exist. See Advice of Charge.
Allow Mapped APN Based Sub Analyzer	Allows mapped APN based Subscriber Analyzer to be applied to the subscriber: ■ true: Applies the Subscriber Analyzer rules associated with the APN received in the Called-Station-Id attribute to the subscriber ■ false ***Note:*** *Only one APN redirection is allowed per subscriber.*
v4v6 Hybrid Allocation State	The policy to use for hybrid v4v6 UE IP allocation, where one IP address is managed externally (RADIUS) and the second IP address is managed internally by the MCC (applies when **UE IP Allocation Mode** specifies to use RADIUS): ■ v4v6-hybrid-allocation-disabled – Hybrid UE IP allocation is disabled. In the event that RADIUS returns only one of the IP addresses, the session setup request is rejected. ■ v4v6-hybrid-allocation-local-pool – If RADIUS allocates one of the IP addresses, MCC attempts to allocate the other IP address from one of the local IP sub pools. ■ v4v6-hybrid-allocation-remote-pool – If RADIUS allocates one of the IP addresses, MCC attempts to allocate the other IP address from one of the remote IP sub pools. This configuration applies only in the case where the UE is requesting a v4v6 IP address and RADIUS allocates only a v4 or a v6 IP address. If the RADIUS does not assign any UE IP address, hybrid allocation mode does not apply. Actions are dependent on the **Remote IP Alloc Fallback Option**.

Table 9-2 Control Profile Parameters

Parameter	Description
Duplicate IP Reserve Request Handling	Controls the subscriber session setup during a duplicate IP assignment (for example, when an external server (such as RADIUS) assigns a UE IP to a subscriber that is already assigned to a different subscriber). Applies when **UE IP Allocation Mode** *is not* set to local-ue-ip-allocation. Values: ■ reject-new-session – Reject the new subscriber session setup and keep the old session. ■ delete-existing-session – Close the existing session and accept the new session creation request with the duplicate IP assignment.
Allow Mapped APN Based Sub Analyser	Specifies whether to allow mapped APN-based sub-analyzer to be applied to the subscriber: ■ true – Maps the generic APN to the specified mapped APN and applies the Subscriber Analyzer rules associated with the mapped APN to the subscriber. ■ false – Maps the generic APN to the specified mapped APN so that external entities, such as RADIUS and policy and charging servers can provide differentiated treatments.
Default Port NBR Interface	The default Port NAT binding record interface.
Default Rx Interface	The default Rx interface.
User Subscription Charging Type	User Subscription Charging Type: ■ no-subscription: No Subscription Type. MCC sends online and offline AVP as enabled ■ postpaid-subscription: Postpaid User Type. MCC sends online AVP disabled and offline AVP as enabled ■ prepaid-subscription: Prepaid User Type. MCC sends online AVP enabled and offline AVP as disabled
Initial User Unknown Error Handling	Initial Diameter user unknown error result code handling: ■ reject-session ■ redirect-session
Redirect on Creation	Specifies whether to redirect the session upon creation: ■ true: If a redirect URL is provisioned, session is redirected to the URL immediately ■ false
MVNO Profile	The Mobile Virtual Network Operator profile for sessions associated with an MVNO and using this Control Profile. The MVNO Profile must already exist. Create it at Zone > *name* > Gateway > Profile > MVNO Profile.
Default S6b Interface	The default S6b interface to use.

Table 9-2 Control Profile Parameters

Parameter	Description
EDR Interface	The Event Data Record Interface Profile to use.
Flow Authorization Interface	Specifies the flow authorization interface to use.
Allocate Delegated Prefix from Local Pool	Allocate the delegated IPv6 prefix from the local IP subpools: ■ enabled ■ disabled
Update Prior Mapped Apn	Specifies whether to update the prior mapped APN when APN mapping is performed: ■ false – If APN mapping is configured on this control profile, the APN mapped prior to the current APN is not populated in the prior mapped APN. ■ true – (default) If APN mapping is configured on this control profile, the APN mapped prior to the current APN is populated in the prior mapped APN.
Data Profile Reselection Trigger Template	Select the Data Profile Reselection Template to use. The Data Profile Reselection Trigger Template must already exist. See Data Profile Reselection Trigger Template.
Profile Type	The QoS Profile to use to provide AMBR and burst sizes for the default bearer: ■ Network QoS Profile: the AMBR unconditionally overrides the user equipment's AMBR request. ■ Default QoS Profile: The AMBR is used only if the user equipment does not request a particular bandwidth (AMBR request is 0).
Field when Profile Type is set to Default QoS Profile	
Default QoS Profile	The default QoS Profile to use if the user equipment does not request a particular bandwidth. The QoS Profile must already exist. See QoS.
Field when Profile Type is set to Network QoS Profile	
Network QoS Profile	The QoS Profile to use to replace any bandwidth request. The QoS Profile must already exist. See QoS.

2 In **Mirrored Accounting Interface List**, select the accounting interface on which the mirrored accounting messages are to be sent. Drag and drop it from the Available list to the Selected list

Only accounting interfaces designated with an interface type of mirrored can be selected. This parameter is only available when a primary accounting interface is configured.

3 In **Delegated Prefix List**, specify the prefix length of the delegated IPv6 prefix to be assigned from local IP subpools:

- **prefixlength**
- **priority** - priority to choose the Delegated IPv6 Prefix to be assigned from local IP subpools.

Data Profile Reselection Trigger Template

The data profile reselection trigger template triggers a data profile switch and associates the template from the control profile. MCC switches the data profile by applying the subscriber analyzer selection based on RAT type. This feature supports switching of data profile with and without PCRF on RAT change: This feature also supports 3GPP to non-3GPP handover and vice versa.

1 In the **Data Profile Reselction Trigger Template** area, configure the parameters as follows:

Table 9-3 Data Profile Reselection Trigger Template Parameters

Parameter	Description
Name	Enter a Control Profile Reselection Trigger Template name.
RAT Change	Specifies whether to enable reselection of a data profile on RAT change: ■ enabled ■ disabled

Subscriber Analyzer

In the **Subscriber Analyzers** area, define the rules that dictate whether to apply a specific set of services to a subscriber:

1 Click the **Modify** icon.

2 Configure the parameters as follows:

- **Event** – Specify whether to associate the workflow with Bearer Setup.
- **Groups** – You can configure multiple groups, each identified by name. If any group matches, the subscriber analyzer is selected. A group can specify multiple triggers, all of which must match for a group to match. If no groups are configured or the groups have no attributes, the subscriber analyzer is ignored and is not part of the selection process during session setup.

  To add a group, click the **Add Group** icon.

  Enter the **Group Name** and click **Add**.

  Drag trigger(s) from the Available Triggers list to the Selected Triggers list, and specify the trigger value, as indicated in the following table.

Table 9-4 Subscriber Analyzer Triggers

Parameter	Description
Name	Key set name
APN Name	Select the Access Point Name.
GTP Proxy Name	Select the GTP Proxy service name.
PGW Name	Select the Packet Data Network Gateway.
PGW IP	Select the Packet Data Network Gateway IP Address.
GGSN Name	Select the Gateway GPRS Support Node.
MCC Name	Select the MCC Gi Gateway.
UE IP Address	Enter User Equipment IP Address.
RAT Type	Select the Radio Access Type: ■ UTRAN ■ GERAN ■ WLAN ■ GAN ■ HSPA Evolution ■ EUTRAN ■ NBIOT EUTRAN
Home PLMNID	Enter the Subscriber's Home PLMNID, 5 or 6 digits.
Serving NW PLMNID	Enter the Serving Network's PLMN ID, 5 or 6 digits.
Serving NW MCC	Enter the Serving Network's Mobile Country Code
Charging Characteristics	Enter the Charging Characteristics information
MVNO Identifier	Enter the MVNO name or Identifier
MVNO Sub Identifier	Enter the MVNO sub name or sub Identifier
Roaming User	Specify whether the user is a roaming user: ■ true ■ false
Credit Control Group	Enter the Credit Control group value.
Gigw Unknown Subscriber Profile	Specify whether the subscriber analyzer is intended for SA-GIGW unknown subscribers: ■ true ■ false

Table 9-4 Subscriber Analyzer Triggers

Parameter	Description
WAG Name	Select the Wireless Access Gateway. The Wireless Access Gateway must already exist. Create it at Zone > *name* > Gateway > WAG.
ePDG Name	Select the ePDG. The ePDG must already exist. Create it at Zone > *name* > Gateway > ePDG.
User Name Prefix	Prefix of the username to match
Realm Name	Domain name portion of the username
IMEI Range	Enter the International Mobile Equipment Identity range.
IMSI Range	Enter the International Mobile Subscriber Identity range.
Cell Global ID	Enter the following values: ■ Cell Global ID PLMNID, 5 or 6 digits. ■ Tracking Area Code
Service Area ID	Enter the following values: ■ Service Area ID PLMN ID, 5 or 6 digits. ■ Location Area Code ■ Service Area Code
Routing Area ID	Enter the following values: ■ Routing Area ID PLMNID, 5 or 6 digits. ■ Location Area Code ■ Routing Area Code
Tracking Area ID	Enter the following values: ■ Tracking Area ID PLMN ID, 5 or 6 digits. ■ Tracking Area Code
E-Utran Cell Global ID	Enter the following values: ■ E-Utran Cell Global ID PLMNID, 5 or 6 digits. ■ E-Utran Cell Identifier

3 Click **Done**. The changes are not saved until you save the workflow.

Service Flow

Service flow is the collection of services and functions to provide for the PDN session.

1. Mark the **Static Service** checkbox to statically bind a service flow to the workflow. Unmark the checkbox to dynamically obtain the services that have been programmed on the system.

Creating a New Service Flow

To create a new Service Flow:

1. Expand **Services** in the right pane.
2. Click **New Service Flow** in the Services list in the right pane.

   Acuitas opens a pop-up configuration window.
3. Make changes in the pop-up window. To add a service to the service flow, drag and drop it to the Services box.
4. Click the **Save** icon.

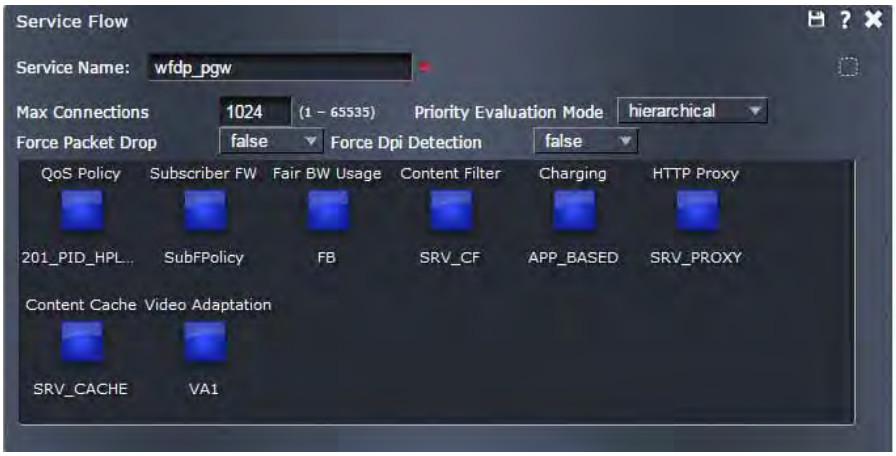
Selecting an Existing Service Flow

To select an existing Service Flow:

1. Expand **Services** in the right pane.

2. To view/modify a service flow, click it in the **Services** pane.

   Acuitas opens a pop-up configuration window.



Make changes in the pop-up window and click the **Save** icon.

To delete a service from the **Services** pane, click the **Delete** icon.

3 To add a service to the service flow, drag and drop it to the Services box.

4 To configure other parameters, click the **Service Flow Settings** icon in the Services box.

Configure the parameters as follows:

Table 9-5 Service Flow Parameters

Parameter	Description
Max Connections	Enter the maximum number of allowed connections.
DPI Pre Detection Max Pkts	DPI pre-detection allows DPI to identify the protocol or application by default. Specifies the maximum number of packets for DPI pre-protocol and application detection.
DPI Pre Detection Max Bytes	DPI pre-detection allows DPI to identify the protocol or application by default. Specifies the maximum number of bytes for DPI pre-protocol and application detection.

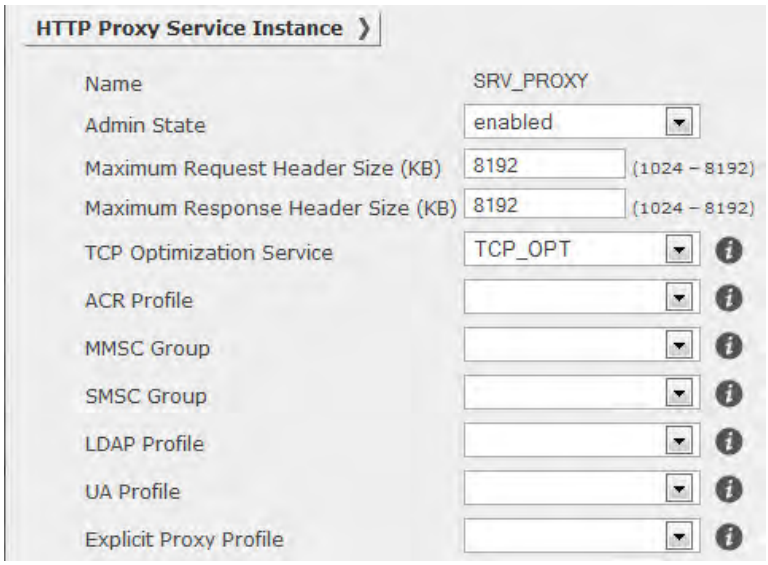
Table 9-5 Service Flow Parameters

Parameter	Description
Force DPI Detection	Specifies whether to force DPI detection to gather DPI-based analytics for all flows: ■ true ■ false
Priority Evaluation Mode	Priority Evaluation Mode when classifying traffic: ■ flat - Use Service Rule priority (ignore Service Flow priority). To make a match, examine all of the Service Rules on all of the Service Flows for best priority. ■ flat-with-pcc-rule-precedence - Any PCC rules in effect have their precedence values compared with the Service Rule priority values, and the PCC rule or Service Rule with the highest priority (lowest numerical value) is selected. ■ hierarchical - Use Service Flow priority and Service Rule priority hierarchically. To make a match, examine the Service Flow in priority order and within each of them, examine the Service Rules in priority order.
Force Packet Drop	Specifies whether to force all the packets to drop both on the access and core side after workflow processing. Set to true when the system is acting as a probe, and you want it to analyze the data and drop the packets: ■ true ■ false
Default CRBN Profile	The default CRBN profile to be used when the PCRF is unreachable and the PGW uses the default Gx policy to set up the session. If the PCRF in unreachable during the session setup and the default Gx policy is enabled, the default CRBN profile is activated for a subscriber. Once the PCRF comes back up and the PGW receives a CCA-I from the PCRF, the default CRBN is deactivated for the subscriber. Applies only when the CRBN Mode is set to CRBN Profile in the PCRF Charging Interface Profile.

5 To modify a service instance, click the instance in the Services box. Acuitas displays the instance in the Carousel below the Services box.

6 Configure the parameters in the Carousel window.

You can view details of the instances in a dropdown list, such as a TCP Optimization Service associated with an HTTP Proxy Service Instance.



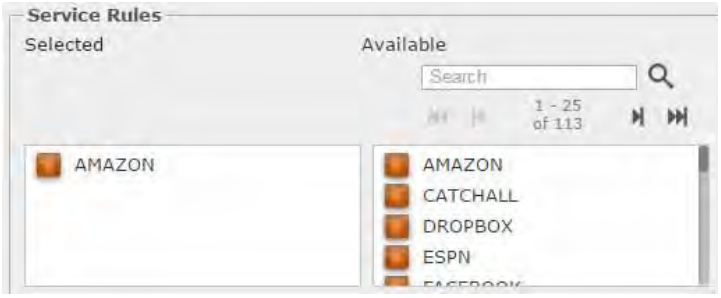
Select the instance from the dropdown list and click the **Inspect Details** icon.

Acuitas opens a pop-up window listing the instance parameters.

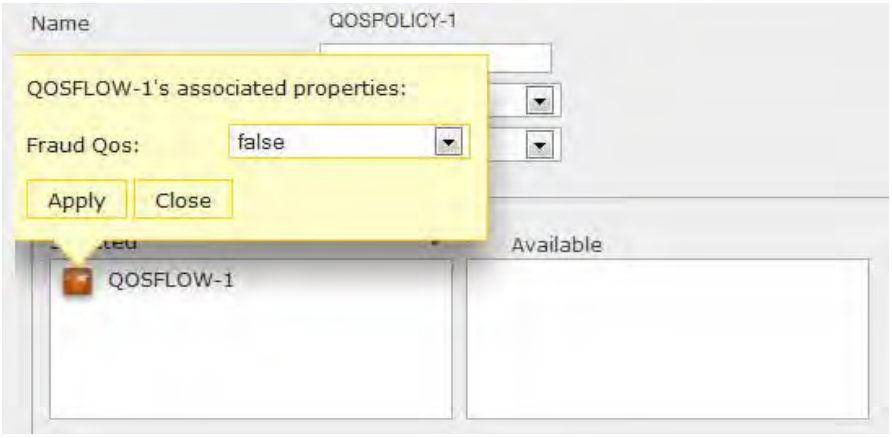
You can add, view, modify, or remove referenced constructs, for example, a QoS Flow referenced in a QoS Policy:

- To add an existing referenced construct, drag and drop it from the Available list to the Selected list.

  Acuitas restricts display of large numbers of object instances to the first 25 instances. Use the Search box to page through and filter configuration object instances based on instance name to list the referenced construct you want.



  If the referenced construct has associated data (indicated with a star icon), Acuitas opens a pop-up configuration window.

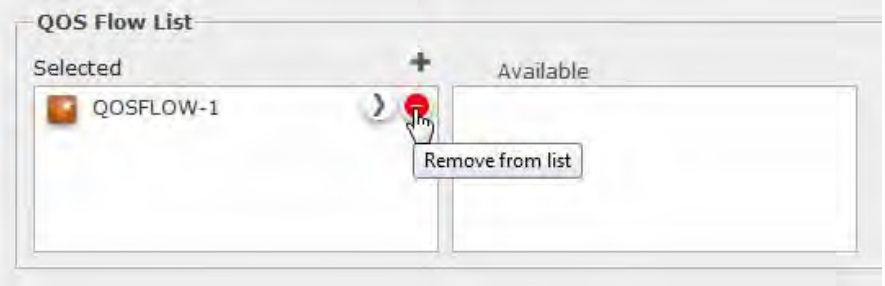


  Configure the parameters in the pop-up window and click **Apply**.

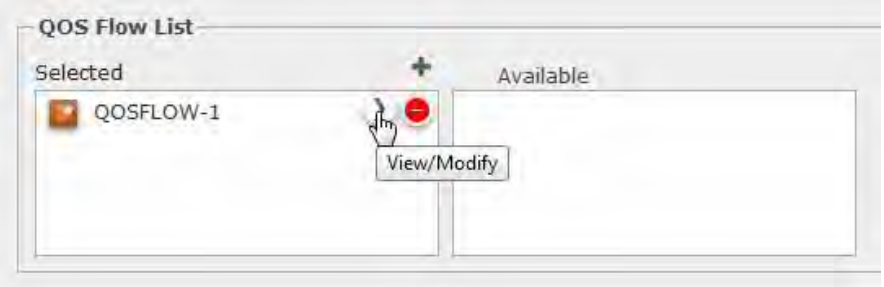
- To create a new instance of a referenced construct, click the **Create New** icon.

  Configure the parameters in the configuration window and click the **Save** icon. .

- To remove a referenced construct from the list, click the **Remove** icon.

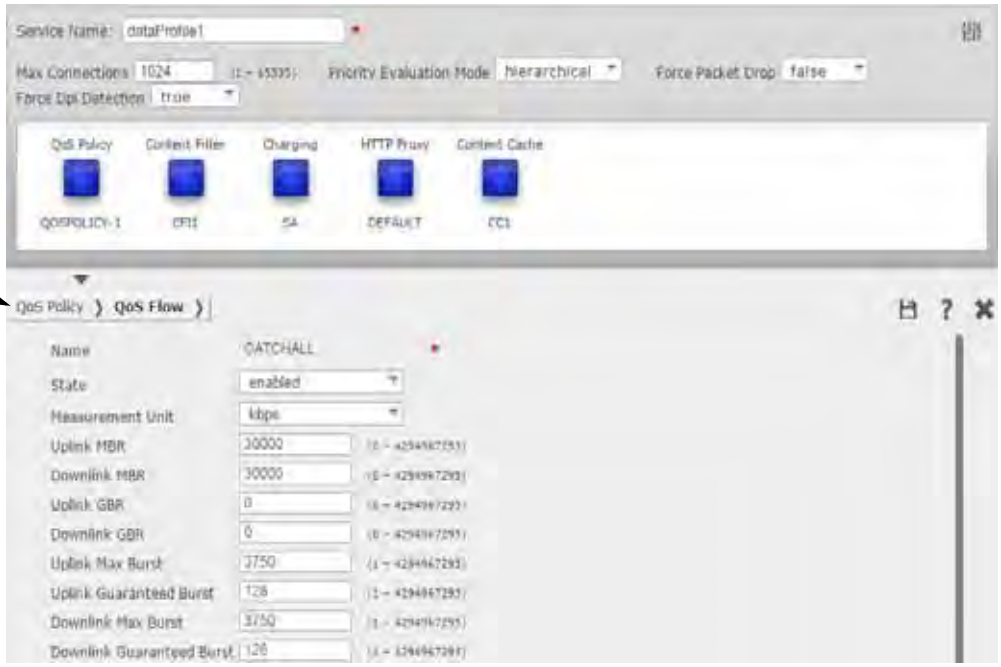


- To view/modify a referenced construct, click the **View/Modify** icon.



The Carousel rotates to display the construct.

To navigate through screens in the Carousel, click the item in the breadcrumbs tab



If you make changes on one screen in the Carousel, and then navigate to another screen, Acuitas highlights the breadcrumbs tab to remind you to save your changes.

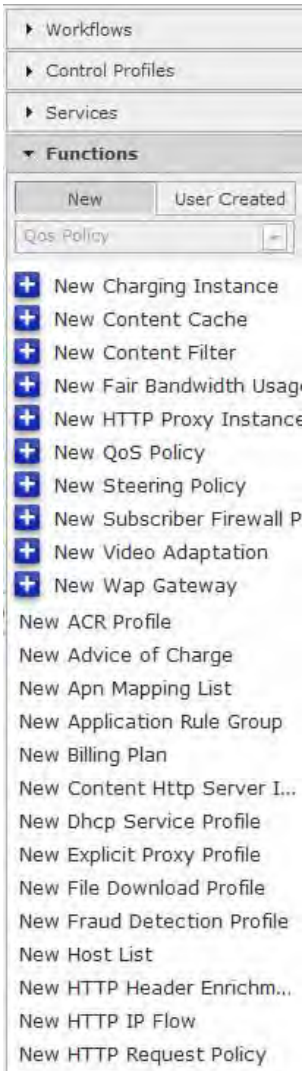
7 To save changes at any screen in the Carousel, click the **Save** icon.

Creating a Service to Add

To create a Service to add:

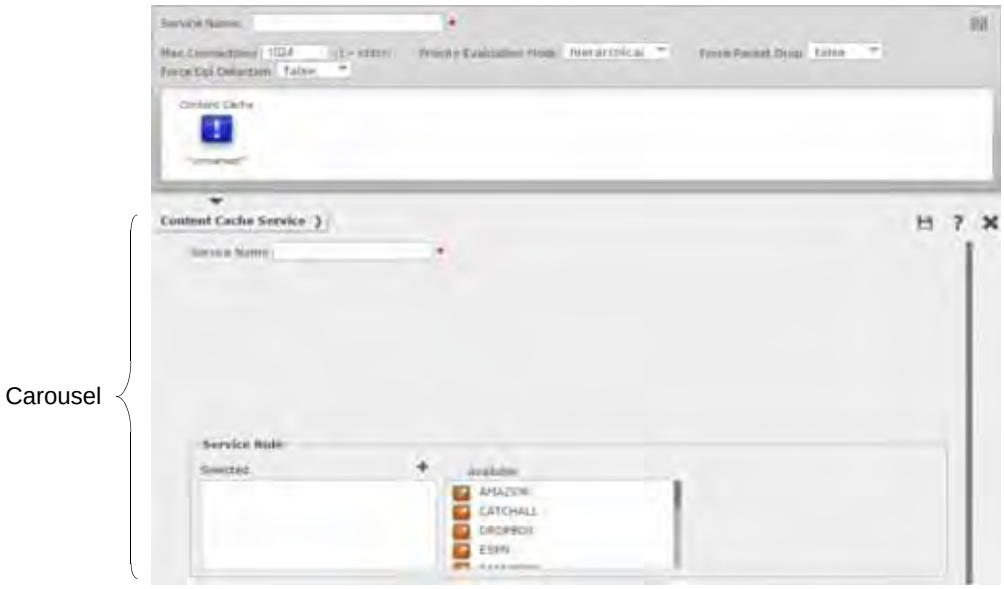
1 To create a service to add, expand **Functions** in the right pane.

2 Click the **New** tab.



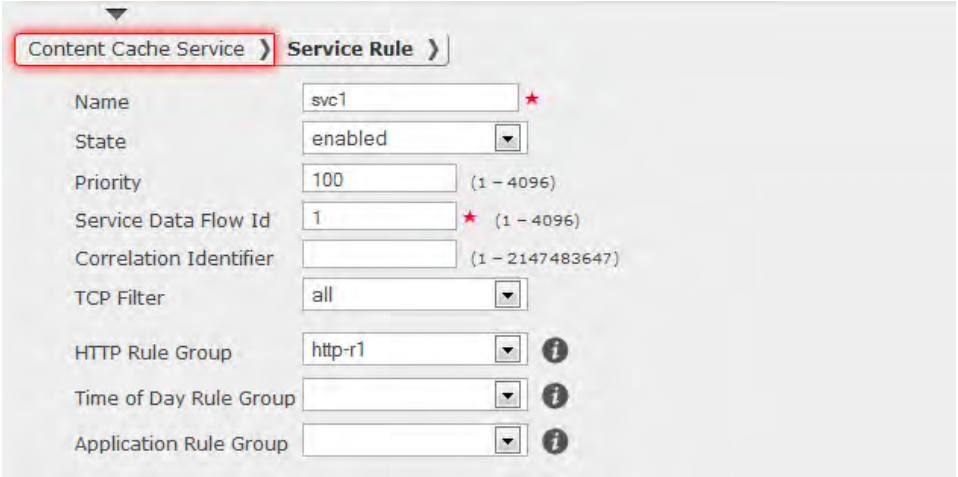
3 To add a new service to the service flow, drag and drop a function's **Plus** icon from the New list to the service flow.

4 To configure the service instance, click the instance in the Services box. Acuitas displays the instance in the Carousel below the Services box.



5 Configure the parameters in the Carousel window.

You can view details of the instances in a dropdown list, such as an HTTP Rule Group associated with a Service Rule.



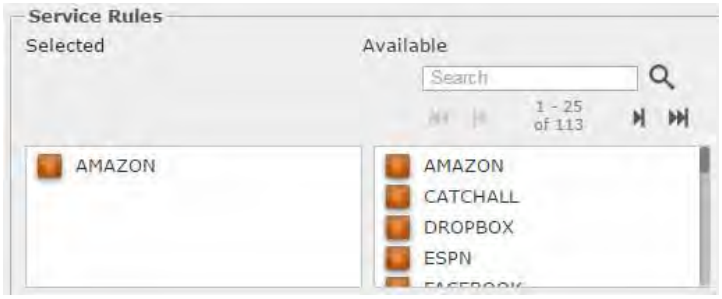
Select the instance from the dropdown list and click the **Inspect Details** icon.

Acuitas opens a pop-up window listing the instance parameters.

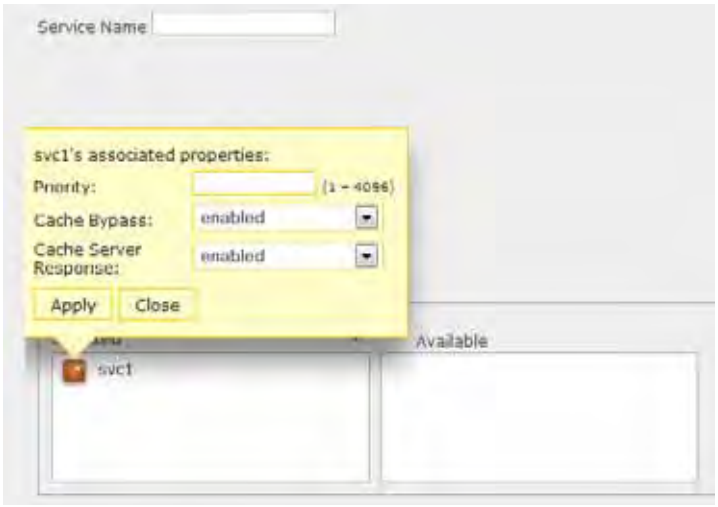
You can add, modify, or remove referenced constructs, for example, a Service Rule referenced in a Content Cache instance:

- To add a referenced construct, drag and drop it from the Available list to the Selected list.

Acuitas restricts display of large numbers of object instances to the first 25 instances. Use the Search box to page through and filter configuration object instances based on instance name to list the referenced construct you want.

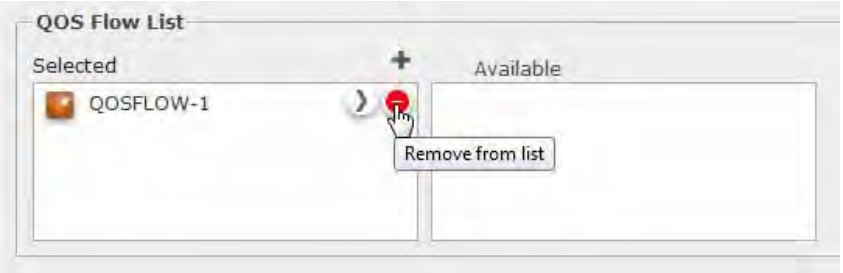


If the referenced construct has associated data (indicated with a star icon), Acuitas opens a pop-up configuration window.



Configure the parameters in the pop-up window and click **Apply**.

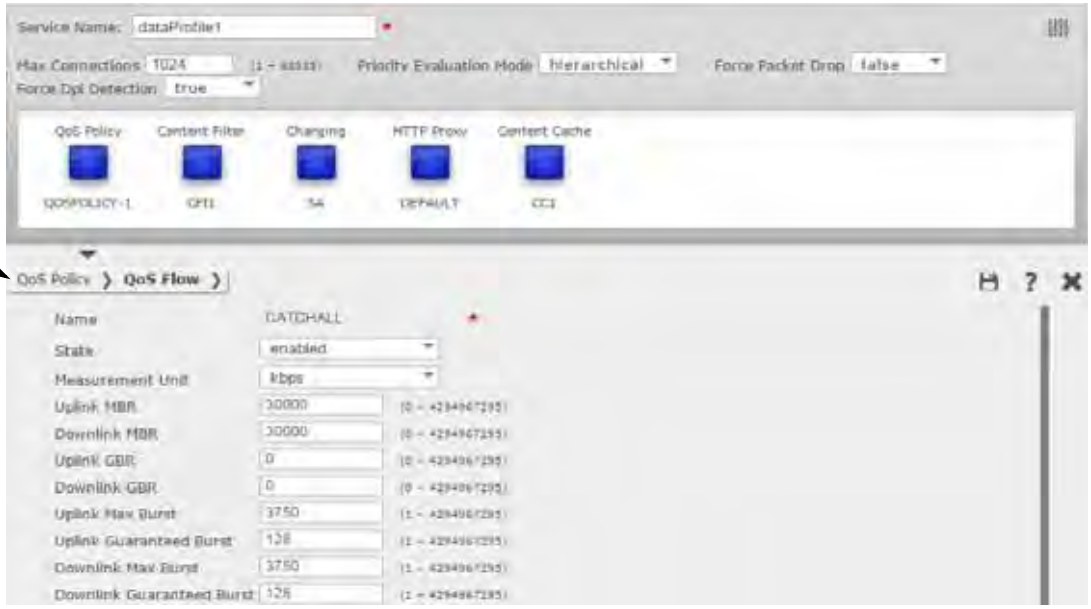
- To create a new instance of a referenced construct, click the **Create New** icon. Configure the parameters in the configuration window and click the **Save** icon. .
- To remove a referenced construct from the list, click the **Remove** icon.



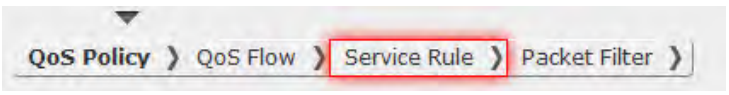
- To view/modify a referenced construct, click the **View/Modify** icon.

The Carousel rotates to display the construct.

To navigate through screens in the Carousel, click the item in the breadcrumbs tab



If you make changes on one screen in the Carousel, and then navigate to another screen, Acuitas highlights the breadcrumbs tab to remind you to save your changes.



6 To save changes at any screen in the Carousel, click the **Save** icon.

7 If you want to create a service but not add it to a service flow, click a function that has a **Plus** icon in the New list.

   a Configure the parameters in the configuration window.

   b Click the **Save** icon.

   The newly added service is added to the **User Created** tab.

8 To configure a function to be used by a service, click the function with no icon in the New list.

   a Configure the parameters in the configuration window.

   b Click the **Save** icon.

   The newly added function is added to the **User Created** tab.

Validating Workflow

Acuitas provides a workflow validation report to identify potential configuration issues, such as a classification match that can never occur because of the priorities of the various workflow objects. The priority of higher-level objects takes precedence over priority of child objects. For example, the priority of a Rating Group takes precedence over the priority of child Service Rules. Classification always occurs based on matches with a higher *effective priority*, which is defined as the priority of the Rating Group, QoS Flow, Subscriber Firewall Flow, or HTTP IP Flow and priority of the child Service Rule. Whenever a lower-level object is used by multiple higher-level objects, effective priority can render some objects unused by the workflow engine.

Workflow validation identifies configuration mismatches by applying the following rules to a given service in a particular workflow:

- The following services should have unique priority values:
  - Rating Group
  - QoS Flow
  - Subscriber Firewall Flow
  - HTTP IP Flow
- A Service Rule can be associated with:
  - Only one higher-level service of a particular type.
  - Multiple higher-level service of different type.

  For example, a Service Rule can be associated with multiple Rating Groups, as long as the Rating Groups *do not* belong to the same Billing Plan.

- When a service has associated Service Rule(s), the Service Rule(s) must have a unique priority values.
- A Packet Filter cannot be shared by multiple simple Service Rules (defined as a Service Rule with Packet Filter(s) but *without* HTTP Rule Group or Protocol Application Rule Group filtering criteria).
- A Packet Filter associated with a Rating Group, QoS Flow, Subscriber Firewall Flow, or HTTP IP Flow (via a simple Service Rule) with one effective priority value cannot contain filter range overlap with those associated with a different effective priority. The overlap applies to all attributes of Packet Filter.

Packet Filter range overlap can be classified as:

- **Total Eclipse** occurs when a lower-priority Packet Filter never takes effect because its filter ranges are narrower than those of a higher-priority Packet Filter.
- **Complete Overlap** occurs when a lower-priority Packet Filter never takes effect because its filter ranges are equal to those of a higher-priority Packet Filter.
- **Partial Overlap** occurs when two Packet Filters share some portion of their filter ranges. The higher-priority Packet Filter takes precedence for matches that fall within the overlapping filter ranges.
- **Catch All** occurs when the filter ranges of a higher-priority Packet Filter are narrower than those of a lower-priority Packet Filter. The lower-priority Packet Filter takes effect (‘catches’) the matches that are outside those of the high-priority Packet Filter.

Note: *The workflow validation report lists overlap warnings only in the case of Time of Day overlap between the Service Rules associated with the Packet Filters. If the Packet Filters have overlapping filter ranges, but are associated with differing Times of Day, the report does not list overlap warnings.*

To run a workflow validation report:

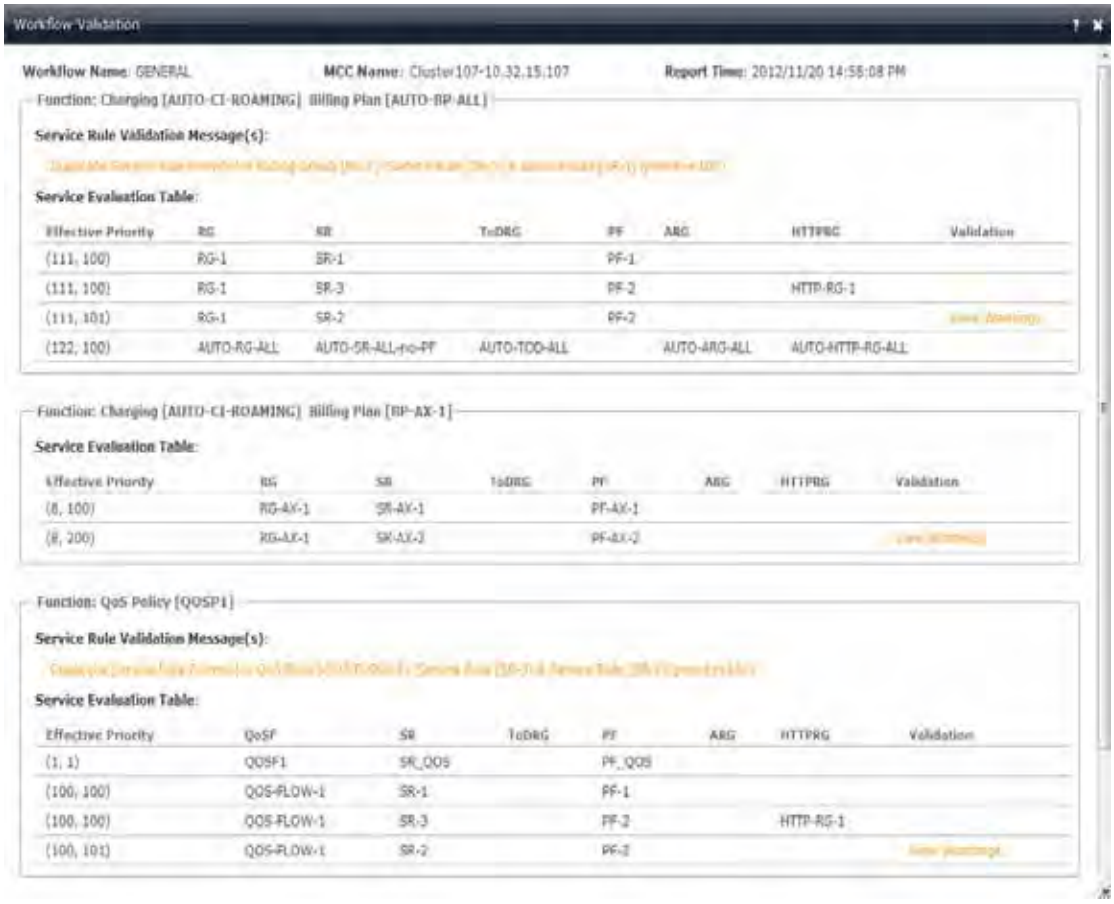
1. Right-click an NE and select **Affirmed Open Workflow**
2. Select the workflow from the workflow list in the right pane.
3. Click the **Validate Workflow** icon.

   Acuitas generates and displays the Workflow Validation Report, listing rule violations and the effective priority of each service.

   The Workflow Validation Report uses the following abbreviations for objects:

   - ARG – Application Rule Group
   - BP – Billing Plan
   - CI – Charging Instance
   - DNSIPF – DNS IP Flow
   - FBWU – Fair Bandwidth Usage
   - HTTPIPF – HTTP IP Flow
   - HTTPP – HTTP Proxy
   - HTTPRG – HTTP Rule Group
   - PF – Packet Filter
   - QoSF – Quality of Service Flow
   - QoSP – Quality of Service Policy
   - RG – Rating Group
   - SFF – Subscriber Firewall Flow
   - SF – Steering Flow
   - SP – Steering Policy
   - SR – Service Rule
   - ToDRG – Time of Day Rule Group
   - TLSRG – TLS Rule Group
   - WAPIPF – WAP Gateway IP Flow

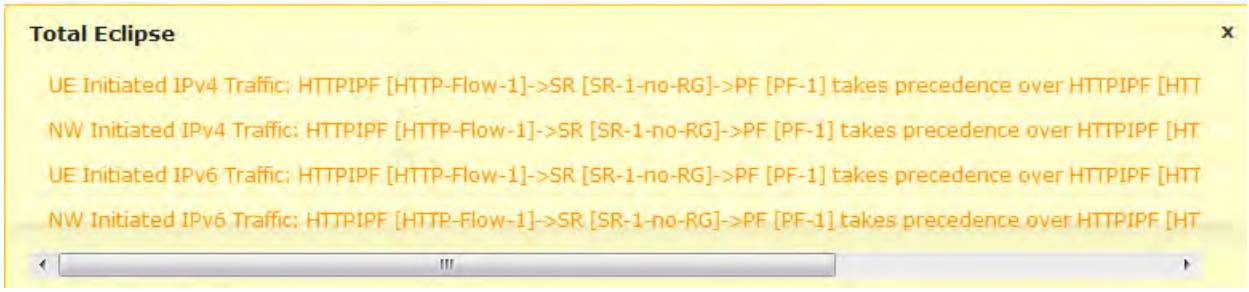
Figure 9-7 Workflow Validation Report



4 To view detailed validation messages, click **View Warnings**.

Acuitas lists the details, such as Packet Filter range overlap.

Figure 9-8 Detailed Validation Messages



Workflow Service Evaluation

Acuitas provides the following workflow service evaluation tools:

- **Workflow Service Evaluation** – Use this tool to identify what services are evoked from a simulated flow by the system workflow engine. A simulated flow specifies the characteristics of a service flow, including Time of Day, Packet Filter, DPI, and HTTP Rule Group parameters. You also specify the Data Profile and its Billing Plan.
- **Workflow Service Comparison** – Use this tool to compare how services are invoked between two simulations:
  - Compare two service flows against a single data profile.
  - Compare a single service flow against two data profiles.

Example Use Case for Service Comparison

You can use the Workflow Service Comparison tool to evaluate a workflow configured for different types of traffic with corresponding charging rates. For example, if you have one charging service that applies a particular charging rate for Skype traffic during peak usage hours and another charging service that applies a different rate during non-peak hours, you can compare how the workflow engine treats each type of traffic.

To do so, you define the following simulated flows:

- **Flow 1:**
  - Time of Day: during peak usage
  - Packet Filter: specific user equipment
  - Application: Sudaphone
  - Protocol/Subprotocol: Skype - video

  And, you specify the data profile and the Billing plan against which to apply the simulated flow.
- **Flow 2:**
  - Time of Day: non-peak usage
  - Packet Filter: specific user equipment
  - Application: Sudaphone
  - Protocol/Subprotocol: Skype - video

  And, you specify the data profile and the Billing plan against which to apply the simulated flow.

The Workflow Service Comparison tool lists what services were matched on the selected flow, so that you can verify that the peak usage Billing plan is evoked.

Workflow Service Evaluation

To run a Workflow Service Evaluation report:

1. Right-click an NE and select **Affirmed Open Workflow**.
2. Select the workflow from the workflow list in the right pane.
3. Click the **Evaluate Services** tab.
4. If desired, select a different NE from the dropdown list.
5. Click **Evaluate**.
6. In the **Flow** field, specify the simulated flow you want to use.

   Or, to create or modify a simulated flow, click the **Modify** icon.

   a. To modify or inspect an existing flow, click the instance in the **Available Flows**.

   b. Configure the parameters as follows:

Table 9-6 Flow Parameters

Parameter	Description
Name	Flow name
Flow State	Flow State: ■ Initial - Flow is initially identified by the 5-tuple (source IP address, source port number, destination IP address, destination port number, and the transport protocol) ■ Established - Flow is established
Time of Day:	
Day	Select the day.
Time	Enter the time (24-hour).
Packet:	
Initiator	Initiator of the connection: ■ UE: User equipment ■ Network
IP Version	IP Version: ■ V4 ■ V6
IP Protocol	IP Protocol values, defined in usr/include/netinet/in.h
UE IP Address	User equipment IPv4/IPv6 address. Set to 0 for all IP addresses.
UE Port	User equipment IPv4/IPv6 port. Set to 0 for all ports.
NW IP Address	Network equipment IPv4/IPv6 address. Set to 0 for all addresses.

Table 9-6 Flow Parameters

Parameter	Description
NW Port	Network equipment port (valid for protocol TCP (6), UDP (17), SCTP (132), only). Set to 0 for all ports.
Fields when Flow State is set to Established:	
DPI:	
Application	Application to detect in DPI
Protocol	Protocol/Subprotocol to detect in DPI
OS and Tether:	
Subscriber OS	Operating system of the user equipment device
Flow OS	Operating system of the individual flow
Flow Tethered	Flow is sourced from a tethered device
HTTP:	
User Agent	String to match against HTTP Request's User-agent header
Host	String to match against HTTP Request's Host header
Referer	String to match against HTTP Request's Referer field
Request URI	String to match against HTTP Request's URI field
Request Method	String to match against HTTP Request's Method field: ■ GET ■ HEAD ■ POST ■ PUT ■ DELETE ■ TRACE ■ OPTIONS
Content Type	String to match against HTTP Request's Content-type header
Response Status Code	Status code to match against HTTP Response's Status line.
Connection Reuse	Whether HTTP persistent connections are used: ■ true ■ false

c Click the **Save** icon.

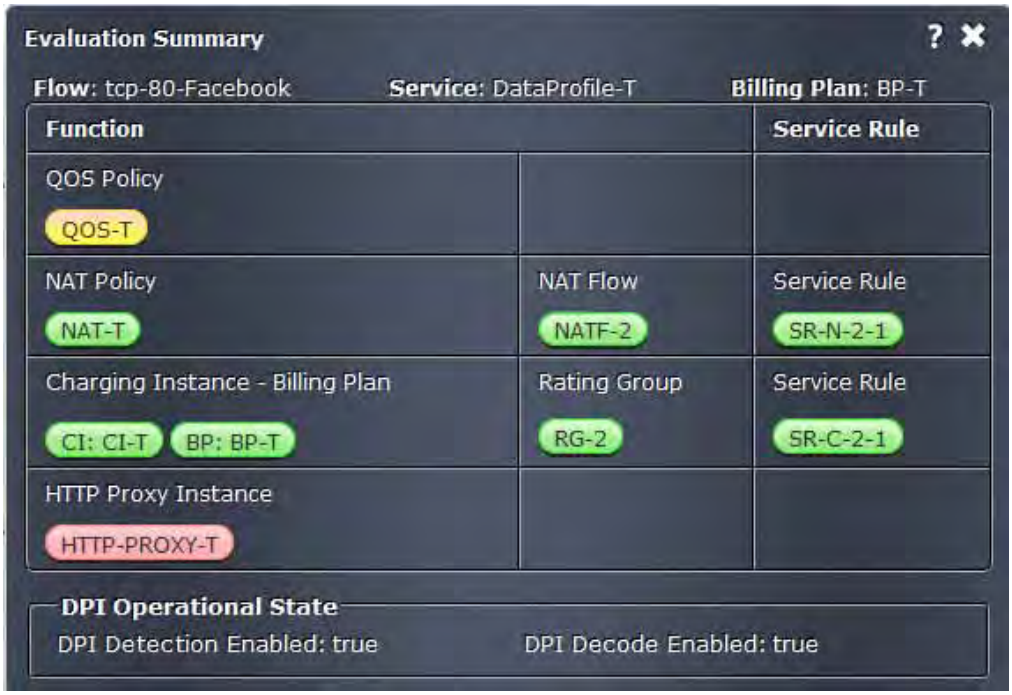
7 In the **Service** field, select the service (data profile) against which to apply the simulated flow.

8 In the **Billing Plan** field, select the Billing Plan against which to apply the simulated flow.

9 Click **Evaluate**.

Acuitas generates and displays the Evaluation Summary, listing what services were matched on the selected flow.

Figure 9-9 Workflow Evaluation Summary



Object instance color indicates whether it resulted in a match:

- Green indicates a Match - the instance was selected
- Yellow indicates Maybe Match - not enough traffic information to make a definitive match
- Red indicates No Match - the instance was not selected
- Grey indicates Not Evaluated - the instance was not evaluated because a match was already made

The Workflow Evaluation Report uses the following abbreviations for objects:

- ARG – Application Rule Group
- BP – Billing Plan
- CI – Charging Instance
- DNSIPF – DNS IP Flow
- FBWU – Fair Bandwidth Usage

- HTTPIPF – HTTP IP Flow
- HTTPP – HTTP Proxy
- HTTPRG – HTTP Rule Group
- PF – Packet Filter
- QoSF – Quality of Service Flow
- QoSP – Quality of Service Policy
- RG – Rating Group
- SFF – Subscriber Firewall Flow
- SF – Steering Flow
- SP – Steering Policy
- SR – Service Rule
- ToDRG – Time of Day Rule Group
- TLSRG – TLS Rule Group
- WAPIPF – WAP Gateway IP Flow

10 Click an object instance to view its configuration settings.

11 To minimize the Evaluation Summary, click the **Close Overlay** icon.

The Evaluation Details screen lists the detailed information of how the workflow engine arrived at the service classification.

Figure 9-10 Workflow Evaluation Details

12 To view an object instance's matching details, click the expansion icon in the Evaluation Details screen. To view all object instances' matching details, click the **Expand/Collapse all rows** icon.

Figure 9-11 Object Instance Details

To view a classifier's details, click the **Show Details** icon.

Acuitas opens a pop-up window listing the details.

Workflow Service Comparison

To run a Workflow Service Comparison report:

1 Right-click an NE and select **Affirmed Open Workflow**.

2 Select the workflow from the workflow list in the right pane.

3 Click the **Evaluate Services** tab.

4 If desired, select a different NE from the dropdown list.

5 Click **Compare**.

6 In the **Flow 1** field, specify the simulated flow you want to use.

To create or modify a simulated flow, click the **Modify** icon.

a To modify or inspect an existing flow, click the instance in the **Available Flows**.

b Configure the parameters as follows:

Table 9-7 Flow Parameters

Parameter	Description
Name	Flow name

Table 9-7 Flow Parameters

Parameter	Description
Flow State	Flow State: ■ Initial - Flow is initially identified by the 5-tuple (source IP address, source port number, destination IP address, destination port number, and the transport protocol) ■ Established - Flow is established
Time of Day:	
Day	Select the day.
Time	Enter the time (24-hour).
Packet:	
Initiator	Initiator of the connection: ■ UE: User equipment ■ Network
IP Version	IP Version: ■ V4 ■ V6
IP Protocol	IP Protocol values, defined in usr/include/netinet/in.h
UE IP Address	User equipment IPv4/IPv6 address. Set to 0 for all IP addresses.
UE Port	User equipment IPv4/IPv6 port. Set to 0 for all ports.
NW IP Address	Network equipment IPv4/IPv6 address. Set to 0 for all addresses.
NW Port	Network equipment port (valid for protocol TCP (6), UDP (17), SCTP (132), only). Set to 0 for all ports.
Fields when Flow State is set to Established:	
DPI:	
Application	Application to detect in DPI
Protocol	Protocol/Subprotocol to detect in DPI
OS and Tether:	
Subscriber OS	Operating system of the user equipment device
Flow OS	Operating system of the individual flow
Flow Tethered	Flow is sourced from a tethered device
HTTP:	
User Agent	String to match against HTTP Request's User-agent header

Table 9-7 Flow Parameters

Parameter	Description
Host	String to match against HTTP Request's Host header
Referer	String to match against HTTP Request's Referer field
Request URI	String to match against HTTP Request's URI field
Request Method	String to match against HTTP Request's Method field: ■ GET ■ HEAD ■ POST ■ PUT ■ DELETE ■ TRACE ■ OPTIONS
Content Type	String to match against HTTP Request's Content-type header
Response Status Code	Status code to match against HTTP Response's Status line.
Connection Reuse	Connection Reuse: ■ true ■ false

c Click the **Save** icon.

7 In the **Flow 2** field, specify the simulated flow you want to use. To compare a single service flow against two data profiles, select the same simulated flow as **Flow 1**. To compare two service flows against a single data profile, specify a different simulated flow.

To create or modify a simulated flow, click the **Modify** icon.

a To modify or inspect an existing flow, click the instance in the **Available Flows**.

b Configure the parameters (see Table 9-7).

c Click the **Save** icon.

8 In the **Service** field, select the service (data profile) against which to apply the simulated flow. To compare two service flows against a single data profile, select the same data profile as **Flow 1**. To compare a single service flow against two data profiles, specify a different data profile.

9 In the **Billing Plan** field, select the Billing Plan against which to apply the simulated flow.

10 Click **Compare**.

Acuitas generates and displays the Comparison Summary, listing what services were matched on the selected flow(s) and listing the differences between the flows.

Object instances that are identical in each flow are labeled with the **Same** icon.

Object instances that are different in each flow are labeled with the **Different** icon.

Figure 9-12 Workflow Comparison Summary

Object instance color indicates whether it resulted in a match:

- Green indicates a Match - the instance was selected
- Yellow indicates Maybe Match - not enough traffic information to make a definitive match
- Red indicates No Match - the instance was not selected
- Grey indicates Not Evaluated - the instance was not evaluated because a match was already made

The Workflow Comparison Report uses the following abbreviations for objects:

- ARG – Application Rule Group
- BP – Billing Plan
- CI – Charging Instance
- DNSIPF – DNS IP Flow

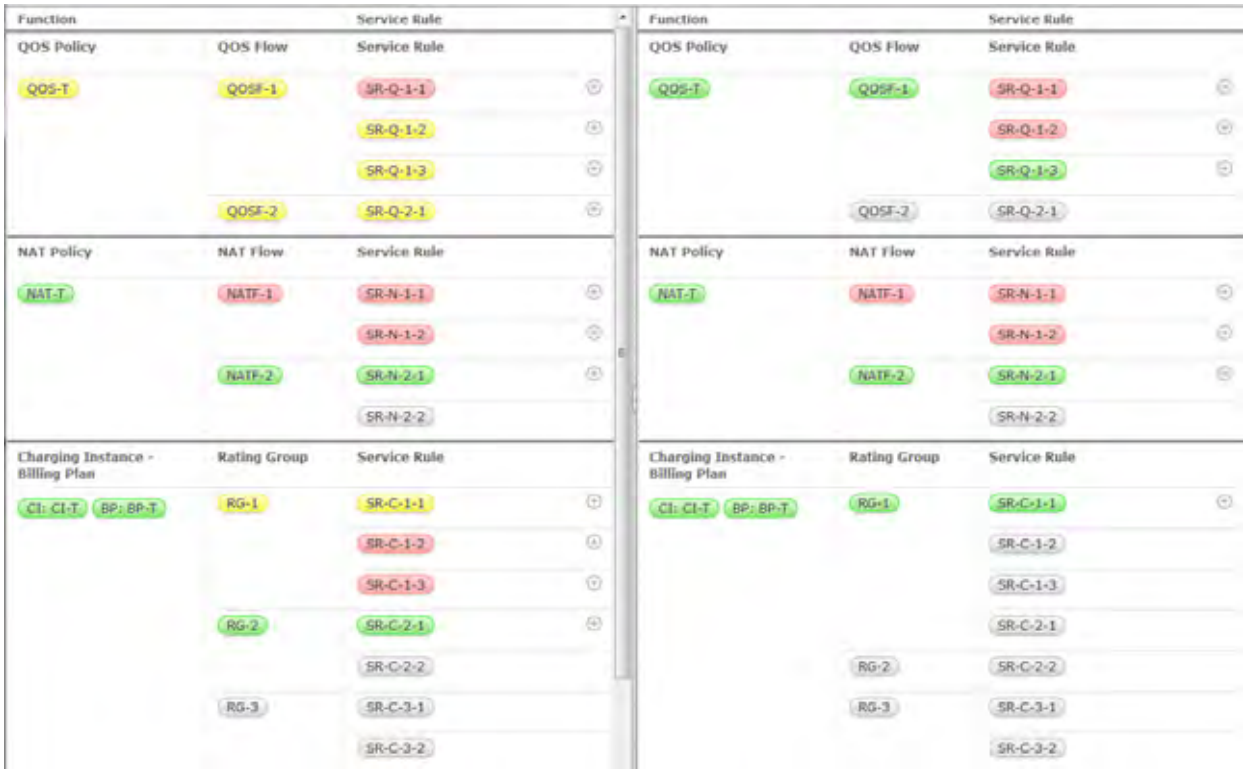
- FBWU – Fair Bandwidth Usage
- HTTPIPF – HTTP IP Flow
- HTTPP – HTTP Proxy
- HTTPRG – HTTP Rule Group
- PF – Packet Filter
- QoSF – Quality of Service Flow
- QoSP – Quality of Service Policy
- RG – Rating Group
- SFF – Subscriber Firewall Flow
- SF – Steering Flow
- SP – Steering Policy
- SR – Service Rule
- ToDRG – Time of Day Rule Group
- TLSRG – TLS Rule Group
- WAPIPF – WAP Gateway IP Flow

11 Click an object instance to view its configuration settings.

12 To close the Comparison Summary, click the **Close Overlay** icon.

The Comparison Details screen lists the detailed information of how the workflow engine arrived at the service classification.

Figure 9-13 Workflow Comparison Details



13 To view an object instance's matching details, click the expansion icon in the Comparison Details screen. To view all object instances' matching details, click the **Expand/Collapse all rows** icon. ⊕

14 To synchronize scrolling of the right and left scroll bars of the Comparison Details window, select the Synchronize Scrolling icon.

When the icon is not selected, the scroll bars separately control their respective panes.

Figure 9-14 Object Instance Details

To view a classifier's details, click the **Show Details** icon.

Acuitas opens a pop-up window listing the details.

Workflow Tracing

You can run a workflow trace report at the subscriber level.

To run a Workflow Trace report:

1. Right-click an NE and select **Affirmed Open Workflow**.
2. Click the **Workflow Tracing** tab.
3. If desired, select a different NE from the dropdown list.
4. To filter the list of subscribers, click **Filter**.
5. Complete the fields in the **Filter Parameters** screen.

   For example, to limit the list of subscribers based upon IMSI range (inclusive), enter a value in the **Start IMSI** field (14-16 digits) and enter a value in the **End IMSI** field.

   And, if desired, mark a checkbox to filter the results:

   - **Idle Only** to list only idle subscribers
   - **Active Only** to list only active subscribers
   - **Visiting Only** to list only visiting subscribers
   - **Home Only** to list only home subscribers
6. Click **Apply** to filter the list.

   Acuitas filters the list of subscribers.
7. Click an IMSI to trace.

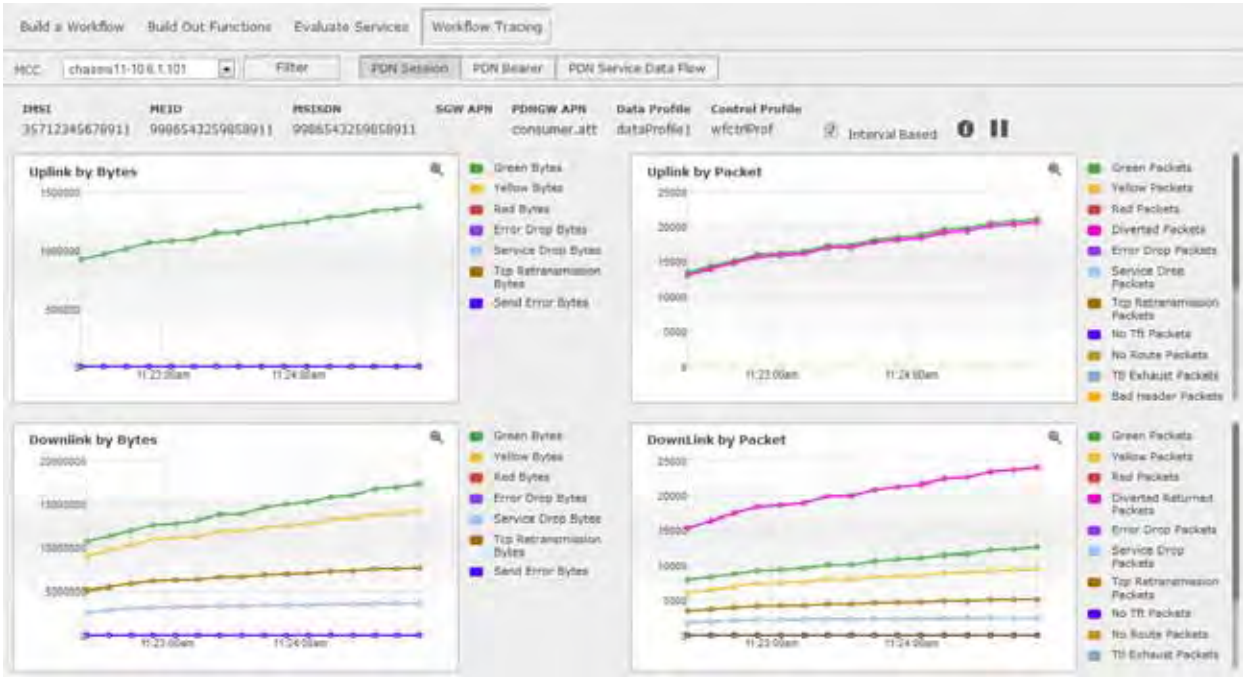
Acuitas graphs the PDN session for that subscriber, showing the uplink and downlink counters. By default, the graphs show cumulative values over time. To view counter differences by interval, mark the **Interval Based** checkbox.

The following table defines the counters:

Table 9-8 Counters

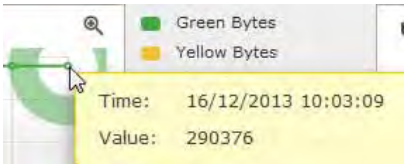
Counter	Description
Green Bytes/Packets	Bytes/Packets that fully conform with QoS Policy
Yellow Bytes/Packets	Bytes/Packets that partially conform with QoS Policy
Red Bytes/Packets	Bytes/Packets that do not conform with QoS Policy
Error Drop Bytes/Packets	Summary counters for Bytes/Packets discarded due to bad headers, bad IP address, or other internal errors
Service Drop Bytes/Packets	Summary counters for Bytes/Packets discarded due to the decision of a workflow service (for example, charging discards due to lack of pre-paid credit)
TCP Retransmission Bytes/Packets	Bytes/Packets detected as TCP retransmissions
Send Error Bytes	Bytes/Packets discarded due to transmit congestion or other internal errors
Diverted Packets	Packets diverted to content services (content cache, content filter, or video adaptation)
Diverted Returned Packets	
No Route Packets	Packets discarded due to no available route
TTL Exhaust Packets	Packets with Time to Live Counter exhausted
Bad Header Packets	Packets with bad headers
Bad IP Addr Packets	Packets with bad IP address
MTU Discard Packets	Packets with DF bit set that exceed MTU
Transmit ICMP Packets	ICMP packets transmitted
Hairpin Policy Discard Packets	
Hairpin Error Discard Packets	
Tunneled Packets	

Figure 9-15 Workflow Trace – PDN Session



8 To view a single data point, point the cursor at a graph.

Acuitas opens a pop-up window that lists the timestamp and data value.



9 To remove a graph from the chart, click the metric in the legend.

The graph is removed at the next polling interval.

10 To pause the chart from updating, click the Pause Update icon.

To resume the chart updating, click the Start Update icon.

11 To increase magnification of a chart, click the Zoom In icon.

To decrease magnification of a chart, click the Zoom Out icon.

12 To view details of the PDN Session, click the **View Details** icon.

Acuitas opens a pop-up window listing the following details:

- General: APN and Gateway information
- Access: Access Control
- Network: Network information
- Bearer: PDN Bearer Information
- Service Data Flow: PDN Service Data Flow Information
- Connections: Active, Total, and Rejected Connection Information
- Workflow Profile: Data Profile and Control Profile Information

Click the **Close** icon to close the window.

13 To show the status and statistics of a PDN bearer, click **PDN Bearer**.

Acuitas graphs the PDN Bearer session for that subscriber, showing uplink and downlink counters. By default, the graphs show cumulative values over time. To view counter differences by interval, mark the **Interval Based** checkbox. Table 9-8 defines the counters.

14 To view details of the PDN Bearer, click the **View Details** icon.

Acuitas opens a pop-up window listing the following details:

- General: Gateway information
- Access: Access Control
- Network: Network Information

Click the **Close** icon to close the window.

15 To show the status and statistics of a one or more PDN service data flows, click **PDN Service Data Flow**.

16 To specify which Service Data Flow(s) to graph, click the **View Details** icon.

Figure 9-16 Service Data Flow List

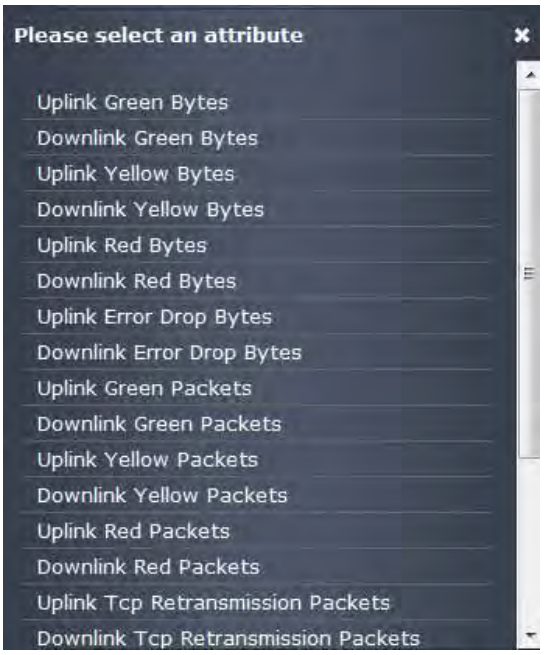
17 Select what Service Data Flow(s) to graph:

- A single Service Data Flow graphs Total Packets and Total Drop Packets
- Multiple Service Data Flows of the same service type graphs your selected uplink or downlink counters against each other

Mark the checkbox(es) and click **View**.

18 If you selected multiple Service Data Flows to graph, select an attribute to graph. The following figure shows the attributes for a charging service.

Figure 9-17 Charging Service Attribute List



Acuitas graphs the PDN service data flow(s) for that subscriber.

When graphing a single Service Data Flow, you can view counter differences by interval. To do so, mark the **Interval Based** checkbox.

Table 9-8 defines the counters.

19 To view details of the PDN service data flow, from the Service Data Flow List, click the **View Details** icon.

Acuitas opens a pop-up window listing the following details:

- Service Type
- Service Flow Name
- Service Rule Name

20 To view further details of the PDN service data flow, click the **Inspect Details** icon.

Acuitas opens a pop-up window listing the additional details.

21 To view further details of an object, click the **Inspect Details** icon.

Acuitas opens a pop-up window listing the additional details.

Click the **Close** icon to close each window.

Comparing/Synchronizing a Workflow on Separate Devices

Acuitas supports the following operations on workflows across two devices:

- **Compare**: Identify the differences between two workflows with the same name on two devices.
- **Synchronize**: Apply a workflow on one device to another device.

Comparing Two Workflows on Separate Devices

When you compare a workflow to another device, Acuitas identifies the differences between the source workflow and the destination workflow of the same name.

To compare two workflows on separate devices:

1. Right-click an NE and select **Affirmed Open Workflow**.
2. Click the **Show Differences/Sync a Workflow** icon.
3. In the **Source Node** list on the left, mark the workflow you want to compare on another device.
4. From the **Destination Node** dropdown, select the device containing the workflow you want to compare.
5. Click **Show Differences**.
6. Click **Cancel** to close the window.

Synchronizing a Workflow to Another Device

To synchronize a provisioned workflow to another device, both devices must be running the same software version.

When you synchronize a workflow to another device, if the destination device already contains a workflow with the same name, the destination workflow is overwritten by the source workflow.

The synchronize operation does not replicate all objects. For example, the operation cannot create Network Context or IP Protocols and all its child objects. If the synchronize operation does not resolve the configuration differences, you must use the Configuration Navigator to manually resolve them.

To synchronize a workflow configuration to another device:

1. Right-click an NE and select **Affirmed Open Workflow**.
2. Click the **Show Differences/Sync a Workflow** icon.
3. In the **Source Node** list on the left, mark the workflow you want to apply to another device.

4 From the **Destination Node** dropdown, select the device where you want to apply the workflow.

5 Click **Sync**.

6 At the confirmation prompt, click **OK**.

Service Functions

Create service functions that are the common building blocks to create service instances.

To configure service functions:

1 Right-click an NE and select **Affirmed Open Workflow**.

2 Use any of the following methods to configure service functions:

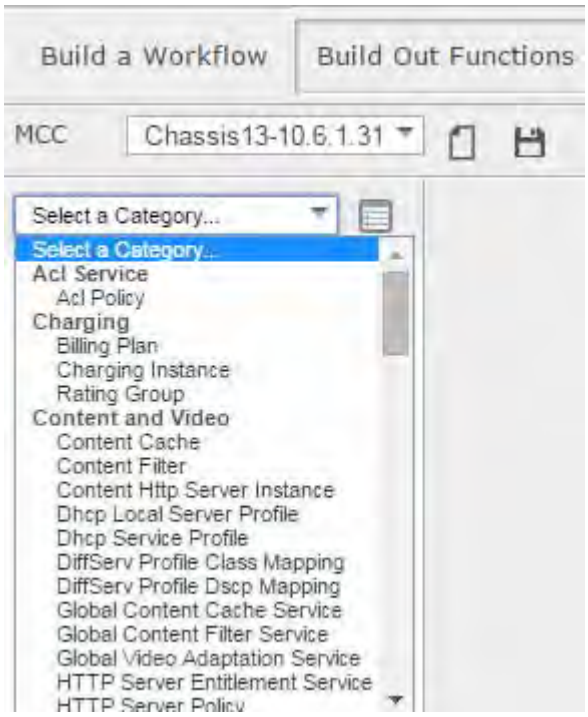
Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click the name of the service function you want to create or modify.

Figure 9-18 Build Out Functions

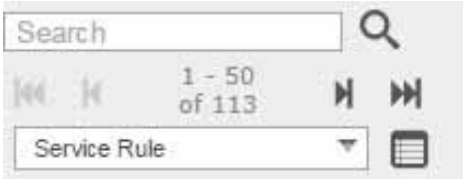


d To create a new instance, click the **Create** icon.

To modify an existing service function or service, click the instance.

Acuitas restricts display of large numbers of object instances to the first 50 instances. Use the Search box to page through and filter configuration object instances based on instance name to list the object instances you want.

Figure 9-19 Search Box



Use the Search text box to search for object instance(s) by instance name. Enter the string contained in the name and click the **Search** icon. For example, enter SR- to list all object instances with names containing SR-.

Use the icons to navigate over multiple groups of results:

– Previous Group

– Next Group

– First Group

– Last Group

Build a Workflow:

a Click the **Build a Workflow** tab.

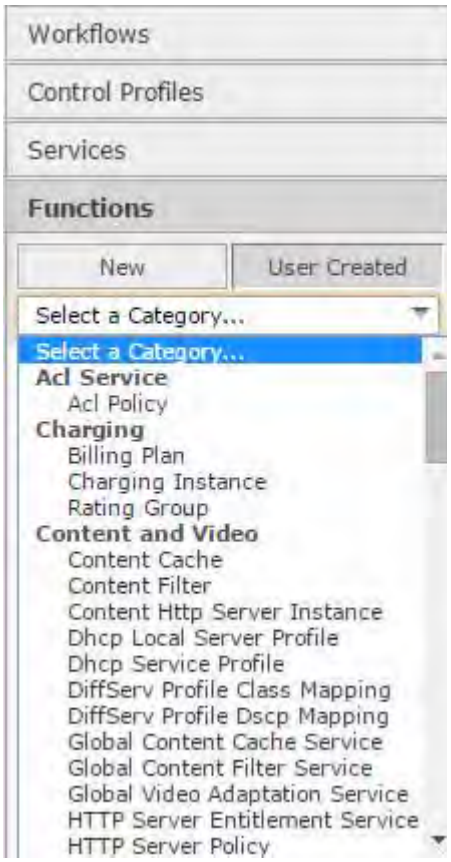
b Expand **Functions** in the right pane.

– To select a function to add, click the **New** tab and click the name of the service function you want to create.

Configure the parameters in the configuration window and click the **Save** icon.

– To select an existing function, click the **User Created** tab.

Figure 9-20 Build a Workflow Functions



Expand **Select a Category** and click the name of the service function you want to modify.

Acuitas restricts display of large numbers of object instances to the first 50 instances. Use the Search box to page through and filter configuration object instances based on instance name to list the object instances you want.

Figure 9-21 Search Box

Use the Search text box to search for particular object instance(s) by instance name. Enter the string contained in the name and click the **Search** icon. For example, enter SR- to list all object instances with names containing SR-.

Use the icons to navigate over multiple groups of results:

– Previous Group

– Next Group

– First Group

– Last Group

Then, click the instance.

Configure the parameters in the configuration window and click the **Save** icon.

ACL List

Operators can apply access control list (ACL) filtering to incoming control traffic to restrict or permit access to MCC interfaces. An ACL contains one or more access control filters. Each access control filter specifies the following:

- The criteria that a packet must match. You define the criteria in a packet filter, which can be based on source and destination IP addresses, source port and destination port, and the networking protocol in use.
- The resulting action, either drop or allow, to take when a match is found.
- A value for prioritizing the access control filter within the ACL, evaluated in sequential order, first to last.

ACL filtering uses an implied *Allow All Traffic* filtering statement, which means if a received packet does not match any defined criteria in the ACL, the packet is allowed. However, you can configure ACL filtering to explicitly deny certain types of traffic by configuring a lowest priority access control filter with a drop action. In this case, you must configure higher priority filters that explicitly permit the types of traffic allowed.

Note: *Affirmed Networks recommends that you configure specific drop/allow filters to ensure accurate traffic filtering.*

ACLs are applied on a network context basis, where access control filters apply to all interfaces within a specified network context. The system supports up to 32 access control filters per ACL.

ACL filtering does not apply to the following types of traffic:

- Routing Protocols, such as BGP, OSPF, BFD
- DNS, SSH, IPv6 ND, DHCP, IKE
- Control Protocols, such as RADIUS, Diameter, GTP', and CALEA, that match explicitly registered IP address/port combinations
- Upstream GTP-U and GRE tunneled WAG traffic

Applying ACL filtering rules may cause unintended results if not used properly. Affirmed Networks recommends contacting the TAC prior to implementation.

To add an ACL List:

1 Use any of the following methods to configure an ACL List:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **ACL List**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New ACL List**.

2 Configure the parameters as follows:

Table 9-9 ACL List Parameters

Parameter	Description
Name	Enter the ACL List name

3 In **ACL Filter**, click the **Create** icon.

4 Configure the following parameters to specify the ACL filter:

Table 9-10 ACL Filter Parameters

Parameter	Description
Name	Enter the ACL filter name
Priority	Enter the ACL filter priority
Action	Action to take for the ACL filter: ■ Allow ■ Drop
Packet Filter	Packet filter to match. This packet filter must already exist. See Packet Filter.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many ACL filters as needed.

7 Click the **Save** icon.

ACL Policy

Operators can apply access control list (ACL) filtering to incoming control traffic to restrict or permit access to MCC interfaces. ACLs are applied on a network context basis, where access control filters apply to all interfaces within a specified network context.

To add an ACL Policy:

1 Use any of the following methods to configure an ACL Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **ACL Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New ACL Policy**.

2 Configure the parameters as follows:

Table 9-11 ACL Policy Parameters

Parameter	Description
Name	Select the Network Context
ACL List	The ACL List to use. The ACL List must already exist. See ACL List.

3 Click the **Save** icon.

Advice of Charge

Advice of Charge defines the action to take once online quota is exhausted, such as block and return a notification message or redirect subsequent HTTP traffic to a configured URL.

To add an Advice of Charge:

1 Use any of the following methods to add an Advice of Charge:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Advice of Charge**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Advice of Charge**.

2 Configure the parameters as follows:

Table 9-12 Advice of Charge Parameters

Parameter	Description
Name	Advice of Charge name.
AOC Hardware ID Format	The AOC Hardware ID Format must already exist. See Aoc Hardware ID Format.
Redirect Code	HTTP Request Redirect Code: ■ 302 found – The requested resource resides temporarily under a different URL ■ 303 See Other – The requested page can be found under a different URL ■ 307 Temporary Redirect – The requested page has moved temporarily to a new URL
Include MAC	Specify whether to include the MAC address in the redirect URL: ■ true ■ false

Table 9-12 Advice of Charge Parameters

Parameter	Description
Include Original URL	Specify whether to include the original requested address in the redirect URL: ■ true ■ false
Include IMSI	Specify whether to include the IMSI in the redirect URL: ■ true ■ false
Include IMEI	Specify whether to include the IMEI in the redirect URL: ■ true ■ false
Include MSISDN	Specify whether to include the MSISDN in the redirect URL: ■ true ■ false
Include Class	Specify whether to include the class information (received from the RADIUS server) in the redirect URL: ■ true ■ false The class information is provided by the RADIUS server and is used to identify the subscriber in subsequent RADIUS accounting messages.
Action	Specify action: ■ redirectUrl ■ notificationMsg
Field when Action is set to notificationMsg:	
Notification Msg	HTTP Request Block Message
Field when Action is set to redirectUrl:	
Redirect URL	HTTP request redirect URL

3 In **Charge Notification List**, click the **Create** icon.

4 Configure the following parameters to specify the notification message to be sent to the user when rejecting:

Table 9-13 Charge Notification Parameters

Parameter	Description
Code	Select the MSCC Result Code

Table 9-13 Charge Notification Parameters

Parameter	Description
MMS Error Code	Select the MMS Error Result Code
Notification Text	Enter the MMS error response text
SMS Notification Text	Enter the SMS notification text

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many Charge Notifications as needed.

7 Click the **Save** icon.

Aoc Hardware ID Format

Use this object to specify AES-encrypted UE hardware information in the redirection URL. This feature is supported for offline charging only.

Note: Redirection is supported only for HTTP.

This feature enables Operators to apply the redirection URL configured in Advice Of Charge which is associated with a Rating Group. The PCRF activates a predefined Service Rule configured under Rating Group.

MCC uses the Advice Of Charge configured in the corresponding Rule Group to create the encrypted hardware ID details. MCC applies the AES encryption on the hardware ID and appends the encrypted hardware ID to the redirection URL configured in Advice Of Charge. MCC sends the redirected URL to the UE for redirection.

To add an Aoc Hardware ID Format:

1 Use any of the following methods to add an Aoc Hardware ID Format:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Aoc Hardware ID Format**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Aoc Hardware ID Format**.

2 Configure the parameters as follows:

Table 9-14 Aoc Hardware ID Format Parameters

Parameter	Description
Name	Name of the Aoc Hardware ID Format
Delimiter	Delimiter to be used in formatting the hardware ID information to be appended in the redirection URL.
Encryption Algorithm	Encryption algorithm to be used in formatting the hardware ID information to be appended in the redirection URL.
Encryption Key	Encryption key for encrypted algorithm.

Table 9-14 Aoc Hardware ID Format Parameters

Parameter	Description
Prepend String	Prepend string for encrypted hardware ID.
Enclosure String	Enclosure string for encrypted hardware ID.

3 Click the **Save** icon.

APN Mapping List

The APN Mapping List provides additional granularity to APN mapping. It contains a list of APN values to be mapped to, based upon user-specific criteria. For example, it could use PAP username criteria to select a specific APN to use for the specific subscriber.

Note: *APN mapping is not supported for emergency APNs.*

To add an APN Mapping List:

1 Use any of the following methods to add an APN Mapping List:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **APN Mapping List**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New APN Mapping List**.

2 Configure the parameters as follows:

Table 9-15 APN Mapping List Parameters

Parameter	Description
Name	APN Mapping List name
User Description	Description of APN Mapping List

3 In **APN Mapping**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-16 APN Mapping Parameters

Parameter	Description
Value	Specify to perform the classification using user@realm or just realm. For example, user1@internet.net or internet.net

Table 9-16 APN Mapping Parameters

Parameter	Description
User Description	Description of the specific APN Mapping.
Mapped Apn Name	The mapped APN to use. The APN must already exist. Create it at Zone > *name* > Gateway > APN.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many APN Mappings as needed.

7 Click the **Save** icon.

Application Rule Group (MCC versions prior to 8.4)

Acuitas does not support this object for MCC 8.4 and later releases. It has been replaced by Protocol Application Rule Group. See Protocol Application Rule Group (8.4 and later MCC version).

The Application Rule Group defines layer 7 applications, protocols, and subprotocols for signature analysis by detecting deterministic and/or heuristic patterns in bidirectional packet flow. Signature Analysis is the key technology that enables Workflow to control application of advanced services on subscriber traffic (such as charging, per-application filtering, QOS, and so on).

An Application Rule Group can select only:

- Applications whose underlying protocols are selected in the Deep Packet Inspection service construct.
- Protocols that are selected in the Deep Packet Inspection service construct.
- Sub protocols whose corresponding protocol is also selected in the Application Rule Group.

To add an Application Rule Group:

1 Use any of the following methods to add an Application Rule Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Application Rule Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Application Rule Group**.

2 Configure the parameters as follows:

- **Name** – Enter an Application Rule Group name.
- **Applications** – Mark the checkbox(es) to select the Application(s) to include in the Application Rule Group.
- **Protocols** – Mark the checkbox(es) to select the protocol(s) to include with the Application Rule Group. To select all protocols in a category, mark the **all-*category*-protocols** checkbox.
- **Subprotocols** – Mark the checkbox(es) to select the subprotocol(s) to include with the Application Rule Group.

Application Rule Group applications, protocols, and subprotocols are listed in the following table:

3 Click the **Save** icon.

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Applications	■ Facebook Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) – Jabber (in Instant Messaging category) ■ MagicJack Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) – SIP (in Voice Over IP category) ■ iTunes Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ MySpace Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ FaceTime Detected using underlying protocols: – SIP (in Voice Over IP category) ■ TruPhone Detected using underlying protocols: – HTTP (in Web category) – SIP (in Voice Over IP category) – Jabber (in Instant Messaging category) ■ Twitter Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ WindowsMedia Detected using underlying protocols: – HTTP (in Web category) ■ Xbox Detected using underlying protocols: – HTTP (in Web category) – XBOX (in Gaming category) ■ RealMedia Detected using underlying protocols: – HTTP (in Web category) ■ Gmail Detected using underlying protocols: – SSL (in Tunnel category) – Jabber (in Instant Messaging category) ■ Goober Detected using underlying protocols: – SIP (in Voice Over IP category) – Goober (in Voice Over IP category) ■ Blackberry Detected using underlying protocols: – HTTP (in Web category) – Blackberry (in Mobile category) ■ iCloud Detected using underlying protocols: – SSL (in Tunnel category) ■ UbuntoOne Detected using underlying protocols: – SSL (in Tunnel category) ■ DropBox Detected using underlying protocols: – SSL (in Tunnel category) ■ GoogleDocs Detected using underlying protocols: – SSL (in Tunnel category) ■ Yuilop Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) – Jabber (in Instant Messaging category) ■ iMessage Detected using underlying protocols: – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ GoToMyPC Detected using underlying protocols: – CitrixGoTo (in Conference category) ■ GoToMeeting Detected using underlying protocols: – CitrixGoTo (in Conference category) ■ WindowsAzure Detected using underlying protocols: – SSL (in Tunnel category) ■ AmazonCloud Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ DailyMotion Detected using underlying protocols: – HTTP (in Web category) ■ Deezer Detected using underlying protocols: – HTTP (in Web category) ■ Grooveshark Detected using underlying protocols: – HTTP (in Web category) ■ Sudaphone Detected using underlying protocols: – SIP (in Voice Over IP category) – Sudaphone (in Voice Over IP category) ■ Office365 Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ CnTV Detected using underlying protocols: – HTTP (in Web category) ■ SinaTV Detected using underlying protocols: – HTTP (in Web category) ■ Youtube Detected using underlying protocols: – HTTP (in Web category) ■ VoipSwitch Detected using underlying protocols: – SIP (in Voice Over IP category) ■ Zynga Detected using underlying protocols: – SSL (in Tunnel category) ■ CrimeCity Detected using underlying protocols: – HTTP (in Web category) ■ ModernWar Detected using underlying protocols: – HTTP (in Web category) ■ Vippie Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Box Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ SkyDrive Detected using underlying protocols: – SSL (in Tunnel category) ■ AdobeCreativeCloud Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Linkedin Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Orkut Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ Hi5 Detected using underlying protocols: – HTTP (in Web category) ■ Soribada Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ ZohoWorkOnline Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Hotmail Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Instagram Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Sugersync Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Wickr Detected using underlying protocols: – HTTP (in Web category) ■ Tigertext Detected using underlying protocols: – SSL (in Tunnel category) – Jabber (in Instant Messaging category) ■ Vibe Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Enlegion Detected using underlying protocols: – HTTP (in Web category) ■ Voxer Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Lovefilm Detected using underlying protocols: – HTTP (in Web category) ■ Friendster Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Burner Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Flickr Detected using underlying protocols: – HTTP (in Web category) ■ LiveCom Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ ICQWebChat Detected using underlying protocols: – HTTP (in Web category) ■ RedTube Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EverNote Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Spreed Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
(Continued)	■ TextPlus Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ XVideos Detected using underlying protocols: – HTTP (in Web category)	■ SnapChat – HTTP (in Web category) – SSL (in Tunnel category)
Applications2 *(additional applications)*	■ Youku Detected using underlying protocols: – HTTP (in Web category) ■ MyMusicTW Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Renren Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Yelp Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AmazonShop Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ none ■ Youporn Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ eBay Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Pornhub Detected using underlying protocols: – HTTP (in Web category)	■ SpiderOak Detected using underlying protocols: – SSL (in Tunnel category) ■ Adrive Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Tumbler ■ Xing ■ GooglePlayMusic ■ Vimeo ■ SalesForce ■ iTunesRadio ■ SinaWeibo ■ Forfone ■ LiveJasmin Detected using underlying protocols: – HTTP (in Web category) ■ JingDong Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IMS Detected using underlying protocols: – SIP (in Voice Over IP category) ■ Baidu Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ TaoBao Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Whatchever Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TTPOD Detected using underlying protocols: – HTTP (in Web category) ■ Three60Mobile Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Pinterest Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Vine Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Net2Phone Detected using underlying protocols: – HTTP (in Web category) ■ FourSquare Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iLiveTo Detected using underlying protocols: – HTTP (in Web category) ■ MEGA Detected using underlying protocols: – HTTP (in Web category) ■ DOOOK Detected using underlying protocols: – HTTP (in Web category) ■ vBulletin Detected using underlying protocols: – HTTP (in Web category) ■ CloudMe Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ YikYak Detected using underlying protocols: – SSL (in Tunnel category) ■ RedMine Detected using underlying protocols: – HTTP (in Web category) ■ iHeartRadio Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AviraAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ NortonAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ KasperskyAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ AVGAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ SoundCloud Detected using underlying protocols: – SSL (in Tunnel category) ■ RDIO Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ AmazonPrimeMusic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RunKeeper Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyBook Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NikePlus Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MAGV Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MAGVKids Detected using underlying protocols: – HTTP (in Web category) ■ DotaLegend Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LETV Detected using underlying protocols: – HTTP (in Web category) ■ MyFitnessPal Detected using underlying protocols: – SSL (in Tunnel category) ■ SOHU Detected using underlying protocols: – HTTP (in Web category) ■ OneKXUN Detected using underlying protocols: – HTTP (in Web category) ■ TVBS Detected using underlying protocols: – HTTP (in Web category) ■ XNXX Detected using underlying protocols: – HTTP (in Web category) ■ CTITV Detected using underlying protocols: – HTTP (in Web category) ■ Endomondo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TimelyTV Detected using underlying protocols: – HTTP (in Web category) ■ WorkoutTrainer Detected using underlying protocols: – HTTP (in Web category) ■ MapMyRun Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Applications3 *(additional applications)*	■ KingOfPirates Detected using underlying protocols: – HTTP (in Web category) ■ TUDOU Detected using underlying protocols: – HTTP (in Web category) ■ Duokan Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MeiLu Detected using underlying protocols: – HTTP (in Web category) ■ Skout Detected using underlying protocols: – HTTP (in Web category) ■ playTales Detected using underlying protocols: – HTTP (in Web category) ■ GameOfWar Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FETnet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FBS Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NationalBaseball Detected using underlying protocols: – HTTP (in Web category) ■ PinkFong Detected using underlying protocols: – HTTP (in Web category) ■ KollectBook Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SPTGTV Detected using underlying protocols: – HTTP (in Web category) ■ CiaomobileHDTV Detected using underlying protocols: – HTTP (in Web category) ■ SkyKing Detected using underlying protocols: – HTTP (in Web category) ■ Moves Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Path Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iWowSystext Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NineKU Detected using underlying protocols: – HTTP (in Web category) ■ NextTV Detected using underlying protocols: – HTTP (in Web category) ■ Syncplicity Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ RealMa Detected using underlying protocols: – HTTP (in Web category) ■ Yuanta Detected using underlying protocols: – HTTP (in Web category) ■ HiNet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyCard Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ KONO Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Speakaboos Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DuoDuo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ WealthGod Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iLeader Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ threeBamboo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Taaze Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Audiko Detected using underlying protocols: – HTTP (in Web category) ■ pubuBookbuffet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MiTake Detected using underlying protocols: – HTTP (in Web category) ■ HyRead Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DisneyStoryTime Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Qualys Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ConstantContact Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Rally Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Intralinks Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ AppleMusic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Naver Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ BookingCom Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ CNN Detected using underlying protocols: – HTTP (in Web category) ■ PayEasy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LineRangers Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IOSAppStore Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyVideo Detected using underlying protocols: – HTTP (in Web category) ■ KingGaming Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ CandyCrush Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ CandyCrushSoda Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ BubbleWitch Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FarmHero Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ WindowsStore Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MineCraft Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Meerkat Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RovioGaming Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AngryBirds Detected using underlying protocols: – HTTP (in Web category) ■ CitrixXenApp Detected using underlying protocols: – HTTP (in Web category) ■ Redditt Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ PayPal Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PlantsVsZombies2 Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ HalfbrickStudios Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)
Applications4 *(additional applications)*	■ gitHub Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ HamiVideo Detected using underlying protocols: – HTTP (in Web category) ■ Slacker Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NicoNico Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AliPay Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ UStream Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NttDocomo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Softbank Detected using underlying protocols: – HTTP (in Web category) ■ TrendMicroWorryFree Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Wikipedia Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Uber Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Yandex Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ VK Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Alibaba Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AliExpress Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ TMall Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NortonSecurity (Supplants NortonAntivirus) Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PochtaRossii Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AfterSchool Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DriveLock Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ QipRu Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MusicalLy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EAGames Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iTunesU Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PopCap Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SurveyMonkey Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NewRelic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Huddle Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ZenDesk Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ OutlookMobile Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Dena Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ BackBlaze Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DocuSign Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ BetterNet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Good ■ AngHami Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Slack Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PokemonGo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NianticLabs Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TwoGIS Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RuTube Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TwoChannel Detected using underlying protocols: – HTTP (in Web category) ■ Prisma Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AmazonPrimeVideo (Supplants Lovefilm) Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Signal Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ KanKan Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Azar ■ SkyGo ■ iCrypt Detected using underlying protocols: – SSL (in Tunnel category) ■ Kinopoisk Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IviRu ■ Tinder Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AnyDesk Detected using underlying protocols: – SSL (in Tunnel category) ■ Tenor Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ APNS Detected using underlying protocols: – HTTP (in Web category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ DigicelPlayGo Detected using underlying protocols: – SSL (in Tunnel category) ■ DigicelMusic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DigicelTopUp Detected using underlying protocols: – HTTP (in Web category) ■ Dubsmash Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyDigicel Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Waze Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ChannelOne Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Giphy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Imgur Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Applications5 *(additional applications)*	■ OneDrive Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iFlix Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AppleServices Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MicrosoftServices Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IcFlix Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LogMeIn Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Shazam Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TuneInRadio Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Badoo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AirBnB Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ HighTail Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EasyTaxi Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TomTom Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TripAdvisor Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ESPN Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DAZN Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MobileStrike Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ KingOfAvalon Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Lineage2 Detected using underlying protocols: – HTTP (in Web category) ■ Lyft Detected using underlying protocols: – HTTP (in Web category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ Trulia Detected using underlying protocols: – HTTP (in Web category) ■ AkamaiCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LimelightCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NickelodeonPlay Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Here Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SimcityBuildit Detected using underlying protocols: – HTTP (in Web category) ■ StarwarsGOH (Galaxy of Heroes) Detected using underlying protocols: – SSL (in Tunnel category) ■ Fastly Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Cloudflare Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LifeChurch Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Vevo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Grindr Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AppleMaps Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AppleGeolocation Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ YoukuTudou Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MeeticGroup Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Sarahah Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Vudu Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Wish Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ Auth0 Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SlingTV Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RackspaceCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ StackpathCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ HouseParty Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LearningHubOnline Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FoxSports Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AmazonServices ■ AmazonDrive ■ Crashlytics Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LoopTradeClassifieds Detected using underlying protocols: – HTTP (in Web category) ■ LoopCaribbeanLocalNews Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LoopPacificLocalNews Detected using underlying protocols: – HTTP (in Web category) ■ Unity Detected using underlying protocols: – SSL (in Tunnel category) ■ Mapbox Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Cedexis Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Smule Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Symantec Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MaxDome Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EpicBrowserProxy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Business	■ all-business-protocols ■ AdobeConnect ■ Citrix ■ ActiveSync ■ JBK3000 ■ Lync Subprotocols: – audio – video – file-transfer ■ SAP ■ UltraBac ■ Fix ■ LicenseExceeded ■ LotusNotes ■ MSexchange Subprotocols: – generic – owa ■ MSNav ■ FUZE ■ KaKao Subprotocols: – generic – kakaoTalk ■ SkypeForBusiness Subprotocols: – generic – audio – video – file-transfer ■ SCADA ■ CrashPlan ■ S7Comm ■ Amazon Subprotocols: – services – chime – cloud – drive – primeMusic – primeVideo – shop ■ Bitcoin ■ Synology ■ StratumMining
Conference	■ all-conference-protocols ■ CitrixGoTo ■ Webex ■ ooVoo
Database	■ all-database-protocols ■ MySQL ■ PostgreSQL ■ TDS ■ msSQL ■ OracleDB ■ CQL (Cassandra Query Language) ■ CIC (Cassandra Intermode Communication)

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
File Transfer	■ all-file-transfer-protocols ■ AFP ■ DirectDownloadLink ■ FTP Subprotocols: – control – data ■ NFS ■ SMB-CIFS ■ TFTP ■ WebDAV ■ HiDrive	■ osUpdate Subprotocols: – Android – iOS – WindowsPhone – MSWindows – Chrome ■ DCE-RPC ■ IDRIVE ■ FLUTE ■ Rsync
Flow *(Operating system of the individual flow. May differ from the subscriber operating system if from a tethered device)*	■ Windows-Desktop ■ Windows ■ Linux ■ MacOS ■ iOS ■ Symbian ■ Android ■ Blackberry	■ WindowsMobile ■ WindowsPhone ■ Tethered – true (indicates this flow is sourced from a tethered device) – false

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
Gaming	■ all-gaming-protocols	■ rFactor
	■ Armagetron	■ Dota2
	■ Battlefield	■ Tibia
	■ ClubPenguin	■ Destiny
	■ CrossFire	■ AgeOfWarringEmpire
	■ Dofus	■ PlayStation
	■ Fiesta	■ SuperCell
	■ Florensia	Subprotocols:
	■ GameKit	– generic
	■ Guildwars	– clashOfClans
	■ QQGame	– boomBeach
	■ Halflife2	– hayDay
	■ MapleStory	– ClashRoyale
	■ PS3	■ LeagueOfLegends
	■ Quake	■ Battlenet
	■ SecondLife	■ GuildWars2
	■ SplashFighter	■ EAOrigin
	■ Steam	■ PathOfExile
	■ WARCRAFT3	■ NintendoNetwork
	■ Wii	■ Lineage2
	■ WorldOfKungFu	■ Minecraft
	■ WorldOfWarcraft	■ Zynga
	■ Xbox	■ EpicGames

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Instant Messaging	■ all-im-protocols ■ GaduGadu Subprotocols: – server – file-transfer – voice – video ■ GoogleTalk Subprotocols: – voice – file-transfer – video ■ IMO ■ IMplus ■ IRC Subprotocols: – file-transfer ■ Nimbuzz ■ Jabber Subprotocols: – voice – file-transfer – video – encrypted ■ MEEBO Subprotocols: – audio – video ■ MSN Subprotocols: – voice – file-transfer – video – webchat ■ MSRP ■ Oscar Subprotocols: – file-transfer – picture-transfer – voice – video ■ POPO ■ Pal Talk Subprotocols: – server – file-transfer – voice – video ■ QQ Subprotocols: – voice – file-transfer – video ■ Usenet ■ Whats App Subprotocols: – generic – file-transfer – video-call – voice-call ■ XDCC ■ Yahoo Subprotocols: – voice – file-transfer – video – webchat – webmail ■ eBuddy

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ WeChat Subprotocols: – generic – voice-live-chat – video-call – chat – data-message – web-chat ■ KikMessenger ■ MPlus ■ HikeMessenger ■ Threema ■ Telegram ■ DOOOK ■ BlueJeans ■ Zalo ■ Hangouts Subprotocols: – unknown – audio – file-transfer – video ■ SnapChat ■ Yuilop Subprotocols: – generic – audio ■ IO ■ AIM Subprotocols: – generic – file-transfer ■ ICQ Subprotocols: – generic – file-transfer – audio – video ■ ZeroMQ ■ Signal ■ WireMessenger Subprotocols: – generic – audio – video
Mail	■ all-mail-protocols ■ IMAP Subprotocols: – generic – encrypted ■ Mapi ■ POP Subprotocols: – pop3generic – pop3encrypted ■ SMTP Subprotocols: – generic – encrypted

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
Mobile	■ all-mobile-protocols ■ BOLT ■ Blackberry Subprotocols: – encrypted – email – messenger ■ MMS (MultimediaMessaging) ■ OperaMini ■ WAP-WSP ■ WAP-WTLS ■ WAP-WTP-WSP	■ Mig33 ■ MQTT Subprotocols: – generic – encrypted ■ SCADA ■ Instagram Subprotocols: – generic – video – file-transfer – chat
Network Management	■ all-network-management-protocols ■ BGP ■ DHCP ■ DHCPv6 ■ DNS ■ EGP ■ ICMP ■ ICMPv6 ■ IGMP ■ IPP ■ Kerberos ■ LDAP Subprotocols: – generic – encrypted ■ LDP ■ MulticastDNS ■ NETBIOS ■ NTP ■ OSPF	■ SCTP ■ SNMP ■ SSDP ■ Syslog ■ RSVP ■ NetFlow ■ iPerf ■ Diameter ■ TACACS ■ NTLM Subprotocols: – plain – encrypted ■ WHOIS ■ RADIUS ■ Megaco ■ SpeedTest ■ T3 ■ OpenFlow ■ IPMI ■ IPFix

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
Peer to Peer	■ all-p2p-protocols ■ ANtsP2P ■ Aimini ■ AppleJuice ■ Ares ■ BitTorrent Subprotocols: – plain – encrypted – utp – utp-encrypted ■ DirectConnect Subprotocols: – hub – peer – adc-peer ■ Filetopia ■ Gnutella ■ KaZaa-Fasttrack	■ Manolito ■ Mojo ■ Mute ■ OFF ■ OpenFT ■ Pando ■ Soulseek ■ StealthNet ■ Thunder-Webthunder ■ WINNY ■ WinMX ■ eDonkey Subprotocols: – plain – encrypted ■ iMesh ■ FreeNet ■ LocalPeerDiscovery
Remote Control	■ all-remote-control-protocols ■ PCAnywhere ■ RDP ■ SSH ■ Skinny ■ TeamViewer ■ Telnet Subprotocols: – generic – tn3270 ■ VNC ■ XDMCP ■ PoisonIvy ■ SOAP	■ IEC61850 Subprotocols: – goose – MMS – SMV ■ PCOverIP ■ ModBus ■ OpcUa ■ DNP3 ■ BACnet ■ Zero ■ CoAP

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Social Networking	■ all-social-networking-protocols ■ Runtastic ■ StreetVoice ■ LivePerson ■ Facebook Subprotocols: – video – encrypted – chat – file-transfer – generic – audio ■ Odnoklassniki ■ MailRu
Standard	■ all-standard-protocols ■ thrift ■ Fasp

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Streaming	■ all-streaming-protocols ■ avi ■ FLASH ■ Feidian ■ Funshion ■ VeohTV Subprotocols: – generic – flash ■ IPTV ■ Icecast ■ Kontiki ■ MicrosoftMediaServer ■ MPEG ■ Move ■ NetFlix Subprotocols: – generic – video ■ OGG ■ ORB Subprotocols: – server – client – client-rtsp – client-rdt – client-wmv – client-wma – client-flash – client-flv – client-3gp – client-upload-download – client-rtp ■ Octoshape ■ PPLIVE Subprotocols: – generic – video ■ PPSTREAM ■ Pandora ■ QQLive ■ QUICKTIME ■ REALMEDIA ■ RTCP ■ RTP ■ RTSP ■ RealDataTransport ■ SOPCAST ■ Shoutcast ■ Slingbox ■ Spotify ■ TVANTS ■ TVUPLAYER ■ UUSEE ■ Vcast ■ WINDOWSMEDIA ■ ZATTOO ■ iPlayer ■ AudioGalaxy ■ Rhapsody ■ Silverlight ■ ITV Subprotocols: – web – stream ■ Demand5 Subprotocols: – web – stream ■ Channel4oD ■ MyVideo Subprotocols: – web – stream ■ Spreecast ■ SIMFY ■ QVOD ■ HULU

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ TWITCH ■ WOWZA ■ MagineTV ■ Periscope ■ SRTP ■ SRTCP ■ PPFilm ■ LeTV
Subscriber *(Operating system of the user equipment device)*	■ Windows-Desktop ■ Windows ■ Linux ■ MacOS ■ iOS ■ Symbian ■ Android ■ Blackberry ■ WindowsMobile ■ WindowsPhone

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
Tunnel	■ all-tunnel-protocols ■ GRE ■ GTP Subprotocols: – control – user-data – prime ■ HamachiVPN ■ IP-in-IP ■ IPSEC Subprotocols: – data – control ■ ISAKMP ■ JAP ■ L2TP ■ NetMotion ■ OpenVPN ■ PPP ■ PPTP ■ SSL Subprotocols: – generic – SPDY ■ SSTP ■ SoftEthernet	■ TOR ■ Teredo ■ UltraSurf ■ VPN-X ■ VTUN ■ YourFreedom ■ SOCKS Subprotocols: – v4 – v5 ■ HTTPTunnel ■ PDProxy ■ CyberGhost ■ ComodoUnite ■ VyprVPN ■ Psiphon ■ ZenmateVPN ■ PIA ■ IPVanish ■ TunnelBear ■ ZeroVPN ■ SurfEasy ■ TigerVPN ■ AviraPhantomVPN ■ TurboVPN ■ VPNMaster

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Voice Over IP	■ all-voip-protocols ■ FiCall ■ Fring Subprotocols: – voice – video ■ Goober ■ H323 ■ IAX ■ Iskoot ■ MGCP Subprotocols: – control – rtp ■ MyPeople Subprotocols: – audio ■ SIP Subprotocols: – vonage – oscar – gadu-gadu – oscar-video – ichat-facetime – MagicJack – audio – video – MSN – yahoo – yahoo-video – MPlus – ChatCube ■ STUN ■ Scydo ■ Skype Subprotocols: – voice – out – video – chat – file-transfer ■ Tango Subprotocols: – audio – video – im – file-transfer ■ TeamSpeak ■ TruPhone ■ Ventrilo ■ Viber Subprotocols: – audio – instant-messaging – file-transfer – out – video ■ VoipSwitch ■ Sudaphone ■ Line Subprotocols: – generic – audio – video ■ Didi Subprotocols: – generic – voice – im ■ TunnelVoice ■ Vippie ■ ChatCube ■ Azar ■ FaceTime

Table 9-17 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Web	■ all-web-protocols ■ HTTP Subprotocols: – generic – voice – video – media ■ WebSocket ■ Wuala ■ WebQQ ■ SPDY Subprotocols: – ssl ■ Google Subprotocols: – encrypted – cloud – drive – docs – plus – play – generic – mail – youtube – maps – earth – fcm – apis – hangoutsGeneric – hangoutsAudio – hangoutsVideo – hangoutsFileTransfer – ads – allo – duo – analytics – calendar ■ QUIC ■ OCSP

CA Certificate List

The CA Certificate List configures a list of TLS Certificate Authority Certificates used for authenticating certificates of end users or network entities. The list can contain a bundle of certificates. Certificates configured in the list must be present in the /public/content/tls/cacerts/ folder on the MCM.

To add a CA Certificate List:

1. Use any of the following methods to add a CA Certificate List:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category**.

   c. Click **CA Certificate List**.

   d. Click the **Create** icon.

   Build a Workflow:

   a. Click the **Build a Workflow** tab.

   b. Expand **Functions**.

   c. Click the **New** tab.

   d. Click **New CA Certificate List**.

2. In **CA Certificate**, click the **Create** icon.

3. Use any of the following methods to specify a Trusted Certificate Authority Root Certificate:

   - **Name** – Enter the Trusted Certificate Authority Root Certificate. Click **Add**.
   - **Choose a CA Certificate** – To select a CA Certificate that has already been uploaded, click **Choose a CA Certificate**. Select the file and click **Select**.

4. To upload a CA Certificate file, click **Browse** in the Upload File field and select the file. Click **Upload**.

5. Repeat step 2 through step 4 to add as many CA certificates as needed.

6. Click the **Save** icon.

Content Filter Blacklist File

Black List is used by a *global* content filter to deny content requests to a specific list of domains or URLs.

To add a Content Filter Blacklist File:

1 Use any of the following methods to add a Content Filter Blacklist File:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Content Filter Blacklist File**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Content Filter Blacklist File**

2 Configure the parameters as follows:

Table 9-18 Blacklist Filter Parameters

Parameter	Description
Name	Black List name
File Type	Address types in the file: ■ Domain ■ URL
Action	Action to take to deny access to any of the domains or URLs in the text file: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL

Table 9-18 Blacklist Filter Parameters

Parameter	Description
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307

3 Click the **Save** icon.

DHCP Local Server Profile

To add a DHCP Local Server Profile:

1 Use any of the following methods to add a DHCP Local Server Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **DHCP Local Server Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New DHCP Local Server Profile**.

2 Configure the parameters as follows:

Table 9-19 DHCP Local Server Profile Parameters

Parameter	Description
DHCP Server Name	DHCP Server profile
Local Server IP Address	IP Address of the local DHCP server
Lease Timer	Lease timer
Primary DNS IP Address	Primary DNS IP address
Secondary DNS IP Address	Secondary DNS IP address
Interface MTU	Interface MTU
Router IP Address	Router IP address

Table 9-19 DHCP Local Server Profile Parameters

Parameter	Description
Subnet Mask	Subnet mask
Prior Subscriber IP Binding Timer	Time (in minutes) to retain the last assigned IP binding even after the session is deleted. If the session is re-established before the timer expires, the same IP Address is assigned. Once the timer expires, the IP Address is released.
Broadcast Address	Broadcast IP address.

3 Click the **Save** icon.

DHCP Service Profile

To add a DHCP Service Profile:

1 Use any of the following methods to add a DHCP Service Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **DHCP Service Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New DHCP Service Profile**.

2 Configure the parameters as follows:

Table 9-20 DHCP Service Profile Parameters

Parameter	Description
Service Name	DHCP Service name.
Admin State	Admin State: ■ enabled ■ disabled

Table 9-20 DHCP Service Profile Parameters

Parameter	Description
DHCP Service Mode	Mode of operation of the DHCP service: ■ dhcp-client: System acts as a client on behalf of the UE in an Enterprise network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server. The DHCP exchange occurs between the system (acting as a DHCP client) and the external DHCP server. The DHCP client uses this information to configure its host and communicate on the internet. ■ dhcp-relay: A DHCP relay agent is any host that forwards DHCP packets between DHCP clients and DHCP servers. DHCP relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway address and, if configured, adds the relay agent information option in the packet and forwards it to the DHCP server. The exchanges occurs between the DHCP server(s) and the UE; the system is in the middle and in the process, learns the UE IP address.
DHCP Network Context	Network Context containing this DHCP Service endpoint
DHCP Service Endpoint	Service endpoint on the Network Context
Enable Domain Name Server	Specify whether to use DNS configuration from external DHCP Server when configured as DHCP Client: ■ true ■ false
Enable Netbios Name Server	Specify whether to use NetBIOS Name Server configuration from external DHCP Server when configured as a DHCP Client: ■ true ■ false

3 In **External DHCP Server**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-21 External DHCP Server Parameters

Parameter	Description
Name	Unique name of the external DHCP Server.

Table 9-21 External DHCP Server Parameters

Parameter	Description
Admin State	Admin State: ■ enabled ■ disabled
IP Address	IP Address
Server IP Allocation Type	The Type of IP address that can be allocated by this external DHCP server: ■ V4 only ■ V6 only ■ V4 or V6

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many External DHCP Server as needed.

7 Click the **Save** icon.

DiffServ Profile Class Mapping

The DiffServ (Differentiated Services) defines priority queuing to ensure cluster and network stability under any traffic load. The Diffserv Profile Class Mapping configures the mapping of DiffServ class to queue priority.

Note: *Individual DSCP code values configured in the DiffServ Profile DSCP Mapping take precedence over the class values configured in this object. If an individual DSCP value is not configured, the queue priority defined for its class is used.*

To add a DiffServ Profile Class Mapping:

1 Use any of the following methods to add a DiffServ Profile Class Mapping:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **DiffServ Profile Class Mapping**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **User Created** tab.

d Expand **Select a Category**.

e Click **DiffServ Profile Class Mapping**.

2 Configure the parameters as follows:

Table 9-22 DiffServ Profile Class Mapping Parameters

Parameter	Description
Cs0	Queue Priority to use for class selector cs0: ■ gold ■ silver ■ bronze ■ best-effort
Cs1	Queue Priority to use for class selector cs1: ■ gold ■ silver ■ bronze ■ best-effort
Cs2	Queue Priority to use for class selector cs2: ■ gold ■ silver ■ bronze ■ best-effort
Cs3	Queue Priority to use for class selector cs3: ■ gold ■ silver ■ bronze ■ best-effort
Cs4	Queue Priority to use for class selector cs4: ■ gold ■ silver ■ bronze ■ best-effort
Cs5	Queue Priority to use for class selector cs5: ■ gold ■ silver ■ bronze ■ best-effort

Table 9-22 DiffServ Profile Class Mapping Parameters

Parameter	Description
Cs6	Queue Priority to use for class selector cs6: ■ gold ■ silver ■ bronze ■ best-effort
Cs7	Queue Priority to use for class selector cs7: ■ gold ■ silver ■ bronze ■ best-effort

3 Click the **Save** icon.

DiffServ Profile DSCP Mapping

The DiffServ (Differentiated Services) Profile defines priority queuing to ensure cluster and network stability under any traffic load. The DiffServ Profile DSCP Mapping configures the mapping of DSCP code to queue priority.

To add a DiffServ Profile DSCP Mapping:

1 Use any of the following methods to add a DiffServ Profile DSCP Mapping:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **DiffServ Profile DSCP Mapping**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New DiffServ Profile DSCP Mapping**.

2 Configure the parameters as follows:

Table 9-23 DiffServ Profile DSCP Mapping Parameters

Parameter	Description
Code	DSCP code value
Queue Priority	Queue Priority to use for the DSCP value: ■ gold ■ silver ■ bronze ■ best-effort If a DSCP mapping is not specified for a given DSCP value, the system uses the priority queue for the class to which the value belongs.

3 Click the **Save** icon.

Domain Rule Group

Domain rule groups are services rules that are used by workflow to classify certain connections and take specific actions for certain domains. Use this object to configure a list of domains for which snooping is enabled. DNS Snooping (DNSS) provides users with access to restricted URLs or sites (for example, social media sites such as Facebook or Twitter).

MCC supports the following matching criteria for domain names:

- begins-with (prefix)
- contains (partial)
- ends-with (suffix)
- exact match
- regular expressions

To add a Domain Rule Group:

1 Use any of the following methods to add a Domain Rule Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Domain Rule Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Domain Rule Group**.

2 Configure the parameters as follows:

Table 9-24 Domain Rule Group Parameters

Parameter	Description
Name	Domain Rule Group name
Rule	Domain Rule to be configured for the rule group
URL List	URL list file to match against the Request's URL. The URL List must already exist. See URL List.

Table 9-24 Domain Rule Group Parameters

Parameter	Description
Domain Name	Specify the domain name to match against: begins-with contains ends-with exact regex (Regular Expression)

3 Click the **Save** icon.

EDR Server Profile

Use this object to configure the EDR (Event Data Record) server Profile (maximum 8) to generate EDRs.

To add an EDR Server Profile:

1 Use any of the following methods to add an EDR Server Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **EDR Server Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New EDR Server Profile**.

2 Configure the parameters as follows:

Table 9-25 EDR Server Profile Parameters

Parameter	Description
Name	Profile name.
Admin State	Admin state of the profile: ■ enabled ■ disabled
IP Address	IP address of the EDR server
Port	TCP port of the EDR server
Network Context	Network context of the EDR server
EDR Source IP	Source IP address to use to reach the EDR server
Transport	Transport type: ■ tcp
Keep Alive	EDR server keep alive interval
TCP User Timeout	Number of seconds for TCP user data retransmission timeout

3 Click the **Save** icon.

Encryption Profile

Use this object to specify the algorithm and keys to be used for header encryption.

The Advanced Encryption Standard (AES) profile stores encryption algorithm information and keys depending on the algorithm configured by the Operator. MCC generates a random IV and includes this as an extra header in each encrypted header. MCC supports a key in hex format (without spaces).

MCC supports the AES-128/192/256-CBC encryption algorithm and Base64 and Hex encoding for the encrypted value.

To add an Encryption Profile:

1 Use any of the following methods to add an Encryption Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Encryption Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Encryption Profile**.

2 Configure the parameters as follows:

Table 9-26 Encryption Profile Parameters

Parameter	Description
Name	Profile name
Admin State	Admin state of the profile: ■ enabled ■ disabled
Encoding	Encoding format for encrypted information: ■ hex ■ base64

Table 9-26 Encryption Profile Parameters

Parameter	Description
Encryption Algorithm	Algorithm used for encryption: ■ aes-128-cbc: Encrypted by Advanced Encryption Standard 128-bit Cipher Block Chaining. Enter the key for AES encryption, in HEX format without spaces. ■ aes-192-cbc: Encrypted by Advanced Encryption Standard 192-bit Cipher Block Chaining. Enter the key for AES encryption, in HEX format without spaces. ■ aes-256-cbc: Encrypted by Advanced Encryption Standard 256-bit Cipher Block Chaining. Enter the key for AES encryption, in HEX format without spaces.

3 Click the **Save** icon.

File Download Profile

The File Download Profile defines parameters for importing lists from a file server.

To add a File Download Profile:

1 Use any of the following methods to add a File Download Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **File Download Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New File Download Profile**.

2 Configure the parameters as follows:

Table 9-27 File Download Profile Parameters

Parameter	Description
Name	File Download Profile name.

Table 9-27 File Download Profile Parameters

Parameter	Description
Automatic Download	Automatic Download: ■ enabled. When enabled, configure an automatic download schedule: Time of Day/Days of Week or Download Interval (which takes precedence) ■ disabled. When disabled, Operators must download the policy list manually (*on demand only* mode). In this mode, the Time of Day/Days of Week and Download Interval objects are configurable but not mandatory. If both are configured, the Download Interval takes precedence and is therefore used for automatic download.
Time of Day	File download time (in 24 hour time)
Retry Count	Number of times to retry the download after a failure.
Retry Interval	Number of minutes to wait to retry the download after a failure.
Server Address	Server address or hostname where the file resides.
Username	File download username.
Password	File download password.
Retain Count	Number of downloads to retain.
Network Context	Network context where the file resides.
Download Interval	Interval, in minutes, for periodic download. Value 0 disables periodic download. Other values override Time of Day and Days of Week download
Days of Week to Download Files	Mark which days to download the file.

3 Click the **Save** icon.

Filter Database Size

MCC blocks URLs listed in a hashed database. Use this object to configure maximum filter entry sizes for different filter types.

To add a Filter Database Size:

1 Use any of the following methods to add a Filter Database Size:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Filter Database Size**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Filter Database Size**.

2 Configure the parameters as follows:

Table 9-28 Filter Database Size Parameters

Parameter	Description
URL List	Set the URL-based filter total entry size. This setting requires a slot reboot on the CSM and SSM.
Static Filter	Set the static filter-based filter total entry size (includes blacklist, whitelist, and static-category) This setting requires a slot reboot on the CSM.
Filter Hash List	Set the filter hash list-based filter total entry size. This setting requires a slot reboot on the CSM.

3 Click the **Save** icon.

Host List

The Host List serves as a whitelist used by the Fraud Detection Profile. It contains the IP addresses that represent legitimate proxies.

To add a Host List:

1 Use any of the following methods to add a Host List:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Host List**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Host List**.

2 Configure the parameters as follows:

- **Name** – Enter the Host List name.

3 In **Host IP Address**, click the **Create** icon.

4 Configure the parameters as follows:

- **Host Entry IP** – Enter the Host IP address.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many IP addresses as needed.

7 Click the **Save** icon.

HTTP Header Enrichment

HTTP Header Enrichment provides the ability to insert, remove, or replace proprietary headers in the HTTP header. These headers are used by origin servers and other nodes in the Operator network to determine the treatment of the packet and for tracking purposes:

- Operator configures the headers to be inserted, removed, or replaced.
- HTTP Proxy supports adding L7 filters for header enrichment.
- Workflow determines the HTTP Proxy instance to use for a subscriber. The HTTP Header Enrichment profile associated with that HTTP Proxy instance is used for the HTTP transaction.
- HTTP Proxy instance supports explicit proxy configuration and any port (in addition to port 80).
- Proxy supports using a pre-configured network context for server-side TCP connections.
- Proxy supports steering traffic to a well-defined IP address and port (in a pre-configured network-context) based on request header based rules.

HTTP Proxy supports embedding variables in HTTP headers. HTTP Header Enrichment functionality supports the following variables:

- IMSI
- MSISDN
- HTTPVERSION

The feature enables support for the following use cases:

- Ut (VoLTE) interface support for adding *X-3GPP-Asserted-Identity* header with embedded *MSISDN* variable. The Ut interface is defined in *3GPP TS 24.623*.
- Adding and updating *Via* header with embedded *HTTPVERSION* variable to HTTP requests and responses. The *Via* header is defined in *IETF RFC7230*.

The HTTP Header Enrichment profile supports the addition of a string macro to include variables for add-header header-string value and rewrite-header header-string append-value. MCC uses "`$()`" in the string macro to indicate a variable. Any "`$`" or "`()`" that does not conform to this format is considered a normal character in the string instead of variable. The string-macro may contain as many variables as needed. The string length limitation is 255.

This features also enables Operators to add or rewrite a *Via* header. If a `Via` header already exists and rewrite is configured, MCC rewrites the header with the original information and appends the configuration with "`,`".

Adding an HTTP Header Enrichment

To add an HTTP Header Enrichment:

1 Use any of the following methods to add an HTTP Header Enrichment:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **HTTP Header Enrichment**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New HTTP Header Enrichment**.

2 Configure the parameters as follows:

- **Name** – Enter the HTTP Header Enrichment name.
- **First Request** – Mark the checkbox to apply the HTTP Header Enrichment add-header and add-cookie only for the first request on a client connection.
- **Encryption Profile** – Configure an encryption profile used to encrypt request header value.

3 In **Request Cookie Custom String**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-29 Add Request Cookie Custom String Parameters

Parameter	Description
Cookie String	Enter the custom string of the cookie.
Cookie Value	Specify the value to include in the cookie: ■ imsi - Include IMSI in the cookie ■ msisdn - Include MSISDN in the cookie ■ value - Value to include for the cookie

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many Request Cookie Custom Strings as needed.

7 In **Request Cookie String**, click the **Create** icon.

8 Configure the parameters as follows:

Table 9-30 Add Request Cookie String Parameters

Parameter	Description
Cookie String	Specify the string of the cookie: ■ User-Identity-Forward-IMSI – Add subscriber IMSI to Cookie ■ User-Identity-Forward-MSISDN – Add subscriber MSISDN to Cookie
Cookie Value	Specify the value to include in the cookie: ■ imsi - Include IMSI in the cookie ■ msisdn - Include MSISDN in the cookie ■ value - Value to include for the cookie

9 Click **Add**.

10 Repeat step 7 through step 9 to add as many Request Cookie Strings as needed.

11 In **Request Header Custom String**, click the **Create** icon.

12 Configure the parameters as follows:

Table 9-31 Request Header Custom String Parameters

Parameter	Description
Header String	Enter the custom string of the header.

Table 9-31 Request Header Custom String Parameters

Parameter	Description
Header Value	Specify the value to include in the header: ■ msisdn - Include MSISDN in the header: – MSISDN – MD5: Include MD5 encrypted MSISDN in the header – Static Encryption: Include static encrypted MSISDN in the header (uses “no padding” to produce a persistent sequence of bytes) – Dynamic Encryption: Include dynamic encrypted MSISDN in the header (uses timestamp to generate a new dynamic value for each PDP context) – encrypted: Include encrypted MSISDN in the header by the algorithm configured in encryption profile – Static-acr – Supports a predefined format value + encrypted value of MSISDN. – Dynamic-acr – Supports a predefined format value + encrypted value of timestamp and MSISDN. ■ ue-ip-addr - Include User Equipment IP Address in the header ■ ue-ip-addr-port - Include User Equipment IP Address port in the header ■ ue-port - Include User Equipment port in the header ■ rat-type - Include Radio Access Type (2G, 3G, or 4G) in the header ■ charging-characteristic - Include Charging Characteristic in the header ■ http-protocol - Include HTTP Protocol (HTTP or HTTPS) in the header ■ serving-gw-ip-address - Include the serving gateway IPv4 address in the header ■ serving-gw-ipv6-address - Include the serving gateway IPv6 address in the header ■ serving-network-plmnid - Include the serving network PLMNID in the header ■ original-apn-name - Include the original APN name in the header ■ mapped-apn-name - Include the mapped APN name in the header ■ reseller-id - Include the reseller ID in the header ■ original-url - Inserts the original URL in the request header prior to sending the request to the server ■ imei - Include IMEI in the header: – IMEI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile

Table 9-31 Request Header Custom String Parameters

Parameter	Description
Header Value ***(Continued)***	■ imsi - Include IMSI in the header: – IMSI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile ■ user-location-info - Include User Location Information in the header: – Cgi - Include Cell Global Information in the header ■ subscriber-id - Include subscriber ID in the header: – ltmi-dynamic-trusted: Include Dynamic Trusted ID in the header – ltmi-external: Include External ID in the header – ltmi-static-trusted: Include Static Trusted ID in the header – plain-text: Include plain text ID in the header ■ ue-ipv4-mapped-ipv6-addr - Include an IPv4 address mapped to an IPv6 address in the header: – IPv6 Prefix- Configure up to a 96-bit IPv6 Prefix to map an IPv4 address into an IPv6 address format ■ time-zone - Include UE time zone and daylight savings in the header. The header value follows the 3GPP standard and uses a 4-digit hex string ■ value - Value to include for the header

13 Click **Add**.

14 Repeat step 11 through step 13 to add as many Request Header Custom Strings as needed.

15 In **Request Header String**, click the **Create** icon.

16 Configure the parameters as follows:

Table 9-32 Request Header String Parameters

Parameter	Description
Header String	Specify the string of the header: ■ X-Forwarded-For – Add X-Forwarded-For header name ■ X-Forwarded-Proto – Add X-Forwarded-Proto header name ■ X-IMSI – Add X-IMSI header name ■ X-MSISDN – Add X-MSISDN header name

Table 9-32 Request Header String Parameters

Parameter	Description
Header Value	Specify the value to include in the header: ■ msisdn - Include MSISDN in the header: – MSISDN – MD5: Include MD5 encrypted MSISDN in the header – Static Encryption: Include static encrypted MSISDN in the header (uses “no padding” to produce a persistent sequence of bytes) – Dynamic Encryption: Include dynamic encrypted MSISDN in the header (uses timestamp to generate a new dynamic value for each PDP context) – encrypted: Include encrypted MSISDN in the header by the algorithm configured in encryption profile – Static-acr – Supports a predefined format value + encrypted value of MSISDN. – Dynamic-acr – Supports a predefined format value + encrypted value of timestamp and MSISDN. ■ ue-ip-addr - Include User Equipment IP Address in the header ■ ue-ip-addr-port - Include User Equipment IP Address port in the header ■ ue-port - Include User Equipment port in the header ■ rat-type - Include Radio Access Type (2G, 3G, or 4G) in the header ■ charging-characteristic - Include Charging Characteristic in the header ■ http-protocol - Include HTTP Protocol (HTTP or HTTPS) in the header ■ serving-gw-ip-address - Include the serving gateway IPv4 address in the header ■ serving-gw-ipv6-address - Include the serving gateway IPv6 address in the header ■ serving-network-plmnid - Include the serving network PLMNID in the header ■ original-apn-name - Include the original APN name in the header ■ mapped-apn-name - Include the mapped APN name in the header ■ reseller-id - Include the reseller ID in the header ■ original-url - Inserts the original URL in the request header prior to sending the request to the server ■ imei - Include IMEI in the header: – IMEI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile

Table 9-32 Request Header String Parameters

Parameter	Description
Header Value ***(Continued)***	■ imsi - Include IMSI in the header: – IMSI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile ■ user-location-info - Include User Location Information in the header: – Cgi - Include Cell Global Information in the header ■ subscriber-id - Include subscriber ID in the header: – ltmi-dynamic-trusted: Include Dynamic Trusted ID in the header – ltmi-external: Include External ID in the header – ltmi-static-trusted: Include Static Trusted ID in the header – plain-text: Include plain text ID in the header ■ ue-ipv4-mapped-ipv6-addr - Include an IPv4 address mapped to an IPv6 address in the header: – IPv6 Prefix- Configure up to a 96-bit IPv6 Prefix to map an IPv4 address into an IPv6 address format ■ time-zone - Include UE time zone and daylight savings in the header. The header value follows the 3GPP standard and uses a 4-digit hex string ■ value - Value to include for the header

17 Click **Add**.

18 Repeat step 15 through step 17 to add as many Response Header Strings as needed.

19 In **Response Header String**, click the **Create** icon.

20 Configure the parameters as follows:

Table 9-33 Add Response Header String Parameters

Parameter	Description
Header String	Specify the string of the header.
Header Value	Specify the value to include in the header.

21 Click **Add**.

22 Repeat step 19 through step 21 to add as many Response Header Strings as needed.

23 Click the **Save** icon.

Removing an HTTP Header Enrichment

To remove an HTTP Header Enrichment string:

1. To remove a string from an HTTP Request or Response, click the **Create** icon in **Remove Header String**.
2. Enter the header string to remove.
3. Click **Add**.
4. To remove additional Header Strings, repeat step 1 through step 3.
5. Click the **Save** icon.

Rewriting an HTTP Header Enrichment

To rewrite an HTTP Header Enrichment string:

1. To rewrite a string in an HTTP Request or Response, click the **Create** icon in **Rewrite Header String**.
2. Configure the parameters as follows:

Table 9-34 Rewrite Request Header String Parameters

Parameter	Description
Header String	Enter the header string to rewrite.
Header Rewrite Option	Rewrite Option: ■ appendValue – Append a value to an existing header. string (any character except Ctrls and seperators, may include variable such as IMSI, MSISDN, HTTPVERSION, example: $(MSISDN)). ■ replaceHeader – Replace header string with a new string (HTTP header field name string). ■ replaceValue – Replace header value with a new value (HTTP token - any character except Ctrls and seperators). Specify the value to rewrite for the header.

3. Click **Add**.
4. To rewrite additional Header Strings, repeat step 1 through step 3.
5. Click the **Save** icon.

To specify that the HTTP Header Enrichment be used by an HTTP Policy, see HTTP Response Policy.

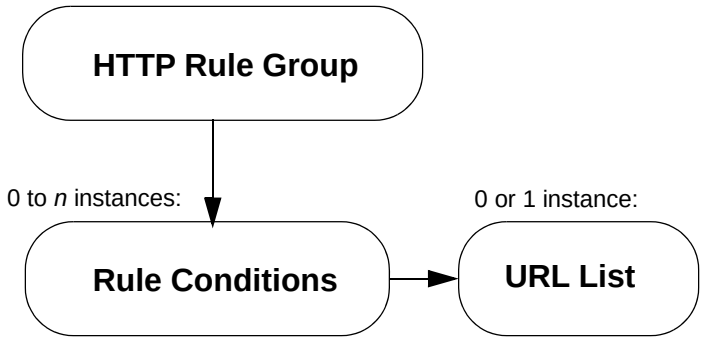
HTTP Rule Group

The HTTP Rule Group function defines a set of rules for matching header attributes in HTTP request and response headers, such as HTTP Request's Host header, HTTP Request's URI, HTTP Request's Content-type header, and so on. This object is referred to by a Service Rule. When a match is found in the header, specific actions or service(s) can be applied, based on where the Service Rule is used, such as terminate/block/redirect/allow action for Content Filter service, Header Enrichment for HTTP-proxy service, and so on.

Note: *If the Service Rule configured for the HTTP Rule Group does not contain a Packet Filter, MCC cannot detect CONNECT requests. For proper operation, Service Rules configured for HTTP Rule Groups that filter on the CONNECT Request Method must also be configured with at least one Packet Filter.*

The following figure illustrates the components of HTTP Rule Group.

Figure 9-22 HTTP Rule Group Components



To add an HTTP Rule Group:

1 Use any of the following methods to add an HTTP Rule Group:

Build Out Functions:

a Expand **Select a Category**.

b Click **HTTP Rule Group**.

c Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New HTTP Rule Group**.

2 Configure the parameters as follows:

- **Rule Group Name** – Enter a Rule Group name.

3 In **Rule Conditions**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-35 Rule Condition Parameters

Parameter	Description
Rule Name	Rule Condition name
URL List	URL list file to match against the HTTP Request's URL. The URL List must already exist. See URL List.
Request Method	String to match against HTTP Request's Method field: ■ GET ■ HEAD ■ POST ■ PUT ■ DELETE ■ TRACE ■ OPTIONS ■ CONNECT
Response Status Code	Status code to match against HTTP Response's Status line.
Host Port Start	The port start value for matching against HTTP request host port. Specify both Host Port Start and Host Port End, even if both values are equal.
Host Port End	The port end value for matching against HTTP request host port. Specify both Host Port Start and Host Port End, even if both values are equal.
Accept	String to match against HTTP Request's Accept header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

Table 9-35 Rule Condition Parameters

Parameter	Description
Content Type	String to match against HTTP Request's Content-type header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Host	String to match against HTTP Request's Host header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Media	Media types to match against response payload: ■ all-video ■ progressive-video – FLV – MP4 – WEBM ■ Abr-video – DASH – HLS – HDS
Referer	String to match against HTTP Request's Referer field: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Request URI	String to match against HTTP Request's URI field: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

Table 9-35 Rule Condition Parameters

Parameter	Description
Response Header	Enter the Header Name for matching against the HTTP response String to match against HTTP response header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Response Payload	Signature to match against response payload at the specific offset. Enter a HEX string without whitespace. Specify an offset in the response payload to look for the signature.
User Agent	String to match against HTTP Request's User-agent header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many Rule Conditions as needed.

7 Click the **Save** icon.

HTTP URL Rewrite

The HTTP URL Rewrite object provides a URL substitution function. Rewritten URLs can provide customized response for certain requests, such as shorter and more relevant-looking links to web pages.

Each URL requested in a WSP or HTTP request is checked for a possible substitution against the configured list. The list contains target URLs mapped, one to one, against substitution URLs. Both the target URLs and substitution URLs must contain the host name (which can include a port number) and can contain any number of segments delimited with the "/" character. The substitution is performed before any other URL-dependent action.

To add an HTTP URL Rewrite:

1 Use any of the following methods to add an HTTP URL Rewrite:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **HTTP URL Rewrite**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New HTTP URL Rewrite**.

2 Configure the parameters as follows:

Table 9-36 Rewrite Rule Parameters

Parameter	Description
Name	Enter a Rewrite Rule name.

Table 9-36 Rewrite Rule Parameters

Parameter	Description
Request URL	Specifies the regular expression pattern to match the HTTP Request URL. Must contain a host name and can contain a port number and URL path. Can contain any number of segments delimited with the "/" character. Omit ‘http://’ from the Request URL pattern. Enclose URLs in double quotation marks. Use parentheses in the Request URL pattern to internally create back-references. You can reference them using the strings $N (1 <= N <= 9) for creating the Substitution URL. For example: Request URL: xyz.com/products/([0-9]+)/(\w+) Substitution URL: xyz.com/show_a_product.php?product_id=$1/$2
Substitution URL	Substitution string to replace the matched HTTP Request URL. Must contain a host name and can contain a port number and URL path. Can contain any number of segments delimited with the "/" character. Omit ‘http://’ from the Substitution URL pattern. Enclose URLs in double quotation marks. Supports back-reference using the strings $N (1 <= N <= 9).
Priority	Rewrite rule priority
Last	Specifies to apply this rule last in this profile, if matched Request URL. When set, any lower priority rules within the profile are ignored.

3 Click the **Save** icon.

Insertion Object List

Use this object to configure an Insertion Object List.

To add an Insertion Object List:

1 Use any of the following methods to add an Insertion Object List:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Insertion Object List**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Insertion Object List**.

2 Configure the parameters as follows:

Table 9-37 Insertion Object List Parameters

Parameter	Description
Name	Object List name
Admin State	Admin State: ■ enabled ■ disabled

3 In **Insertion Object**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-38 Insertion Object Parameters

Parameter	Description
Name	Object name
Admin State	Enable/disable the insertion object: ■ enabled ■ disabled

Table 9-38 Insertion Object Parameters

Parameter	Description
Type	Content insertion object type: ■ image ■ link ■ video
Title	Title for the content insertion object
Click Through URL	Specify the click through URL.
Object Location	Object Location: ■ filename ■ URL Enter the filename of the local object or the URL of the remote object.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many insertion object as needed.

7 Click the **Save** icon.

IP List

Use this object to configure an IP Address List.

To add an IP Address List:

1 Use any of the following methods to add an IP Address List:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **IP Address List**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New IP List**.

2 Configure the parameters as follows:

Table 9-39 IP List Parameters

Parameter	Description
Name	IP Address list name
User Description	IP Address list Description

3 In **IP Address**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-40 IP Address Parameters

Parameter	Description
Address	IP Address (v4) or prefix (v4/v6)
User Description	IP Address description

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many IP Addresses as needed.

7 In **IP Range**, click the **Create** icon.

8 Configure the parameters as follows:

Table 9-41 IP Range Parameters

Parameter	Description
Start Address	Start IP Address (v4) or prefix (v4/v6)
End Address	End IP Address (v4) or prefix (v4/v6)
User Description	IP Address range description

9 Click **Add**.

10 Repeat step 7 through step 9 to add as many IP Ranges as needed.

11 Click the **Save** icon.

LDAP Interface

Use this object to configure the Lightweight Directory Access Protocol (LDAP) services.

- Feature Group – Enable and configure LDAP feature group attributes such as the action to take if a match appears in the blacklist, define a list of LDAP attributes, and define enforcement rules.
- Remote Server – A list of configured remove servers with the same or different priority.
- Profile – Enable and configure LDAP profile attributes such as the default action to take if LDAP failure occurs, feature groups for this profile, network context for the LDAP server, priority, and the remote LDAP servers for this profile.

The Lightweight Directory Access Protocol (LDAP) is an application protocol for reading and writing directories over an IP network. It uses TCP/IP port 389 and UDP port 389. It is used to query and update an X.500 directory. LDAP is specified in a series of IETFs and RFCs, using the description language ASN.1. Affirmed Networks supports the latest specification, RFC 4511, Version 3.

LDAP Server

To add an LDAP Server:

1 Use any of the following methods to add an LDAP Server:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **LDAP Server**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New LDAP Server**.

2 Configure the parameters as follows:

Table 9-42 LDAP Server Parameters

Parameter	Description
Name	LDAP server name.

Table 9-42 LDAP Server Parameters

Parameter	Description
Admin State	Admin state: ■ enabled ■ disable
Password	LDAP server bind password
Address	LDAP server IP address
Port	LDAP server port
Timeout	LDAP server timeout value, in seconds
Base DN	LDAP server base distinguished name string
Bind Retry	LDAP Server bind retry
Bind DN	LDAP Server bind distinguished name string
Idle Timeout	LDAP server connection idle timeout (in seconds) used to ping the server. If no activity occurs on this server connection for more than this idle timeout value, a abandon message is sent to the server serving as a ping. The response from server is to reset the timer on monitoring this connection. Otherwise, the connection is closed.
Version	LDAP Server version

3 Click the **Save** icon.

LDAP Profile

If the priority of the servers is the same in a given profile, the LDAP agent performs round-robin load balancing. If the priority of the servers differs, the LDAP agent uses priority-based load balancing.

The LDAP agent performs the following actions based on the priority of the servers in a given profile.

LDAP Agent Action	Same Priority	Different Priority	Mix of Priorities
Tries the next active client connection for each LDAP search request in a round robin fashion. ■ If no active client connections exist, the LDAP agent reverts to the current active client server connection. ■ If all client connections are inactive in a given priority, the LDAP agent tries the next priority servers in the server configuration.	X		X
If all client connections are inactive in entire profile, the LDAP agent retries the servers from the server configuration Entry Index order since priority is same for all servers).	X		
Tries the same active client connection for each LDAP search request as long the server connection is in service and no other server client connections are active in that priority group.		X	X
If the current client connection is inactive, the LDAP agent tries the next priority active client connections.		X	X
If all client connections are inactive, the LDAP agent retries the servers from priority order.		X	X

To add an LDAP Profile:

1 Use any of the following methods to add an LDAP Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **LDAP Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New LDAP Profile**.

2 Configure the parameters as follows:

Table 9-43 LDAP Profile Parameters

Parameter	Description
Name	LDAP Profile name.
Admin State	Admin state: ■ enabled ■ disable
Network Context	Network Context to use to connect to the LDAP server.
Loopback IP	Select the Loopback IP Address from the configured Network Context to be used as the local address, when connecting to the servers. Because a server may be used by different profiles, the same Loopback IP Address must be used in all profiles that use the same Network Context, configured or not. The Loopback IP Address must already exist. Create it at Network Context > *name* > Loopback IP.
The LDAP agent applications (that is, GW/HTTP Proxy) set the LDAP query key values based on the Lookup Key Type and Lookup Key String	
Lookup Key String	Enter the LDAP lookup key string
Lookup Key Type	Select the lookup key type: ■ ue-msisdn ■ ue-ip-address
Sort Attribute Name	Enter the LDAP attribute name to use to sort the search results. If not specified, the results are given in the order in which they are received from LDAP server.
Sort Order	Sort order to be used to sort multiple entries in the response from the server, based on the configured Sort Attribute Name. The entries are sorted as follows: ■ all (default) – MCC selects all attributes (up to 100) from matching entries in the order in which they are received. If no Sort Attribute Name is configured, all entries are matching entries. ■ ascending-first – MCC selects the first matching entry after all entries are sorted in ascending order based on the Sort Attribute Name. ■ descending-first – MCC selects the first matching entry after all entries are sorted in descending order based on the Sort Attribute Name. ■ first – MCC selects the first server that has a matching attribute based on the Sort Attribute Name.
Action	Action to take in case of permanent LDAP failure: ■ Allow ■ Block

Table 9-43 LDAP Profile Parameters

Parameter	Description
Fields when Action is set to Block:	
SMS Notification	SMS Notification text
MMS Response	MMS Error Response
Feature Group	Select the Feature Group(s) to add to the profile. To select a Feature Group, drag and drop it from the Available list to the Selected list.
Server	Select the LDAP server(s) for the profile. To select an LDAP serve, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

LDAP Feature Group

To add an LDAP Feature Group:

1 Use any of the following methods to add an LDAP Feature Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **LDAP Feature Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New LDAP Feature Group**.

2 Configure the parameters as follows:

Table 9-44 LDAP Feature Group Parameters

Parameter	Description
Name	LDAP Feature Group name.
Admin State	Admin state: ■ enabled ■ disable

Table 9-44 LDAP Feature Group Parameters

Parameter	Description
Enforce	Mark the checkbox to have the attributes checked, even in cases of parameter error.
Action	LDAP action to take if attribute list and MMS blacklist matches: ■ Allow ■ Block
Fields when Action is set to Block:	
SMS Notification	SMS Notification text
MMS Response	MMS Error Response

3 In **Attributes**, click the **Create** icon.

4 Configure the list of LDAP attributes to be checked upon LDAP response, as follows:

- **Attribute Name** – Enter the attribute name.
- **Priority** – Enter the priority.
- **Attribute Value**: Specify the attribute type and its value:
  - String value: Specify the LDAP attribute value string to be checked against its value in the LDAP response
  - Date value: Specifies to check LDAP attribute value in the LDAP response against the current date
  - Destination Regex: Specify the Regular Expression to be checked against the destination address
  - MMS Blacklist: Select the MMS Blacklist to be checked against the destination address
- **String** – Specify the string to match.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many Attributes as needed.

7 Click the **Save** icon.

Loopback IP List

Use this object to configure a Loopback IP List.

To add a Loopback IP List:

1. Use any of the following methods to add a Loopback IP List:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category**.

   c. Click **Loopback IP List**.

   d. Click the **Create** icon.

   Build a Workflow:

   a. Click the **Build a Workflow** tab.

   b. Expand **Functions**.

   c. Click the **New** tab.

   d. Click **New Loopback IP List**.

2. Configure the parameters as follows:

   - **Name** – Enter the Loopback IP List name.

3. In **Network Context**, click the **Create** icon.

4. Configure the parameters as follows:

   - **Name** – Enter the Network Context that contains the loopback IP addresses.
   - **Loopback IP** – Select the Loopback IP addresse(s) to add to the list. To select a Loopback IP address, drag and drop it from the Available list to the Selected list.

5. Click **Add**.

6. Click the **Save** icon.

Malware Category

To add a Malware Category:

1. Use any of the following methods to add a Malware Category:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category**.

   c. Click **Malware Category**.

   d. Click the **Create** icon.

   Build a Workflow:

   a. Click the **Build a Workflow** tab.

   b. Expand **Functions**.

   c. Click the **New** tab.

   d. Click **New Malware Category**.

2. Configure the parameters as follows:

3. Configure the parameters as follows:

   - **Name** – Malware Category group name

4. In **Malware Category**, click the **Create** icon.

5. Configure the parameters as follows:

   - **Name** – Select the Malware category name:
     - malware-domain
     - malware-attack-botnet
     - malware-spyware
     - malware-object
     - potential-malware-victim

6. Click **Add**.

7. Repeat step 4 through step 6 to add as many Malware Categories as needed.

8. Click the **Save** icon.

Multimedia Messaging Service

Use this object to configure a Multimedia Messaging Service (MMS). MMS provides messaging capabilities for delivery of multimedia messages, composed of text, audio, graphics, photographs, and other media types on a network.

MMS packets can be routed among a pool of configured Multimedia Messaging Service Centers, based on:

- MMS originator and destination address
- MMS Short code value, range, and regex (Regular Expression)
- MMSC Load balance suffix range (Round-Robin)
- MMSC Message ID suffix
- Default MMSC in the group
- Backup MMSC

MMSCs are evaluated based on priority.

The MCA20 supports routing of all MM1, MM3, and MM4 PDUs to/from the MMSCs application server.

Multimedia Messaging Service Center

To add a Multimedia Messaging Service Center:

1 Use any of the following methods to add a Multimedia Messaging Service Center:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Mmsc**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Mmsc**.

2 Configure the parameters as follows:

Table 9-45 Multimedia Messaging Service Center Parameters

Parameter	Description
Name	Multimedia Messaging Service Center name.
Priority	Multimedia Messaging Service Center priority
URL	Multimedia Messaging Service Center's URL location. The current URL is replaced with this URL.
Transcode	Mark the checkbox to enable message transcoding for this MMSC. When an MMS message is downloaded, transcode it according to the UA Profile. See UA Profile.
Message ID Suffix	Message ID suffix for the MMSC.
Fall Back MMSC	Select the backup MMSC.
Host	MMSC hostname (for example, mms.era.pl)
Address	IP Address for the MMSC, can be IP v4 or IP v6.
Port	Port for the MMSC.
Maximum Message Size	Maximum message size, in KB.
Error Response	Enter the error response when the maximum message size is exceeded
Maximum Number Recipients	Maximum number of recipients
Error Response	Enter the error response when the maximum number of recipients is exceeded

3 In **Short Code Range**, click the **Create** icon.

4 Configure the parameters as follows:

- **Range** – Enter the Start Value and End Value that represents the Short Code range used to route MMS packets.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many Short Code ranges as needed.

7 In **Short Code Value**, click the **Create** icon.

8 Configure the parameters as follows:

- **Value** – Enter the Short Code value.

9 Click **Add**.

10 Repeat step 7 through step 9 to add as many Short Code values as needed.

11 In **Short Code Regex**, click the **Create** icon.

12 Configure the parameters as follows:

- **Regex** – Enter the Short Code Regular Expression.

13 Click **Add**.

14 Repeat step 11 through step 13 to add as many Short Code Regular Expressions as needed.

15 In **Load Balance Suffix**, click the **Create** icon.

16 Configure the parameters as follows:

- **Range** – Enter the Start Value and End Value that represents the Load Balance Suffix range.

17 Click **Add**.

18 Repeat step 15 through step 17 to add as many Load Balance Suffixes as needed.

19 Click the **Save** icon.

Multimedia Messaging Service Center Group

To configure a group of MMSCs:

1 Use any of the following methods to add a Multimedia Messaging Service Center Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Mmsc Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Mmsc Group**.

2 Configure the parameters as follows:

- **Name**: Multimedia Messaging Service Center group name
- **Reject Invalid MMS Requests**: Mark the checkbox to reject GET requests if the host does not match MMSC host configuraiton.

- **Mmsc**: Select the Multimedia Messaging Service Center(s) to add to the group. To select an MMSC, drag and drop it from the Available list to the Selected list.

  Mark the **Default** checkbox to set it as the default MMSC in the group.

3 Click the **Save** icon.

MMS Error Response

Use this object to configure error response status and text in case of rejected MM requests:

To configure MMS error response:

1 Use any of the following methods to add an MMS error response:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Mms Error Response**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New MMS Error Response**.

2 Configure the parameters as follows:

Table 9-46 Error Response Parameters

Parameter	Description
Name	Error response name
Default Error Response	
User Agent Prefix	Select the User Agent Prefix
Response Status	Select the MM-PDU X-MMS Response Status
Response Text	Enter the MM-PDU X-MMS Response Text

3 In **User Agent Prefix**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-47 User Agent Prefix Parameters

Parameter	Description
User Agent Prefix	Enter the User Agent Prefix
Response Status	Select the MM-PDU X-MMS Response Status, such as Error-service-denied
Response Text	Enter the MM-PDU X-MMS Response Text, such as Protection of minors: forbidden

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many User Agent Prefixes as needed.

7 Click the **Save** icon.

MMS Blacklist

Use this object to configure a list of destination addresses to match in To/Cc/Bcc.

To configure an MMS destination address blacklist:

1 Use any of the following methods to add an MMS blacklist:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Mms Blacklist**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New MMS Blacklist**.

2 Configure the parameters as follows:

- **Name**: Blacklist name
- **LDAP in Use**: Mark the checkbox to specify that LDAP query is in use

3 In **Destination Address**, click the **Create** icon.

4 Configure the parameters as follows:

- **Regex**: Regular expression to match the destination address, such as ^900[0-9][0-9][0-9]$

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many User Agent Prefixes as needed.

7 Click the **Save** icon.

MMS MM3 Profile

The MM3 interface allows the MMSC to exchange messages with external servers such as E-mail servers and SMSCs. The interface is typically based on IP-based E-mail protocols (such as SNMP).

To configure an MMS MM3 Profile:

1 Use any of the following methods to add an MMS MM3 Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **MMS MM3 Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New MMS MM3 Profile**.

2 Configure the parameters as follows:

Table 9-48 MM3 Profile Parameters

Parameter	Description
Name	MM3 Profile name
SMTP Server Name	SMTP Server domain name
SMTP Server Port	SMTP Server Port
PC Profile Filename	The PC-Profile file to be used for transcoding. Click **Choose PC Profile File** to select a PC Profile that has already been uploaded. Select the file and click **Select**. To upload a PC Profile file, click **Browse** in the Upload File field and select the file. Click **Upload**.

3 Click the **Save** icon.

MMS STI Profile

Use this object to configure a Standard Transcoder Interface profile.

To configure an MMS STI Profile:

1 Use any of the following methods to add an MMS STI Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **MMS STI Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New MMS STI Profile**.

2 Configure the parameters as follows:

Table 9-49 STI Profile Parameters

Parameter	Description
Name	STI Profile Name
URI	SRI Profile URI

3 Click the **Save** icon.

Packet Filter

The Packet Filter function defines the packet filter or service data flow configuration identified by:

- User Equipment IP address range
- Network IP address range
- User Equipment port range
- Network port range
- IP Protocol
- Flow initiator

To add a Packet Filter:

1 Use any of the following methods to add a Packet Filter:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Packet Filter**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Packet Filter**.

2 Configure the parameters as follows:

Table 9-50 Packet Filter Parameters

Parameter	Description
Name	Packet Filter name
IP Version	IP Version: ■ V4 only ■ V6 only ■ V4 or V6
UE IP Address Start	User equipment IPv4 address range start (inclusive)
Network IP Address Start	Network equipment IPv4 address range start (inclusive)

Table 9-50 Packet Filter Parameters

Parameter	Description
UE IP V6 Address Start	User equipment IPv6 address range start (inclusive)
Network IP V6 Address Start	Network equipment IPv6 address range start (inclusive)
UE Port Start	User equipment port range start value (valid for protocol TCP (6), UDP (17), SCTP (132) only)
UE Port End	User equipment port range end value (valid for protocol TCP (6), UDP (17), SCTP (132) only)
Network Port Start	Network equipment port range start value (valid for protocol TCP (6), UDP (17), SCTP (132) only)
Network Port End	Network equipment port range end value (valid for protocol TCP (6), UDP (17), SCTP (132) only)
Protocol	IP Protocol values, defined in usr/include/netinet/in.h
Initiator	Initiator of the connection: ■ UE: User equipment ■ Network ■ Both
UE IP Address End	User equipment IPv4 address range end (inclusive)
Network IP Address End	Network equipment IPv4 address range end (inclusive)
UE IP V6 Address End	User equipment IPv6 address range end (inclusive)
Network IP V6 Address End	Network equipment IPv6 address range end (inclusive)
Min Uplink TTL	Minimum value of the connection Time to Live. This setting enables Operators to differentiate charging based on minimum TTL values by configuring different charging groups with different service rules containing packet filters with TTL values to treat connections with different TTL differently.
Max Uplink TTL	Maximum value of the connection Time to Live. This setting enables Operators to differentiate charging based on maximum TTL values by configuring different charging groups with different service rules containing packet filters with TTL values to treat connections with different TTL differently.

3 Click the **Save** icon.

QoS

QoS configures default and network Quality of Service characteristics associated with subscribers.

To add a QoS:

1 Use any of the following methods to add a QoS:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **QoS**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New QoS**.

2 Configure the parameters as follows:

Table 9-51 QoS Parameters

Parameter	Description
Name	QoS name
Measurement Unit	Rate Measurement unit: ■ Kbps ■ Mbps ■ Gbps
Apn Uplink Ambr	Uplink Access Point Name Aggregate Maximum Bit Rate
Apn Downlink Ambr	Downlink Access Point Name Aggregate Maximum Bit Rate
Uplink Burst Size	Uplink Burst Size, in Kbytes
Downlink Burst Size	Downlink Burst Size, in Kbytes

Table 9-51 QoS Parameters

Parameter	Description
QCI	QoS Class Identifier: ■ 1: Operator controlled Voice Calling ■ 2: Operator controlled Video Calling ■ 3: Operator controlled Real-time Gaming ■ 4: Operator controlled Streaming of Pre-recorded Video ■ 5: Signaling for Operator controlled applications ■ 6: Websites prioritized by Operator ■ 7: Operator controlled Live Video Streaming or Interactive Gaming ■ 8: All other traffic for premium subscriber ■ 9: All other traffic for regular subscriber
ARP	Allocation and Retention Priority

3 Click the **Save** icon.

SCTP Profile

Use this object to configure an SCTP (Stream Control Transmission Protocol) Profile.

To add an SCTP Profile:

1 Use any of the following methods to add an SCTP profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **SCTP Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New SCTP Profile**.

2 Configure the parameters as follows:

Table 9-52 SCTP Profile Parameters

Parameter	Description
Name	Service Rule name
Init Retry	Max number of attempts to retransmit the init message after which the attempted association is terminated.
Heartbeat Interval	Periodic time interval (in msecs) at which the SCTP heart beat message are sent. Value zero disables SCTP heart beats.
Max Heartbeat Retransmit	Maximum number of attempts to retransmit the heart beat message and if the peer fails to respond, the association is terminated.
RTO Initial	The initial retransmission time out value. Subsequent SCTP RTO will be recomputed starting from this value.
RTO Min	The minimum RTO value (in msecs) that any subsequent recomputed RTO may never go below.
RTO Max	The maximum RTO value (in msecs) that any subsequent recomputed RTO may never exceed.

3 Click the **Save** icon.

Service Rule

The Service Rule is associated with a specific Service Data Flow, protocol analyzer, HTTP rule group, Protocol Application Rule Group, and/or Time of Day rule group. Service Rules are referenced in other services, such as QoS Flow, Rating Group (charging), Subscriber Firewall Flow, Proxy HTTP IP Flow, and so on. Each rule has a unique service data flow identifier and an optional (non-unique) Correlation Identifier to be logged in CDR/EDR.

For a Service Rule to match, all of the following filters (if specified) must match:

- At least one Packet Filter
- At least one Time of Day Rule
- At least one HTTP Content Rule
- At least one Protocol Application Rule Group Rule. If multiple rules are specified in a rule group, at least one of the rules in the rule group must match.

Service Rules support the following separate categorization of traffic:

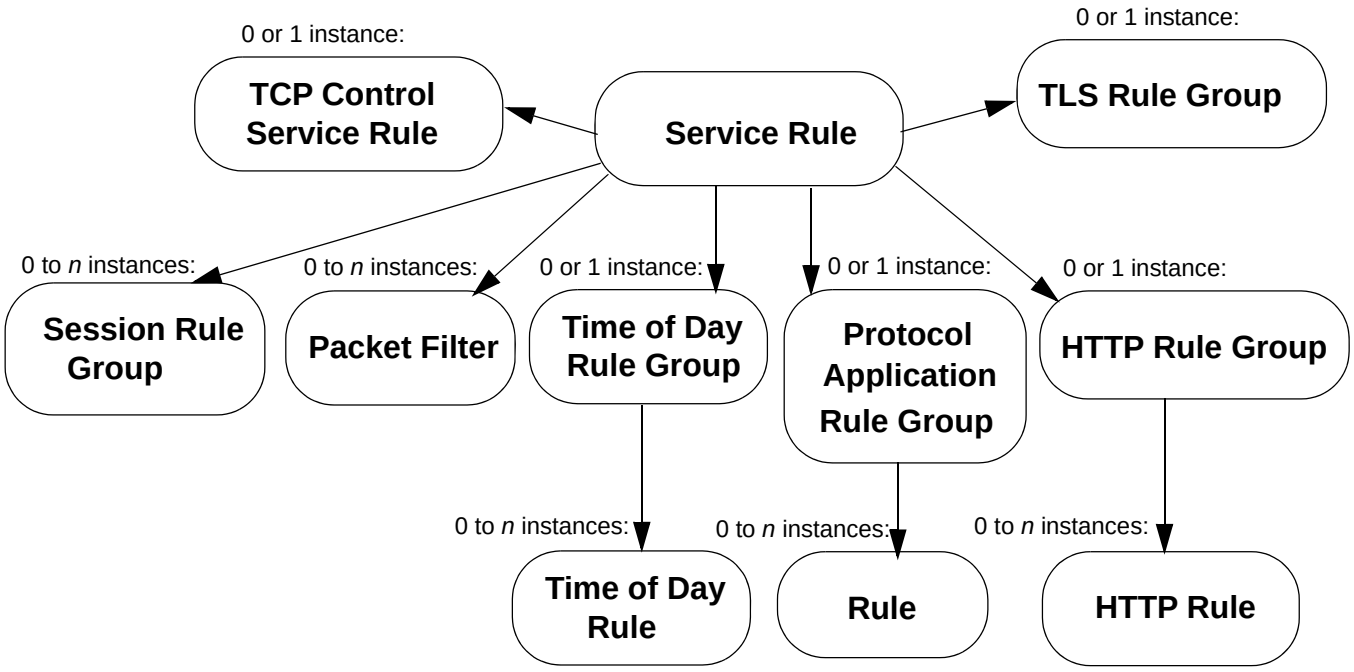
- TCP control traffic – Defined as TCP packets with IP total length equal to the IP header plus the TCP header.
- TCP data traffic and non-TCP traffic

This feature requires Service Rules to be paired to account for both types of traffic; one is the TCP Control Service Rule, one is the TCP Data Control Service Rule.

The following figure illustrates the components of Service Rule.

Figure 9-23 Service Rule Components

Note: TCP Control Service Rule can be paired only with a TCP Data Service Rule.



To add a Service Rule:

1 Use any of the following methods to add a Service Rule:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Service Rule**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Service Rule**.

2 Configure the parameters as follows:

Table 9-53 Service Rule Parameters

Parameter	Description
Name	Service Rule name
Admin State	Admin state: ■ enabled ■ disable
Priority	Service Rule priority Allows service flows to select a service rule from a list of service rules based on priority.
Service Data Flow ID	Numerical identifier for the Service Rule The identifier does not have to be unique. Operators can configure multiple Service Rules with the same Service Data Flow ID so that multiple PCC rules can map to one service ID. When generating CDRs, MCC creates a separate service container for each service ID so associating multiple PCC rules (Service Rules) with the same service ID (SDF ID) reduces the number of service containers created in each CDR.
Correlation Identifier	Non-unique numerical identifier for the Service Rule
TCP Filter	Specifies the TCP accounting category of the Service Rule: ■ all: accounts for all traffic ■ data: accounts for TCP data traffic and non-TCP traffic ■ control: accounts for TCP control traffic (packets with IP total length equal to the IP header plus the TCP header) When set to Data or All, the Service Rule may specify Packet Filter(s), a Time of Day Rule Group, a Protocol Application Rule Group, and an HTTP Rule Group. When set to Control, the Service Rule cannot have child objects. Multiple TCP Data Service Rules can link to the same TCP Control Service Rule.
TCP Control Service Rule	When **TCP Filter** is set to Data, specifies the linked TCP Control Service Rule for accounting (required).
Time of Day Rule Group	Select the Time of Day Rule Group to bind with the Service Rule. It specifies the days and times for service rule activation. The Time of Day Rule Group must already exist. See Time of Day Rule Group.

Table 9-53 Service Rule Parameters

Parameter	Description
Protocol Application Rule Group	Select the Protocol Application Rule Group to bind with the Service Rule. The Protocol Application Rule Group must already exist. See Protocol Application Rule Group (8.4 and later MCC version). ***Note:*** *If the Service Rule specifies both an Application Rule Group and an HTTP rule group, and the Application Rule Group specifies a protocol, it must be protocol HTTP. Or you can leave the protocol unspecified and configure an application instead.*
HTTP Rule Group	HTTP rule group (L7 HTTP Header based filter) to bind with the Service Rule (Optional) The HTTP rule group must already exist. See HTTP Rule Group.
Service Activation	Specifies when to use or skip the service flow for packet classification: ■ always on - always use this service flow for classification ■ external activation - use the activation state of the service flow to determine whether to use or skip the service flow for packet classification.
TLS Rule Group	The TLS Rule Group for matching on SNI (Server Name Indication) and Server certificate CN (Common Name) fields of a TLS handshake. The TLS Rule Group must already exist. See TLS Rule Group.
Domain Rule Group	Optional Domain name rules. The Domain Rule Group must already exist. See Domain Rule Group.
Session Rule Group	Optional Session name rules. The Session Rule Group must already exist. See Session Rule Group.
PCC Rule Name	Applies when **Service Activation** is set to **external activation**. The Charging Rule name from PCRF to support service rule grouping. This option allows for multiple service rules with the same name but with different priorities and different correlation IDs. For example, you can apply the same PCC Rule Name to a set of service rules (some with Packet Filters, some with HTTP Rule Groups, and some with TLS Groups), all of which can be activated by a single Charging Rule Name installation from the PCRF. You can activate a list of service rules that share the same PCC Rule Name and apply the configuration to the following objects: ■ Online/offline rating group ■ Metering rating group ■ QoS flow You can associate a maximum of 32 service rules with one Service Rule Group.

Table 9-53 Service Rule Parameters

Parameter	Description
Install Default Bearer Packet Filters on UE	Specifies whether the TFT defined in the charging action should be sent to the UE: ■ enabled ■ disable When enabled, the PGW does not send packet filters included in the service rule to UE.
Packet Filter	Select the packet filter(s) to bind with the Service Rule. This packet filter must already exist. See Packet Filter. To select a packet filter, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Session Rule Group

Use this object to configure a list of rule groups that can be configured for RAT type, MBR matching, and/or device characteristics.

Video adaptation and video pacing use a Service Rule to match a Serving Policy. When HTTP proxy receives an HTTP response from the origin server, MCC adjusts the video adaptation QoE or video-pacing attributes based on the UE RAT type or bandwidth. MCC supports dynamic video adaption and video pacing adjustment according to the RAT type IE in the RADIUS accounting start message and the UE real-time throughput.

And, Operators can use device characteristics to configure differentiated rate-limiting bit rates based on device-type or device screen size.

To add a Session Rule Group:

1 Use any of the following methods to add a Session Rule Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Session Rule Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Session Rule Group**.

2 Click **Service Rule Group**.

3 Configure the parameter as follows:

- **Name** – Enter a Session Rule Group name.

4 To add a Session rule, in **Rule**, click the **Create** icon.

To modify a Session rule, select the instance and click the **Modify** icon.

5 Configure the parameters as follows:

Table 9-54 Rule Condition Parameters

Parameter	Description
Name	Rule name

Table 9-54 Rule Condition Parameters

Parameter	Description
RAT Type	RAT (Radio Technology) used by the mobile device: ■ E-UTRAN ■ GAN ■ GERAN ■ HSPA-EV ■ NON-3GPP ■ UTRAN ■ VIRTUAL ■ WLAN ■ NBIOT-EUTRAN
Device Type	Device type from the device database list: ■ HANDHELD ■ FEATURE-PHONE ■ SMART-PHONE ■ MODEM ■ DONGLE ■ TABLET ■ VEHICLE ■ CONNECTED-DEVICE ■ ROUTER ■ MODULE ■ EBOOK ■ FEMTO-AP
Max Screen Height	Maximum screen height of the device
Max Screen Width	Maximum screen width of the device
Min Screen Height	Minimum screen height of the device
Min Screen Width	Minimum screen width of the device
Congestion Level	Congestion level for applying optimization: ■ Mild ■ Moderate ■ Severe
Downlink MBR	Downlink Maximum Bit Rate range, in Kbps. Specify a start and end value.

Table 9-54 Rule Condition Parameters

Parameter	Description
Device Make	String to match against the device name: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Device Model	String to match against the device model: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

6 Click **Add** (or **Modify)**.

7 Repeat step 4 through step 6 to add as many session rules as needed.

8 Click the **Save** icon.

Short Message Service

Use this object to configure a Short Message Service. The Short Message Service feature enables Operators to configure the SMS text message, a group of Short Message Service Centers, and a Short Message Service Center profile.

Short Message Service Center Profile

To add a Short Message Service Center Profile:

1 Use any of the following methods to add a Short Message Service Center Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **SMSC Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New SMSC Profile**.

2 Configure the parameters as follows:

Table 9-55 Short Message Service Center Profile Parameters

Parameter	Description
Name	Short Message Service Center name.
Username	User name to log onto the Short Message Service Center.
Password	Password to log onto the Short Message Service Center.
IP Address	Short Message Service Center IP address
Port	Short Message Service Center port

3 Click the **Save** icon.

Short Message Service Center Group

To configure a group of SMSCs:

1 Use any of the following methods to add a Short Message Service Center Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **SMSC Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New SMSC Group**.

2 Configure the parameters as follows:

Table 9-56 Short Message Service Center Group Parameters

Parameter	Description
Name	Short Message Service Center group name.
Network Context	Network Context to use.
Loopback Address	Select the Loopback IP Address to add to the group. To select a Loopback IP Address, drag and drop it from the Available list to the Selected list.
Short Message Service Profile	Select the Short Message Service Profile(s) to add to the group. The SMS Profile must already exist. See Short Message Service Center Profile. To select a Short Message Service Profile, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Short Message Service Notification

To configure SMS notification text messages:

1 Use any of the following methods to add a Short Message Service notifications:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **SMS Notification**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New SMS Notification**.

2 Configure the parameters as follows:

Table 9-57 Short Message Service Notification Parameters

Parameter	Description
Cause	Message cause

Table 9-57 Short Message Service Notification Parameters

Parameter	Description
Brand	Brand/Market Segment
SMS Text	SMS text

3 Click the **Save** icon.

Static DNS Map

The static DNS map is used for DNS lookups in HTTP Proxy. The static DNS map configures a set of IP addresses and a host to avoid performing a DNS lookup through configured DNS server(s). When an HTTP Proxy service specifies a static DNS map, it uses the map's configured IP Address list to open server connections for HTTP request.

To add a Static DNS Map:

1 Use any of the following methods to add a Static DNS Map:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Static DNS Map**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New DNS Map**.

2 Configure the parameter as follows:

Table 9-58 Static DNS Map Parameters

Parameter	Description
Name	Static DNS map name
Network Context	Network Context associated with the static map
Returned Addr Order	Specifies how the returned host address list is constructed: ■ static ■ round-robin

3 In **Host**, click the **Create** icon.

4 Configure the parameters as follows:

- **Host** – Specify the Static DNS host
- **IP Address** – Specify the Host IP Address.

5 Click **Add**.

6 Repeat step 3 through step 5 to add additional Addresses as needed. You can specify up to 5 IPv4 addresses and 5 IPv6 addresses.

7 Click the **Save** icon.

TCP Optimization Profile

TCP optimization features are applied to data traffic passing through the Multi Protocol Proxy function. The TCP Optimization Profile specifies changes to the TCP/IP stack targeted to improve throughput and user experience in the mobile network.

To add a TCP Optimization Profile:

1 Use any of the following methods to add a TCP Optimization Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **TCP Optimization Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New TCP Optimization Profile**.

2 Configure the parameters as follows:

Table 9-59 TCP Optimization Profile Parameters

Parameter	Description
Receive Mss	TCP received maximum segment size, in bytes
Fast Retransmit Dupacks	TCP number of duplicate acknowledgments to trigger the fast retransmit algorithm.

Table 9-59 TCP Optimization Profile Parameters

Parameter	Description
Congestion Control	TCP Congestion Control algorithm: ■ bic ■ cubic ■ highspeed ■ htcp ■ hybla ■ illinois ■ lp ■ reno ■ scalable ■ vegas ■ veno ■ westwood ■ yeah
Send Buffer Size	TCP send buffer size, in bytes
Recv Buffer Size	TCP receive buffer size, in bytes
Initial Congestion Window	TCP initial congestion window, in bytes. This feature prevents the congestion control algorithm from activating prematurely for wireless links with higher latency.
Window Size	TCP window size, in bytes
Slow Start	TCP Slow Start After Idle option: ■ enabled ■ disabled Disabling this feature causes the congestion window to time out after an idle period, preventing slow start algorithm for persistent connections
Nagle Algorithm	TCP Nagle Algorithm option: ■ enabled ■ disabled Enabling this feature reduces the overhead in the wireless link and allows combining small packets at the source.
Recv Buffer Auto Tuning	TCP Receive Buffer Auto-Tuning option (enable or disable auto-tuning of TCP window): ■ enabled ■ disabled

3 Click the **Save** icon.

Time of Day Rule Group

The Time of Day Rule Group defines a group of rules used to provide time-of-day filtering. The Time of Day Group contains Time of Day filters, each keyed by Day, Start Time, and End Time. If one of the Time of Day filters matches, the Time of Day Specification is matched.

To add a Time of Day Rule Group:

1 Use any of the following methods to add a Time of Day Rule Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Time of Day Rule Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New Time of Day Rule Group**.

2 Configure the parameters as follows:

Table 9-60 Time of Day Rule Group Parameters

Parameter	Description
Name	Time of Day Rule Group name
Day	Select the day.
Start Time	Enter the start time.
End Time	Enter the end time.

3 Click the **Save** icon.

TLS Rule Group

The TLS Rule Group defines a set of rules for matching on SNI (Server Name Indication) and Server certificate CN (Common Name) fields of a TLS handshake. When a match is found, specific actions or service(s) can be applied, based on where the Service Rule is used, such as QoS and charging policies for HTTPS traffic.

Within a rule, you can specify SNI or Common Name matching or both. If you specify both, each must match for the rule to be considered a match.

To add a TLS Rule Group:

1 Use any of the following methods to add a TLS Rule Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **TLS Rule Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New TLS Rule Group**.

2 Configure the parameter as follows:

- **Name** – Enter a TLS Rule Group name.

3 To add a TLS rule, in **Rule**, click the **Create** icon.

To modify a TLS rule, select the instance and click the **Modify** icon.

4 Configure the parameters as follows:

Table 9-61 Rule Condition Parameters

Parameter	Description
Rule Name	Rule Condition name

Table 9-61 Rule Condition Parameters

Parameter	Description
SNI	String to match against the incoming Server Name Indication: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
SNI URL List	URL List to match against the incoming Server Name Indication.
Server Common Name	String to match against the incoming Common Name: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

5 Click **Add** (or **Modify)**.

6 Repeat step 3 through step 5 to add as many TLS rules as needed.

7 Click the **Save** icon.

TLS Termination Policy

The TLS Termination Policy configures policies for terminating TLS connections on behalf of Operator's or Operator Partners' servers. The policy is applied when TLS connection's destination IP address matches the network context and one of the configured server addresses in the TLS Termination Policy.

The policy must also include server's certificate and private key that authenticate TLS connections on behalf of the server. If the private key is password-protected (recommended) a key passphrase must also be configured.

Server certificates and private keys configured in the TLS Termination Policy must be present in the /public/content/tls/servercerts/ folder on the MCM.

To add a TLS Termination Policy:

1 Use any of the following methods to add a TLS Termination Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **TLS Termination Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New TLS Termination Policy**.

2 Configure the parameters as follows:

Table 9-62 TLS Termination Policy Parameters

Parameter	Description
Name	TLS Termination Policy name
Network Context	Network Context through which the TLS server is reachable.

3 To add a TLS server IP Address, in **Server IP**, click the **Create** icon.

To modify a TLS server IP Address, select the instance and click the **Modify** icon.

4 Configure the parameter as follows:

- **IP Address** – Enter the TLS server IP address.

5 Click **Add** (or **Modify)**.

6 Repeat step 3 through step 5 to add as many TLS server IP Addresses as needed.

7 To add a TLS server, in **Sites**, click the **Create** icon.

8 Configure the parameter as follows:

Table 9-63 Sites Parameters

Parameter	Description
Name	TLS server virtual name
Certificate	TLS server certificate filename. Click **Choose Certificate File** to select a certificate that has already been uploaded. Select the file and click **Select**. To upload a certificate file, click **Browse** in the Upload Certificate & Key Files field. Select the file and click **Upload**.
Key	TLS server key filename. Click **Choose Key File** to select a server key file that has already been uploaded. Select the file and click **Select**. To upload a key file, click **Browse** in the Upload Certificate & Key Files field. Select the file and click **Upload**.
Key Passphrase	TLS server key file passphrase.
Default	Mark the checkbox to set this site as the default site in the list.

9 Click the **Save** icon.

UA Profile

Use this object to configure a User Agent Profile.

To add a User Agent Profile:

1 Use any of the following methods to add a User Agent Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **UA Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New UA Profile**.

2 Configure the parameters as follows:

- **Name** – Enter the UA Profile name.

3 To create a new User Agent Key, in **User Agent Key**, click the **Create** icon.

To modify a User Agent Key, select the instance and click the **Modify** icon.

4 Configure the association between the User Agent and the UA Profile file as follows:

Table 9-64 User Agent Key Parameters

Parameter	Description
User Agent Key	Enter a User Agent Key.
Filename	Click **Choose UA Profile File** to select a UA Profile that has already been uploaded. Select the file and click **Select**. To upload a UA Profile file, click **Browse** in the Upload File field. Select the file and click **Upload**. The file can be a single file or an archive file (with .tar, .tar.gz, .gz, or .gzip extension). Acuitas uses tar to expand the archive file to its individual files.

5 Click **Add** (or **Modify)**.

6 Repeat step 3 through step 5 to add as many User Agent Keys as needed.

7 To delete a User Agent Key, select the instance and click the delete icon.

8 To validate a UA Profile with the User Agent Key, select the instance and click the **Validate** icon.

9 In **UA Profile Default**, configure the association between the Default User Agent and UA Profile file as follows:

Table 9-65 Default User Agent Key Parameters

Parameter	Description
User Agent Key	Select the User Agent Key.
Filename	Click **Choose UA Profile File** to select a UA Profile that has already been uploaded. Select the file and click **Select**. To upload a UA Profile file, click **Browse** in the Upload File field. Select the file and click **Upload**. The file can be a single file or an archive file (with .tar, .tar.gz, .gz, or .gzip extension). Acuitas uses tar to expand the archive file to its individual files.

10 Click the **Save** icon.

URL List

URL List defines a list of URLs. This object is referred to by HTTP Rule Group and used as rules to match HTTP Request's URL.

The following guidelines apply to the URL List file format:

- The file used to configure the URL List must be a text file.
- The filter database is built when the URL List is configured and the file exists at designated location on MCC. Operators may import the file from the remote server or from local file. If the file is imported from the local file, the file is uploaded to the directory /public/content/policylists/url/userlists/ on the MCC. For import instructions, see HTTP Filter File Management.
- If you make changes to the file, you must import the file from the CLI (using the content-filter import debug command) to rebuild the database for the new file to take effect.
- The file should have a Fully Qualified Domain Name (FQDN) for each line for HTTP request URL prefix or exact-match:
  - The protocol schema is ignored and anything before "//" and including "//" is skipped. Only the URL following "//" is used.
  - If line contains a star "*", the entry is added in the database using the string before "*" for URL prefix-match. Otherwise, the entry is added in the database for URL exact-match.

To add a URL List:

1 Use any of the following methods to add a URL list:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **URL List**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions**.

c Click the **New** tab.

d Click **New URL List**.

2 Configure the parameters as follows:

Table 9-66 URL List Parameters

Parameter	Description
Name	URL list name
Import as URL Prefix	Specifies whether to treat URLs in the list as URL prefixes, rather than exact match URLs.
Import From	Specifies to import from: ■ **Import from server**: references a file to be imported from a file server and configures a rule for importing the file. ■ **Import from local file**: references a file name for importing the file on local directory: */public/content/policylists/url/userlists/* The URL List database is built after an import action. The file contains a list of URLs in the following format. In the file, each URL is a string in the following format: http[s]://<*domain-name*>[:<*port*>]/[<*url-path*>][/*] The *port*, *url-path*, and terminating /* are optional. If /* is used, the URL is treated as an URL prefix rather than the exact-match URL. If you make changes to the file, you must import the file to rebuild the database for the new file to take effect. For import instructions, see HTTP Filter File Management.
Filename	Filename containing the URL list (such as folder/file-${DATE:yyyymmdd}.txt)
File Download Profile	Select the File Download Profile that defines parameters for importing the list from a file server. The File Download Profile must already exist. See File Download Profile.

1 Click the **Save** icon.

Services

Create service instances for various services.

To configure services:

1. Right-click an NE and select **Affirmed Open Workflow**.
2. Use any of the following methods to configure services:

Build Out Functions:

a. Click the **Build Out Functions** tab.

b. Expand **Select a Category** in the left pane.

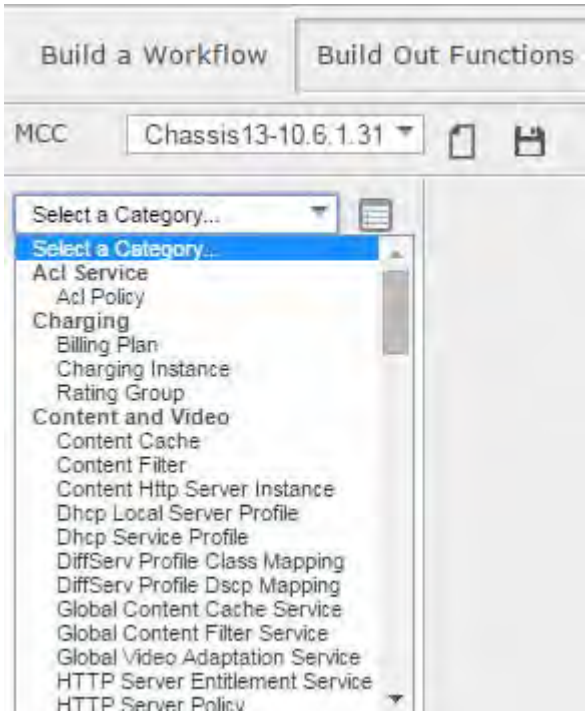
c. Click the service you want to create or modify.

d. To create a new instance, click the **Create** icon.

To modify an existing service, click the instance.

e. Configure the parameters in the configuration window and click the **Save** icon.

Figure 9-24 Build Out Functions



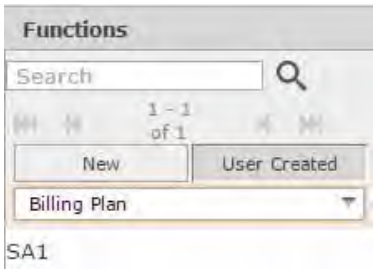
Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

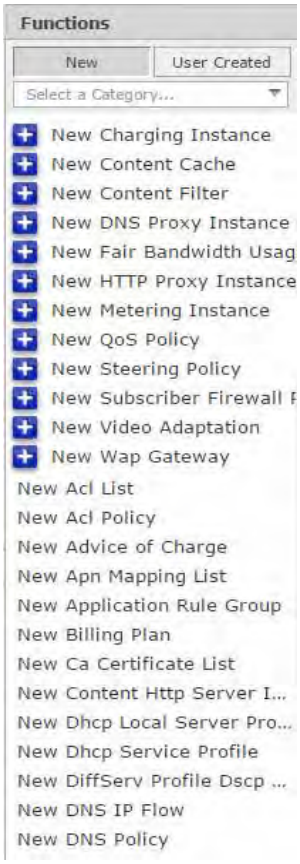
c To select an existing service, click the **User Created** tab. Expand **Select a Category**.

Figure 9-25 User Created Workflow Functions



To select a service to add, click the **New** tab.

Figure 9-26 New Workflow Functions



d Click the service you want to create or modify.

e Configure the parameters in the configuration window and click the **Save** icon.

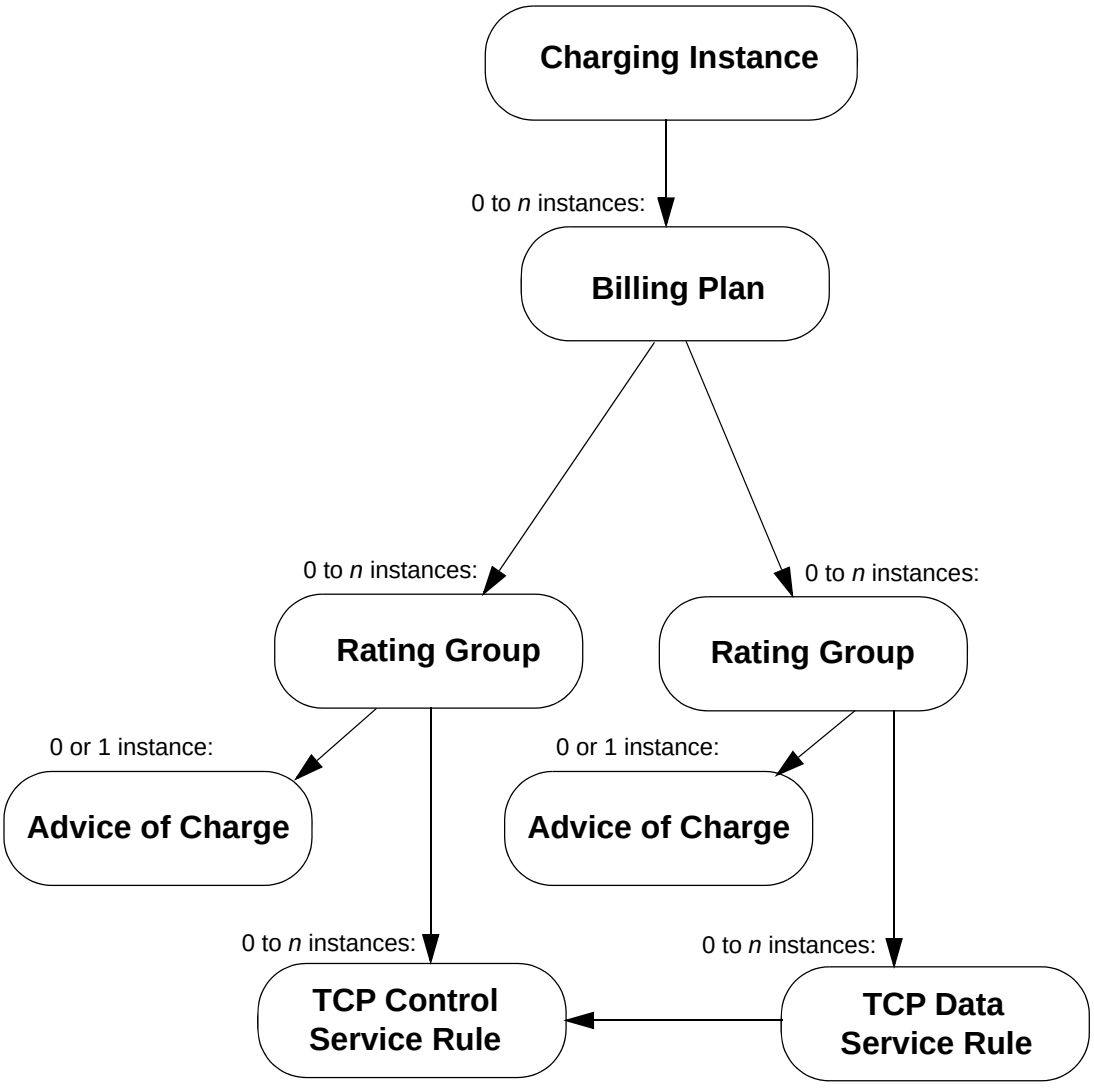
Charging

Charging includes:

- Rating Group – Defines the basis for charging service data flows
- Billing Plan – Defines the charging method to be applied to list of Rating Groups
- Charging Instance – Binds one or more billing plans

The following figure illustrates the components of Charging.

Figure 9-27 Charging Components



Rating Group

The Rating Group defines the basis for charging the service data flows. It defines the mapping between usage units (octets, time, or event) and cost. Quota management can occur at the rating group level or at a higher shared credit-pool level.

The Service Rule supports the following separate categorization of traffic, which can be used for charging:

- TCP control traffic – Defined as TCP packets with IP total length equal to the IP header plus the TCP header.
- TCP data traffic and non-TCP traffic

This feature requires Service Rules to be paired to account for both types of traffic; one is the TCP Control Service Rule, one is the TCP Data Control Service Rule. The previous figure illustrates this pairing. For more information, see Service Rule.

To add a Rating Group:

1 Use any of the following methods to add a Rating Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Rating Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Rating Group**.

2 Configure the parameters as follows:

Table 9-67 Rating Group Parameters

Parameter	Description
Name	Rating Group name
State	Admin State: ■ enabled ■ disabled
Advice of Charge	Advice of Charge The Advice of Charge must already exist. See Advice of Charge.

Table 9-67 Rating Group Parameters

Parameter	Description
Charging Method	Charging Method: ■ online - prepaid/closed-loop ■ offline - postpaid/open-loop ■ local ■ no charge - subscriber traffic that uses this rating group is either not charged or CDRs are not generated for this rating group. This feature is useful when an Operator wants to exclude certain flows such as DNS requests or portal requests used to charge subscribers. ■ metering ■ no metering ■ afind - AF Indication for SDF detection
Quota ID	Unique Rating Group ID
Priority	Rating Group priority Priority resolves conflicts in the case of a multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object. Thus, the Rating Group priority takes precedence over the associated service rule priority.
Multiplier	Multiplier applied to volume and event charging
Measurement Method	Measurement method: ■ time ■ volume ■ both: time and volume ■ event (applies only when Charging Method is set to offline or local)
Volume Measurement Count	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Volume measurement count: ■ total octets ■ input octets ■ output octets
Volume Measurement Layer	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Volume measurement layer: ■ layer3: counts the entire IP datagram ■ layer4: excludes the IP header ■ layer7: excludes the IP header and the UDP/TCP/SCTP header

Table 9-67 Rating Group Parameters

Parameter	Description
TCP Retransmission	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Inclusion or exclusion of TCP retransmissions in volume counts.
Credit Pool ID	***Note:*** *Applies when Charging Method is set to Online.* Credit pool used to grant credit blocks. ***Note:*** *Enter 0 if no credit pool is used.*
Quota Hold Time	Hold time after inactivity, in seconds.
Reporting Level	Policy control reporting level: ■ rating group ■ service rule
Quota Consumption Time	***Note:*** *Applies when Measurement Method is set to Time or Time and Volume.* Inactivity timeout for time-based accounting, in seconds.
Time Threshold	***Note:*** *Applies when Measurement Method is set to Time or Time and Volume.* Time threshold, in seconds ***Note:*** *Enter 0 if thresholding not desired*
Volume Threshold	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Volume threshold, in bytes ***Note:*** *Enter 0 if thresholding not desired*
Event Threshold	***Note:*** *Applies when Measurement Method is set to Event.* Event threshold. ***Note:*** *Enter 0 if thresholding not desired*
Credit Authorization Event	***Note:*** *Applies when Charging Method is set to Online.* Credit authorization beginning stage: ■ bearerSetup: first control signaling packet ■ firstSdfPkt: first data packet
Quota Blacklist Timer	***Note:*** *Applies when Charging Method is set to Online.* Quota Black List Timer, in minutes. Specifies how frequently to send grant requests after termination or suspension for this Rating Group.
Service Type	Service type: ■ data ■ mms-mo (inbound, mobile originated) ■ mms-mt (outbound, mobile termination)

Table 9-67 Rating Group Parameters

Parameter	Description
Home Sub Charge	Specifies whether to use the rating group for home subscriber charging: ■ enabled ■ disabled
Roamer Sub Charge	Specifies whether to use the rating group for roaming subscriber charging: ■ enabled ■ disabled
CDR Interim Time	***Note:*** *Applies when Charging Method is set to Offline.* Interim for interim CDR generation, in seconds.
Monitor Key	***Note:*** *Applies when Charging Method is set to Metering.* Monitor Key associated with the PCRF. When the PCRF requests usage monitoring via Gx messaging, the Gateway uses the monitoring key to locate and activate the corresponding rating group.
Service Activation	Specifies when to use or skip the service flow for packet classification: ■ always on - always use this service flow for classification ■ external activation - use the activation state of the service flow to determine whether to use or skip the service flow for packet classification. This setting allows the Gateway to dynamically activate/deactivate Rating Groups.
MMS MT OCS Size	***Note:*** *Applies when Service Type is set to mms-mt.* Message size (in bytes) to be used for MMS-MT charging.
Enable Local CDR	***Note:*** *Applies when Charging Method is set to Online.* Specifies whether to enable local CDRs for the rating group: ■ enabled ■ disabled
OCS Response Grace Period	***Note:*** *Applies when Charging Method is set to Online.* Number of seconds to pass traffic while waiting for an OCS response.
Requested Unit Value	Requested unit value for this Rating Group
SDF Inactivity Time	***Note:*** *Applies when Charging Method is set to Afind.* Inactivity time of SDF for AF Notification (in seconds). SDF is disabled upon the timer expiry.

Table 9-67 Rating Group Parameters

Parameter	Description
Service Rules	Select the service rule(s) to link with the Rating Group. The Service Rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Billing Plan

The Billing Plan defines the charging method to be applied to list of Rating Groups. Multiple billing plans can be used to charge differently for home-area, roaming, preferential-roaming, fraudulent activity, and so on.

To add a Billing Plan:

1 Use any of the following methods to add a Billing Plan:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Billing Plan**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Billing Plan**.

2 Configure the parameters as follows:

Table 9-68 Billing Plan Parameters

Parameter	Description
Name	Billing Plan name
Rating Group	Select the Rating Group(s). The Rating Group must already exist. See Rating Group. To select a Rating Group, drag and drop it from the Available list to the Selected list.

Table 9-68 Billing Plan Parameters

Parameter	Description
Fraud Charging	Set to true to designate this Rating Group for charging of fraudulent activity within this Billing Plan.

3 In **Service Rules**, drag and drop the as many Service Rules as needed from the Available list to the Selected list.

4 Configure the parameters as follows:

Table 9-69 Service Rule Parameters

Parameter	Description
Weight	This setting allows you to apply a scaling factor to a service rule that is also associated with a rating group. For example, you could have different scaling factors for the same rating groups, depending on the billing plan.
Priority Override	Priority to override the Service Rule's priority when used with this billing plan.

5 Click **Apply**.

6 Click the **Save** icon.

Charging Instance

The Charging Instance is made up of multiple billing plans. Billing plan selection is based on charging characteristics.

To add a Charging Instance:

1 Use any of the following methods to add a Charging Instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Charging Instance**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Charging Instance**.

2 Configure the parameters as follows:

Table 9-70 Charging Instance Parameters

Parameter	Description
Name	Charging Instance name
State	Charging administrative state: ■ enabled ■ disabled
Priority Evaluation Mode	Priority Evaluation Mode when classifying traffic: ■ flat - Use Service Rule priority (ignore Rating Group priority). To make a match, examine all of the Service Rules on all of the Rating Groups for best priority. ■ flat-with-pcc-rule-precedence - Any PCC rules in effect have their precedence values compared with the Service Rule priority values, and the PCC rule or Service Rule with the highest priority (lowest numerical value) is selected. ■ hierarchical - Use Rating Group priority and Service Rule priority hierarchically. To make a match, examine the Rating Group in priority order and within each of them, examining the Service Rules in priority order.

3 In **Billing Plan Map**, drag and drop the as many Billing Plans as needed from the Available list to the Selected list.

4 Configure the parameters as follows:

Table 9-71 Billing Plan Parameters

Parameter	Description
Charging Characteristic	Enter the Charging Characteristic. This number could be one provisioned in each user's subscription data, per-APN, or for the entire profile at HSS. It is significant inside the user's home network. It can be used by the Operator to specify data as CDF address, OCS address, interim reporting interval/volume for on-line charging, tariff times, and so on. It is attached to the billing plan as a method to associate the charging profile to a particular subscriber.

5 Click **Apply**.

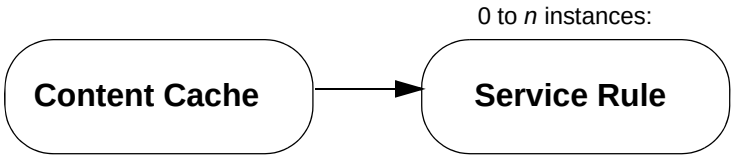
6 Click the **Save** icon.

Content Cache

The Content Cache service configures the behavior of the web and video cache on the system. The system provides the ability to store cached content at the edge of the network for mobile delivery, resulting in reduced Internet bandwidth consumption and reduced latency.

The following figure illustrates the components of content cache.

Figure 9-28 Content Cache Components



Content Cache Service

To add a Content Cache Service:

1 Use any of the following methods to add a Content Cache Service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Global Content Cache Service**.

d Click **Global Content Cache Service**.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **User Created** tab.

d Expand **Select a Category**.

e Click **Global Content Cache Service**.

f Click **Global Content Cache Service**.

2 Configure the parameters as follows:

Table 9-72 Content Cache Service Parameters

Parameter	Description
Admin State	Content cache administrative state: ■ enabled ■ disabled ***Note:*** *HTTP Proxy Admin State must be enabled before content cache Admin State can be enabled.*
Cache YouTube	Mark the checkbox to enable caching of YouTube videos.
Cache Metacafe	Mark the checkbox to enable caching of Metacafe videos.
Cache Dailymotion	Mark the checkbox to enable caching of Dailymotion videos.
Eviction Policy	Configure cache eviction policy: ■ LRU ■ LFU
Max Cache Life	Maximum cache lifetime, in seconds
Max Object Size Memory	Maximum object size that can be cached in memory (multiple of 4K)
Max Object Size Disk	Maximum object size that can be cached on disk (multiple of 4K)
Min Hit Cache	Minimum number of hits to cache object.

3 Click the **Save** icon.

Content Cache Instance

To add a Content Cache Instance:

1 Use any of the following methods to add a Content Cache instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Content Cache**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Content Cache**.

2 Configure the parameters as follows:

- **Service Name** – Enter a Content Cache service name.

3 Configure the parameters as follows:

Table 9-73 Service Rule Parameters

Parameter	Description
Service Rule	Service Rule. The Service Rule must already exist. See Service Rule. ***Note:*** *The Service Rule must contain an HTTP Rule Group.* To select a Service Rule, drag and drop it from the Available list to the Selected list.
Priority	Service Rule Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Cache Bypass	Enable/Disable serving from cache: ■ disabled ■ enabled
Cache Server Response	Enable/Disable caching the response from the server: ■ disabled ■ enabled

4 Click **Apply**.

5 Click the **Save** icon.

Content Filter

The Content Filter configures the filtering capability for a subscriber workflow. The user's HTTP transactions can be filtered using the following filter types:

- Blacklist
- Whitelist, containing a list of domains or URLs to allow
- Static Category
- Service Rule
- Online Category Group
- Malware Category Group
- Phishing Category
- IWF Category

For each of these filter types, the Operator can specify the corresponding filtering action (allow, block, redirect, terminate) for a matching HTTP request.

The filter types Online Category Group, Malware Category Group, Phishing Category and IWF Category require configuration of the Content Categorization. Content Categorization uses third party databases for categorization of user requests. User requests are categorized to one or more of well-known Online Categories, Malware categories, the Phishing category or the IWF category.

These well-known categories are maintained online by a third party. The the Affirmed Networks system updates the databases periodically, as often as every hour.

Operators can also filter web search engine results for the Bing, Google, and YouTube search engines using the Safe Search feature.

To enable a Content Filter, the HTTP Proxy service must be enabled.

Global Content Filters

Global content filters include:

- Content Filter Blacklist — Deny files that contain a list of domains or URLs to block/terminate/redirect. For a global content filter, the Operator can configure up to ten Blacklist files.
- Content Filter Whitelist — Files that contain a list of domains or URLs to allow. For a global content filter, the Operator can configure up to ten Whitelist files.

If a global filter is not configured, HTTP traffic is filtered at the instance level. The following content-filtering guidelines apply to the file format:

- Must be a text file.
- The file must be uploaded through Acuitas and located on the MCC when the Content Filter is configured. For import instructions, see HTTP Filter File Management.
- If you make changes to the file, you must import the file to rebuild the database for the new file to take effect.
- When the File Type is domain, the file should have a Fully Qualified Domain Name (FQDN) for each line for HTTP request HOST exact-match:
  - The protocol schema is ignored and anything before "//" and including "//" is skipped. Only the domain name following "//" is used.
  - If line contains only the domain (without the forward slash), only the domain is added to the database for HOST exact-match.
  - If line contains a URL (with a forward slash), only the domain name is added in the database for HOST exact-match.
  - If line contains a star "*", the line is ignored.
- When the File Type is url, the file should have a Fully Qualified Domain Name (FQDN) for each line for HTTP request HOST or URL exact-match:
  - The protocol schema is ignored and anything before "//" and including "//" is skipped. Only the URL following "//" is used.
  - If line contains only the domain (without the forward slash), the entry is added to the database for HOST exact-match.
  - If line contains a URL (with a forward slash), the entry is added in the database for URL exact-match.
  - If line contains a star "*", the line is ignored.

Content Filter Static Category Filters

Operators can define Static Content Categories for matching user traffic. The Static Category is initialized with a list of URLs or domains (host names) specified in an Operator defined file.

For a Content Filter instance, the Operator can configure up to 16 Static Category filters, each with the action (allow/block/terminate/redirect) to be applied.

Content Filter Service Rule Filters

Operators can also specify a Service Rule that contains the HTTP rule groups to be matched with a request.

The HTTP rules can specify criteria for matching user requests against HTTP request fields including:

- Request Method
- Request URI
- URL List
- Response Status Code
- Accept Header
- Content-Type Header
- Host Header
- Referer Header
- User-Agent Header

For a global content filter, the Operator can configure one Service Rule with action block/terminate/redirect.

Content Filter Online Category Group Filters

With content categorization configured, user requests can be categorized to one or more well-known Online Categories.

Operators can group a set of the well-known Online Categories using the Online Category Group configuration object. For each Online Category Group, the Operator can define a filter with action block, terminate, redirect, or allow.

Online Categories are listed in the following table:

Table 9-74 Online Categories

Name	Sites that...
abortion	Provide information or arguments in favor of or against abortion; describe abortion procedures; offer help in obtaining or avoiding abortion; provide testimonials on the physical, social, mental, moral, or emotional effects of abortion.
advertising	Provide Internet advertising services.
alcohol	Promote or sell alcoholic beverages; supply recipes or paraphernalia to make alcoholic beverages; glorify, tout, or otherwise encourage alcohol consumption or intoxication.
alcohol kids	Include the promotion, glamorization, or encouragement of drinking alcohol to excess that is aimed at children or that may have a significant appeal to children.
anonymizer	Offer anonymous access to websites through a PHP or CGI proxy, allowing users to gain access to websites blocked by corporate and school proxies as well as parental control filtering solutions.

Table 9-74 Online Categories

Name	Sites that...
art-and-museums	Include art galleries, artists, and museums. Includes all types of visual arts such as performing arts, theater, painting, drawing, sculpture, photography, natural history, science, and children's museums.
art-nudes	Contain non-pornographic, tasteful, and artful display of the naked body.
automated-web-application	Allow a computer to automatically open an http connection for reasons such as checking for operating system or application updates.
automotive	Relate to motor vehicles, dealers, sales and clubs.
bikini	Offer the sale of bikinis, mico-kinis, mono-kinis, and thongs marketed as beachwear rather than swimwear. Also sites that feature galleries and/or videos of models in bikinis.
blogging	Contain blogs.
business	Are sponsored by or devoted to individual businesses not covered by any other categories.
cash-gambling	Involve the wagering and exchange of money online.
chat	Offer users the ability to chat online.
content-delivery-service	Are content delivery/distribution networks (CDN) designed to accelerate the delivery of content rich Internet pages or large files to end users.
criminal-skills	Provide instruction for threatening or violating the security of property or the privacy of people; and how to avoid complying with legally mandated duties and obligations.
cults	Feature well-known, organized new religious movements and sects regarded as exploitative or unorthodox.
cyberbullying	Contain targeted, deliberate, and slanderous or offensive content about other people with the intent to torment, threaten, humiliate or defame them. Content is often sexual, malicious or hostile in nature and is submitted via interactive digital technology. Examples include malicious gossip; inappropriate photos posted without consent
drugs	Promote, offer, sell, supply, encourage or otherwise advocate the recreational or illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
dynamic	Contain both appropriate and inappropriate user-generated content like social networking or blogging sites. Also, sites in which the page content changes based how the user interacts with it (for example, an Internet search).
education	Represent schools or other educational facilities, faculty, or alumni groups.
energy	Represent companies involved with the production and distribution of energy.
enterprise-webmail	Provide online e-mail services.
entertainment	Relate to personal entertainment as well as the entertainment industry.
filesharing	Make files available for other users to download over the Internet or private networks.

Table 9-74 Online Categories

Name	Sites that...
finance-and-investing	Provide the opportunity to establish, plan, research, or manage personal finances and investments.
food-and-restaurants	Provide information about food, recipes, specialty food shops, catering, food delivery, and restaurants.
forums-and-messageboards	Provide a web application enabling users to participate in the discussion of numerous topics, often in conjunction with online communities.
freeware-and-shareware	Offer online software download.
gambling	Allow users to place bets or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing bets; receive instructions, assistance or training on participating in games of chance.
gaming	Sites related to computer or video games, game downloads, and online game sites.
glamour	Emphasize, promote, or provide information on how to achieve physical attractiveness, allure, charm, beauty, or style with respect to personal appearance.
gore	Display graphic violence and/or the infliction of pain or injuries. Gross violence towards humans or animals, such as scenes of dismemberment, torture, massive blood and gore, sadism, and other types of excessive violence.
government	Sites sponsored by government branches or agencies.
hacking	Promote or provide the means to practice illegal or unauthorized acts of computer crime using technology or computer-programming skills.
hate	Advocate hostility or aggression toward individuals or groups on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics; sites that denigrate others on the basis of those characteristics or justifies inequality on the basis of those characteristics; sites that purport to use scientific or other commonly accredited methods to justify said aggression, hostility, or denigration.
health	Provide information or advice on personal health or medical services, health insurance, procedures, or devices; sites that include information on diets, nutrition, therapies, and counseling services.
hobby	Provide information on private pastimes.
hosting	Provide individuals or organizations with online systems for storing images, video, or any content accessible via the Web.
internet-telephony	Enable users to make telephone calls via the Internet or obtain information or software for that purpose.
job-search	Provide assistance or tools to help to find employment.
kids	Provide a safe and interesting Internet experience for children under 12 years of age.
law	Offer legal content and services.
lifestyles	Contain general material relevant to sexual orientation.

Table 9-74 Online Categories

Name	Sites that...
mature-content	Contain sexually explicit information that is not of a medical or scientific nature.
military	Are sponsored by military branches or agencies as well as official and personal sites related to military history, ideology, or specific branches of the military.
mobile-entertainment	Offer a range of add-ons for handheld devices, such as ringtones, wallpapers, games, and videos.
music	Are related to the music industry.
news	Report, inform, or comment, on current events or contemporary issues of the day, including sports, weather, editorials, and human interest news.
non-profit	Are owned by non-profit organizations.
obscene	Contain obscene material.
occult	Promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, or supernatural beings.
online-backup-and-storage	Provide the ability to backup or upload data files to the Internet providing long term storage, access from other computers or locations, or the ability to share data files with other users.
peer-to-peer	Provide centralized peer-to-peer networks.
personals-and-dating	Promote or provide opportunity for establishing or continuing romantic relationships.
pets	Are related to the care, maintenance, purchase, rescue, or breeding of any animal for companionship and enjoyment.
photography	Are related to taking, sharing, printing, studying, or manipulating photos at all skill levels, whether casual, amateur or professional.
placeholder	Are owned by domain name registrars, domain brokers, or Internet advertising publishers. They usually display dynamically generated content with the intent to monetize on traffic through linked advertising listings.
plagiarism	Are primarily designed to allow students to cheat at school by taking the work or ideas of someone else and pass it off as their own.
politics	Are related to politicians, election campaigns, political organizations, and publications. Includes official homepages of politicians and political parties and personal sites about politics and grass-root movements.
pornography	Contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
portal	Offer a broad array of resources and services, such as email, forums, search engines, and on-line shopping malls.
real-estate	Are involved in the real estate business.
reference	Serve as a general resource to the public and feature factual information produced by authoritative and trusted sources.
religion	Are about religion or any set of beliefs and practices that have the function of addressing the fundamental questions of human identity, ethics, death, and the existence of the Divine.

Table 9-74 Online Categories

Name	Sites that...
remote-access	Offer software/services that allow a computer or portable device to remotely control or monitor another computer or device via the Internet or another network.
science	Provide research materials in the natural and life sciences.
search	Support searching the Internet, news groups, or indexes and directories.
self-harm	Describe or discuss ways in which to self harm including eating disorders and self-injury.
sexual-education	Provide educational information on reproduction and sexual development, sexually transmitted disease, contraception, safe sexual practices, sexuality, and sexual orientation
shopping	Provide the means to purchase products or services online.
sports	Promote or provide information about spectator sports.
streaming-media	Host streaming media like television, movies, video, radio, or other media.
suicide	Describe or promote suicide.
technology-and-telecommunication	Provide information pertaining to computers, the Internet, and telecommunication.
tobacco	Encourage, promote, offer for sale or otherwise encourage the consumption of tobacco.
tobacco kids	Include the promotion, glamorization, or encouragement of smoking that is aimed at children or that may have a significant appeal to children.
travel	Promote or provide opportunity for travel planning in a general sense, particularly finding and making travel reservations.
violence	Advocate or provide instructions for causing physical harm to people or property through use of weapons, explosives, pranks, or other types of violence.
virtual-community	Offer a variety of tools and mechanisms to enable a group of people to communicate and interact via the Internet.
weapons	Describe or offer for sale weapons including guns, ammunition, firearm accessories, knives, and martial arts.
webmail	Provide free, web-based email services, accessible through any Internet browser.
wedding	Are related to the traditions, customs, planning, and products involved in a marriage, commitment ceremony, or civil unions.
Note: *The following categories are for sites formatted for small format browsers like WML and xHTML:*	
wireless-business	Are sponsored by or devoted to individual businesses not covered by any other categories.
wireless-chat-sms	Offer users the ability to chat online.
wireless-dynamic	Contain both appropriate and inappropriate user-generated content like social networking or blogging sites. Also, sites in which the page content changes based how the user interacts with it (for example, an Internet search).

Table 9-74 Online Categories

Name	Sites that...
wireless-entertainment	Offer a range of add-ons for handheld devices, such as ringtones, wallpapers, games, and videos.
wireless-finance	Provide the opportunity to establish, plan, research, or manage personal finances.
wireless-gambling	Allow users to place bets or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing bets; receive instructions, assistance or training on participating in games of chance.
wireless-news	Primarily report, inform, or comment, on current events or contemporary issues of the day. Includes sports, weather, editorials, and human interest news.
wireless-personals-and-dating	Promote or provide opportunity for establishing or continuing romantic relationships.
wireless-pornography	Contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
wireless-sports	Promote or provide information about spectator sports.
wireless-travel	Promote or provide opportunity for travel planning in a general sense, particularly finding and making travel reservations.
unknown	Are unknown to the category database.

Content Filter Malware Category Group Filters

With content categorization configured, user requests can be categorized to one or more well-known malware categories:

- malware-attack-botnet – Sites associated with malware that causes a system to perform automated tasks over the Internet.
- malware-domain – Sites where the domain was found to either contain malware or take advantage of other exploits to deliver adware, spyware, or malware.
- malware-object – Sites that contain direct links to malware file downloads (such as . exe, .dll, .ocx, and others). These URLs are generally highly malicious.
- malware-spyware – Sites of domains associated with vendors and distributors of spyware, adware, greyware, and other potentially unwanted advertising software. Some may run exploits to facilitate the installation of this unwanted software.
- potential-malware-victim – Sites that click fraud and adware components use when “phoning home” that could signal a device is infected with spyware or adware. This category should be used only for reporting, not for blocking as the target URLs can be legitimate sites.

A set of the well-known malware categories can be grouped using the Malware Category Group configuration object. For each Malware Category Group, the Operator can define a filter with action block, terminate, redirect, or allow.

Content Filter IWF Category Filters

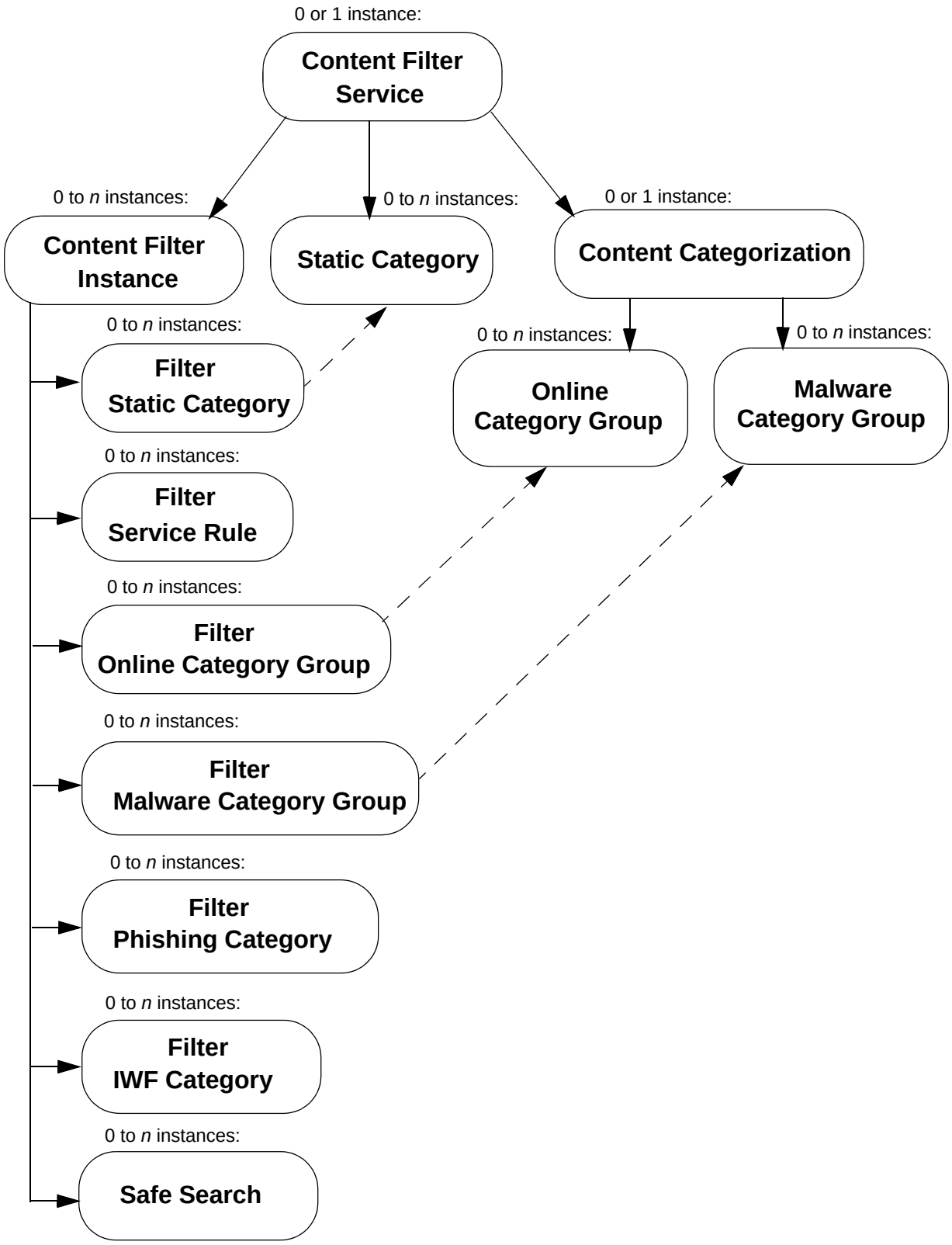
With content categorization configured, user requests can be categorized to a well-known Internet Watch Foundation category. The IWF category contains web sites hosting illegal child abuse images and content anywhere in the world.

The category is sourced from the list maintained by Internet Watch Foundation at http://www.iwf.org.uk

For the IWF category, the Operator can define a filter with action block, terminate, redirect, or allow.

The following figure illustrates the components of a content filter.

Figure 9-29 Content Filter Components



Content Filter Service

To add a Content Filter Service:

1 Use any of the following methods to add a Content Filter service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Global Content Filter Service**.

d Click **Global Content Filter Service**.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **User Created** tab.

d Expand **Select a Category**.

e Click **Global Content Filter Service**.

f Click **Global Content Filter Service**.

2 Configure the parameters as follows:

- **Admin State** – Select the filter administrative state.

3 In **Content Categorization**, configure the database parameters as follows:

Table 9-75 Content Categorization Parameters

Parameter	Description
Customer ID	Customer identification string
Network Context	The Network Context to use when connecting to third-party server to update category databases
URL Categorization	Enable/Disable URL Categorization: ■ Enabled ■ Disabled
Malware Categorization	Enable/Disable Malware categorization: ■ Enabled ■ Disabled When enabled, the content filter categorizes requests to the categories: malware-all, malware-domain, malware-object, malware-spyware, malware-victim.

Table 9-75 Content Categorization Parameters

Parameter	Description
Phishing Categorization	Enable/Disable Phishing categorization: ■ Enabled ■ Disabled When enabled, the content filter categorizes requests to the phishing category.
IWF Categorization	Enable/Disable IWF child abuse categorization: ■ Enabled ■ Disabled When enabled, the content filter categorizes requests to the IWF child abuse category.
Real Time Categorization	Enable/Disable real-time categorization of web pages containing dynamic or unknown content: ■ Enabled ■ Disabled When enabled and a page with dynamic content (that is, search engine or social networking page) is accessed, the content filter categorizes the page using real-time categorization engine. When dynamic categorization is disabled, the content filter categorizes the page as a dynamic category. ***Note:*** *Enabling this option can impact performance.*
Categorization Log Level	Set the categorization log level.
Database Update Interval	Database update interval, in hours.

4 Click the **Save** icon.

Content Filter Instance

To add a Content Filter Instance:

1 Use any of the following methods to add a Content Filter instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Content Filter**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b. Expand **Functions** in the right pane.

c. Click the **New** tab.

d. Click **New Content Filter**.

2. Configure the parameters as follows:

- **Service Name** – Enter a Content Filter name.
- **Global Filtering** – Set to **on** if this Content Filter is a Global Content Filter Service (applies to all subscribers).

  Set to **off** if this Content Filter is a Content Filtering Instance (non-global).

3. In **IWF Category**, configure the content filter for the IWF category. Configure the parameters as follows:

Table 9-76 IWF Category Parameters

Parameter	Description
Priority	IWF category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Action	Service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Block Notification Message	Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307

4. In **Malware Category Group**, click the **Create** icon. to configure a content filter using a malware category group that takes effect only for the enabled Content Categorization. Configure the parameters as follows:

Table 9-77 Malware Category Parameters

Parameter	Description
Category	Malware category that specifies a list of domains or URLs. The malware category must already exist. See Malware Category.
Priority	Content category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Action	Service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

5 Click **Add**.

6 Repeat step 4 through step 5 to add as many Malware Categories as needed.

7 In **Online Category Group**, click the **Create** icon. to configure a content filter using an online category group that takes effect only for the enabled Content Categorization. Configure the parameters as follows:

Table 9-78 Online Category Parameters

Parameter	Description
Category	Online category that specifies a list of domains or URLs. The online category must already exist. Create it at Services > Content Filter > Content Categorization > Online Category Group.
Priority	Content category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Action	Service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

8 Click **Add**.

9 Repeat step 7 through step 8 to add as many Online Categories as needed.

10 In **Phishing Category**, configure the content filter for the Phishing category:

Table 9-79 Phishing Parameters

Parameter	Description
Priority	Phishing category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Action	Service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Block Notification Message	Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307

11 In **Filter Hash List**, click the **Create** icon. to configure a content filter using a Filter Hash List. Configure the parameters as follows:

Table 9-80 Filter Hash List Parameters

Parameter	Description
Name	Name of the Filter Hash List. The Filter Hash List must already exist.
Priority	Filter Hash List Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block

Table 9-80 Filter Hash List Parameters

Parameter	Description
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message to include in the 403 status code in the response body
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

12 Click **Add**.

13 Repeat step 11 through step 12 to add as many Online Categories as needed.

14 In **Service Rule**, click the **Create** icon.

15 Configure the parameters as follows:

Table 9-81 Service Rule Parameters

Parameter	Description
Service Rule	Select the Service Rule. The Service Rule must already exist. See Service Rule. ***Note:*** *The Service Rule must contain an HTTP Rule Group.*
Priority	Service Rule Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.

Table 9-81 Service Rule Parameters

Parameter	Description
Action	Service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL The following variables can be used as part of redirect URL: ■ $(IMEI) ■ $(MSISDN) ■ $(IMSI) ■ $(UEIPADDR) ■ $(TIMESTAMP) – milliseconds since Epoch ■ $(RANDOM) – 16 random octets ■ $(ORIGINALURL) ■ $(SHA256[]) - base64 encoded hash of information (different macros or plain text) inside the square brackets
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

16 Click **Add**.

17 Repeat step 14 through step 16 to add as many Service Rules as needed.

18 In **Static Category**, click the **Create** icon.

19 Configure the parameters as follows:

Table 9-82 Static Category Parameters

Parameter	Description
Category	Content category that specifies a list of domains or URLs. The Content category must already exist. See Adding Categories.
Priority	Content category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Action	Service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
Fields when Action is set to Block:	
Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

20 Click **Add**.

21 Repeat step 18 through step 20 to add as many Static Categories as needed.

22 In **Safe Search**, enable Safe Search filtering capability. Search engines such Bing, Google, and YouTube provide a safe-search filtering mechanism that acts as an automated filter of inappropriate content. When configured for a specific subscriber, the system enforces safe-search even if an attempt is made to disable it from the UE. The system content filter supports the capability to enforce safe-search per search engine and per subscriber.

Configure the parameters as follows:

Table 9-83 Safe Search Parameters

Parameter	Description
Google	Enable/disable Google Safe Search filtering capability, which removes sites that contain inappropriate content from search results: ■ Enabled ■ Disabled
Bing	Enable/disable Bing Safe Search filtering capability, which removes sites that contain inappropriate content from search results: ■ Enabled ■ Disabled
Youtube	Enable/disable YouTube Safe Search filtering capability, which removes sites that contain inappropriate content from search results: ■ Enabled ■ Disabled

23 In **Protocol Filtering**, enable this filter instance for different protocols:

- **HTTP** – Select enabled to enable this filter for HTTP protocol service.
- **HTTPS** – Select enabled to enable this filter for HTTPS protocol service.

24 Click the **Save** icon.

Static Category

To add a Static Category:

1 Use any of the following methods to add a Static Category:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Static Category**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Static Category**.

2 Configure the parameters as follows:

Table 9-84 Static Category Parameters

Parameter	Description
Name	Category name
File Type	Address types in the file: ■ Domain ■ URL
File Name	Name of the category file

3 Click the **Save** icon.

Online Category Group

To add an Online Category Group:

1 Use any of the following methods to add an Online Category Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Online Category Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Online Category Group**.

2 Configure the parameters as follows:

■ **Name** – Enter an online category group name.

3 In **Online Category**, click the **Create** icon.

4 Configure the parameters as follows:

■ **Name** – Select an Online Category name.

For a list of Online Categories, see Content Filter Online Category Group Filters.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many Online Categories as needed.

7 Click the **Save** icon.

Content HTTP Server Instance

Use this object to configure an HTTP Server Service instance associated with an MMS STI service.

To add a Content HTTP Server Service instance:

1 Use any of the following methods to configure a Content HTTP Server Service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Content HTTP Server Instance**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Content HTTP Server Instance**.

2 Configure the parameters as follows:

Table 9-85 Content HTTP Server Instance Parameters

Parameter	Description
Service Name	Content HTTP Server Service instance name
Admin State	Admin state: ■ enabled ■ disable
Mms Sti	MMS STI profile associated with the HTTP Server Instance. The MMS STI profile already exist. See MMS STI Profile.
UA Profile	User Agent associated with this HTTP Server Service. The User Agent must already exist. See UA Profile.
Content Insertion:	

Table 9-85 Content HTTP Server Instance Parameters

Parameter	Description
Admin State	Content Insertion Admin state: ■ enabled ■ disable
Loopback IP List	Loopback IP Address list used for content insertion. The Loopback IP List must already exist. See Loopback IP List.
HTTP Server Policy:	
Name	Select the HTTP Server Policy to associate with the HTTP Server instance
Network Context:	
Network Context	Select the Network Context.
Loopback Addr	Select the Loopback IP Address
Port	Enter the Loopback IP Port

3 Click the **Save** icon.

Content Insertion Profile

The HTTP Proxy operates in content-insertion mode on the configurable URL/domain. The Request Policy and HTTP Server instance is associated with a configured Content Insertion Profile. The Content Insertion Profile supports:

- Insertion of local or remote hosted images or videos (such as, advertisements)
- Insertion of externally hosted content on ad server via URL links
- Banners located at the top/bottom of the page or centrally located overlays

For example, Operators can configure a Request Policy with specific domains/URL in order to insert advertisements. The UE attempts to access the specific domain/URL on which a rule is configured for content insertion.

Content insertion is a three stage process:

1. Upon receiving the response from the origin-server, the HTTP Proxy inserts the required javascript link based on the configured Request Policy, Server Instance, and Content Insertion Profile.
2. After the UE receives the HTML page with the inserted javascript link, the UE makes a request to the HTTP proxy for the javascript. The HTTP proxy generates a javascript based on the Content Insertion Profile.
3. The request for assets (either local or remote) contained within the generated Javascript (images, videos, etc.) are served based on the configured Content Insertion Profile.

To add a Content Insertion Profile:

1. Use any of the following methods to configure a Content Insertion Profile:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category** in the left pane.

   c. Click **Content Insertion Profile**.

   d. Click the **Create** icon.

   Build a Workflow:

   a. Click the **Build a Workflow** tab.

   b. Expand **Functions** in the right pane.

   c. Click the **New** tab.

   d. Click **New Content Insertion Profile**.

2 Configure the parameters as follows:

Table 9-86 Content Insertion Profile Parameters

Parameter	Description
Name	Profile name
Admin State	Admin State: ■ enabled ■ disabled

3 In **Insertion Object List**, click the **Create** icon.

4 Configure the parameters as follows:

- **Name** – Select the insertion object list. The insertion object list must already exist. See Insertion Object List.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many insertion object lists as needed.

7 In **Insertion Style**, in the **Style** field, specify to configure a banner or overlay.

8 For Banner, configure the parameters as follows:

Table 9-87 Banner Parameters

Parameter	Description
Position	Position of the banner: ■ Top ■ Bottom

9 For Overlay, configure the parameters as follows:

Table 9-88 Overlay Parameters

Parameter	Description
Timeout	Specify the number of seconds to keep the overlay
Close Button	Enable/disable the close button: ■ enabled ■ disabled

10 Click the **Save** icon.

Default Policy Cause Code List

Use this object to configure the Diameter credit control failover behavior on the Gx/Gy interfaces based on the result code received in the CCA error message.

You configure a list of result code ranges (3xxx-5xxx) and when a CCA message is received with a non-success result code (other than 2001), the default Gx policy/Gy quota (if enabled on the interface) is used to set up the session if the received result code is present in the result code list. Also, for each result code range in the list, Operators can specify whether or not the PGW retransmits the request to a secondary server before applying the default Gx policy/Gy quota.

To add a Default Policy Cause Code List:

1. Use any of the following methods to add a Default Policy Cause Code List:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category** in the left pane.

   c. Click **Default Policy Cause Code List**.

   Build a Workflow:

   a. Click the **Build a Workflow** tab.

   b. Expand **Functions** in the right pane.

   c. Click the **User Created** tab.

   d. Expand **Select a Category**.

   e. Click **Default Policy Cause Code List**.

2. Configure the parameters as follows:

   - **Name** – Enter the Default Policy Cause Code List name.

3. In **Range**, click the **Create Range** icon.

4. Configure the parameters as follows:

Table 9-89 Range Parameters

Parameter	Description
Range Name	Range name.

Table 9-89 Range Parameters

Parameter	Description
Retry Secondary	Specifies whether the PGW retransmits the request to a secondary server before applying the default Gx policy/Gy quota when the result code received in the CCA error message is within the configured range. ■ enabled – (default) When the primary server returns a result code within the configured range, the PGW retransmits the request to a secondary server before applying the default Gx policy/Gy quota. ■ disabled – When the primary server returns a result code within the configured range, the PGW uses the default Gx policy/Gy quota to set up the session and does not retransmit the request to the secondary server.
Cause Code Range Low	Specifies the low end of the result code range. ***Note:*** *Ensure the result code range does not overlap with any previously configured ranges.* ***Note:*** *To configure a range with a single result code, configure the low and high value with the same code.*
Cause Code Range High	Specifies the high end of the result code range. ***Note:*** *Ensure the result code range does not overlap with any previously configured ranges.* ***Note:*** *To configure a range with a single result code, configure the low and high value with the same code.*

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many ranges as needed.

7 Click the **Save** icon.

DNS Proxy Service

Use this object to configure a DNS proxy and caching service.

The DNS caching service is used to reduce the amount of DNS message traffic towards an Operator's DNS servers. When enabled, the DNS caching service caches DNS response traffic, allowing subsequent DNS lookup requests for the same domains to be served locally from the DNS cache. Separate caches are maintained per network context, and the DNS caching service observes the time-to-live (TTL) contained in each DNS response to age out individual cache entries.

Additional cache-control configuration parameters allow the Operator to:

- Enable/disable the entire DNS cache
- Enable/disable the caching of DNS response data on a per-DNS server basis
- Override the TTL values that are used to age DNS cache entries

The DNS caching service also supports a configurable static host mapping table, allowing Operators to associate up to five IP addresses to a domain name. This configuration table is loaded into the DNS cache, and any request for a domain that is statically mapped is served directly by the MCC without any further exchange with an Operator's DNS servers. Each static mapping table can also be associated with a network context, allowing different IP addresses to be returned, based on the network context in which a UE resides.

To add a DNS Proxy Service:

1 Use any of the following methods to add a DNS Proxy service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Global DNS Proxy Service**.

d Click **Global DNS Proxy Service**.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **User Created** tab.

d Expand **Select a Category**.

e Click **Global DNS Proxy Service**.

f Click **Global DNS Proxy Service**.

2 Configure the parameters as follows:

Table 9-90 DNS Proxy Parameters

Parameter	Description
Admin State	DNS Proxy administrative state: ■ enabled ■ disabled
Pending Request Timeout	Time in seconds to retain pending DNS request cache entries.
Max Cache Entries	Maximum number of cache entries for each DNS cache.
Positive Response TTL Override	TTL Override in seconds for caching positive DNS responses.
Negative Response TTL Override	TTL Override in seconds for caching negative DNS responses.
Static Map Entry TTL	TTL to return in any response for a static DNS entry.

3 Click the **Save** icon.

DNS Proxy Service Instance

To add a DNS Proxy Service Instance:

1 Use any of the following methods to add a DNS Proxy Service instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **DNS Proxy Instance**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New DNS Proxy Instance**.

2 Configure the parameters as follows:

Table 9-91 DNS Proxy Instance Parameters

Parameter	Description
Name	DNS Proxy Instance name

Table 9-91 DNS Proxy Instance Parameters

Parameter	Description
Admin State	Enable/Disable DNS Proxy instance: ■ disabled ■ enabled
DNS IP Flow	Select the DNS IP Flow(s) The DNS IP Flow must already exist. See DNS IP Flow. To select an DNS IP Flow, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

DNS Policy

DNS Proxy supports the DNS whitelisting capability. This feature allows Operators to only allow DNS queries to trusted DNS servers. This feature prevents any DNS fraud where the user may have configured the IP address of a rogue DNS server.

To add a DNS Policy:

1 Use any of the following methods to add a DNS Policy instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **DNS Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New DNS Policy**.

2 Configure the parameters as follows:

Table 9-92 DNS Policy Parameters

Parameter	Description
Name	DNS policy name

Table 9-92 DNS Policy Parameters

Parameter	Description
Admin State	Enable/Disable DNS policy: ■ disabled ■ enabled
Priority	DNS policy priority
Cache Control	DNS response cache control action for this policy: ■ cache-all ■ cache-none
Action	DNS request action for this policy: ■ allow ■ block ■ redirect The action dictates how the DNS server handles DNS requests. Configuration guidelines for each action are outlined in Table 9-93.
Redirect IP List	Select the DNS Redirect IP list. ***Note:*** *The IP list must not use IP address ranges.* The IP list must already exist. See IP List.

3 Click the **Save** icon.

Table 9-93 Configuration Guidelines for Policy Action

Action	DNS Server Response	Configuration Guidelines
allow	Allow DNS queries to Operator-hosted DNS servers (designated DNS servers in the network) Allow DNS queries to other trusted DNS servers (for example Google DNS)	**1** Configure a set of service-construct packet-filter objects for all Operator-hosted and other trusted DNS servers. **2** Configure services dns-proxy dns-ip-flow and associate it with the packet-filter for the trusted DNS servers. **3** Optionally, associate the dns-ip-flow with a dns-policy with action set to **`allow`** (default). The DNS-proxy based on the configuration above matches the DNS query with one of the packet-filters and the dns-ip-flow. Since the dns-ip-flow has a dns-policy with action set to **`allow`**, the dns packet is forwarded unaltered to the trusted DNS server.

block	Block DNS queries to untrusted DNS servers	1 Configure a catch-all service-construct packet-filter object for all other (untrusted) DNS servers. 2 Configure services dns-proxy dns-ip-flow with a lower priority and associate it with the packet-filter for the untrusted DNS servers. 3 Associate the dns-ip-flow with a dns-policy with action set to **`block`**.
redirect	Redirect DNS queries to untrusted DNS servers to a set of designated DNS servers	1 Configure a catch-all service-construct packet-filter object for all other (untrusted) DNS servers. 2 Configure services dns-proxy dns-ip-flow" with a lower priority and associate it with the packet-filter for the untrusted DNS servers. 3 Associate the dns-ip-flow with a dns-policy with action set to **`redirect`**. 4 Set the dns-policy redirect-ip-list to refer to a service-construct ip-list containing a list of IP addresses of trusted DNS servers.

DNS Reverse Cache

DNS reverse cache is a database to look up an IP address (IPv4 or IPv6) and return a list of host names that resolve to that IP address. This database is generated with information extracted from DNS responses by the DNS proxy. DNS reverse cache supports two modes:

- If the number of Domain Rule Groups is large and Regular Expression is expensive, all DNS responses are reverse cached.
- If the number of Domain Rule Groups is small and Regular Expression matching is relatively less expensive, only the Regular Expression matching DNS responses are reverse cached.

DNS reverse cache is used by a Domain Rule Group. See Domain Rule Group.

To add a DNS Reverse Cache:

1 Use any of the following methods to add a DNS Reverse Cache:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **DNS Reverse Cache**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New DNS Reverse Cache**.

2 Configure the parameters as follows:

Table 9-94 DNS Reverse Cache Parameters

Parameter	Description
Admin State	Enable/Disable DNS Reverse Cache: ■ disabled ■ enabled
Domain Rule Group Filtering	Enable/Disable Domain Rule Group filtering: ■ disabled ■ enabled
Max Cache Entries	Maximum number of reverse cache entries for each DNS cache.
Cache Full Alarm Threshold	Percent of the cache size that, when full, signals an alarm.
TTL Override	In Type, specify the a TTL override type: ■ add: Specify the value to add. ■ multiply-by: Specify the value to multiple by. ■ set: Specify the value to set.

3 Click the **Save** icon.

DNS IP Flow

To add a DNS IP Flow:

1 Use any of the following methods to add a DNS Proxy IP Flow:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **DNS IP Flow**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New IP Flow**.

2 Configure the parameters as follows:

Table 9-95 DNS IP Flow Parameters

Parameter	Description
Name	DNS IP Flow name
Admin State	Enable/Disable DNS IP Flow: ■ disabled ■ enabled
Priority	DNS IP Flow priority
Tunnel Detection Profile	DNS tunnel detection profile associated with this proxy instance. The Tunnel Detection Profile must already exist. See Tunnel Detection Profile.
Service Rule	Select the Service Rule to associate with the DNS IP flow. The service rule must already exist. See Service Rule. To select a Service Rule, drag and drop it from the Available list to the Selected list.
DNS Policy	Select the DNS Policies to associate with the DNS IP flow. The DNS Policy must already exist. See DNS Policy. To select a DNS Policy, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Domain Tunnel Age Time

Use this object to configure inactive blocking domain age time for DNS tunnel detection.

To add a Domain Tunnel Age Time:

1 Use any of the following methods to add a Domain Tunnel Age Time:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Domain Tunnel Age Time**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Domain Tunnel Age Time**.

2 Configure the parameters as follows:

Table 9-96 Domain Tunnel Age Time Parameters

Parameter	Description
Domain List Age Time	Inactive blocking domain age time for DNS tunnel detection
Domain List Age Time Units	Age time units: ■ seconds ■ minutes ■ hours ■ days

3 Click the **Save** icon.

Tunnel Detection Profile

Use this object to detect and block DNS tunneling transactions and receive notification of those actions. These settings reduce the possibility of DNS packets being sent to a fraud domain.

To add a Tunnel Detection Profile:

1 Use any of the following methods to add a Tunnel Detection Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Tunnel Detection Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Tunnel Detection Profile**.

2 Configure the parameters as follows:

Table 9-97 Tunnel Detection Profile Parameters

Parameter	Description
Admin State	Tunnel Detection administrative state: ■ enabled ■ disabled
Domain Cache Size	Number of the recent domains to monitor
Refresh Rate	Refresh rate for monitor interval, in seconds
Domain Penalty Time	Penalty time for blocked domain, in seconds
Clean Time	Time to turn off detail monitoring after the total hit is under threshold and there is no blocked domain, in seconds
Single Domain Threshold	Threshold for hitting rate of one singe domain in detail monitoring mode
Total DNS Hit Threshold	Threshold for overall DNS traffic rate to turn on detail monitoring mode

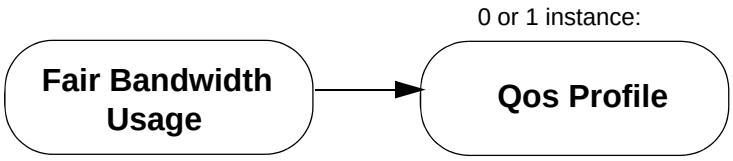
3 Click the **Save** icon.

Fair Bandwidth Usage

Fair Bandwidth Usage Management is a category of services aimed at normalizing bandwidth use when monthly subscription levels are breached. Typically, when monthly volumes are breached, the user is rate limited at a throughput defined by the carrier until the end of the subscription period. At the beginning of a new subscription period, the service is restored to the subscribed throughput rate.

The following figure illustrates the components of Fair Bandwidth Usage.

Figure 9-30 Fair Bandwidth Usage Components



To add a Fair Bandwidth Usage:

1 Use any of the following methods to add a Fair Bandwidth Usage:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Fair Bandwidth Usage**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Fair Bandwidth Usage**.

2 Configure the parameters as follows:

Table 9-98 Fair Bandwidth Usage Parameters

Parameter	Description
Name	Fair Bandwidth Usage name

Table 9-98 Fair Bandwidth Usage Parameters

Parameter	Description
Measurement Unit	Measurement unit: ■ kB ■ mB ■ gB
Reset Interval	Reset timeout interval that triggers fallback to default parameters
Minor Volume Threshold	The usage threshold at which to transition the session to utilize the **Minor QOS Profile Id**.
Minor QoS Profile Id	The Minor QoS Profile to use when the **Minor Volume Threshold** is reached. The QoS Profile must already exist. See QoS.

3 Click the **Save** icon.

HTTP Proxy (MCC versions prior to 8.4)

Acuitas does not support this object for MCC 8.4 and later releases. It has been replaced by Multi Protocol Proxy. See Multi Protocol Proxy (8.4 and later MCC versions).

HTTP Proxy acts as an intermediary for requests from clients seeking resources from other servers. The HTTP Proxy is an intercepting forward proxy that acts like the server to the UE and acts like a client to the origin server.

The HTTP Proxy function supports:

- Separate Request Policy and Response Policy to allow the Operator to specify the actions separately for request phase and response phase.
- Request Policy to notify the origin servers of the private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
- On-the-fly HTTP compression for supported client requests or all client requests.
- Setting the global compression level.
- Fraud Detection handling – HTTP Proxy performs DNS validation and Header consistency checks to determine if a request is destined for a legitimate domain or destined for a rogue proxy. If the destination IP address is not within the defined range or domain returned by the DNS lookup, the system determines if a free browsing proxy is in use and enforces a specified action (allow the traffic and charge for it and/or reduce its QoS to a specified level).
- HTTP Proxy latency – HTTP Proxy forwards HTTP request and response data as soon as possible. Fragments of request/response body are received, processed, and immediately streamed, ensuring low forwarding latencies. Typical request and response forwarding latency is within several tens of milliseconds.

  However, the HTTP Proxy transaction latency may increase when:

  – Client or server socket back-pressure due to network congestion, QoS bandwidth, or burst limits.
  – Optimization features are applied (such as compression, minification, web image optimization, preemptive, DNS, and so on).
  – Request store-and-forward-limit option is used (applies to requests using the option. The added latency depends on the request size and client uplink speed).
  – Response buffering-limit option is used (applies to responses using the option. The added latency depends on response size and client downlink speed).
  – Large objects are served from disk cache on a system with rotational media.
  – Back-End Forwarding is enabled in the system.

The HTTP Proxy service retrieves the following VSAs from the PCRF via the Gx interface and distributes these VSAs to the HTTP Proxy. MCC uses these VSAs to customize HTTP Proxy services for a particular subscriber.

- VsaEntitlement – Indicates the type of service to which the subscriber is entitled.
- VsaPaymentType – Indicates subscriber payment type. Possible values include:
  - PO – Postpaid subscriber.
  - PR – Prepaid subscriber.
  - SL
- VsaSubId – Indicates the subscriber ID.
- VsaHttpPolicy – Customize HTTP Proxy services. Possible values include:
  - NOPRXY – HTTP Proxy is disabled for the subscriber.
  - NOGZIP – Gzip compression is disabled for the subscriber.
  - NOTFD – No Toll Free Data (TFD).
  - NOVIDEO – Video optimization is disabled for the subscriber.
- VsaResellerId – Indicates the subscriber's reseller ID.
- VsaMiDial – Indicates whether the subscriber opted out from Long Term Mobile ID (LTMI) header enrichment or opted for static trusted ID in LTMI header enrichment.

Service VSAs received by the PGW are listed in Subscriber > PDN Session.

The HTTP Proxy service allows users to load unoptimized content using shortcut keys from web browsers. The shortcut keys trigger a no-cache HTTP request header to disable the following HTTP optimization features:

- DNS Preemption
- Minification
- Web image optimization
- Zip compression
- Video adaptation online transcoding

Table 9-99 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
F5	All	Refreshes a page with If-Modified-Since header, but no no-cache header

Table 9-99 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
<Ctrl>F5	Internet Explorer10 Chrome Firefox	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>F5	Chrome	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>Reload	Safari	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache

From the **Services** tab, expand **HTTP Proxy** in the left pane.

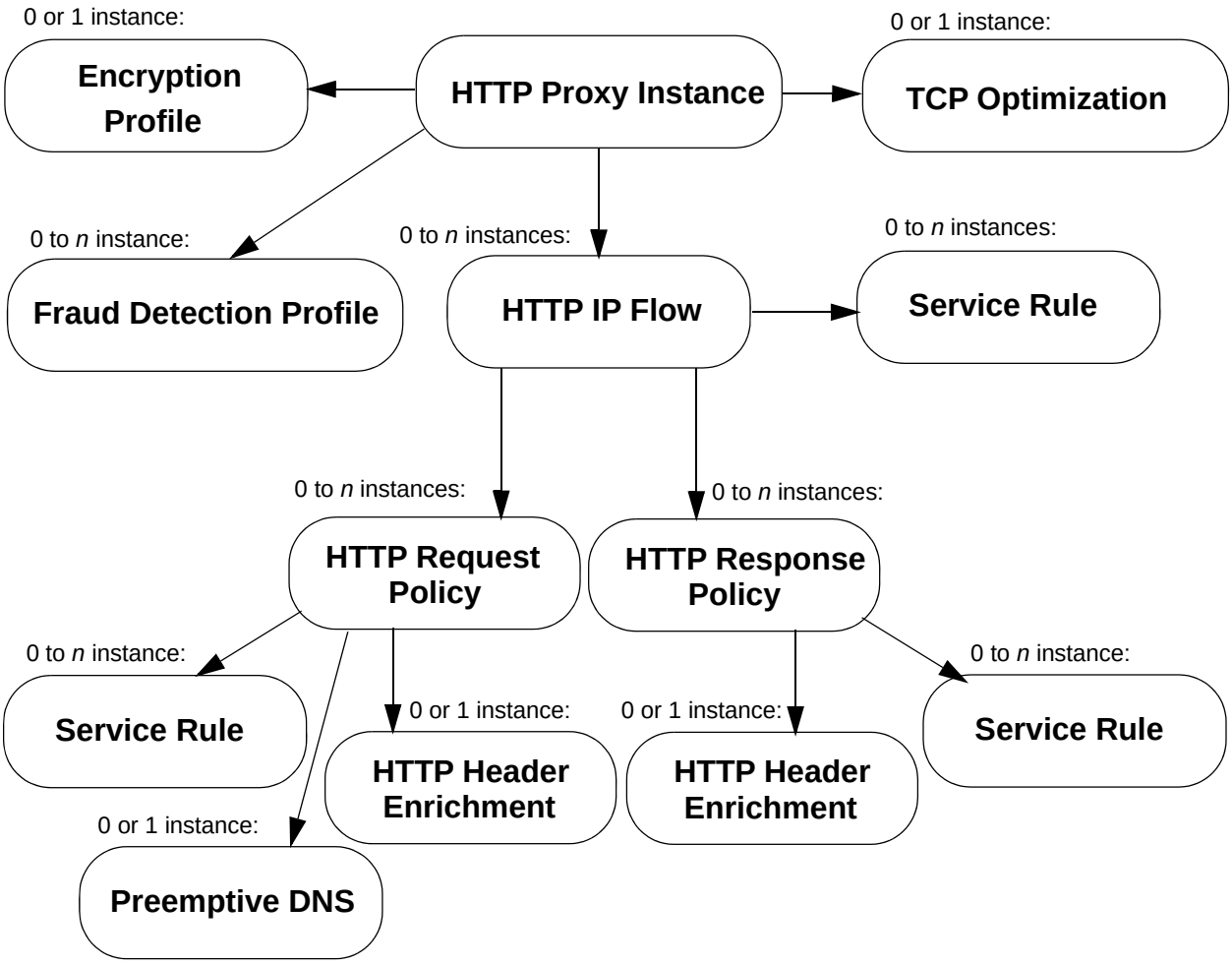
HTTP Proxy includes:

- ABR Optimization Profile
- Back End Forwarding
- Encryption Profile
- Explicit Proxy Profile
- Fraud Detection Profile
- HTTP IP Flow
- HTTP Request Policy
- HTTP Response Policy
- HTTPS Profile
- HTTP Proxy Instance
- Long Term Mobile ID (LTMI)
- Minify
- Optimization Overload Control
- Preemptive DNS
- Server Connections

- Service Data Flow
- TCP Splicing Policy
- TCP Splicing Profile
- Steering Gateway Group
- Web Image Optimization

The following figure illustrates the major components of HTTP Proxy.

Figure 9-31 HTTP Proxy Components



HTTP Proxy Service

1 Use any of the following methods to add an HTTP Proxy Service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Global HTTP Proxy Service**.

d Click **Global HTTP Proxy Service**.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **User Created** tab.

d Expand **Select a Category**.

e Click **Global HTTP Proxy Service**.

f Click **Global HTTP Proxy Service**.

2 Configure the parameters as follows:

Table 9-100 HTTP Proxy Parameters

Parameter	Description
Admin State	HTTP Proxy administrative state: ■ enabled ■ disabled
Client Idle Timeout	Client idle timeout, in seconds
Compress Level	Global compression level: ■ default-compression ■ best-compression ■ best-speed
Static DNS Map	Static DNS map to use to avoid doing DNS lookup through configured DNS server(s). The HTTP Proxy service uses the map's IP Address list to open server connections for HTTP request. The Static DNS map must already exist. See Static DNS Map.
ABR Optimization Profile:	
Name	ABR Optimization Profile name. The ABR Optimization Profile must already exist. See ABR Optimization Profile.

Table 9-100 HTTP Proxy Parameters

Parameter	Description
Admin State	ABR Optimization Profile administrative state: ■ enabled ■ disabled
Client Connections:	
Request Wait Time	Configure the client connection HTTP request wait time in milliseconds (value 0 indicates forever). Reverse hand-off is implemented and if the HTTP request is found, it is handed back to the HTTP proxy and continues to process as HTTP traffic.
Back End Forwarding:	
Admin State	Back end forwarding administrative state: ■ enabled ■ disabled
Maximum Idle Connections	Maximum number of idle connections per back end proxy
Preemptive DNS:	
Admin State	Preemptive DNS administrative state: ■ enabled ■ disable
Server Connections:	
Idle Timeout	Server connection idle timeout, in seconds.
Maximum Idle Timeout	Maximum number of idle connections per server.
Maximum Idle Connections	Total maximum number of idle server connections. Value 0 disables keeping idle connections.
Web Image Optimization:	
Admin State	Web Image Optimization administrative state: ■ enabled ■ disable
Minify:	
Admin State	Minify administrative state: ■ enabled ■ disable
Video Pacing: Video pacing is sending video data to the client at a restricted rate. The video is not completely streamed at the fastest possible rate, instead it is throttled.	

Table 9-100 HTTP Proxy Parameters

Parameter	Description
Admin State	Video Pactng administrative state: ■ enabled ■ disable
LTMI:	
The following parameters control the key import (download) from the key server using HTTPS:	
Key Import Interval	Key import interval, in minutes, zero turns off key import
Key Server URL	Network Context used for non-HTTP connections. It overrides the Network Context selected by a higher-level object.
Key Server Username	Key Server username for basic authentication.
Key Server Password	Key Server password for basic authentication.
Key Server Network Context	Key server network context
The following parameters control if and how the LTMI ID is generated:	
ID Gen Admin State	Enable/Disable LTMI ID generation: ■ enabled ■ disable
Trusted ID Divisor	Number of minutes for trusted ID rotation interval (for example, 6 months rotation = 259,200 minutes)
External ID Divisor	Number of minutes for external ID rotation interval (for example, 24 hour rotation = 1440 minutes.
Network Carrier Code	Code used in dynamic mobile IDs to identify the carrier.
Opt Out String	String used to search the opt out value to see if a subscriber has opted out of Dynamic Mobile ID. When a subscriber opts out this feature, no LTMI is inserted in the HTTP request header. If the miDial string exactly matches the Opt Out String, then the subscriber completely opts out of LTMI.
Static Trusted ID String	Ending of the search string used to identify opt out value for static trusted ID. If the miDial string ends with the Static Trusted ID String, then the Static Trusted ID is used instead of the Dynamic Trusted ID. For example, if the Static Trusted ID String is configured as "#" and the miDail string is "xyz#" (ending with "#"), then the Static Trusted ID is used instead of the Dynamic Trusted ID.

3 Click the **Save** icon.

HTTP Request Policy

To add an HTTP Request Policy:

1 Use any of the following methods to add an HTTP Request Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP Request Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Request Policy**.

2 Configure the parameters as follows:

Table 9-101 HTTP Request Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
HTTP Protocol	Protocol used towards origin server: ■ ue-http-protocol: preserves original UE protocol ■ http ■ https
Steering Group	Steering Group to use for the HTTP requests. The Steering Group must already exist. See Steering GW Group.
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for server connections.
Store Forward Buffer Limit	Maximum data to store before forwarding request to server, in KB. When the HTTP Request Policy is applied, the server connection is not opened until the received request buffer size reaches this value or entire request is received. If zero, request is immediately forwarded.

Table 9-101 HTTP Request Policy Parameters

Parameter	Description
Bypass HTTP Proxy	Specifies whether to bypass HTTP proxy for this policy: ■ disabled ■ enabled When enabled, the request is TCP spliced.
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds, removes, or replaces the specified HTTP headers/cookies in the HTTP request header. The Header Enrichment Profile must already exist. See HTTP Header Enrichment.
URL Rewrite Profile	Select the HTTP URL Rewrite Profile object. The HTTP URL Rewrite object must already exist. See HTTP URL Rewrite.
DNS Resolution	Specify whether to use DNS resolution to look up destination.
Force Compression	Specify whether to force on-the-fly HTTP compression for all client requests.
Compress Inline	Specify whether to enable on-the-fly HTTP compression for supported client requests.
Forced Cache Access Notification	Enable/Disable Forced Cache Object Access Notification to the origin server: ■ disabled ■ enabled When enabled, HTTP request policy notifies the origin servers of private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
Preemptive DNS	Specify whether to apply HTTP Proxy service level preemptive DNS for this policy: ■ on ■ off
Compress Min Size	Minimum response size in bytes required for compression to take effect
Web Image Optimization	Select the Web Image Optimization to use for HTTP requests. The Web Image Optimization must already exist. See Web Image Optimization Profile.

Table 9-101 HTTP Request Policy Parameters

Parameter	Description
Server TCP Optimization Profile	Select the TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.
Compress Max Size	Enter the maximum response size in bytes allowed for compression to take effect.
Minify Javascript	Mark the checkbox to minify JavaScript (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify HTML	Mark the checkbox to minify HTML (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify Min Size	The minimum response size in bytes required for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Max Size	The maximum response size in bytes allowed for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Css Choice	Select minify-css to minify CSS (to remove unnecessary characters such as blank characters and new line characters from source code)
Gateway IP Address	IP address for explicit Proxy. Use this parameter to steer traffic to an explicit proxy address, for cases where the mobile terminals have a hardcoded proxy IP address.
Gateway Port	Port for explicit Proxy
Service Rule	Select the service rule(s). The service rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTP Response Policy

To add an HTTP Response Policy:

1 Use any of the following methods to add an HTTP Response Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP Response Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Response Policy**.

2 Configure the parameters as follows:

Table 9-102 HTTP Response Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. The Header Enrichment Profile must already exist. See HTTP Header Enrichment. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds, removes, or replaces the specified HTTP headers/cookies in the HTTP request header.
Video Pacing Burst Time	Video Pacing burst time, in seconds. Represents the time for which the video data should be sent at a burst.
Video Pacing Factor	Video Pacing factor (scale factor 1/100) at which the video should be paced. Set to zero to disable pacing. For example, setting a Video Pacing Burst Time of 20s and a Video Pacing Factor of 100 specifies to send the initial 20 seconds of video at the maximum possible rate and to pace the video by a factor of 100 (that is, 1* bit-rate of the video).
Rate Limiting Burst Size	Rate limiting burst size, in bytes
Rate Limiting Bit Rate	Rate limiting bit rate, in bps

Table 9-102 HTTP Response Policy Parameters

Parameter	Description
Buffering Limit	Maximum data to store when processing response from origin server, in KB. When the HTTP Response Policy is applied, HTTP Proxy uses this value to determine the biggest response data size to be stored while sending the response to client. When the limit is reached, HTTP Proxy stops reading from the server socket until space is freed after some data sent to client.
Service Rule	Select the service rule(s). The service rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTP IP Flow

Configure one or more HTTP IP Flows to be processed by HTTP Proxy.

To steer traffic destined to an explicit proxy address, configured the HTTP IP Flow with a Service Rule containing a Packet Filter with matching destination IP and destination port values.

To add an HTTP IP Flow:

1 Use any of the following methods to add an HTTP IP Flow:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP IP Flow**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP IP Flow**.

2 Configure the parameters as follows:

Table 9-103 HTTP IP Flow Parameters

Parameter	Description
Name	HTTP Proxy IP Flow name
Priority	HTTP Proxy IP Flow priority
HTTP Protocol	HTTP transport protocol for the IP Flow: ■ HTTP ■ HTTPS ■ TCP TCP splicing provides the ability to enable TCP optimization for TCP-based protocols such as SFTP, FTP and HTTPS. The TCP splicing stitches the client and server TCP connections, enabling the Operator to configure the TCP parameters to be used for the client connections separately. MCC can be configured as a TCP splicing and support the following: ■ Terminate a TCP connection from the client and apply a set of TCP optimization parameters. ■ Originate a TCP connection to the server and apply a set of TCP optimization parameters. ■ Forward TCP traffic between the client and server TCP connections without parsing or disturbing the packets. ■ Teardown the TCP connections when the peer closes the sockets or idle exceeded timeout.
IP Transparency	Enable/Disable IP Transparency for the IP Flow: ■ disabled ■ enabled When IP Transparency is enabled, HTTP requests forwarded by the HTTP Proxy to origin servers contain the UE's original IP address as the source TCP/IP address in the IP packet. IP transparent proxy is an HTTP proxy mode of operation where HTTP client IP addresses (UE addresses) are used as a source when originating network-side connections to Web origin servers. HTTP proxy, using the client addresses, hides its own network identity and becomes IP transparent to Internet origin servers. When IP transparency is used, origin servers are able to determine the identity of Web clients based on the source IP addresses of the HTTP/HTTPS connections. In non-IP Transparent mode, HTTP proxy uses MCC IP loopback addresses when originating network-side connections.
State	Enable/Disable HTTP Proxy IP Flow: ■ disabled ■ enabled

Table 9-103 HTTP IP Flow Parameters

Parameter	Description
HTTP Request Policy	Select the HTTP Request Policies to bind to the IP flow. The HTTP Request Policies must already exist. See HTTP Request Policy. To select a HTTP Request Policy, drag and drop it from the Available list to the Selected list.
HTTP Response Policy	Select the HTTP Response Policies to bind to the IP flow. The HTTP Responce Policy must already exist. See HTTP Response Policy. To select a HTTP Response Policy, drag and drop it from the Available list to the Selected list.
Service Rules	Select the service rule(s) to bind with the IP flow. The Service Rule must already exist. See Service Rule. ***Note:*** *The Service Rule cannot contain an HTTP Rule Group.* To select a service rule, drag and drop it from the Available list to the Selected list.
TCP Splicing Policy	Select the TCP Splicing Policies to bind to the IP flow. The TCP Splicing Policy must already exist. See TCP Splicing Policy. To select a TCP Splicing Policy, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Encryption Profile

The Encryption Profile controls MSISDN encryption.

To add an Encryption Profile:

1 Use any of the following methods to add an Encryption Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **ACR Encryption Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New ACR Encryption Profile**.

2 Configure the parameters as follows:

Table 9-104 Encryption Profile Parameters

Parameter	Description
Name	Encryption Profile name
Admin State	Enable/Disable Encryption Profile: ■ disabled ■ enabled
Public Key Filename	The name of the public key file to be used for MSISDN encryption. The file should be placed in /tosdb/content/publickeys. Click **Choose Public Key File** to select a public key file that has already been uploaded. To upload a public key file, click **Browse** and select the public key file. Click **Upload**.
File Type	Type of public key file: ■ PEM ■ DER ■ X509

3 Click the **Save** icon.

HTTP Proxy Instance

To add an HTTP Proxy Instance:

1 Use any of the following methods to add an HTTP Proxy Instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP Proxy Instance**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Proxy Instance**.

2 Configure the parameters as follows:

Table 9-105 HTTP Proxy Instance Parameters

Parameter	Description
Name	HTTP Proxy Instance name
Admin State	Enable/Disable HTTP Proxy instance: ■ disabled ■ enabled
TCP Optimization Service	Select the TCP optimization service. The TCP optimization service must already exist. See TCP Optimization Profile.
Encryption Profile	Select the Encryption Profile. The Encryption Profile must already exist. See Encryption Profile.
MMSC Group	Select the Multimedia Messaging Service Center group. The MMSC group must already exist. See Multimedia Messaging Service Center Group.
SMSC Group	Select the Short Message Service group. The SMSC group must already exist. See Short Message Service Center Group.
LDAP Profile	Select the LDAP Profile. The LDAP Profile must already exist. See LDAP Profile.
UA Profile	Select the User Agent Profile. The UA Profile must already exist. See UA Profile.
HTTPS Profile	Select the HTTPS Profile. The HTTPS Profile must already exist. See HTTPS Profile.
Explicit Proxy Profile	Select the Explicit Proxy Profile. The Explicit Proxy Profile must already exist. See Explicit Proxy Profile.
Fraud Detection Profile	Select the Fraud Detection Profile. The Fraud Detection Profile must already exist. See Fraud Detection Profile.
Non HTTP Profile (TCP Splicing Profile)	Select the TCP Splicing Profile. The TCP Splicing Profile must already exist. See TCP Splicing Profile.
HTDR Profile	Select the HTTP Transaction Record Profile The HTTP Transaction Record Profile must already exist. See HTTP Transaction Record Profile.

Table 9-105 HTTP Proxy Instance Parameters

Parameter	Description
TCP Measurement:	
Admin State	Enable/Disable TCP measurement: ■ disabled ■ enabled - MCC calculates the TCP performance parameters for the specified sampling frequency for both uplink and downlink connections
Sampling Interval	TCP measurement sampling interval, in milliseconds
Mild Congestion Level	Mild congestion level for applying optimization (throughput in kbps)
Moderate Congestion Level	Moderate congestion level for applying optimization (throughput in kbps)
Severe Congestion Level	Severe congestion level for applying optimization (throughput in kbps)
Server Connections:	
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by the gateway subsystem.
TCP Optimization Profile	TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.
Loopback IP List	Loopback IP List for server connections. The Loopback IP List must already exist. See Loopback IP List.
Loopback Selection Algorithm	Specifies the loopback selection algorithm: ■ round-robin: HTTP Proxy selects a loopback IP from a Loopback IP List in a round-robin fashion for connections initiated to HTTP origin servers ■ session sticky: HTTP Proxy uses the same loopback IP for all connections for a given session
IP Family Preference	Specifies the preferred server connection IP family: ■ IPv4 – HTTP proxy requests both IPv4 and IPv6 server addresses and uses the IPv4 address unless it is unavailable. ■ IPv6 – HTTP proxy requests both IPv4 and IPv6 server addresses and uses the IPv6 address unless it is unavailable. ■ client-ip-family – HTTP proxy requests both IPv4 and IPv6 server addresses and uses the client-ip-family address unless it is unavailable.
Loopback Address	Select the Loopback Addresses(s). To select a Loopback Address, drag and drop it from the Available list to the Selected list.

Table 9-105 HTTP Proxy Instance Parameters

Parameter	Description
HTTP IP Flow	Select the HTTP IP Flow(s). The HTTP IP Flow must already exist. See HTTP IP Flow. To select a IP Flow, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Server Connections

To configure HTTP Proxy server connections:

1 Use any of the following methods to configure server connections:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Server Connections**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Server Connections**.

2 Configure the parameters as follows:

Table 9-106 Server Connections Parameters

Parameter	Description
Idle Timeout	Server connection idle timeout, in seconds.
Max Server Idle	Maximum number of idle connections per server. Value 0 disables keeping idle connections.
Max Total Idle	Total maximum number of idle server connections. Value 0 disables keeping idle connections.

3 Click the **Save** icon.

ABR Optimization Profile

Use this object to configure an ABR rate limiting optimization profile.

To configure an ABR Optimization Profile:

1 Use any of the following methods to configure an ABR Optimization Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **ABR Optimization Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New ABR Optimization Profile**.

2 Configure the parameters as follows:

Table 9-107 ABR Optimization Profile Parameters

Parameter	Description
Name	Optimization Profile name
Admin State	Enable/Disable the Profile: ■ disabled ■ enabled
Burst Size	Rate limiting burst size
Burst Size Unit	Burst size unit : ■ bytes ■ kbytes ■ mbytes ■ gbytes
Secondary Segment Threshold	Minimum segment threshold for bypassing secondary rate-limiting
Secondary Segment Threshold Unit	Secondary segment threshold unit: ■ bytes ■ kbytes ■ mbytes

Table 9-107 ABR Optimization Profile Parameters

Parameter	Description
Bitrate	Rate limiting bitrate
Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Secondary Segment Bitrate	Rate limiting bitrate (bits per second) for secondary segments.
Secondary Segment Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Savings Estimation Admin State	Enable/Disable estimation of optimization byte savings attributed to ABR pacing. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on content: ■ disabled ■ enabled
Sampling Interval	Sampling interval for savings estimation
Sampling Interval Unit	Sampling interval unit: ■ min ■ hr

3 Click the **Save** icon.

Explicit Proxy Profile

Use this object to configure an explicit proxy address profile.

To add an Explicit Proxy Address Profile:

1 Use any of the following methods to configure an Explicit Proxy Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Explicit Proxy Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Explicit Proxy Profile**.

2 Configure the parameters as follows:

- **Name** — Explicit Proxy Profile name.

3 In **Explicit Proxy NetworkContext**, click the **Create** icon.

4 Configure the parameters as follows:

- **Name** — Network Context to use for the explicit proxy address list.

5 In **Explicit Proxy Address**, click the **Create** icon.

6 Configure the parameters as follows:

Table 9-108 Explicit Proxy Address Parameters

Parameter	Description
Name	Export Proxy Address string
IP Address	IP Address
Port	Port

7 Click **Add**.

8 Repeat step 5 through step 7 to add as many Explicit Proxy addresses as needed.

9 Click **Add**.

10 Repeat step 2 through step 9 to add as many Explicit Proxy network contexts as needed.

11 Click the **Save** icon.

Fraud Detection Profile

The Fraud Detection Profile enables the gateway to detect and take a configured action on subscriber devices attempting data connections through fraudulent use of a web proxy. For example, the system can detect fraudulent users utilizing rogue HTTP proxies to spoof HTTP URLs for free rated sites, such as those the Carrier assigns for browsing promotions and partnerships.

To configure Fraud Detection Profile:

1 Use any of the following methods to configure a Fraud Detection Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Fraud Detection Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Fraud Detection Profile**.

2 Configure the parameters as follows:

Table 9-109 Fraud Detection Profile Parameters

Parameter	Description
Name	Fraud Detection Profile name.
Admin State	Enable/disable the Fraud Detection service: ■ enabled ■ disabled
Action	Action to take when fraud is detected: ■ allow ■ block
Block Notification Message	*Applies when Action is set to block:* HTTP Request Block Message used in the '403 forbidden' response sent to the client.

Table 9-109 Fraud Detection Profile Parameters

Parameter	Description
Service Rule	Service Rule to apply to the Fraud Detection Profile. The Service Rule specifies which requests to subject to the fraud check. For example, to apply the fraud check only to free rated websites for browsing promotions and partnerships, configure the Service Rule with the list of free-rated domains. If the fraud detection Service Rule is not configured, fraud checks are performed for *all* HTTP requests. The Service Rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.
Whitelist	Whitelist to apply to the Fraud Detection Profile. The Whitelist contains the IP addresses that represent legitimate proxies. The Whitelist must already exist. See Host List. To select a Whitelist, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTPS Profile

Use this object to enable HTTP Proxy support for HTTPS (HTTP Secure) - an HTTP protocol variant that uses secure TLS, rather than TCP, connections for communication with clients and/or servers.

MCC HTTP Proxy supports the following HTTPS features:

- HTTPS termination of client TLS connections
- HTTPS origination of TLS connections to HTTPS servers
- HTTPS pass-through

When HTTP Proxy is used to terminate clients' TLS connections to HTTPS servers, the HTTPS Profile must include TLS Termination Policies for the servers. Once terminated, HTTP Proxy decrypts and processes user HTTPS requests and applies enabled content features.

When HTTP Proxy is used to originate HTTPS server connections, server authentication is performed using a list of trusted CA certificates configured in the HTTPS Profile.

HTTPS traffic for which no TLS Termination Policy is configured bypasses HTTP Proxy logic and is passed-through between the client and server. Because the HTTPS pass-through traffic is not processed by HTTP-Proxy, content features are not applied to HTTP requests on these connections. However, connection-level features such as TCP Optimization are supported.

To add an HTTPS Profile:

1 Use any of the following methods to configure an HTTPS Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTPS Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTPS Profile**.

2 Configure the parameters as follows:

Table 9-110 HTTPS Profile Parameters

Parameter	Description
Name	HTTPS Profile name
Admin State	Admin state: ■ enabled ■ disable
Ca Certificate List	HTTPS Origination CA certificate list The Ca Certificate List must already exist. See CA Certificate List.
TLS Protocol Logging	Enable debug logging for openssl when this HTTPS Profile is used: ■ enabled ■ disable
TLS Termination Policy	Select the TLS Termination Policy to include in the HTTPS Profile. The TLS Termination Policy must already exist. See TLS Termination Policy. To select a TLS Termination Policy, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTP Transaction Record Profile

HTTP Transaction Data Records provides information about each HTTP transaction that traverses the NE. The data is represented in comma-separated values format (CSV) and written as a string of CSV values.

The HTTP Transaction Data record can include such information as:

- Time information: Request timestamp and latency information
- Subscriber information: IMSI, MSISDN, etc.
- Connection information: Network context, source and destination address, etc.
- Request information: HTTP request information
- Response information: HTTP response information
- Compression information: Compression and bytes saved, if compression is applied

- Web image Optimization information: Information about web image optimization and bytes saved, if applied.
- Video information: Information about any video served and bytes saved, if applied.
- Minification information: Information about minification and bytes saved, if applied.

The Operator can customize the records in certain positions and can include or omit certain records. Configure the following values in the Service Construct > Data Record Template > HTTP Proxy > HTTP Transaction:

- *Present Flag* – Indicates whether to include the data field in the CDR. By default, this value is set to conditional for all data fields, indicating that the data field will be filled in CDRs when available.
- *Position Index* – Location of the data field in the CDR. A pre-defined order exists for each data field if positionIndex is not configured.
- *Format Type* – The format for the data field. If not configured, the format type uses the default.
- *Length* – The fixed length of the data field. The length defaults to zero indicating the data field is written out as it is.
- *Alignment* – The alignment of the data field. If not configured, the alignment defaults to left aligned.
- *Padding* – The character used for padding when the field has a fixed length.

HTTP Transaction Data Records information can be used to:

- Calculate details, such as bandwidth savings when features like Web Image Optimization and video adaptation are enabled.
- Provide the basis for charging
- Measure analytics

Specify the HTTP transaction record profile in an HTTP Proxy instance tied to the workflow for it to take effect.

To configure HTTP Transaction Record Profile:

1. Use any of the following methods to configure an HTTP Transaction Record Profile:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category** in the left pane.

c Click **HTTP Transaction Record Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Transaction Record Profile**.

2 Configure the parameters as follows:

Table 9-111 HTTP Transaction Record Profile Parameters

Parameter	Description
Name	HTTP Transaction Data Record profile name
File Type	File type for streaming HTDR record locally: ■ Event Log ■ Data Record ■ Corefiles ■ RAM Disk-Storage ■ Storage ■ Ext-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming HTDR record locally
Encode Format	Format type: ■ CSV
Transaction Template	HTTP Transaction Record Template. Configure at Service Construct > Data Record Template > HTTP Proxy > HTTP Transaction
Record URL Length	Length to which the URL field should be truncated in the record

3 Click the **Save** icon.

Long Term Mobile ID

Use this object to configure a Long Term Mobile ID (LTMI). It supports insertion of encrypted subscriber ID in an HTTP request header to allow the subscriber ID to be communicated to origin server in a secure manner.

MCC supports the following levels of encoding/encryption formats:

- Plain Text
- LTMI Static Trusted
- LTMI dynamic Trusted
- LTMI External

Operators can opt out of the LTMI feature using the Opt Out String and Static Trusted ID String.

MCC supports the following text string VSAs used to generate LTMI and the reseller ID header. The VSAs are retrieved from the PCRF when a call is established, and delivered to the HTTP Proxy when an HTTP request header is processed.

- subID
- miDial
- resellerID

Using HTTPS, the MCC periodically downloads encryption keys from a key server. The keys can be manually imported using import LTMI key or automatically imported from the key server by configuring the minute interval using key-import-interval.

To add a long term mobile ID:

1 Use any of the following methods to configure an LTMI:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **LTMI**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New LTMI**.

2 Configure the parameters as follows:

Table 9-112 LTMI Parameters

Parameter	Description
The following parameters control the key import (download) from the key server using HTTPS:	
Key Import Interval	Key import interval, in minutes, zero turns off key import
Key Server URL	Network Context used for non-HTTP connections. It overrides the Network Context selected by a higher-level object.
Key Server Username	Key Server username for basic authentication.
Key Server Password	Key Server password for basic authentication.
Key Server Network Context	Key server network context
The following parameters control if and how the LTMI ID is generated:	
ID Gen Admin State	Enable/Disable LTMI ID generation: ■ enabled ■ disable
Trusted ID Divisor	Number of minutes for trusted ID rotation interval (for example, 6 months rotation = 259,200 minutes)
External ID Divisor	Number of minutes for external ID rotation interval (for example, 24 hour rotation = 1440 minutes.
Network Carrier Code	Code used in dynamic mobile IDs to identify the carrier.
Opt Out String	String used to search the opt out value to see if a subscriber has opted out of Dynamic Mobile ID. When a subscriber opts out this feature, no LTMI is inserted in the HTTP request header. If the miDial string exactly matches the Opt Out String, then the subscriber completely opts out of LTMI.
Static Trusted ID String	Ending of the search string used to identify opt out value for static trusted ID. If the miDial string ends with the Static Trusted ID String, then the Static Trusted ID is used instead of the Dynamic Trusted ID. For example, if the Static Trusted ID String is configured as "#" and the miDail string is "xyz#" (ending with "#"), then the Static Trusted ID is used instead of the Dynamic Trusted ID.
Extra Curl Option	Passes additional option to the curl command used to download the LTMI key.

3 Click the **Save** icon.

Steering GW Group

Use this object to configure a group of Steering Destinations.

To add a Steering GW Group:

1 Use any of the following methods to configure a Steering GW Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Steering GW Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Steering GW Group**.

2 Configure the parameters as follows:

- **Name**: Steering GW Group name.

3 In **Steering GW**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-113 Steering GW Parameters

Parameter	Description
Name	HTTP Steering Destination Name
IP Address	IP address for Steering Destination
Port	Port for Steering Destination Port
Host Name	Host Name (FQDN) of the Steering Destination

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many steering GW as needed.

7 Click the **Save** icon.

TCP Splicing Policy

Use this object to configure a policy that controls the behavior of the TCP connections that match an HTTP IP Flow. The matched traffic is forwarded to a TCP splicing component and spliced to the server.

To configure a TCP Splicing Policy:

1 Use any of the following methods to configure a TCP Splicing Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **TCP Splicing Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New TCP Splicing Policy**.

2 Click **TCP Splicing Policy**.

3 Configure the parameters as follows:

Table 9-114 TCP Splicing Policy Parameters

Parameter	Description
Name	Content TCP Splicing Policy Name
Priority	Priority of the TCP Splicing Policy, must be unique
TCP Splicing Profile	TCP Splicing Profile associated with this policy. The TCP Splicing Profile must already exist. See TCP Splicing Profile.

4 In **Service Rules**, drag and drop the as many Service Rules as needed from the Available list to the Selected list.

5 Click the **Save** icon.

TCP Splicing Profile

Use this object to configure a profile for handling of splicing traffic (data forwarding between client and server TCP connections).

HTTP proxy supports forwarding of non-HTTP traffic received on port 80. The TCP splicing component of HTTP proxy is responsible for handling of non-HTTP traffic. The component maintains a pair of client-side and server-side connections and forwards data between these connections.

To configure a TCP Splicing Profile:

1 Use any of the following methods to configure a TCP Splicing Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **TCP Splicing Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New TCP Splicing Profile**.

2 Configure the parameters as follows:

Table 9-115 TCP Splicing Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Network Context Override	Network Context used for the TCP Splicing Profile. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for splicing server connections

Table 9-115 TCP Splicing Profile Parameters

Parameter	Description
Steering Group	Configure the Steering Destinations to use for this profile. Configure the Steering Destinations to use for this profile. The Steering Group allows the UDP flow to be steered to the destination configured within itself, when the profile is selected. In the packet processing, after UDP policies are evaluated, the associated traffic-control-profile is selected. The steering group within the profile can have multiple steering-destinations. A round-robin approach is used between destinations. In case of a single steering-destination, the current UDP flow is steered to that destination. The Steering Destinations must already exist. See Steering GW Group.
Toll Free Data	Mark the checkbox to specify that toll free data applies for this profile.
Upstream Buffering Limit	Maximum data to store when processing upstream data, in KB.
Downstream Buffering Limit	Maximum data to store when processing downstream data, in KB.
Rate Limiting:	
Admin State	Admin state: ■ enabled ■ disable
Burst Size	Burst size
Burst Size Units	Burst size units: ■ bytes ■ kbytes ■ mbytes ■ gbytes
Bitrate	Bitrate
Bitrate Units	Bitrate units: ■ bps ■ kbps ■ mbps ■ gbps
Savings Estimation:	

Table 9-115 TCP Splicing Profile Parameters

Parameter	Description
Admin State	Admin state: estimation of optimization byte savings attributed to rate-limited HTTPS video traffic. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on video sessions: ■ enabled ■ disable
Sampling Interval	Sampling interval for savings estimation
Sampling Interval Unit	Unit for sampling interval for savings estimation: ■ min ■ hr

3 Click the **Save** icon.

Toll Free Profile

Use this object to configure a toll free profile to support Toll Free Data (TFD). TFD is a feature in which a third-party (content provider) pays for a subscriber's data usage when the subscriber is downloading or using the third-party company's Apps, Websites, and services. If a toll free profile is enabled, TFD is turned on for that proxy instance.

To configure a Toll Free Profile:

1 Use any of the following methods to configure a Toll Free Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Toll Free Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Toll Free Profile**.

2 Configure the parameters as follows:

Table 9-116 Toll Free Profile Parameters

Parameter	Description
CA Certificate List	CA root certificate. The CA certificate must first be placed in */public/content/tls/cacerts* before it can be configured. The Ca Certificate List must already exist. See CA Certificate List.
Certificate URL	URL prefix for certificates (for example, http://certificateserver/)
Certificate File Extension	Certificate file extension
CRL URL	URL for Certificate Revocation List (string starting with http://) When toll-free-data manifest is received before Certificate Revocation List (CRL) is available to the MCC, the manifest is processed. After parsing and signature verification, the manifest is installed into the subscriber service profile. The manifest, using revoked content provider certificate, is only removed when the UE triggers a manifest refresh (re-downloads the manifest again).
Network Context	Network context for accessing the certificate server
Loopback IP	Loopback interface for accessing the certificate server
File Type	File type for streaming the Toll Free Data record locally: ■ Event Log ■ Data Record ■ Corefiles ■ Storage ■ Ext-Storage ■ RAM Disk-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming the Toll Free Data record locally
TFD Template	Toll Free Data record template

3 Click the **Save** icon.

Web Image Optimization Profile

The HTTP Proxy Web Image Optimization Profile defines image compression and transcoding to produce a large gain in bandwidth savings for the Operator.

The profile specifies image conversion parameters such as re-compression, metadata, quality, percentage, and size. For example, you can configure the predicted size savings percentage threshold that can be optimized, such as a target JPEG quality between 0 (coarsest) and 100 (finest quantization). You associate a Web Image Optimization Profile with an HTTP Request Policy.

To configure HTTP Proxy Web Image Optimization Profile:

1 Use any of the following methods to configure a HTTP Proxy Web Image Optimization Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Web Image Optimization Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Web Image Optimization Profile**.

2 Configure the parameters as follows:

Table 9-117 Web Image Optimization Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Convert PNG to JPEG	Mark the checkbox to allow conversion of PNG to JPEG.
Convert GIF to PNG	Mark the checkbox to allow conversion of GIF to PNG.
Convert GIF to JPEG	Mark the checkbox to allow conversion of GIF to JPEG.
Sample JPEG to 420	Mark the checkbox to allow 4:2:0 chroma subsampling of JPEG.
Interlace Image	Mark the checkbox to allow interlace image
Quantize Image	Mark the checkbox to allow requantization of palettized image.
Resize Image	Mark the checkbox to allow resizing of image.

Table 9-117 Web Image Optimization Profile Parameters

Parameter	Description
Remove Metadata	Mark the checkbox to allow removal of image metadata.
Target JPEG Quality	Target JPEG quality, with 0 being the coarsest quantization, and 100 being the finest quantization.
Target Max Size	Target maximum size (in KB) that can be optimized.
Source Min Size	Source minimum size (in KB) that can be optimized.
Size Saving Threshold	Predicted size saving percentage threshold that can be optimized.
Source Max Size	Source maximum size (in KB) that can be optimized.

3 Click the **Save** icon.

HTTP Server Entitlement Service

Use this object to configure an Entitlement Service mapping.

The entitlement server is used by subscriber mobile devices to obtain information as to which services a subscriber is entitled. The entitlement server provides the ability for the UE to query and determine if a subscriber is entitled to certain services. The entitlement server is also used to obtain a signed MSISDN that is used with the registration server.

The entitlement server supports two types of entitlement:

- *Simple (http)* – Uses GET requests with no security. The simple entitlement protocol flow is as follows:
  - Subscriber device sends HTTP GET request to entitlement server; the URL contains service name
  - Entitlement server responds with HTTP status code (success or disallowed) for the queried service
- *Secure (https)* – Uses POST method and the body is in JSON format. The entitlement.py script contains the certificates to chain back to the Trusted Certificate Authority.

  The secure entitlement protocol flow is as follows:
  - PGW obtains a list of services to which the subscriber is entitled. The Gx interface contains a set of Vendor Specific Attributes (VSAs)
  - Subscriber Device sends HTTPS POST request to Entitlement Server; the payload used JSON formatting and gzip compression
  - Entitlement Server responds with subscriber status code (success or disallowed) for each queried service
  - Entitlement Server responds with MSISDN and signature of the nonce+MSIDSN for the MSISDN query
  - HTTP response is sent in the gzipped JSON format

An Entitlement Service global configuration specifies the mapping between the URI and the internal VSA name. Affirmed Networks implements the entitlement server using a server plugin method. The plugin uses this mapping to determine whether the service exists in the Vendor Specific Attributes (VSAs) coming in from the service-metadata.

To add an Entitlement Service:

1 Use any of the following methods to configure an HTTP Entitlement Service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP Server Entitlement Service**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Server Entitlement Service**.

2 Configure the parameters as follows:

Table 9-118 HTTP Server Entitlement Service Parameters

Parameter	Description
Name	Entitlement service name.
URI	URI of the service. If configured, the URI must be unique.
Entitlement VSA Value	Entitlement Vendor Specific Attribute Value

3 Click the **Save** icon.

HTTP Server Policy

For an entitlement server, associate two HTTP Server Policies with the instance: simple and secure entitlement. The policies reference a server plugin script that is responsible for processing the request and generating a response and a Service Rule to match the request to a policy. Associate this policy with a Service Rule.

To add an HTTP Server Policy:

1 Use any of the following methods to configure an HTTP Server Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP Server Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Server Policy**.

2 Configure the parameters as follows:

Table 9-119 HTTP Server Parameters

Parameter	Description
Name	HTTP Server Policy name
Priority	Priority of the http-server-policy, must be unique This value resolves conflicts in the case of multiple policies. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Server Plugin	Server plugin associated to this policy
Service Rule	Select the service rule(s) to link with the HTTP Server Policy. The service rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Metering Service

The metering service instance contains a set of metering rating groups to convey the usage counts to the gateway. Each metering rating group has a configurable threshold and an optional AOC landing page URL.

To add a Metering Service instance:

1 Use any of the following methods to add a Metering Service instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Metering Instance**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Metering Instance**.

2 Configure the parameters as follows:

Table 9-120 Metering Instance Parameters

Parameter	Description
Name	Metering Service instance name
State	Admin state: ■ enabled ■ disable
Rating Group List	Select the Rating Groups to associate with the Metering Instance. The Rating Group must already exist. See Rating Group. To select a Rating Group, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Multi Protocol Proxy (8.4 and later MCC versions)

Multi Protocol Proxy acts as an intermediary for requests from clients seeking resources from other servers. The Multi Protocol Proxy is an intercepting forward proxy that acts like the server to the UE and acts like a client to the origin server.

The Multi Protocol Proxy function supports:

- Separate Request Policy and Response Policy to allow the Operator to specify the actions separately for request phase and response phase.
- Request Policy to notify the origin servers of the private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
- On-the-fly HTTP compression for supported client requests or all client requests.
- Setting the global compression level.
- Fraud Detection handling – Multi Protocol Proxy performs DNS validation and Header consistency checks to determine if a request is destined for a legitimate domain or destined for a rogue proxy. If the destination IP address is not within the defined range or domain returned by the DNS lookup, the system determines if a free browsing proxy is in use and enforces a specified action (allow the traffic and charge for it and/or reduce its QoS to a specified level).
- Multi Protocol Proxy latency – Multi Protocol Proxy forwards HTTP request and response data as soon as possible. Fragments of request/response body are received, processed, and immediately streamed, ensuring low forwarding latencies. Typical request and response forwarding latency is within several tens of milliseconds.

  However, the Multi Protocol Proxy transaction latency may increase when:

  – Client or server socket back-pressure due to network congestion, QoS bandwidth, or burst limits.
  – Optimization features are applied (such as compression, minification, web image optimization, preemptive, DNS, and so on).
  – Request store-and-forward-limit option is used (applies to requests using the option. The added latency depends on the request size and client uplink speed).
  – Response buffering-limit option is used (applies to responses using the option. The added latency depends on response size and client downlink speed).
  – Large objects are served from disk cache on a system with rotational media.
  – Back-End Forwarding is enabled in the system.

The Multi Protocol Proxy service retrieves the following VSAs from the PCRF via the Gx interface and distributes these VSAs to the Multi Protocol Proxy. MCC uses these VSAs to customize Multi Protocol Proxy services for a particular subscriber.

- VsaEntitlement – Indicates the type of service to which the subscriber is entitled.
- VsaPaymentType – Indicates subscriber payment type. Possible values include:
  - PO – Postpaid subscriber.
  - PR – Prepaid subscriber.
  - SL
- VsaSubId – Indicates the subscriber ID.
- VsaHttpPolicy – Customize Multi Protocol Proxy services. Possible values include:
  - NOPRXY – Multi Protocol Proxy is disabled for the subscriber.
  - NOGZIP – Gzip compression is disabled for the subscriber.
  - NOTFD – No Toll Free Data (TFD).
  - NOVIDEO – Video optimization is disabled for the subscriber.
- VsaResellerId – Indicates the subscriber's reseller ID.
- VsaMiDial – Indicates whether the subscriber opted out from Long Term Mobile ID (LTMI) header enrichment or opted for static trusted ID in LTMI header enrichment.

Service VSAs received by the PGW are listed in Subscriber > PDN Session.

The Multi Protocol Proxy service allows users to load unoptimized content using shortcut keys from web browsers. The shortcut keys trigger a no-cache HTTP request header to disable the following HTTP optimization features:

- DNS Preemption
- Minification
- Web image optimization
- Zip compression
- Video adaptation online transcoding

Table 9-121 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
F5	All	Refreshes a page with If-Modified-Since header, but no no-cache header

Table 9-121 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
<Ctrl>F5	Internet Explorer10 Chrome Firefox	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>F5	Chrome	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>Reload	Safari	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache

From the **Services** tab, expand **Multi Protocol Proxy** in the left pane.

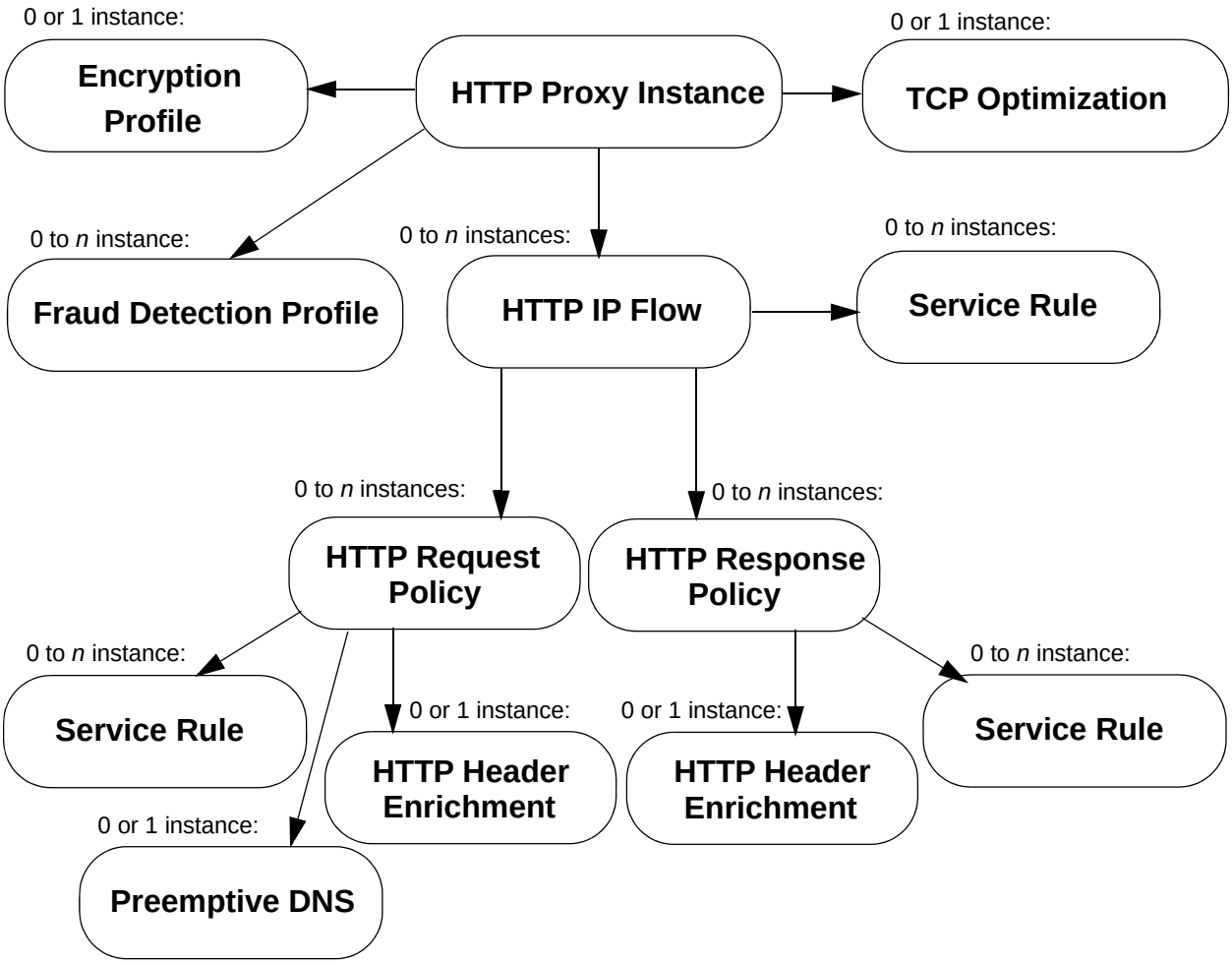
Multi Protocol Proxy includes:

- ABR Optimization Profile
- Back End Forwarding
- Encryption Profile
- Explicit Proxy Profile
- Fraud Detection Profile
- HTTP IP Flow
- HTTP Request Policy
- HTTP Response Policy
- HTTPS Profile
- HTTP Proxy Instance
- Long Term Mobile ID (LTMI)
- Minify
- Optimization Overload Control
- Preemptive DNS
- Server Connections

- Service Data Flow
- TCP Splicing Policy
- TCP Splicing Profile
- Steering Gateway Group
- Web Image Optimization

The following figure illustrates the major components of Multi Protocol Proxy.

Figure 9-32 Multi Protocol Proxy Components



Multi Protocol Proxy Service

1 Use any of the following methods to add a Multi Protocol Proxy Service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Global Multi Protocol Proxy Service**.

d Click **Global Multi Protocol Proxy Service**.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **User Created** tab.

d Expand **Select a Category**.

e Click **Global Multi Protocol Proxy Service**.

f Click **Global Multi Protocol Proxy Service**.

2 Configure the parameters as follows:

Table 9-122 Multi Protocol Proxy Parameters

Parameter	Description
Admin State	Multi Protocol Proxy administrative state: ■ enabled ■ disabled
Client Idle Timeout	Client idle timeout, in seconds
Compress Level	Global compression level: ■ default-compression ■ best-compression ■ best-speed
Static DNS Map	Static DNS map to use to avoid doing DNS lookup through configured DNS server(s). The Multi Protocol Proxy service uses the map's IP Address list to open server connections for HTTP request. The Static DNS map must already exist. See Static DNS Map.
ABR Optimization Profile:	
Name	ABR Optimization Profile name. The ABR Optimization Profile must already exist. See ABR Optimization Profile.

Table 9-122 Multi Protocol Proxy Parameters

Parameter	Description
Admin State	ABR Optimization Profile administrative state: ■ enabled ■ disabled
Client Connections:	
Request Wait Time	Configure the client connection HTTP request wait time in milliseconds (value 0 indicates forever). Reverse hand-off is implemented and if the HTTP request is found, it is handed back to the Multi Protocol Proxy and continues to process as HTTP traffic.
Back End Forwarding:	
Admin State	Back end forwarding administrative state: ■ enabled ■ disabled
Maximum Idle Connections	Maximum number of idle connections per back end proxy
Preemptive DNS:	
Admin State	Preemptive DNS administrative state: ■ enabled ■ disable
Server Connections:	
Idle Timeout	Server connection idle timeout, in seconds.
Maximum Idle Timeout	Maximum number of idle connections per server.
Maximum Idle Connections	Total maximum number of idle server connections. Value 0 disables keeping idle connections.
Web Image Optimization:	
Admin State	Web Image Optimization administrative state: ■ enabled ■ disable
Minify:	
Admin State	Minify administrative state: ■ enabled ■ disable
Video Pacing: Video pacing is sending video data to the client at a restricted rate. The video is not completely streamed at the fastest possible rate, instead it is throttled.	

Table 9-122 Multi Protocol Proxy Parameters

Parameter	Description
Admin State	Video Pactng administrative state: ■ enabled ■ disable
LTMI:	
The following parameters control the key import (download) from the key server using HTTPS:	
Key Import Interval	Key import interval, in minutes, zero turns off key import
Key Server URL	Network Context used for non-HTTP connections. It overrides the Network Context selected by a higher-level object.
Key Server Username	Key Server username for basic authentication.
Key Server Password	Key Server password for basic authentication.
Key Server Network Context	Key server network context
The following parameters control if and how the LTMI ID is generated:	
ID Gen Admin State	Enable/Disable LTMI ID generation: ■ enabled ■ disable
Trusted ID Divisor	Number of minutes for trusted ID rotation interval (for example, 6 months rotation = 259,200 minutes)
External ID Divisor	Number of minutes for external ID rotation interval (for example, 24 hour rotation = 1440 minutes.
Network Carrier Code	Code used in dynamic mobile IDs to identify the carrier.
Opt Out String	String used to search the opt out value to see if a subscriber has opted out of Dynamic Mobile ID. When a subscriber opts out this feature, no LTMI is inserted in the HTTP request header. If the miDial string exactly matches the Opt Out String, then the subscriber completely opts out of LTMI.
Static Trusted ID String	Ending of the search string used to identify opt out value for static trusted ID. If the miDial string ends with the Static Trusted ID String, then the Static Trusted ID is used instead of the Dynamic Trusted ID. For example, if the Static Trusted ID String is configured as "#" and the miDail string is "xyz#" (ending with "#"), then the Static Trusted ID is used instead of the Dynamic Trusted ID.

3 Click the **Save** icon.

HTTP Request Policy

To add an HTTP Request Policy:

1 Use any of the following methods to add an HTTP Request Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP Request Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Request Policy**.

2 Configure the parameters as follows:

Table 9-123 HTTP Request Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
HTTP Protocol	Protocol used towards origin server: ■ ue-http-protocol: preserves original UE protocol ■ http ■ https
Steering Group	Steering Group to use for the HTTP requests. The Steering Group must already exist. See Steering GW Group.
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for server connections.
Store Forward Buffer Limit	Maximum data to store before forwarding request to server, in KB. When the HTTP Request Policy is applied, the server connection is not opened until the received request buffer size reaches this value or entire request is received. If zero, request is immediately forwarded.

Table 9-123 HTTP Request Policy Parameters

Parameter	Description
Bypass HTTP Proxy	Specifies whether to bypass HTTP proxy for this policy: ■ disabled ■ enabled When enabled, the request is TCP spliced.
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds, removes, or replaces the specified HTTP headers/cookies in the HTTP request header. The Header Enrichment Profile must already exist. See HTTP Header Enrichment.
URL Rewrite Profile	Select the HTTP URL Rewrite Profile object. The HTTP URL Rewrite object must already exist. See HTTP URL Rewrite.
DNS Resolution	Specify whether to use DNS resolution to look up destination.
Force Compression	Specify whether to force on-the-fly HTTP compression for all client requests.
Compress Inline	Specify whether to enable on-the-fly HTTP compression for supported client requests.
Forced Cache Access Notification	Enable/Disable Forced Cache Object Access Notification to the origin server: ■ disabled ■ enabled When enabled, HTTP request policy notifies the origin servers of private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
Preemptive DNS	Specify whether to apply HTTP Proxy service level preemptive DNS for this policy: ■ on ■ off
Compress Min Size	Minimum response size in bytes required for compression to take effect
Web Image Optimization	Select the Web Image Optimization to use for HTTP requests. The Web Image Optimization must already exist. See Web Image Optimization Profile.

Table 9-123 HTTP Request Policy Parameters

Parameter	Description
Server TCP Optimization Profile	Select the TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.
Compress Max Size	Enter the maximum response size in bytes allowed for compression to take effect.
Minify Javascript	Mark the checkbox to minify JavaScript (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify HTML	Mark the checkbox to minify HTML (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify Min Size	The minimum response size in bytes required for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Max Size	The maximum response size in bytes allowed for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Css Choice	Select minify-css to minify CSS (to remove unnecessary characters such as blank characters and new line characters from source code)
Gateway IP Address	IP address for explicit Proxy. Use this parameter to steer traffic to an explicit proxy address, for cases where the mobile terminals have a hardcoded proxy IP address.
Gateway Port	Port for explicit Proxy
Service Rule	Select the service rule(s). The service rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTP Response Policy

To add an HTTP Response Policy:

1 Use any of the following methods to add an HTTP Response Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTP Response Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Response Policy**.

2 Configure the parameters as follows:

Table 9-124 HTTP Response Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. The Header Enrichment Profile must already exist. See HTTP Header Enrichment. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds, removes, or replaces the specified HTTP headers/cookies in the HTTP request header.
Video Pacing Burst Time	Video Pacing burst time, in seconds. Represents the time for which the video data should be sent at a burst.
Video Pacing Factor	Video Pacing factor (scale factor 1/100) at which the video should be paced. Set to zero to disable pacing. For example, setting a Video Pacing Burst Time of 20s and a Video Pacing Factor of 100 specifies to send the initial 20 seconds of video at the maximum possible rate and to pace the video by a factor of 100 (that is, 1* bit-rate of the video).
Rate Limiting Burst Size	Rate limiting burst size, in bytes
Rate Limiting Bit Rate	Rate limiting bit rate, in bps

Table 9-124 HTTP Response Policy Parameters

Parameter	Description
Buffering Limit	Maximum data to store when processing response from origin server, in KB. When the HTTP Response Policy is applied, HTTP Proxy uses this value to determine the biggest response data size to be stored while sending the response to client. When the limit is reached, HTTP Proxy stops reading from the server socket until space is freed after some data sent to client.
Service Rule	Select the service rule(s). The service rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

IP Flow

Configure one or more IP Flows to be processed by Multi Protocol Proxy.

To steer traffic destined to an explicit proxy address, configured the IP Flow with a Service Rule containing a Packet Filter with matching destination IP and destination port values.

To add an IP Flow:

1 Use any of the following methods to add an IP Flow:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **IP Flow**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New IP Flow**.

2 Configure the parameters as follows:

Table 9-125 IP Flow Parameters

Parameter	Description
Name	IP Flow name
Priority	IP Flow priority
HTTP Protocol	HTTP transport protocol for the IP Flow: ■ HTTP ■ HTTPS ■ TCP ■ UDP TCP splicing provides the ability to enable TCP optimization for TCP-based protocols such as SFTP, FTP and HTTPS. The TCP splicing stitches the client and server TCP connections, enabling the Operator to configure the TCP parameters to be used for the client connections separately. MCC can be configured as a TCP splicing and support the following: ■ Terminate a TCP connection from the client and apply a set of TCP optimization parameters. ■ Originate a TCP connection to the server and apply a set of TCP optimization parameters. ■ Forward TCP traffic between the client and server TCP connections without parsing or disturbing the packets. ■ Teardown the TCP connections when the peer closes the sockets or idle exceeded timeout.
IP Transparency	Enable/Disable IP Transparency for the IP Flow: ■ disabled ■ enabled When IP Transparency is enabled, HTTP requests forwarded by the HTTP Proxy to origin servers contain the UE's original IP address as the source TCP/IP address in the IP packet. IP transparent proxy is an HTTP proxy mode of operation where HTTP client IP addresses (UE addresses) are used as a source when originating network-side connections to Web origin servers. HTTP proxy, using the client addresses, hides its own network identity and becomes IP transparent to Internet origin servers. When IP transparency is used, origin servers are able to determine the identity of Web clients based on the source IP addresses of the HTTP/HTTPS connections. In non-IP Transparent mode, HTTP proxy uses MCC IP loopback addresses when originating network-side connections.
State	Enable/Disable IP Flow: ■ disabled ■ enabled

Table 9-125 IP Flow Parameters

Parameter	Description
HTTP Request Policy	Select the HTTP Request Policies to bind to the IP flow. The HTTP Request Policies must already exist. See HTTP Request Policy. To select a HTTP Request Policy, drag and drop it from the Available list to the Selected list.
HTTP Response Policy	Select the HTTP Response Policies to bind to the IP flow. The HTTP Responce Policy must already exist. See HTTP Response Policy. To select a HTTP Response Policy, drag and drop it from the Available list to the Selected list.
Service Rules	Select the service rule(s) to bind with the IP flow. The Service Rule must already exist. See Service Rule. ***Note:*** *The Service Rule cannot contain an HTTP Rule Group.* To select a service rule, drag and drop it from the Available list to the Selected list.
TCP Splicing Policy	Select the TCP Splicing Policies to bind to the IP flow. The TCP Splicing Policy must already exist. See TCP Splicing Policy. To select a TCP Splicing Policy, drag and drop it from the Available list to the Selected list.
UDP Policy	Select the QUIC Policies to bind to the IP flow. The TCP Splicing Policy must already exist. To select a QUIC Policy, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Encryption Profile

The Encryption Profile controls MSISDN encryption.

To add an Encryption Profile:

1 Use any of the following methods to add an Encryption Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Encryption Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Encryption Profile**.

2 Configure the parameters as follows:

Table 9-126 Encryption Profile Parameters

Parameter	Description
Name	Encryption Profile name
Admin State	Enable/Disable Encryption Profile: ■ disabled ■ enabled
Public Key Filename	The name of the public key file to be used for MSISDN encryption. The file should be placed in /tosdb/content/publickeys. Click **Choose Public Key File** to select a public key file that has already been uploaded. To upload a public key file, click **Browse** and select the public key file. Click **Upload**.
File Type	Type of public key file: ■ PEM ■ DER ■ X509

3 Click the **Save** icon.

Proxy Instance

To add a Proxy Instance:

1 Use any of the following methods to add a Proxy Instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Instance**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Instance**.

2 Configure the parameters as follows:

Table 9-127 Instance Parameters

Parameter	Description
Name	HTTP Proxy Service Instance name
Admin State	Enable/Disable HTTP Proxy instance: ■ disabled ■ enabled
TCP Optimization Service	Select the TCP optimization service. The TCP optimization service must already exist. See TCP Optimization Profile.
Encryption Profile	Select the Encryption Profile. The Encryption Profile must already exist. See Encryption Profile.
MMSC Group	Select the Multimedia Messaging Service Center group. The MMSC group must already exist. See Multimedia Messaging Service Center Group.
SMSC Group	Select the Short Message Service group. The SMSC group must already exist. See Short Message Service Center Group.
LDAP Profile	Select the LDAP Profile. The LDAP Profile must already exist. See LDAP Profile.
UA Profile	Select the User Agent Profile. The UA Profile must already exist. See UA Profile.
HTTPS Profile	Select the HTTPS Profile. The HTTPS Profile must already exist. See HTTPS Profile.
Explicit Proxy Profile	Select the Explicit Proxy Profile. The Explicit Proxy Profile must already exist. See Explicit Proxy Profile.
Fraud Detection Profile	Select the Fraud Detection Profile. The Fraud Detection Profile must already exist. See Fraud Detection Profile.

Table 9-127 Instance Parameters

Parameter	Description
Non HTTP Profile (TCP Splicing Profile)	Select the TCP Splicing Profile. The TCP Splicing Profile must already exist. See Traffic Control Profile.
HTDR Profile	Select the HTTP Transaction Record Profile The HTTP Transaction Record Profile must already exist. See HTTP Transaction Record Profile.
TCP Measurement:	
Admin State	Enable/Disable TCP measurement: ■ disabled ■ enabled - MCC calculates the TCP performance parameters for the specified sampling frequency for both uplink and downlink connections
Sampling Interval	TCP measurement sampling interval, in milliseconds
Mild Congestion Level	Mild congestion level for applying optimization (throughput in kbps)
Moderate Congestion Level	Moderate congestion level for applying optimization (throughput in kbps)
Severe Congestion Level	Severe congestion level for applying optimization (throughput in kbps)
Server Connections:	
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by the gateway subsystem.
TCP Optimization Profile	TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.
Loopback IP List	Loopback IP List for server connections. The Loopback IP List must already exist. See Loopback IP List.
Loopback Selection Algorithm	Specifies the loopback selection algorithm: ■ round-robin: Selects a loopback IP from a Loopback IP List in a round-robin fashion for connections initiated to HTTP origin servers ■ session sticky: Uses the same loopback IP for all connections for a given session

Table 9-127 Instance Parameters

Parameter	Description
IP Family Preference	Specifies the preferred server connection IP family: ■ IPv4 – Requests both IPv4 and IPv6 server addresses and uses the IPv4 address unless it is unavailable. ■ IPv6 – Requests both IPv4 and IPv6 server addresses and uses the IPv6 address unless it is unavailable. ■ client-ip-family – Requests both IPv4 and IPv6 server addresses and uses the client-ip-family address unless it is unavailable.
Loopback Address	Select the Loopback Addresses(s). To select a Loopback Address, drag and drop it from the Available list to the Selected list.
IP Flow	Select the IP Flow(s). The IP Flow must already exist. See IP Flow. To select an IP Flow, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Server Connections

To configure server connections:

1 Use any of the following methods to configure server connections:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Server Connections**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Server Connections**.

2 Configure the parameters as follows:

Table 9-128 Server Connections Parameters

Parameter	Description
Idle Timeout	Server connection idle timeout, in seconds.
Max Server Idle	Maximum number of idle connections per server. Value 0 disables keeping idle connections.
Max Total Idle	Total maximum number of idle server connections. Value 0 disables keeping idle connections.

3 Click the **Save** icon.

ABR Optimization Profile

Use this object to configure an ABR rate limiting optimization profile.

To configure an ABR Optimization Profile:

1 Use any of the following methods to configure an ABR Optimization Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **ABR Optimization Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New ABR Optimization Profile**.

2 Configure the parameters as follows:

Table 9-129 ABR Optimization Profile Parameters

Parameter	Description
Name	Optimization Profile name
Admin State	Enable/Disable the Profile: ■ disabled ■ enabled
Burst Size	Rate limiting burst size

Table 9-129 ABR Optimization Profile Parameters

Parameter	Description
Burst Size Unit	Burst size unit : ■ bytes ■ kbytes ■ mbytes ■ gbytes
Secondary Segment Threshold	Minimum segment threshold for bypassing secondary rate-limiting
Secondary Segment Threshold Unit	Secondary segment threshold unit: ■ bytes ■ kbytes ■ mbytes
Bitrate	Rate limiting bitrate
Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Secondary Segment Bitrate	Rate limiting bitrate (bits per second) for secondary segments.
Secondary Segment Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Savings Estimation Admin State	Enable/Disable estimation of optimization byte savings attributed to ABR pacing. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on content: ■ disabled ■ enabled
Sampling Interval	Sampling interval for savings estimation
Sampling Interval Unit	Sampling interval unit: ■ min ■ hr

3 Click the **Save** icon.

Explicit Proxy Profile

Use this object to configure an explicit proxy address profile.

To add an Explicit Proxy Address Profile:

1 Use any of the following methods to configure an Explicit Proxy Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Explicit Proxy Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Explicit Proxy Profile**.

2 Configure the parameters as follows:

- **Name** — Explicit Proxy Profile name.

3 In **Explicit Proxy NetworkContext**, click the **Create** icon.

4 Configure the parameters as follows:

- **Name** — Network Context to use for the explicit proxy address list.

5 In **Explicit Proxy Address**, click the **Create** icon.

6 Configure the parameters as follows:

Table 9-130 Explicit Proxy Address Parameters

Parameter	Description
Name	Export Proxy Address string
IP Address	IP Address
Port	Port

7 Click **Add**.

8 Repeat step 5 through step 7 to add as many Explicit Proxy addresses as needed.

9 Click **Add**.

10 Repeat step 2 through step 9 to add as many Explicit Proxy network contexts as needed.

11 Click the **Save** icon.

Fraud Detection Profile

The Fraud Detection Profile enables the gateway to detect and take a configured action on subscriber devices attempting data connections through fraudulent use of a web proxy. For example, the system can detect fraudulent users utilizing rogue HTTP proxies to spoof HTTP URLs for free rated sites, such as those the Carrier assigns for browsing promotions and partnerships.

To configure Fraud Detection Profile:

1 Use any of the following methods to configure a Fraud Detection Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Fraud Detection Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Fraud Detection Profile**.

2 Configure the parameters as follows:

Table 9-131 Fraud Detection Profile Parameters

Parameter	Description
Name	Fraud Detection Profile name.
Admin State	Enable/disable the Fraud Detection service: ■ enabled ■ disabled
Action	Action to take when fraud is detected: ■ allow ■ block
Block Notification Message	*Applies when Action is set to block:* HTTP Request Block Message used in the ‘403 forbidden’ response sent to the client.

Table 9-131 Fraud Detection Profile Parameters

Parameter	Description
Service Rule	Service Rule to apply to the Fraud Detection Profile. The Service Rule specifies which requests to subject to the fraud check. For example, to apply the fraud check only to free rated websites for browsing promotions and partnerships, configure the Service Rule with the list of free-rated domains. If the fraud detection Service Rule is not configured, fraud checks are performed for *all* HTTP requests. The Service Rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.
Whitelist	Whitelist to apply to the Fraud Detection Profile. The Whitelist contains the IP addresses that represent legitimate proxies. The Whitelist must already exist. See Host List. To select a Whitelist, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTPS Profile

Use this object to enable HTTP Proxy support for HTTPS (HTTP Secure) - an HTTP protocol variant that uses secure TLS, rather than TCP, connections for communication with clients and/or servers.

MCC HTTP Proxy supports the following HTTPS features:

- HTTPS termination of client TLS connections
- HTTPS origination of TLS connections to HTTPS servers
- HTTPS pass-through

When HTTP Proxy is used to terminate clients' TLS connections to HTTPS servers, the HTTPS Profile must include TLS Termination Policies for the servers. Once terminated, HTTP Proxy decrypts and processes user HTTPS requests and applies enabled content features.

When HTTP Proxy is used to originate HTTPS server connections, server authentication is performed using a list of trusted CA certificates configured in the HTTPS Profile.

HTTPS traffic for which no TLS Termination Policy is configured bypasses HTTP Proxy logic and is passed-through between the client and server. Because the HTTPS pass-through traffic is not processed by HTTP-Proxy, content features are not applied to HTTP requests on these connections. However, connection-level features such as TCP Optimization are supported.

To add an HTTPS Profile:

1 Use any of the following methods to configure an HTTPS Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **HTTPS Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTPS Profile**.

2 Configure the parameters as follows:

Table 9-132 HTTPS Profile Parameters

Parameter	Description
Name	HTTPS Profile name
Admin State	Admin state: ■ enabled ■ disable
Ca Certificate List	HTTPS Origination CA certificate list The Ca Certificate List must already exist. See CA Certificate List.
TLS Protocol Logging	Enable debug logging for openssl when this HTTPS Profile is used: ■ enabled ■ disable
TLS Termination Policy	Select the TLS Termination Policy to include in the HTTPS Profile. The TLS Termination Policy must already exist. See TLS Termination Policy. To select a TLS Termination Policy, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTP Transaction Record Profile

HTTP Transaction Data Records provides information about each HTTP transaction that traverses the NE. The data is represented in comma-separated values format (CSV) and written as a string of CSV values.

The HTTP Transaction Data record can include such information as:

- Time information: Request timestamp and latency information
- Subscriber information: IMSI, MSISDN, etc.
- Connection information: Network context, source and destination address, etc.
- Request information: HTTP request information
- Response information: HTTP response information
- Compression information: Compression and bytes saved, if compression is applied

- Web image Optimization information: Information about web image optimization and bytes saved, if applied.
- Video information: Information about any video served and bytes saved, if applied.
- Minification information: Information about minification and bytes saved, if applied.

The Operator can customize the records in certain positions and can include or omit certain records. Configure the following values in the Service Construct > Data Record Template > Multi Protocol Proxy > HTTP Transaction:

- *Present Flag* – Indicates whether to include the data field in the CDR. By default, this value is set to conditional for all data fields, indicating that the data field will be filled in CDRs when available.
- *Position Index* – Location of the data field in the CDR. A pre-defined order exists for each data field if positionIndex is not configured.
- *Format Type* – The format for the data field. If not configured, the format type uses the default.
- *Length* – The fixed length of the data field. The length defaults to zero indicating the data field is written out as it is.
- *Alignment* – The alignment of the data field. If not configured, the alignment defaults to left aligned.
- *Padding* – The character used for padding when the field has a fixed length.

HTTP Transaction Data Records information can be used to:

- Calculate details, such as bandwidth savings when features like Web Image Optimization and video adaptation are enabled.
- Provide the basis for charging
- Measure analytics

Specify the HTTP transaction record profile in an HTTP Proxy instance tied to the workflow for it to take effect.

To configure HTTP Transaction Record Profile:

1. Use any of the following methods to configure an HTTP Transaction Record Profile:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category** in the left pane.

c Click **HTTP Transaction Record Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New HTTP Transaction Record Profile**.

2 Configure the parameters as follows:

Table 9-133 HTTP Transaction Record Profile Parameters

Parameter	Description
Name	HTTP Transaction Data Record profile name
File Type	File type for streaming HTDR record locally: ■ Event Log ■ Data Record ■ Corefiles ■ RAM Disk-Storage ■ Storage ■ Ext-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming HTDR record locally
Encode Format	Format type: ■ CSV
Transaction Template	HTTP Transaction Record Template. Configure at Service Construct > Data Record Template > Multi Protocol Proxy > HTTP Transaction
Record URL Length	Length to which the URL field should be truncated in the record

3 Click the **Save** icon.

Long Term Mobile ID

Use this object to configure a Long Term Mobile ID (LTMI). It supports insertion of encrypted subscriber ID in an HTTP request header to allow the subscriber ID to be communicated to origin server in a secure manner.

MCC supports the following levels of encoding/encryption formats:

- Plain Text
- LTMI Static Trusted
- LTMI dynamic Trusted
- LTMI External

Operators can opt out of the LTMI feature using the Opt Out String and Static Trusted ID String.

MCC supports the following text string VSAs used to generate LTMI and the reseller ID header. The VSAs are retrieved from the PCRF when a call is established, and delivered to the HTTP Proxy when an HTTP request header is processed.

- subID
- miDial
- resellerID

Using HTTPS, the MCC periodically downloads encryption keys from a key server. The keys can be manually imported using import LTMI key or automatically imported from the key server by configuring the minute interval using key-import-interval.

To add a long term mobile ID:

1 Use any of the following methods to configure an LTMI:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **LTMI**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New LTMI**.

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **LTMI**.

4 Configure the parameters as follows:

Table 9-134 LTMI Parameters

Parameter	Description
The following parameters control the key import (download) from the key server using HTTPS:	
Key Import Interval	Key import interval, in minutes, zero turns off key import
Key Server URL	Network Context used for non-HTTP connections. It overrides the Network Context selected by a higher-level object.
Key Server Username	Key Server username for basic authentication.
Key Server Password	Key Server password for basic authentication.
Key Server Network Context	Key server network context
The following parameters control if and how the LTMI ID is generated:	
ID Gen Admin State	Enable/Disable LTMI ID generation: ■ enabled ■ disable
Trusted ID Divisor	Number of minutes for trusted ID rotation interval (for example, 6 months rotation = 259,200 minutes)
External ID Divisor	Number of minutes for external ID rotation interval (for example, 24 hour rotation = 1440 minutes.
Network Carrier Code	Code used in dynamic mobile IDs to identify the carrier.
Opt Out String	String used to search the opt out value to see if a subscriber has opted out of Dynamic Mobile ID. When a subscriber opts out this feature, no LTMI is inserted in the HTTP request header. If the miDial string exactly matches the Opt Out String, then the subscriber completely opts out of LTMI.
Static Trusted ID String	Ending of the search string used to identify opt out value for static trusted ID. If the miDial string ends with the Static Trusted ID String, then the Static Trusted ID is used instead of the Dynamic Trusted ID. For example, if the Static Trusted ID String is configured as "#" and the miDail string is "xyz#" (ending with "#"), then the Static Trusted ID is used instead of the Dynamic Trusted ID.

5 Click the **Save** icon.

Steering GW Group

Use this object to configure a group of Steering Destinations.

To add a Steering GW Group:

1 Use any of the following methods to configure a Steering GW Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Steering GW Group**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Steering GW Group**.

2 Configure the parameters as follows:

- **Name**: Steering GW Group name.

3 In **Steering GW**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-135 Steering GW Parameters

Parameter	Description
Name	HTTP Steering Destination Name
IP Address	IP address for Steering Destination
Port	Port for Steering Destination Port
Host Name	Host Name (FQDN) of the Steering Destination

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many steering GW as needed.

7 Click the **Save** icon.

TCP Splicing Policy

Use this object to configure a policy that controls the behavior of the TCP connections that match an HTTP IP Flow. The matched traffic is forwarded to a TCP splicing component and spliced to the server.

To configure a TCP Splicing Policy:

1 Use any of the following methods to configure a TCP Splicing Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **TCP Splicing Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New TCP Splicing Policy**.

2 Click **TCP Splicing Policy**.

3 Configure the parameters as follows:

Table 9-136 TCP Splicing Policy Parameters

Parameter	Description
Name	Content TCP Splicing Policy Name
Priority	Priority of the TCP Splicing Policy, must be unique
Traffic Control Profile	Traffic Control Profile associated with this policy. The Traffic Control Profile must already exist. See Traffic Control Profile.

4 In **Service Rules**, drag and drop the as many Service Rules as needed from the Available list to the Selected list.

5 Click the **Save** icon.

Traffic Control Profile

Use this object to configure a profile for handling of splicing traffic (data forwarding between client and server TCP connections).

Multi Protocol Proxy supports forwarding of non-HTTP traffic received on port 80. The traffic control component of Multi Protocol Proxy is responsible for handling of non-HTTP traffic. The component maintains a pair of client-side and server-side connections and forwards data between these connections.

To configure a Traffic Control Profile:

1 Use any of the following methods to configure a Traffic Control Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Traffic Control Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Traffic Control Profile**.

2 Configure the parameters as follows:

Table 9-137 Traffic Control Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Network Context Override	Network Context used for the TCP Splicing Profile. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for splicing server connections

Table 9-137 Traffic Control Profile Parameters

Parameter	Description
Steering Group	Configure the Steering Destinations to use for this profile. Configure the Steering Destinations to use for this profile. The Steering Group allows the UDP flow to be steered to the destination configured within itself, when the profile is selected. In the packet processing, after UDP policies are evaluated, the associated traffic-control-profile is selected. The steering group within the profile can have multiple steering-destinations. A round-robin approach is used between destinations. In case of a single steering-destination, the current UDP flow is steered to that destination. The Steering Destinations must already exist. See Steering GW Group.
Toll Free Data	Mark the checkbox to specify that toll free data applies for this profile.
Upstream Buffering Limit	Maximum data to store when processing upstream data, in KB.
Downstream Buffering Limit	Maximum data to store when processing downstream data, in KB.
Rate Limiting:	
Admin State	Admin state: ■ enabled ■ disable
Burst Size	Burst size
Burst Size Units	Burst size units: ■ bytes ■ kbytes ■ mbytes ■ gbytes
Bitrate	Bitrate
Bitrate Units	Bitrate units: ■ bps ■ kbps ■ mbps ■ gbps
Savings Estimation:	

Table 9-137 Traffic Control Profile Parameters

Parameter	Description
Admin State	Admin state: estimation of optimization byte savings attributed to rate-limited HTTPS video traffic. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on video sessions: ■ enabled ■ disable
Sampling Interval	Sampling interval for savings estimation
Sampling Interval Unit	Unit for sampling interval for savings estimation: ■ min ■ hr

3 Click the **Save** icon.

Toll Free Profile

Use this object to configure a toll free profile to support Toll Free Data (TFD). TFD is a feature in which a third-party (content provider) pays for a subscriber's data usage when the subscriber is downloading or using the third-party company's Apps, Websites, and services. If a toll free profile is enabled, TFD is turned on for that proxy instance.

To configure a Toll Free Profile:

1 Use any of the following methods to configure a Toll Free Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Toll Free Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Toll Free Profile**.

2 Configure the parameters as follows:

Table 9-138 Toll Free Profile Parameters

Parameter	Description
CA Certificate List	CA root certificate. The CA certificate must first be placed in */public/content/tls/cacerts* before it can be configured. The Ca Certificate List must already exist. See CA Certificate List.
Certificate URL	URL prefix for certificates (for example, http://certificateserver/)
Certificate File Extension	Certificate file extension
CRL URL	URL for Certificate Revocation List (string starting with http://) When toll-free-data manifest is received before Certificate Revocation List (CRL) is available to the MCC, the manifest is processed. After parsing and signature verification, the manifest is installed into the subscriber service profile. The manifest, using revoked content provider certificate, is only removed when the UE triggers a manifest refresh (re-downloads the manifest again).
Network Context	Network context for accessing the certificate server
Loopback IP	Loopback interface for accessing the certificate server
File Type	File type for streaming the Toll Free Data record locally: ■ Event Log ■ Data Record ■ Corefiles ■ Storage ■ Ext-Storage ■ RAM Disk-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming the Toll Free Data record locally
TFD Template	Toll Free Data record template

3 Click the **Save** icon.

Web Image Optimization Profile

The Multi Protocol Proxy Web Image Optimization Profile defines image compression and transcoding to produce a large gain in bandwidth savings for the Operator.

The profile specifies image conversion parameters such as re-compression, metadata, quality, percentage, and size. For example, you can configure the predicted size savings percentage threshold that can be optimized, such as a target JPEG quality between 0 (coarsest) and 100 (finest quantization). You associate a Web Image Optimization Profile with an HTTP Request Policy.

To configure Multi Protocol Proxy Web Image Optimization Profile:

1 Use any of the following methods to configure a Multi Protocol Proxy Web Image Optimization Profile:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Web Image Optimization Profile**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Web Image Optimization Profile**.

2 Configure the parameters as follows:

Table 9-139 Web Image Optimization Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Convert PNG to JPEG	Mark the checkbox to allow conversion of PNG to JPEG.
Convert GIF to PNG	Mark the checkbox to allow conversion of GIF to PNG.
Convert GIF to JPEG	Mark the checkbox to allow conversion of GIF to JPEG.
Sample JPEG to 420	Mark the checkbox to allow 4:2:0 chroma subsampling of JPEG.
Interlace Image	Mark the checkbox to allow interlace image
Quantize Image	Mark the checkbox to allow requantization of palettized image.
Resize Image	Mark the checkbox to allow resizing of image.

Table 9-139 Web Image Optimization Profile Parameters

Parameter	Description
Remove Metadata	Mark the checkbox to allow removal of image metadata.
Target JPEG Quality	Target JPEG quality, with 0 being the coarsest quantization, and 100 being the finest quantization.
Target Max Size	Target maximum size (in KB) that can be optimized.
Source Min Size	Source minimum size (in KB) that can be optimized.
Size Saving Threshold	Predicted size saving percentage threshold that can be optimized.
Source Max Size	Source maximum size (in KB) that can be optimized.

3 Click the **Save** icon.

Protocol Application Rule Group (8.4 and later MCC version)

The Protocol Application Rule Group defines layer 7 applications and protocols for Signature Analysis by detecting deterministic and/or heuristic patterns in bidirectional packet flow. Signature Analysis is the key technology that enables Workflow to control application of advanced services on subscriber traffic (such as charging, per-application filtering, QoS, and so on).

Use the Protocol Application Rule Group to configure rules that match on the following connection attributes:

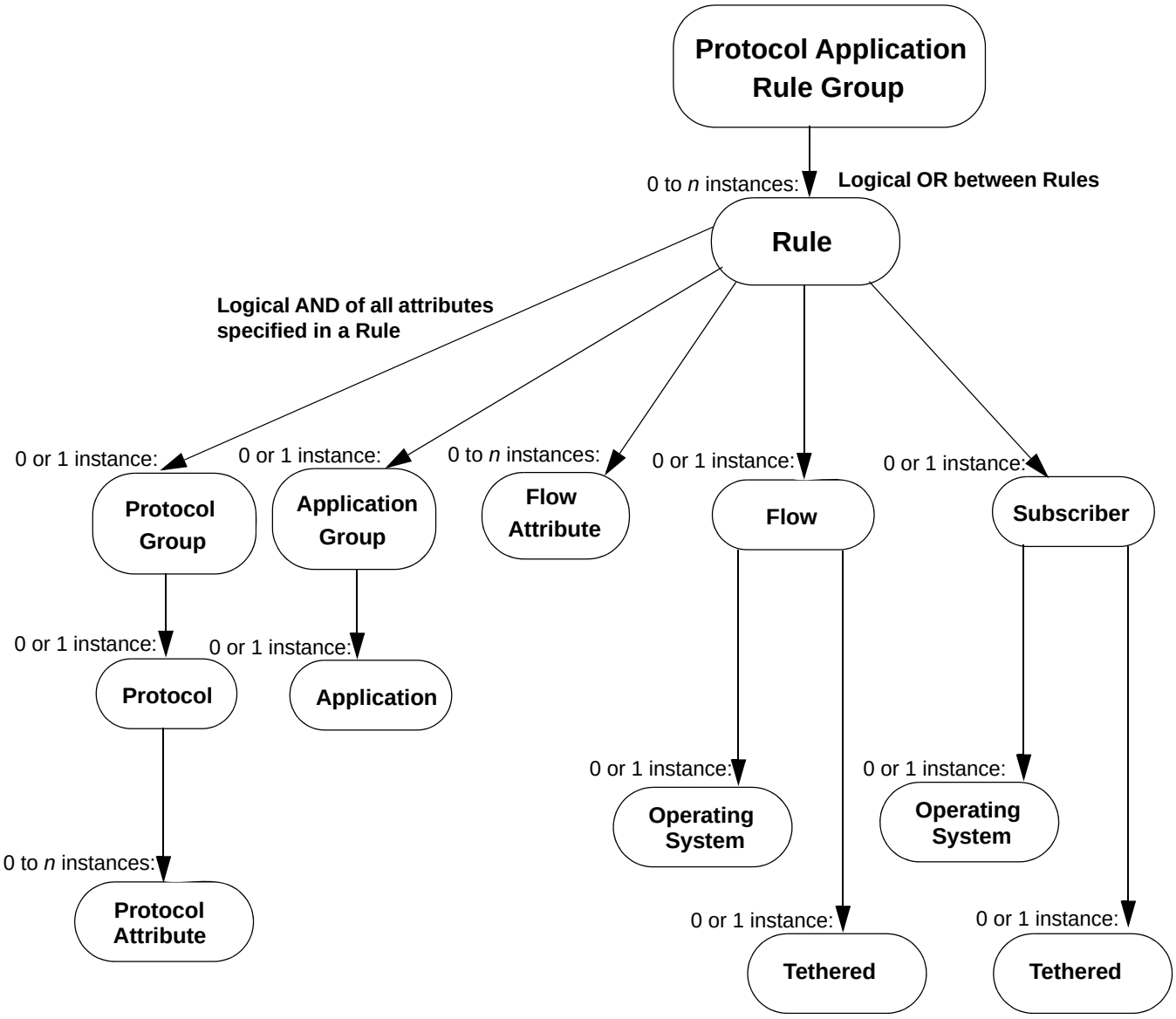
- Applications
- Flow attributes
- Protocols
- Protocol attributes
- Operating system
- Tethering

The following are the rules for matching with a Protocol Application Rule Group rule:

- If an application is specified, it must match.
- If a protocol is specified, it must match.
- If one or more protocol attributes are specified, all of them must match.
- If one or more flow attributes are specified, all of them must match.
- If the subscriber operating system is specified, then it must match.
- If the flow operating system is specified, then it must match.
- If the subscriber tethering status is specified, then it must match.
- If the flow tethering status is specified, then it must match.

The following figure illustrates the components of Protocol Application Rule Group.

Figure 9-33 Protocol Application Rule Group Components



To add a Protocol Application Rule Group:

1 Use any of the following methods to add a Protocol Application Rule Group:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category**.

c Click **Protocol Application Rule Group**.

d Click the **Create** icon.

Build a Workflow:

a. Click the **Build a Workflow** tab.

b. Expand **Functions**.

c. Click the **New** tab.

d. Click **New Protocol Application Rule Group**.

2. Configure the parameters as follows:

- **Name** – Enter a Protocol Application Rule Group name.

3. In Rule, configure the parameters as follows:

Table 9-140 Protocol Application Rule Group Parameters

Parameter	Description
Name	Enter a rule name
Application Group:	
Name	Select the Application Group to include in the Protocol Application Rule Group: ■ Business ■ Conference ■ Database ■ E-Commerce ■ File Transfer ■ Gaming ■ Generic ■ Industrial ■ Mail ■ Messaging ■ Mobile ■ Network Management ■ Peer to Peer ■ Remote Control ■ Sharehosting ■ Social ■ Streaming ■ Tunnel ■ Voice Over IP ■ Web
Application Name	Select the Application to include in the Protocol Application Rule Group. The applications available are filtered based on the specified Application Group.

Table 9-140 Protocol Application Rule Group Parameters

Parameter	Description
Flow Attribute	Select the Flow Attribute(s) to include in the Protocol Application Rule Group: ■ amazon-cloud ■ android ■ apache ■ audio ■ blackberry ■ chat ■ chrome ■ ddl ■ encrypted ■ file-transfer ■ google ■ ios ■ mail ■ mariadb-server ■ microsoft-windows ■ mysql-server ■ none ■ ntlm ■ out ■ outlook_web_access ■ picture ■ stream ■ video ■ web ■ windows-mobile If you specify multiple Flow Attributes, a connection must match all the specified attributes for it to match the rule.

Table 9-140 Protocol Application Rule Group Parameters

Parameter	Description
Subscriber:	
Operating System *(Operating system of the user equipment device)*	Select the Subscriber Operating System to include in the Protocol Application Rule Group: ■ Android ■ Blackberry ■ Chrome ■ Darwin ■ Linux ■ OS X ■ Other ■ Symbian ■ Windows ■ WindowsMobile ■ WindowsPhone ■ iOS
Tethered	Specify whether there are tethered devices behind this subscriber: ■ true ■ false
Flow:	
Operating System *(Operating system of the individual flow. May differ from the subscriber operating system if from a tethered device)*	Select the Subscriber Operating System to include in the Protocol Application Rule Group: ■ Android ■ Blackberry ■ Chrome ■ Darwin ■ Linux ■ OS X ■ Other ■ Symbian ■ Windows ■ WindowsMobile ■ WindowsPhone ■ iOS
Tethered	Specify whether there are tethered devices behind this flow: ■ true ■ false

Table 9-140 Protocol Application Rule Group Parameters

Parameter	Description
Protocol Group:	
Name	Select the Protocol Group to include in the Protocol Application Rule Group: ■ Business ■ Conference ■ Database ■ E-Commerce ■ File Transfer ■ Gaming ■ Generic ■ Industrial ■ Mail ■ Messaging ■ Mobile ■ Network Management ■ Peer to Peer ■ Remote Control ■ Sharehosting ■ Social ■ Streaming ■ Tunnel ■ Voice Over IP ■ Web
Protocol Name	Select the Protocol to include in the Protocol Application Rule Group. The protocols available are filtered based on the specified Protocol.
Protocol Attribute Name	Select the Protocol Attribute(s) to include in the Protocol Application Rule Group. The protocols attributes available are filtered based on the specified Protocol Name. If you specify multiple Protocol Attributes, a connection must match all the specified attributes for it to match the rule.
To add additional rules, click the **Create** icon.	

4 Click the **Save** icon.

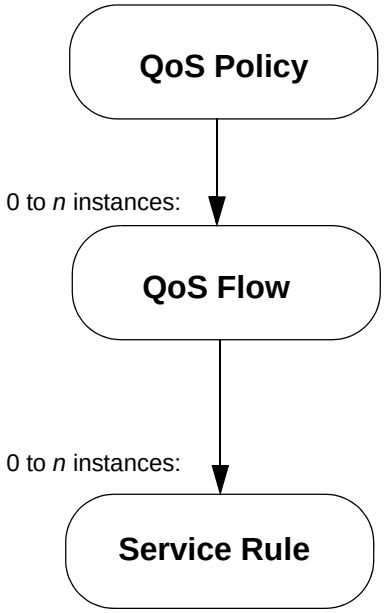
Quality of Service

Quality of Service includes:

- QoS Flow – Allows for service data flow-level rate enforcement
- QoS Policy – Defines the QoS to be given to a list of QoS Flows

The following figure illustrates the components of Quality of Service.

Figure 9-34 Quality of Service Components



QoS Flow

The QoS Flow service allows for service data flow-level rate enforcement. You can link service rule(s) to the QoS Flow to specify the actions to take on traffic that matches at least one of its service rules. For example, you can limit the amount of ICMP traffic to specified uplink and/or downlink rates. QCI/ARP values are compared to the default bearer to determine if a dedicated bearer is required.

To add a QoS Flow:

1 Use any of the following methods to add a QoS Flow:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **QoS Flow**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New QoS Flow**.

2 Configure the parameters as follows:

Table 9-141 QoS Flow Parameters

Parameter	Description
Name	QoS Flow name
State	Admin State: ■ enabled ■ disabled
Measurement Unit	Measurement Unit: ■ kbps ■ mbps ■ gbps
Uplink MBR	Uplink Maximum Bit Rate
Downlink MBR	Downlink Maximum Bit Rate
Uplink GBR	Uplink Guaranteed Bit Rate
Downlink GBR	Downlink Guaranteed Bit Rate
Uplink Max Burst	Uplink Max Burst, in Kbytes
Uplink Guaranteed Burst	Uplink Guaranteed Burst, in Kbytes
Downlink Max Burst	Downlink Max Burst, in Kbytes
Downlink Guaranteed Burst	Downlink Guaranteed Burst, in Kbytes

Table 9-141 QoS Flow Parameters

Parameter	Description
Qci	***Note:*** *Applies when Bearer Control is set to Network Initiated or User Initiated.* QoS Class Identifier: ■ 1: Operator controlled Voice Calling ■ 2: Operator controlled Video Calling ■ 3: Operator controlled Real-time Gaming ■ 4: Operator controlled Streaming of Pre-recorded Video ■ 5: Signaling for Operator controlled applications ■ 6: Websites prioritized by Operator ■ 7: Operator controlled Live Video Streaming or Interactive Gaming ■ 8: All other traffic for premium subscriber ■ 9: All other traffic for regular subscribe
Arp	***Note:*** *Applies when Bearer Control is set to Network Initiated or User Initiated.* Allocation and Retention Policy Higher values are preferred.
Gate	Gate: ■ Block ■ Pass ■ Pass Upstream ■ Pass Downstream
Priority	QoS Flow Priority. Priority resolves conflicts in the case of a multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object. Thus, QoS Flow priority takes precedence over the associated service rule priority.
Bearer Control	Specifies the Bearer Control: ■ Network Initiated ■ User Initiated ■ Default Bearer
DSCP	Optional flow-level override to bearer QCI/DSCP mapping (the DSCP derived from the bearer QCI.)

Table 9-141 QoS Flow Parameters

Parameter	Description
Service Activation	Specifies when to use or skip the service flow for packet classification: ■ always on - always use this service flow for classification ■ external activation - use the activation state of the service flow to determine whether to use or skip the service flow for packet classification. This setting allows the Gateway to dynamically activate/deactivate Rating Groups.
Aggregate QoS Flow	Specifies whether this QoS Flow is an aggregate flow: ■ true ■ false
Service Rule List	Select the service rule(s) to link with the QoS Flow. The service rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

QoS Policy

The QoS Policy defines the QoS to be given to a list of QoS Flows, each of which can be prioritized.

To add a QoS Policy:

1 Use any of the following methods to add a QoS Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **QoS Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New QoS Policy**.

2 Configure the parameters as follows:

Table 9-142 QoS Policy Parameters

Parameter	Description
Name	QoS Policy name
Package Id	Policy instance in the AAA server
State	Admin State: ■ enabled ■ disabled
Priority Evaluation Mode	Priority Evaluation Mode: ■ flat - Use Service Rule priority (ignore QoS Flow priority). To make a match, examine all of the Service Rules on all of the QoS Flows for best priority. ■ flat-with-pcc-rule-precedence - Any PCC rules in effect have their precedence values compared with the Service Rule priority values, and the PCC rule or Service Rule with the highest priority (lowest numerical value) is selected. ■ hierarchical - Use QoS Flow priority and Service Rule priority hierarchically. To make a match, examine the QoS Flows in priority order and within each of them, examining the Service Rules in priority order.
Geo Redundant Group	Select the Geographic Redundancy Group to associate with the QoS Policy. The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager. To select a Geographic Redundancy Group, drag and drop it from the Available list to the Selected list.
QoS Flow List	Select the QoS Flow(s) to link with the QoS Policy. The QoS Flow must already exist. See QoS Flow. To select a QoS Flow, drag and drop it from the Available list to the Selected list.
Fraud QoS	Set to true to designate this QoS Flow for handling of fraudulent activity within this QoS Policy.
Dscp Replacement Mode	Allows the mapping of the DSCP value in the IPv4/6 header of an egress packet to a configurable 802.1Q VLAN priority. The DSCP value can be replaced in either the outer IP header or in both the inner and outer IP header: ■ outer: replaces the dscp value in only the outer IP header ■ both: replaces the dscp value in both the inner and outer IP header
Aggregate QoS Policy	Specifies whether this QoS Policy is an aggregate policy: ■ true ■ false

3 In **Qci Dscp Map List**, click the **Create** icon.

4 Configure the parameters as follows:

Table 9-143 Qci Dscp Map Parameters

Parameter	Description
Qci	QoS Class Identifier: ■ 1: Operator controlled Voice Calling ■ 2: Operator controlled Video Calling ■ 3: Operator controlled Real-time Gaming ■ 4: Operator controlled Streaming of Pre-recorded Video ■ 5: Signaling for Operator controlled applications ■ 6: Websites prioritized by Operator ■ 7: Operator controlled Live Video Streaming or Interactive Gaming ■ 8: All other traffic for premium subscriber ■ 9: All other traffic for regular subscriber
Dscp	Select the Diffserv Code Point Map.

5 Click **Add**.

6 Repeat step 3 through step 5 to add as many Qci Dscp Maps as needed.

7 Click the **Save** icon.

Realm List

Use this object to configure the Realm/Username@realm list.

To add a Realm List:

1 Use any of the following methods to configure a realm list:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Realm List**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Realm List**.

2 Configure the parameters as follows:

Table 9-144 Realm List Parameters

Parameter	Description
Name	Realm list name
User Description	Realm list description
Value	Specific username or realm value
User Description	Description of the specific username or realm

3 Click the **Save** icon.

SMTP Proxy

Use this object to configure an Simple Mail Transfer Protocol proxy instance for handling SMTP traffic.

To add an SMTP Proxy instance:

1 Use any of the following methods to configure an SMTP proxy instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **SMTP Proxy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New SMTP Proxy**.

2 Configure the parameters as follows:

Table 9-145 SMTP Proxy Instance Parameters

Parameter	Description
Name	Content SMTP Proxy instance name
Admin State	Admin state: ■ enabled ■ disable
Mms Mm3	MMS MM3 Instance associated with the HTTP Server Instance. The MMS MM3 instance must already exist. See MMS MM3 Profile.
Network Context	Select the Network Context.
Loopback IP Addr	Select the Loopback IP Address
Port	Enter the Loopback IP Port

3 Click the **Save** icon.

Steering Service

The Steering Service allows the normal routing of a packet to be overridden for upstream subscriber traffic based on the configured Steering Policy.

Steering allows upstream subscriber traffic to be force-routed to a specific next hop or into a specific tunnel. Steering is compatible with NAT, as an upstream packet can be source NAT'd and steered. Steering is subservient to the Multi Protocol Proxy and its dependent services – if the packet is to be proxied, steering is ignored.

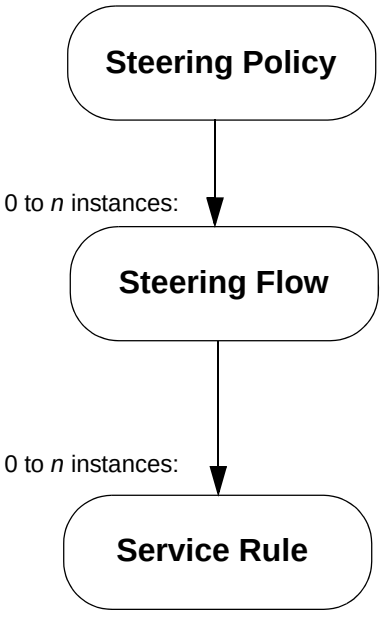
Steering can be based on any of the inputs present on the Service Rule:

- L3/4 Packet Filter
- Time of Day Rule Group
- DPI Protocol Application Rule Group
- L7 HTTP Rule Group

Note: *The Steering Service does not support steering into IPSec tunnels.*

The following figure illustrates the components of the Steering Service.

Figure 9-35 Steering Service Components



Steering Flow

The Steering Flow service allows for upstream subscriber traffic steering. You can link service rule(s) to the Steering Flow to specify the actions to take on traffic that matches at least one of its service rules.

To add a Steering Flow:

1 Use any of the following methods to add a Steering Flow:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Steering Flow**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Steering Flow**.

2 Configure the parameters as follows:

Table 9-146 Steering Flow Parameters

Parameter	Description
Name	Steering Flow name
Admin State	Admin State: ■ enabled ■ disabled
Priority	Steering Flow Priority. This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Action	Action to take for this steering flow: ■ steering ■ no steering
Network Context	***Note:*** *Applies when* ***Action*** *is set to Steering.* Network Context of the tunnel or next hop on which upstream traffic is to be sent.

Table 9-146 Steering Flow Parameters

Parameter	Description
Tunnel	***Note:*** *Applies when* ***Action*** *is set to Steering.* Name of the tunnel or next hop on which upstream traffic is to be sent.
Service Rule List	Select the service rule(s) to link with the Steering Flow. The service rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Steering Policy

To add a Steering Policy:

1 Use any of the following methods to add a Steering Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Steering Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Steering Policy**.

2 Configure the parameters as follows:

Table 9-147 Steering Policy Parameters

Parameter	Description
Name	Steering Policy name
State	Admin State: ■ enabled ■ disabled

Table 9-147 Steering Policy Parameters

Parameter	Description
Steering Flow List	Select the Steering Flow(s) to link with the Steering Policy. The Steering Flow must already exist. See Steering Flow. To select a Steering Flow, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

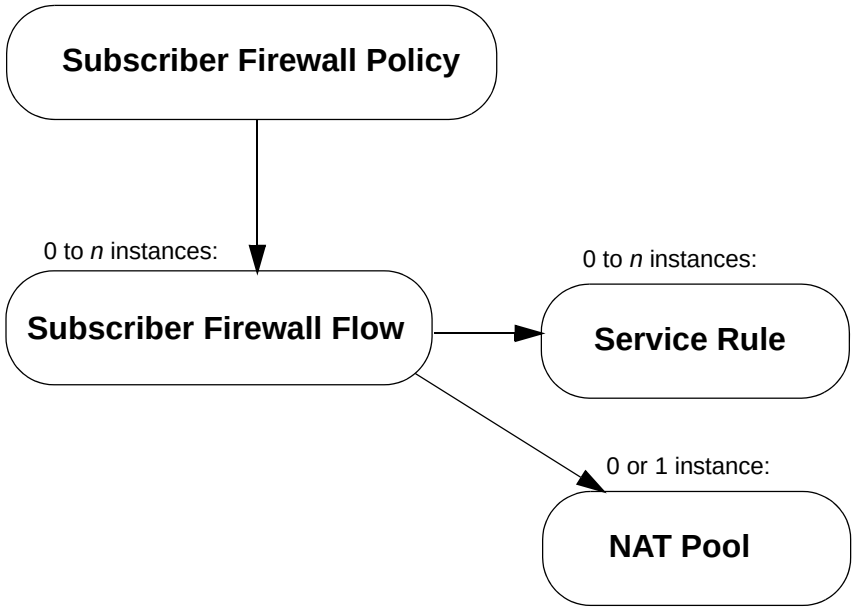
Subscriber Firewall

Subscriber Firewall includes:

- Subscriber Firewall Flow – Defines Network Address and Port Translation treatment of multiple classified traffic flows
- Subscriber Firewall Policy – Binds one or more (prioritized) Subscriber Firewall Flows and defines the NAT treatment to be applied when associated with a service flow.

The following figure illustrates the components of Subscriber Firewall Service.

Figure 9-36 Subscriber Firewall Service Components



Subscriber Firewall Flow

The Subscriber Firewall flow allows differentiated Network Address and Port Translation treatment of multiple classified traffic flows. Network Address and Port Translation is used to map private UE IP addresses to a limited pool of public IP addresses. For example, certain traffic can be mapped to public addresses from one particular NAT pool, other traffic may be mapped to another NAT pool, and some traffic may not be mapped at all.

To add a Subscriber Firewall Flow:

1 Use any of the following methods to add a Subscriber Firewall Flow:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Subscriber Firewall Flow**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Subscriber Firewall Flow**.

2 Configure the parameters as follows:

Table 9-148 Subscriber Firewall Flow Parameters

Parameter	Description
Name	Subscriber Firewall Flow name
State	Admin state: ■ enabled ■ disable
Priority	Subscriber Firewall Flow priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Action	Action to apply: ■ NAT: Apply Network Address and Port Translation treatment (default) ■ Pass ■ Drop

Table 9-148 Subscriber Firewall Flow Parameters

Parameter	Description
NAT Pool	NAT Pool associated with this Subscriber Firewall Flow. The NAT Pool must already exist. Create it at Network Context > *name* > Nat Pool.
ALG	ALG application: ■ FTP ■ RTCP ■ SIP ■ TFTP
Flow Auth	Enables flow authorization on the subscriber firewall flow: ■ enabled ■ disable Applies only when **Action** is set to NAT.
NAT Flow Filter Mode	NAT Flow Filter Mode: ■ address-dependent ■ address-port-dependent ■ endpoint-independent ■ not-set
NAT Flow Binding Time	Timer (in seconds) to persist NAT address/port bindings even after connection close is initiated. ***Note:*** *MCC keeps the address mapping binding (NAT'ed IP) persistent for this timer period by keeping the connection object alive even after the data connection is deleted. This helps in reusing the same NAT'ed IP for the connections, if the connection returns within the nat-binding-time period. However, setting this timer puts strain on resources.*
Service Rule List	Select the service rule(s) to bind with the Subscriber Firewall Flow. The Service Rule must already exist. See Service Rule. To select a service rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Subscriber Firewall Policy

Subscriber Firewall Policy binds one or more (prioritized) Subscriber Firewall flows and defines the NAT treatment to be applied when associated with a service flow.

To add a Subscriber Firewall Policy:

1 Use any of the following methods to add a Subscriber Firewall Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Subscriber Firewall Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Subscriber Firewall Policy**.

2 Configure the parameters as follows:

Table 9-149 Subscriber Firewall Policy Parameters

Parameter	Description
Name	Subscriber Firewall Policy name
State	Admin state: ■ enabled ■ disable
Subscriber Firewall Flow List	Select the Subscriber Firewall Flow(s) to bind with the Subscriber Firewall Policy The Subscriber Firewall Flow must already exist. See Subscriber Firewall Flow. To select a Subscriber Firewall Flow, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Video Adaptation (MCC versions prior to 9.0)

Acuitas does not support video adaptation services for MCC 9.0 and later releases.

Use this object to configure video adaptation services.

To enable a video adaptation service, the HTTP Proxy service must be enabled.

A video adaptation service is applied to HTTP traffic for a subscriber workflow when the following conditions are met:

- Subscriber workflow has an associated video adaptation instance
- Content is video
- Content Cache service is enabled

The system supports the following target container types and source <=> target combinations.

Offline Transcoding	Online Transcoding
■ MP4 <=> FLV ■ MP4 => MP4 ■ FLV => FLV ■ WebM => WebM	■ MP4 => MP4 ■ FLV => FLV ■ WebM => WebM

Note: *Video pacing and online and offline transcoding is not supported for range requests, including those received from the server categorized as follows:*

HTTP Response status 206 “Partial Content”
HTTP Response status 200 “OK” that includes a “Range” header
HTTP Response status 200 “OK” to an HTTP Request that includes a range specification in the URI

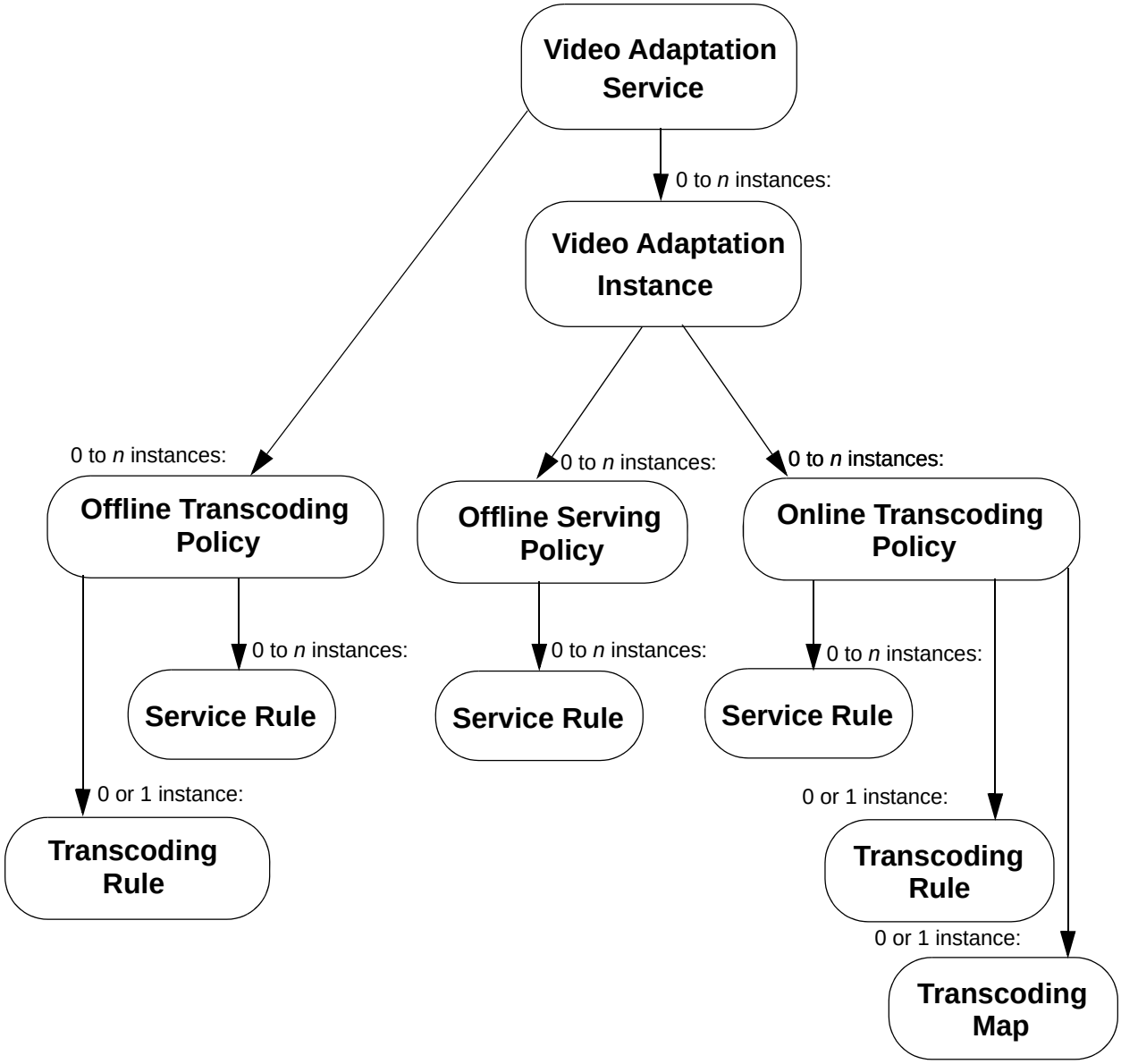
The system supports five QoE grades and resolutions per container type. It supports the following video-adaptation profiles for MP4, FLV, and WebM container types:

Supported Container Type	Media Container	Values					
MP4, FLV, WebM	QoE Grade	0	1	2	3	4	5
MP4, FLV, WebM	Max Video Height	180	240	360	480	720	1080
MP4, FLV, WebM	Max Video Width	320	428	640	854	1280	1920

Supported Container Type	Media Container	Values					
MP4, FLV, WebM	Max Video Frame Rate	30	30	30	30	30	30
MP4, FLV, WebM	Pref Video Bitrate Type	333	442	748	1179	2407	5172
MP4, FLV	Pref Video Codec	h264	h264	h264	h264	h264	h264
WebM		vp8	vp8	vp8	vp8	vp8	vp8
MP4, FLV	Video Profile	main	main	main	main	main	main
WebM		N/A	N/A	N/A	N/A	N/A	N/A

The following figure illustrates the components of video adaptation.

Figure 9-37 Video Adaptation Components



Video Adaptation Service

To add a Video Adaptation service:

1 Use any of the following methods to add a Video Adaptation service:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Global Video Adaptation Service**.

d Click **Global Video Adaptation Service**.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **User Created** tab.

d Expand **Select a Category**.

e Click **Global Video Adaptation Service**.

f Click **Global Video Adaptation Service**.

2 Configure the parameters as follows:

Table 9-150 Video Adaptation Service Parameters

Parameter	Description
Admin State	Admin State of the Video Adaptation service for both offline and online transcoding: ■ enabled ■ disabled

3 Click the **Save** icon.

Video Adaptation Instance

The following instance guidelines apply:

- Each instance has a maximum QoE. The system uses the QoE under the serving policy if there is a match instead of the QoE under instance.
- The instance supports a transcoding policy for online transcoding. Multiple service rules can be configured to the policy.
- If the optional media container is not specified, the system uses the original content type.
- For offline transcoding:
  - If no service rule is configured under the serving policy, the system uses the original content.
  - If the requested container type does not exist in the cache, the system uses the original content from the origin server or cache.

To add a Video Adaptation instance:

1. Use any of the following methods to add a Video Adaptation instance:

   Build Out Functions:

   a. Click the **Build Out Functions** tab.

   b. Expand **Select a Category** in the left pane.

   c. Click **Video Adaptation**.

   d. Click the **Create** icon.

   Build a Workflow:

   a. Click the **Build a Workflow** tab.

   b. Expand **Functions** in the right pane.

   c. Click the **New** tab.

   d. Click **New Video Adaptation**.

2. Configure the parameters as follows:

   - **Service Name** – Enter a Video Adaptation name.
   - **Max. Quality of Experience Grade** – Enter the maximum quality of experience grade allowed (0-5).

     Streaming bitrates for Quality of Experience (QoE) are as follows:

     – QoE 0: Less than 333 kbps

     – QoE 1: From 333 to 442 kbps

     – QoE 2: From 442 to 748 kbps

- QoE 3: From 748 to 1179 kbps
- QoE 4: From 1179 to 2407 kbps
- QoE 5: From 2407 to 5179 kbps

3 In **Offline Transcoding**, configure the parameters as follows:

Table 9-151 Offline Transcoding Parameters

Parameter	Description
Admin State	Enable/Disable Video Adaptation Service Offline Transcoding: ■ enabled ■ disable
Serving Policy	Select the Offline Serving Policy used to serve adapted videos to clients. The Offline Serving Policy must already exist. See Offline Transcoding Policy. To select a Serving Policy, drag and drop it from the Available list to the Selected list.

4 In **Online Transcoding**, configure the parameters as follows:

Table 9-152 Online Transcoding Parameters

Parameter	Description
Admin State	Enable/Disable Video Adaptation Service Offline Transcoding: ■ enabled ■ disable
Transcoding Policy	Select the Online Transcoding Policy. The Transcoding Policy must already exist. See Online Transcoding Policy. To select a Transcoding Policy, drag and drop it from the Available list to the Selected list.

5 Click the **Save** icon.

Offline Transcoding Policy

Offline transcoding caches the original video from the origin server and transcodes the video into different QoE grades and multiple container types. The system serves the video to the user from the cache when subsequent requests are made for the same video. Transcoded videos are served as they are completed, rather than waiting for all QoE grades to complete.

To add an Offline Transcoding Policy:

1 Use any of the following methods to add an Offline Transcoding Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Offline Transcoding Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Offline Transcoding Policy**.

2 Configure the parameters as follows:

Table 9-153 Transcoding Policy Parameters

Parameter	Description
Name	Transcoding Policy name
Admin State	Enable/Disable Offline Transcoding Policy: ■ enabled ■ disable
Priority	Enter the Priority
Transcoding Rule	Select the Transcoding Rule. The Transcoding Rule must already exist. See Transcoding Rule.
Target Container Types	You can configure up to three target container types. Select the target container type: ■ FLV ■ MP4 ■ WebM

3 Click the **Save** icon.

Offline Serving Policy

Use this object to configure the Serving Policy used to serve adapted videos to clients.

To add an Offline Serving Policy:

1 Use any of the following methods to add an Offline Serving Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Offline Serving Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Offline Serving Policy**.

2 Configure the parameters as follows:

Table 9-154 Serving Policy Parameters

Parameter	Description
Name	Serving Policy name
Admin State	Enable/Disable Serving Policy: ■ enabled ■ disable
Priority	Enter the Priority
Container Type	Select the target media container type serving to clients: ■ FLV ■ MP4 ■ WebM
QoE Grade	Select the serving quality of experience grade (0-5).
Service Rule	Service Rule(s). The Service Rule must already exist. See Service Rule. To select a Service Rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

Transcoding Map

The transcoding map enables Operators to adjust the parameters of the target video based on the characteristics of the source video. When the transcoding map is configured, it is used by OTF (on-the-fly) video transcoder instead of the QoE profile. The transcoding map is passed from the HTTP proxy layer to the intermediate OTF library. The OTF library is responsible for communicating with the lower-level streaming transcoder layer that uses these abstract parameters to derive a set of tangible parameters for use in the transcoding process.

Note: *If the transcoding instance has both transcoding map and QoE defined, transcoding map takes priority and QoE is used if the source mapping does not match.*

To add a Transcoding Map:

1 Use any of the following methods to add a Transcoding Map:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Trasncoding Map**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Transcoding Map**.

2 Configure the parameters as follows:

Table 9-155 Transcoding Map Parameters

Parameter	Description
Name	Transcoding Map name
Entry Name	Transcoding Map entry name
Priority	Enter the Priority. Must be unique.

Table 9-155 Transcoding Map Parameters

Parameter	Description
Container Types	Source containers on which the matching is performed. You can configure up to three source container types. Select the target container type: ■ FLV ■ MP4 ■ WebM
Source Audio Sampling Rate in KHz	
Min	Min value of the source audio sampling rate in KHz. Configuring only the minimum value indicates that any value greater than or equal to that rate would match.
Max	Max value of the source audio sampling rate in KHz.
Source Bitrate in bits-per-second	
Min	Min bitrate value in bits per second. Configuring only the minimum value indicates that any value greater than or equal to that rate would match.
Max	Max bitrate value in bits per second.
Source Frame Rate	
Min	Lower bound value. Configuring only the lower bound value indicates that any value greater than or equal to that rate would match.
Max	Upper bound value.
Resolution	
Max Width	Maximum width value for resolution
Max Height	Maximum height value for resolution
Min Width	Minimum width value for resolution
Min Height	Minimum height value for resolution
Target: target parameters to which to transcode. *Configure the target parameters as percentages of the source parameters. The lower layers use the percentage value to compute the actual used values. The target parameters define the maximum allowable values. The actual value may be the maximum value or lower.*	
Max Audio Sampling Rate	Maximum target (less than or equal to) value for audio sampling rate in KHz.

Table 9-155 Transcoding Map Parameters

Parameter	Description
Min Audio Channel Count	Maximum number of allowed audio channels in the target video. ■ monoaural ■ stereo
Bypass	Bypasses transcoding: ■ True: all other parameters are ignored and source parameter transcoding is bypassed ■ False
Target Bitrate of the target video	
Max or Percentage	Bitrate as maximum or percentage: ■ max-bitrate: Maximum (Lesser than or equal to) value for bitrate in bits-per-second. Configure as a maximum value indicating that the target bitrate does not exceed the given amount. ■ percentage-bitrate: Target bitrate as a percentage (of the source) values. Configure as a percentage value, indicating the percentage of the source bitrate.
Bitrate Value	Maximum or percentage value
Target Frame Rate of the target video	
Max or Percentage	Bitrate as maximum or percentage: ■ max-framerate: Maximum value for frame rate. Configure as a maximum value indicating that the target framerate does not exceed the given amount. If the target frame rate is not configured or exceeds the origianl frame rate, the original frame rate is used. ■ percentage-framerate: Target frame rate as a percentage (of the source) frame rate. Configure as a percentage value, indicating the percentage of the source framerate. If the target frame rate is not configured, the original frame rate is used.
Frame Rate Value	Maximum or percentage value
Target Resolution of the target video	
Max or Percentage	Resolution as maximum or percentage: ■ max: Maximum height/width value ■ percentage-resolution: Target resolution as a percentage (of the source) resolution.
Max Width	Maximum (Lesser than or equal to) width value for resolution
Max Height	Maximum (Lesser than or equal to) height value for resolution
Percentage Resolution	Target resolution as a percentage (of the source) resolution

3 Click the **Save** icon.

Transcoding Rule

Use this object to configure a rule to be eligible for transcoding.

To add a Transcoding Rule:

1 Use any of the following methods to add a Trascoding Rule:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Trasncoding Rule**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Transcoding Rule**.

2 Configure the parameters as follows:

Table 9-156 Transcoding Rule Parameters

Parameter	Description
Name	Transcoding rule name
Max Object Size	Maximum object size to be eligible for transcoding, in kbytes.
Min Object Size	Minimum object size to be eligible for transcoding, in kbytes.
Max Duration	Maximum duration to be eligible for transcoding, in seconds.
Min Duration	Minimum duration to be eligible for transcoding, in seconds.
Max Bitrate	Maximum bitrate to be eligible for transcoding, in bits per second.
Max Framerate	Maximum framerate to be eligible for transcoding.
Source Container Types	You can configure up to three source container types. Select the target container type: ■ FLV ■ MP4 ■ WebM

Table 9-156 Transcoding Rule Parameters

Parameter	Description
Min Savings Threshold	Minimum saving s bitrate threshold to be elible for transcoding, in percentage.

3 Click the **Save** icon.

Online Transcoding Policy

Online transcoding is used to compress video contents in real-time when video is playing back from a user's device. The original data is decoded and then encoded into a target format with a lower QoE grade.

To add an Online Transcoding Policy:

1 Use any of the following methods to add an Online Transcoding Policy:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **Online Transcoding Policy**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New Online Transcoding Policy**.

2 Configure the parameters as follows:

Table 9-157 Transcoding Policy Parameters

Parameter	Description
Name	Serving Policy name
Admin State	Enable/Disable Online Transcoding Policy: ■ enabled ■ disable
Priority	Enter the Priority
Max QoE Grade	Select the maximum quality of experience grade allowed (0-5).

Table 9-157 Transcoding Policy Parameters

Parameter	Description
Transcoding Rule	Select the Transcoding Rule. The Transcoding Rule must already exist. See Transcoding Rule.
Speed Level	Select the transcoding speed level: ■ Slow ■ Medium ■ Fast
Transcoding Map	The transcoding map associated with this policy. The Transcoding Map must already exist. See Transcoding Map.
Service Rule	Service Rule(s). The Service Rule must already exist. See Service Rule. To select a Service Rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

WAP Gateway

The WAP Gateway processes WAP requests and translates them to HTTP requests. The WAP Gateway enables mobile device users to access information over a wireless network by translating pages into a form suitable for mobile devices.

WAP Gateway Instance

Use this object to configure a Wireless Application Protocol Gateway instance.

To add a WAP Gateway Service Instance:

1 Use any of the following methods to configure a WAP Gateway instance:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **WAP Gateway**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New WAP Gateway**.

2 Configure the parameters as follows:

Table 9-158 WAP Gateway Instance Parameters

Parameter	Description
Name	WAP Gateway Service instance name
Admin State	Admin state: ■ enabled ■ disable
WAP IP Flow	WAP IP Flow(s). The WAP IP Flow must already exist. See WAP IP Flow. To select a WAP IP Flow, drag and drop it from the Available list to the Selected list.
Wireless Transport Layer Security:	
Admin State	Admin state: ■ enabled ■ disable

Table 9-158 WAP Gateway Instance Parameters

Parameter	Description
Gateway Certificate	Enter the gateway certificate file name.
Gateway Key	Enter the gateway private key file name.

3 Click the **Save** icon.

WAP IP Flow

Use this object to configure a Wireless Application Protocol IP Flow.

To add a WAP Gateway IP Flow:

1 Use any of the following methods to configure a WAP IP Flow:

Build Out Functions:

a Click the **Build Out Functions** tab.

b Expand **Select a Category** in the left pane.

c Click **WAP IP Flow**.

d Click the **Create** icon.

Build a Workflow:

a Click the **Build a Workflow** tab.

b Expand **Functions** in the right pane.

c Click the **New** tab.

d Click **New WAP IP Flow**.

2 Configure the parameters as follows:

Table 9-159 WAP IP Flow Parameters

Parameter	Description
Name	WAP IP Flow name
Admin State	Admin state: ■ enabled ■ disable
Priority	WAP IP Flow priority This value resolves conflicts in the case of multiple service instances.

Table 9-159 WAP IP Flow Parameters

Parameter	Description
Service Rule	Service Rule(s). The Service Rule must already exist. See Service Rule. To select a Service Rule, drag and drop it from the Available list to the Selected list.

3 Click the **Save** icon.

HTTP Filter File Management

You can configure the following types of control lists:

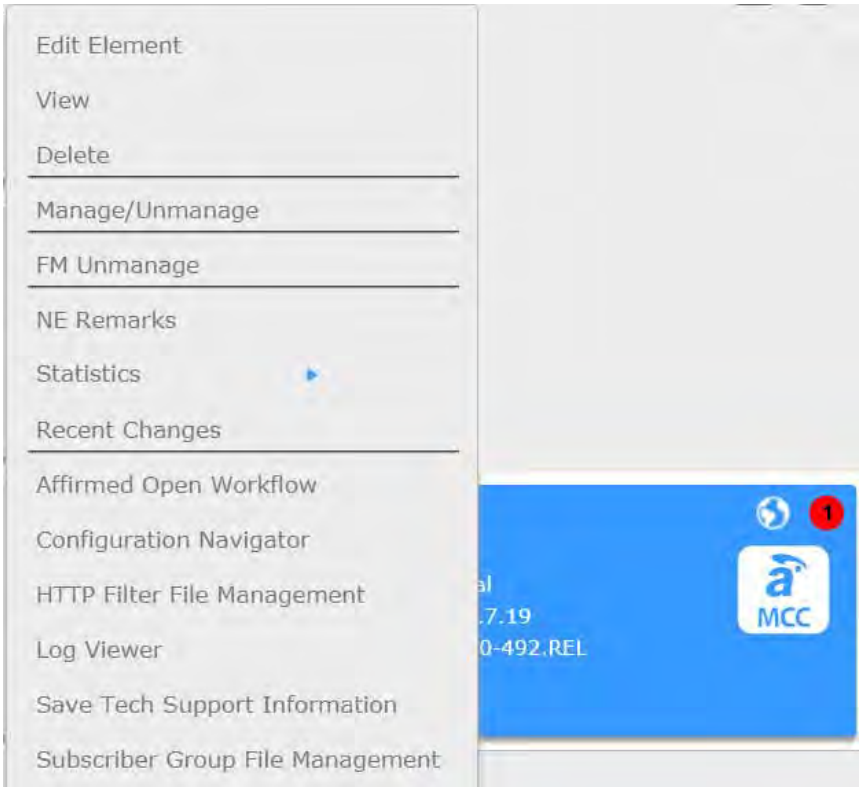
- **URL List** defines a list of URLs. This object can be used by any of the MCC services including Multi Protocol Proxy, Content Filtering, Charging, QoS, and so on. For example, a URL list can be referred to by HTTP Rule Group and used as rules to match HTTP Request's URL.
- **Category** is used by an *instance* of a content filter to either allow (white list) or deny (black list) content requests to a specific list of domains or URLs.

Note: *To use the HTTP Filter File Management application, you must have Configuration > MCC Configuration > Service Provisioning – Content > Admin security group permissions. For instructions, see Specifying Permissions by Security Group.*

To manage HTTP Filter Files:

1 Right-click an NE and select **HTTP Filter File Management**.

Figure 9-38 HTTP Filter File Management



Acuitas lists the HTTP filter files in the system.

In the case of a large number of files, Acuitas displays them over multiple pages. The current page and entry count are listed at the bottom of the window.

To specify how many files you want displayed per page, select the value in the Show Entries box.

Click **First**, **Previous**, **Next**, or **Last** to navigate over multiple pages. To navigate to a specific page, click the page number.

Use the **Search** text box at the top on the window to search for a particular file based on its name, permissions, or size.

Adding URL Lists

The file used to configure the URL List must be a text file. In the file, each URL is a string in the following format:

http[s]://<*domain-name*>[:<*port*>]/[<*url-path*>][/*]

The *port*, *url-path*, and terminating /* are optional. If /* is used, the URL is treated as an URL prefix rather than the exact-match URL.

Acuitas uploads the URL List file to MCC and creates the corresponding url-list object. The file is uploaded to the /public/content/policylists/url/userlists directory on the MCM.

For Create and Modify operations, Acuitas automatically invokes the Import operation.

To add a URL list:

1. Right-click an NE and select **HTTP Filter File Management**.

   Acuitas lists the HTTP filter files in the system.

2. Click **Create URL List**.
3. In **Upload File**, click **Choose File** to upload a text file of URLs.
4. Select the text file and click **Upload**.
5. Once the file uploads, configure the parameters as follows:

Table 9-160 URL List Parameters

Parameter	Description
Name	URL List name
File Type	Local file is the only file type supported: ■ importFromLocalFile

Table 9-160 URL List Parameters

Parameter	Description
File Name	Name of the uploaded URL list file

6 Click **Create**.

Modifying or Deleting URL Lists

To modify or delete a URL list:

1 Right-click an NE and select **HTTP Filter File Management**.

Acuitas lists the HTTP filter files in the system.

2 Select the URL list and click **Modify**.

3 To modify the URL list, make the necessary changes and click **Update**:

Table 9-161 URL List Parameters

Parameter	Description
Name	Displays the URL List name
File Type	Local file is the only file type supported: ■ importFromLocalFile
File Name	Name of the uploaded URL List file

To delete a URL list, click **Delete**.

Viewing the Contents of a URL List File

To view the contents of a URL list file:

1 Right-click an NE and select **HTTP Filter File Management**.

Acuitas lists the HTTP filter files in the system.

2 Select the URL list and click **View File**.

3 When prompted, specify how you want the file saved and click **Save**.

4 When you have finished, close the window.

Adding Categories

To add a Category:

1. Right-click an NE and select **HTTP Filter File Management**.

   Acuitas lists the HTTP filter files in the system.

2. Click **Create Category**.
3. In **Upload File**, click **Browse** to upload a text file of domains or URLs.
4. Select the text file and click **Upload**.
5. Once the file uploads, configure the parameters as follows:

Table 9-162 Category Parameters

Parameter	Description
Name	Category name
File Type	Address types in the file: ■ Domain ■ URL
File Name	Name of the uploaded category file

6. Click **Create**.

To specify that the category be used by a content filter to either allow (white list) or deny (black list) content requests to a specific list of domains or URLs, see Content Filter.

Modifying or Deleting Categories

To modify or delete a category:

1. Right-click an NE and select **HTTP Filter File Management**.

   Acuitas lists the HTTP filter files in the system.

2. Select the category and click **Modify**.
3. To modify the category, make the necessary changes and click **Update**:

Table 9-163 Category Parameters

Parameter	Description
Upload File	To upload a text file of domains or URLs, click **Choose File**. Select the text file and click **Upload**.
Name	Category name
File Type	Address types in the file: ■ Domain ■ URL
File Name	Name of the uploaded category file

To delete the category, click **Delete**.

To specify that the category be used by a content filter to either allow (white list) or deny (black list) content requests to a specific list of domains or URLs, see Content Filter.

Viewing the Contents of a Category File

To view the contents of a category file:

1. Right-click an NE and select **HTTP Filter File Management**.

   Acuitas lists the HTTP filter files in the system.

2. Select the category and click **View File**.
3. When prompted, specify how you want the file saved and click **Save**.
4. When you have finished, close the window.

Viewing HTTP Filter File List

To view the list of a HTTP filter files on the system:

1. Right-click an NE and select **HTTP Filter File Management**.

   Acuitas lists the HTTP filter files in the system.

2. Click **View File List**.

   Acuitas displays the **File List** window, listing the URL list and category files in the system.

   In the case of a large number of files, Acuitas displays them over multiple pages. The current page and entry count are listed at the bottom of the window.

   To specify how many files you want displayed per page, select the value in the Show Entries box.

   Click **First**, **Previous**, **Next**, or **Last** to navigate over multiple pages. To navigate to a specific page, click the page number.

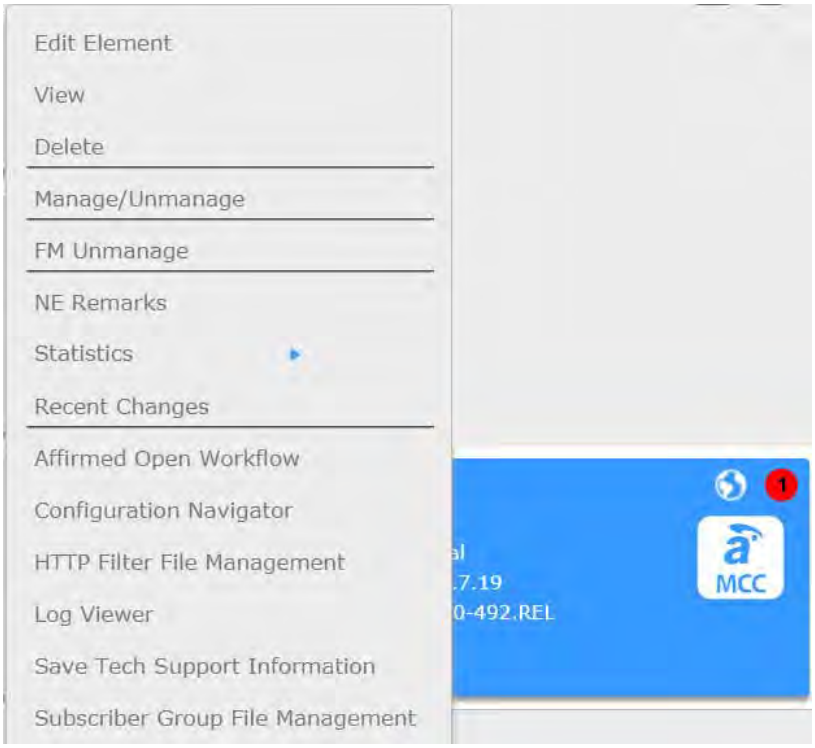
   Use the **Search** text box at the top on the window to search for a particular file based on its name, permissions, or size.

3. When you have finished, close the window.

Configuration Navigator

The Configuration Navigator includes all the configuration parameters of the system. To access the Configuration Navigator application, right-click an NE and select **Configuration Navigator**.

Figure 10-1 Accessing the Configuration Navigator Application



Navigating the System

The **Configuration Navigator** has an easy-to-use graphical user interface with a tree-based listing of the managed objects in the left pane and specific configuration information in the right pane.

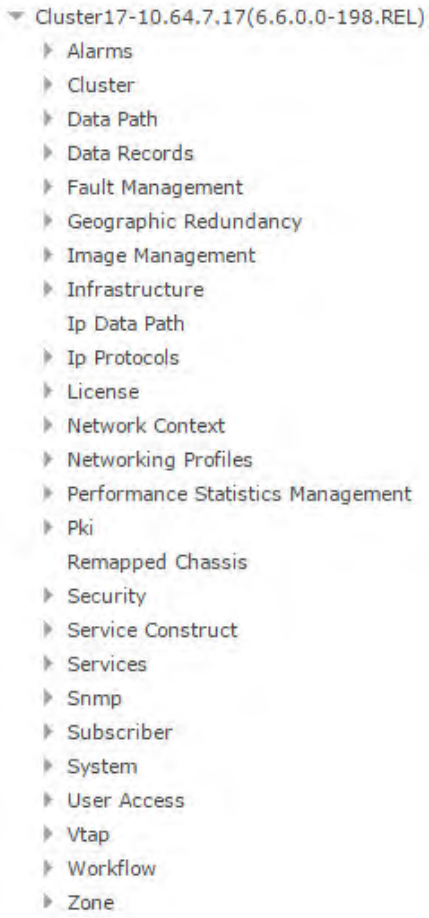
The specific objects you see in the Configuration Navigator depends on your security group permissions. Only the management functions granted to you are available. For instructions, see Specifying Permissions by Security Group.

Note: *For configuration information for the MCC MME, see the Affirmed Networks MCC MME Configuration Management Reference Guide.*

Tree Display

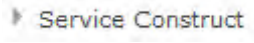
In the left pane, the **Configuration Navigator** displays managed objects using an expandable tree. Expand the NE to view the objects.

Figure 10-2 Configuration Navigator Tree

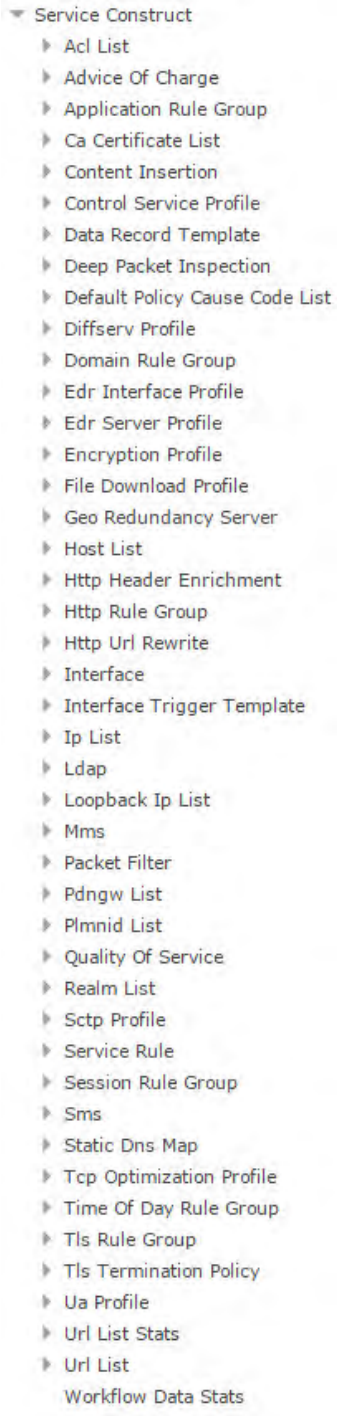


In the tree, the expansion icon indicates which objects contain other objects:

- If the expansion icon points to the right, the object is closed.



- If the expansion icon points down, the object is open, and the names of its contained objects are listed below it.



You navigate through objects in the tree much like you navigate through folders and files listed in a file management program. Click the expansion icons to open and close objects in the tree display.

Refreshing the Tree

At each level of the tree, you can refresh the tree with the latest data. Doing so is useful in cases such as:

- When you view alarms and statistics where the list of child objects could dynamically change on the system.
- When you expand an object to see its instances and the CLI adds another instance.

In these cases, changes are not reflected in the tree until you refresh the tree. To do so, right-click an object in the tree and select **Refresh**.

Paging and Filtering Configuration Object Instances

In the Configuration Navigator, Acuitas restricts display of large numbers of object instances to the first 50 instances. You can page through and filter configuration object instances based on instance name to list the object instances you want.

To page and filter instances:

1. Expand the object type in the tree.
2. Right-click the object in the tree and click **Search**.

Figure 10-3 Search Box

- To navigate over multiple groups of results, use the paging icons:
  - Previous Group
  - Next Group

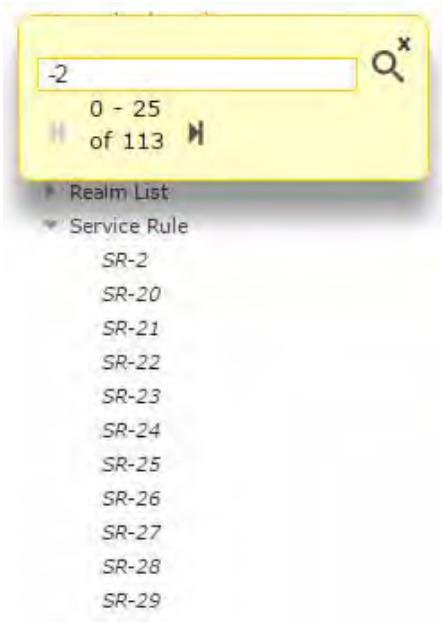
  Then, expand the object in the tree to list its instances.

- To search for particular object instance(s) based on the instance name, use the Search text box. Enter the string contained in the name and click the **Search** icon.

  For example, enter -2 to list all object instances with names containing -2.

  Then, expand the object in the tree to list its instances.

Figure 10-4 Filtered Instances



Configuration Window

In the right pane, the **Configuration Navigator** displays the detailed configuration information for an object selected in the tree. The information displayed depends on which object you select.

Figure 10-5 Configuration Parameters for Selected Card

You can make changes to any parameter that is not Read-only.

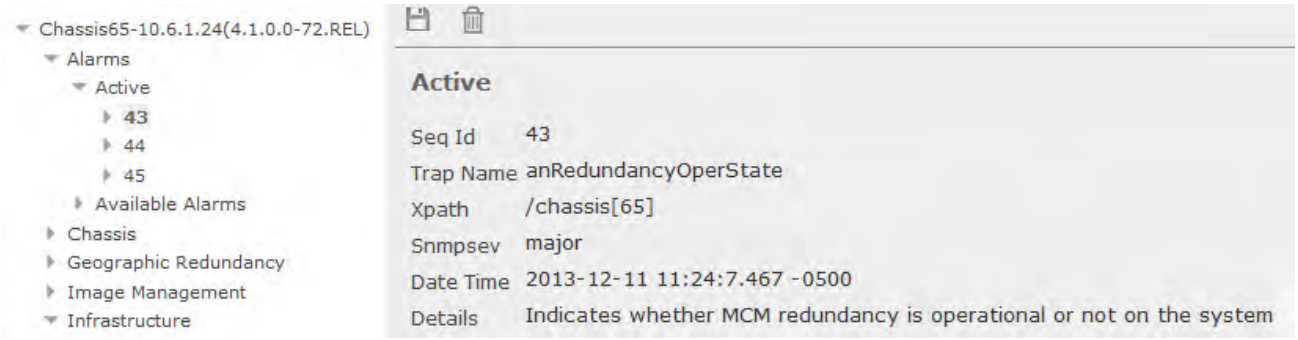
1 Click the **Save** icon.

Alarms

Alarms includes:

- Active – List of active alarms by sequence ID. Click a sequence ID in the tree to view the details of the alarm in the configuration window.

Figure 10-6 Active Alarm Details



- Available Alarms – List of all available alarms. Click an alarm in the tree to Enable/Disable it or change its description or severity level.

Figure 10-7 Available Alarm

Cluster

Use this object to manage a logical group of virtual nodes.

To manage a cluster:

1. Click **Cluster** in the tree.
2. Configure the parameters as follows:

Table 10-1 Cluster Parameters

Parameter	Description
ID	Cluster ID Range: 1-127
Building Block Strategy	Strategy to use to create virtual node personalities. For more information, see Node Personalities.
Max ASMS	Maximum number of ASMs in the cluster (to cap dynamic ASM expansion in the cluster). ***Note:*** *Modifying this value disrupts in-progress connections.*
vCPU Allocation Profile	The optimization capability for VMs on a cluster-wide basis according to expected traffic. Higher numbers use more CPU resources to provide increased bandwidth. This parameter adjusts how much the system allocates to a target machine for background cores, master cores, kernel NIC interface (KNI) processing cores, hard drives, and remaining system cores left for proxy processing. ***Note:*** *This setting does not take effect until the VM is rebooted.*
ASM IO Level	ASM I/O optimization level. Higher numbers use more CPU resources to provide increased I/O bandwidth. Setting this parameter to a value higher than the default causes ISM/IWM/ASMs to consume more DPDK cores. If DPDK does not have enough cores, the ISM/IWM/ASM cannot come up. The anPacketengineError alarm is raised, the ISM/IWM/ASM is placed into a fault state, and all packet processing is stopped. To resolve this situation, refer to the deployment guide and ensure the ISM/IWM/ASMs have at least the minimum cores configured for the desired asm-io-level. ***Note:*** *Changes to this value require a ISM/IWM/ASM reboot to take effect.*
SSM IO Level	***Note:*** I/O optimization level for SSM/IOM/WSM/ISM/IWM. Higher numbers use more CPU resources to provide increased I/O bandwidth. ***Note:*** *Changes to this value require a VM reboot to take effect.*

Table 10-1 Cluster Parameters

Parameter	Description
Max Nat Workflow Modules	Maximum number of workflow modules supported by NAT. Previously, when a cluster booted, the port range was allocated into 15 blocks and the MCM assigned one of the 15 port blocks to an SSM when it joined the system. This parameter specifies to carve the port range into a specific number of blocks. To efficiently use the address space defined in your NAT pools, Affirmed Networks recommends setting this parameter to coincide with the number of SSMs/WSMs in your cluster. For example, in a cluster with only three SSMs/WSMs, set this parameter to 3 even though the parameter defaults to 15.

3 Click the **Save** icon.

Node Personalities

Node personality defines which services are started on a given node in a cluster. A node can be configured to use a specific personality, each of which runs a predefined collection of functionality sets. This feature allows Operators to run specialized card/nodes with the exact services they want and increases MCC performance.

To configure personalities, first specify a *Building Block Strategy* for the cluster. The strategy specifies the supported combinations of node personalities to build the cluster. The Building Block Strategies are:

- **compact Strategy** — For traditional MCM, CSM, and SSM nodes.

  Contents:

  – MCM (Management Control Module)

  – SSM (Subscriber Services Module)

  – CSM (Control/Content Services Module)

- **advanced-services-separation Strategy** — Optimized for small clusters (less than 12 nodes). This strategy separates the advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) from the Call-Control Management services (PGW, SGW, and GGSN). Systems that do not provide advanced services *should not* deploy the ASM personality node in this strategy. Systems that do provide advanced services do need to deploy the ASM personality node.

  Contents:

  – MCM (Management Control Module)

  – SSM (Subscriber Services Module)

  – ASM (Advanced Services Module – Content services)

  – CPM (Control Plane Module)

- **control-services-separation Strategy**: This strategy separates the centralized and distributed aspects of the Call-Control Management services. If either the advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) or the Call-Control Management services (PGW, SGW, and GGSN) increase over time, the cluster can be expanded/scaled to support the growth.

  Contents:

  – MCM (Management Control Module)

  – ASM (Advanced Services Module – Content services)

  – SSM (Subscriber Services Module)

  – CCM (Centralized Control Module)

  – DCM (Distributed Control Module)

- **specialized Strategy** — Optimized for large clusters (more than 12 nodes). In addition to the separation provided by advanced-service-separation, this strategy separates the I/O and the workflow services on the SSM node. In addition, it separates the centralized and distributed aspects of the Call-Control Management services. Systems that do not provide advanced services do not need to deploy the ASM personality node in this strategy. Systems that do provide advanced services do need to deploy the ASM personality node. Applies to cluster nodes only.

  Contents:

  – MCM (Management Control Module)

  – IOM (I/O Module)

  – WSM (Workflow Services Module)

  – ASM (Advanced Services Module – Content services)

  – CCM (Centralized Control Module)

  – DCM (Distributed Control Module)

- **integrated-services Strategy** — Centralizes the execution of data forwarding services (workflow and I/O) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM and Call-Control Management services (PGW, SGW, and GGSN) in another VM. As a result, the cluster can be expanded/scaled to independently support growth of gateway call control services, workflow, I/O, and content services.

  Contents:

  – MCM (Management Control Module)

  – CPM (Control Plane Module)

  – ISM (Integrated Services Module: Content and Subscriber Services)

    The ISM provides a one-stop processing node for data forwarding services and content services.

- **integrated-workflow Strategy** — Centralizes the execution of data forwarding services (workflow) and advanced services (such as Multi Protocol Proxy, Cache, and Video Transcoding) in one VM, Call-Control Management services (PGW, SGW, and GGSN) in another VM, and I/O services in another VM. As a result, the cluster can be expanded/scaled to independently support growth of gateway call control services, workflow, and content services.

  Contents:

  – MCM (Management Control Module)

  – CPM (Control Plane Module)

  – IOM (I/O Module)

  – IWM (Integrated Workflow Module)

    The IWM provides a one-stop processing node for workflow services and content services.

Then, when you configure a node for the cluster, select the node type and node personality.

- Node type:
  - CSM: Control/Content Services Module
  - MCM: Management Configuration Module
  - SSM: Subscriber Services Module
  - vCSM: Virtual Control/Content Services Module
  - vMCM: Virtual Management Configuration Module
  - vSSM: Virtual Subscriber Services Module
- Node Personality: The personalities available for a node are filtered based on the Building Block Strategy specified for the cluster.

  The various personalities are described in the following table.

Table 10-2 Personalities

Personality	Description
CCM: Centralized Control Module ***Note:*** *Do not set Admin State to disabled for CCM personality.*	*Applies to node type vCSM* Runs the centralized tasks needed for call-control functionality and routing protocols.
DCM: Distributed Control Module	*Applies to node type vCSM* Runs the distributed tasks needed for call-control functionality (mainly the PGW, SGW, and RADIUS tasks).
CPM: Control Plane Module ***Note:*** *Do not set Admin State to disabled for CPM Personality,*	*Applies to node type vCSM* Runs all tasks needed for call-control functionality.
IOM: I/O Module ***Note:*** *Do not set Admin State to disabled for IOM personality.*	*Applies to node type vSSM* Is responsible for receiving packets into the MCC and sending the packets out.
WSM: Workflow Services Module	*Applies to node type vSSM* Provides workflow services.
SSM: Subscriber Services Module	*Applies to node type vSSM* Runs all services provided by IOM and WSM.
ASM: Advanced Services Module	*Applies to node type vCSM* Runs the tasks needed for providing advanced services like Multi Protocol Proxy, Cache, WAP GW, etc.
CSM: Control/Content Services Module	*Applies to node type vCSM* Runs all services provided by CPM and ASM.

Table 10-2 Personalities

Personality	Description
ISM: Integrated Services Module	*Applies to node type vSSM* Runs content and subscriber services
IWM: Integrated Workflow Module	*Applies to node type vSSM* Runs workflow services and content services

Value-Added Services Guidelines

When deploying Value-Added Services (VAS), use the following VM provisioning guidelines:

- Use one of the following cluster building block strategies:
  - specialized (preferred)
  - advanced-services-separation (small deployments only)
  - compact (small deployments only)
  - integrated-services
  - integrated-workflow
- Provision a sufficient number of CSM VMs as required for your network deployment:
  - use CCM, DCM, and ASM personalities for specialized cluster building block strategy
  - use CPM and ASM personalities for advanced-content-separation cluster building block strategy
  - use default v-CSM personality for compact cluster building block strategy
  - use ISM personality for integrated-services building block strategy
  - use IWM personality for integrated-workflow building block strategy
- For ISMs and IWMs, designate a minimum of 16 vCPUs. Performance and throughput at any vCPU provisioning level (including 16 vCPUs) depends on traffic profiles and call models. Between this assignment and the setting in ASM optimization level, you can scale performance and throughput based on the network services you provide in your network deployment.
- Designate a dedicated CPU to each ASM by setting the processor affinity.
- Set the number of ASM virtual cores to the number of CPU cores minus 10%, reserving the remainder for the VM hypervisor. For example:
  - 18 on CPU with 20 virtual cores
  - 22 on CPU with 24 virtual cores

When deploying CPU intensive functionality, including image and video transcoding, the minimum number of virtual cores is 18.

- Provision memory for ASMs or CSM VMs running Value-Added Services:
  - minimum of 55GB for typical deployments
  - minimum of 32GB evaluation deployments with a limited number (up to a few hundred) of subscribers

Scale In Limitations

Scale In have the following limitations:

- On Scale In of a DCM, some sessions that do not passively get closed (on the gateway that is being removed) will be closed, disrupting the traffic belonging to those sessions.
- On Scale In of an ASM, some HTTP connections that do not close during the dry-up period will be closed. The UE can re-establish a new connection.
- When a WSM node is disabled as part of dynamic scaling, the grid removes the range of FSAPIs that were earlier assigned to the card. The gateway migrates all of the sessions using FSAPIs of this card to another active SSM (or WSM) node. As a result, workflow sessions are deleted on an old FSAPI and a new workflow session are created with the new FSAPI. The following limitations arise with this implementation:
  - During the session migration from an old FSAPI to a new FSAPI, data may be lost in the timing window between when the session is deleted on the old FSAPI and recreated on the new FSAPI.
  - If Proxy is enabled, all of the connection data information maintained by wfdivert module will be lost and the corresponding HTTP transactions will timeout. The same limitation applies to all of the Content services that use this module (SIP, WAP Gateway, SMTP Proxy).
  - If NAT is enabled, all of the active connections (not just TCP connections) will be lost. They must be reestablished after the workflow session is recreated on the new WSM. The same limitation applies to all the supported ALGs, as the flow state is not synchronized with a standby (SIP, RTSP, FTP, TFTP ALGs).
  - When an NE is deployed as a PGW or GGSN, the reassembly of fragmented packets that originate from UE is performed in the workflow manager module. As part of dynamic contraction, when a session is migrated to another SSM (WSM), any fragments that have not yet completed reassembly will be lost (because after FSAPI migration, the workflow for this session is anchored on a different WSM.)

– The grid can choose to use WSM modules as backup for FSAPIs assigned to other cards. When a WSM is Scaled Out, the grid designates one of the remaining cards to work as a backup for those FSAPIs for which the WSM being disabled was serving as backup. Thus, the backup for certain FSAPIs will move from one node to another during both dynamic WSM expansion and contraction. This condition exposes a timing window if (even before the workflow sessions on the backup FSAPIs are fully set up) the SSM(WSM) with the active FSAPI either reboot or crash. Data will be lost during this timing window. This condition is expected to be transient, as normal operation is expected to resume as soon as the workflow session is created on the SSM(WSM).

Control Plane Protection

Use this object to configure automatic protection switching of the inter-node control data plane. The object enables the (1+1) redundancy feature and requires two distinct VLAN for inter-node data connectivity protection.

To manage control plane protection:

1. Expand **Cluster** in the tree.
2. Expand a Cluster ID.
3. Click **Control Plane Protection**.

Control Plane Protection child objects and their parameters are listed in the following table:

Table 10-3 Control Plane Protection Child Objects and Parameters

Object	Parameter	Description
Keep Alive	Node ID	Node ID
	Peer Node ID	Peer Node ID
	Port A Most Recent Rx MS	Port A most recent received Keep Alive (in milliseconds)
	Port B Most Recent Rx MS	Port B most recent received Keep Alive (in milliseconds)
Status *Control plane redundancy table*	Node ID	Node ID
	Using Port	Port used
	Num Switchovers	Number of Switchovers
	Elapsed Time Since Switchover MS	Elapsed Time Since Switchover (in milliseconds)
	Bitmap Reachable Nodes Port A	Bitmap of reachable nodes for Port A
	Bitmap Reachable Nodes Port B	Bitmap of reachable nodes for Port B
	Most Recent Switchover Cause	Cause of most recent switchover

Data Plane Protection

Use this object to configure automatic protection switching of the inter-node data plane. The object enables the (N+1) redundancy feature and configures the VLAN IDs for each of the data plane networks.

To manage data plane protection:

1. Expand **Cluster** in the tree.
2. Expand a Cluster ID.
3. Click **Data Plane Protection**.
4. Configure the parameters as follows:

Table 10-4 Data Plane Protection Parameters

Parameter	Description
Admin State	Automatic Protection administrative state: ■ enabled ■ disabled
Detached Node Interval	Number of seconds a node must be detached from the data plane before initiating a reset operation.
Mode	Mode: ■ protected-paths-AB: Monitoring Paths A and B ■ unprotected-paths-A: Monitoring Path A only
Reset Detached Nodes	Initiate a node reset operation for nodes that become detached from the data plane.
VLAN ID A	VLAN ID of external VLAN I
VLAN ID B	VLAN ID of external VLAN 2

5. Click the **Save** icon.

Data Plane Protection child objects and their parameters are listed in the following table:

Table 10-5 Data Plane Protection Child Objects and Parameters

Object	Parameter	Description
Keep Alive	Node ID	Source Node that is receiving keep-alives.
	Peer Node ID	Source Node is receiving keep-alives from this peer (that is, the sender).
	Port A Most Recent Rx MS	The elapsed milliseconds since a keep-alive was received from the peer.
	Port A Most Recent Rx+Tx MS	The elapsed milliseconds since a keep-alive was received from the peer where the peer is indicating that it is receiving keep-alives from the source node (that is, a keep-alive indicating connectivity in both directions is successful).
	5 Minute History Percent Rx Port A	The percentage time the link has been receiving keep-alives from the peer over the past 5-minute interval.
	5 Minute History Percent Rx+Tx Port A	The percentage time the link has been receiving keep-alive from the peer over the past 5-minute interval, where peer is receiving from the source node.
	Port B Most Recent Rx MS	The elapsed milliseconds since a keep-alive was received from the peer.
	Port B Most Recent Rx+Tx MS	The elapsed milliseconds since a keep-alive was received from the peer where the peer is indicating that it is receiving keep-alives from the source node (that is, a keep-alive indicating connectivity in both directions is successful).
	5 Minute History Percent Rx Port B	The percentage time the link has been receiving keep-alives from the peer over the past 5-minute interval.
	5 Minute History Percent Rx+Tx Port B	The percentage time the link has been receiving keep-alive from the peer over the past 5-minute interval, where peer is receiving from the source node.

Table 10-5 Data Plane Protection Child Objects and Parameters

Object	Parameter	Description
Status *Indicates the reachability of remote nodes over each of the fabric ports*	Node ID	Source Node Number
	Using Port	Port used: A, B, A+B Indicates the source node is using either entirely redundant path A, B, or combination of A and B to reach other nodes. When MCM controller 7 is active, the preferred (or default) redundant data path is A, and when MCM controller 8 is active, the preferred path is B. If both ports A + B are in use, it implies a connectivity health check has failed on the preferred path.
	Num Switchovers	Number of times the source node has changed a path selection for at least one other node.
	Bitmap Reachable Nodes Port A	Indicates a bit map (in hexadecimal) of other nodes that are reachable over port A. For example, for the reported value 0x000000000037, the hexadecimal value 37 is 00110111 in binary. The lowest order bit (rightmost) refers to node 1, next bit slot 2, and so on. The value 00110111 implies nodes 1,2,3,5,6 are reachable over port A.
	Bitmap Reachable Nodes Port B	Indicates a bit map (in hexadecimal) of other nodes that are reachable over redundanct port B. For example, for the reported value 0x000000000037, the hexadecimal value 37 is 00110111 in binary. The lowest order bit (rightmost) refers to node 1, next bit slot 2, and so on. The value 00110111 implies nodes 1,2,3,5,6 are reachable over port B.
	Most Recent Switchover Cause	A date time stamp and cause for the most recent change in path selection (which is based on keep-alive connectivity health checks). For example: 2015-05-04T14:34:55-0400 Switching to path:B map: fffffffffff, (A=eth1.700, B=eth3.800), active MCM path B Because the active MCM controller is mcm-8, the preferred path is port B. All known nodes are reachable over path B. The map variable (hexadecimal 0xfffffffffff) indicates all 1's in binary, implying all nodes can be reached using port B. Value '0' in the map indicates redundant port A for the corresponding node.

GNP Sub Pool

Use this object to configure the GNP Subpool range used for internal routing addresses.

To manage GNP Subpool:

1. Expand **Cluster** in the tree.
2. Expand a Cluster ID.
3. Click **GNP Sub Pool**.
4. Configure the parameters as follows:

Table 10-6 GNP Sub Pool Parameters

Parameter	Description
Range Start	Starting value for IPv4 address of the GNP of the GNP sub-pool range
Range End	Ending value for IPv4 address of the GNP of the GNP sub-pool range
Prefix Length	CIDR prefix length of the GNP sub-pool range

5. Click the **Save** icon.

Node

Use this object to configure and view status of virtual nodes.

To configure a node:

1. Expand **Cluster** in the tree.
2. Expand a Cluster ID.
3. Expand **Node**.
4. Click a Node ID.
5. Configure the parameters as follows:

Table 10-7 Node Parameters

Parameter	Description
Node Commands	To issue a card command, select the command and click **Select**: ■ Reboot
ID	Card ID
Type	Card type: ■ CSM: Control/Content Services Module ■ MCM: Management Configuration Module ■ SSM: Subscriber Services Module ■ vCSM: Virtual Control/Content Services Module ■ vMCM: Virtual Management Configuration Module ■ vSSM: Virtual Subscriber Services Module ■ Empty
Personality	Node Personality: ■ ASM: Advanced Services Module ■ CCM: Centralized Control Module ■ CPM: Control Plane Module ■ CSM: Control/Content Services Module ■ DCM: Distributed Control Module ■ IOM: I/O Module ■ MCM: Management Control Module ■ SSM: Subscriber Services Module ■ WSM: Workflow Services Module The personalities available are filtered based on the Building Block Strategy specified for the cluster. For more information on personalities, see Node Personalities.

Table 10-7 Node Parameters

Parameter	Description
Admin State	Card administrative state: enabled: Card is providing full service. Tasks are active and running on the card. The overall capacity of system goes up by the capacity of this card. disabled: Card is out of service. Tasks are not running on the card and the card is powered down. The tasks for this card are no longer listed. This state of this card is similar to that of a card that is not yet provisioned. The overall capacity of the system goes down by the capacity of this card. maintenance: Card has stopped processing new service and is gradually transferring existing services elsewhere. The tasks on this card are alloted time (specified by the **Dry Up Period**) to transfer existing services. This card cannot serve as a backup for services provided by other cards. The standby tasks on this card are moved elsewhere. This card cannot serve as a provider of any global scope services, therefore any global scope tasks that are active on this card are switched over to their backups. Any standby global scope tasks from this card are moved to other enabled cards. The global scope services are provided with a very short Dry Up Period before switching over. Do not set Admin State to disabled for the following node personalities: ■ CPM ■ CCM ■ IOM
Data Fabric IP Address A	Data Fabric IP Address port A
Data Fabric Prefix Length A	Prefix Length of the Data Fabric IP Address port A
Data Fabric MTU A	MTU on Data Fabric port A ***Note:*** *Applies to VM cards only*
Data Fabric IP Address B	Data Fabric IP Address port B
Data Fabric Prefix Length B	Prefix Length of the Data Fabric IP Address port B
Data Fabric MTU B	MTU on Data Fabric port B ***Note:*** *Applies to VM cards only*
The MCC allocates redundant resources on nodes that share the least fate with nodes where the active resource is running. This feature maximizes the chances that a standby is able to take over when an active resource encounters an outage. The physical location properties of a node (such as site, rack, shelf, blade, and node ID) are used to determine the fate-sharing costs between the active and standby pair. When creating a cluster node, configure the physical location parameters (Site, Rack, Shelf, Blade). If you later change any of these values, you must reboot the cluster for proper fate-sharing to take effect.	

Table 10-7 Node Parameters

Parameter	Description
Site	Physical site where the VM is hosted ***Note:*** *Applies to VM cards only*
Rack	Physical rack where the VM is hosted ***Note:*** *Applies to VM cards only*
Shelf	Shelf where the VM is hosted ***Note:*** *Applies to VM cards only*
Blade	Blade index where the VM is hosted, such as the slot number of the blade within the blade system ***Note:*** *Applies to VM cards only*
IP Address	Management IP address of the hardware, such as the enclosure Onboard Administrator IP of the blade system ***Note:*** *Applies to VM cards only*
VM IP Address	Management IP Address of the VM host ***Note:*** *Applies to VM cards only*
VM Name	Name of the VM host ***Note:*** *Applies to VM cards only*
Dry Up Period	Number of seconds allowed for process to shed work before going idle.

6 Click the **Save** icon.

Node child objects and their parameters are listed in the following table:

Table 10-8 Node Child Objects and Parameters

Object	Parameter	Description
Fault Detail	Fault Filename	Fault filename
	Time	Fault time
	Notes	Fault notes
Fault Summary	Seconds Since Epoch	Epoch timestamp when the crash occurred
	Fault Filename	Fault filename
	Time	Fault time

Table 10-8 Node Child Objects and Parameters

Object	Parameter	Description
Critical Service	Cache	Service name and State of Cache service
	P-Gateway	Service name and State of P-Gateway service
	Proxy	Service name and State of Proxy service
	S-Gateway	Service name and State of S-Gateway service
	Transcoding	Service name and State of Transcoding service
Disk Cache	Disk Cache Commands	To issue a disk cache command, select the command and click **Select**: ■ Format ■ Check Errors
	Disk ID	Disk ID
	Admin State	Disk Admin State
Disk Status	Disk ID	Disk ID
	Name	Disk Name
	Admin State	Disk Admin State
	Oper Status	Disk Oper Status
	Disk Size	Disk Size
	Disk Usage	Disk Usage
	Use Percent	Disk Use Percent
	Disk Error	Disk Error
Disk Perf Stats Statistics listing the free disk space available on the node	Images	For each, statistics include: Disk Size Disk Usage Use Percent, calculated as Disk Usage divided by Disk Size, times 100.)
	Operational Image	
	Prepared Image	
	Proxy Cache	
	RAM Storage	
	Rollback Image	
	Storage	
File Mgmt Statistics		

Table 10-8 Node Child Objects and Parameters

Object	Parameter	Description
Processes Displays the actual processes running on a node. It is useful for checking any process and its status. You can sort the processes in ascending or descending order by any of these fields. To sort, click the field name.	CPU Number	
	Task Name	
	Service Name	
	HA State	
	Oper State	
	CPU Utilization	
	Memory Utilization	
	Flash Utilization	
	IP Address	
	Port	
	PID	
	Release	
Ramdisk Is used to store Charging Data Records (CDR) and NAT Binding Records (NBR) to volatile storage for v-MCM node types. For more information on using RAMDISK, see RAMDISK.	Size	Ramdisk Size
	Admin State	Ramdisk Admin State
Task	Dryup	Connections in the process of shedding work before going idle: ■ Number of connections ■ Percentage of connections
	Operation Detail	Task operation detail
	Statistics	Task statistics

RAMDISK

Use this object to store Charging Data Records (CDR) and NAT Binding Records (NBR) to volatile storage for v-MCM node types. The MCC performs a vMCM memory check when 512 M or higher RAMDISK is requested. The total amount of vMCM memory required is 8G plus the RAMDISK memory. A vMCM with 8G supports 128/256M RAMDISK.

To configure RAMDISK:

1. Expand **Cluster** in the tree.
2. Expand a Cluster ID.
3. Expand **Node**.
4. Expand a Node ID.
5. Click **Ramdisk**.
6. Configure the parameters as follows:

Table 10-9 RAMDISK Parameters

Parameter	Description
Size	RAMDISK size Valid values are 128M, 256M, 512M, 1G, 2G, 4G, 8G, 16G (512M and greater require a minimum RAM of (8GB + size) on the v-MCM). Once enabled on the active MCM, subsequent changes to this value require a switchover or reboot to take effect.
Admin State	Admin State: ■ enabled ■ disabled Once enabled on the active MCM, subsequent changes to this value require a switchover or reboot to take effect.

7. Click the **Save** icon.

To view the RAMDISK status, expand a Node ID in the tree, and click **Disk Status**.

To direct CDR/NBR onto RAMDISK, configure a File Management Profile of type RAM Data Record for file upload and purging. Specify a Profile Name to be used as the prefix prepended to all NBR files associated with the profile. For details, see File Management.

For NBR records, configure a port NBR interface service profile of type RAM Data Record. For details, see Interface: Port NBR Service.

Note: CDR/NBR records are stored on RAMDISK on the active MCM. In the case of MCM failure or switchover, any records that have not shipped to the remote server (since the last transfer) are lost. To minimize loss of files, set the Upload Frequency of the File Management Profile to the minimum value of 1 minute.

Statistics

Use this object to view cluster statistics by slot.

To view cluster statistics:

1. Expand a Cluster ID in the tree.
2. Click **Statistics**.

Cluster summary parameters are:

- Slot Number
- CPU Number
- CPU Utilization
- Memory Utilization
- Process Count

Summary

Use this object to view cluster summary by slot.

To view cluster summary:

1. Expand a Cluster ID in the tree.
2. Click **Summary**.

Cluster summary parameters are:

- Slot Number
- CPU Number
- Type
- Personality
- Model
- Admin State
- HA State
- CPU State
- CPU Uptime

- Release: An asterisk after the release number indicates that one or more node tasks are not yet operationally up. Depending on the configuration, some tasks can take longer than others to come up. When all nodes are operationally up, the cluster is fully operational.

TND Peer Statistics

Use this object to view peer TNDM statistics by CPU.

To view peer TNDM statistics:

1. Expand a Cluster ID in the tree.
2. Click **TND Peer Stats**.

TND Total Statistics

Use this object to view TNDM statistics on an aggregated basis across all CPUs.

To view total TNDM statistics:

1. Expand a Cluster ID in the tree.
2. Click **TND Total Stats**.

Data Path

Use this object to manage various elements of MCC Fastpath.

To view Data Path:

1 Expand **Data Path** in the tree.

Data Path child objects and their parameters are listed in the following table:

Table 10-10 Data Path Child Objects and Parameters

Object	Parameter	Description
GRE	Tunnel Summary	GRE Tunnel summary
DPI	DPI	Control DPI
	Tethering Detection Algorithm	Control tethering detection algorithms
	Tethering Quality Index	Percentage value for Quality Index (Confidence Index) to mark connection as tethered.
	Decode First HTTP Transaction Only	On persistent HTTP connections, specifies whether to send packets of all HTTP transactions to the DPI engine for decoding: ■ enabled – On persistent HTTP connections, as soon as fastpath detects the first server response header, the connection is closed (at L7 level) and subsequent HTTP transactions are not sent to the DPI engine for decoding. This setting can cause classification errors, as DPI examines only the first transaction. ■ disabled – On persistent HTTP connections, packets of all HTTP transactions are sent to the DPI engine for decoding.
Iom	Data Statistics	Display IOM data statistics
	Module Statistics	Display IOM module statistics
	Table	Table Statistics
	Statistics Control	Control data path related statistics behavior
	Workflow	Workflow Statistics

Data Records

Use this object to view data record statistics.

Detail

Use this object to view detail statistics for each source (TOS task) of data records.

To view detail statistics:

1. Expand **Data Records** in the tree.
2. Expand **Detail**.
3. Click an instance.

   Detail statistics parameters are:

   - Agent: Name of the Agent receiving the records
   - Source: Name of the task generating the records
   - Records Attempted: Data Records Attempt made
   - Records Failed: Number of records for which send failed
   - Records Succeeded: Number of records for which send to agent succeeded
   - Records Written: Number of records written to disk
   - Records Write Failed: Number of records for which write failed

Statistics

Use this object to view data record statistics.

To view data statistics:

1. Expand **Data Records** in the tree.
2. Expand **Statistics**.
3. Click an instance.

   Data statistics parameters are:

   - Agent: Name of the Agent task
   - Records Written: Total number of records written to disk
   - Records Failed: Total records failed

Fault Management

Use this object to manage Fault Management throttle limits on duplicate events to prevent trap storms.

To manage Fault Management throttle limits:

1. Expand **Fault Management** in the tree.
2. Click **Throttle Limits**.
3. Configure the parameters as follows:

Table 10-11 Throttle Limit Parameters

Parameter	Description
Event Limit	Number of events per alarm type that can be forwarded per time period (0 disables throttling). The length of each time period is defined by the system. The default is 1 second.

4. Click the **Save** icon.

To view the historical list of actions taken by Fault Management director:

1. Expand **Fault Management** in the tree.
2. Click **History**.

Fault Management history parameters are:

- Date Time
- Slot Number
- CPU Number
- Last Fault Action

Flow Idle Timeout Profile

Use this object to specify one or more entries of Flow Idle Timeout Rule. This object is bound to the Data Profile.

To add a Flow Idle Timeout Profile:

1. Click **Flow Idle Timeout Profile** in the tree.
2. Configure the parameters as follows:
   - **Name** – Enter a Flow Idle Timeout Profile name.
3. Click the **Save** icon.
4. Expand **Flow Idle Timeout Profile**.
5. Expand the Flow Idle Timeout Profile you added.
6. Click **Flow Idle Timeout Rule**.
7. Configure the parameters as follows:
   - **Name** – Select the Flow Idle Timeout Rule name. The Flow Idle Timeout Rule must already exist. See Flow Idle Timeout Rule.
8. Click the **Save** icon.

Geographic Redundancy Group

A Geographic Redundancy Group is a collaborative system of two geographically-separated cluster functioning as standby partners for each other. A Geographic Redundancy group has a designated primary and a designated secondary system.

Note: *It is recommended that you use the Geographic Redundancy Manager application to configure Geographic Redundancy Groups. For instructions, see* *Geographic Redundancy Manager*.

To add a Geographic Redundancy Group:

1. Expand **Geographic Redundancy** in the tree.
2. Click **Group**.
3. Configure the parameters as follows:

Table 10-12 Geographic Redundancy Parameters

Parameter	Description
Name	Enter a Geographic Redundancy Group name.
Admin State	Admin State: ■ enabled ■ disabled Set to enabled to initialize and start the redundancy mechanism (such as synchronization in hot mode). Setting to disable invalidates any synchronized data and sets the mechanism into an non-ready state.
Role	The instance configured HA backup role: ■ primary - Specifies which node is “active” under normal network conditions. ■ secondary - Specifies which node is “standby” under normal network conditions.
Manual State	The manually configured HA state (the Operator current desired state): ■ active ■ standby

Table 10-12 Geographic Redundancy Parameters

Parameter	Description
Mode	The instance configured HA mode: ■ warm-manual - no session synchronization occurs between nodes, failovers are Operator controlled ■ hot-auto - synchronization of per-session data occurs between nodes, failovers are automatically triggered based on network health monitoring results ■ hot-manual - synchronization of per-session data occurs between nodes, failovers are Operator controlled
Group ID	Configure the unique group ID that matches with the peer
Failed Session Resync Max Duration Geo Standby	Maximum duration (in seconds) in which the failed session on the geo-redundant standby cluster should attempt to be restored. For value 0, no attempt is made to restore/resync the failed session on the geo-redundant standby for that geo-redundant group. In addition, any existing failed sessions marked for restoration are cleared.

4 Click the **Save** icon.

To view Geographic Redundancy Group status:

1 Expand **Geographic Redundancy** in the tree.

2 Expand **Redundancy Group Status**.

3 Click a group.

Geographic Redundancy Group statistics parameters are:

- Name
- Admin State
- Group ID
- Role
- Mode
- Manual State
- Runtime State — Specifies the current runtime state of the redundancy group. In manual mode, this value always reflects the manually configured HA state. In hot-auto mode, the HA state can change based on faults or failures in network connectivity.
- Oper Status
- Sync Records — Number of records in queue to be synchronized from active (record source) to standby (record sink).

- Geo Link State — Reflects the state of the connection between primary and secondary NEs
- Peer State
- Peer Oper Status
- Peer Sync Records

Net Link Status

Network Link status displays the current connectivity status with neighboring NEs that are critical to the successful operation of the node. Links that are *shared* refer to common interfaces (such as IP Addresses) that are shared between the primary and secondary nodes. Because each node advertises routes to the shared addresses, but with different route metrics or costs, it is expected that a shared link service is normally up at only one of the nodes. Links that are *private* refer to non-shared interfaces used to determine connectivity with neighboring network elements. In the normal network with no faults, it is expected that both the primary and secondary local link status are up.

To view Net Link status:

1. Expand **Geographic Redundancy** in the tree.
2. Expand **Net Link Status**.
3. Click a group.

   Link Status parameters are:

   - Group Name
   - Link type – Indicates whether the link used to monitor neighboring network elements is a shared link among the primary and secondary NE's or a private (local) link.
   - Link Service – Identifies the neighboring NE being monitored.
   - Status – Identifies outcome of monitoring (up or down).
   - Peer Status – When NEs are connected, identifies the redundant peer's perspective of the network element monitoring.

     For shared links under normal network conditions, only the active node is expected to show a status of up and peer normally shows down, because the IP address is shared but routing metrics prefer the active node over the standby.

Image Management

Use this object to manage images.

To configure image management:

1. Click **Image Management** in the tree.
2. To issue an image management command, select the command and click **Select**:
   - **removeAdminVersion** - Remove a version.

     Inputs:

     – Version - Version to Remove
   - **upgrade** - Upgrade the node.

     Inputs:

     – Version - Version to upgrade to

     – Force - Specify that the operation wait to complete until both MCMs have caught up (rather than wait for all cards to catch up)
   - **onlineupgrade** - Online Upgrade the node.

     Inputs:

     – Version - Version to upgrade to (from Display Available Admin Versions)

     – Drain - Drain timeout in seconds. Allows tasks to drain of work before being replaced. It can reduce the disruption caused by replacement, but may significantly extend the time to complete the upgrade (especially if Strategy is Task Reset)

     – Strategy - Reset strategy to control how many tasks are replaced at a time: Card Reset, TOS Reset, Task Reset

     – Continue on payload timeout - Continue the upgrade even when payload nodes fail to fully reach Oper State up. Use this option to enable the OSU to continue even if a TOS task hangs during a payload OSU. If a task hang occurs, the OSU continues but service is impacted.
   - **prepare** - Prepare the node for upgrade.

     Inputs:

     – Version

     – Force - Specify that the operation wait to complete until both MCMs have caught up (rather than wait for all cards to catch up)
   - **rollback** - Rollback the node to the previous version (specified in Rollback Version)

     Inputs:

     – Force - Specify that the operation wait to complete until both MCMs have caught up (rather than wait for all cards to catch up)

- **reset** - Reset the upgrade engine after a failure in order to retry
- **available-admin-versions** - Display the versions currently available for upgrade.
- **progress** - Display the activation progress during upgrade or rollback
- **online-upgrade-plan** - Considers the metadata, the options, and the system state and displays how an Online Upgrade would proceed if issued at this time.

  Inputs:

  – Version - Version to upgrade to (from Display Available Admin Versions)

  – Drain - Drain timeout per card in seconds. Allows tasks to drain of work before being replaced. It can reduce the disruption caused by replacement, but may significantly extend the time to complete the upgrade (especially if Strategy is Task Reset)

  – Strategy - Reset strategy to control how many tasks are replaced at a time: Card Reset, TOS Reset, Task Reset
- **last-activation-result** - Report on the progress of last upgrade
- **firmwareupgrade** - Upgrade firmware for all FRUs associated with the specified card slot.
- **releasemodifier** - Change the release modifier version (for example, of a DPI signature analysis definitions file) applied to the current release version.

  Inputs:

  – Version - Version to apply to the current release

  – Rollback - Modifier type to which to toggle back to the last version (from Release Modifier Status).

  – Original - Modifier type to which to revert back to the original version (from Release Modifier Status)

3 Click **Execute**.

For more details on image management commands, see Online Software Upgrade.

Online Software Upgrade

The system supports online software upgrade, which moves the software image to the new release while the NE continues to provide service.

Note: *Prior to performing the upgrade, contact the TAC to verify the supported upgrade paths.*

Online software upgrade automatically selects a least-impact reset strategy based on the difference between the current and the new release:

- **Card Reset**: If the kernel/rootfs dependencies have changed, the system performs a card reset to update the kernel/rootfs.
- **Task Reset**: If only one or more task's dependencies have changed, the system restarts only those tasks. The other tasks are rebased.
- **TOS Reset**: If a task's dependencies are unchanged, the task is notified to use the new release's directory without being restarted.

Prerequisites

Prior to performing the upgrade, verify the following conditions are met:

- Node must be redundant
- Node must be fully up (all tasks Operationally up)
- Data model of the new release must be identical or a superset of the current release

prepare Command

The optional **prepare** command prepares the node for upgrade. Affirmed Networks recommends preparing a release outside of a maintenance window. It involves two steps:

- *Preparing for the upgrade* – Open the image files and copy them to the system.
- *Performing the upgrade* – Perform the upgrade steps to trigger the upgrade. The node reboots after the upgrade completes.

To prepare for upgrade:

1. Copy the release file (an-<*version*>.tgz) to /public/images.
2. Click **Image Management** in the tree.

3 To perform the prepare:

   a Under **Image Management Commands**, select **prepare**.

   b Click **Select**.

   c Enter the version.

   d To specify that the operation wait to complete until both MCMs have caught up (rather than wait for all cards to catch up), mark the **Force** checkbox.

   e Click **Execute**.

4 To observe the prepare progress:

   a Under **Image Management Commands**, select **progress**.

   b Click **Select**.

   c Click **Execute**.

5 To check the progress of the completed or failed prepare:

   a Under **Image Management Commands**, select **last-activation-result**.

   b Click **Select**.

   c Click **Execute**.

6 To list the prepared version:

   a Expand **Image Management** > **Status**.

   b Click an instance.

```
                                        OPERATIONAL      ACTIVATION  ROLLBACK
STATE    ID  SLOT  CPU  ADMIN VERSION    VERSION          STATUS      VERSION          PREPARED VERSION
-------------------------------------------------------------------------------------------------------
active   21  8     1    3.1.2.0-138.REL  3.1.2.0-138.REL  Idle        3.1.2.0-107.REL  3.1.2.1-138.REL.ENG
```

onlineupgrade Command

The **onlineupgrade** command moves the software image to the new release.

To perform the online upgrade:

1 Copy the release file (an-<*version*>.tgz) to /public/images.

2 Click **Image Management** in the tree.

3 To perform the upgrade:

   a Under **Image Management Commands**, select **onlineupgrade**.

   b Click **Select**.

   c Specify the following inputs.

   – Version - Version to upgrade to

- Drain - Drain timeout in seconds. Allows tasks to drain of work before being replaced. It can reduce the disruption caused by replacement, but may significantly extend the time to complete the upgrade (especially if Strategy is Task Reset)
- Strategy - Reset strategy to control how many tasks are replaced at a time: Card Reset, TOS Reset, Task Reset
- Continue on payload timeout - Continue the upgrade even when payload nodes fail to fully reach Oper State up. Use this option to enable the OSU to continue even if a TOS task hangs during a payload OSU. If a task hang occurs, the OSU continues but service is impacted.

d Click **Execute**.

4 To observe the upgrade progress:

a Under **Image Management Commands**, select **progress**.

b Click **Select**.

c Click **Execute**.

5 To check the progress of the completed or failed upgrade:

a Under **Image Management Commands**, select **last-activation-result**.

b Click **Select**.

c Click **Execute**.

6 To list the new version in the Admin Version and Operational Version columns and the rollback version in the Rollback Version column:

a Expand **Image Management** > **Status**.

b Click an instance.

```
                                        OPERATIONAL      ACTIVATION  ROLLBACK
STATE    ID  SLOT  CPU  ADMIN VERSION    VERSION          STATUS      VERSION          PREPARED VERSION
-------------------------------------------------------------------------------------------------------
active   21  8     1    3.1.2.0-138.REL  3.1.2.0-138.REL  Idle        3.1.2.0-107.REL  3.1.2.1-138.REL.ENG
```

As an alternative, to list the new release in the Release column:

a Expand **Cluster** in the tree.

b Expand the cluster instance.

c Click **Summary**.

```
    SLOT    CPU                        ADMIN    HA       CPU
ID  NUMBER  NUMBER  TYPE  MODEL        STATE    STATE    STATE  CPU UPTIME            RELEASE
-------------------------------------------------------------------------------------------------------
13  1       1       csm   XE60         enabled  active   up     D:000 H:01 M:49 S:29  3.0.0.0-283.REL
    5       1       ssm   PP81         enabled  active   up     D:000 H:01 M:48 S:34  3.0.0.0-283.REL
    5       2       ssm   PP81         enabled  active   up     D:000 H:01 M:48 S:34  3.0.0.0-283.REL
    7       1       mcm   FM40-COM-EXP enabled  active   up     D:000 H:01 M:53 S:00  3.0.0.0-283.REL
    8       1       mcm   FM40-COM-EXP enabled  standby  up     D:000 H:01 M:52 S:27  3.0.0.0-283.REL
    10      1       ssm   PP81         enabled  active   up     D:000 H:01 M:49 S:26  3.0.0.0-283.REL
    10      2       ssm   PP81         enabled  active   up     D:000 H:01 M:49 S:34  3.0.0.0-283.REL
    12      1       csm   XE60         enabled  active   up     D:000 H:01 M:48 S:46  3.0.0.0-283.REL
```

Failed Online Upgrade

If **Image Management** > **Status** lists Activation Status Failed, you can recover from the failure.

```
                                      OPERATIONAL      ACTIVATION  ROLLBACK
STATE    ID  SLOT  CPU  ADMIN VERSION  VERSION          STATUS      VERSION          PREPARED VERSION
-------------------------------------------------------------------------------------------------------
active   21  8     1    3.1.2.0-138.REL  3.1.2.0-138.REL  Failed      3.1.2.0-107.REL  3.1.2.1-138.REL.ENG
```

If the failure occurred during validation, the Prepared Version column lists the new release. If the failure occurred post-validation, the Rollback Version column lists the previous release.

To recover the failure:

1. To reset the upgrade engine:
   a. Under **Image Management Commands**, select **reset**.
   b. Click **Select**.
   c. Click **Execute**.
2. In the case of a post-validation failure, perform a rollback to restore the system to the original state:
   a. Under **Image Management Commands**, select **rollback**.
   b. Click **Select**.
   c. To specify that the operation wait to complete until both MCMs have caught up (rather than wait for all cards to catch up), mark the **Force** checkbox.
   d. Click **Execute**.

rollback Command

The **`rollback`** command returns the NE to the previous release and configuration:

- If the last operation was an upgrade, rollback activates the previous release and reboots the node.
- If the last operation was a successful online upgrade, rollback activates the previous release and reboots the node.
- If the last operation was a failed online upgrade, rollback activates the original release and reboots the node.

To perform the rollback:

1. To perform a rollback to restore the system to the original state:
   a. Under **Image Management Commands**, select **rollback**.
   b. Click **Select**.
   c. To specify that the operation wait to complete until both MCMs have caught up (rather than wait for all cards to catch up), mark the **Force** checkbox.
   d. Click **Execute**.
2. To observe the rollback progress:
   a. Under **Image Management Commands**, select **progress**.
   b. Click **Select**.
   c. Click **Execute**.
3. Enter the following command to check the progress of the completed or failed rollback:
   a. Under **Image Management Commands**, select **last-activation-result**.
   b. Click **Select**.
   c. Click **Execute**.

releasemodifier Command

The **releasemodifier** command changes the release modifier version (for example, of a DPI signature analysis definitions file) applied to the current release version.

You can:

- Specify a modifier image version to apply to the current release
- Toggle to the last modifier image version (listed as Rollback Version in **Release Modifier Status**)
- Revert to the original modifier image (listed as Original Version in **Release Modifier Status**)

To perform the release modifier:

1. Copy the modifier image file (sig-<*date*>.tgz) to /public/images.
2. Click **Image Management** in the tree.
3. Under **Image Management Commands**, select **releasemodifier**.
4. Click **Select**.
5. Specify the change:
   - To specify a modifier image version to apply to the current release, enter it in **Version**.
   - To toggle to the last modifier image version, select the modifier type in **Rollback**.
   - To revert to the original modifier image version, select the modifier type in **Original**.
6. Click **Execute**.

Card Status

Use this object to view real-time image management status of each card.

To view image management card status:

1. Expand **Image Management** in the tree.
2. Expand **Card Status**.
3. Click an instance.

Table 10-13 Image Management Card Status Parameters

Parameter	Description
ID	Cluster ID
Slot	Card slot
CPU	CPU number
State	Card State: ■ expected ■ actual
Exp Seq	Expected sequence number
MAS Seq	Master sequence number
Rollback RFS	Version of the Rollback Root Filesystem
Rollback TOS	Version of the Rollback TOS
Operational RFS	Version of the Operational Root Filesystem
Operational TOS	Version of the Operational TOS
Prepared RFS	Version of the Prepared Root Filesystem
Prepared TOS	Version of the Prepared TOS
Next Boot RFS	Version of the Next Boot Root Filesystem
Agent Status	Agent Status: ■ working ■ waiting ■ retry ■ done ■ error
Comment	Comment on activity

Release Modifier Status

Use this object to view current modifier status.

To view image management release modifier status:

1. Expand **Image Management** in the tree.
2. Expand **Release Modifier Status**.
3. Click an instance.

Table 10-14 Image Management Release Modifier Status Parameters

Parameter	Description
Release Role	Release role: ■ Rollback ■ Operational ■ Prepared
Release Version	Card release version
Release Modifier	Release modifier type
Operational Version	Release modifier version currently running.
Rollback Version	Release modifier version available for rollback
Original Version	Release modifier version shipped with this release version

Status

Use this object to view image management status of the active MCM.

To view image management status:

1. Expand **Image Management** in the tree.
2. Expand **Status**.
3. Click an instance.

Table 10-15 Image Management Status Parameters

Parameter	Description
State	Card State: ■ active
ID	Cluster ID
Slot	Card slot
CPU	CPU number

Table 10-15 Image Management Status Parameters

Parameter	Description
Admin Version	Current upgrade admin version
Operational Version	Version currently running.
Activation Status	Activation Status: ■ Idle ■ Succeeded ■ Failed ■ Prepare in Progress ■ Upgrade in Progress ■ Online Upgrade in Progress ■ TOS Upgrade in Progress ■ Rollback in Progress ■ Firmware Upgrade in Progress ■ Release Modifier Upgrade in Progress ■ Release Modifier Rollback in Progress ■ Release Modifier Revert to Original in Progress
Rollback Version	Version available for rollback
Prepared Version	Version shipped with this release version

Infrastructure

Use this object to configure infrastructure.

Dynamic Scale

Note: *It is recommended that you use the VNF Manager application to configure dynamic scaling. For instructions, see Configuring Dynamic Scale Out/Scale In.*

Use this object to configure dynamic scaling.

To configure dynamic scaling:

1. Expand **Infrastructure** in the tree.
2. Expand **Dynamic Scale**.
3. Configure the parameters as follows:

Table 10-16 Dynamic Scale Parameters

Object	Parameter	Description
Advanced Services Module (ASM)	Node Connection Capacity	Configure per ASM node connection limit.
	Node Throughput Capacity	Configure per ASM node throughput (in MB) limit.
	Disk Size	Configure per ASM node disk size in GB.
Distributed Control Module (DCM)	Node Session Capacity	Configure per DCM node session limit
Workflow Services Module (WSM)	Node Session Capacity	Configure per WSM node session limit

4. Click the **Save** icon.

EDR

Use this option to view Event Data Record statistics.

To view EDR statistics:

1. Expand **Infrastructure** in the tree.
2. Expand **EDR**.
3. Expand the record type:
   - EDR Bearer Statistics
   - EDR Flow Statistics
   - EDR HTTP Statistics
   - EDR Server Statistics
   - EDR Session Statistics
4. Click an instance.

Export IP

Use this object to specify a separate Network Context Loopback IP to enable export users associated with an export SSH group to access export files, such as Charging Data Records (CDR), without having to connect through the standard management-context, mgmt-ip address.

You can enable/disable the Network Context to act as a Secure Copy Protocol (SCP) or SFTP login port. Connections are made through the Loopback IP address on the north/south subnet using port 2221 (Note: Some export transfers may experience lower performance rates using this port).

Only those users specified in the export ssh group are allowed connections on port 2221. Use the Infrastructure > File Management Profile object to configure the Export Rule and Export User parameters to allow users access to the export interface. See File Management.

Depending on the Loopback IP address you choose for the export-ip Network Context, you may need to create a default route on the client machine to forward traffic intended for the Loopback IP to the Network Context's *Interface IP* address. The system will recognize this address as the correct route.

To configure an export IP:

1. Expand **Infrastructure** in the tree.
2. Expand **Export IP**.
3. Click **Mgmtip**.

Mgmtip parameters are listed in the following table:

Table 10-17 Mgmt Ip Parameters

Parameter	Description
Network Context	Name of a Network Context provisioned on the MCC.
Loopback IP	Name of the loopback IP address to be used for export SCP/SFTP.

4 Click the **Save** icon.

File Management

Use this object to configure a Data File Management profile for file upload and purging.

Use the following Profile Commands to trigger transferring and rotating the file:

- trigger_file_rotate – Trigger file rotate for this profile, that is close current file and open a new one
- trigger_file_transfer – Trigger file transfer for this profile

Use Case: Storing Gz/Rf SGW CDRs to a File in the Event of a Failure

You can configure a Data File Management profile to create a local file in which to store Gz/Rf SGW CDRs in the event of a failure (when the remote server is unavailable). For details on this configuration, see *Storing Gz/Rf SGW CDRs to a File in the Event of a Failure* in the *Affirmed Networks Charging Data Records Specification*.

To configure a data file management profile:

1 Expand **Infrastructure** in the tree.

2 Expand **File Management**.

3 Click **Profile**.

Data File Management profile parameters are listed in the following table:

Table 10-18 Data File Management Profile Parameters

Parameter	Description
Type	File type: ■ Event Log ■ Data Record ■ Other ■ Core Files ■ RAM DataRecord ■ RAM Disk-Storage ■ Storage ■ Ext-Storage ■ PSM ■ Tech-Support ■ Gz-Record ■ Gy-Record
Prefix	Filename Prefix
Export Rule	Specifies the rules to apply when exporting file to ./export directory: ■ exportrule-default – The system exports files to the */public/logs/datarecord.lnk/gz/export* directory and applies purge rules for this file profile to all files in the directory. ■ exportrule-gy-custom1 – The system exports files to the */public/logs/datarecord.lnk/gy/export/AP_primary* directory according to the custom1 format configured for CCR-T records ■ exportrule-gz-custom1 – The system exports files to the */public/logs/datarecord.lnk/gz/export* directory according to the custom1 format configured for Gz/Rf SGW/PGW CDRs. ■ exportrule-none – Specifies that there is no export rule for this file profile. In this case, the MCC sends (pushes) the files to the remote SFTP server based on the upload parameters configured for the file profile.
Export User	Specifies the user that has read/write access to the files in the */public/logs/datarecord.lnk/gz/export* directory.
Purge Thr	Percentage utilization at which to transfer/purge files.
Purge Low Thr	Percentage utilization at which to stop transferring/purging files.
File Rotate Size Bytes	Size (in bytes) at which files should be rotated.
File Rotate Num Records	Number of records at which to rotate the files.
File Transfer Enabled	File transfer: ■ Enabled ■ Disabled

Table 10-18 Data File Management Profile Parameters

Parameter	Description
Dest URL	URL/IP Address for the file sftp server
Dest Port	Port of the file sftp server
Username	Username to log into the file sftp server
Password	Password to log into the file sftp server
Upload Dir Path	Path on the sftp server to which to upload the files.
Upload Frequency	Frequency to upload files: ■ 1 minutes ■ 5 minutes ■ 15 minutes ■ 30 minutes ■ 1 hour ■ 2 hours ■ 3 hours ■ 6 hours ■ 12 hours ■ 1 day ■ 7 days ■ 14 days ■ 21 days ■ 30 days ■ 1 year
Upload Offset Secs	Adds this offset in seconds.

Table 10-18 Data File Management Profile Parameters

Parameter	Description
File Rotate Frequency	Frequency to rotate files: ■ 1 minutes ■ 5 minutes ■ 15 minutes ■ 30 minutes ■ 1 hour ■ 2 hours ■ 3 hours ■ 6 hours ■ 12 hours ■ 1 day ■ 7 days ■ 14 days ■ 21 days ■ 30 days ■ 1 year The file is rotated at this specified amount of time only if the current file has not reached the configured size (File Rotate Size Bytes) or configured number of records (File Rotate Num Records) within that time. For example, if this parameter is set to 1 hour and within that hour, the file reaches the maximum number of records, the file is rotated immediately and *is not* rotated upon reaching the 1-hour time interval.
File Rotate Empty	Specifies to rotate the files when empty: ■ enabled – Empty CDR/HTDR files are rotated based on the configured File Rotate Frequency interval. ■ disabled – Empty CDR/HTDR files are not rotated.

Table 10-18 Data File Management Profile Parameters

Parameter	Description
Purge File Older Than	Purge file older than: ■ 1 minutes ■ 5 minutes ■ 15 minutes ■ 30 minutes ■ 1 hour ■ 2 hours ■ 3 hours ■ 6 hours ■ 12 hours ■ 1 day ■ 7 days ■ 14 days ■ 21 days ■ 30 days ■ 1 year
Purge Enabled	Enable/disable purge/cleanup for this file: ■ enabled ■ disabled
Compress Enabled	Specifies whether to compress (zip) the file when it is closed: ■ enabled ■ disabled Compressed data recored files are stored in */public/logs/datarecord.lnk*. Compressed event logs are stored in */var/log/eventlog*.
Compress Format	For data records, specifies the format to compress the file: ■ *gzip* – (default) The data records are written to a file. After the file is closed, it is gzipped. ■ *raw* – The data records are written in zlib raw format. The zlib raw format provides better performance compared the gzip format because the records are compressed on the source before sending them to the agent for writing. Affirmed Networks recommends using the zlib raw format if you expect the system to generate data records at a rate higher than 10K data records per second.

Table 10-18 Data File Management Profile Parameters

Parameter	Description
Sequence Field Width	To facilitate file retrieval and processing, the MCC automatically appends a sequence number to the filename to indicate which file it is. This setting specifies the width of the sequence number appended to filenames, for files such as CDR, HTDR, and event log files. The width dictates the number of leading zeros to prepend to the filename sequence number. For example, when the Sequence Field Width is set to 7, a three-digit sequence number would be prepended with four zeros: pgwcdr20161114163821_0000123.csv
File Name Format	Customizes the file naming convention for local CDRs (ASN.1 only). *Applies only to the datarecord profile:* ■ default – The MCC uses the default file naming convention for local CDR files: <filename-prefix><YYYYMMDDHHMMSS>_<123>.csv ■ custom1 – The MCC uses the following custom file naming convention for local CDR files (ASN.1 only): `<filename-prefix>_MM_DD_YYYY_hh_mm_ss_<#records>_file<123>.u` where – `filename-prefix` – Indicates the prefix of the filename in which to store CDRs. – `MM_DD_YYYY_hh_mm_ss` – Represents the timestamp. – `#records` – Represents the number of records stored in the file, starting with 0. – `123` – Represents the file sequence number. The number of leading zeros prepended to the file sequence number depends on the value configured for the `sequence-field-width`. For example, if the `sequence-field-width` is set to 6, the sequence number will start with 000001. ***Note:*** *In the rare case of an uncontrolled MCM switchover caused by a crash in the DataRecordAgentMCM process or an MCM kernel crash, the currently open CDR files will remain with a record count of 0, indicating that the number of records could not be determined when the file was closed.*
Private Information	For gz-records, specifies optional private information appended to the filename.
File Extension	For gz-records, specifies the optional file-extension appended to the filename.

4 Click the **Save** icon.

Event Logging

Use this object to configure event log parameters.

Note: *The clocks on the CSM30s synchronize with the clock on the MCM20 using the SNTP protocol. It may take several hours for the clocks to synchronize to sub-millisecond granularity. Until synchronization occurs, the protocol logs coming from different CSM30s may appear to be out of order.*

Sample Use Case

MCC logs any configuration changes made to the system. By default, these CLI audit logs are captured to a log file located on the system's disk. Operators can configure the system to stream the CLI audit logs to a remote syslog server, using the following steps:

1. Configure a log policy to capture only the CLI audit logs to the system's syslog facility.
2. Set the sink type to `printf` so that the log is written out to the */var/log/messages* (that is, syslog) file.
3. Configure the syslog facility to stream the logs to a remote server.

   The following is a sample log policy for this use case.

   Note: Two filters (`component` = `Nml` and `componentlogid` = `9`) are required to log only the executed CLI commands.

   Infrastructure > Logging > Event Log > Policy:

   Name

   Log Type: Debug

   Filter Field: Component

   Filter Value Value: Nml

   Filter Value Exclude: False

   Filter Field: Component Log ID

   Filter Value Value: 9

   Filter Value Exclude: False

   Sinks: Name

   Sinks Type: printf

To configure event log parameters:

1 Expand **Infrastructure** in the tree.

2 Expand **Logging**.

3 Expand **Event Log**.

4 Click **Policy**.

Event Log Policy parameters are listed in the following table:

Table 10-19 Event Log Policy Parameters

Parameter	Description
Name	Log name
Admin State	Enable/Disable the policy: ■ enabled ■ disabled
Log Type	Log type to collect for this policy: ■ debug: captures various events in the system ■ protocol: captures control and data packets ■ record-debug ■ record-protocol

5 Click the **Save** icon.

Event Log Policy child objects and their parameters are listed in the following table:

Table 10-20 Event Log Policy Child Objects and Parameters

Object	Parameter	Description
Filter Field	Filter Field	Field on which to filter: ■ APN ■ Component ■ Component Log ID ■ CPU ■ GW Name ■ HTTP Request Type ■ IMEI ■ IMSI ■ IP Address ■ MAC Address ■ MSISDN ■ NAI ■ NPU Flow ID ■ NPU Number ■ NPU Slot ■ Port Number ■ Service ■ Severity ■ Slot ■ TE ID ■ VPN

Table 10-20 Event Log Policy Child Objects and Parameters

Object	Parameter	Description
Filter Value	Value	String value based on the Filter Field
	Exclude	Specifies whether to exclude logs with the filter value: ■ false ■ true
Protocol Logging Filter Field *(Applies when Event Log Type is set to protocol or record-protocol)*	Filter Field	Field on which to filter: ■ Destination IP Address ■ Destination Port Number ■ IMEI ■ IMSI ■ IP Address Pair ■ IP Protocol ■ IP Address ■ MSISDN ■ Packet Direction ■ Packet Type ■ Protocol ■ Source IP Address ■ Source Port Number
Filter Value	Value	String value based on the Filter Field
	Exclude	Specifies whether to exclude logs with the filter value: ■ false ■ true
Interface *(Applies when Event Log Type is set to protocol or record-protocol and Filter Value is set to a particular protocol)*	Value	Interface to use
	Exclude	Specifies whether to exclude logs with the filter value: ■ false ■ true

Table 10-20 Event Log Policy Child Objects and Parameters

Object	Parameter	Description
Sinks *(Each sink must refer to a unique Infrastructure > File Management > Profile > Prefix. The prefix must be unique across all Event Log policies.)*	Name	Sink Name
	Type	Sink Type: ■ Printft ■ File
	File Name	File Name: ■ * ■ Critical ■ TOS ■ /var/log/psm/*
	File Format	File Format: ■ ASCII ■ Binary ■ PCAP ■ PCAPNG

Viewing Protocol Logs with Packet Analyzers

MCC performs protocol logging using application software that receives only Application Layer Packets (not Layer3 or Layer4 packet header information). To view Protocol Logs with packet analyzers, it is recommended that you configure the analyzer to ignore Layer3 and Layer4 header fields, otherwise the tool may incorrectly analyze those layers.

For example, to do so in Wireshark:

1. Select **Edit** > **Preferences** > **Protocol**.
2. Select an individual protocol, such as TCP.
3. Unmark the checkbox that specifies to analyze that data.
4. Click **Apply**.
5. Repeat step 2 through step 4 for the other protocols.

System Logging

Use this object to stream system logs to a remote logging server or multiple remote logging servers. System logs contain messages from the Linux subsystem, kernel, and other services/daemons running on the system. System logs are stored in */var/log/messages**.

To configure system log parameters:

1. Expand **Infrastructure** in the tree.
2. Expand **Logging**.
3. Expand **Sys Log**.
4. To allow tagging of syslog messages between the timestamp and hostname fields, you can assign a mnemonic string to help identify the VM and cluster to determine the origin of the messages.
   a. To do so, click **Hostname Prefix**.
   b. Configure the parameters as follows:
      – **Prefix** – Enter the string used to tag syslog entries.
   c. Click the **Save** icon.
5. Click **Stream Server**.

   Stream server parameters are listed in the following table:

Table 10-21 System Log Policy Parameters

Parameter	Description
IP	Remote server IP address
Port	Remote server port
Protocol	Protocol: ■ TCP ■ UDP

6. Click the **Save** icon.

NTP Server

Use this object to configure an NTP server.

To configure an NTP server:

1. Expand **Infrastructure** in the tree.
2. Expand **NTP Server**.
3. Specify IPv4 or IPv6 server:
   a. For an IPv4 server, click **IPv4**.
   b. For an IPv6 server, click **IPv6**.
4. Configure the parameters as follows:
   - **IP** – Enter the NTP server IP Address.
5. Click the **Save** icon.

Status

Use this object to view status of NTP peers. Note that the list may truncate the display of long IPv6 addresses.

To view NTP status:

1. Expand **Infrastructure** in the tree.
2. Expand **NTP Server**.
3. Expand **Status**.
4. Click an NTP peer.

LED status parameters are:

- Remote: Peer specified in the NTP configuration
- Sync: Time source sync status
- Ref ID: remote source's synchronization source
- St: stratum level of the source
- T: type
- When: Number of seconds passed since last response
- Poll: Polling interval for source, in seconds
- Reach: Success or failure to reach source (377 indicates all attempts were successful)
- Delay: Roundtrip time to receive a reply, in seconds
- Offset: Time difference between the client server and source, in milliseconds
- Jitter: Time difference between the client server and source, in milliseconds

OOM

Use this object to configure TOS Cgroup Out of Memory functionality.

To configure OOM:

1. Expand **Infrastructure** in the tree.
2. Click **OOM**.
3. Configure the parameters as follows:

Table 10-22 OOM Parameters

Parameter	Description
Admin	Enable or Disable TOS Cgroup OOM killer: ■ enabled ■ disabled
Faults	Enable or Disable fault-images when process is killed by TOS OOM killer: ■ enabled ■ disabled
Memory Profile	Enable/Disable capture of memory-profile when memory overload is hit: ■ enabled ■ disabled

4. Click the **Save** icon.
5. To configure the memory limit for TOS Cgroup (percentage of the total RAM available for Linux applications), expand **OOM**.
6. Click **TOS Cgroup Mem Limit**.

7 Configure the parameters as follows:

Table 10-23 Memory Limit Parameters

Parameter	Description
Personality	Node Personality: ■ ASM: Advanced Services Module ■ CCM: Centralized Control Module ■ CPM: Control Plane Module ■ CSM: Control/Content Services Module ■ DCM: Distributed Control Module ■ IOM: I/O Module ■ MCM: Management Control Module ■ SSM: Subscriber Services Module ■ WSM: Workflow Services Module The personalities available are filtered based on the Building Block Strategy specified for the cluster. For more information on personalities, see Node Personalities.
Memory Limit	Memory limit: percentage of the total RAM available for Linux applications

8 Click the **Save** icon.

To view all recovery action taken for an event:

1 Expand **Fault Management** in the tree.

2 Click **History**.

Peer Overload Control

Use this object to configure Peer Overload Control, which detects overload on peer servers and any potential network issues on the access network to peer servers. Specifically, this feature detects any potential transient failure condition by reducing the message load on the peer interface. After the peer link recovers, the system increases the messaging rate to its original rate. This feature also detects overload on peer servers by enforcing a maximum messaging rate.

Profile

Use this option to configure the pacer. The pacer lowers the rate of requests being made to the peer under overload conditions and supports priority levels of messages/requests. The pacer also enables the display of statistics for overload conditions and success/drop counts. The pacer issues an alarms when it is in an overload state and clears the alarm when the overload state resolves.

To configure the profile:

1. Expand **Infrastructure** in the tree.
2. Expand **Peer Overload Control**.
3. Click **Profile**.
4. Configure the parameters as follows:

Table 10-24 Profile Parameters

Parameter	Description
Max Supported	Maximum number of requests the peer can handle per second.
Failure Rate	The rate the pacer used to determine whether it should increase or decrease its next intervals outgoing rate. For example, if the failure-rate value is set to 20%, the pacer determines the failure rate for the last interval as follows: ■ If the failure rate is > 20%, the pacer reduces the outgoing request for the next upcoming interval. ■ If the failure rate is <20%, the pacer increases the outgoing request for the next upcoming interval.
Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5).
Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (5).
High Priority Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5) for high-priority messages.
High Priority Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (10) for high-priority messages.

Table 10-24 Profile Parameters

Parameter	Description
Medium Priority Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5) for medium-priority messages.
Medium Priority Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (10) for medium-priority messages.
Low Priority Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5) for low-priority messages.
Low Priority Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (10) for low-priority messages.
Time Interval	The length of each interval in milliseconds. At the end of the interval, the pacer adjusts its outgoing rates.

5 Click the **Save** icon.

Configuration

Use this option to view pacer configuration.

To view pacer configuration:

1 Expand **Infrastructure** in the tree.

2 Expand **Peer Overload Control**.

3 Expand **Configuration**.

4 Click a pacer instance.

5 The pacer parameters as follows:

Table 10-25 Pacer Parameters

Parameter	Description
Max Supported	Maximum number of requests the peer can handle per second.
Failure Rate	The rate the pacer used to determine whether it should increase or decrease its next intervals outgoing rate. For example, if the failure-rate value is set to 20%, the pacer determines the failure rate for the last interval as follows: ■ If the failure rate is > 20%, the pacer reduces the outgoing request for the next upcoming interval. ■ If the failure rate is <20%, the pacer increases the outgoing request for the next upcoming interval.

Table 10-25 Pacer Parameters

Parameter	Description
Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5).
Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (5).
High Priority Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5) for high-priority messages.
High Priority Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (10) for high-priority messages.
Medium Priority Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5) for medium-priority messages.
Medium Priority Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (10) for medium-priority messages.
Low Priority Increment Rate	When the pacer is increasing the outgoing request rate, it increments the rate based on a value between 0 ..100 (5) for low-priority messages.
Low Priority Decrement Rate	When the pacer is decreasing the outgoing request rate, it decrements the rate based on a value between 0 ..100 (10) for low-priority messages.
Time Interval	The length of each interval in milliseconds. At the end of the interval, the pacer adjusts its outgoing rates.

Counters Detail

Use this option to view pacer counters detail statistics.

To view counters detail statistics:

1. Expand **Infrastructure** in the tree.
2. Expand **Peer Overload Control**.
3. Expand **Counters Detail**.
4. Click a pacer instance.

   Pacer counters detail statistics are:

   - highcredits
   - highfailures
   - highrejects

- highsuccesses
- lowcredits
- lowfailures
- lowrejects
- lowsuccesses
- mediumcredits
- mediumfailures
- mediumrejects
- mediumsuccesses

Counters Detail Cumulative

Use this option to view pacer counters detail cumulative statistics.

To view counters detail cumulative statistics:

1. Expand **Infrastructure** in the tree.
2. Expand **Peer Overload Control**.
3. Click **Counters Detail Cumulative**.

Pacer counters detail cumulative statistics are:

- highcredits
- highfailures
- highrejects
- highsuccesses
- lowcredits
- lowfailures
- lowrejects
- lowsuccesses
- mediumcredits
- mediumfailures
- mediumrejects
- mediumsuccesses

Counters Summary

Use this option to view pacer counters summary statistics.

To view counters summary statistics:

1. Expand **Infrastructure** in the tree.
2. Expand **Peer Overload Control**.
3. Click **Counters Summary**.

Pacer counters detail cumulative statistics are:

- credits
- failurerate
- failures
- rejects
- successes

Counters Summary Cumulative

Use this option to view pacer counters summary cumulative statistics.

To view counters summary cumulative statistics:

1. Expand **Infrastructure** in the tree.
2. Expand **Peer Overload Control**.
3. Click **Counters Summary Cumulative**.

Pacer counters summary cumulative statistics are:

- credits
- failures
- rejects
- successes

Pacer Rates

Use this option to view pacer rate statistics.

To view counters rate statistics:

1. Expand **Infrastructure** in the tree.
2. Expand **Peer Overload Control**.
3. Click **Rates**.

Pacer rate statistics are:

- highrate

- lowrate
- mediumrate
- rate

Time Zone

To configure time zone:

1. Expand **Infrastructure** in the tree.
2. Click **Time Zone**.
3. Configure the parameters as follows:
   - **Zone** – Enter the system time zone.
4. Click the **Save** icon.

IP Protocols

Use this object to manage IP network protocols.

BFD

The Bidirectional Forwarding Detection (BFD) network protocol is used to detect forwarding path failures between two peer routers. BFD peers are not required to be directly connected. BFD provides a low-overhead fault detection mechanism for all media types, encapsulations, topologies, and routing protocols.

In networks that deploy L2/L3 switches, link status is not always indicative to the health of the forwarding plane between two peers. Unlike BGP, static routes have no mechanism to detect a failed next-hop that is connected to an L2/L3 switch, thereby creating a situation where traffic is routed to a next-hop that is no longer available. To avoid this situation, Operators can utilize BFD for static routes. BFD can create sessions for all static routes that use a particular interface, or BFD can be configured for an individual static route.

To configure BFD parameters:

1. Expand **IP Protocols** in the tree.
2. Expand **BFD**.
3. To configure a BFD timer profile, click **BFD Timer Profile**.
4. Configure the parameters as follows:

Table 10-26 BFD Timer Profile Parameters

Parameter	Description
Name	Timer profile name
Tx Interval	Transmit interval in milliseconds
Rx Interval	Minimum receive interval in milliseconds
Multiplier	The multiplier value to use to determine how long to hold a hello packet before declaring an adjacency down

5. Click the **Save** icon.
6. To configure and manage BFD session with a network context, click **Instance**.
7. Configure the parameters as follows:

Table 10-27 BFD Instance Parameters

Parameter	Description
Network Context	Network Context for this BFD instance

Table 10-27 BFD Instance Parameters

Parameter	Description
Slow Timer	Interval for the slow timer, in milliseconds
GTSM Admin State	Enable or disable BFD GTSM protection: ■ enabled ■ disabled
GTSM TTL	BFD GTSM time to live value
Echo Mode	Mark the checkbox to set BFD session to echo mode.

8 Click the **Save** icon.

BFD Instance child objects and their parameters are listed in the following table:

Table 10-28 BFD Instance Child Objects and Parameters

Object	Parameter	Description
All Sessions Summary		Lists BFD sessions summary
BFD Auth Profile	Name	BFD Auth Profile name
	Auth Type	Authentication type: ■ simple ■ keyed MD5 ■ meticulous keyed MD5 ■ keyed SHA1 ■ meticulous keyed SHA1
	Key Chain	The associated key chain.
BFD Interface	BFD interface	Select the name of the IP interface
	Enable All Static	Mark the checkbox to enable BFD sessions for all IPv4/IPv6 static routes on this interfaces
	Echo Interval	BFD echo-mode interval
	BFD Timer Profile	Select the BFD Timer Profile
	BFD Auth Profile	Select the BFD Auth Profile
BFD Multihop Peer	BFD Peer Address	IP address of the peer
	BFD Timer Profile	Select the BFD Timer Profile
	BFD Auth Profile	Select the BFD Auth Profile

Table 10-28 BFD Instance Child Objects and Parameters

Object	Parameter	Description
BFD Static Route	BFD Route Dest	BFD Static Route Destination
	BFD Route Prefix	BFD Static Route Prefix
	BFD Route Next Hop	BFD Static Route Next Hop
	Admin State	Enable BFD for Static Route
Interfaces		Lists the BFD interface information
Key Chain	Name	Configure a chain of authentication keys (ID, key string)
Process Status		Lists the BFD instance
Session Details		Lists the BFD session details
Sessions		Lists the BFD session information

BGP Routers

To configure BGP router parameters:

1. Expand **IP Protocols** in the tree.
2. Expand **BGP**.
3. Click **Router**.
4. Configure the parameters as follows:

Table 10-29 BGP Router Parameters

Parameter	Description
Network Context	Network Context for this BGP router
Local AS	Autonomous System number for this BGP router
Router ID	Router ID <A.B.C.D>
Always Compare Med	Mark the checkbox to use MED in the path selection when comparing paths from different ASs.
Default Local Preference	Default local preference value
Extended ASN Cap	Mark the checkbox to enable 4-octet ASN support. Cannot be modified once the BGP router has been created.

5. Click the **Save** icon.

BGP router child objects and their parameters are listed in the following table:

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
Best Path	Compare Router ID	User Router ID in route selection
	Don't Compare Originator ID	Do not use Originator Id in route selection
	Don't Tie Break On Age	Do not use route selection in route selection
	AS Path Ignore	Do not use AS path in route selection
BGP Logging	All	Enable all logging
	Log Partial	Enable logging for specific areas.
BGP Timers	Keep Alive	Keep Alive timer for all peers, in seconds
	Hold Time	Hold timer for all peers, in seconds
Clear All		Clear all routes in all address families: ■ hard: Clear routes by resetting peerings ■ soft: Clear routes without resetting peerings
Graceful Restart	Fake Key	Enable fake key
	Restart Time	Restart time, in seconds.
	Stalepath Time	Stalepath time, in seconds.
IPv4 Unicast Address Family	Auto Summary	Mark the checkbox to automatically summarize IPv4 routes to classful boundaries.
IPv4 Unicast Address Family > Aggregate Address Configure a route aggregation policy. By default, the summarized routes will continue to be advertised and the summary route will have the atomic aggregate attribute.	Prefix	IPv4 prefix (A.B.C.D.)
	Prefix Length	Prefix length
	Summary Only	Mark the checkbox to suppress advertisement of the summarized routes.
	AS Set	Mark the checkbox to include the summarized routes in the summary route advertisement instead of the atomic aggregate attribute.
IPv4 Unicast Address Family > Clear		Clear dampening or flap-statistics
IPv4 Unicast Address Family > Dampening	Admin State	Admin state of dampening for this address family: ■ enable ■ disable

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
IPv4 Unicast Address Family > Dampening > R Dampening	Reachability Half Life	Reachability half life, in minutes. When a BGP route flaps, it is assigned a penalty. The penalty is decreased by half after each Reachability Half Life period.
	Reuse Limit	Reuse limit value. When the route flapping penalty decreases and falls below this reuse limit, the route is unsuppressed.
	Suppress Limit	Suppress limit value. A route is suppressed when its penalty exceeds this limit.
	Max Suppress Time	Maximum amount of time a route can be suppressed, in minutes.
	Unreachability Half Life	Unreachability half life for penalty, in minutes
IPv4 Unicast Address Family > Dampening Show	Dampening Show	Show detailed information about dampening.
IPv4 Unicast Address Family > Neighbor	Peering Name	Select the name of the IP interface
	Default Originate	Advertise the default route
	Soft Reconfiguration Inbound	Enable local storage of received updates. BGP soft-reconfiguration allows for the storage of incoming update information to RIB-IN for a specific peer. If configured, soft clearing occurs without tearing down the session. It is useful for re-evaluating the inbound policy on the same set of incoming updates.
	Next Hop Self	Set router as next-hop for all routes advertised to peer.
	Allowas In	Enables accepting route updates with the local AS number in the AS Path attribute. This attribute. is configurable per neighbor and address family. When MCC receives a BGP route update with the local AS in the AS Path attribute, it rejects the route. When Allowas In is configured for a neighbor, MCC accepts a route with its local AS in the AS Path attribute. The Allowas In configuration relaxes the AS Path loop check for BGP updates. The number of times our own AS Path is present in the update is also configurable per neighbor and address family.
IPv4 Unicast Address Family > Neighbor > Capabilities Configure the capabilities of this peering	Graceful Restart	Mark the checkbox to advertise support of graceful restart

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
IPv4 Unicast Address Family > Neighbor > Distribute List Apply access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Access List Type	Specify access list type: ■ standard access list ■ named access list
	Standard Access List/Named Access list	Specify the Standard Access List/Named Access list
IPv4 Unicast Address Family > Neighbor > Filter List Apply AS path access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	AS Path Access List	Select the name of the AS path access list
IPv4 Unicast Address Family > Neighbor > Maximum Prefix Configure the maximum number of prefixes accepted on this peering.	Max Value	Specify the maximum number of prefixes to be accepted on this peering. If the Max Value is reached, the peering is shut down and an error event is logged.
	Threshold	Specify the number of received prefixes to trigger “warning” events. Express as percentage of Max Value.
	Warning Only	Mark the checkbox to only log “error” message when the number of prefixes reaches Max Value and keep the peering active.
IPv4 Unicast Address Family > Neighbor > Prefix List Apply prefix list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Prefix List Name	Select the name of the prefix list
IPv4 Unicast Address Family > Neighbor > Route Map Apply route map filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Route Map Name	Select the name of the route map
IPv4 Unicast Address Family > Redistribute	Protocol	Protocol type to redistribute into BGP: ■ connected ■ static
	Route Map Tag	Name of the Route map to filter redistributed routes

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
IPv4 Unicast Address Family > Route Detail	Prefix	IPv4 prefix (A.B.C.D.)
	Prefix Length	Prefix length
IPv4 Unicast Address Family > Route Table	Entry	Lists the summary of IPv4 unicast route
IPv6 Unicast Address Family > Aggregate Address Configure a route aggregation policy. By default, the summarized routes will continue to be advertised and the summary route will have the atomic aggregate attribute.	Prefix	IPv6 prefix
	Prefix Length	Prefix length
	Summary Only	Mark the checkbox to suppress advertisement of the summarized routes.
	AS Set	Mark the checkbox to include the summarized routes in the summary route advertisement instead of the atomic aggregate attribute.
IPv6 Unicast Address Family > Clear		Clear dampening or flap-statistics
IPv6 Unicast Address Family > Dampening	Admin State	Admin state of dampening for this address family: ■ enable ■ disable
IPv6 Unicast Address Family > Dampening > R Dampening	Reachability Half Life	Reachability half life, in minutes. When a BGP route flaps, it is assigned a penalty. The penalty is decreased by half after each Reachability Half Life period.
	Reuse Limit	Reuse limit value. When the route flapping penalty decreases and falls below this reuse limit, the route is unsuppressed.
	Suppress Limit	Suppress limit value. A route is suppressed when its penalty exceeds this limit.
	Max Suppress Time	Maximum amount of time a route can be suppressed, in minutes.
	Unreachability Half Life	Unreachability half life for penalty, in minutes
IPv6 Unicast Address Family > Dampening Show	Dampening Show	Show detailed information about dampening.

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
IPv6 Unicast Address Family > Neighbor	Peering Name	Select the name of the IP interface
	Default Originate	Advertise the default route
	Soft Reconfiguration Inbound	Enable local storage of received updates. BGP soft-reconfiguration allows for the storage of incoming update information to RIB-IN for a specific peer. If configured, soft clearing occurs without tearing down the session. It is useful for re-evaluating the inbound policy on the same set of incoming updates.
	Next Hop Self	Set router as next-hop for all routes advertised to peer.
	Allowas In	Enables accepting route updates with the local AS number in the AS Path attribute. This attribute. is configurable per neighbor and address family. When MCC receives a BGP route update with the local AS in the AS Path attribute, it rejects the route. When Allowas In is configured for a neighbor, MCC accepts a route with its local AS in the AS Path attribute. The Allowas In configuration relaxes the AS Path loop check for BGP updates. The number of times our own AS Path is present in the update is also configurable per neighbor and address family.
IPv6 Unicast Address Family > Neighbor > Capabilities Configure the capabilities of this peering	Graceful Restart	Mark the checkbox to advertise support of graceful restart
IPv6 Unicast Address Family > Neighbor > Distribute List Apply access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Access List Type	Specify access list type: ■ standard access list ■ named access list
	Standard Access List/Named Access list	Specify the Standard Access List/Named Access list
IPv6 Unicast Address Family > Neighbor > Filter List Apply AS path access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	AS Path Access List	Select the name of the AS path access list

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
IPv6 Unicast Address Family > Neighbor > Maximum Prefix Configure the maximum number of prefixes accepted on this peering	Max Value	Specify the maximum number of prefixes to be accepted on this peering. If the Max Value is reached, the peering is shut down and an error event is logged.
	Threshold	Specify the number of received prefixes to trigger “warning” events. Express as percentage of Max Value.
	Warning Only	Mark the checkbox to only log “error” message when the number of prefixes reaches Max Value and keep the peering active.
IPv6 Unicast Address Family > Neighbor > Prefix List Apply prefix list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Prefix List Name	Select the name of the prefix list
IPv6 Unicast Address Family > Neighbor > Route Map Apply route map filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Route Map Name	Select the name of the route map
IPv6 Unicast Address Family > Redistribute	Protocol	Protocol type to redistribute into BGP: ■ connected ■ static
	Route Map Tag	Name of the Route map to filter redistributed routes
IPv6 Unicast Address Family > Route Detail		Show details of an IPv6 route. Specify route in format <prefix> <prefix-length>. For example, 3ffe:1234:5678::48
IPv6 Unicast Address Family > Route Table	Entry	Lists the summary of IPv6 unicast routes
Max Paths Configure equal-cost multi-path routing support	EBGP	Set the maximum number of EBGP ECMP routes allowed to a destination
	IBGP	Set the maximum number of IBGP ECMP routes allowed to a destination

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
Neighbor	Peering Name	Peering name
	Neighbor Addr	Neighbor IP address
	Remote AS	Autonomous system of remote neighbor. Cannot be modified once the neighbor has been created.
	Connection Retry Time	Time between attempts to connect to the peer, in seconds.
	Ebgp Multihop	Enable multi-hop EBGP peering and set the maximum time to live.
	Password	Enable MD5 authentication on peering and set the password. When the password contains blank characters, enclose the entire string in quotation marks.
	Fall Over BFD	Enable bi-derectional forwarding detection: ■ single-hop ■ multi-hop
	Local AS	Local autonomous system number for this peering. Both the router ASN and this ASN are prepended to Path Attributes advertised on this peering. ***Note:*** *The behavior of this setting is modified by the* Local AS No Prepend *setting.*
	Advertisement Interval	Minimum interval between routing updates sent on this peering. Set to 0 to send an update immediately after a routing change.
	Local AS No Prepend	When a Local AS value is set on this peering, setting this parameter prevents the router's ASN from being included in the path attributes for prefixes advertised by this peering. When a Local AS value is set on this peering, but this parameter is not set, both the router ASN and the peering ASN are prepended to the path attributes advertised on this peering. When a Local AS value is set on this peering and this parameter is set, only the peering ASN is prepended to path attributes advertised on this peering (the router ASN is suppressed. If Local AS is not configured for this peering, this parameter is ignored and only the router ASN is prepended to the path attributes advertised on this peering.
Neighbor > Capabilities	Route Refresh	Mark the checkbox to advertise support of route-refresh

Table 10-30 BGP Router Child Objects and Parameters

Object	Parameter	Description
Neighbor > Clear	Clear Command	Clear routes: ■ hard ■ soft
Neighbor > Detail	Entry	Lists summary of peering state.
Neighbor > Timers	Keep Alive	Keep Alive timer, in seconds
	Hold Time	Hold timer, in seconds
Neighbor > Update Source	Interface Selection	Specify the interface to act as the source of this peering session. You can configure multiple neighbors with the same remote address but you must configure a different Update Source address for each neighbor. MCC uses the Update Source address as the local address for the neighbor.
Policy		Lists the routing policies
Summary		Lists the BGP summary information

BGP VPN Routers

To configure BGP routing with VPN parameters:

1. Expand **IP Protocols** in the tree.
2. Expand **BGP VPN**.
3. Click **Router**.
4. Configure the parameters as follows:

Table 10-31 BGP VPN Router Parameters

Parameter	Description
Network Context	Network Context for this BGP router
Local AS	Autonomous System number for this BGP router
Router ID	Router ID <A.B.C.D>
Always Compare Med	Mark the checkbox to use MED in the path selection when comparing paths from different ASs.
Default Local Preference	Default local preference value

Table 10-31 BGP VPN Router Parameters

Parameter	Description
Extended ASN Cap	Mark the checkbox to enable 4-octet ASN support. Cannot be modified once the BGP router has been created.

5 Click the **Save** icon.

BGP VPN router child objects and their parameters are listed in the following table:

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
Best Path	Compare Router ID	User Router ID in route selection
	Don’t Compare Originator ID	Do not use Originator Id in route selection
	Don’t Tie Break On Age	Do not use route selection in route selection
	AS Path Ignore	Do not use AS path in route selection
BGP Logging	All	Enable all logging
	Log Partial	Enable logging for specific areas.
BGP Timers	Keep Alive	Keep Alive timer for all peers, in seconds
	Hold Time	Hold timer for all peers, in seconds
Clear > All	All Command	Clear all routes in all address families: ■ hard: Clear routes by resetting peerings ■ soft: Clear routes without resetting peerings
Graceful Restart	Fake Key	Enable fake key
	Restart Time	Restart time, in seconds.
	Stalepath Time	Stalepath time, in seconds.
IPv4 Unicast Address Family	Auto Summary	Mark the checkbox to automatically summarize IPv4 routes to classful boundaries.
IPv4 Unicast Address Family > Aggregate Address Configure a route aggregation policy. By default, the summarized routes will continue to be advertised and the summary route will have the atomic aggregate attribute.	Prefix	IPv4 prefix (A.B.C.D.)
	Prefix Length	Prefix length
	Summary Only	Mark the checkbox to suppress advertisement of the summarized routes.
	AS Set	Mark the checkbox to include the summarized routes in the summary route advertisement instead of the atomic aggregate attribute.

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
IPv4 Unicast Address Family > Clear	Clear Command	Clear dampening or flap-statistics
IPv4 Unicast Address Family > Dampening	Admin State	Admin state of dampening for this address family: ■ enable ■ disable
IPv4 Unicast Address Family > Dampening > R Dampening	Reachability Half Life	Reachability half life, in minutes. When a BGP route flaps, it is assigned a penalty. The penalty is decreased by half after each Reachability Half Life period.
	Reuse Limit	Reuse limit value. When the route flapping penalty decreases and falls below this reuse limit, the route is unsuppressed.
	Suppress Limit	Suppress limit value. A route is suppressed when its penalty exceed this limit.
	Max Suppress Time	Maximum amount of time a route can be suppressed, in minutes.
	Unreachability Half Life	Unreachability half life for penalty, in minutes
IPv4 Unicast Address Family > Dampening Show	Dampening Show	Show detailed information about dampening.
IPv4 Unicast Address Family > Neighbor	Peering Name	Select the name of the IP interface
	Default Originate	Advertise the default route
	Soft Reconfiguration Inbound	Enable local storage of received updates. BGP soft-reconfiguration allows for the storage of incoming update information to RIB-IN for a specific peer. If configured, soft clearing occurs without tearing down the session. It is useful for re-evaluating the inbound policy on the same set of incoming updates.
	Next Hop Self	Set router as next-hop for all routes advertised to peer.
	Allowas In	Enables accepting route updates with the local AS number in the AS Path attribute. This attribute. is configurable per neighbor and address family. When MCC receives a BGP route update with the local AS in the AS Path attribute, it rejects the route. When **`allowas-in`** is configured for a neighbor, MCC accepts a route with its local AS in the AS Path attribute. The **`allowas-in`** configuration relaxes the AS Path loop check for BGP updates. The number of times our own AS Path is present in the update is also configurable per neighbor and address family.

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
IPv4 Unicast Address Family > Neighbor > Capabilities Configure the capabilities of this peering	Graceful Restart	Mark the checkbox to advertise support of graceful restart
IPv4 Unicast Address Family > Neighbor > Distribute List Apply access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Access List Type	Access List Type: ■ standard access list ■ named access list
	Access List	Specify the standard (1-99) or standard expanded (1300 - 1999) access list or the named access list
IPv4 Unicast Address Family > Neighbor > Filter List Apply AS path access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	AS Path Access List	Select the name of the AS path access list
IPv4 Unicast Address Family > Neighbor > Maximum Prefix Configure the maximum number of prefixes accepted on this peering	Max Value	Specify the maximum number of prefixes to be accepted on this peering. If the Max Value is reached, the peering is shut down and an error event is logged.
	Threshold	Specify the number of received prefixes to trigger “warning” events. Express as percentage of Max Value.
	Warning Only	Mark the checkbox to only log “error” message when the number of prefixes reaches Max Value and keep the peering active.
IPv4 Unicast Address Family > Neighbor > Prefix List Apply prefix list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Prefix List Name	Select the name of the prefix list
IPv4 Unicast Address Family > Neighbor > Route Map Apply route map filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Route Map Name	Select the name of the route map

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
IPv4 Unicast Address Family > Redistribute	Protocol	Protocol type to redistribute into BGP: ■ connected ■ static
	Route Map Tag	Name of the Route map to filter redistributed routes
IPv4 Unicast Address Family > Route Detail	Prefix	IPv4 prefix (A.B.C.D.)
	Prefix Length	Prefix length
IPv4 Unicast Address Family > Route Table	Entry	Lists the summary of IPv4 unicast routes
IPv6 Unicast Address Family > Aggregate Address Configure a route aggregation policy. By default, the summarized routes will continue to be advertised and the summary route will have the atomic aggregate attribute.	Prefix	IPv6 prefix
	Prefix Length	Prefix length
	Summary Only	Mark the checkbox to suppress advertisement of the summarized routes.
	AS Set	Mark the checkbox to include the summarized routes in the summary route advertisement instead of the atomic aggregate attribute.
IPv6 Unicast Address Family > Clear	Clear Command	Clear dampening or flap-statistics
IPv6 Unicast Address Family > Dampening	Admin State	Admin state of dampening for this address family: ■ enable ■ disable
IPv6 Unicast Address Family >Dampening > R Dampening	Reachability Half Life	Reachability half life, in minutes. When a BGP route flaps, it is assigned a penalty. The penalty is decreased by half after each Reachability Half Life period.
	Reuse Limit	Reuse limit value. When the route flapping penalty decreases and falls below this reuse limit, the route is unsuppressed.
	Suppress Limit	Suppress limit value. A route is suppressed when its penalty exceeds this limit.
	Max Suppress Time	Maximum amount of time a route can be suppressed, in minutes.
	Unreachability Half Life	Unreachability half life for penalty, in minutes
IPv6 Unicast Address Family > Dampening Show	Dampening Show	Show detailed information about dampening.

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
IPv6 Unicast Address Family > Neighbor Manage IPv6 Unicast address family features on a neighbor peering	Peering Name	Select the name of the IP interface
	Default Originate	Advertise the default route
	Soft Reconfiguration Inbound	Enable local storage of received updates. BGP soft-reconfiguration allows for the storage of incoming update information to RIB-IN for a specific peer. If configured, soft clearing occurs without tearing down the session. It is useful for re-evaluating the inbound policy on the same set of incoming updates.
	Next Hop Self	Set router as next-hop for all routes advertised to peer.
	Allowas In	Enables accepting route updates with the local AS number in the AS Path attribute. This attribute. is configurable per neighbor and address family. When MCC receives a BGP route update with the local AS in the AS Path attribute, it rejects the route. When **`allowas-in`** is configured for a neighbor, MCC accepts a route with its local AS in the AS Path attribute. The **`allowas-in`** configuration relaxes the AS Path loop check for BGP updates. The number of times our own AS Path is present in the update is also configurable per neighbor and address family.
IPv6 Unicast Address Family > Redistribute Redistribution policy configuration	Protocol	Protocol type to redistribute into BGP: ■ connected ■ static
	Route Map Tag	Name of the Route map to filter redistributed routes
IPv6 Unicast Address Family > Route Detail		Show details of an IPv6 route. Specify route in format <prefix> <prefix-length>. For example, 3ffe:1234:5678::48
IPv6 Unicast Address Family > Route Table	Entry	Lists the summary of IPv6 unicast routes
Max Paths Configure equal-cost multi-path routing support	EBGP	Set the maximum number of EBGP ECMP routes allowed to a destination
	IBGP	Set the maximum number of IBGP ECMP routes allowed to a destination

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
Neighbor Configure and mange BGP neighbors	Peering Name	Peering name
	Neighbor Addr	Neighbor IP address. Cannot be modified once the neighbor has been created.
	Remote AS	Autonomous system of remote neighbor. Cannot be modified once the neighbor has been created.
	Connection Retry Time	Time between attempts to connect to the peer, in seconds.
	Ebgp Multihop	Enable multi-hop EBGP peering and set the maximum time to live.
	Password	Enable MD5 authentication on peering and set the password. When the password contains blank characters, enclose the entire string in quotation marks.
	Fall Over BFD	Enable bi-derectional forwarding detection: ■ single-hop ■ multi-hop
	Local AS	Local autonomous system number for this peering. Both the router ASN and this ASN are prepended to Path Attributes advertised on this peering. ***Note:*** *The behavior of this setting is modified by the* Local AS No Prepend *setting.*
	Advertisement Interval	Minimum interval between routing updates sent on this peering. Set to 0 to send an update immediately after a routing change.
	Local AS No Prepend	When a Local AS value is set on this peering, setting this parameter prevents the router's ASN from being included in the path attributes for prefixes advertised by this peering. When a Local AS value is set on this peering, but this parameter is not set, both the router ASN and the peering ASN are prepended to the path attributes advertised on this peering. When a Local AS value is set on this peering and this parameter is set, only the peering ASN is prepended to path attributes advertised on this peering (the router ASN is suppressed. If Local AS is not configured for this peering, this parameter is ignored and only the router ASN is prepended to the path attributes advertised on this peering.
Neighbor > Capabilities	Route Refresh	Mark the checkbox to advertise support of route refresh

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
Neighbor > Clear	Clear Command	Clear routes: ■ hard ■ soft
Neighbor > Detail	Entry	Lists summary of peering state.
Neighbor > Timers	Keep Alive	Keep Alive timer, in seconds
	Hold Time	Hold timer, in seconds
Neighbor > Update Source	Interface Selection	Specify the interface to act as the source of this peering session: ■ phy-interface ■ loopback
		Specify the physical interface as the source of the peering session.
Policy		Lists the routing policies
Summary	Entry	Lists the BGP summary information
IPv4 Unicast Address Family > Neighbor	Peering Name	Select the name of the IP interface
	Send Community	Type of community support: ■ standard ■ extended ■ both
	Next Hop Self	Set router as next-hop for all routes advertised to peer.
VPNv4 Unicast Address Family > Neighbor > Capabilities Configure the capabilities of this peering	Graceful Restart	Mark the checkbox to advertise support of graceful restart
VPNv4 Unicast Address Family > Neighbor > Distribute List Apply access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Access List Type	Specify access list type: ■ standard access list ■ named access list
	Standard Access List/Named Access list	Specify the Standard Access List/Named Access list

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
VPNv4 Unicast Address Family > Neighbor > Filter List Apply AS path access list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	AS Path Access List	Select the name of the AS path access list
VPNv4 Unicast Address Family > Neighbor > Maximum Prefix Configure the maximum number of prefixes accepted on this peering	Max Value	Specify the maximum number of prefixes to be accepted on this peering. If the Max Value is reached, the peering is shut down and an error event is logged.
	Threshold	Specify the number of received prefixes to trigger “warning” events. Express as percentage of Max Value.
	Warning Only	Mark the checkbox to only log “error” message when the number of prefixes reaches Max Value and keep the peering active.
VPNv4 Unicast Address Family > Neighbor > Prefix List Apply prefix list filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Prefix List Name	Select the name of the prefix list
VPNv4 Unicast Address Family > Neighbor > Route Map Apply route map filtering to inbound and outbound update messages carried by this peering	Direction	Specify filter direction: ■ in ■ out
	Route Map Name	Select the name of the route map
VPNv4 Unicast Address Family > Route Detail		Show details of an IPv4 unicast route address. Specify route in format <prefix> <prefix-length>. For example, 3ffe:1234:5678::48
VPNv4 Unicast Address Family > Route Detail		Show details of an IPv4 route. Specify route in format <prefix> <prefix-length>. For example, 10.16.0.0.24.
VPNv4 Unicast Address Family > Route Table	Entry	Lists the summary of VPNv4 NLRIs

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
IPv6 Unicast Address Family > Neighbor	Peering Name	Select the name of the IP interface
	Send Community	Type of community support: ■ standard ■ extended ■ both
	Next Hop Self	Set router as next-hop for all routes advertised to peer.
IPv6 Unicast Address Family > Route Table	Entry	Lists all IPv6 NLRIs
VRF Configure and manage VRFs	Network Context	Network Context supporting this VRF
	Route Distinguisher	Route Distinguisher: <ASN:<nn> or <IPv4 Address>:<nn> Cannot be modifies once the VRF has been created.
	Import Map	Route map to filter routes imported in VRF. Applies after import route targets.
VRF > IPv4 Unicast Address Family	Auto Summary	Mark the checkbox to automatically summarize IPv4 routes to classful boundaries
VRF > IPv4 Unicast Address Family > Max Paths Configure equal-cost multi-path routing support	EBGP	Set the maximum number of EBGP ECMP routes allowed to a destination
	IBGP	Set the maximum number of IBGP ECMP routes allowed to a destination
VRF > IPv4 Unicast Address Family > Redistribute	Protocol	Protocol type to redistribute into BGP: ■ connected ■ static
	Route Map Tag	Name of the Route map to filter redistributed routes
VRF > IPv4 Unicast Address Family > Route Table	Entry	Lists MPLS labels for IPv4 NLRI
VRF > IPv6 Unicast Address Family > Redistribute	Protocol	Protocol type to redistribute into BGP: ■ connected ■ static
	Route Map Tag	Name of the Route map to filter redistributed routes
VRF > IPv6 Unicast Address Family > Route Table	Entry	Lists MPLS labels for IPv6 NLRI

Table 10-32 BGP VPN Router Child Objects and Parameters

Object	Parameter	Description
VRF > Route Target	Direction	Filter direction: ■ import ■ export ■ both
	Value	Route Target Value: <ASN:<nn> or <IPv4 Address>:<nn>

NAT

save-map Command

Use the save-map command to save a deterministic NAT map in CSV format for a given NAT pool into a file with a name *<nat-pool-name><timestamp>.csv at location /var/corefiles/diags/* .

To execute the save-map command:

1. Expand **IP Protocols** in the tree.
2. Expand **Nat**.
3. Click **Deterministic**.
4. Under Deterministic Commands, select **save-map**.
5. Click **Select**.
6. Select the **Network Context** and **Nat Pool** to use as input.
7. Click **Execute**.

View UE IP Address Details

You can view UE IP address details (UE sub-pool network-context name, UE pool name, UE IP sub-pool name, UE IP, NAT sub-pool network-context name) and pdn-session-id (if session using NAT IP and NAT port exists in MCC). The system also displays NAT IP, NAT port-chunk, NAT IP sub-pool name, and NAT pool name.

To view UE IP address details:

1. Expand **IP Protocols** in the tree.
2. Expand **Nat**.
3. Expand **Deterministic**.
4. Click **Nat To Ue Binding**.

5 Configure the parameters as follows:

Table 10-33 Nat to UE Binding Parameters

Parameter	Description
NAT Network Context	NAT Network Context
NAT IP	NAT IP Address
NAT Port	NAT Port

View Deterministic NAT Resources

You can view deterministic NAT resources (NAT IP, NAT port-chunks, NAT IP sub-pool name, NAT pool name, and network-context name) and pdn-session-id (if session with given UE IP exists in MCC), for a given UE IP address and UE IP network-context name. The system also displays UE IP, UE IP sub-pool name, UE pool name, and network-context name.

To view deterministic NAT Resources:

1 Expand **IP Protocols** in the tree.

2 Expand **Nat**.

3 Expand **Deterministic**.

4 Click **Ue To NAT Binding**.

5 Configure the parameters as follows:

Table 10-34 UE to Nat Binding Parameters

Parameter	Description
UE Network Context	UE Network Context
UE IP	UE IP Address

NSM Logging

To configure NSM logging parameters:

1. Expand **IP Protocols** in the tree.
2. Click **Log Nsm**.
3. Configure the parameters as follows:

Table 10-35 NSM Parameters

Parameter	Description
All	Mark the checkbox to enable all NSM logs
Event	Mark the checkbox to enable Event logs
Kernel	Mark the checkbox to enable Kernel logs
Packet	Mark the checkbox to enable Packet logs

4. Click the **Save** icon.

OSPFv2 Routers

To configure OSPFv2 router parameters:

1. Expand **IP Protocols** in the tree.
2. Expand **Ospfv2**.
3. Click **Router**.
4. Configure the parameters as follows:

Table 10-36 Router Parameters

Parameter	Description
Network Context	Network Context for this OSPF router
Auto Cost Reference Bandwidth	Use reference bandwidth method to assign OSPF cost
Capability Opaque	Enable Opaque LSA capability: ■ true ■ false
Compatible Rfc1583	Compatible with RFC 1583
Default Metric	Set metric of redistributed routes
Max Concurrent Dd	Set the limit for the concurrent database descriptors

Table 10-36 Router Parameters

Parameter	Description
OSPF Abr Type	OSPF ABR Type: ■ Standard ■ Cisco ■ IBM ■ Shortcut
Router Id	Router ID for this OSPF process
Bfd All Interfaces	Mark the checkbox to enable BFD for all OSPF neighbors.

5 Click the **Save** icon.

6 To configure logging for all OSPF routers, expand **OSPF Logging**.

7 Click the log you want to enable (All, Events, Interface FSM, LSA, Neighbor FSM, NSM, Packet, Route)

8 Mark the checkboxes for the items you want.

9 Click the **Save** icon.

10 To configure the response of OSPF routers to a neighbor restart, click **Restart Response**.

11 Configure the parameters as follows:

- **Grace Period** – Enter a grace period in seconds.

12 Click the **Save** icon.

Restart Response child objects and their parameters are listed in the following table:

Table 10-37 Restart Response Child Objects and Parameters

Object	Parameter	Description
Helper	Max Grace Period	Helper maximum grace period.
Never Router ID	Router ID	Router ID Router id <A.B.C.D> of neighbor for which to never act as helper
Restart Policy		

OSPFv3 Routers

To configure OSPFv3 router parameters:

1. Expand **IP Protocols** in the tree.
2. Expand **Ospfv3**.
3. Click **Router**.
4. Configure the parameters as follows:

Table 10-38 Router Parameters

Parameter	Description
Network Context	Network Context for this OSPFv3 router
Auto Cost Reference Bandwidth	Use reference bandwidth method to assign OSPFv3 cost
DB Summary Opt	Enable database summary optimization: ■ enabled ■ disabled
Default Metric	Set metric of redistributed routes
Max Concurrent Dd	Set the limit for the concurrent database descriptors
Router Id	Router ID for this OSPF process
Bfd All Interfaces	Mark the checkbox to enable BFD for all OSPF neighbors.

5. Click the **Save** icon.

Policy

To configure routing policies:

1. Expand **IP Protocols** in the tree.
2. Expand **Policy**.

Policy child objects and their parameters are listed in the following table:

Table 10-39 Policy Child Objects and Parameters

Object	Parameter	Description
Access List Status	Entry	Shows configured Standard Access Lists

Table 10-39 Policy Child Objects and Parameters

Object	Parameter	Description
Access List	ID	Access List ID
	Remark	Access list entry comment (max 100 characters)
	Line	Number, Action (deny or permit), and ACL choice (IP Host, Wildcard Any, or Address and Mask) for this entry
Access List Word	ID	Access List ID
	Remark	Access list entry comment (max 100 characters)
	Line	Number, Action (deny or permit), address to match, mask as a prefix length, and exact match.
AS Path Access List	Name	AS Path name
	Line	Number, action (deny or permit), and regular expression to match BGP autonomous system path for this entry
AS Path List	Entry	Shows configured AS Path Lists
Comm List Status	Entry	Shows configured Community Lists
Comm List	ID	Community List ID
	Description	Community List description
Comm List Extended	ID	Community List ID
	Description	Community List description
Comm List Word	ID	Community List ID
	Description	Community List description
Comm List Word Extended	ID	Community List ID
	Description	Community List description
Prefix List Status	Entry	Shows configured Prefix Lists
Prefix List	Name	IPv4 Prefix list name
	Description	Access list entry comment (max 100 characters)
	Line	Number, action (deny or permit), LE range, GE range, network address, and prefix length for this entry
Prefix List IPv6 Status	Entry	Shows configured IPv6 Prefix Lists

Table 10-39 Policy Child Objects and Parameters

Object	Parameter	Description
Prefix List IPv6	Name	IPv6 Prefix list name
	Description	Access list entry comment (max 100 characters)
	Line	Number, action (deny or permit), LE range, GE range, network address, and prefix length for this entry
Route Map Status	Entry	Shows configured route maps
Route Map	Tag	Route map tag
	Action	Route map action: ■ permit ■ deny
	Seq Number	Sequence number

Routing Options

Multi-Active routing mode provides distributed routing control as a form of high availability for routing. Multi-Active routing mode provides faster geo-redundancy failover time compared to the BGP graceful-restart routing control failure recovery (default behavior).

Configuration is applied concurrently on all CSMs. The routing processes are active concurrently on CSMs for all network-contexts. BGP peering is distributed across all BGP processes. The assignment of BGP peers to CSMs is performed automatically during configuration.

In the event of a CSM failure, the BGP peers that are assigned to the failed CSM will be down, causing a partial loss of routing information. BGP peers will be reassigned to different CSMs if the current assigned CSM is administratively disabled.

To configure routing options:

1. Expand **IP Protocols** in the tree.
2. Click **Routing Options**.
3. Configure the parameters as follows:
   - **Multi Active Routing Mode**: Enable or Disable Multi Active Routing Mode.
   - **Geored RMG Deglitch Interval**: RMG failure deglitch interval, in seconds.
4. Click the **Save** icon.

TCP

Use this object to manage the kernel TCP configuration. MCC supports the following TCP optimization enhancement options:

- TCP FRTO config
- TCP ECN config
- TCP memory threshold config (low, pressure, high)

To manage kernal TCP configuration:

1. Expand **IP Protocols** in the tree.
2. Click **TCP**.
3. Configure the parameters as follows:

Table 10-40 TCP Parameters

Object	Description
Max Syn Backlog	Configure TCP IPv4 max syn backlog size on each VM that runs a ContentMgr process.
Tcp Frto	Configure TCP F-RTO options. F-RTO is an enhanced recovery algorithm for TCP retransmission timeouts (RTOs). It is used in wireless environments where packet loss is typically due to random radio interference rather than intermediate router congestion. Options include: ■ disable-frto – Disable this functionality. ■ basic-frto – Enable the basic version F-RTO algorithm is enabled. ■ sack-enhanced-frto – Enable SACK-enhanced F-RTO if flow uses SACK. The basic version can also be used when SACK is in use. ***Note:*** *F-RTO may negatively impact with the packet counting of the SACK-enabled TCP flow.*
Tcp Ecn	Configure TCP ECN options. Enable RFC 2884 Explicit Congestion Notification. When enabled, connectivity to some destinations may be affected due to older, misbehaving routers along the path, causing connections to be dropped. This file can have one of the following values: ■ disable-ecn – Neither initiate nor accept ECN. ■ enable-with-request-ecn-outgoing – ECN when requested by incoming connections and also request ECN on outgoing connection attempts. ■ enable-without-request-ecn-on-outgoing – ECN when requested by incoming connections, but do not request ECN on outgoing connections.

Table 10-40 TCP Parameters

Object	Description
Tcp Mem Low Threshold	Configure TCP memory options (measured in units of the system page size) to track its memory usage. MCC calculates the defaults at boot time from the amount of available memory. Configure the low threshold of TCP stack memory(KB). TCP does not regulate its memory allocation when the number of pages it has allocated globally is below this number.
Tcp Mem Pressure Threshold	Configure TCP memory options (measured in units of the system page size) to track its memory usage. MCC calculates the defaults at boot time from the amount of available memory. Configure the pressure point of TCP stack memory(KB). When the amount of memory allocated by TCP exceeds this number of pages, TCP moderates its memory consumption. This memory pressure state is lifted after the number of allocated pages falls below the low mark.
Tcp Mem High Threshold	Configure TCP memory options (measured in units of the system page size) to track its memory usage. MCC calculates the defaults at boot time from the amount of available memory. Configure the high threshold of tcp stack memory (KB). The maximum number of pages, globally, that TCP allocates. This value overrides any other limits imposed by the kernel.
Tcp Early Retrans	Configure the Early Retransmit (ER) and Tail Loss Probe (TLP) options to enhance TCP optimization during short Web transactions. ER and TLP work together to reduce data transfer delays by converting retransmission timeouts caused by tail losses (losses at the end of transactions) into fast recovery. ■ delayed-er ■ delayed-er-and-tlp ■ disable-er enable-er ■ enable-tlp-only

4 Click the **Save** icon.

5 To configure auto-tuning range for the TCP receive buffer size, expand **TCP**.

6 Click **Auto Tuning Recv Buffer**.

7 Configure the parameters as follows. TCP dynamically adjusts the size of the receive buffer within the configured range, depending on available memory.

Table 10-41 Auto Tuning Recv Buffer Parameters

Object	Description
Rmem Min	Set the minimum size of the receive buffer for each socket, in bytes.
Rmem Default	Set the default size of the receive buffer for each socket, in bytes.
Rmem Max	Set the maximum size of the receive buffer for each socket, in bytes.

8 Click the **Save** icon.

9 To configure auto-tuning range for the TCP send buffer size, expand **TCP**.

10 Click **Auto Tuning Send Buffer**.

11 Configure the parameters as follows. TCP dynamically adjusts the size of the send buffer within the configured range, depending on available memory.

Table 10-42 Auto Tuning Send Buffer Parameters

Object	Description
Wmem Min	Set the minimum size of the send buffer for each socket, in bytes.
Wmem Default	Set the default size of the send buffer for each socket, in bytes.
Wmem Max	Set the maximum size of the send buffer for each socket, in bytes.

12 Click the **Save** icon.

Statistics

Use this object to view the TCP Performance statistics.

To view TCP Performance Statistics:

1. Expand **IP Protocols** in the tree.
2. Expand **TCP**.
3. Expand **Statistics**.
4. Expand **Cluster Level** or **Node Level**.
5. Expand **Summary**.
6. Click an instance.

Performance statistics are:

- Number of TCP sockets in use
- Number of orphan TCP sockets
- Number of TCP sockets established
- Number of Time Wait TCP sockets
- TCP memory currently in use (KB)
- TCP memory peak in use (KB)
- TCP event number of sent sync-cookies

MME

Use this object to manage the MCC Mobility Management Entity (MME).

Note: *For configuration information for the MCC MME, see the Affirmed Networks MCC MME Configuration Management Reference Guide.*

Note: *To configure an MME, you must have the Configuration > MME Configuration > Read/Write security group permission. For instructions, see Specifying Permissions by Security Group.*

To configure MME parameters:

1. Expand **MME** in the tree.
2. Click a parameter to configure it.
3. Click the **Save** icon.

Viewing MME Real Time Statistics

Note: *For performance information for the MCC MME, see the Affirmed Networks MCC MME Performance Management Reference Guide.*

Note: *To view Real Time Statistics, you must have the Configuration > MME Configuration > Read security group permission. For instructions, see Specifying Permissions by Security Group.*

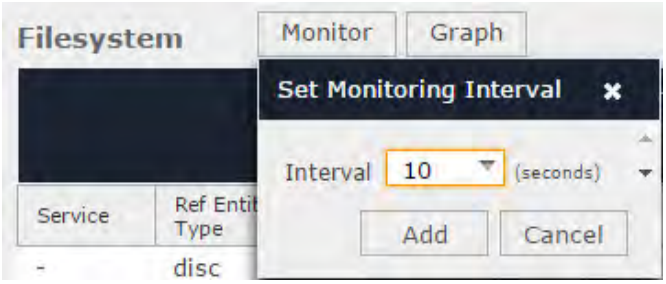
To view MME real time statistics:

1. Expand **MME** in the tree.
2. Expand **Statistics**.
3. Expand the statistics Group-set.
4. Click the statistic table.

   Acuitas retrieves the data and displays textual report of the values.

5 To specify a polling interval to refresh a chart/graph display of statistics, click the **Monitor** tab.

Figure 10-8 Monitor Interval



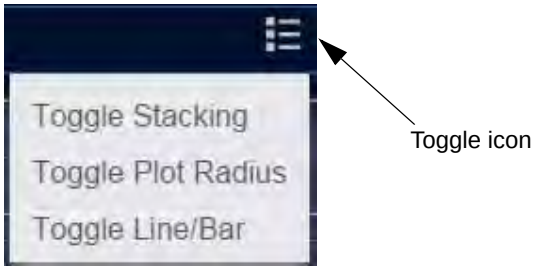
6 Enter the **Interval** value, in seconds, and click **Add**.

7 To view the statistics in a chart/graph display, click the **Graph** tab.

Acuitas retrieves the data and displays a chart/graph of the values in a separate window. The chart/graph is refreshed and redrawn whenever new data is collected based on the polling interval.

8 Click the **Toggle** icon and select the graphic format.

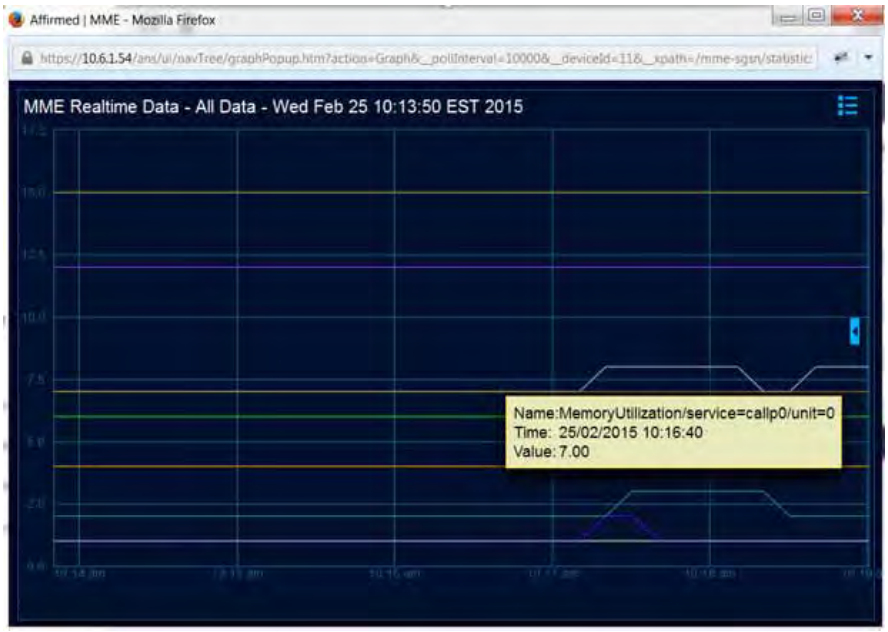
Figure 10-9 Graphic Format



9 To view a single data point, point the cursor at a graph.

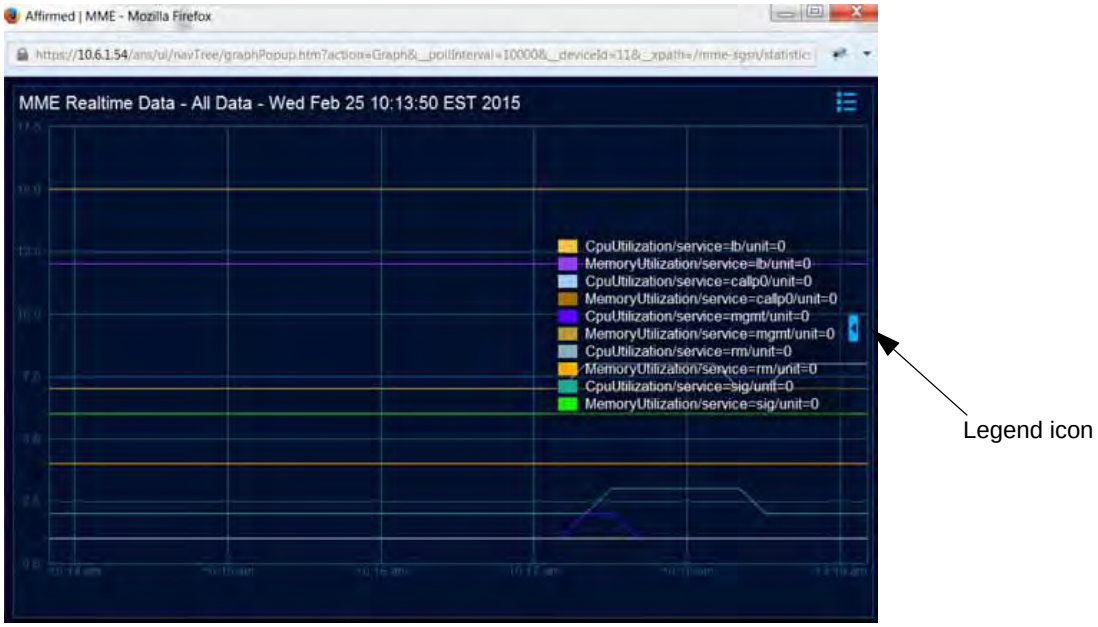
Acuitas opens a pop-up window that lists the timestamp and data value.

Figure 10-10 Data Point Details



10 To view the chart/graph legend, click the **Legend** icon.

Figure 10-11 Graph with Legend



11 To remove a graph from the chart, click the metric in the legend.

The graph is removed at the next polling interval.

12 Click the **Close** icon to close the chart/graph window.

Network Context

Use this object to create a virtual IP routing domain. Each Network Context maintains its own instance of configuration settings, IP address pools, and routing tables.

To configure Network Context parameters:

1 Click **Network Context** in the tree.

2 Configure the parameters as follows:

Table 10-43 Network Context Parameters

Object	Description
Name	Network Context name
Security	Specifies whether to enable or disable security firewall operations for this Network Context: ■ enabled ■ disabled Once security is enabled on a Network Context, security is applied to all packets entering and exiting the Network Context. The action taken on each packet is specified by the security rules configured on the Network Context. By default, if packets do not match any of the configured rules, they are dropped. Enabling security on a network rerquires additional memory – 4 GB on one of the control plane VMs (CSM/CPM) and 3 GB on each of the data-plane VMs (ISM/SSM/WSM/IOM).
Number of Security Services	Number of security tasks servicing this network context
Pass Local IKE Packets	Specifies whether to pass all local IKE packets without applying security policy for this Network Context: ■ true – pass all local packets without applying a security policy. IKE requests are automatically passed. ■ false – pass only those local packets that conform to a configured security policy. MCC performs a security policy lookup of the IKE requests.
Security Geo Redundancy Group	Geographic Redundancy group, if any, associated with the security tasks of this network context
TCP MSS Adjust	TCP MSS Adjustment to override the MTU in TCP connections. Is overridden by the IP Interface TCP MSS Adjust if also set.

Table 10-43 Network Context Parameters

Object	Description
Mapped UE Pool Network Context	Network context containing UE pools to be shared with this network context.
VRF Lightweight	Used for VPN Virtual Routing and Forwarding (VRF) purposes only. For more information, see VRF Lightweight.
Neighbor Discovery Profile	Neighbor Discovery Profile to use. This Neighbor Discovery Profile must already exist. See Neighbor Discovery Profile.
Tunnel Fragmentation Type	Specifies whether to fragment tunneled packets in the inner or outer IP header, if necessary: ■ inner ■ outer
Block GTP-U Error Pkt	Specifies whether to send GTP-U Error Indication messages when Tunnel Endpoint Identifier (TEID) is not found or FSAPI is invalid: ■ true ■ false
IP Shared Subnet	Specifies whether to allow multiple interfaces in the IP subnet range in a network context: ■ enabled ■ disabled Setting to enabled helps to achieve IP address conservation and L3-level bundling (similar to LAG at L2 level). Before changing the setting from enabled to disabled, all IP interfaces in the shared subnet must be deleted. This feature is supported on both IPv4 and IPv6 IP addresses on TWAG, ePDG, GiLAN, and SAEGW with and without NAT, and proxy with and without steering and IP transparency.
Control DSCP Value	DiffServ Code Point value with which to mark control IP packets on this network context

3 Click the **Save** icon.

Network Context child objects are listed in the following table:

Table 10-44 Network Context Child Objects

Object	Description
Access Interface	Lists access side IP interfaces

Table 10-44 Network Context Child Objects

Object	Description
Arp	Configures static ARP entries
Dns	Configures query settings and DNS Server IP addresses ***Note:*** *Modifying any attribute re-establishes connections to all servers in the Network Context as the change takes immediate effect. And, it cancels all pending queries on the connections, returning failure to applications.*
Interested Geo Red Groups	Configures interested Geo Redundancy Groups
Ip	Lists IP interface and route information
Ip Interface	Configures IP interface parameters
Ip Route	Lists the IP routes information
Ip Sub Pool	Configures IP Sub Pool. If OSPF is enabled, IP sub pool addresses are advertised over all IP interfaces in the network context, making the addresses reachable on all of the IP interfaces.
Logical Mgmt IP Interface	Configures logical management IP address
Loopback Ip	Lists loopback IP addresses. Loopback IP is used as control and data endpoint addresses. A maximum of 255 IP addresses are supported per cluster.
Mgmt IP Interface	Configures management IP interface parameters
Nat Pool	Configures NAT pool
Nat Sub Pool Statistics	Lists NAT subpool statistics
Network Context Statistics	Lists Network Context statistics
Service Endpoint	Configures service endpoints
Tunnel	Configures GRE/L2TP tunnels. Tunneling provides a private path for transporting packets through an otherwise public network by encapsulating packets inside a transport protocol.
UE Apn Ip Mgmt Status	Lists status of UE IP management on APNs associated with this Network Context.
UE Ip Binding	Lists PDN session information associated with an IP belonging to a UE IP subpool
UE Ip Mgmt Statistics	Lists IP management statistics
UE Ip Subpool Statistics	Lists IP management statistics for IP Sub Pools
UE Ip Subpool Status	Lists status of IP Sub Pools associated with UE Pools

Table 10-44 Network Context Child Objects

Object	Description
UE Pool	Configures UE pool associated with an IP Sub Pool and specifies whether the IP Sub Pool IP addresses/prefixes are managed locally or remotely (for example, using RADIUS). For local UE pools, support for a quarantine timer before reusing a released IP address. Also enables the system to re-use IP addresses in the Quarantine queue if no more are available in the IP Sub Pools associated with the IE Pool.
UE Pool Statistics	Lists IP management statistics for UE pools
UE Pool Status	Lists status of UE pools

VRF Lightweight

User this parameter only for VPN Virtual Routing and Forwarding (VRF) lightweight purposes.

Note: *VAS services/BGP/OSPF cannot run in this context.*

As part of network context scaling, MCC supports two Network Context types; *lightweight* and *normal*. MCC supports 128 normal Network Contexts and 2000 lightweight Network Contexts. See the following table to configure a normal or lightweight Network Context based the Network Context scenario.

Network Context Scenario	Normal Network Context	Lightweight Network Context
Content services such as Proxy, VAS services	Mandatory	Not supported
Any kind of gateway control traffic (GTP)	Mandatory	Not supported
BGP/OSPF protocol	Mandatory	Not supported
Interfaces need to be configured	Mandatory	Not supported
BGP VPN VRFs can be configured	Optional - use the lightweight setting when scaling is required	Preferred setting
Enterprise VRFs on Gi side	Optional - use the lightweight setting when scaling is required	Preferred setting
IPSec tunnel required	Mandatory	Not supported
RADIUS	Optional	Optional
DHCP client or relay required	Mandatory	Not supported

Network Context Scenario	Normal Network Context	Lightweight Network Context
Diameter traffic	Mandatory	Not supported

Example Network Context Scenarios

This section describes example Network Context scenarios and recommended lightweight or normal settings.

- Network Context is required to separate AAA traffic on GGSN. Use *normal* Network Context
- Operator must configure a separate network-context for an enterprise customer that uses their own DHCP allocation scheme or AAA server (for example, DHCP allocation is performed in an enterprise network). Since DHCP control traffic is required for this VRF, Operators must use the *normal* Network Context and must not use the *lightweight* Network Context.
- If enterprise customers require separate VRFs for each customer and most customers use local address allocation schemes, Affirmed Networks recommends using a *lightweight* Network Context.

Limitations

This section lists the limitations in configuring normal and lightweight Network Contexts.

- Operators cannot modify the VRF Lghtweight parameter or convert a normal Network Context to a lightweight Network Context or vice versa. This object must be set to either normal or lightweight during the initial creation and cannot be modified.

Note: *To modify this attribute, you must delete the current configuration for that Network Context and add a new Network Context.*

- After upgrading, all existing Network Context are converted to normal Network Context. If you require a lightweight Network Context, they must remove the current configuration for that Network Context and add it as a lightweight Network Context.

Neighbor Discovery Profile

Use this object to set attributes in router advertisement message.

To configure Neighbor Discovery Profile:

1. Expand **Networking Profiles** in the tree.
2. Click **Neighbor Discovery Profile**.
3. Configure the parameters as follows:

Table 10-45 Neighbor Discovery Profile Parameters

Object	Description
Name	Neighbor Discovery Profile name
RA MTU	MTU for IPv6 Neighbor Discovery Router Advertisements
Retransmit Timer	Time in seconds between retransmitted Neighbor Solicitation messages
Default Lifetime	The lifetime associated with the default router in seconds
Reachable Time	Time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.
Number Unsolicited RA	The number of unsolicited router advertisements the MCC would send when a UE attaches to the network.
Suppress RA	Specifies whether to suppress sending icmpv6 Router Advertisements: ■ true ■ false

4. Click the **Save** icon.

Performance Statistics Management

Use this object to view status of Performance Statistics Management.

To view Performance Statistics Management status:

1. Expand **Performance Statistics Management** in the tree.
2. Click **Table Status**.

Performance Statistic status parameters are:

- Name
- Collection Start Time
- Next Collection Time
- Collection Attempts
- Collection Success
- Collection Partial
- Collection Failure
- Collection Outstanding
- Avg Collection Time
- Max Collection Time
- Min Collection Time
- Avg Num Rows Per Collection
- Max Num Rows Per Collection
- Min Num Rows Per Collection

Pki

Use this object to install, remove, and update a pki object.

The pki director:

- Secures and tracks (via traps) pki objects in defined subdirectories on */tosdb/certs*
- Provides an internal client to allow tos applications to access pki objects and their status
- Monitors the expiration and revocation of x509 certificates
- Monitors the update available status of x509 certificate revocation lists
- Tracks key files and unreadable files (encrypted keys)
- Attempts to automatically re-download expiring x509 certificates and update available x509 certificate revocation lists when these objects were installed with a specified http source.

For details on cluster hierarchy to aid in the configuration of ssh pk, see the *Affirmed Networks System Administration Guide*.

install Command

Use the install command to install pki object using any of the following sources: http/https, file/public, or cut and paste.

To use the install command:

1. Click **Pki** in the tree.
2. Configure the parameters as follows:
   - **Pki Commands** – Select **install** and click **Select**.
3. Configure the parameters as follows:

Table 10-46 install Command Parameters

Parameter	Description
Type	Select the Pki type to install the object in: ■ public ■ private ■ ca ■ tls-ca ■ tls-server ■ tfd ■ epdg ■ user
Name	Override the name implied by source/altsource or give name if using cut and paste.
Source	Scp or http source to get the object from
Altsource	Alternate http source to get the object from
Object	Allow cut and paste of the object as a quoted text

4 Click **Execute**.

From http/https

The install attempts to immediately get the object. If the object does not exist on the http/https server, the file is empty, or the file is flawed, the command fails.

The command succeeds even if the server is unreachable, and MCC reattempts to get the object every hour until it either succeeds or the Operator removes the object. If repeated attempts take longer than 24 hours, MCC generates a periodic trap indicating that the object is still unreachable but the get attempts continue. When in this state, the object is not yet on the disk and is therefore unusable.

From a Local Disk

If the source is a file path under the */public* directory, then MCC moves the file to the chosen type after parsing the file. Moving the object also removes it from the former location. The file install attempts to move the file. If the file is not found, is flawed, or not located in */public*, the command fails.

Using Cut and Paste

The object can be given as a cut and paste quoted string of the certificate/key contents. The quoted string can contain spaces but cannot contain control characters. Replace any newlines with **\n** in the quoted string.

Using scp/sftp

To install an object using scp/sftp, push the object to the */public/certs/public*, */public/certs/private*, or */public/images* directory using your choice of scp/sftp clients. Otherwise, pull the object to one of those directories using **filecommand**. Then, follow the guidelines for local disk.

Object	Description	HTTP/HTTPS Source Guidelines	File/Public Source Guidelines	Cut/Paste Source Guidelines
altsource	Alternate http source to get the object from.	Supply the alternate source in the form of the http address of the file. For example: http://10.6.1.108/exampl eca_cert.pem.	Do not specify.	Do not specify.
name	Override the name implied by source/altsource or give name if using cut and paste.	Optionally, specify a different filename than the http filename. This may be useful if the application expects the name in a certain form or with a certain name extension.	Optionally, specify a different filename.	Specify a name.
object	Allow cut and paste of the object as a quoted text.	Do not specify.	Do not specify.	Must be a quoted string containing no control characters. Substitute **/n** for any new lines.
source	/public file or http source to get the object from.	Specify a source from which to get the object.		

Object	Description	HTTP/HTTPS Source Guidelines	File/Public Source Guidelines	Cut/Paste Source Guidelines
type	Pki type to install the object in. public|private|ca|tls-ca|tls-server|tfd|epdg|user|	Optionally, specify an object type that determines the subdirectory under */tosdb/certs* in which the object is stored. MCC retains the public and private types for backward compatibility. The admin or content group users can directly read and write these files through the CLI at /public/certs/public and /public/certs/private. As a result, these files are less secure. Other object types are named for the application likely to look in them for pki objects and are only visible to root users. Affirmed Networks recommends using these objects types. If type is not specified, MCC uses the default public.		Optionally, specify an object type that determines the subdirectory in which /tosdb/certs is stored.

remove Command

Use the remove command to remove all records in all states from the named object. The command removes an expired or revoked object or removes a state updating record that will never reach its source.

To use the remove command:

1. Click **Pki** in the tree.
2. Configure the parameters as follows:
   - **Pki Commands** – Select **remove** and click **Select**.
3. Configure the parameters as follows:

Table 10-47 remove Command Parameters

Parameter	Description
Type	Select the Pki type to remove the object from: ■ public ■ private ■ ca ■ tls-ca ■ tls-server ■ tfd ■ epdg ■ user
Name	Name of the pki object to be removed

4 Click **Execute**.

update Command

Use the update command to generate an updating state record for an existing object, which was originally installed with an http source, without impacting the existing disk file. When the attempt succeeds, MCC replaces the existing file and removes the updating record.

Note: *This command is only valid on pki objects installed using http/https and where their source is known to the system.*

To use the update command:

1 Click **Pki** in the tree.

2 Configure the parameters as follows:

- **Pki Commands** – Select **update** and click **Select**.

3 Configure the parameters as follows:

Table 10-48 update Command Parameters

Parameter	Description
Type	Select the Pki type to update: ■ public ■ private ■ ca ■ tls-ca ■ tls-server ■ tfd ■ epdg ■ user
Name	Name of the pki object to update

4 Click **Execute**.

Viewing pki Objects

To view pki objects:

1 Expand **Pki** in the tree.

2 Expand **Objects**.

3 Click an object instance.

Acuitas lists the object settings.

- Type
- Name
- State: State **ready** and state **invalid** records represent files on the disk. State **updating** and state **pending** records represent queued attempts to get or update the objects to the cluster.
- Modified: Represents the modify data for disk objects and the time the updating/pending record was created for those records.
- Encoding
- Format
- Description

Security

Use this object to configure security related to the Internet Key Exchange (IKE) call control.

The system supports firewall capability, including ACL filtering and IPsec. The firewall is enabled on a network context.

The firewall filters all incoming traffic before it is sent to the network. Operators configure the firewall with policy rules and optionally, IPSec tunnels. The policy rules implement Layer 3/4 packet filtering and can be specified as follows:

- Source/Destination Packet Filter
- Linked to a Control Flow Filter (that is, RADIUS and Diameter) in order to specify the filter based on the IP addresses and ports utilized by the protocol interface.
- Linked to Source/Destination IP pools in order to specify the filter based on the IP address ranges utilized by the address pools.

Use the information in Table 10-49 as a guideline when configuring IPSec security tunnels. Keep the following points in mind:

- Initiators always require tunnel PSK and tunnel local ID.
- V1 main mode responders require tunnel PSK and tunnel Remote Identity.
- V1 aggressive mode and V2 responders require authentication Remote Secret.
- V2-V1 fallback does not support the V1 aggressive mode option.
- An IP sec tunnel does not get setup if the matching proposal is not within the first 15 proposals.
- The MCC has a limit of 15 when evaluating proposals received in IPSec tunnel initialization messages and re-key. Any proposal beyond the limit of 15 is not considered and the IPSec tunnel is not created.

Table 10-49 IPSec Security Tunnel Configuration Guidelines

Specified					Required?				
Manual Key	IKE Version	V1-aggressive	Auto-initiate	Responder -only	Tunnel PSK	Tunnel Local ID	Tunnel Remote ID	Authentication Remote Secret	Special Considerations
Y	N/A	N/A	N/A	N/A	N	N	N	N	No IKE
N	V2	N/A	N	N	Y	Y	N	Y	V2 initiator and responder
-	-	-	N	Y	N	N	N	Y	V2 responder only
-	-	-	Y	N/A	Y	Y	N	N	V2 initiator only
-	V1	N	N	N	Y	Y	Y	N	V1 main mode initiator and responder
-	-	-	N	Y	Y	N	Y	N	V1 main mode responder only
-	-	-	Y	N/A	Y	Y	N	N	V1 main mode initiator only
-	V1	Y	N	N	Y	Y	N	Y	V1 aggressive mode initiator and responder
-	-	-	N	Y	N	N	N	Y	V1 aggressive mode responder only
-	-	-	Y	N/A	Y	Y	N	N	V1 aggressive mode initiator only
-	V2-V1	N/A	N	N	Y	Y	Y	Y	V2 or V1 main mode initiator and responder
-	-	-	N	Y	N	N	Y	Y	V2 or V1 main mode responder only
-	-	-	Y	N/A	Y	Y	N	N	V2 or V1 main mode initiator only

To configure security:

1 Click **Security** in the tree.

2 Configure the parameters as follows:

Table 10-50 Security Parameters

Parameter	Description
HW Assist	***Note:*** *Applies only to the AN3000 hardware platform. If you are operating MCC on a virtual platform, this parameter is ignored.* Enables hardware-assisted Diffie-Hellman calculations for the Affirmed Networks AN3000 hardware platform: ■ Enabled: all Diffie-Hellman calculations are performed using the hardware acceleration components of the Subscriber Services Module (SSM) on the AN3000 platform. ■ None: all Diffie-Hellman calculations are performed using software on the Content Services Module (CSM).
Cookie Threshold	Cookie thresholds limit the number of Security Associations (SAs) that can be half open/created before a cookie challenge is raised. This added security is to prevent Denial of Service (DoS) attacks. For IKEv2, the cookie-threshold value specifies the number of half-open SAs as a percentage of the maximum number of allowed tunnels, above which cookie-challenges are enabled.
Asynchronous Transactions	Specifies whether to allow SPM to set up transforms in parallel ■ true ■ false
Return Routability Check	Options for MOBIKE return routability check: ■ before-update: Specifies to perform a return routability check before the MOBIKE change occurs. ■ after-update: Specifies to perform a return routability check after the MOBIKE change occurs. ■ no-check: Specifies that no return routability check be performed

3 Click the **Save** icon.

4 Expand **Security**.

5 Expand **Authentication**.

6 To configure an authentication domain, click **Domain**.

7 Configure the parameters as follows:

Table 10-51 Domain Parameters

Parameter	Description
Name	Domain object name
Network Context	Network Context for this domain.

Table 10-51 Domain Parameters

Parameter	Description
Type	Authentication domain Type: ■ pki-plus-eap: authentication-domain type for ePDG IPsec applications ■ eap-gtc: authentication-domain type for ePDG IPsec applications ■ pki: pki authentication-domain type to allow non-ePDG applications to utilize PKI-based authentication.
EAP Only	Specifies whether to allow a UE to connect to an ePDG without requiring a certificate from the ePDG.: ■ true ■ false
Suppress Certreq to Initiator	Suppresses the sending of a CERTREQ in an IKE_SA_INIT response when EAP authentication is used: ■ true prevents the ePDG from sending a CERTREQ notification to the UE when the authentication domain is set to **`type pki-plus-eap`**. ■ false allows the ePDG to send a CERTREQ notification to the UE when the authentication domain is set to **`type pki-plus-eap`**.
EAP Additional Methods	Supported EAP methods: EAP-MSCHAPv2, EAP-TLS Requires Security to be administratively toggled to take effect.
EAP GTC Request Text	Text to be displayed to the user during the EAP-GTC exchange. If not entered, the default string is Password.

8 Click the **Save** icon.

9 To configure the public key infrastructure, click **PKI Certificate Management**.

10 Configure the parameters as follows:

Table 10-52 PKI Certificate Management Parameters

Parameter	Description
Name	PKI object name
Network Context	Network Context
File Name	Filename (without the extension) containing the certificate and private key (if local) or the CA certificate and an optional CRL (if ca-trust or intermediate-trust). Certificate files must have the extension .crt, private key files must have the extension .prv, CRL files must have the extension .crl

Table 10-52 PKI Certificate Management Parameters

Parameter	Description
File Type	File format: ■ pem ■ binary
Authentication Domain	Associated authentication domain - if not specified the default is used
Key Passphrase	If private key file is encrypted, the passphrase used to decrypt the file. Supported encryption formats are: SSH proprietary, SSH client version 1 RSA, SSH client version 2 RSA or DSA, PKCS#8
Certificate Type	Certification type: ■ local ■ ca-trust ■ intermediate-trust

11 Click the **Save** icon.

12 To configure pre-shared keys used to authenticate IKE peers, click **Remote Secret**.

13 Configure the parameters as follows:

Table 10-53 Remote Secret Parameters

Parameter	Description
Network Context	Network Context for this Remote Secret.
Name	Remote Secret object name
Secret	Remote Secret string.
Identity Type	Identity Type: ■ email ■ fully qualified domain name ■ IP address Enter the associated Identity value.

14 Click the **Save** icon.

15 To configure security rules and transforms, expand **Policy**.

16 To configure a security tunnel (bidirectional IPSec Security Association with respect to an IKE peer), click **Tunnel**.

17 Configure the parameters as follows:

Table 10-54 Tunnel Parameters

Parameter	Description
Network Context	Network Context for this transform.
Name	Tunnel name
Loopback IP	Local loopback IP address to use for tunnel encapsulation and/or IKE negotiation. The Loopback IP must already exist. Create it at Network Context > *name* > Loopback IP.
Remote IP	Remote IP address to use for tunnel encapsulation and/or IKE negotiation.
Options	Mark the checkbox(es) to enable various options controlling this tunnel: ■ ikev1-aggressive-mode ■ long-sequence-numbers-only ■ anti-replay ■ responder-only ■ responder-uses-remote-secret ■ auto-initiate ■ transport-mode ■ short-sequence-numbers-only ■ ipsec-pre-frag (fragment before applying IPsec)
IKE Lifetime	Lifetime, in seconds, of the phase 1 IKE Security Association (value 0 indicates none)
IPSec Lifetime	Lifetime, in seconds, of the phase 2 IPSec Security Association (value 0 indicates none)
IKE Version	IKE version for this tunnel: ■ v1 ■ v2 ■ v2-fallback-v1

Table 10-54 Tunnel Parameters

Parameter	Description
IKE groups	Mark the checkbox(es) to allow Diffie-Helman IKE groups for this tunnel: ■ group-01 ■ group-02 ■ group-05 ■ group-14 ■ group-15 ■ group-16 ■ group-17 ■ group-18 ■ group-19 ■ group-20 ■ group-21
PFS groups	Mark the checkbox(es) to allow Diffie-Helman Perfect Forward Security groups for this tunnel: ■ group-01 ■ group-02 ■ group-05 ■ group-14 ■ group-15 ■ group-16 ■ group-17 ■ group-18 ■ group-19 ■ group-20 ■ group-21
Pre Shared Key	Pre-shared key for IKE negotiation. This key must also be configured on the remote peer. Is mandatory for all **Options** except responder-only.
Tunnel Alarm On	Enables an alarm indication when IPsec tunnels are removed and established between the MCC and its remote IPsec peers: ■ true ■ false When set to true, MCC generates the following alarms: ■ *TUNNEL-DOWN* – All IPsec tunnels are removed between MCC and a specific IPsec peer. ■ *TUNNEL-UP* – A new IPsec tunnel is established between MCC and a specific IPsec peer.

Table 10-54 Tunnel Parameters

Parameter	Description
Authentication Domain	Associated authentication domain - if not specified the default is used
Second Authentication Domain	Authentication domain -for second authentication exchange
IKE V2 PSK Select Source	***Note:*** *Affects the pre-shared key selection and has no impact on the identity validation performed as part of the IKE V2 negotiation sequence.* Specifies the source from which a pre-shared key is selected for IKE V2 negotiations: ■ remote-identity – The identity provided by the remote peer as its identity is used to select the pre-shared key from the authentication configuration. ■ local-identity – The identity provided by the remote peer as that of the MCC device is used to select the pre-shared key from the authentication configuration. ■ from-tunnel – The pre-shared key configured for the tunnel is selected.
Epdg Specific No GW Found Error Code	IKEv2 error code used to indicate no GW is available to process request. Is used by the ePDG GW serv ice.
Tunneled Network Context	Network Context for which this tunnel carries traffic.
Dead Peer Detection	Time, in seconds, to detect a dead IKE peer. Value 0 disables dead peer detection.
Mobike	Specifies whether to enable MOBIKE (for responder mode only): ■ enabled ■ disabled
Max Number of Child SAs	Specifies the maximum number of child SAs per tunnel
Anonymous Idi	Supports the authentication of the ePDG by the UE prior to sending an IMSI during the IKE_AUTH process. Supports the use of an anonymous IDi (Identification:Initiator) in the IKE_AUTH exchange. During the exchange, the UE first sends an anonymous IDi to the ePDG. After the UE has validated the ePDG certificate, the ePDG extracts the IMSI from the EAP Response/Identity. Specify the IKEv2 IDi values(s) for anonymous IKE AUTH (IMSI protection)
Ike Fragmentation	Specifies whether to IPSec IKEv2 message fragmentation (RFC 7383): ■ enabled ■ disabled This feature allows IKEv2 to interoperate with IKEv2 peers that support IKE Fragmentation. IKE fragmentation is used only if both peers advertise support for IKE fragmentation in a NOTIFY payload during IKE_SA_INIT.

Table 10-54 Tunnel Parameters

Parameter	Description
Ike Fragment Size	IKEv2 fragmentation maximum fragement packet size. If this value is not set, the default fragment size is selected by the tunnel's loopback IP: 576 for an IPv4 address and 1280 for an IPv6 address. The incoming fragment size is defined by the peer and not negotiated.

18 Click the **Save** icon.

19 To configure IKE transform selections, expand the tunnel you added.

20 Click **IKE Transform**.

21 Configure the parameters as follows:

Table 10-55 IKE Transform Parameters

Parameter	Description
Name	Transform name
Cipher	IKE encryption algorithm: ■ 3des ■ aes128 ■ aes192 ■ aes256 ■ aesctr128 ■ aesctr192 ■ aesctr256
Auth	Supported integrity algorithm: ■ md5 ■ sha1 ■ sha256 ■ sha384 ■ sh5a12 ■ aes-xcbc
Prf	Supported Pseudorandom Function algorithm: ■ md5 ■ sha1 ■ sha256 ■ sha384 ■ sh512 ■ aes-xcbc

22 Click the **Save** icon.

23 To configure IPSec transform selections, expand the tunnel you added.

24 Click **IPSec Transform**.

25 Configure the parameters as follows:

Table 10-56 IPSec Transform Parameters

Parameter	Description
Name	Transform name
Cipher	ESP encryption algorithm: ■ 3des ■ aes128 ■ aes192 ■ aes256 ■ aesctr128 ■ aesctr192 ■ aesctr256 ■ aes128gcm8 ■ aes128gcm16 ■ aes192gcm8 ■ aes192gcm16 ■ aes256gcm8 ■ aes256gcm16 ■ null
Auth	Supported integrity algorithm: ■ md5 ■ sha1 ■ sha256 ■ sha384 ■ sha512 ■ aes-xcbc

26 Click the **Save** icon.

27 To configure a manual key for this tunnel, expand the tunnel you added.

When you specify a manual key, all IKE parameters become obsolete.

28 Click **Manual Key**.

29 Configure the parameters as follows:

Table 10-57 Manual Key Parameters

Parameter	Description
Note: *Each transform requires a different key length.*	
SPI In	Incoming security policy index
SPI Out	Outgoing security policy index
Cipher In	Ingress manual cipher key (hexadecimal string).
Cipher Out	Egress manual cipher key (hexadecimal string).
Authentication In	Ingress manual authentication key (hexadecimal string).
Authentication Out	Egress manual authentication key (hexadecimal string).

30 Click the **Save** icon.

31 To configure a local IKE identity for this tunnel, expand the tunnel you added.

32 Click **Local Identity**.

33 Configure the parameters as follows:

Table 10-58 Local Identity Parameters

Parameter	Description
Enforce	Specifies whether to enforce the remote identity must match what is signalled by the peer: ■ true ■ false
Type	Identity Type: ■ email ■ fully qualified domain name ■ IP address Enter the associated Local Identity value.

34 Click the **Save** icon.

35 To configure a remote IKE identity for this tunnel, expand the tunnel you added.

36 Click **Remote Identity**.

37 Configure the parameters as follows:

Table 10-59 Remote Identity Parameters

Parameter	Description
Enforce	Specifies whether to enforce the remote identity must match what is signalled by the peer: ■ true ■ false
Type	Identity Type: ■ email ■ fully qualified domain name ■ IP address Enter the associated Remote Identity value.

38 Click the **Save** icon.

39 To configure a traffic filter to associate with the tunnel, click **Rule**.

40 Configure the parameters as follows:

Table 10-60 Rule Parameters

Parameter	Description
Network Context	Network Context for this rule.
Name	Rule name
Priority	Evaluation priority for this rule. Overlapping rules must have unique priority. Set the security policy rules' priorities such that the more specific rule has a higher priority.
Action	Action for this rule: ■ pass ■ drop ■ reject
Clone Reverse	Mark the checkbox to specify whether to automatically clone this rule, reversing **Source**/**Destination**. Use this option for most situations. Only omit it when asymmetrical security is required. ***Note:*** *Applies when IP Pool Type is User Equipment Pool or NAT Pool*

Table 10-60 Rule Parameters

Parameter	Description
Tunnel	Tunnel to apply to traffic: ■ To Tunnel: Tunnel to apply to traffic initiated from the source address towards the destination address ■ From Tunnel: Tunnel to apply to traffic initiated from the destination address towards the local address Select the associated tunnel.
Control Flow Filter Type	The control flow specification of the traffic selector: ■ RADIUS ■ DIAMETER Select the associated interface.
Source IP Pool Type	IP Pool used as the source IP specification: ■ User Equipment Pool ■ NAT Pool Select the associated interface.
Destination IP Pool Type	IP Pool used as the destination IP specification: ■ User Equipment Pool ■ NAT Pool Select the associated interface.

Sample Rule Configuration:

The following sample configuration allows any packets between 100.100.100.0/24 and 200.200.200/24, but drops UDP traffic between 100.100.100.10 and 200.200.200.10.

```
an3000-mcm-slot7cpu1# show running-config security policy rule
management-context
security policy rule management-context drop-10
 priority 100
 action   drop
 clone-reverse
 source-packet-filter spf
  protocol 17
  ip-start 100.100.100.10
  ip-end   100.100.100.10
 !
 destination-packet-filter dpf
  protocol 17
  ip-start 200.200.200.10
```

```
  ip-end   200.200.200.10
 !
!
security policy rule management-context pass-range
 priority 500
 action   pass
 clone-reverse
 source-packet-filter spf
  protocol 255
  ip-start 100.100.100.0
  ip-end   100.100.100.255
 !
 destination-packet-filter dpf
  protocol 255
  ip-start 200.200.200.0
  ip-end   200.200.200.255
 !
```

41 In **Source Packet Filter**, configure the following parameters:

Table 10-61 Source Packet Filter Parameters

Parameter	Description
Name	Packet Filter Name
Protocol	IP protocol values. Value 255 represents all protocols
IP Start	Starting inclusive IP address
Port Start	Starting inclusive port
Port End	Ending inclusive port
Range	Source Packet Filter range: ■ IP End ■ IP Prefix Length Enter the associated value.

To add additional Source Packet Filters, click the **Create** icon.

42 In **Destination Packet Filter**, configure the following parameters:

Table 10-62 Destination Packet Filter Parameters

Parameter	Description
Name	Packet Filter Name
Protocol	IP protocol values. Value 255 represents all protocols.
IP Start	Starting inclusive IP address
Port Start	Starting inclusive port
Port End	Ending inclusive port
Range	Destination Packet Filter range: ■ IP End ■ IP Prefix Length Enter the associated value.

To add additional Destination Packet Filters, click the **Create** icon.

43 Click the **Save** icon.

Debug

Use this object to enable IKE key-material logging on a per network context basis. Logging allows for diagnosing problems with ePDG sessions and is intended as a diagnostic tool only.

Logged key-material table files can be generated for use in Wireshark through use of the Infrastructure > Logging > Event Log > Policy object.

To configure security debug settings:

1. Expand **Security** in the tree.
2. Click **Debug**.
3. Configure the parameters as follows:
   - **Network Context** – Select the Network Context to use for this security debug.
4. Click the **Save** icon.
5. Expand the security Network Context in the tree.
6. Click **Key Logging**.
7. Configure the parameters as follows:
   - **Type** – Select the type of keys to log for connection debugging (ikev1, ikev2, esp).
8. Click the **Save** icon.

History

Use this object to control the security transaction history feature. When the security transaction history feature is enabled, the IPSec processing module records each Internet Key Exchange (IKE) and IPSec security association negotiation in a set of history buffers that can be displayed. The configuration provides four separate history buffers:

- IPSec Failures
- IPSec Completions
- IKE Failures
- IKE Completions

The depth (number of entries) of each history buffer can be individually set.

To configure History settings:

1. Expand **Security** in the tree.
2. Click **History**.
3. Configure the parameters as follows:

Table 10-63 History Parameters

Parameter	Description
Admin State	Admin State: ■ enabled ■ disabled
IPSec SA Failure Depth	The history buffer depth (number of entries) for unsuccessful IPSec security associations (SA) negotiations.
IPSec SA Completion Depth	The history buffer depth (number of entries) for successful IPSec security associations (SA) negotiations
IKE SA Failure Depth	History buffer depth (number of entries) for unsuccessful IKE security associations (SA) exchanges
IKE SA Completion Depth	History buffer depth (number of entries) for successful IKE security associations (SA) exchanges.

4. Click the Save icon.
5. To view security transaction history, expand **History**.
6. Expand the history you want to view:
   - IPSec Failures
   - IPSec Completions
   - IKE Failures
   - IKE Completions
7. Click an instance to view the history statistics.

Redundancy Stats

Use this object to display security redundancy statistics.

To view Redundancy statistics:

1. Expand **Security** in the tree.
2. Click **Redundancy Stats**.

   Acuitas lists the security redundancy statistics.

Statistics

Use this object to display the security statistics.

To view Security statistics:

1. Expand **Security** in the tree.
2. Expand **Statistics**.
3. To view security packet statistics at the CPU level, expand **CPU Level**.
4. Expand **Data Stats**.
5. Click a CPU instance.

   Acuitas lists the security packet statistics for that CPU.
6. To view security packet statistics on an aggregated basis across all CPUs, expand **Data Stats**.
7. Click an instance.

   Acuitas lists the security packet statistics.
8. To view network context statistics, click **Network Context**.

   Network context statistics parameters are listed in the following table:

Table 10-64 Network Context Statistics Parameters

Parameter	Description
Name	Network Context name
Current IKE Tunnels	Number of current IKE tunnels
Total IKE Tunnels	Number of total IKE tunnels
Total IKE Failed Tunnels	Number of total failed IKE tunnels
Total IKE Rekeyed Tunnels	Number of total rekeyed IKE tunnels
Current IPSec Tunnels	Number of current IPSec tunnels
Total IPSec Tunnels	Number of total IPSec tunnels
Total IPSec Failed Tunnels	Number of total failed IPSec tunnels
Current Transforms	Number of current transforms
Total Transforms	Number of total transforms
Rekeyed Transforms	Number of rekeyed transforms
Current Rules	Number of current rules
Total Rules	Number of total rules
Current Flows	Number of current flows

Table 10-64 Network Context Statistics Parameters

Parameter	Description
Total Flows	Number of total flows

9 To view security rules, click **Rule Stats**.

Rule statistics parameters are listed in the following table:

Table 10-65 Rule Statistics Parameters

Parameter	Description
Network Context	Network Context for this rule
Name	Rule name
Current Flows	Number of current flows using this rule
Total Flows	Number of total flows using this rule

Service Constructs

Service constructs are the common building blocks to create service instances used in workflow. Workflow defines the treatment of a service flow across various services.

Note: *As an alternative procedure, use the Affirmed Open Workflow application to define service constructs. For instructions, see Affirmed Open Workflow*

Service constructs are listed in the following table.

Table 10-66 Service Constructs

Service Construct	Description
ACL List	Defines the action to take when and an unknown IP address attempts to access the NE.
Advice of Charge	Defines the action to take after online quota is exhausted, such as block and return a notification message or redirect subsequent HTTP traffic to a configured URL.
Aoc Hardware ID Format	Specifies AES-encrypted UE hardware information in the redirection URL.
CA Certificate List	Defines a list of TLS CA-Certificates.
Content Insertion	Defines content insertion mode by which Multi Protocol Proxy operates.

Table 10-66 Service Constructs

Service Construct	Description
Data Record Template	Define the format of a data record. The data record can be a Radius message, Diameter message, or Charging Data Record (CDR) in local CDR file. The format of a data record is determined by the data fields in the record. For Radius and Diameter data record, Operators can configure whether or not to include the fields (optional AVPs) in the messages. For CDR record, Operators can configure: ■ **Field Delimiter** – character to use as a delimiter between fields. ■ By default, **Field Delimiter** is set to a dot (.) ■ **Present Flag** – whether or not to include the data field in CDR. ■ By default, Present Flag is set to conditional for all data fields (data field filled in CDR when available). ■ **Position Index** – where the data field is populated in CDR. ■ There is predefined order for each data field if **Position Index** is not configured. ■ **Format Type** – format type of the data field. ■ There is default format for each data field, if not configured. ■ **Length** – fixed length of the data field. ■ By default, **Length** is set to 0 (the data field is written out as it is). ■ **Alignment** – alignment of the data field. ■ It is set to left alignment, if not configured. ■ **Padding** – character used for padding when the field has fixed length.
Deep Packet Inspection	Enables deep packet inspection function and lists bit counters for protocols detected by signature analysis
Device Database	Define device characteristics such as device type, make, model, screen width, and screen height in applying data services.
DHCP Local Server Profile	Defines DHCP local server profile.
DHCP Mapping Template	Used to customize incoming and outgoing DHCP messages when the MCC TWAG is operating as a DHCP relay agent or as a DHCP server.
DHCP Service Profile	Enables DHCP-enabled UE IP allocation.

Table 10-66 Service Constructs

Service Construct	Description
Diameter Result Code Policy List	Configures the Diameter credit control failover behavior on the Gx/Gy interfaces based on the result code received in the CCA error message.
Diffserv Profile	Defines parameters for priority queuing.
Domain Rule Group	Configures a list of domains for which snooping is enabled.
EDR Flow Network Stats Profile	Configures the EDR (Event Data Record) flow network profile.
EDR Interface Profile	Configures the EDR (Event Data Record) Interface Profile to generate EDRs.
EDR Server Profile	Configures the EDR (Event Data Record) server Profile to generate EDRs
EDR Session Data Stats Profile	Enables EDR (Event Data Record) session volume measurement reporting.
Encryption Profile	Specifies the algorithm and keys to be used for header encryption.
Event Trigger Template	Specifies the events that trigger an interim update on the offline charging interface and to trigger the closure of an interim CDR.
File Download Profile	Defines parameters for importing lists from a file server
Filter Hash List	Imports a Filter Hash List
Flow Idle Timeout Filter	Defines parameters to identify application traffic and configure the tuple: destination port range and protocol
Flow Idle Timeout Rule	Defines parameters of connection timeout, priority of the rule, and the mapping to the Flow Idle Timeout Filter
Geo Redundancy Server	Defines parameters for Geographic Redundancy Standby Server
Gy Event Trigger Template	Specifies the Gy events that trigger the closure and sending of an interim CDR on the Gz/Rf interface.
Health Check Profile	Configures a health-check mechanism to detect if a monitored service is down or overloaded.
Host List	Serves as a whitelist used by the Fraud Detection Profile. It contains the IP addresses that represent legitimate proxies.
HTTP Header Enrichment	Defines the HTTP headers/cookies that an HTTP Policy adds, removes, or replaces in the HTTP request header

Table 10-66 Service Constructs

Service Construct	Description
HTTP Rule Group	Defines a set of rules for matching header attributes in HTTP request and response headers
HTTP Server	Defines an HTTP Server
HTTP Server List	Specifies a list of HTTP Server
HTTP URL Rewrite	Defines a set of rewrite-rules used in HTTP Policy for URL substitution.
IMSI Range	Specifies to generate SGW CDRs based on a list of configured IMSI ranges
IMSI Range List	Specifies a list of IMSI ranges
Interface > AAA Interface Group	Configures the Accounting Authentication Authorization interface group, including: ■ Diameter service for each diameter service interface (PCRF, OSC, and OFCS). ■ Diameter peer ■ Radius Server Group, containing a list of peers (Radius servers) with which the NE communicates.
Interface > Accounting Service	Configures the Radius accounting service. The accounting service references a Radius server group previously configured.
Interface > Authorization Service	References a Radius server group previously configured. The Radius access request record attributes can be controlled by associating the service with an access request template.
Interface > Flow Authorization Interface	Used for subscriber authentication when a Network Address Translation (NAT) IPv4 Address is allocated for an IPv6 UE for the configured services/flows.
Interface > GW Session Learner	Specifies the Mobile Content Cloud Gi Gateway session learner interfaces
Interface > IPMS Interface	Configures an IPMS interface group
Interface > Offline Charging	Configures an Offline Charging Interface Profile
Interface > Online Charging	Configures an Online Charging Interface Profile
Interface > PCRF Charging	Configures a PCRF Charging Interface Profile
Interface > Policy Server Interface	Configures a Policy Server Interface
Interface > Port NBR Service	Configures a Port NAT Binding Record Interface Service Profile
Interface > Rx Interface	Specifies the Rx interface

Table 10-66 Service Constructs

Service Construct	Description
Interface > S6b Interface	Specifies the S6b interface
IP List	Configures an IP Address List
LDAP Feature Group	Configures an LDAP Feature Group
LDAP Profile	Configures an LDAP Profile
LDAP Remote Server	Configures an LDAP Remote Server
Loopback IP List	Configures a Loopback IP List
Multimedia Messaging Service MM3 Profile	Configures a Multimedia Messaging Service MM3 interface
Multimedia Messaging Service Blacklist	Configures a Multimedia Messaging Service destination address blacklist
Multimedia Messaging Service Center	Configures a Multimedia Messaging Service Center
Multimedia Messaging Service Center Error Responses	Configures error response status and text in case of rejected Multimedia Messaging requests.
Multimedia Messaging Service Center Group	Configures a group of Multimedia Messaging Service Centers
Multimedia Messaging Service STI Profile	Configures a Multimedia Messaging Service Standard Transcoder Interface Profile
Network Profile	Configures the network profile on the User Plane
Packet Filter	Defines the packet filter or service data flow configuration identified by: ■ User Equipment IP address ■ Network IP address ■ User Equipment port range ■ Network port range ■ IP Protocol ■ Flow initiator
PLMN ID List	Configures home and roaming (visiting) subscribers.
Protocol Application Rule Group	Defines layer 7 applications, protocols, and subprotocols for signature analysis by detecting deterministic and/or heuristic patterns in bidirectional packet flow. Signature Analysis is the key technology that enables Workflow to control application of advanced services on subscriber traffic (such as charging, per-application filtering, QOS, and so on).

Table 10-66 Service Constructs

Service Construct	Description
Quality of Service	Configures default and network Quality of Service characteristics associated with subscribers.
RADIUS Mapping Template	Used to customize incoming and outgoing RADIUS authentication messages transmitted between the MCC TWAG and RADIUS server.
Realm List	Configures the Realm/Username@realm list.
SCTP Profile	Configures an SCTP (Stream Control Transmission Protocol) Profile
Service Rule	Is associated with a specific Service Data Flow, protocol analyzer, and/or HTTP Rule Group. Service Rules are referenced in other services. Each rule has a unique service data flow identifier and an optional (non-unique) Correlation Identifier to be logged in CDR/EDR.
Session Rule Group	Configures a list of rule groups that can be configured for RAT type, MBR matching, or both.
Short Message Service Center Group	Configures a group of SMSCs
Short Message Service Notification	Configures SMS notification text messages
Short Message Service Center Profile	Configures a Short Message Service Center Profile
Static DNS Map	Configures a static DNS map for DNS lookups in HTTP Proxy
Subscriber Group	Defines a group of subscribers whose traffic is rate-limited to a configured aggregate QoS Policy.
TCP Optimization Profile	Specifies changes to the TCP/IP stack targeted to improve throughput and user experience in the mobile network.
Time of Day Rule Group	Defines a group of rules used to provide time-of-day filtering.
TLS Rule Group	Defines a set of rules for matching on SNI (Server Name Indication) and Server certificate CN (Common Name) fields of a TLS handshake.
TLS Termination Policy	Defines a TLS Termination Policy
UA Profile	Configures a User Agent Profile.
URL List	Defines a list of URLs.
URL List Stats	Lists URL List statistics.

Table 10-66 Service Constructs

Service Construct	Description
Workflow Data Stats	Lists Workflow Data statistics.

ACL List

Operators can apply access control list (ACL) filtering to incoming control traffic to restrict or permit access to MCC interfaces. An ACL contains one or more access control filters. Each access control filter specifies the following:

- The criteria that a packet must match. You define the criteria in a packet filter, which can be based on source and destination IP addresses, source port and destination port, and the networking protocol in use.
- The resulting action, either drop or allow, to take when a match is found.
- A value for prioritizing the access control filter within the ACL, evaluated in sequential order, first to last.

ACL filtering uses an implied *Allow All Traffic* filtering statement, which means if a received packet does not match any defined criteria in the ACL, the packet is allowed. However, you can configure ACL filtering to explicitly deny certain types of traffic by configuring a lowest priority access control filter with a drop action. In this case, you must configure higher priority filters that explicitly permit the types of traffic allowed.

Note: *Affirmed Networks recommends that you configure specific drop/allow filters to ensure accurate traffic filtering.*

ACLs are applied on a network context basis, where access control filters apply to all interfaces within a specified network context. The system supports up to 32 access control filters per ACL.

ACL filtering does not apply to the following types of traffic:

- Routing Protocols, such as BGP, OSPF, BFD
- DNS, SSH, IPv6 ND, DHCP, IKE
- Control Protocols, such as RADIUS, Diameter, GTP', and CALEA, that match explicitly registered IP address/port combinations
- Upstream GTP-U and GRE tunneled WAG traffic

Applying ACL filtering rules may cause unintended results if not used properly. Affirmed Networks recommends contacting the TAC prior to implementation.

To add an ACL List:

1. Expand **Service Construct** in the tree.
2. Click **ACL List**.
3. Configure the parameters as follows:
   - **Name** – Enter an ACL List name.
4. Click the **Save** icon.
5. Expand **ACL List**.
6. Expand the ACL list you added.
7. Click **ACL Filter**.
8. Configure the parameters as follows:

Table 10-67 ACL Filter Parameters

Parameter	Description
Name	Enter the ACL filter name
Priority	Enter the ACL filter priority
Action	Action to take for the ACL filter: ■ Allow ■ Drop
Packet Filter	Packet filter to match. This packet filter must already exist. See Packet Filter.

9. Click the **Save** icon.
10. Repeat step 7 through step 9 to add as many ACL Filters as needed.

Advice of Charge

Defines the action to take after online quota is exhausted, such as block and return a notification message or redirect subsequent HTTP traffic to a configured URL.

To add an Advice of Charge:

1. Expand **Service Construct** in the tree.
2. Click **Advice of Charge**.
3. Configure the parameters as follows:
   - **Name** – Enter an Advice of Charge name.
   - **AOC Hardware ID Format**. The AOC Hardware ID Format must already exist. See Aoc Hardware ID Format.
4. In **HTTP**, configure the following parameters to specify the action message to be sent to the user:

Table 10-68 HTTP Parameters

Parameter	Description
Redirect Code	HTTP Request Redirect Code: ■ 302 found – The requested resource resides temporarily under a different URL ■ 303 See Other – The requested page can be found under a different URL ■ 307 Temporary Redirect – The requested page has moved temporarily to a new URL
Include MAC	Specify whether to include the MAC address in the redirect URL: ■ true ■ false
Include Original URL	Specify whether to include the original requested address in the redirect URL: ■ true ■ false
Include IMSI	Specify whether to include the IMSI in the redirect URL: ■ true ■ false
Include IMEI	Specify whether to include the IMEI in the redirect URL: ■ true ■ false

Table 10-68 HTTP Parameters

Parameter	Description
Include MSISDN	Specify whether to include the MSISDN in the redirect URL: ■ true ■ false
Include Class	Specify whether to include the class information in the redirect URL: ■ true ■ false The class information is provided by the RADIUS server and is used to identify the subscriber in subsequent RADIUS accounting messages.
Action	Specify action: ■ redirect-url ■ notification-msg
Field when Action is set to notification-msg:	
Notification Message	HTTP Request Block Message
Field when Action is set to redirect-url:	
Redirect URL	HTTP Request Redirect URL

5 In **Charging Notification List**, configure the following parameters to specify the notification message to be sent to the user when rejecting:

Table 10-69 Charging Notification List Parameters

Parameter	Description
Mscc Result Code	Select the MSCC Result Code
Mms Result Code	Select the MMS Error Response Code
Notification Text	Enter the MMS notification text
SMS Notification Text	Enter the SMS notification text

To add additional Charging Notifications, click the **Create** icon.

6 Click the **Save** icon.

Aoc Hardware ID Format

Use this object to specify AES-encrypted UE hardware information in the redirection URL. This feature is supported for offline charging only.

Note: Redirection is supported only for HTTP.

This feature enables Operators to apply the redirection URL configured in Advice Of Charge which is associated with a Rating Group. The PCRF activates a predefined Service Rule configured under Rating Group.

MCC uses the Advice Of Charge configured in the corresponding Rule Group to create the encrypted hardware ID details. MCC applies the AES encryption on the hardware ID and appends the encrypted hardware ID to the redirection URL configured in Advice Of Charge. MCC sends the redirected URL to the UE for redirection.

To add an Aoc Hardware ID Format:

1. Expand **Service Construct** in the tree.
2. Click **Aoc Hardware ID Format**.
3. Configure the parameters as follows:

Table 10-70 Aoc Hardware ID Format Parameters

Parameter	Description
Name	Name of the Aoc Hardware ID Format
Delimiter	Delimiter to be used in formatting the hardware ID information to be appended in the redirection URL.
Encryption Algorithm	Encryption algorithm to be used in formatting the hardware ID information to be appended in the redirection URL.
Encryption Key	Encryption key for encrypted algorithm.
Prepend String	Prepend string for encrypted hardware ID.
Enclosure String	Enclosure string for encrypted hardware ID.

4. Click the **Save** icon.

Application Rule Group (MCC versions prior to 8.4)

Acuitas does not support this object for MCC 8.4 and later releases. It has been replaced by Protocol Application Rule Group. See Protocol Application Rule Group (8.4 and later MCC version).

The Application Rule Group defines layer 7 applications, protocols, and subprotocols for Signature Analysis by detecting deterministic and/or heuristic patterns in bidirectional packet flow. Signature Analysis is the key technology that enables Workflow to control application of advanced services on subscriber traffic (such as charging, per-application filtering, QOS, and so on).

An Application Rule Group can select only:

- Applications whose underlying protocols are selected in the Deep Packet Inspection service construct.
- Protocols that are selected in the Deep Packet Inspection service construct.
- Sub protocols whose corresponding protocol is also selected in the Application Rule Group.

(See Deep Packet Inspection (MCC versions prior to 8.4).)

To add an Application Rule Group:

1. Expand **Service Construct** in the tree.
2. Click **Application Rule Group**.
3. Configure the parameters as follows:
   - **Name** – Enter an Application Rule Group name.
   - **Applications** – Mark the checkbox(es) to select the Application(s) to include in the Application Rule Group.
   - **Protocols** – Mark the checkbox(es) to select the protocol(s) to include with the Application Rule Group. To select all protocols in a category, mark the **all-*category*-protocols** checkbox.
   - **Subprotocols** – Mark the checkbox(es) to select the subprotocol(s) to include with the Application Rule Group.

   Application Rule Group applications, protocols, and subprotocols are listed in the following table:
4. Click the **Save** icon.

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Applications	■ Facebook Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) – Jabber (in Instant Messaging category) ■ MagicJack Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) – SIP (in Voice Over IP category) ■ iTunes Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ MySpace Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ FaceTime Detected using underlying protocols: – SIP (in Voice Over IP category) ■ TruPhone Detected using underlying protocols: – HTTP (in Web category) – SIP (in Voice Over IP category) – Jabber (in Instant Messaging category) ■ Twitter Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ WindowsMedia Detected using underlying protocols: – HTTP (in Web category) ■ Xbox Detected using underlying protocols: – HTTP (in Web category) – XBOX (in Gaming category) ■ RealMedia Detected using underlying protocols: – HTTP (in Web category) ■ Gmail Detected using underlying protocols: – SSL (in Tunnel category) – Jabber (in Instant Messaging category) ■ Goober Detected using underlying protocols: – SIP (in Voice Over IP category) – Goober (in Voice Over IP category) ■ Blackberry Detected using underlying protocols: – HTTP (in Web category) – Blackberry (in Mobile category) ■ iCloud Detected using underlying protocols: – SSL (in Tunnel category) ■ UbuntoOne Detected using underlying protocols: – SSL (in Tunnel category) ■ DropBox Detected using underlying protocols: – SSL (in Tunnel category) ■ GoogleDocs Detected using underlying protocols: – SSL (in Tunnel category) ■ Yuilop Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) – Jabber (in Instant Messaging category) ■ iMessage Detected using underlying protocols: – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ GoToMyPC Detected using underlying protocols: – CitrixGoTo (in Conference category) ■ GoToMeeting Detected using underlying protocols: – CitrixGoTo (in Conference category) ■ WindowsAzure Detected using underlying protocols: – SSL (in Tunnel category) ■ AmazonCloud Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ DailyMotion Detected using underlying protocols: – HTTP (in Web category) ■ Deezer Detected using underlying protocols: – HTTP (in Web category) ■ Grooveshark Detected using underlying protocols: – HTTP (in Web category) ■ Sudaphone Detected using underlying protocols: – SIP (in Voice Over IP category) – Sudaphone (in Voice Over IP category) ■ Office365 Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ CnTV Detected using underlying protocols: – HTTP (in Web category) ■ SinaTV Detected using underlying protocols: – HTTP (in Web category) ■ Youtube Detected using underlying protocols: – HTTP (in Web category) ■ VoipSwitch Detected using underlying protocols: – SIP (in Voice Over IP category) ■ Zynga Detected using underlying protocols: – SSL (in Tunnel category) ■ CrimeCity Detected using underlying protocols: – HTTP (in Web category) ■ ModernWar Detected using underlying protocols: – HTTP (in Web category) ■ Vippie Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Box Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ SkyDrive Detected using underlying protocols: – SSL (in Tunnel category) ■ AdobeCreativeCloud Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Linkedin Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Orkut Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ Hi5 Detected using underlying protocols: – HTTP (in Web category) ■ Soribada Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ ZohoWorkOnline Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Hotmail Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Instagram Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Sugersync Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Wickr Detected using underlying protocols: – HTTP (in Web category) ■ Tigertext Detected using underlying protocols: – SSL (in Tunnel category) – Jabber (in Instant Messaging category) ■ Vibe Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Enlegion Detected using underlying protocols: – HTTP (in Web category) ■ Voxer Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Lovefilm Detected using underlying protocols: – HTTP (in Web category) ■ Friendster Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Burner Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ Flickr Detected using underlying protocols: – HTTP (in Web category) ■ LiveCom Detected using underlying protocols: – SSL (in Tunnel category) – HTTP (in Web category) ■ ICQWebChat Detected using underlying protocols: – HTTP (in Web category) ■ RedTube Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EverNote Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Spreed Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
(Continued)	■ TextPlus Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ XVideos Detected using underlying protocols: – HTTP (in Web category)	■ SnapChat – HTTP (in Web category) – SSL (in Tunnel category)
Applications2 *(additional applications)*	■ Youku Detected using underlying protocols: – HTTP (in Web category) ■ MyMusicTW Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Renren Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Yelp Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AmazonShop Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ none ■ Youporn Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ eBay Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Pornhub Detected using underlying protocols: – HTTP (in Web category)	■ SpiderOak Detected using underlying protocols: – SSL (in Tunnel category) ■ Adrive Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Tumbler ■ Xing ■ GooglePlayMusic ■ Vimeo ■ SalesForce ■ iTunesRadio ■ SinaWeibo ■ Forfone ■ LiveJasmin Detected using underlying protocols: – HTTP (in Web category) ■ JingDong Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IMS Detected using underlying protocols: – SIP (in Voice Over IP category) ■ Baidu Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ TaoBao Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Whatchever Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TTPOD Detected using underlying protocols: – HTTP (in Web category) ■ Three60Mobile Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Pinterest Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Vine Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Net2Phone Detected using underlying protocols: – HTTP (in Web category) ■ FourSquare Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iLiveTo Detected using underlying protocols: – HTTP (in Web category) ■ MEGA Detected using underlying protocols: – HTTP (in Web category) ■ DOOOK Detected using underlying protocols: – HTTP (in Web category) ■ vBulletin Detected using underlying protocols: – HTTP (in Web category) ■ CloudMe Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ YikYak Detected using underlying protocols: – SSL (in Tunnel category) ■ RedMine Detected using underlying protocols: – HTTP (in Web category) ■ iHeartRadio Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AviraAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ NortonAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ KasperskyAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ AVGAntivirus Detected using underlying protocols: – HTTP (in Web category) ■ SoundCloud Detected using underlying protocols: – SSL (in Tunnel category) ■ RDIO Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ AmazonPrimeMusic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RunKeeper Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyBook Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NikePlus Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MAGV Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MAGVKids Detected using underlying protocols: – HTTP (in Web category) ■ DotaLegend Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LETV Detected using underlying protocols: – HTTP (in Web category) ■ MyFitnessPal Detected using underlying protocols: – SSL (in Tunnel category) ■ SOHU Detected using underlying protocols: – HTTP (in Web category) ■ OneKXUN Detected using underlying protocols: – HTTP (in Web category) ■ TVBS Detected using underlying protocols: – HTTP (in Web category) ■ XNXX Detected using underlying protocols: – HTTP (in Web category) ■ CTITV Detected using underlying protocols: – HTTP (in Web category) ■ Endomondo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TimelyTV Detected using underlying protocols: – HTTP (in Web category) ■ WorkoutTrainer Detected using underlying protocols: – HTTP (in Web category) ■ MapMyRun Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Applications3 *(additional applications)*	■ KingOfPirates Detected using underlying protocols: – HTTP (in Web category) ■ TUDOU Detected using underlying protocols: – HTTP (in Web category) ■ Duokan Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MeiLu Detected using underlying protocols: – HTTP (in Web category) ■ Skout Detected using underlying protocols: – HTTP (in Web category) ■ playTales Detected using underlying protocols: – HTTP (in Web category) ■ GameOfWar Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FETnet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FBS Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NationalBaseball Detected using underlying protocols: – HTTP (in Web category) ■ PinkFong Detected using underlying protocols: – HTTP (in Web category) ■ KollectBook Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SPTGTV Detected using underlying protocols: – HTTP (in Web category) ■ CiaomobileHDTV Detected using underlying protocols: – HTTP (in Web category) ■ SkyKing Detected using underlying protocols: – HTTP (in Web category) ■ Moves Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Path Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iWowSystext Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NineKU Detected using underlying protocols: – HTTP (in Web category) ■ NextTV Detected using underlying protocols: – HTTP (in Web category) ■ Syncplicity Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ RealMa Detected using underlying protocols: – HTTP (in Web category) ■ Yuanta Detected using underlying protocols: – HTTP (in Web category) ■ HiNet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyCard Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ KONO Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Speakaboos Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DuoDuo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ WealthGod Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iLeader Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ threeBamboo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Taaze Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Audiko Detected using underlying protocols: – HTTP (in Web category) ■ pubuBookbuffet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MiTake Detected using underlying protocols: – HTTP (in Web category) ■ HyRead Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DisneyStoryTime Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Qualys Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ConstantContact Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Rally Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Intralinks Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ AppleMusic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Naver Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ BookingCom Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ CNN Detected using underlying protocols: – HTTP (in Web category) ■ PayEasy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LineRangers Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IOSAppStore Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyVideo Detected using underlying protocols: – HTTP (in Web category) ■ KingGaming Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ CandyCrush Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ CandyCrushSoda Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ BubbleWitch Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FarmHero Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ WindowsStore Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MineCraft Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Meerkat Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RovioGaming Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AngryBirds Detected using underlying protocols: – HTTP (in Web category) ■ CitrixXenApp Detected using underlying protocols: – HTTP (in Web category) ■ Redditt Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
(Continued)	■ PayPal Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PlantsVsZombies2 Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)	■ HalfbrickStudios Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)
Applications4 *(additional applications)*	■ gitHub Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ HamiVideo Detected using underlying protocols: – HTTP (in Web category) ■ Slacker Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NicoNico Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AliPay Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ UStream Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NttDocomo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Softbank Detected using underlying protocols: – HTTP (in Web category)	■ TrendMicroWorryFree Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Wikipedia Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Uber Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Yandex Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ VK Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Alibaba Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AliExpress Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ TMall Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NortonSecurity (Supplants NortonAntivirus) Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PochtaRossii Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AfterSchool Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DriveLock Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ QipRu Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MusicalLy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EAGames Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iTunesU Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PopCap Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SurveyMonkey Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NewRelic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Huddle Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ZenDesk Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ OutlookMobile Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Dena Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ BackBlaze Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DocuSign Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ BetterNet Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Good ■ AngHami Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Slack Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ PokemonGo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NianticLabs Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TwoGIS Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RuTube Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TwoChannel Detected using underlying protocols: – HTTP (in Web category) ■ Prisma Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AmazonPrimeVideo (Supplants Lovefilm) Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Signal Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ KanKan Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Azar ■ SkyGo ■ iCrypt Detected using underlying protocols: – SSL (in Tunnel category) ■ Kinopoisk Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IviRu ■ Tinder Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AnyDesk Detected using underlying protocols: – SSL (in Tunnel category) ■ Tenor Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ APNS Detected using underlying protocols: – HTTP (in Web category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ DigicelPlayGo Detected using underlying protocols: – SSL (in Tunnel category) ■ DigicelMusic Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DigicelTopUp Detected using underlying protocols: – HTTP (in Web category) ■ Dubsmash Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MyDigicel Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Waze Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ChannelOne Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Giphy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Imgur Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Applications5 *(additional applications)*	■ OneDrive Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ iFlix Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AppleServices Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MicrosoftServices Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ IcFlix Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LogMeIn Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Shazam Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TuneInRadio Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Badoo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AirBnB Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ HighTail Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EasyTaxi Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TomTom Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ TripAdvisor Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ ESPN Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ DAZN Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MobileStrike Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ KingOfAvalon Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Lineage2 Detected using underlying protocols: – HTTP (in Web category) ■ Lyft Detected using underlying protocols: – HTTP (in Web category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ Trulia Detected using underlying protocols: – HTTP (in Web category) ■ AkamaiCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LimelightCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ NickelodeonPlay Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Here Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SimcityBuildit Detected using underlying protocols: – HTTP (in Web category) ■ StarwarsGOH (Galaxy of Heroes) Detected using underlying protocols: – SSL (in Tunnel category) ■ Fastly Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Cloudflare Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LifeChurch Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Vevo Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Grindr Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AppleMaps Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AppleGeolocation Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ YoukuTudou Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MeeticGroup Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Sarahah Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Vudu Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Wish Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ Auth0 Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ SlingTV Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ RackspaceCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ StackpathCloud Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ HouseParty Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LearningHubOnline Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ FoxSports Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ AmazonServices ■ AmazonDrive ■ Crashlytics Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LoopTradeClassifieds Detected using underlying protocols: – HTTP (in Web category) ■ LoopCaribbeanLocalNews Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ LoopPacificLocalNews Detected using underlying protocols: – HTTP (in Web category) ■ Unity Detected using underlying protocols: – SSL (in Tunnel category) ■ Mapbox Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Cedexis Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Smule Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ Symantec Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ MaxDome Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category) ■ EpicBrowserProxy Detected using underlying protocols: – HTTP (in Web category) – SSL (in Tunnel category)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Business	■ all-business-protocols ■ AdobeConnect ■ Citrix ■ ActiveSync ■ JBK3000 ■ Lync Subprotocols: – audio – video – file-transfer ■ SAP ■ UltraBac ■ Fix ■ LicenseExceeded ■ LotusNotes ■ MSexchange Subprotocols: – generic – owa ■ MSNav ■ FUZE ■ KaKao Subprotocols: – generic – kakaoTalk ■ SkypeForBusiness Subprotocols: – generic – audio – video – file-transfer ■ SCADA ■ CrashPlan ■ S7Comm ■ Amazon Subprotocols: – services – chime – cloud – drive – primeMusic – primeVideo – shop ■ Bitcoin ■ Synology ■ StratumMining
Conference	■ all-conference-protocols ■ CitrixGoTo ■ Webex ■ ooVoo
Database	■ all-database-protocols ■ MySQL ■ PostgreSQL ■ TDS ■ msSQL ■ OracleDB ■ CQL (Cassandra Query Language) ■ CIC (Cassandra Intermode Communication)

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
File Transfer	■ all-file-transfer-protocols ■ AFP ■ DirectDownloadLink ■ FTP Subprotocols: – control – data ■ NFS ■ SMB-CIFS ■ TFTP ■ WebDAV ■ HiDrive	■ osUpdate Subprotocols: – Android – iOS – WindowsPhone – MSWindows – Chrome ■ DCE-RPC ■ IDRIVE ■ FLUTE ■ Rsync
Flow *(Operating system of the individual flow. May differ from the subscriber operating system if from a tethered device)*	■ Windows-Desktop ■ Windows ■ Linux ■ MacOS ■ iOS ■ Symbian ■ Android ■ Blackberry	■ WindowsMobile ■ WindowsPhone ■ Tethered – true (indicates this flow is sourced from a tethered device) – false

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
Gaming	■ all-gaming-protocols	■ rFactor
	■ Armagetron	■ Dota2
	■ Battlefield	■ Tibia
	■ ClubPenguin	■ Destiny
	■ CrossFire	■ AgeOfWarringEmpire
	■ Dofus	■ PlayStation
	■ Fiesta	■ SuperCell
	■ Florensia	Subprotocols:
	■ GameKit	– generic
	■ Guildwars	– clashOfClans
	■ QQGame	– boomBeach
	■ Halflife2	– hayDay
	■ MapleStory	– ClashRoyale
	■ PS3	■ LeagueOfLegends
	■ Quake	■ Battlenet
	■ SecondLife	■ GuildWars2
	■ SplashFighter	■ EAOrigin
	■ Steam	■ PathOfExile
	■ WARCRAFT3	■ NintendoNetwork
	■ Wii	■ Lineage2
	■ WorldOfKungFu	■ Minecraft
	■ WorldOfWarcraft	■ Zynga
	■ Xbox	■ EpicGames

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Instant Messaging	■ all-im-protocols ■ GaduGadu Subprotocols: – server – file-transfer – voice – video ■ GoogleTalk Subprotocols: – voice – file-transfer – video ■ IMO ■ IMplus ■ IRC Subprotocols: – file-transfer ■ Nimbuzz ■ Jabber Subprotocols: – voice – file-transfer – video – encrypted ■ MEEBO Subprotocols: – audio – video ■ MSN Subprotocols: – voice – file-transfer – video – webchat ■ MSRP ■ Oscar Subprotocols: – file-transfer – picture-transfer – voice – video ■ POPO ■ Pal Talk Subprotocols: – server – file-transfer – voice – video ■ QQ Subprotocols: – voice – file-transfer – video ■ Usenet ■ Whats App Subprotocols: – generic – file-transfer – video-call – voice-call ■ XDCC ■ Yahoo Subprotocols: – voice – file-transfer – video – webchat – webmail ■ eBuddy

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ WeChat Subprotocols: – generic – voice-live-chat – video-call – chat – data-message – web-chat ■ KikMessenger ■ MPlus ■ HikeMessenger ■ Threema ■ Telegram ■ DOOOK ■ BlueJeans ■ Zalo ■ Hangouts Subprotocols: – unknown – audio – file-transfer – video ■ SnapChat ■ Yuilop Subprotocols: – generic – audio ■ IO ■ AIM Subprotocols: – generic – file-transfer ■ ICQ Subprotocols: – generic – file-transfer – audio – video ■ ZeroMQ ■ Signal ■ WireMessenger Subprotocols: – generic – audio – video
Mail	■ all-mail-protocols ■ IMAP Subprotocols: – generic – encrypted ■ Mapi ■ POP Subprotocols: – pop3generic – pop3encrypted ■ SMTP Subprotocols: – generic – encrypted

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
Mobile	■ all-mobile-protocols ■ BOLT ■ Blackberry Subprotocols: – encrypted – email – messenger ■ MMS (MultimediaMessaging) ■ OperaMini ■ WAP-WSP ■ WAP-WTLS ■ WAP-WTP-WSP	■ Mig33 ■ MQTT Subprotocols: – generic – encrypted ■ SCADA ■ Instagram Subprotocols: – generic – video – file-transfer – chat
Network Management	■ all-network-management-protocols ■ BGP ■ DHCP ■ DHCPv6 ■ DNS ■ EGP ■ ICMP ■ ICMPv6 ■ IGMP ■ IPP ■ Kerberos ■ LDAP Subprotocols: – generic – encrypted ■ LDP ■ MulticastDNS ■ NETBIOS ■ NTP ■ OSPF	■ SCTP ■ SNMP ■ SSDP ■ Syslog ■ RSVP ■ NetFlow ■ iPerf ■ Diameter ■ TACACS ■ NTLM Subprotocols: – plain – encrypted ■ WHOIS ■ RADIUS ■ Megaco ■ SpeedTest ■ T3 ■ OpenFlow ■ IPMI ■ IPFix

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols	
Peer to Peer	■ all-p2p-protocols ■ ANtsP2P ■ Aimini ■ AppleJuice ■ Ares ■ BitTorrent Subprotocols: – plain – encrypted – utp – utp-encrypted ■ DirectConnect Subprotocols: – hub – peer – adc-peer ■ Filetopia ■ Gnutella ■ KaZaa-Fasttrack	■ Manolito ■ Mojo ■ Mute ■ OFF ■ OpenFT ■ Pando ■ Soulseek ■ StealthNet ■ Thunder-Webthunder ■ WINNY ■ WinMX ■ eDonkey Subprotocols: – plain – encrypted ■ iMesh ■ FreeNet ■ LocalPeerDiscovery
Remote Control	■ all-remote-control-protocols ■ PCAnywhere ■ RDP ■ SSH ■ Skinny ■ TeamViewer ■ Telnet Subprotocols: – generic – tn3270 ■ VNC ■ XDMCP ■ PoisonIvy ■ SOAP	■ IEC61850 Subprotocols: – goose – MMS – SMV ■ PCOverIP ■ ModBus ■ OpcUa ■ DNP3 ■ BACnet ■ Zero ■ CoAP

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Social Networking	■ all-social-networking-protocols ■ Runtastic ■ StreetVoice ■ LivePerson ■ Facebook Subprotocols: – video – encrypted – chat – file-transfer – generic – audio ■ Odnoklassniki ■ MailRu
Standard	■ all-standard-protocols ■ thrift ■ Fasp

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Streaming	■ all-streaming-protocols ■ avi ■ FLASH ■ Feidian ■ Funshion ■ VeohTV Subprotocols: – generic – flash ■ IPTV ■ Icecast ■ Kontiki ■ MicrosoftMediaServer ■ MPEG ■ Move ■ NetFlix Subprotocols: – generic – video ■ OGG ■ ORB Subprotocols: – server – client – client-rtsp – client-rdt – client-wmv – client-wma – client-flash – client-flv – client-3gp – client-upload-download – client-rtp ■ Octoshape ■ PPLIVE Subprotocols: – generic – video ■ PPSTREAM ■ Pandora ■ QQLive ■ QUICKTIME ■ REALMEDIA ■ RTCP ■ RTP ■ RTSP ■ RealDataTransport ■ SOPCAST ■ Shoutcast ■ Slingbox ■ Spotify ■ TVANTS ■ TVUPLAYER ■ UUSEE ■ Vcast ■ WINDOWSMEDIA ■ ZATTOO ■ iPlayer ■ AudioGalaxy ■ Rhapsody ■ Silverlight ■ ITV Subprotocols: – web – stream ■ Demand5 Subprotocols: – web – stream ■ Channel4oD ■ MyVideo Subprotocols: – web – stream ■ Spreecast ■ SIMFY ■ QVOD ■ HULU

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
(Continued)	■ TWITCH ■ WOWZA ■ MagineTV ■ Periscope ■ SRTP ■ SRTCP ■ PPFilm ■ LeTV
Subscriber *(Operating system of the user equipment device)*	■ Windows-Desktop ■ Windows ■ Linux ■ MacOS ■ iOS ■ Symbian ■ Android ■ Blackberry ■ WindowsMobile ■ WindowsPhone
Tunnel	■ all-tunnel-protocols ■ GRE ■ GTP Subprotocols: – control – user-data – prime ■ HamachiVPN ■ IP-in-IP ■ IPSEC Subprotocols: – data – control ■ ISAKMP ■ JAP ■ L2TP ■ NetMotion ■ OpenVPN ■ PPP ■ PPTP ■ SSL Subprotocols: – generic – SPDY ■ SSTP ■ SoftEthernet ■ TOR ■ Teredo ■ UltraSurf ■ VPN-X ■ VTUN ■ YourFreedom ■ SOCKS Subprotocols: – v4 – v5 ■ HTTPTunnel ■ PDProxy ■ CyberGhost ■ ComodoUnite ■ VyprVPN ■ Psiphon ■ ZenmateVPN ■ PIA ■ IPVanish ■ TunnelBear ■ ZeroVPN ■ SurfEasy ■ TigerVPN ■ AviraPhantomVPN ■ TurboVPN ■ VPNMaster

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Voice Over IP	■ all-voip-protocols ■ FiCall ■ Fring Subprotocols: – voice – video ■ Goober ■ H323 ■ IAX ■ Iskoot ■ MGCP Subprotocols: – control – rtp ■ MyPeople Subprotocols: – audio ■ SIP Subprotocols: – vonage – oscar – gadu-gadu – oscar-video – ichat-facetime – MagicJack – audio – video – MSN – yahoo – yahoo-video – MPlus – ChatCube ■ STUN ■ Scydo ■ Skype Subprotocols: – voice – out – video – chat – file-transfer ■ Tango Subprotocols: – audio – video – im – file-transfer ■ TeamSpeak ■ TruPhone ■ Ventrilo ■ Viber Subprotocols: – audio – instant-messaging – file-transfer – out – video ■ VoipSwitch ■ Sudaphone ■ Line Subprotocols: – generic – audio – video ■ Didi Subprotocols: – generic – voice – im ■ TunnelVoice ■ Vippie ■ ChatCube ■ Azar ■ FaceTime

Table 10-71 Application Rule Group Settings

Category	Applications/Protocols/Subprotocols
Web	■ all-web-protocols ■ HTTP Subprotocols: – generic – voice – video – media ■ WebSocket ■ Wuala ■ WebQQ ■ SPDY Subprotocols: – ssl ■ Google Subprotocols: – encrypted – cloud – drive – docs – plus – play – generic – mail – youtube – maps – earth – fcm – apis – hangoutsGeneric – hangoutsAudio – hangoutsVideo – hangoutsFileTransfer – ads – allo – duo – analytics – calendar ■ QUIC ■ OCSP

CA Certificate List

The CA Certificate List configures a list of TLS Certificate Authority Certificates used for authenticating certificates of end users or network entities. The list can contain a bundle of certificates. Certificates configured in the list must be present in the /public/content/tls/cacerts/ folder on the MCM.

To add a CA Certificate List:

1. Expand **Service Construct** in the tree.
2. Click **CA Certificate List**.
3. Configure the parameter as follows:
   - **Name** – Enter a TLS CA certificate list name.
4. Click the **Save** icon.
5. Expand **CA Certificate List**.
6. Expand the CA certificate list you added.
7. Click **CA Certificate**.
8. Configure the parameters as follows:
   - **Name** – Enter the Trusted Certificate Authority Root Certificate.
9. Click the **Save** icon.
10. Repeat step 7 through step 9 to add as many CA certificates as needed.

Code Mapping Lists

To add a Code Mapping Lists:

1. Expand **Service Construct** in the tree.
2. Click **Code Mapping Lists**.
3. Configure the parameters as follows:

Table 10-72 Code Mapping Lists Parameters

Parameter	Description
Code Type	Type of code: ■ unused ■ s2b ■ swm ■ s2a ■ sta ■ swm-experimental
GW Name	Gateway using the code
Incoming Code	Incoming code value
Incoming Code Description	Incoming code description
List Name	List name
Outgoing Code	Outgoing code value

4. Click the **Save** icon.

Content Insertion

The HTTP Proxy operates in content-insertion mode on the configurable URL/domain. The Request Policy and HTTP Server instance is associated with a configured Content Insertion Profile. The Content Insertion Profile supports:

- Insertion of local or remote hosted images or videos (such as, advertisements)
- Insertion of externally hosted content on ad server via URL links
- Banners located at the top/bottom of the page or centrally located overlays

For example, Operators can configure a Request Policy with specific domains/URL in order to insert advertisements. The UE attempts to access the specific domain/URL on which a rule is configured for content insertion.

Content insertion is a three stage process:

1. Upon receiving the response from the origin-server, the HTTP Proxy inserts the required javascript link based on the configured Request Policy, Server Instance, and Content Insertion Profile.
2. After the UE receives the HTML page with the inserted javascript link, the UE makes a request to the HTTP proxy for the javascript. The HTTP proxy generates a javascript based on the Content Insertion Profile.
3. The request for assets (either local or remote) contained within the generated Javascript (images, videos, etc.) are served based on the configured Content Insertion Profile.

Insertion Object List

To add a Insertion Object List:

1. Expand **Service Construct** in the tree.
2. Expand **Content Insertion**.
3. Click **Insertion Object List**.
4. Configure the parameters as follows:

Table 10-73 Insertion Object List Parameters

Parameter	Description
Name	Object List name
Admin State	Admin State: ■ enabled ■ disabled

5. In **Insertion Object**, configure the parameter as follows:

Table 10-74 Insertion Object Parameters

Parameter	Description
Name	Object name
Admin State	Enable/disable the insertion object: ■ enabled ■ disabled
Type	Content insertion object type: ■ image ■ link ■ video
Title	Title for the content insertion object
Click Through URL	Specify the click through URL.
Object Location	Object Location: ■ filename ■ URL Enter the filename of the local object or the URL of the remote object.

To add additional insertion objects, click the **Create** icon.

6 Click the **Save** icon.

Content Insertion Profile

To add a Content Insertion Profile:

1 Expand **Service Construct** in the tree.

2 Expand **Content Insertion**.

3 Click **Content Insertion Profile**.

4 Configure the parameters as follows:

Table 10-75 Content Insertion Profile Parameters

Parameter	Description
Name	Profile name
Admin State	Admin State: ■ enabled ■ disabled

5 In **Insertion Object List**, configure the parameter as follows:

- **Name** – Select the insertion object list. The insertion object list must already exist. See Insertion Object List.

To add additional insertion object lists, click the **Create** icon.

6 In **Insertion Style**, in the **Style** field, specify to configure a banner or overlay.

7 For Banner, configure the parameters as follows:

Table 10-76 Banner Parameters

Parameter	Description
Position	Position of the banner: ■ Top ■ Bottom

8 For Overlay, configure the parameters as follows:

Table 10-77 Overlay Parameters

Parameter	Description
Timeout	Specify the number of seconds to keep the overlay
Close Button	Enable/disable the close button: ■ enabled ■ disabled

9 Click the **Save** icon.

Data Record Template

Data Record Template defines the format of a data record. The data record can be a RADIUS message, Diameter message, Charging Data Record (CDR) in local CDR file, or NBR (NAT binding record) in a local file.

The format of a data record is determined by the data fields in the record.

For RADIUS and Diameter data record, Operators can configure whether or not to include the fields (optional AVPs) in the messages.

For CDR record, Operators can configure:

- **Field Delimiter** – Character to use as a delimiter between fields.

  By default, **Field Delimiter** is set to a dot (.)

- **Present Flag** – Whether or not to include the data field in CDR.

  By default, Present Flag is set to conditional for all data fields (data field filled in CDR when available).

For Charging Local record, Operators can also configure:

- **Position Index** – Position where the data field is populated in CDR.

  There is predefined order for each data field if **Position Index** is not configured.

- **Format Type** – Format type of the data field.

  There is default format for each data field, if not configured.

- **Length** – Fixed length of the data field.

  By default, **Length** is set to 0 (the data field is written out as it is).

- **Alignment** – Alignment of the data field.

  It is set to left alignment, if not configured.

- **Padding** – Character used for padding when the field has fixed length.

Deep Packet Inspection (MCC versions prior to 8.4)

Acuitas does not support this object for MCC 8.4 and later releases.

Use this object to enable the deep packet inspection function for protocols detected by Signature Analysis. Signature Analysis is the key technology that enables Workflow to control application of advanced services on subscriber traffic (such as charging, per-application filtering, and so on).

To enable the Deep Packet Inspection function:

1. Expand **Service Construct** in the tree.
2. Click **Deep Packet Inspection**.
3. Configure the parameter as follows:
   - **Admin State** – Set to Enabled.
4. By default, all protocols are enabled for detection.

   The list of selected protocols is used to initialize the DPI detection engine when the fastpath application on the SSM is started or restarted. To reduce the CPU cycles used for DPI detection, you can restrict the set of protocols.

   The Deep Packet Inspection service *cannot* deselect:

   - Underlying protocols of applications that are selected in an Application Rule Group service construct.
   - Protocols that are selected in an Application Rule Group service construct.

   (See Application Rule Group (MCC versions prior to 8.4).)

   To specify individual protocols for detection:

   a. Click a Category.
   b. Mark the checkbox(es) to select the protocol(s) for detection. To select all protocols in a category, mark the **all-*category*-protocols** checkbox.

5. Click the **Save** icon.

Once the deep packet inspection function is enabled, you can view the statistics (bit counters) of the various selected protocols.

Device Database

Use this object to specify device characteristics to configure data services such as data filters used to allow/block traffic for a particular class of devices based on the device-type parameter and also configure differentiated rate-limiting bit rates based on device-type or device screen size.

This feature supports the following device database characteristics: TAC (Type Allocation Code), device-type, make (or brand), model, screen-width, and screen-height. The TAC information is extracted from the first 8 digits of the 15/16 digit IMEI. The device-type field indicates the type of device that corresponds to a particular TAC. Options include: handheld, feature-phone, smart-phone, modem, dongle, tablet, vehicle, connected-device, router, module, ebook, and femto-app.

The device database is in CSV format and must be previously imported into MCC. MCC obtains the database attributes during session establishment. The device database contains a mapping of the TAC of a device to its specific parameters. The database is either the GSMA device map or a modified version of the GSMA device map and may also contain a subset of GSMA device map fields.

The following guidelines apply to this feature:

- The device database must be in CSV format.
- The first line in the CSV file must contain the field names (as MCC uses this information for parsing). The files are stored in MCC.
- The header information is case sensitive.
- MCC supports a maximum of 300,000 database entries.
- If the database is modified, the existing session's values are not changed.
- The database supports a single level of lookup.

The session rule group is used for service rule matching, based on device parameters (see Session Rule Group).

To add a Device Database:

1. Expand **Service Construct** in the tree.
2. Click **Device Database**.
3. Configure the parameters as follows:

Table 10-78 Device Database Parameters

Parameter	Description
Name	Device database name

Table 10-78 Device Database Parameters

Parameter	Description
Import From	Specifies to import from: ■ **Import from server**: references a device database file to be imported from a file server and configures a rule for importing the file. ■ **Import from local file**: references a file name for importing the device database file on local directory. The file should be in the following directory: /tosdb/content/policylists/<*list-type*>/' If you make changes to the file, you must import the file to rebuild the database for the new file to take effect. For import instructions, see Import Command.
Filename	Filename containing the device database (such as folder/file-${DATE:yyyymmdd}.txt)
File Download Profile	Select the File Download Profile that defines parameters for importing the device database from a file server. The File Download Profile must already exist. See File Download Profile.
CSV Field Names	
TAC	Configure a string to indicate the name of the TAC field
Device Type	Configure a string to indicate the name of the device-type field
Make	Configure a string to indicate the name of the make (brand) field
Model	Configure a string to indicate the name of the model field
Screen Width	Configure a string to indicate the name of the screen width field
Screen Height	Configure a string to indicate the name of the screen height field

4 Click the **Save** icon.

Import Command

To manually import the Device Database:

1 Click the Device Database you added.

2 Configure the parameters as follows:

- **Device Database Command** – Select **Import** and click **Select**.

3 Mark the checkboxes to disable alarm notification and/or a log entry if the import fails and click **Execute**.

Device Database Statistics

To view Device Database statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Device Database Stats**.
3. Click **Summary**.

   Acuitas lists the download Summary for each Device Database, including:

   - Import File Name
   - Last Import File Size(Bytes)
   - Last Import Number
   - Last Import Resultt: Success or N/A
   - Last Import Time
   - Import Typee: manual or scheduled
   - Device database name
   - Next Scheduled Import Time
   - Number Of Accepted Entries
   - Number Of Rejected Entries
4. Expand **Import History**.
5. Click the Device Database.

   Acuitas lists the Import History for all the retained Device Database downloads, including Device database name and result.
6. Expand **Detail**.
7. Click the Device Database.

   Acuitas lists the Detail for the Device Database download, including:

   - Accepted Entries
   - Import File Name
   - Last Import File Size(Bytes)
   - Last Import Number
   - Last Import Resultt: Success or N/A
   - Last Import Time
   - Import Type: manual or scheduled
   - Device-Database name
   - Next Scheduled Import Time
   - Number Of Accepted Entries

- Number Of Rejected Entries
- Rejected Entries

DHCP Local Server Profile

To add a DHCP Local Server Profile:

1. Expand **Service Construct** in the tree.
2. Expand **Control Service Profile**.
3. Click **DHCP Local Server Profile**.
4. Configure the parameters as follows:

Table 10-79 DHCP Local Server Profile Parameters

Parameter	Description
DHCP Server Name	DHCP Server profile
Local Server IP Address	IP Address of the local DHCP server
Lease Timer	Lease timer
Primary DNS IP Address	Primary DNS IP address
Secondary DNS IP Address	Secondary DNS IP address
Interface MTU	Interface MTU
Router IP Address	Router IP address
Subnet Mask	Subnet mask
Prior Subscriber IP Binding Timer	Time (in minutes) to retain the last assigned IP binding even after the session is deleted. If the session is re-established before the timer expires, the same IP Address is assigned. Once the timer expires, the IP Address is released.
Broadcast Address	Broadcast IP address.

5. Click the **Save** icon.

DHCP Local Server Statistics

To view DHCP Local Server Statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Control Service Profile**.
3. Expand **DHCP**.
4. Expand **Local Server Statistics**.

5 Click **All**.

Statistics parameters are:

- Discovers Received
- Requests Received
- Releases Received
- Unsupported Messages Received
- Message Options Decode Errors Received
- Server Id Option Decode Errors Received
- Requested Ip Option Decode Errors Received
- Lease Time Option Decode Errors Received
- Receive Errors
- Offers Transmitted
- Declines Transmitted
- Acks Transmitted
- Nacks Transmitted
- Transmit Errors

DHCP Mapping Template

The DHCP Mapping template allows Operators to customize incoming and outgoing DHCP messages when the MCC TWAG is operating as a DHCP relay agent or as a DHCP server. With the DHCP Mapping template, Operators can customize the DHCP options contained within DHCP messages.

The DHCP Mapping template can be applied at the TWAG RADIUS Client Session Learner interface-level or at the DHCP Trigger Tunnel interface-level. The system applies the template at the DHCP Trigger Tunnel interface-level first and if there is no template at the DHCP Trigger Tunnel interface-level, the system applies the template at the TWAG RADIUS Client interface-level.

To add a DHCP Mapping Template:

1 Expand **Service Construct** in the tree.

2 Expand **DHCP Mapping**.

3 Click **Template**.

4 Configure the parameter as follows:

- **Name** – DHCP Mapping Template name.

5 Click the **Save** icon.

6 To add DHCP attribute, expand the DHCP Mapping Template you added.

7 Click **Attribute**.

8 Configure the parameters as follows:

Table 10-80 Attribute Parameters

Parameter	Description
Name	The name of the DHCP attribute to be modified. Any DHCP Option from 1 to 255 is configurable, with the following exceptions: ■ 1 – DHCP_OPTION_SUBNET_MASK ■ 3 – DHCP_OPTION_ROUTER ■ 6 – DHCP_OPTION_DNS_SERVER ■ 12 – DHCP_OPTION_HOST_NAME ■ 15 – DHCP_OPTION_DOMAIN_NAME ■ 26 – DHCP_OPTION_INTERFACE_MTU ■ 28 – DHCP_OPTION_BROADCAST_ADDRESS ■ 50 – DHCP_OPTION_REQUESTED_IP ■ 51 – DHCP_OPTION_IP_LEASE_TIME ■ 53 – DHCP_OPTION_MESSAGE_TYPE ■ 54 – DHCP_OPTION_SERVER_ID ■ 55 – DHCP_OPTION_PARAM_REQ_LIST ■ 58 – DHCP_OPTION_IP_RENEWAL_TIME ■ 59 – DHCP_OPTION_IP_REBINDING_TIME ■ 61 – DHCP_OPTION_CLIENT_IDENTIFIER ■ 120 – DHCP_OPTION_PCSCF_ADDRESS ■ 255 – DHCP_OPTION_END

Table 10-80 Attribute Parameters

Parameter	Description
From	The value of the specified session data item will replace the value of the outgoing DHCP attribute: ■ apnname ■ imei ■ imsi ■ macaddr ■ macaddr_1colon ■ macaddr_2colon ■ macaddr_colon ■ macaddr_hyphen ■ msisdn ■ nai ■ nil – Use to exclude a DHCP option from an outgoing or incoming DHCP message. ■ tunnellocalip ■ tunnelremoteip ■ user1, user2, user3, user4, user5, user6, user7, user8, user9, user10 Use **user1**, **user2**, **user3**, **user4**, **user5**, **user6**, **user7**, **user8**, **user9**, or **user10** to allow an incoming template to save a value from a DHCP option and pass it on to a DHCP option in an outgoing template.
From Format	Specifies a substitution string to replace the value of the specified session data in the outgoing DHCP attribute into a text string. Use "$*item*" to identify the session data item. In special cases, you can use "$$" to substitute a "$" character. Use the form "${item}" to identify the session data item if "$item" is followed by alphanumeric text. Enclose the substitution string in double quotation marks. Example: **From Format** `"imsi=$imsi,user=$nai"` This example substitutes the session IMSI and NAI with the resulting value. If the IMSI is "12345678901234" and the NAI is "foo@mytest.org", the resulting value of the attribute would be "imsi=12345678901234,user=foo@mytest.org".

Table 10-80 Attribute Parameters

Parameter	Description
To	The value of the specified session data item will be set using the value from the incoming RADIUS attribute: ■ apnname ■ imei ■ imsi ■ macaddr ■ msisdn ■ nai ■ nil – Use to exclude an attribute from an outgoing or incoming RADIUS message. ■ tunnellocalip ■ tunnelremoteip ■ user1, user2, user3, user4, user5, user6, user7, user8, user9, user10 Use **user1**, **user2**, **user3**, **user4**, **user5**, **user6**, **user7**, **user8**, **user9**, or **user10** to allow an incoming template to save a value from an attribute and pass it on to an attribute in an outgoing template.
To Format	Specifies the regular expression (PCRE) pattern to match against the incoming RADIUS attribute. The regular expression must have match groups surrounded by parentheses to select the text to be extracted from the incoming RADIUS attribute. Each match group is set in the session data items specified in the **To List** parameter in the order listed. Enclose the regular expression in double quotation marks. Example: **To Format** `“imsi=(.*),user=(.*)”`
To List	Specifies the name of the session data items in which to store the extracted values. If more than one data item is listed, the session data names must be contained within square brackets. Each match group specified in the `to-format` parameter is set in the session data items in the order listed in the **To List**. Example: **To Format** `“imsi=(.*),user=(.*)”` **To List** `[imsi nai]` The system takes the incoming attribute value of “imsi=12345678901234,user=foo@mytest.org” and stores the IMSI value of 12345678901234 and NAI value of “foo@mytest.org in the session’s data. ***Note:*** *If the number of match groups found does not equal the number of items in the* **To List** *parameter, the system does not modify the session data for the specified DHCP attribute.*

9 Click the **Save** icon.

If the **From** or **From Format** setting fails, the attribute is removed from the outgoing DHCP message.

If the **To** or **To Format**/**To List** setting fails, the system records the failure in the statistics.

Once you have configured the DHCP Mapping template, you need to associate the template with a TWAG RADIUS Client Session Learner interface and a DHCP message type. You can apply the DHCP Mapping template at the TWAG RADIUS Client Session Learner interface-level or at the DHCP Trigger Tunnel interface-level.

The system applies the template at the DHCP Trigger Tunnel interface-level first and if there is no template at the DHCP Trigger Tunnel interface-level, the system applies the template at the TWAG RADIUS Client interface-level.

DHCP Mapping Template Statistics

To view DHCP Mapping Template statistics:

1 Expand **Service Construct** in the tree.

2 Expand **DHCP Mapping**.

3 Expand **Statistics**.

4 Click an instance.

The following statistics are available:

Num Outgoing Replacements	Total number of outgoing replacements
Num Outgoing Removals	Total number of outgoing attributes removed (from nil)
Num Outgoing Format Substitutions	Number of outgoing substitutions using from-format
Num Outgoing Replacement Failures	Number of outgoing replacement failures
Num Incoming Replacements	Total number of incoming replacements
Num Incoming Removals	Total number of incoming attributes removed (to nil)
Num Incoming Matches	Number of incoming matches using to-format
Num Incoming Match Failures	Number of match failures using to-format
Num Incoming Replacement Failures	Number of incoming replacement failures

Diameter Result Code Policy List

Use this object to configure the Mobile Content Cloud (MCC) to take specific action based on the result code received in the Credit-Control-Answer (CCA) message over the Gy interface. Operators have the ability to configure actions per subscriber-type (home/roaming/both) and to separate actions for Diameter result codes received in the CCA message at the Multiple-Services-Credit-Control (MSCC) level and at the command level. Operators can also specify whether the PGW/GGSN retransmits the request to a secondary server before applying the configured action.

To add a Diameter Result Code Policy List:

1. Expand **Service Construct** in the tree.
2. Click **Diameter Result Code Policy List**.
3. Configure the parameters as follows:
   - **Name** – Enter the Diameter Result Code Policy List name.
4. In **Policy**, configure the parameters as follows:

Table 10-81 Policy Parameters

Parameter	Description
Range Name	Range name.
Retry Secondary *(Applies to command-level result codes only)*	Specifies whether the PGW/GGSN retransmits the request to a secondary server before applying the configured action. ■ enabled – (default) When the primary server returns a command-level result code within the configured range, the PGW retransmits the request to a secondary server before applying the configured action. ■ disabled – When the primary server returns a command-level result code within the configured range, the PGW applies the configured action without retransmitting the request to the secondary server.
Subscriber Type (*Applies to the Gy interface only*)	Specifies the type of subscriber to which the configured action is applied. ■ home ■ roaming ■ both The home/roaming subscriber status is based on the home/roaming PLMN ID lists configured on the PGW/GGSN. A subscriber is classified as *roaming* if the serving node PLMN ID is part of the roaming PLMN ID list. If the serving PLMN ID is not found in either the roaming or home PLMN ID lists, the PGW/GGSN uses the value configured in the **Default Gtp Peer Classification** parameter in the Zone > *name* > Gateway > Profile > Gateway Common to determine the home/roaming subscriber status.

Table 10-81 Policy Parameters

Parameter	Description
Result Code Range	Specifies the low and high end of the result code range. ■ low ■ high ***Note:*** *Ensure the result code range does not overlap with any previously configured ranges.* ***Note:*** *To configure a range with a single result code, configure the low and high value with the same code.*
Action (*Applies to the Gy interface only*)	Specifies the action that the PGW/GGSN takes when the result code received in the CCA message is within the configured range. **Actions for command-level result codes:** ■ block – Block all online rating groups for the subscriber that are in active/blocked states. Online rating groups that have not been activated will not be set to blocked. ■ default-action – The system treats all CCA error result codes as temporary failures. If the OCS returns a CCA error message (result code other than 2001) at the command level, the message is retransmitted and the default quota may be applied and the Gy rejoin timer started based on the configuration. In this case, the PGW/GGSN does not process the OCS response. ■ redirect – Redirect traffic to the configured URL for all online rating groups that are in active/blocked states. Online rating groups that have not been activated will not be set to redirect. Specify the Redirect URL. ■ terminate – Terminate the session immediately. If the PGW/GGSN receives a CCA error message (result code other than 2001) at the command level and if the Service Construct > Interface > Online Charging > Command Level Result Code Policy List is configured but the result code is not in the list, the PGW terminates the session. The Command Level Result Code Policy List overrides the Mscc Command Level Result Code Policy List

Table 10-81 Policy Parameters

Parameter	Description
Action *(Continued)* (*Applies to the Gy interface only*)	**Actions for MSCC-level result codes:** ■ block – Block all traffic for a specific rating group immediately regardless of the quota allocated for the rating group. The Final-Unit-Action AVP within the MSCC AVP is ignored. ■ default-action – If the OCS returns a CCA error message (result code other than 2001) at the MSCC level, the gateway executes the action indicated in the Final-Unit-Action (FUA) AVP if set to REDIRECT or RESTRICT-ACCESS. If the FUA is set to TERMINATE or the CCA does not contain the FUA AVP, then all traffic for the rating group is blocked. Also, the Used-Service-Units received in the MSCC AVP are ignored. ■ redirect – Redirect traffic to the configured URL for a specific rating group immediately regardless of the quota allocated for the rating group. The Final-Unit-Action AVP within the MSCC AVP is ignored. Specify the Redirect URL. ■ terminate – Terminate the session immediately regardless of the quota allocated for the rating group. The Final-Unit-Action AVP within the MSCC AVP is ignored. If the PGW/GGSN receives a CCA error message (result code other than 2001) at the MSCC-level and if the Service Construct > Interface > Online Charging > MSCC Level Result Code Policy List is configured but the result code is not in the list, the PGW processes subscriber traffic for the specific rating group using the default-action option. The Mscc Command Level Result Code Policy List is only considered when the command-level result code is 2001.
To add additional Policies, click the **Create** icon.	

5 Click the **Save** icon.

DHCP Service Profile

Use this object to obtain the NBNS and/or the DNS configuration from the external DHCP Server for subscribers configured to use a DHCP Client.

To add a DHCP Service Profile:

1. Expand **Service Construct** in the tree.
2. Expand **Control Service Profile**.
3. Click **DHCP Service Profile**.
4. Configure the parameters as follows:

Table 10-82 DHCP Service Profile Parameters

Parameter	Description
DHCP Service Name	DHCP Service name.
Admin State	Admin State: ■ enabled ■ disabled
DHCP Service Mode	Mode of operation of the DHCP service: ■ dhcp-client: System acts as a client on behalf of the UE in an Enterprise network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server. The DHCP exchange occurs between the system (acting as a DHCP client) and the external DHCP server. The DHCP client uses this information to configure its host and communicate on the internet. ■ dhcp-relay: A DHCP relay agent is any host that forwards DHCP packets between DHCP clients and DHCP servers. DHCP relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway address and, if configured, adds the relay agent information option in the packet and forwards it to the DHCP server. The exchanges occurs between the DHCP server(s) and the UE; the system is in the middle and in the process, learns the UE IP address.
DHCP Network Context	Network Context containing this DHCP Service endpoint
DHCP Service Endpoint	Service endpoint on the Network Context

Table 10-82 DHCP Service Profile Parameters

Parameter	Description
Enable Domain Name Server	Specify whether to use DNS configuration from external DHCP Server when configured as DHCP Client: ■ true ■ false
Enable Netbios Name Server	Specify whether to use NetBIOS Name Server configuration from external DHCP Server when configured as a DHCP Client: ■ true ■ false
External DHCP Server To add additional External DHCP Servers, click the **Create** icon.	
Name	Unique name of the external DHCP Server.
Admin State	Admin State: ■ enabled ■ disabled
IP Address	IP Address
Server IP Allocation Type	The Type of IP address that can be allocated by this external DHCP server: ■ V4 only ■ V6 only ■ V4 or V6

5 Click the **Save** icon.

Diffserv Profile

The Diffserv (Differentiated Services) Profile defines priority queuing to ensure cluster and network stability under any traffic load.

To add a Diffserv Profile:

1 Expand **Service Construct** in the tree.

2 Expand **Diffserv Profile**.

3 To configure the mapping of DSCP codes to queue priorities, click **Dscp Mapping**.

4 Configure the parameters as follows:

Table 10-83 DSCP Mapping Parameters

Parameter	Description
Code	DSCP code value: ■ dscp_0_be ■ dscp_01 *through* dscp_09 ■ dscp_10_af11 ■ dscp_11 ■ dscp_12_af12 ■ dscp_13 ■ dscp_14_af13 ■ dscp_15 *through* dscp_17 ■ dscp_18_af21 ■ dscp_19 ■ dscp_20_af22 ■ dscp_21 ■ dscp_22_af23 ■ dscp_23 *through* dscp_25 ■ dscp_26_af31 ■ dscp_27 ■ dscp_28_af32 ■ dscp_29 ■ dscp_30_af33 ■ dscp_31 *through* dscp_33 ■ dscp_34_af41 ■ dscp_35 ■ dscp_36_af42 ■ dscp_37 ■ dscp_38_af43 ■ dscp_39 *through* dscp_43 ■ dscp_44_va ■ dscp_45 ■ dscp_46_ef ■ dscp_47 *through* dscp_63

Table 10-83 DSCP Mapping Parameters

Parameter	Description
Queue Priority	Queue Priority to use for the DSCP value: ■ gold ■ silver ■ bronze ■ best-effort If a DSCP mapping is not specified for a given DSCP value, the system uses the priority queue for the class to which the value belongs.

5 Click the **Save** icon.

6 To configure the mapping of DiffServ class to queue priority, click **Class Mapping**.

7 Configure the parameters as follows:

Table 10-84 Class Mapping Parameters

Parameter	Description
Note: *Individual DSCP code values configured in* ***Dscp Mapping*** *take precedence over the class values configured here. If an individual DSCP value is not configured, the queue priority defined for its class is used.*	
Cs0	Queue Priority to use for class selector cs0: ■ gold ■ silver ■ bronze ■ best-effort
Cs1	Queue Priority to use for class selector cs1: ■ gold ■ silver ■ bronze ■ best-effort
Cs2	Queue Priority to use for class selector cs2: ■ gold ■ silver ■ bronze ■ best-effort

Table 10-84 Class Mapping Parameters

Parameter	Description
Cs3	Queue Priority to use for class selector cs3: ■ gold ■ silver ■ bronze ■ best-effort
Cs4	Queue Priority to use for class selector cs4: ■ gold ■ silver ■ bronze ■ best-effort
Cs5	Queue Priority to use for class selector cs5: ■ gold ■ silver ■ bronze ■ best-effort
Cs6	Queue Priority to use for class selector cs6: ■ gold ■ silver ■ bronze ■ best-effort
Cs7	Queue Priority to use for class selector cs7: ■ gold ■ silver ■ bronze ■ best-effort

8 Click the **Save** icon.

Domain Rule Group

Domain rule groups are services rules that are used by workflow to classify certain connections and take specific actions for certain domains. Use this object to configure a list of domains for which snooping is enabled. DNS Snooping (DNSS) provides users with access to restricted URLs or sites (for example, social media sites such as Facebook or Twitter).

MCC supports the following matching criteria for domain names:

- begins-with (prefix)
- contains (partial)
- ends-with (suffix)
- exact match
- regular expressions

To add a Domain Rule Group:

1. Expand **Service Construct** in the tree.
2. Click **Domain Rule Group**.
3. Configure the parameters as follows:
   - **Name** – Enter a Domain Rule Group name.
4. In **Rule**, configure the parameters as follows:

Table 10-85 Rule Condition Parameters

Parameter	Description
Name	Rule Condition name
URL List	URL list file to match against the Request's URL. The URL List must already exist. See URL List.
Domain Name	Specify the domain name to match against: begins-with contains ends-with exact regex: Regular Expression
To add additional rules, click the **Create** icon.	

5. Click the **Save** icon.

EDR Flow Network Stats Profile

Use this object to configure the EDR (Event Data Record) flow network profile. This profile contains configuration required for flow level network-stats-info record.

To add an EDR Flow Network Stats Profile:

1. Expand **Service Construct** in the tree.
2. Click **EDR Flow Network Stats Profile**.
3. Configure the parameters as follows:

Table 10-86 EDR Flow Network Stats Profile Parameters

Parameter	Description
Name	Profile name.
Measurement Layer	TCP/IP layer to be used for network-stats attributes calculation: ■ layer3: counts the entire IP datagram ■ layer4: excludes the IP header ■ layer7: excludes the IP header and the UDP/TCP/SCTP header
Include ICMP	Include/exclude ICMP traffic from network-stats attributes calculation: ■ True ■ False
Activity Duration Time Interval	Time interval to be used for flow activity duration calculation in uplink/downlink direction
Peak Throughput Time Interval	Time interval to be used for flow peak throughput calculation in uplink/downlink direction

4. Click the **Save** icon.

EDR Interface Profile

Use this object to configure the EDR (Event Data Record) Interface Profile (maximum 256) to generate EDRs.

To add an EDR Interface Profile:

1. Expand **Service Construct** in the tree.
2. Click **EDR Interface Profile**.
3. Configure the parameters as follows:

Table 10-87 EDR Interface Profile Parameters

Parameter	Description
Name	Profile name.
Admin State	Admin state of the profile: ■ enabled ■ disabled
Session Statistics Interval	Time interval, in seconds, between Session and Bearer Interim event data records. Default 0 (disabled)
Flow Statistics Interval	Time interval, in seconds, between Flow Interim event data records. Default: 600 (enabled)
Flow Min Lifetime	Number of seconds to wait before generating initial Flow event data record following flow creation. Default: 60 (enabled)
Max Url Length	Length to which the URL field should be truncated.
Session Data Stats Profile	EDR data session profile to be applied on attributes reported via session data statistics. The Session Data Stats Profile must already exist. See EDR Session Data Stats Profile. If Session Data Stats Profile is configured and attached to EDR Interface Profile , only session related attributes are reported in EDR.
Flow Network Stats Profile	EDR session profile to be applied on attributes reported via flow network statistics. The Flow Network Stats Profile must already exist. See EDR Flow Network Stats Profile. If no Flow Network Stats Profile is attached to EDR Interface Profile, default values for the parameters are used to calculate the peak throughput and activity duration.

4. In **EDR Service Profile**, configure the parameters as follows:

Table 10-88 EDR Service Profile Parameters

Parameter	Description
Name	Profile name.

Table 10-88 EDR Service Profile Parameters

Parameter	Description
Admin State	Admin state of the profile: ■ enabled ■ disabled
Primary Server	Primary EDR server for this EDR service
Secondary Server	Secondary EDR server for this EDR service

5 To configure the EDR Profile(s) and specify the EDR record information to send to the EDR server, configure the parameters as follows.

Table 10-89 Record Info Parameters

Parameter	Description
Bearer EDR Profile:	
Admin State	Admin state of the profile: ■ enabled ■ disabled
Bearer Info	Enable/Disable bearer information: ■ enabled ■ disabled
Bearer Qos Information	Enable/Disable bearer QoS information: ■ enabled ■ disabled
Data Statistics	Enable/Disable data statistics: ■ enabled ■ disabled
Edr Cause Codes	Enable/Disable EDR cause codes: ■ enabled ■ disabled
Flow EDR Profile:	
Admin State	Admin state of the profile: ■ enabled ■ disabled
Data Statistics	Enable/Disable data statistics: ■ enabled ■ disabled

Table 10-89 Record Info Parameters

Parameter	Description
DPI Info	Enable/Disable flow deep packet inspection information: ■ enabled ■ disabled
Network Perf Info	Enable/Disable flow network-perf-information: ■ enabled ■ disabled
Subscriber Info	Enable/Disable flow subscriber information: ■ enabled ■ disabled
TCP Retransmission Info	Enable/Disable flow TCP retransmission statistics: ■ enabled ■ disabled
Network Stats Info	Enable/Disable flow network statistics: ■ enabled ■ disabled
NAT Binding Info	Enable/Disable reporting NAT IP address and NAT port information: ■ **`enabled`** ■ **`disabled`**
HTTP EDR Profile:	
Admin State	Admin state of the profile: ■ enabled ■ disabled
Cache Info	Enable/Disable HTTP cache information: ■ enabled ■ disabled
Compression Info	Enable/Disable HTTP compression information: ■ enabled ■ disabled
Connection Info	Enable/Disable HTTP connection information: ■ enabled ■ disabled
DPI Info	Enable/Disable deep packet inspection information: enabled disabled

Table 10-89 Record Info Parameters

Parameter	Description
Entitlement Info	Enable/Disable entitlement information: ■ enabled ■ disabled
Filter Info	Enable/Disable content filter information: ■ enabled ■ disabled
Http Subscriber Info	Enable/Disable HTTP subscriber information: ■ enabled ■ disabled
Manifest Information	Enable/Disable HTTP manifest information: ■ enabled ■ disabled
Minification Information	Enable/Disable HTTP minification information: ■ enabled ■ disabled
Preempt Dns Info	Enable/Disable HTTP preempt DNS information: ■ enabled ■ disabled
Request Info	Enable/Disable HTTP request information: ■ enabled ■ disabled
Response Info	Enable/Disable HTTP response information: ■ enabled ■ disabled
Tcp Client Connection Info	Enable/Disable HTTP TCP client connection information: ■ enabled ■ disabled
Tcp Server Connection Info	Enable/Disable HTTP TCP server connection information: ■ enabled ■ disabled
Tcp Splicing Info	Enable/Disable HTTP TCP Splicing information: ■ enabled ■ disabled

Table 10-89 Record Info Parameters

Parameter	Description
Time Info	Enable/Disable HTTP time information: ■ enabled ■ disabled
UDP Proxy Info	Enable/Disable UDP Proxy information: ■ enabled ■ disabled
Video Info	Enable/Disable HTTP video information: ■ enabled ■ disabled
Web Image Opt Info	Enable/Disable HTTP web image optimization information: ■ enabled ■ disabled
Pilot EDR Profile:	
Admin State	Admin state of the profile: ■ enabled ■ disabled
Start Records	Enable/Disable START records: ■ enabled ■ disabled
Stop Records	Enable/Disable STOP records: ■ enabled ■ disabled
NAT Binding Records	Enable/Disable NAT Binding records: ■ enabled ■ disabled
RAT Change Records	Enable/Disable RAT Change records: ■ enabled ■ disabled
RTT EDR Profile:	
Admin State	Admin state of the profile: ■ enabled ■ disabled

Table 10-89 Record Info Parameters

Parameter	Description
Gtp S5 Records	Enable/Disable GTP S5 records: ■ enabled ■ disabled
Gtp S8 Records	Enable/Disable GTP S8 records: ■ enabled ■ disabled
Gtp S11 Records	Enable/Disable GTP S11 records: ■ enabled ■ disabled
Gtp S4 Records	Enable/Disable GTP S4 records: ■ enabled ■ disabled
Gtp S2a Records	Enable/Disable GTP S2a records: ■ enabled ■ disabled
Gtp S2b Records	Enable/Disable GTP S2b records: ■ enabled ■ disabled
Gtp Gn Records	Enable/Disable GTP Gn records: ■ enabled ■ disabled
Gtp Gp Records	Enable/Disable GTP Gp records: ■ enabled ■ disabled
Diameter Gx Records	Enable/Disable Diameter Gx records: ■ enabled ■ disabled
Diameter Gy Records	Enable/Disable Diameter Gy records: ■ enabled ■ disabled
Diameter S6b Records	Enable/Disable Diameter S6b records: ■ enabled ■ disabled

Table 10-89 Record Info Parameters

Parameter	Description
Diameter Swm Records	Enable/Disable Diameter SWm records: ■ enabled ■ disabled
Ike Swu Records	Enable/Disable IKE SWu records: ■ enabled ■ disabled
Session EDR Profile:	
Admin State	Admin state of the profile: ■ enabled ■ disabled
Data Statistics	Enable/Disable data statistics: ■ enabled ■ disabled
Edr Cause Codes	Enable/Disable EDR cause codes: ■ enabled ■ disabled
Gateway Info	Enable/Disable gateway information: ■ enabled ■ disabled
Serving Network Info	Enable/Disable serving network information: ■ enabled ■ disabled
Session Qos Info	Enable/Disable session QoS information: ■ enabled ■ disabled
Session Subscriber Info	Enable/Disable session subscriber information: ■ enabled ■ disabled
Session User Csg Info	Enable/Disable session user csg information: ■ enabled ■ disabled
Network Stats Info	Enable/Disable network statistics: ■ enabled ■ disabled

6 Click the **Save** icon.

7 For SESSION, BEARER, FLOW, Pilot, and RTT EDR records, in **Record Type**, configure the parameters as follows:

Table 10-90 Record Type Parameters

Parameter	Description
Attempt Records	Enable/Disable ATTEMPT records: ■ **enabled** ■ **disabled** *Applies to SESSION and BEARER records only.*
Interim Records	Enable/Disable INTERIM records: ■ **enabled** ■ **disabled** *Applies to SESSION, BEARER, and FLOW records only.*
Start Records	Enable/Disable START records: ■ **enabled** ■ **disabled** *Applies to SESSION, BEARER, FLOW, and Pilot records only.*
Stop Records	Enable/Disable STOP records: ■ **enabled** ■ **disabled** *Applies to SESSION, BEARER, FLOW, and Pilot records only.*
NAT Binding Records	Enable/Disable NAT Binding Records records: ■ **enabled** ■ **disabled** *Applies to Pilot records only.*
RAT Type Change Records	Enable/Disable RAT Type Change records: ■ **enabled** ■ **disabled** *Applies to Pilot records only.*
GTP S5 Records	Enable/Disable GTP S5 records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
GTP S8 Records	Enable/Disable GTP S8 records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*

Table 10-90 Record Type Parameters

Parameter	Description
GTP S11 Records	Enable/Disable GTP S11 records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
GTP S4 Records	Enable/Disable GTP S4 records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
GTP S2a Records	Enable/Disable GTP S2a records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
GTP S2b Records	Enable/Disable GTP S2b records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
GTP Gn Records	Enable/Disable GTP Gn records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
GTP Gp Records	Enable/Disable GTP Gp records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
Diameter Gx Records	Enable/Disable Diameter Gx records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
Diameter Gy Records	Enable/Disable Diameter Gy records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
Diameter S6b Records	Enable/Disable Diameter S6b records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*

Table 10-90 Record Type Parameters

Parameter	Description
Diameter SWm Records	Enable/Disable Diameter SWm records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*
IKE SWu Records	Enable/Disable IKE SWu records: ■ **enabled** ■ **disabled** *Applies to RTT records only.*

8 Click the **Save** icon.

EDR Server Profile

Use this object to configure the EDR (Event Data Record) server Profile (maximum 8) to generate EDRs.

To add an EDR Server Profile:

1 Expand **Service Construct** in the tree.

2 Click **EDR Server Profile**.

3 Configure the parameters as follows:

Table 10-91 EDR Server Profile Parameters

Parameter	Description
Name	Profile name.
Admin State	Admin state of the profile: ■ enabled ■ disabled
IP Address	IP address of the EDR server
Port	TCP port of the EDR server
Network Context	Network context of the EDR server
EDR Source IP	Source IP address to use to reach the EDR server
Transport	Transport type: ■ tcp ■ udp

Table 10-91 EDR Server Profile Parameters

Parameter	Description
Encoding	Encoding type: ■ protobuf ■ tlv (type-length-value)
Keep Alive	EDR server keep alive interval
TCP User Timeout	Number of seconds for TCP user data retransmission timeout

4 Click the **Save** icon.

EDR Session Data Stats Profile

Use this object to enable EDR (Event Data Record) session volume measurement reporting. This profile carries configuration required for session level data statistics record.

To add an EDR Session Data Stats Profile:

1 Expand **Service Construct** in the tree.

2 Click **EDR Session Data Stats Profile**.

3 Configure the parameters as follows:

Table 10-92 EDR Session Data Stats Profile Parameters

Parameter	Description
Name	Profile name.
Measurement Layer	TCP/IP layer to be used for bucket volume calculation: ■ layer3: counts the entire IP datagram ■ layer4: excludes the IP header ■ layer7: excludes the IP header and the UDP/TCP/SCTP header
Include ICMP	Include/exclude ICMP traffic in peak throughput and activity duration calculation: ■ True ■ False
Activity Duration Time Interval	Time interval to be used for session activity duration calculation in uplink/downlink direction
Peak Throughput Time Interval	Time interval to be used for session peak throughput calculation in uplink/downlink direction

Table 10-92 EDR Session Data Stats Profile Parameters

Parameter	Description
Bucket Volume Time Interval	Time interval to be used for session volume throughput calculation in uplink/downlink direction

4 Click the **Save** icon.

Encryption Profile

Use this object to specify the algorithm and keys to be used for header encryption.

The Advanced Encryption Standard (AES) profile stores encryption algorithm information and keys depending on the algorithm configured by the Operator. MCC generates a random IV and includes this as an extra header in each encrypted header. MCC supports a key in hex format (without spaces).

MCC supports the AES-128/192/256-CBC encryption algorithm and Base64 and Hex encoding for the encrypted value.

To add an Encryption Profile:

1 Expand **Service Construct** in the tree.

2 Click **Encryption Profile**.

3 Configure the parameters as follows:

Table 10-93 Encryption Profile Parameters

Parameter	Description
Name	Profile name
Admin State	Admin state of the profile: ■ enabled ■ disabled
Encoding	Encoding format for encrypted information: ■ hex ■ base64

Table 10-93 Encryption Profile Parameters

Parameter	Description
Encryption Algorithm	Algorithm used for encryption: ■ aes-128-cbc: Encrypted by Advanced Encryption Standard 128-bit Cipher Block Chaining. Enter the key for AES encryption, in HEX format without spaces. ■ aes-192-cbc: Encrypted by Advanced Encryption Standard 192-bit Cipher Block Chaining. Enter the key for AES encryption, in HEX format without spaces. ■ aes-256-cbc: Encrypted by Advanced Encryption Standard 256-bit Cipher Block Chaining. Enter the key for AES encryption, in HEX format without spaces. ■ rc4md5-128: Encrypted by Rivest Cipher 4 128-bit Stream Cipher encryption. Enter the key for RC4 encryption, as an alphanumeric string of 8 through 15 characters without spaces.

4 Click the **Save** icon.

Event Trigger Template

Use this object to specify the events that trigger an interim update on the offline charging interface and to trigger the closure of an interim CDR.

You associate the Event Trigger Template with an Accounting, Offline, or Online Charging interface.

To add an Event Trigger Template:

1. Expand **Service Construct** in the tree.
2. Expand **Interface Trigger Template**.
3. Click **Event Trigger Template**.
4. Configure the parameters as follows:

Table 10-94 Event Trigger Template Parameters

Parameter	Description
Template Name	Event Trigger Template name
QoS Change Close Trigger	Specifies whether a QoS Change triggers an update. Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of QoS Change events to trigger a CDR close.
Serving Node Change Close Trigger	Specifies whether a Serving Node Change triggers an update. Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of Serving Node Change events to trigger a CDR close. In the case of the SGW, the serving node is the MME.
Serving Node PLMN Change Close Trigger	Specifies whether a Serving Node PLMN Change triggers an update. Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of Serving Node PLMN Change events to trigger a CDR close. ***Note:*** *Applies to PGW and GGSN only.*
User Location Change Close Trigger	Specifies whether a User Location Change triggers an update. Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of User Location Change events to trigger a CDR close.
RAT Type Change Close Trigger	Specifies whether a RAT Type Change triggers an update. Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of RAT Type Change events to trigger a CDR close.

Table 10-94 Event Trigger Template Parameters

Parameter	Description
User CSG Change Close Trigger	Specifies whether a user Closed Subscriber Group (CSG) Change triggers an update. Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of user CSG Change events to trigger a CDR close.
UE Time Zone Change Close Trigger	Specifies whether a UE Time Zone Change triggers an update. Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of UE Time Zone Change events to trigger a CDR close.
MME Node Change Close Trigger	Specifies whether an MME Node Change triggers an update (SGW only). Value 0 disables the trigger, value 1 - 20 enables the trigger. In the case of offline interfaces, the value specifies the number of MME Node Change events to trigger a CDR close. ***Note:*** *Applies to SGW only.*
Volume Limit Close Trigger	If Data Volume Limit is enabled on the interface (to generate a new CDR), specifies the number of events to trigger a CDR close. Enter a value 1 - 20. ***Note:*** *Applies to offline interfaces only.*
Time Limit Close Trigger	If interim updates are enabled on the interface, specifies the number of events to trigger a CDR close. Enter a value 1 - 20. ***Note:*** *Applies to offline interfaces only.*

5 Click the **Save** icon.

File Download Profile

The File Download Profile defines parameters for importing lists from a file server.

To add a File Download Profile:

1. Expand **Service Construct** in the tree.
2. Click **File Download Profile**.
3. Configure the parameters as follows:

Table 10-95 File Download Profile Parameters

Parameter	Description
Name	File Download Profile name.
Automatic Download	Automatic Download: ■ enabled. When enabled, configure an automatic download schedule: Time of Day/Days of Week or Download Interval (which takes precedence) ■ disabled. When disabled, Operators must download the policy list manually (*on demand only* mode). In this mode, the Time of Day/Days of Week and Download Interval objects are configurable but not mandatory. If both are configured, the Download Interval takes precedence and is therefore used for automatic download.
Time of Day	File download time (in 24 hour time).
Retry Count	Number of times to retry the download after a failure.
Retry Interval	Number of minutes to wait to retry the download after a failure.
Server Address	Server address or hostname where the file resides.
Username	File download username.
Password	File download password.
Retain Count	Number of downloads to retain.
Network Context	Network context where the file resides.
Download Interval	Interval, in minutes, for periodic download. Value 0 disables periodic download. Other values override Time of Day and Days of Week download schedule.
Days of Week	Select the day to download the file. To add additional days, click the **Create** icon.

4. Click the **Save** icon.

Filter Hash List

To add a Filter Hash List:

1. Expand **Service Construct** in the tree.
2. Click **Filter Hash List**.
3. Configure the parameters as follows:
   - **Name** – Filter Hash List name.
4. Click the **Save** icon.
5. To specify where to import the file from, expand the Filter Hash List you added.
   a. To import from a local file, click **Import from Local File**. In **Filename**, specify the local filename.
   b. To import from a server file, click **Import from Server**. In **File Download Profile**, select the File Download Profile that defines parameters for importing the list from a file server. The File Download Profile must already exist. See File Download Profile.
6. Click the **Save** icon.

Filter Hash List Import History

Use this object to view filter hash list import history.

To view filter hash list import history:

1. Expand **Service Construct** in the tree.
2. Expand **Filter Hash List**.
3. Expand **Import History**.
4. Click an instance.

   Filter hash list import history parameters are:
   - Import Time
   - Import Result: Success or error
   - Import File Size
   - Number of Accept Entries
   - Number of Reject Entries
   - Import File Name
   - Import Type: manual or scheduled

Filter Hash List Summary

Use this object to view filter hash list summary.

To view filter hash list summary:

1. Expand **Service Construct** in the tree.
2. Expand **Filter Hash List**.
3. Expand **Summary**.
4. Click an instance.

   Acuitas lists the filter hash list summary, including:

   - Last Import Time
   - Last Import Result: Success or error
   - Last Import Type: manual or scheduled
   - Last Import Number
   - Last Import File Size (in bytes)
   - Next Import Time
   - Number of Accepted Entries
   - Number of Rejected Entries
   - Import File Name

Flow Idle Timeout Filter

The Flow Idle Timeout Filter defines parameters to identify application traffic and configure the tuple: destination port range and protocol.

To add a Flow Idle Timout Filter:

1. Expand **Service Construct** in the tree.
2. Click **Flow Idle Timeout Filter**.
3. Configure the parameters as follows:

Table 10-96 Flow Idle Timeout Filter Parameters

Parameter	Description
Name	File Download Profile name.
Network Port Start	Network equipment port range start value
Network Port End	Network equipment port range end value
Protocol	IP protocol values (e.g., all: 255, ICMP: 1, TCP: 6, UDP: 17etc)

4. Click the **Save** icon.

Flow Idle Timeout Rule

The Flow Idle Timeout Rule defines parameters of connection timeout, priority of the rule, and the mapping to the Flow Idle Timeout Filter.

To add a Flow Idle Timout Rule:

1. Expand **Service Construct** in the tree.
2. Click **Flow Idle Timeout Rule**.
3. Configure the parameters as follows:

Table 10-97 Flow Idle Timeout Rule Parameters

Parameter	Description
Name	File Download Profile name.
Conn Idle Ttimeout	Connection idle timeout (in seconds). The value 2160000 is a long timeout of about 25 days.
Priority	Priority of the flow timeout rule, value 1 indicates highest priority

4. Click the **Save** icon.
5. Expand the Flow Idle Timeout Rule you added.

6 Click **Flow Idle Timeout Filter**.

7 Select the Flow Idle Tiemout Filter to associate with this rule. The Flow Idle Tiemout Filter must already exist. See Flow Idle Timeout Filter.

8 Click the **Save** icon.

Geo Redundancy Server

The Geo Redundancy Server defines parameters for the Geographic Redundancy Hot Standby Server.

Note: *It is recommended that you use the Geographic Redundancy Manager application to configure Geographic Redundancy Servers. For instructions, see Geographic Redundancy Manager.*

To add a Geo Redundancy Server:

1 Expand **Service Construct** in the tree.

2 Click **Geo Redundancy Server**.

3 Configure the parameters as follows:

Table 10-98 Geo Redundancy Server Parameters

Parameter	Description
Geo Redundancy Group	Geographic Redundancy group to which this loopback belongs.
Network Context	Network context containing this Geographic Redundancy Server service endpoint
Service Endpoint	Service Endpoint for this Geographic Redundancy Server service. The Service Endpoint must already exist. Create it at Network Context > *name* > Service Endpoint
Remote IP Address	IP address for the remote peer in the group
Remote Base Port	Port number for the remote peer in the group
Failover Soak Interval	Number of seconds to pause after a failover before considering another failover
Link Timeout	Number of seconds of missed keep-alive packets from the peer before declaring geo link down

Table 10-98 Geo Redundancy Server Parameters

Parameter	Description
DSCP Value	DSCP value to include in the TOS field in geo-redundancy packets, allowing the packets to receive a particular forwarding treatment as they are routed. DSCP code value: ■ dscp_0_be ■ dscp_01 *through* dscp_09 ■ dscp_10_af11 ■ dscp_11 ■ dscp_12_af12 ■ dscp_13 ■ dscp_14_af13 ■ dscp_15 *through* dscp_17 ■ dscp_18_af21 ■ dscp_19 ■ dscp_20_af22 ■ dscp_21 ■ dscp_22_af23 ■ dscp_23 *through* dscp_25 ■ dscp_26_af31 ■ dscp_27 ■ dscp_28_af32 ■ dscp_29 ■ dscp_30_af33 ■ dscp_31 *through* dscp_33 ■ dscp_34_af41 ■ dscp_35 ■ dscp_36_af42 ■ dscp_37 ■ dscp_38_af43 ■ dscp_39 *through* dscp_43 ■ dscp_44_va ■ dscp_45 ■ dscp_46_ef ■ dscp_47 *through* dscp_63

4 Click the **Save** icon.

5 To specify network connectivity monitoring for automatic failover, expand the Geo Redundancy Server you added.

6 Click **Connectivity Monitoring Params**.

7 Configure the parameters as follows:

- **Monitor AAA** – Set to enabled to monitor Accounting Authentication Authorization interface to govern fault detection and automatic failover.
- **Monitor PCRF** – Set to enabled to monitor PCRF to govern fault detection and automatic failover.
- **Monitor OCS** – Set to enabled to monitor OCS to govern fault detection and automatic failover.
- **Monitor S6B** – Set to enabled to monitor S6B to govern fault detection and automatic failover.
- **Monitor RMG** – Set to enabled to monitor Routing Monitoring Groups as an IP layer network health indicator

8 Click the **Save** icon.

Gy Event Trigger Template

Use this object to specify the Gy events that trigger the closure and sending of an interim CDR on the Gz/Rf interface. You associate the Gy Event Trigger Template with an Gz Offline interface.

To add a Gy Event Trigger Template:

1 Expand **Service Construct** in the tree.

2 Expand **Interface Trigger Template**.

3 Click **Gy Event Trigger Template**.

4 Configure the parameters as follows:

- **Template Name**: Gy Event Trigger Template name

5 Click the **Save** icon.

6 Expand **Gy Event Trigger Template**.

7 Expand the Gy Event Trigger Template you added.

8 Click the Gy Event you want to configure:

- Final Close Trigger
- Forced Reauthorisation Close Trigger
- Quota Exhausted Close Trigger
- Quota Holding Time Close Trigger
- Rating Condition Change Close Trigger
- Tariff Time Change Close Trigger
- Validity Time Close Trigger

- Volume Quota Threshold Close Trigger

9 Configure the parameters as follows:

Table 10-99 Gy Event Trigger Template Parameters

Parameter	Description
Recurrence Count	Specifies the maximum number of service data containers added to a CDR per closure event. Upon reaching this limit, offline charging CDRs are closed and transfered to the OFCS. Value 0 disables the trigger, value 1 - 20 enables the trigger.
Change Condition Value	Specifies the change condition value to use in the rating group level service data container created for this Gy event. If set to **0**, the change condition value in the service data container is set as defined in 3GPP 32.298.

10 Click the **Save** icon.

Health Check Profile

Use this object to configure a health-check mechanism to detect if a monitored service is down or overloaded. MCC then uses this information for traffic-handling decisions.

To add a Health Check Profile:

1 Expand **Service Construct** in the tree.

2 Click **Health Check Profile**.

3 Configure the parameters as follows:

Table 10-100 Gy Event Trigger Template Parameters

Parameter	Description
Name	Health Check Profile name
Admin State	Admin state of Health Check Profile: ■ Enabled ■ Disabled
Interval	Time interval between successive health checks in units of ms
Protocol	Service Protocol for the host/IP: ■ ftp
Timeout	Timeout for the destination in units of ms
Max Attempts	Max number of attempts for the destination
Loopback IP List	Loopback Ip List for the Health Check Profile. The Loopback IP List must already exist. See Loopback IP List.

Table 10-100 Gy Event Trigger Template Parameters

Parameter	Description
Network Context	Network Context to use for Health Check Profile

4 Click the **Save** icon.

Host List

The Host List serves as a whitelist used by the Fraud Detection Profile. It contains the IP addresses that represent legitimate proxies.

To add a Host List:

1 Expand **Service Construct** in the tree.

2 Click **Host List**.

3 Configure the parameters as follows:

- **Name** – Enter the Host List name.

4 Click the **Save** icon.

5 Expand **Host List**.

6 Expand the Host List you added.

7 Click **IP Address**.

8 Configure the parameters as follows:

- **Host Entry IP** – Enter the Host IP address.

9 Click the **Save** icon.

10 Repeat step 7 through step 9 to add as many IP addresses as needed.

HTTP Header Enrichment

HTTP Header Enrichment provides the ability to insert, remove, or replace proprietary headers in the HTTP header. These headers are used by origin servers and other nodes in the Operator network to determine the treatment of the packet and for tracking purposes:

- Operator configures the headers to be inserted, removed, or replaced.
- HTTP Proxy supports adding L7 filters for header enrichment.
- Workflow determines the HTTP Proxy instance to use for a subscriber. The HTTP Header Enrichment profile associated with that HTTP Proxy instance is used for the HTTP transaction.
- HTTP Proxy instance supports explicit proxy configuration and any port (in addition to port 80).
- Proxy supports using a pre-configured network context for server-side TCP connections.
- Proxy supports steering traffic to a well-defined IP address and port (in a pre-configured network-context) based on request header based rules.

HTTP Proxy supports embedding variables in HTTP headers. HTTP Header Enrichment functionality supports the following variables:

- IMSI
- MSISDN
- HTTPVERSION

The feature enables support for the following use cases:

- Ut (VoLTE) interface support for adding *X-3GPP-Asserted-Identity* header with embedded *MSISDN* variable. The Ut interface is defined in *3GPP TS 24.623*.
- Adding and updating *Via* header with embedded *HTTPVERSION* variable to HTTP requests and responses. The *Via* header is defined in *IETF RFC7230*.

The HTTP Header Enrichment profile supports the addition of a string macro to include variables for add-header header-string value and rewrite-header header-string append-value. MCC uses "`$()`" in the string macro to indicate a variable. Any "`$`" or "`()`" that does not conform to this format is considered a normal character in the string instead of variable. The string-macro may contain as many variables as needed. The string length limitation is 255.

This features also enables Operators to add or rewrite a *Via* header. If a `Via` header already exists and rewrite is configured, MCC rewrites the header with the original information and appends the configuration with "`,`".

To add an HTTP Header Enrichment:

1. Expand **Service Construct** in the tree.
2. Click **HTTP Header Enrichment**.
3. Configure the parameters as follows:
   - **Name** – Enter the HTTP Header Enrichment name.
   - **First Request** – Mark the checkbox to apply the HTTP Header Enrichment add-header and add-cookie only for the first request on a client connection.
   - **Encryption Profile** – Configure an encryption profile used to encrypt request header value.
4. To add a Request Header String, configure the **Request Header String** parameters as follows:

Table 10-101 Request Header String Parameters

Parameter	Description
Header String	Specify the string of the header: ■ X-Forwarded-For – Add X-Forwarded-For header name ■ X-Forwarded-Proto – Add X-Forwarded-Proto header name ■ X-IMSI – Add X-IMSI header name ■ X-MSISDN – Add X-MSISDN header name

Table 10-101 Request Header String Parameters

Parameter	Description
Header Value	Specify the value to include in the header: ■ msisdn - Include MSISDN in the header: – MSISDN – MD5: Include MD5 encrypted MSISDN in the header – Static Encryption: Include static encrypted MSISDN in the header (uses “no padding” to produce a persistent sequence of bytes) – Dynamic Encryption: Include dynamic encrypted MSISDN in the header (uses timestamp to generate a new dynamic value for each PDP context) – encrypted: Include encrypted MSISDN in the header by the algorithm configured in encryption profile – Static-acr – Supports a predefined format value + encrypted value of MSISDN. – Dynamic-acr – Supports a predefined format value + encrypted value of timestamp and MSISDN. ■ ue-ip-addr - Include User Equipment IP Address in the header ■ ue-ip-addr-port - Include User Equipment IP Address port in the header ■ ue-port - Include User Equipment port in the header ■ rat-type - Include Radio Access Type (2G, 3G, or 4G) in the header ■ charging-characteristic - Include Charging Characteristic in the header ■ http-protocol - Include HTTP Protocol (HTTP or HTTPS) in the header ■ serving-gw-ip-address - Include the serving gateway IPv4 address in the header ■ serving-gw-ipv6-address - Include the serving gateway IPv6 address in the header ■ serving-network-plmnid - Include the serving network PLMNID in the header ■ original-apn-name - Include the original APN name in the header ■ mapped-apn-name - Include the mapped APN name in the header ■ reseller-id - Include the reseller ID in the header ■ original-url - Inserts the original URL in the request header prior to sending the request to the server ■ imei - Include IMEI in the header: – IMEI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile

Table 10-101 Request Header String Parameters

Parameter	Description
Header Value ***(Continued)***	■ imsi - Include IMSI in the header: – IMSI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile ■ user-location-info - Include User Location Information in the header: – Cgi - Include Cell Global Information in the header ■ subscriber-id - Include subscriber ID in the header: – ltmi-dynamic-trusted: Include Dynamic Trusted ID in the header – ltmi-external: Include External ID in the header – ltmi-static-trusted: Include Static Trusted ID in the header – plain-text: Include plain text ID in the header ■ ue-ipv4-mapped-ipv6-addr - Include an IPv4 address mapped to an IPv6 address in the header: – IPv6 Prefix- Configure up to a 96-bit IPv6 Prefix to map an IPv4 address into an IPv6 address format ■ time-zone - Include UE time zone and daylight savings in the header. The header value follows the 3GPP standard and uses a 4-digit hex string ■ value - Value to include for the header: – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted value in the header by the algorithm configured in encryption profile – ltmi-dynamic-trusted: Encrypt data using Dynamic Trusted LTMI algorithm in the header – ltmi-external: Encrypt data using External LTMI algorithm in the header – ltmi-static-trusted: Encrypt data using Static Trusted LTMI algorithm in the header

To add additional Request Header Strings, click the **Create** icon.

5 Click the **Save** icon.

6 To add a Request Header Custom String, configure the **Request Header Custom String** parameters as follows:

Table 10-102 Request Header Custom String Parameters

Parameter	Description
Header String	Enter the custom string of the header.
Header Value	Specify the value to include in the header: ■ msisdn - Include MSISDN in the header: – MSISDN – MD5: Include MD5 encrypted MSISDN in the header – Static Encryption: Include static encrypted MSISDN in the header (uses “no padding” to produce a persistent sequence of bytes) – Dynamic Encryption: Include dynamic encrypted MSISDN in the header (uses timestamp to generate a new dynamic value for each PDP context) – encrypted: Include encrypted MSISDN in the header by the algorithm configured in encryption profile – Static-acr – Supports a predefined format value + encrypted value of MSISDN. – Dynamic-acr – Supports a predefined format value + encrypted value of timestamp and MSISDN. ■ ue-ip-addr - Include User Equipment IP Address in the header ■ ue-ip-addr-port - Include User Equipment IP Address port in the header ■ ue-port - Include User Equipment port in the header ■ rat-type - Include Radio Access Type (2G, 3G, or 4G) in the header ■ charging-characteristic - Include Charging Characteristic in the header ■ http-protocol - Include HTTP Protocol (HTTP or HTTPS) in the header ■ serving-gw-ip-address - Include the serving gateway IPv4 address in the header ■ serving-gw-ipv6-address - Include the serving gateway IPv6 address in the header ■ serving-network-plmnid - Include the serving network PLMNID in the header ■ original-apn-name - Include the original APN name in the header ■ mapped-apn-name - Include the mapped APN name in the header

Table 10-102 Request Header Custom String Parameters

Parameter	Description
Header Value ***(Continued)***	■ reseller-id - Include the reseller ID in the header ■ original-url - Inserts the original URL in the request header prior to sending the request to the server ■ imei - Include IMEI in the header: – IMEI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile ■ imsi - Include IMSI in the header: – IMSI – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted custom value in the header by the algorithm configured in encryption profile ■ user-location-info - Include User Location Information in the header: – Cgi - Include Cell Global Information in the header ■ subscriber-id - Include subscriber ID in the header: – ltmi-dynamic-trusted: Include Dynamic Trusted ID in the header – ltmi-external: Include External ID in the header – ltmi-static-trusted: Include Static Trusted ID in the header – plain-text: Include plain text ID in the header ■ ue-ipv4-mapped-ipv6-addr - Include an IPv4 address mapped to an IPv6 address in the header: – IPv6 Prefix- Configure up to a 96-bit IPv6 Prefix to map an IPv4 address into an IPv6 address format ■ time-zone - Include UE time zone and daylight savings in the header. The header value follows the 3GPP standard and uses a 4-digit hex string ■ value - Value to include for the header: – MD5: Include MD5 hashed custom value in the header – encrypted: Include encrypted value in the header by the algorithm configured in encryption profile – ltmi-dynamic-trusted: Encrypt data using Dynamic Trusted LTMI algorithm in the header – ltmi-external: Encrypt data using External LTMI algorithm in the header – ltmi-static-trusted: Encrypt data using Static Trusted LTMI algorithm in the header

To add additional Request Header Custom Strings, click the **Create** icon.

7 To add a Request Cookie String, configure the **Request Cookie String** parameters, as follows:

Table 10-103 Add Request Cookie String Parameters

Parameter	Description
Cookie String	Specify the string of the cookie: ■ User-Identity-Forward-IMSI – Add subscriber IMSI to Cookie ■ User-Identity-Forward-MSISDN – Add subscriber MSISDN to Cookie
Cookie Value	Specify the value to include in the cookie: ■ imsi - Include IMSI in the cookie ■ msisdn - Include MSISDN in the cookie ■ value - Value to include for the cookie

To add additional Request Cookie Strings, click the **Create** icon.

8 To add a Request Cookie Custom String, configure the **Request Cookie Custom String** parameters, as follows:

Table 10-104 Add Request Cookie Custom String Parameters

Parameter	Description
Cookie String	Enter the custom string of the cookie.
Cookie Value	Specify the value to include in the cookie: ■ imsi - Include IMSI in the cookie ■ msisdn - Include MSISDN in the cookie ■ value - Value to include for the cookie

To add additional Request Cookie Custom Strings, click the **Create** icon.

9 To add a Response Header String, configure the **Response Header String** parameters as follows:

Table 10-105 Add Response Header String Parameters

Parameter	Description
Header String	Specify the string of the header.
Header Value	Specify the value to include in the header.

To add additional Response Header Strings, click the **Create** icon.

10 Click the **Save** icon.

To remove an HTTP Header Enrichment string:

1 To remove a string from an HTTP Request or Response, configure the **Remove Header String** parameters as follows:

Table 10-106 Remove Header String Parameters

Parameter	Description
Header String	Enter the header string to remove.

To remove additional Header Strings, click the **Create** icon.

2 Click the **Save** icon.

To rewrite an HTTP Header Enrichment string:

1 To rewrite a string in an HTTP Request or Response, configure the **Rewrite Header String** parameters as follows:

Table 10-107 Rewrite Request Header String Parameters

Parameter	Description
Header String	Enter the header string to rewrite.
Rewrite Option	Rewrite Option: ■ appendValue – Append a value to an existing header. string (any character except Ctrls and seperators, may include variable such as IMSI, MSISDN, HTTPVERSION, example: $(MSISDN)). ■ replaceHeader – Replace header string with a new string (HTTP header field name string). ■ replaceValue – Replace header value with a new value (HTTP token - any character except Ctrls and seperators). Specify the value to rewrite for the header.

2 To rewrite additional Header Strings, click the **Create** icon.

3 Click the **Save** icon.

To specify that the HTTP Header Enrichment be used by an HTTP Policy, see HTTP Response Policy.

HTTP Rule Group

The HTTP Rule Group construct defines a set of rules for matching header attributes in HTTP request and response headers, such as HTTP Request's Host header, HTTP Request's URI, HTTP Request's Content-type header, and so on. This object is referred to by a Service Rule. When a match is found in the header, specific actions or service(s) can be applied, based on where the Service Rule is used, such as terminate/block/redirect/allow action for Content Filter service, Header Enrichment for HTTP-proxy service, and so on.

Note: *If the Service Rule configured for the HTTP Rule Group does not contain a Packet Filter, MCC cannot detect CONNECT requests. For proper operation, Service Rules configured for HTTP Rule Groups that filter on the CONNECT Request Method must also be configured with at least one Packet Filter.*

To add an HTTP Rule Group:

1. Expand **Service Construct** in the tree.
2. Click **HTTP Rule Group**.
3. Configure the parameters as follows:
   - **Name** – Enter an HTTP Rule Group name.
4. In **Rule**, configure the parameters as follows:

Table 10-108 Rule Condition Parameters

Parameter	Description
Name	Rule Condition name
URL List	URL list file to match against the HTTP Request's URL. The URL List must already exist. See URL List.
Request Method	String to match against HTTP Request's Method field: ■ GET ■ HEAD ■ POST ■ PUT ■ DELETE ■ TRACE ■ OPTIONS ■ CONNECT
Response Status Code	Status code to match against HTTP Response's Status line.

Table 10-108 Rule Condition Parameters

Parameter	Description
Host Port Start	The port start value for matching against HTTP request host port. Specify both Host Port Start and Host Port End, even if both values are equal.
Host Port End	The port end value for matching against HTTP request host port. Specify both Host Port Start and Host Port End, even if both values are equal.
Accept	String to match against HTTP Request's Accept header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Content Type	String to match against HTTP Request's Content-type header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Host	String to match against HTTP Request's Host header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Media	Media types to match against response payload: ■ all-video ■ progressive-video – FLV – MP4 – WEBM ■ Abr-video – DASH – HLS – HDS

Table 10-108 Rule Condition Parameters

Parameter	Description
Referer	String to match against HTTP Request's Referer field: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Request URI	String to match against HTTP Request's URI field: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Response Header	Enter the Header Name for matching against the HTTP response String to match against HTTP response header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
Response Payload	Signature to match against response payload at the specific offset. Enter a HEX string without whitespace. Specify an offset in the response payload to look for the signature.
User Agent	String to match against HTTP Request's User-agent header: ■ beginsWith ■ endsWith ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

To add additional Rule Conditions, click the **Create** icon.

5 Click the **Save** icon.

HTTP Server

Use this object to specify an HTTP Server.

To add an HTTP Server:

1. Expand **Service Construct** in the tree.
2. Click **HTTP Server**.
3. Configure the parameters as follows:

Table 10-109 HTTP Server Parameters

Parameter	Description
Name	Enter an HTTP Server name.
Admin State	Admin state of HTTP Server: ■ Enabled ■ Disabled
Idle Timeout	Server connection idle timeout, in seconds.
Network Context	Network Context to be used to select the Loopback IP.
Loopback IP	Loopback IP to use to connect to the HTTP Server.
Server IP Address	Server IP address
Server Port	Server port
URL Path	Server URL path

4. Click the **Save** icon.

HTTP Server List

Use this object to specify a list of HTTP Servers.

To add an HTTP Server List:

1. Expand **Service Construct** in the tree.
2. Click **HTTP Server List**.
3. Configure the parameters as follows:
   - **Name** – Enter an HTTP Server List name.
4. Click the **Save** icon.
5. Expand the HTTP Server List you added.
6. To configure the specific HTTP Server, click **HTTP Server**.

7 Configure the parameters as follows:

- **Name** – Enter an HTTP Server name.

8 Click the **Save** icon.

9 Repeat step 6 through step 8 to add as many HTTP Server name as needed.

HTTP URL Rewrite

The HTTP URL Rewrite profile provides a URL substitution function. Rewritten URLs can provide customized response for certain requests, such as shorter and more relevant-looking links to web pages.

Each URL requested in a WSP or HTTP request is checked for a possible substitution against the configured list. The list contains target URLs mapped, one to one, against substitution URLs. Both the target URLs and substitution URLs must contain the host name (which can include a port number) and can contain any number of segments delimited with the "/" character. The substitution is performed before any other URL-dependent action.

To add an HTTP URL Rewrite:

1. Expand **Service Construct** in the tree.
2. Click **HTTP URL Rewrite**.
3. Configure the parameters as follows:
   - **Name** – Enter an HTTP URL Rewrite Profile name.
4. Click the **Save** icon.
5. Expand **HTTP URL Rewrite Profile**.
6. Expand the HTTP URL Rewrite Profile you added.
7. Click **Rewrite Rule**.
8. Configure the parameters as follows:

Table 10-110 Rewrite Rule Parameters

Parameter	Description
Name	Enter a Rewrite Rule name.
Request URL	Specifies the regular expression pattern to match the HTTP Request URL. Must contain a host name and can contain a port number and URL path. Can contain any number of segments delimited with the "/" character. Omit ‘http://’ from the Request URL pattern. Enclose URLs in double quotation marks. Use parentheses in the Request URL pattern to internally create back-references. You can reference them using the strings $N (1 <= N <= 9) for creating the Substitution URL. For example: Request URL: xyz.com/products/([0-9]+)/(\w+) Substitution URL: xyz.com/show_a_product.php?product_id=$1/$2

Table 10-110 Rewrite Rule Parameters

Parameter	Description
Substitution URL	Substitution string to replace the matched HTTP Request URL. Must contain a host name and can contain a port number and URL path. Can contain any number of segments delimited with the "/" character. Omit ‘http://’ from the Substitution URL pattern. Enclose URLs in double quotation marks. Supports back-reference using the strings $N (1 <= N <= 9).
Priority	Rewrite rule priority
Last	Specifies to apply this rule last in this profile, if matched Request URL. When set, any lower priority rules within the profile are ignored.

9 Click the **Save** icon.

IMSI Range

Use this object to generate SGW CDRs based on a list of configured IMSI ranges. This feature applies to all offline-charging interfaces (local, Ga, Gz) and both standalone and co-located SGW sessions.

When the SGW receives a Create Session Request and the SGW **CDR Mode** is configured as imsi-range, the SGW tries to match the subscriber's IMSI with any of the IMSI ranges within the list. If an entry is found, the SGW generates CDRs for that session. If an entry is not found, the SGW does not generate CDRs for the session.

To generate SGW CDRs based on a list of configured IMSI ranges, all offline charging interfaces configured on an MCC SGW must have the **CDR Mode** configured as imsi-range and must be configured with the same IMSI range list.

If an IMSI for a session, which was not generating SGW CDRs initially, is added to the IMSI list, SGW CDRs are generated for subsequent sessions from the same IMSI. However, sessions that exist before an IMSI range is added to a list will not generate SGW CDRs.

To add an IMSI Range:

1. Expand **Service Construct** in the tree.
2. Click **IMSI Range**.
3. Configure the parameters as follows:

Table 10-111 IMSI Range Parameters

Parameter	Description
Name	Enter an IMSI range name.
Start	IMSI range start value
End	IMSI range end value

4. Click the **Save** icon.

IMSI Range List

Use this object to generate SGW CDRs based on a list of configured IMSI ranges. This feature applies to all offline-charging interfaces (local, Ga, Gz) and both standalone and co-located SGW sessions.

When the SGW receives a Create Session Request and the SGW **CDR Mode** is configured as imsi-range, the SGW tries to match the subscriber's IMSI with any of the IMSI ranges within the list. If an entry is found, the SGW generates CDRs for that session. If an entry is not found, the SGW does not generate CDRs for the session.

To generate SGW CDRs based on a list of configured IMSI ranges, all offline charging interfaces configured on an MCC SGW must have the **CDR Mode** configured as imsi-range and must be configured with the same IMSI range list.

Sessions that exist before the IMSI list is configured do not generate SGW CDRs based on a list of configured IMSI ranges.

To add an IMSI Range List:

1. Expand **Service Construct** in the tree.
2. Click **IMSI Range List**.
3. Configure the parameters as follows:

Table 10-112 IMSI Range List Parameters

Parameter	Description
Name	Enter an IMSI range list name.
IMSI Range Name	Enter an IMSI range name. The IMSI range must already exist. See IMSI Range.

4. Click the **Save** icon.

Interface: Accounting Service

Use this object to configure the RADIUS Accounting Service. The Accounting Service references a RADIUS server group previously configured.

To add an Accounting Service:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **Accounting Service**.
4. Configure the parameters as follows:

Table 10-113 Accounting Service Parameters

Parameter	Description
Name	Accounting Interface Profile name
Admin State	Admin state of accounting service: ■ Enabled ■ Disabled
Is OFC Enabled	Controls whether the system stores accounting messages locally to the disk when the remote RADIUS server is unavailable. When the remote server becomes available, the system sends the pending accounting messages. OFC enabled on Accounting Interface: ■ True ■ False
Ignore Radius Failure	Controls whether the GGSN/PGW processes a RADIUS failure response or ignores the failure and continues with the create PDP context/session procedure: ■ True – The GGSN/PGW ignores the RADIUS failure response and continues with the Create PDP Context/Session procedure ■ False – The GGSN/PGW processes the RADIUS failure response and rejects the Create PDP Context/Session Request. By default, if the GGSN/PGW receives a RADIUS (Authorization/Accounting) failure response, it rejects the create PDP context/session request. Set this parameter to true to configure the GGSN/PGW to ignore RADIUS failure responses. ***Note:*** *Changes to this setting take effect immediately.*

Table 10-113 Accounting Service Parameters

Parameter	Description
Wait for Accounting Response	Controls whether the GGSN/PGW waits for an Accounting-Response from the RADIUS Accounting server prior to sending the Create/Delete PDP Context/Session Response: ■ True – The GGSN/PGW waits for an Accounting-Response before sending a Create/Delete PDP Context Response or Create/Delete Session Response to the SGSN/SGW. ■ False – The GGSN/PGW sends the Create/Delete PDP Context Response or Create/Delete Session Response to the SGSN/SGW without waiting for an Accounting-Response. By default, the GGSN/PGW waits for an Accounting-Response from the RADIUS Accounting server prior to sending a Create/Delete PDP Context/Session Response to the SGSN/SGW. Set this parameter to false to configure the GGSN/PGW to send a Create/Delete PDP Context/Session Response without waiting for an Accounting-Response.
NAS Port Type	NAS Port Type to be sent to the remote peer: ■ virtual ■ wireless-other
Acct Session ID Format	Controls whether to include/exclude the PDN session start time in the RADIUS Acct-Session-Id and Acct-Multi-Session-Id AVPs sent in RADIUS Access-Request and Accounting-Request messages. ■ default – The PGW/GGSN does not include the PDN session start time in the Acct-Session-Id and Acct-Multi-Session-Id AVPs sent in RADIUS Access-Request and Accounting-Request messages. ■ include-timestamp – The PGW/GGSN includes the PDN session start time in the Acct-Session-Id and Acct-Multi-Session-Id AVPs sent in RADIUS Access-Request and Accounting-Request messages. ***Note:*** *The Acct-Session-Id and Acct-Multi-Session-Id must be consistent across authorization and accounting messages. Therefore, when the workflow control profile has both a default authorization and default accounting interface configured, the acct-session-id-format configured for the accounting-service takes precedence and applies to the Acct-Session-Id and Acct-Multi-Session-Id AVPs in both the Accounting and Authorization messages.*

Table 10-113 Accounting Service Parameters

Parameter	Description
Apn Reporting	APN to use when reporting APN to external devices: ■ original — Initial APN ■ mapped — Final / current APN ■ prior-mapped — APN mapped prior to the mapped (final / current) APN. This setting allows APN Reporting to continue to be based on the previously-mapped APN (even following a remap to a final APN) ■ custom — Customized Access Point Name (APN) reported on external interfaces. The customized APN is used in the Called-Station-ID AVP in messages in the external interfaces ***Note:*** *The APN Reporting value configured at the interface level overrides the APN Reporting value configured for the Control Profile. If the APN Reporting value is not configured at the interface level, the Called-Station-ID AVP and User-Name AVP will be filled based on the APN Reporting value configured for the Control Profile.*
Interface Type	Interface Type: ■ primary – Interface providing the RADIUS accounting messages to be mirrored. ■ mirrored – Interface on which the mirrored messages are sent.
Delay Failure Handling Until All Responses	Specifies whether the GGSN/PGW waits for the Accounting-Response from all of the RADIUS servers to which an Accounting-Request START message was sent before processing a RADIUS failure response. Once the GGSN/PGW receives all of the Accounting-Response messages, it sends an Accounting-Request STOP to all of the RADIUS servers, except the RADIUS servers for which the Accounting-Request START message failed. ■ true – The GGSN/PGW waits for the Accounting-Response from all of the RADIUS servers to which an Accounting-Request START message was sent before processing a RADIUS accounting failure. After receiving all Accounting-Request START responses, the GGSN/PGW sends an Accounting-Request STOP message to all RADIUS servers, except the RADIUS servers for which the Accounting-Request START message failed. ■ false – The GGSN/PGW processes the RADIUS accounting failure response immediately and sends Accounting-Request STOP messages to only those servers from which it had received an Accounting-Response START message and clears the session. This parameter can only be configured for the primary RADIUS accounting interface and applies for all mirrored RADIUS accounting interfaces configured in the Control Profile with which the primary RADIUS accounting interface is associated. ***Note:*** *Changes to this setting take effect immediately.*

Table 10-113 Accounting Service Parameters

Parameter	Description
Service Node	Service Node: ■ Pdngw - Packet Data Network Gateway
Configure interim updates on the primary accounting interface: ***Note:*** *These parameters are only displayed when the interface type is set to primary. The mirrored accounting interface(s) inherits the configuration for these parameters from the primary accounting interface.*	
Interim Updates	Enable or disable interim updates to the RADIUS server. ■ Enabled ■ Disabled
Interim Update Interval	Specifies the maximum number of seconds that the gateway waits before generating a new accounting record.
Data Volume Limit	Specifies the maximum number of kilobytes that the gateway maintains before generating a new accounting record. The volume usage counts are reset when a accounting record is closed and sent.
Interface Trigger Template	***Note:*** *Deprecated: use Event Trigger Template instead.*
Event Trigger Template	Event Trigger Template to use. The Event Trigger Template must already exist. See Event Trigger Template.
Protocol Type	Protocol Type: ■ RADIUS
Server Group	Select the Server Group for the interface. The Server Group must already exist. See RADIUS Client Server Group.
Start Template	PDN GW Start Record Template
Interim Template	PDN GW Interim Record Template
Stop Template	PDN GW Stop Record Template
Report Rg Usage	Enable or disable Rating-Group-level usage statistics reporting to the Accounting Server: ■ Enabled – The MCC GGSN/PGW sends rating-group level statistics within the SN-Ecs-Data-Volume VSA in Radius Accounting-Request messages. ■ Disabled – The MCC GGSN/PGW does not send rating-group level statistics in Radius Accounting-Request messages.

5 In **Rg Quota List to Report**, configure a list of rating groups to which to report usage statistics. In this case, the SN-Ecs-Data-Volume VSA only contains statistics for the rating groups within the configured rating group quota-id range.

Configure the parameters as follows:

Table 10-114 Rg Quota List to Report Parameters

Parameter	Description
Rg Quota ID Range Name	Rule Group Quota ID name
Rg Quota ID Start	Start of the rating group quota-id range
Rg Quota ID End	End of the rating group quota-id range

6 Click the **Save** icon.

Interface: Authorization Service

The Authorization Service references a RADIUS server group previously configured. The RADIUS access request record attributes can be controlled by associating the service with an access request template.

To add an Authorization Service:

1 Expand **Service Construct** in the tree.

2 Expand **Interface**.

3 Click **Authorization Service**.

4 Configure the parameters as follows:

Table 10-115 Authorization Service Parameters

Parameter	Description
Name	Authorization Interface Profile name
Admin State	Admin state of authorization service: ■ Enabled ■ Disabled
Server Group	Service Profile for the interface
Framed Route Default Metric	Configures a default metric if AAA returns Framed-Routes with missing metrics. If this setting is not configured, a Framed-Route with missing metrics is ignored.

Table 10-115 Authorization Service Parameters

Parameter	Description
Ignore Radius Failure	Controls whether the GGSN/PGW processes a RADIUS failure response or ignores the failure and continues with the create PDP context/session procedure: ■ True – The GGSN/PGW ignores the RADIUS failure response and continues with the Create PDP Context/Session procedure ■ False – The GGSN/PGW processes the RADIUS failure response and rejects the Create PDP Context/Session Request. By default, if the GGSN/PGW receives a RADIUS (Authorization/Accounting) failure response, it rejects the create PDP context/session request. Set this parameter to true to configure the GGSN/PGW to ignore RADIUS failure responses. ***Note:*** *Changes to this setting take effect immediately.*
NAS Port Type	NAS Port Type to be sent to the remote peer: ■ virtual ■ wireless-other
Acct Session ID Format	Controls whether to include/exclude the PDN session start time in the RADIUS Acct-Session-Id and Acct-Multi-Session-Id AVPs sent in RADIUS Access-Request and Accounting-Request messages. ■ default – The PGW/GGSN does not include the PDN session start time in the Acct-Session-Id and Acct-Multi-Session-Id AVPs sent in RADIUS Access-Request and Accounting-Request messages. ■ include-timestamp – The PGW/GGSN includes the PDN session start time in the Acct-Session-Id and Acct-Multi-Session-Id AVPs sent in RADIUS Access-Request and Accounting-Request messages. ***Note:*** *The Acct-Session-Id and Acct-Multi-Session-Id must be consistent across authorization and accounting messages. Therefore, when the workflow control profile has both a default authorization and default accounting interface configured, the acct-session-id-format configured for the accounting-service takes precedence and applies to the Acct-Session-Id and Acct-Multi-Session-Id AVPs in both the Accounting and Authorization messages.*

Table 10-115 Authorization Service Parameters

Parameter	Description
Apn Reporting	APN to use when reporting APN to external devices: ■ original — Initial APN ■ mapped — Final / current APN ■ prior-mapped — APN mapped prior to the mapped (final / current) APN. This setting allows APN Reporting to continue to be based on the previously-mapped APN (even following a remap to a final APN) ■ custom — Customized Access Point Name (APN) reported on external interfaces. The customized APN is used in the Called-Station-ID AVP in messages in the external interfaces ***Note:*** *The APN Reporting value configured at the interface level overrides the APN Reporting value configured for the Control Profile. If the APN Reporting value is not configured at the interface level, the Called-Station-ID AVP and User-Name AVP will be filled based on the APN Reporting value configured for the Control Profile.*
Service Node	Service Node: ■ Ggsn - Gateway GPRS Support Node ■ Pgw - Packet Data Network Gateway ■ Sgw - Serving Gateway
Access Accept Template	Select the associated Access Accept Record template. The Access Request Record template must already exist. Create it at Service Construct > Data Record Template > *Service Node value* > Auth > Radius > Access Accpt.
Access Req Template	Select the associated Access Request Record template. The Access Request Record template must already exist. Create it at Service Construct > Data Record Template > *Service Node value* > Auth > Radius > Access Req.

5 Click the **Save** icon.

Interface: Flow Authorization Interface

The flow authorization interface can be used for subscriber authentication when a Network Address Translation (NAT) IPv4 Address is allocated for an IPv6 UE for the configured services/flows. The MCC flow authorization interface is a Diameter-based interface between the Packet Data Network Gateway (PGW) and Diameter server that processes AA-Request (AAR) messages and sends AA-Answer (AAA) messages back to the PGW.

If a NAT IPv4 Address is allocated for a subscriber when flow authorization is enabled on the NAT service rule (associated with the subscriber firewall flow) and the subscriber's Workflow Control profile is configured with a flow authorization interface, the PGW sends an AAR message to the Diameter server and waits for a response. All packets received on the connection are dropped until the PGW receives a AAA message from the Diameter server. If the authorization is successful, the PGW processes the packets on the flow.

If the authorization fails or the PGW does not receive a response within the configured time limit (Retransmit Timeout), the PGW retransmits the request until the configured retry limit is reached (Retransmit Count). If the configured retry limit is reached and the PGW has not received a response from the Diameter server, the PGW deletes the connection.

To add a Flow Authorization Interface:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **Flow Authorization Interface**.
4. Configure the parameters as follows:

Table 10-116 Flow Authorization Interface Parameters

Parameter	Description
Name	Flow Authorization Interface Profile name
Admin State	Specifies the admin state of the interface. ■ Enabled ■ Disabled
Note: *Affirmed Networks recommends using the default values for the Retransmit Count and Retransmit Timeout parameters. The MCC has an internal timeout timer of 60 seconds after which any received AAA message is ignored. Therefore, the total timeout duration configured for the Retransmit Count and Retransmit Timeout should be less than 60 seconds.*	
Retransmit Count	Specifies the maximum number of retransmit attempts to the Diameter server. The default is 3 retransmit attempts.
Retransmit Timeout	Specifies the time interval to wait before attempting to retransmit, in seconds. The default is 3000 milliseconds.

Table 10-116 Flow Authorization Interface Parameters

Parameter	Description
Auth Aapplication ID	Specifies the application ID (standard or non-standard). This is any value up to 32 bits.

5 Click the **Save** icon.

6 To associate the Diameter server group and data record templates with the flow authorization interface, expand the flow authorization interface you added.

7 Expand **Service Node**.

8 Expand **Pgw**.

9 Expand **Prot Type**.

10 Click **Diameter**.

11 Configure the parameters as follows:

Table 10-117 Flow Authorization Diameter Interface Parameters

Parameter	Description
Server Group	Specify the Service Profile for the selected streaming protocol.
AAR Template	Specify the name of the AA-Request data record template.
AAA Template	Specify the name of the AA-Answer data record template.

12 Click the **Save** icon.

Interface: Gateway Session Learner

Use this object to specify the Mobile Content Cloud Gi Gateway session learner interfaces.

To specify the gateway session learner interfaces:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **Gw Session Learner**.
4. To configure the RADIUS Proxy Session Learner interface (used for WAG and GiGW), click **Radius Proxy**.
5. Configure the parameters as follows:

Table 10-118 RADIUS Proxy Parameters

Parameter	Description
Name	RADIUS Proxy interface name
Admin State	Admin state of RADIUS Proxy gateway session learner interface: ■ Enabled ■ Disabled
Enable UE IPv6	Enable IPv6 user data: ■ True ■ False
Activation Timer Duration	Time to wait for session to fully activate (in seconds). If timer expires, the session is cleared.
Clear Session if Moved	Specifies whether an existing call should be cleared and the session re-established when a session moves from this session learner interface to another: ■ True ■ False

6. In **Radius Client Server Group Mapping**, configure the parameters as follows:

Table 10-119 Server Group Mapping Parameters

Parameter	Description
Priority	Server group mapping priority
Server Group	RADIUS Client Server Group The RADIUS Client Server Group must already exist. See RADIUS Client Server Group.
Mapped APN name	Mapped APN name

Table 10-119 Server Group Mapping Parameters

Parameter	Description
Server Group Type	Server Group type: ■ NotApplicable ■ Authorization ■ Accounting
Generate Accounting Stop	Specify whether to generate and send Accounting stop: ■ disabled ■ enabled
Type of List	Type of list: ■ PLMNID (Specify home-list or roaming list) ■ Realm (Specify the realm-list)
Radius Mapping Message Type	Specifies the name of the RADIUS message type to which this template will be applied. ■ access-request ■ access-accept ■ coa-request
Radius Mapping Template Name	The RADIUS Proxy Server mapping template. The Template must already exist. See RADIUS Mapping Template.

To add additional Server Group Mapping, click the **Create** icon.

7 In **Radius Server**, configure the parameters as follows:

Table 10-120 RADIUS Server Parameters

Parameter	Description
Server Group	RADIUS Server Server Group. The RADIUS Server Server Group must already exist. See RADIUS Server Server Group
Enable Wag L3 Access	Enables a Layer 3 connection to transport user data between the access point (AP) and the TWAG: ■ True ■ False
Radius Mapping Message Type	Specifies the name of the RADIUS message type to which this template will be applied. ■ access-request ■ access-accept ■ access-challenge
Radius Mapping Template Name	The RADIUS mapping template. The Template must already exist. See RADIUS Mapping Template.

To add additional RADIUS Mapping Templates, click the **Create** icon.

8 Click the **Save** icon.

9 To configure the RADIUS Server Session Learner interface (used for GiGW), click **Radius Server**.

10 Configure the parameters as follows:

Table 10-121 RADIUS Server Parameters

Parameter	Description
Name	RADIUS Server interface name
Admin State	Admin state of the RADIUS Server gateway session learner interface: ■ Enabled ■ Disabled
RADIUS Server Server Group	The RADIUS Server Server Group. The RADIUS Server Server Group must already exist. See RADIUS Server Server Group.

11 Click the **Save** icon.

12 To configure the Trusted WLAN Access Gateway interface with no authentication prior to setting up the PDN session, click **Twag Inband Authentication**.

13 Configure the parameters as follows:

Table 10-122 TWAG Inband Authentication Parameters

Parameter	Description
Name	Trusted WLAN Access Gateway interface name
Admin State	Admin state of TWAG RADIUS client gateway session learner interface: ■ Enabled ■ Disabled
APN Name	Default APN to use for PDN session
Enable UE IPv6	Enable IPv6 user data: ■ True ■ False
Activation Timer Duration	Time to wait for session to fully activate (in seconds). If timer expires, the session is cleared.
PLMNID	Default PLMNID to use for non-SIM based UEs. Is used to generate an IMSI for use over the S2a interface.

Table 10-122 TWAG Inband Authentication Parameters

Parameter	Description
Derive IMEI from MAC	Specifies whether to derive IMEI for a UE from its MAC address: ■ true – When the Session Learner interface receives a DHCP message, it creates a pseudo-IMEI from the MAC address received in the DHCP message and uses it as the IMEI in all communication messages going forward. ■ false – The Session Learner interface does not create a pseudo-IMEI when it receives a DHCP message.

14 Click the **Save** icon.

15 To configure a DHCP trigger interface for PDN session setup, expand the Twag Inband Authentication you added.

16 Click **DHCP Trigger Tunnel Interface**. If no VLANS are provisioned, it represents all untagged traffic. If VLANS are provisioned, only sessions on the tunnel with the specific VLANS are selected.

17 Configure the parameters as follows:

Table 10-123 DHCP Trigger Tunnel Interface Parameters

Parameter	Description
Network Context	Network context of tunnel interface
Tunnel Interface	The tunnel interface. The tunnel interface must already exist. Create it at Network Context > *name* > Tunnel.
User Description	Description of the tunnel interface

18 In **VLAN**, configure the parameters as follows:

Table 10-124 VLAN Parameters

Parameter	Description
VLAN Value	Specific VLAN value
VLAN Description	VLAN description

To add additional VLANs, click the **Create** icon.

19 Click the **Save** icon.

20 To configure the Trusted WLAN Access Gateway interface with RADIUS authentication prior to setting up a PDN session, click **Twag Radius Client**.

21 Configure the parameters as follows:

Table 10-125 TWAG RADIUS Client Parameters

Parameter	Description
Name	Trusted WLAN Access Gateway interface name
Admin State	Admin state of TWAG RADIUS client gateway session learner interface: ■ Enabled ■ Disabled
Mode	Mode of Operation: ■ Mode1 ■ Mode2
APN Name	Default APN to use for PDN session
Enable UE IPv6	Enable IPv6 user data: ■ True ■ False
Activation Timer Duration	Time to wait for session to fully activate (in seconds). If timer expires, the session is cleared.
Clear Session if Moved	Specifies whether an existing call should be cleared and the session re-established when a session moves from this session learner interface to another: ■ True ■ False
PLMNID	Default PLMNID to use for non-SIM based UEs. Is used to generate an IMSI for use over the S2a interface.
Derive IMEI from MAC	Specifies whether to derive IMEI for a UE from its MAC address: ■ true – When the Session Learner interface receives a DHCP message, it creates a pseudo-IMEI from the MAC address received in the DHCP message and uses it as the IMEI in all communication messages going forward. ■ false – The Session Learner interface does not create a pseudo-IMEI when it receives a DHCP message.

22 In **DHCP Mapping**, configure the DHCP mapping template. Configure the parameters as follows:

Table 10-126 DHCP Mapping Parameters

Parameter	Description
Message Type	DHCP Message Type: ■ dhcp-discover ■ dhcp-offer ■ dhcp-request ■ dhcp-ack
Template Name	The DHCP mapping template. The Template must already exist. See DHCP Mapping Template.

23 In **DHCP Trigger Tunnel Interface**, configure the DHCP Trigger interface for PDN session setup. If no VLANs are provisioned, it represents all untagged traffic. If VLANs are provisioned, only sessions on the tunnel with the specific VLANs are selected.

Configure the parameters as follows:

Table 10-127 DHCP Trigger Tunnel Interface Parameters

Parameter	Description
Network Context	Network context of tunnel interface
Tunnel Interface	The tunnel interface. The tunnel interface must already exist. Create it at Network Context > *name* > Tunnel.
User Description	Description of the tunnel interface
APN Name	Default APN to use for the PDN session
DHCP Discover	DHCP option value mapping template to apply to this message type. The Template must already exist. See DHCP Mapping Template.
DHCP Offer	DHCP option value mapping template to apply to this message type. The Template must already exist. See DHCP Mapping Template.
DHCP Request	DHCP option value mapping template to apply to this message type. The Template must already exist. See DHCP Mapping Template.
DHCP ACK	DHCP option value mapping template to apply to this message type. The Template must already exist. See DHCP Mapping Template.

To add additional DHCP Trigger Tunnel Interfaces, click the **Create** icon.

24 In **Radius Client**, configure the parameters as follows:

Table 10-128 RADIUS Client Parameters

Parameter	Description
Server Group	RADIUS Client Server Group The RADIUS Client Server Group must already exist. See RADIUS Client Server Group.
User Password	User password to use
Access Request Template	Access Request Record Template The Access Request Record template must already exist. Create it at Service Construct > Data Record Template > *Service Node value* > Auth > Radius > Access Req.
Access Accept Template	Access Accept Record Template The Access Request Record template must already exist. Create it at Service Construct > Data Record Template > *Service Node value* > Auth > Radius > Access Accpt.
CoA Request Template	Change-of-Authorization Request Record Template The CoA Request Record template must already exist. Create it at Service Construct > Data Record Template > *Service Node value* > Auth > Radius > Coa Request.
CoA ACK Template	Change-of-Authorization ACK Record Template The CoA ACK Record template must already exist. Create it at Service Construct > Data Record Template > *Service Node value* > Auth > Radius > Coa Ack.
CoA NACK Template	Change-of-Authorization NACK Record Template The CoA NACK Record template must already exist. Create it at Service Construct > Data Record Template > *Service Node value* > Auth > Radius > Coa Nack.

25 In **Radius Mapping**, configure the RADIUS Client attribute mapping template. Configure the parameters as follows:

Table 10-129 RADIUS Mapping Parameters

Parameter	Description
Message Type	Specifies the name of the RADIUS message type to which this template will be applied. ■ access-request ■ access-accept ■ coa-request
Template Name	The RADIUS mapping template. The Template must already exist. See RADIUS Mapping Template.

To add additional RADIUS Mappings, click the **Create** icon.

26 Click the **Save** icon.

27 To configure the Session Learner GiGw interface with LDAP Client, click **GiGw Ldap Client**.

28 Configure the parameters as follows:

Table 10-130 GiGw LDAP Client Parameters

Parameter	Description
Name	GiGw LDAP interface name
Admin State	Admin state of GiGw LDAP client: ■ Enabled ■ Disabled
LDAP Interface Profile	LDAP interface profile. The LDAP profile must already exist. See LDAP Profile.

29 Click the **Save** icon.

30 To configure the Session Learner GiGw interface with IP trigger and local configuration, click **GiGw IP local**.

31 Configure the parameters as follows:

Table 10-131 GiGw IP Local Parameters

Parameter	Description
Name	GiGw IP with local configuration interface name
Admin State	Admin state of GiGw IP with local configuration interface: ■ Enabled ■ Disabled

32 Click the **Save** icon.

33 To configure the Session Learner TWAG interface with Diameter authentication prior to setting up a PDN session, click **Non 3gpp Access Diameter Client**.

34 Configure the parameters as follows:

Table 10-132 Non 3gpp Access Diameter Client Parameters

Parameter	Description
Name	Non 3gpp Access Diameter Client name

Table 10-132 Non 3gpp Access Diameter Client Parameters

Parameter	Description
Admin State	Admin state of Gateway Session Learner interface: ■ Enabled ■ Disabled
Interface Type	Interface type: ■ STA ■ STM

35 In **Diameter Client Server Group Mapping**, configure the parameters for the Diameter client configuration for Session Learner TWAG interface, as follows:

Table 10-133 Server Group Mapping Parameters

Parameter	Description
Priority	Server group priority
Server Group	Diameter client server group
Mapped APN Name	Mapped Access Point Name The APN must already exist. Create it at Zone > *name* > Gateway > APN.
Type of List	List type: ■ PLMNID: List of PLMNIDs to map to server group ■ Realm: List of realms/usernames to map to server group Select the list name.

To add additional Diameter clients, click the **Create** icon.

36 In **Radius Server Trigger**, select the RADIUS Server Server Group. The RADIUS Server Server Group must already exist. See RADIUS Server Server Group.

37 Click the **Save** icon.

Interface: IPMS Interface

Use this object to configure the IPMS interface group.

To specify the IPMS interface group:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **IPMS Interface**.
4. Click **Server Group**.
5. Configure the parameters as follows:

Table 10-134 Server Group Parameters

Parameter	Description
Name	IPMS Server Group name
Admin State	Admin state of this external IPMS server: ■ Enabled ■ Disabled
IPMS Network Context	Network Context for IPMS interface.
Loopback IP	Signaling port IP Address
Local Port	Local (IPMS) UDP port number
UE IP Network Context	Network Context - UE IP network context

6. In **IPMS Server**, configure the parameters as follows:

Table 10-135 IPMS Server Parameters

Parameter	Description
Name	Name of the external IPMS Server. Must be unique.
Remote IPMS Server IP Address	Remote (IPMS Server) IP address

To add additional IPMS Servers, click the **Create** icon.

7. Click the **Save** icon.

Server Status

Use this object to view status of server group peer.

To view server status:

1. Expand **Server Status**.
2. Expand **Peer Status**.
3. Click an instance.

Peer status parameters are:

- IPMS Interface Name
- IPMS Peer Name
- Operational Status
- Operational Reason
- Admin Status
- Local IP Address
- Local IP Port
- Remote IP Address
- Remote Port

Statistics

Use this object to view IPMS interface statistics.

To view statistics:

1. Expand **Statistics**.
2. Expand **Peer**.
3. Click an instance.

Statistics parameters are:

- num-ue-id-requests-rx
- num-ue-id-answers-tx
- num-ue-id-requests-mmsc-rx
- num-ue-id-requests-ustore-rx
- num-ue-id-requests-ipnms-rx
- num-ue-id-requests-phonebill-rx
- num-ue-id-requests-wap-gw-rx
- num-ue-id-request-etc-rx
- num-ue-id-requests-ipv4-rx

- num-ue-id-requests-ipv6-rx
- num-ue-id-answers-success-tx
- num-ue-id-answers-partial-success-tx
- num-ue-id-answers-invalid-structure-tx
- num-ue-id-answers-system-overload-tx
- num-ue-id-answers-tps-controlled-tx
- num-ue-id-answers-no-subscribers-tx
- num-ue-id-answers-undefined-errors-tx
- num-ue-id-answers-failed-tx
- num-ue-id-answers-ipv4-tx
- num-ue-id-answers-ipv6-tx
- num-ue-id-request-unregistered-server
- num-ue-id-misc-drops

Interface: AAA Interface Group

Use this object to configure the Accounting Authentication Authorization interface group, including Diameter, GTPP, and RADIUS parameters.

AVP Flags

Use this object to configure the default AVP flag values for Diameter AVPs on a specific Diameter interface (Gx, Gy, Gz, SWm, STa, and S6b).

Diameter AVPs have flags that indicate to the receiver how each AVP must be handled in Diameter messages. An AVP can have one or both of these flags set:

- Mandatory “M” flag – Indicates that support for this AVP is required. If either the AVP or its value is not recognized, then the message is not processed.
- Vendor-specific “V” flag – Indicates that this AVP has the optional Vendor ID field and when set, the AVP belongs to the specific vendor code address space.

For example, if the RAT-Type AVP has the Mandatory flag and Vendor-Specific flag set by default, all Diameter messages must have this AVP, otherwise the message is not processed. Also, when this AVP is sent, the Vendor ID field will be populated with the value associated with the specific Vendor.

With this feature, if the Operator changes the RAT-Type AVP Flag setting so that only the Vendor-Specific flag is set for the Gx interface, then subsequent Gx messages may or may not have this AVP. However, the Vendor ID field will still be populated with the value associated with the specific Vendor when this AVP is sent.

To add an AVP flag:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Diameter**.
5. Click **AVP Flags**.
6. Configure the parameters as follows:

Table 10-136 APV Flags Parameters

Parameter	Description
Name	AVP flage name
Attribute ID	Attribute ID
Vendor ID	Vendor ID

7 Click the **Save** icon.

8 Expand the AVP flag you added.

9 Click the Diameter interface for which you want to set a flag value (Gx|Gy|Gz|S6bSta|Swm.

10 Configure the parameters as follows:

- **Flag Value**: Specify the flag value for the Diameter AVP:
  - If an AVP has a non-zero Vendor ID, the possible flag values are vendor-specific and mandatory-and-vendor-specific.
  - If an AVP has a Vendor ID of zero, the possible flag values are none and mandatory.

11 Click the **Save** icon.

Diameter Node Admin

Use this object to configure a Diameter service for each diameter service interface (PCRF, OCS, and OFCS).

To add a Diameter Node Admin:

1 Expand **Service Construct** in the tree.

2 Expand **Interface**.

3 Expand **AAA Interface Group**.

4 Expand **Diameter**.

5 Click **Node Admin**.

6 Configure the parameters as follows:

Table 10-137 Diameter Node Admin Parameters

Parameter	Description
Name	Local Diameter node name
Node Role	Local node role: ■ client ■ server
Origin Host	Local HostName in FQDN. The value is used in the origin-host AVP in the Diameter request message.
Origin Realm	Local Realm Name. The value is used in the origin-realm AVP in the request message.
Network Context	Network Context - selected from VPN Group list Restricts the inbound diameter messages by accepting only inbound messages on the IP interfaces in the interface group.

Table 10-137 Diameter Node Admin Parameters

Parameter	Description
Loopback IP	Signaling port IP Address
Secondary Loopback IP	Signaling port Secondary IP Address This feature adds the ability to configure a secondary loopback IP address for the local Diameter node and Diameter peer to support SCTP Multi-homing. SCTP multi-homing enables the MCC to switchover to an alternate path in the case of a failure on the primary path. The MCC reverts back to the primary path once the primary connection becomes available. The primary and secondary loopback IP addresses can be IPv4, IPv6, or a mix of IPv4/IPv6. MCC supports socket creation to be associated to a single network context. SCTP multi-homing are supported in a single network context. ***Note:*** *Applies only when Transport is set to SCTP.*
Transport	Transport type: ■ TCP ■ SCTP
Port	Signaling port number
Connection Attempt Count	Maximum number of connection retry attempts to the server.
Connection Attempt Timeout	Tc timer, in seconds, as described in RFC 6733. Specifies how frequently to send transport connection attempts to a peer with whom no active transport connection exists.
Cea Timeout	Wait time (in seconds) for receiving a Capability Exchange Answer.
Dwr Timer	Device Watchdog Request timer duration (in seconds). Number of seconds the Diameter node waits for a Device-Watchdog-Answer (DWA) after sending a Device-Watchdog-Request (DWR) to the Diameter peer. ***Note:*** *When the DWR Timer expires, the Diameter node retransmits the DWR to the Diameter peer and the DWR Retry Timer is started.*
Dwr Retry Timer	Device Watchdog Response wait timer duration (in seconds). Number of seconds the Diameter node waits for a DWA after retransmitting a Dwr Retry Timer once the first dwr-timer expires. ***Note:*** *The DWR Retry Timer is typically set at a shorter interval than the DWR Timer.*
Dwr Retry Count	Maximum number of Device Watchdog Retry attempts to the Diameter peer before declaring the peer down.

Table 10-137 Diameter Node Admin Parameters

Parameter	Description
Cer Origin State ID Mode	Specifies whether to increase the value of the Origin-State-Id AVP, sent in CER messages, for every new Diameter connection. When the value of the Origin-State-Id AVP is increased and sent in the CER message, the Diameter peer that receives the message can infer that sessions associated with a lower Origin-State-ID value are no longer active: ■ static – The MCC updates the value of the Origin-State-Id AVP sent in CER messages with the static value, configured using the Cer Origin State ID Static Value parameter. ■ timestamp – For every new Diameter connection, the MCC updates the value of the Origin-State-Id AVP sent in CER messages with the current timestamp. The Diameter peer that receives the message can infer that sessions associated with a lower Origin-State-ID value are no longer active.
Cer Origin State ID Static Value	If Cer Origin State ID Mode is set to static, specify the static Origin-State-Id value sent in CER messages.
Geo Redundant Group	The Geographic Redundancy Group The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.
Net Health Report Enabled	Specifies whether to monitor network health towards the AAA interface: ■ true ■ false
Link Type	Specifies whether the link used to monitor neighboring network elements is a shared link among the primary and secondary NE's or a private (local) link: ■ private ■ shared
Product Name	Diameter product name
Vendor ID	Diameter vendor ID
SCTP Profile	The SCTP attributes used for client connections The SCTP Profile must already exist. See SCTP Profile. ***Note:*** *Applies only when Transport is set to SCTP.*

Table 10-137 Diameter Node Admin Parameters

Parameter	Description
Send Destination Host AVP	Specifies whether to send the Destination Host AVP in the first request to the server before receiving a response: ■ true – The PGW sends the statically configured Destination-Host and Destination-Realm in the initial ACR message to the OFCS via the Gz/Rf interface. ■ false – The PGW does not send the statically configured Destination-Host and Destination-Realm in the initial ACR message to the OFCS via the Gz/Rf interface. The PGW uses the values from the Origin-Host/Origin-Realm AVPs received in the ACA response to fill the Destination-Host and Destination-Realm AVPs in subsequent ACR messages. ***Note:*** *Applies to Gz/Rf interfaces only*

7 Click the **Save** icon.

8 Expand **Node Admin**.

9 Expand the Diameter Node Admin you added.

10 Click **Peer**.

11 Configure the parameters as follows:

Table 10-138 Peer Parameters

Parameter	Description
Host Name	Peer Host name
Peer Identifier	Peer External Identifier
Origin Host	Local Host Name
Origin Realm	Local Realm Name
Dest Realm	Destination Realm Name
Dest IP Address	IP Address of Peer (can be an IPv4 or IPv6 address)
Dest Port	Signaling port number
Role	Primary or secondary (default is primary if not configured). *Primary peers* are active peers used for diameter sessions and *secondary peers* or backup peers are used for diameter sessions only when the active peers are down. When multiple active peers are configured for the diameter interface, the system uses a round-robin approach to select peers.
Backup Peer Name	Backup peer identity.

Table 10-138 Peer Parameters

Parameter	Description
Admin State	Admin state of Diameter Peer. When enabled (default), the system attempts to establish peer connection. The admin state must be disabled prior to deleting or modifying a peer entry.
Override Dest Hostname	Specify the hostname to override. MCC overrides the static configuration for the Destination-Host AVP sent in CCR-Initial messages on the Gy interface.
Secret Key	Secret key string shared for a connection
Secondary Loopback IP	Signaling port Secondary IP Address This feature adds the ability to configure a secondary loopback IP address for the local Diameter node and Diameter peer to support SCTP Multi-homing. SCTP multi-homing enables the MCC to switchover to an alternate path in the case of a failure on the primary path. The MCC reverts back to the primary path once the primary connection becomes available. The primary and secondary loopback IP addresses can be IPv4, IPv6, or a mix of IPv4/IPv6. MCC supports socket creation to be associated to a single network context. SCTP multi-homing are supported in a single network context. ***Note:*** *Applies only when Transport is set to SCTP.*
Weight	Specifies the weight allocated to this Diameter peer. The Diameter peer with the highest weight (10) receives the most distribution of new session requests. The default is 1 (lowest weight). When set to 0, the MCC places the peer in *maintenance mode* and stops sending new session requests (for example, CCR-I) to this peer, but continues to send requests (for example, CCR-Update/CCR-Terminate) for existing sessions. ***Note:*** *Applies to Gy/Gx/Gz/STa/Swm/S6b interfaces.*

12 Click the **Save** icon.

Diameter Node Status

Use this object to display the local Diameter Node operational status.

To view Diameter Node status:

1 Expand **Service Construct** in the tree.

2 Expand **Interface**.

3 Expand **AAA Interface Group**.

4 Expand **Diameter**.

5 Expand **Node Status**.

6 Click a Diameter Node Admin instance.

7 Diameter Node Status parameters are listed in the following table:

Table 10-139 Diameter Node Status Parameters

Parameter	Description
Name	Local Diameter node name
Origin Host	Local HostName in FQDN. The value is used in the origin-host AVP in the diameter request message.
Origin Realm	Local Realm Name. The value is used in the origin-realm AVP in the request message.
Host IP Address	Signaling port IP Address
Transport	Transport type: ■ TCP ■ SCTP
Port	Signaling port number
Geo Redundant Group	Geo Redundant Group
Status	Signaling port Status: ■ In service - the local diameter node is up ready for peer connection establishment. ■ Out of Service - the local diameter node is down.

Peer Command Statistics

Use this object to display the peer command stats.

To view Diameter Node status:

1 Expand **Service Construct** in the tree.

2 Expand **Interface**.

3 Expand **AAA Interface Group**.

4 Expand **Diameter**.

5 Expand **Peer Cmd Stats**.

6 Click a Diameter Peer instance.

Peer Command statistics parameters are listed in the following table:

Table 10-140 Peer Command Status Parameters

Parameter	Description
Node Name	Local Diameter node name

Table 10-140 Peer Command Status Parameters

Parameter	Description
Host Name	Peer host name FQDN
Command Code	Diameter command code
Realm	Peer realm name
Number OUT Request	Total number of requests of the command sent to the peer
Number OUT Response	Total number of responses for the command sent to the peer
Number IN Request	Total number of requests received from the peer
Number IN Response	Total number of responses received from the peer

Peer Statistics

Use this object to view the total number of inbound/outbound requests/responses, protocol errors and failures for each peer communication.

To view peer statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Diameter**.
5. Expand **Peer Stats**.
6. Click a Diameter Peer instance.

Peer statistics parameters are listed in the following table:

Table 10-141 Peer Statistics Parameters

Parameter	Description
Node Name	Local Diameter node name
Host name	Peer host name FQDN
Realm	Peer Realm name
Num Protocol Error	Total number of protocol errors
Num Permanent Failure	Total number of request failures to the peer
Num Routing Failure	Total number of routing failures to the peer
Num Out Request	Total number of requests sent to the peer
Num Out Response	Total number of responses sent to the peer

Table 10-141 Peer Statistics Parameters

Parameter	Description
Num In Request	Total number of requests received from the peer
Num In Response	Total number of responses received from the peer

Peer Status

Use this object to display the peer connection status.

To view Peer status:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Diameter**.
5. Expand **Peer Status**.
6. Click a Diameter Peer instance.
7. Diameter Peer Status parameters are listed in the following table:

Table 10-142 Peer Status Parameters

Parameter	Description
Node Name	Local Diameter node name
Host Name	Peer Host name FQDN
Realm	Peer Realm Name
IP Address	IP Address of Peer (can be an IPv4 or IPv6 address)
Port	Peer port number
Transport	Transport type: ■ TCP ■ SCTP
Role	Primary or secondary (default is primary if not configured). *Primary peers* are active peers used for diameter sessions and *secondary peers* or backup peers are used for diameter sessions only when the active peers are down. When multiple active peers are configured for the diameter interface, a round-robin approach is used to select peers.
Backup Host Name	Backup server identity. Only allowed for secondary peer.

Table 10-142 Peer Status Parameters

Parameter	Description
Status	Peer Status: ■ INITIAL - the initial state of the peer connection when first created. The peer connection has never been opened. ■ OKAY - the connection is up ■ OKAY-FLOWOFF - the connection is up, but the flow status is OFF, indicating that PGWs cannot send CCR messages to that peer.
Last State Change Timestamp	Time when the peer status last changed

Diameter Performance Statistics

Use this object to view the Diameter performance statistics for the Gx, Gy, and Gz interfaces.

To view Diameter performance statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Diameter**.
5. Expand **Statistics**.
6. Expand **Cluster Level**.
7. Expand **Peer**.
8. Expand **Diameter Interface Type**.
9. Click a Diameter Peer instance to view the statistics.

GTPP Node Admin

Use this object to configure a GTPP service.

To add a GTPP Node Admin:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **GTPP**.
5. Click **Node Admin**.
6. Configure the parameters as follows:

Table 10-143 GTPP Node Admin Parameters

Parameter	Description
Name	Local GTPP node name
Admin State	Admin State of the GTPP Service Profile: ■ enabled ■ disabled
Version	3gpp 32.298 version type: ■ 8.4 ■ 9.0
Network Context	Network Context - selected from VPN Group list
Host Port	Server group host port number
Loopback IP	Server group host IP Address
Geo Redundant Group	The Geographic Redundancy Group The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.
Data Record Response as Echo Success	Specifies whether to consider a CDR Data Record Transfer Response an Echo Response over the Ga interface: ■ enabled ■ disabled When enabled, MCC considers a Data Record Transfer Response received during the Echo Response timeout period to be a successful Echo Response, in order to maintain the primary active link from the PGW to the CGF over the Ga interface.
Peer Transaction Window Size	Maximum number of CDR transactions allowed in the queue per GTPP server group across all gateway tasks. If this parameter is not configured, the MCC uses the value configured for the Peer > Pacer Max Transactions Per Interval parameter. When neither this parameter and Peer > Pacer Max Transactions Per Interval is configured, the default value of 128 transactions per task is set. If a GTPP server group is not shared by both the SGW and PGW, it is recommended that you set this parameter to twice the expected amount. If the number of outstanding transactions exceeds the value set for this parameter, the MCC declares the GTPP server group congested and no other transaction can be initiated until the congestion is cleared. Unsent CDR messages are buffered both in memory and on disk and retransmitted once the congestion state clears.

7 Click the **Save** icon.

8 To specify the Data Record Format Version sent in the data record packet for CDR encoding, expand **Node Admin**.

9 Expand the GTPP Node Admin you added.

10 Click **GA Record Version**.

11 Configure the parameters as follows:

Table 10-144 GA Record Version Parameters

Parameter	Description
Application Identifier	Identifies the CDR application. For example, the Application Identifier has a value of 1 (decimal) if used for charging purposes.
Release Identifier	Indicates the 3GPP TS 32.298 release used to encode the CDR. The Release Identifier value corresponds to the first digit of the version number of the 3GPP TS 32.298 document, as shown on the cover sheet. Values include: ■ 8 ■ 9 ■ 10 ■ 11 ■ 12
Version Identifier	Identifies the version of the 3GPP TS 32.298 document used to encode the CDR. The Version Identifier value corresponds to the second digit in the version number of the 3GPP TS 32.298 document, as shown on the cover sheet, plus 1. For example, the Version Identifier for version 10.8.0 is 9. ***Note:*** *The system does not automatically generate the fields in interim and stop data record templates according to the 3GPP 32.298 release identified in this parameter. Operators must configure the interim and stop data record templates accordingly.*

12 Click the **Save** icon.

13 To configure the peer, expand **Node Admin**.

14 Expand the GTPP Node Admin you added.

15 Click **Peer**.

16 Click a peer instance.

17 Configure the parameters as follows:

Table 10-145 Peer Parameters

Parameter	Description
Name	Peer CGF name

Table 10-145 Peer Parameters

Parameter	Description
IP Address	IP Address of Peer
Port	Signaling port number
Transport	Transport type: ■ TCP ■ UDP
Role	Primary or secondary (default is primary if not configured).
Admin State	Admin state of GTPP Peer. When enabled (default), the system attempts to establish a peer connection. ■ enabled ■ disabled
Data Record Max Retries	Maximum number of retries for sending data record
Data Record Response Timeout	Data record response timeout, in seconds
Echo Max Retries	Maximum number of echo request attempts
Echo Response Timeout	Echo response timeout, in seconds
Periodic Health Check Timeout	Periodic health check interval, in seconds
Pacer Max Transactions Per Interval	Maximum number of outstanding Data Record Transfer Requests sent to a GTPP peer per time interval.
Pacer Time Interval	The CDR transaction time interval, in milliseconds, after which the pacer resets its outgoing transaction count. ***Note:*** *Applies only when Pacer Max Transactions Per Interval is set to a value.*

18 Click the **Save** icon.

GTPP Node Status

Use this object to display the GTPP Service Server Group status.

To view GTPP Node status:

1 Expand **Service Construct** in the tree.

2 Expand **Interface**.

3 Expand **AAA Interface Group**.

4 Expand **GTPP**.

5 Expand **Node Status**.

6 Click an instance.

7 GTPP Node Status parameters are listed in the following table:

Table 10-146 GTPP Node Status Parameters

Parameter	Description
Name	GTPP Server Group name
Admin Status	GTPP Server Group Admin Status
Oper Status	GTPP Server Group Oper Status
Host Port	Server group host port number
Host IP Address	Server group host IP address
Dropped Packets	Number of dropped packets
Duplicate Packets	Number of duplicate packets
Sequence Over Run Packets	Number of packets with duplicate sequence numbers

Peer Command Statistics

Use this object to display the number of protocol messages sent to/from the peer.

To view GTPP Node status:

1 Expand **Service Construct** in the tree.

2 Expand **Interface**.

3 Expand **AAA Interface Group**.

4 Expand **GTPP**.

5 Expand **Peer Cmd Stats**.

6 Click an instance.

Peer Command statistics parameters are listed in the following table:

Table 10-147 Peer Command Status Parameters

Parameter	Description
Host Name	Local GTPP Node name
Name	Peer Host name
Echo Req Transmitted	Number of Echo Request messages transmitted.
Echo Resp Received	Number of Echo Response messages received.
Echo Req Received	Number of Echo Request messages received.

Table 10-147 Peer Command Status Parameters

Parameter	Description
Echo Resp Transmitted	Number of Echo Response messages transmitted.
Node Alive Req Transmitted	Number of Node Alive Request messages transmitted.
Node Alive Resp Received	Number of Node Alive Response messages received.
Node Alive Req Received	Number of Node Alive Request messages received.
Node Alive Resp Transmitted	Number of Node Alive Response messages transmitted.
Data Record Req Transmitted	Number of Data Record Request messages transmitted.
Data Record Resp Received	Number of Data Record Response messages received.
Redirection Resp Received	Number of Redirection Response messages received.
Redirection Resp Transmitted	Number of Redirection Response messages transmitted.
Potential Duplicate Rec Transmitted	Number of Potential Duplicate Record Data Records transmitted.
Potential Duplicate Empty Rec Transmitted	Number of Potential Duplicate Empty Data Record messages transmitted.
Cancel Req Transmitted	Number of Cancel Request messages transmitted.
Release Req Transmitted	Number of Release Request messages transmitted.
Potential Duplicate Record Received	Number of Potential Duplicate Record Data Records received.
Request Accepted Received	Number of Request Accepted messages received.
Request Fulfilled Received	Number of Request Fulfilled messages received.

Peer Statistics

Use this object to view the total number of aggregate messages and generic errors sent to/from the peer.

To view peer statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **GTPP**.
5. Expand **Peer Stats**.
6. Click a GTPP Peer instance.

Peer statistics parameters are listed in the following table:

Table 10-148 Peer Statistics Parameters

Parameter	Description
Host name	Local GTPP node name
Num Protocol Error	Total number of protocol errors
Num Permanent Failure	Total number of request failures to the peer
Num Routing Failure	Total number of routing failures to the peer
Num Pacer No Credit Failure	Total number of requests failed due to no credit available at pacer
Num Out Request	Total number of requests sent to the peer
Num Out Response	Total number of responses sent to the peer
Num In Response	Total number of responses received from the peer
Num Link Bounces	Total number of times link is bounced
Num Decode Resume Acknowledge	Total number of resume acknowledge decode success
Num Decode Resume Notification	Total number of resume notification decode success
Num Decode Suspend Acknowledge	Total number of suspend acknowledge decode success
Num Decode Suspend Notification	Total number of suspend notification decode success
Num Encode Resume Acknowledge	Total number of resume acknowledge encode success
Num Encode Resume Notification	Total number of resume notification encode success
Num Encode Suspend Acknowledge	Total number of suspend acknowledge encode success
Num Encode Suspend Notification	Total number of suspend notification encode success
Num Resume Acknowledge Decode Failure	Total number of resume acknowledge decode failure
Num Resume Acknowledge Encode Failure	Total number of resume acknowledge encode failure
Num Resume Notification Decode Failure	Total number of resume notification decode failure
Num Resume Notification Encode Failure	Total number of resume notification encode failure

Table 10-148 Peer Statistics Parameters

Parameter	Description
Num Suspend Acknowledge Decode Failure	Total number of suspend acknowledge decode failure
Num Suspend Acknowledge Encode Failure	Total number of suspend acknowledge encode failure
Num Suspend Notification Decode Failure	Total number of suspend notification decode failure
Num Suspend Notification Encode Failure	Total number of suspend notification encode failure
Pacer High Water Mark	Highest number of credits requested across all intervals

Peer Status

Use this object to display the GTPP peer link status.

To view GTPP peer status:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **GTPP**.
5. Expand **Peer Status**.
6. Click a GTPP Peer instance.
7. GTPP Peer Status parameters are listed in the following table:

Table 10-149 Peer Status Parameters

Parameter	Description
Node Name	Local GTPP node name
IP Address	IP Address of Peer
Port	Peer port number
Transport	Transport type: ■ TCP ■ UDP
Role	Primary or secondary (default is primary if not configured).
Admin Status	Peer node admin status

Table 10-149 Peer Status Parameters

Parameter	Description
Oper Status	Peer node oper tatus: ■ OKAY - the connection is up ■ SUSPECT - failover has been initiated on the connection. ■ DOWN - connection has been closed. ■ REOPEN - attempting to reopen a closed connection ■ INITIAL - the initial state of the peer connection when first created. The peer connection has never been opened.
Data Record Retry Count	Max number of retried for sending data record
Data Record Response Timeout	Data record response timeout, in seconds
Echo Retry Count	Max number of echo request attempts
Echo Response Timer	Echo response timeout, in seconds
Periodic Health Check Timer	Periodic health check interval, in seconds

GTPP Performance Statistics

Use this object to view the GTPP performance statistics.

To view GTPP performance statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **GTPP**.
5. Expand **Statistics**.
6. Expand **Cluster Level**.
7. Expand **Peer**.
8. Expand **Node Name**.
9. Click a GTPP Peer instance to view the statistics.

RADIUS Client Server Group

The RADIUS client server group is a container for a group or list of RADIUS server peers. Each RADIUS server group contains a list of peers (RADIUS servers) with which the system communicates.

You must configure separate server groups for RADIUS authorization and RADIUS accounting. The RADIUS server groups can be attached to either an authorization interface or an accounting interface.

Whenever a RADIUS client does not receive response from a server, it tries another active server in the server group (the server must serve the same subscribers). This feature helps reduce subscriber session failures when one server is down or during a short failure.

To add a RADIUS Client Server Group:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Radius Client**.
5. Click **Server Group**.
6. Configure the parameters as follows:

Table 10-150 Server Group Parameters

Parameter	Description
Name	RADIUS Server group name
Geo Redundant Group	The Geographic Redundancy Group. The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.

Table 10-150 Server Group Parameters

Parameter	Description
Remote Health Check	The Remote Health Check procedure maintains the client RADIUS peer status based on the actual status of the remote RADIUS Server. Specifies whether the Server Group requires the Remote Health Check procedure: ■ true ■ false When Remote Health Check is set to true and a RADIUS peer interface is configured, the MCC triggers the ERHC procedure. The RADIUS client sends a RADIUS Auth/Acct health check message (depending on the configured Server Group Type) and waits for the response. Based on the response, the RADIUS client updates the Oper State of the applicable RADIUS peer interface to UP and sends an indication to the OFC agent (provided that this is the first RADIUS peer in which the status is set to UP for that server group). The peer is moved from the Configured List to the Active Peer List and the peer is ready to serve.
Remote Health Check Period	Time period between remote health check procedures, in seconds.
Remote Health Check Response Period	Remote health check response wait time, in seconds
Remote Health Check Retry Count	Number of times to retry health check before declaring remote server as down
Server Group Type	Server Group type: ■ NotApplicable ■ Authorization ■ Accounting
NAS IP Address	NAS IP Address to be used in RADIUS request messages for multiple peers within the RADIUS server group. ***Note:*** *If you do not configure the NAS IP Address, the MCC device sends the RADIUS peer's local loopback address in the NAS IP Address attribute.*
NAS Identifier	NAS Identifier to be used in RADIUS request messages for multiple peers within a single RADIUS client server group. ***Note:*** *If you do not configure the NAS Identifier, the MCC device sends a string form of the RADIUS peer's local loopback address in the NAS Identifier attribute.*
Net Health Report Enabled	Specifies whether to monitor network health towards the AAA interface: ■ true ■ false

Table 10-150 Server Group Parameters

Parameter	Description
Link Type	Specifies whether the link used to monitor neighboring network elements is a shared link among the primary and secondary NE's or a private (local) link: ■ private ■ shared
Session Aware Peer Selection	Specifies whether to support session aware peer selection: ■ true – All RADIUS Accounting requests for a given session are sent to the same RADIUS peer. If a RADIUS peer is unavailable, the subsequent RADIUS Accounting Messages are transmitted to other active peers in the same RADIUS Server Group (in a round-robin fashion) ■ false – RADIUS Accounting requests for a given session are sent to Peers selected in round-robin fashion.
Peer Retry Mode	***Note:*** *Disable the Admin State of all RADIUS server peers in the RADIUS server group before modifying this parameter.* Specifies peer retry mode: ■ Sequential – If the device does not receive a response from a remote RADIUS server peer within the configured time limit, it retransmits the request to the *same* peer (until the request retry limit is reached) before selecting another active peer in the same group (in a round-robin fashion). ■ Alternate – If the device does not receive a response from a remote RADIUS server peer within the configured time limit, it retransmits the request to the *next* active peer in the same group (in a round-robin fashion). ■ Alternate with Priority – All new requests are sent to the RADIUS server peer with the highest priority (with 1 being the highest). If the RADIUS server peer with the highest priority is unavailable, the request is sent to the peer with the next highest priority in the same group. If multiple RADIUS server peers are assigned the highest priority (1), the RADIUS client (running on the MCC GW) uses a round-robin approach to select from among those peers for new requests.
Response Expected	Controls whether the MCC gateway should expect a response from the mirrored RADIUS accounting server(s) (server to which mirrored messages are sent): ■ true – The MCC gateway expects to receive a response from the RADIUS accounting servers in this RADIUS server group. ■ false – The MCC gateway does not expect to receive a response from the RADIUS accounting servers in this RADIUS server group and as a result, the RADIUS accounting servers remain in an operationally Up state. When set to false, RADIUS Health Check must be disabled for this RADIUS server group.

Table 10-150 Server Group Parameters

Parameter	Description
Pacer Max Transactions per Interval	Specifies the maximum number of transactions sent to a RADIUS peer per time interval.
Pacer Time Interval	Specifies the RADIUS transaction time interval, in milliseconds, after which the pacer resets its outgoing transaction count. ***Note:*** *The value configured for the Pacer Max Transactions per Interval is shared between multiple CSMs in one cluster.*

7 Click the **Save** icon.

8 Expand **Server Group**.

9 Expand the RADIUS Client Server Group you added.

10 Click **Peer**.

11 Configure the parameters as follows:

Table 10-151 Peer Parameters

Parameter	Description
Name	Peer RADIUS client name
Admin State	Admin State: ■ enable ■ disabled ■ maintenance
Secret Key	Secret key string shared for a connection
Network Context	Network Context - selected from VPN Group list
Remote IP Address	Remote IP Address
Loopback IP	Signaling port IP Address
Local Port	Local Signaling port number
Remote Port	Remote Signaling port number
Max Num Response Timeout	Maximum number of retransmit attempts allowed for a server group after which the RADIUS client rejects the request. ***Note:*** *Affirmed Networks recommends that all RADIUS server peers within a server group use the same value for this parameter. If the peers use different values, any of the values may apply.*
Server Type	Peer Server Type: ■ Primary ■ Secondary

Table 10-151 Peer Parameters

Parameter	Description
Server Resp Timeout Value	Number of seconds to wait before the system retransmits the request either to the same RADIUS server peer (if it is the only one in the server group) or to the next active peer in the server group.
Server Dead Timeout Value	Number of seconds to wait before attempting to reconnect to the non-responsive RADIUS server peer after moving the peer from a pending state to an inactive state. For more information, see the *Affirmed Networks RADIUS Interface Specification*.
Server Dead Num Attempts	Number of consecutive unanswered requests allowed for a peer before the system declares a RADIUS server peer down.
Num Local Ports	Number of RADIUS client ports per RADIUS peer. The value configured for this parameter is in addition to one port used for net health. For RADIUS peers configured with normal (non-VRF-lightweight) network contexts, when adding more RADIUS peers, this value must be reduced to meet the following criteria: **Total peers * (Num Local Ports + 1) < 3000**
Priority	Specifies the RADIUS server peer priority within the RADIUS server group (round-robin among the highest priority peers). ***Note:*** *Affirmed Networks recommends only using this parameter when the Peer Retry Mode parameter is set to Alternate with Priority.*
Disable the Admin State of the remote RADIUS server peer before modifying either of the following parameters:	
Disconnect Coa Server Admin State	Specifies whether to receive and process Disconnect-Request messages from the server. ■ enabled ■ disabled
Disconnect Coa Local Server Port	Specify the Local RADIUS server UDP port number to which Disconnect-Request messages are sent. ***Note:*** *Ensure that the disconnect local server port does not conflict (same IP and same port) with the local port range of any of the configured RADIUS server peers.* *If multiple RADIUS server peers have the same local IP and the same disconnect local server port, only one RADIUS disconnect server is instantiated.*

12 Click the **Save** icon.

RADIUS Procedure Statistics

Use this object to view RADIUS service procedure statistics.

To view RADIUS statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Radius Client**.
5. Expand **Statistics**.
6. Expand **Cluster Level**, **Grid Level**, or **Slot Level**.
7. Expand **Proc Stats**.
8. To view statistics for all peers, expand **All**.

   To view statistics for a particular peer, expand **Peer**.
9. Click an instance.

Peer command statistics parameters are listed in the following table:

Table 10-152 RADIUS Service Procedure Statistics Parameters

Parameter	Description
Num Access Req Tx	Number of Access Requests sent to peer
Num Access Accept Rx	Number of Access Accepts received from peer
Num Access Reject Rx	Number of Access Rejects received from peer
Num Access Challenge Rx	Number of Access Challenges received from peer
Num Account Request Start Tx	Number of Account Request Starts sent to peer
Num Account Request Start Resp Rx	Number of Account Request Starts Responses received from peer
Num Account Request Stop Tx	Number of Account Request Stop sent to peer
Num Account Request Stop Resp Rx	Number of Account Request Stop Responses received from peer
Num Account Request Interim Update Tx	Number of Account Request Interim Update sent to peer
Num Account Request Interim Update Resp Rx	Number of Account Request Interim Update Responses received from peer
Num Disconnect Request Rx	Number of Disconnect Request received from peer
Num Disconnect Ack Tx	Number of Disconnect ACK sent to peer

Table 10-152 RADIUS Service Procedure Statistics Parameters

Parameter	Description
Num Disconnect Nack Tx	Number of Disconnect NACK sent to peer
Num Coa Request Rx	Number of Coa Request received from peer
Num Coa Ack Tx	Number of Coa ACK sent to peer
Num Coa Nack Tx	Number of Coa NACK sent to peer
Num Account Request On Tx	Number of Account Request On sent to peer
Num Account Request On Resp Rx	Number of Account Request On Responses received from peer
Num Account Request Off Tx	Number of Account Request Off sent to peer
Num Account Request Off Resp Rx	Number of Account Request Off Responses received from peer

RADIUS Client Server Status

Use this object to view RADIUS Client Server Group and peer status information.

To view RADIUS peer and RADIUS Client Server Group status:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **RADIUS Client**.
5. Expand **Server Status**.
6. Expand **Peer Status**.
7. Click a RADIUS Peer instance.
8. Detailed Server Group Peer Status parameters are listed in the following table:

Table 10-153 Server Group Peer Status Parameters

Parameter	Description
RADIUS Server Group Name	RADIUS Server Group name
RADIUS Peer Name	RADIUS Peer name
Slot	Slot number
Operational Status	Operational Status
Operational Reason	Operational Reason if state is Operationally Down
Admin Status	Admin Status

Table 10-153 Server Group Peer Status Parameters

Parameter	Description
Local IP Address	Local IP Address of RADIUS Interface. Can be IPv4/IPv6.
Local Port Start	Starting local port number
Local Port End	Ending local port number
Remote IP Address	Remote IP Address of RADIUS Interface. Can be IPv4/IPv6/
Remote Port	Remote Port Number
Priority	RADIUS server peer priority within the RADIUS server group

9 Expand **Server Group Status**.

10 Click a Server Group instance.

11 Server Group Peer Status parameters are listed in the following table:

Table 10-154 Server Group Status Parameters

Parameter	Description
Name	RADIUS Server Group name
Operational Status	Operational Status

12 Expand **Server Group Peer Status**.

13 Click a Server Group Peer instance.

14 Server Group Peer Status parameters are listed in the following table:

Table 10-155 Server Group Peer Status Parameters

Parameter	Description
RADIUS Server Group Name	RADIUS Server Group name
RADIUS Peer Name	RADIUS Peer name
Operational Status	Operational Status
Admin Status	Admin Status

RADIUS Server Server Group

To add a RADIUS Server Server Group:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Radius Server**.
5. Click **Server Group**.
6. Configure the parameters as follows:
   - **Name**: RADIUS Server group name
   - **DSCP Value**: Select the DiffServ Code Point value with which to mark all IP packets on this server group.
7. Click the **Save** icon.
8. Expand **Server Group**.
9. Expand the RADIUS Server Server Group you added.
10. Click **Server**.
11. Configure the parameters as follows:

Table 10-156 Server Parameters

Parameter	Description
Name	Peer RADIUS client name
Admin State	Admin State: ■ enable ■ disabled ■ maintenance
Network Context	Network Context - selected from VPN Group list
Note: *A RADIUS server server-group can be configured with either a Server IP Address or an External Server IP Address, but not both.*	
Server IP Address	RADIUS server IP Address
Ext Server IP Address	RADIUS external server IP Address Specifies the IP address of an external RADIUS server. Can be IPv4 or IPv6. When this parameter is configured, the system mirrors RADIUS Accounting-Request messages, received from a RADIUS client, to the GiGW and then forwards these Accounting-Request messages to an external RADIUS server.

Table 10-156 Server Parameters

Parameter	Description
Server Port	RADIUS server listening UDP port number When the Ext Server IP Address parameter is configured, this parameter specifies the port number of the external RADIUS server to which RADIUS Accounting-Requests are sent when mirrored to the GiGW.

12 Click the **Save** icon.

13 Expand the server you added.

14 Click **Client**.

15 Configure the parameters as follows:

Table 10-157 Client Parameters

Parameter	Description
Name	Radius client name
Client IP Address	Radius client IP address
Secret Key	Secret key string shared for a connection ***Note:*** *Does not apply when the Ext Server IP Address parameter is configured.*
Suppress Radius Response	Specifies whether Radius response is needed for this Radius client: ■ Enabled ■ Disabled
Send Radius Disconnect Request	Whether to send Radius disconnect request to Radius client when session is terminated by network: ■ True ■ False ***Note:*** *Applies only to non3GPP style WAG:*
Disconnect Client Port	Radius client listening UDP port number ***Note:*** *Applies only to non3GPP style WAG:*

16 Click the **Save** icon.

Statistics

Use this object to view the RADIUS Server Group statistics.

To view RADIUS Server Group Statistics:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Expand **AAA Interface Group**.
4. Expand **Radius Server**.
5. Expand **Statistics**.
6. Expand **Cluster Level**.
7. Expand **Server Stats**.
8. Expand **All** or **Server**.
9. Click an instance.

   The statistics are:

   - Num Rx: Number of messages received
   - Num Access Req Rx: Number of access requests received
   - Num Account Req Rx: Number of account requests received
   - Num Drop Errors Rx: Number of received messaged dropped in error
   - Num Access Accept Tx: Number of access accepts sent
   - Num Access Reject Tx: Number of access rejects sent
   - Num Access Challenge Tx: Number of access challenges sent
   - Num Account Resp Tx: Number of account responses sent

Interface: Offline Charging

Use this object to configure an Offline Charging Interface Profile.

To add an Offline Charging Interface Profile:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **Offline Charging**.
4. Configure the parameters as follows:

Table 10-158 Offline Charging Parameters

Parameter	Description
Name	Offline Charging interface profile name
Admin State	Admin state of Offline Charging interface: ■ Enabled ■ Disabled
Service Context ID	Service Context ID content (Maximum length 64 characters)
Session ID Format	Format for the Session-Id AVP sent on the Gz/Rf interface: ■ v0 – The Session-ID AVP format represents the optional value for the session setup time in decimal format. For example: *example.com;1450803134;2148532240;8;**1450812272**;262229* where ***1450812272*** represents the session setup time in decimal format. ■ v1 – The Session-ID AVP format represents the optional value for the session setup time in hex format. This format applies to the Gz/Rf interface only. For example: ***01**-example.com;1450803134;2148532240;8;**5679A370**-262229* where ***01*** is a prefix indicating that this Session-ID format is using version 1 (v1) and ***5679A370*** represents the session setup time in hex format. Note that the delimiter after the timestamp uses a dash (-) instead of a semi-colon (;).

Table 10-158 Offline Charging Parameters

Parameter	Description
User Name Type	Offline Charging User Name Type (format) to be used if not present in PCO: ■ apn ■ default-username ■ imsi ■ imsi-plus-apn ■ imsi-plus-apnnionly ■ msisdn ■ msisdn-plus-apn ■ msisdn-plus-apnnionly ■ imsi-nai-prefix-0 ■ imsi-nai-no-prefix ■ none This setting overrides the **user name type** present at the APN level. However, if this User Name Type parameter is set to **none**, the APN level **user name type** is used.
CDR Report Level	Specifies the level at which to generate CDRs: ■ bearer: generates offline charging CDRs sent via the Gz/Rf interface to the OFCS at the bearer level ■ pdn-session: enables session-level Gz/Rf CDR reporting based on the default bearer. MCC sends the Start CDR when the default bearer is activated upon initial session setup. When session-level Gz/Rf CDR reporting is enabled, ensure that the local interface for offline charging is disabled. ***Note:*** *Applies to Gz/Rf CDRs only.*
Service Node	Service Node: ■ GGSN - Gateway GPRS Support Node ■ PGW - Packet Data Network Gateway ■ SGW - Serving Gateway ■ WAG - Wireless Access Gateway

Table 10-158 Offline Charging Parameters

Parameter	Description
Suppress Zero Traffic Containers	Suppress the creation of service containers in PGW/GGSN CDRs for service rules with no traffic: ■ enabled – When generating CDRs, the MCC does not create service containers for service rules with no traffic. ■ disabled – When generating CDRs, the MCC creates service containers for service rules with no traffic. All service rules configured as event triggers, such as QoS change or ULI change, will have at least one service container even when the MCC is configured to suppress the creation of service containers for service rules with no traffic. This is to indicate the event trigger. This feature applies to PGW/GGSN CDRs (CSV/ASN.1 format) for each offline interface (local/Ga/Gz).
Interim Updates	Interim updates to the Offline Charging Server: ■ Enabled ■ Disabled
Interim Update Interval	Specifies the maximum number of seconds that the gateway waits before generating a new CDR. The timer resets when a CDR is sent.
Data Volume Limit	Specifies the maximum number of kilobytes that the gateway maintains across all service containers (for a bearer) before generating a new CDR. The volume usage counts are reset when a CDR is closed and sent.
Interface Trigger Template	***Note:*** *Deprecated: use Event Trigger Template or Gy Event Trigger Template instead.*
Event Trigger Template	Event Trigger Template to use. The Event Trigger Template must already exist. See Event Trigger Template.
Gy Event Trigger Template	Gy Event Trigger Template to use for CDR close. The Gy Event Trigger Template must already exist. See Health Check Profile.
Encode NAI In ASN1 MSISDN	Specifies to include/exclude the Nature of Address Indicator (NAI) in the Served Mobile Subscriber Integrated Services Digital Network-Number (MSISDN) field when generating SGW local ASN.1 and GTPP CDRs. Previously, it was only available for PGW/GGSN local ASN.1 and GTPP CDRs. ■ Enabled ■ Disabled When enabled, the NAI is included in the Served MSISDN field when generating SGW local ASN.1 and GTPP CDRs.

Table 10-158 Offline Charging Parameters

Parameter	Description
Num Service Containers	If interim updates are enabled on the interface, specifies the maximum number of service containers that the gateway maintains per CDR at the bearer-level. Upon reaching this limit, the gateway transfers the service containers in an interim CDR to the offline server.
CDR Close Time	If interim updates are enabled on the interface, specifies the maximum number of seconds for storing closed service containers before transferring service containers in an interim CDR to the offline server.
CDR Mode	Controls the SGW mode for generating SGW CDRs: ■ stand-alone – SGW CDRs are generated only for stand-alone SGW sessions (home or roaming). Stand-alone SGW sessions have PGW sessions anchored on a device other than the MCC. ■ roam-in – SGW CDRs are generated only for a subset of stand-alone SGW sessions that are roaming-in (the subscriber's PLMN is part of the roaming PLMN list configured on the SGW). ■ co-located – SGW CDRs are generated for both stand-alone SGW sessions and co-located SGW sessions. Co-located sessions have both SGW and PGW services located on the same MCC. ■ imsi-range – SGW CDRs are generated based on a list of configured IMSI ranges. ***Note:*** *Applies to Gz/Rf SGW CDRs only.*
CDR Start Trigger	Controls when to trigger the SGW Gz/Rf Start CDR in the current SGW Mode: ■ create-session-request – CDR triggered with the Create-Session-Request message ■ modify-bearer-request – CDR triggered with Modify-Bearer-Request message ***Note:*** *Applies to Gz/Rf SGW CDRs only.*
Offline Charging IMSI List	IMSI range list to use to generate SGW CDRs. The IMSI range list must already exist. See IMSI Range List. ***Note:*** *Applies only when CDR Mode is set to imsi-range.*
Unique CDR Node ID	Specifies to use a unique node ID per SGW/PDNGW process: ■ Enabled ■ Disabled

Table 10-158 Offline Charging Parameters

Parameter	Description
Apn Reporting	APN to use when reporting APN to external devices: ■ original — Initial APN ■ mapped — Final / current APN ■ prior-mapped — APN mapped prior to the mapped (final / current) APN. This setting allows APN Reporting to continue to be based on the previously-mapped APN (even following a remap to a final APN) ■ custom — Customized Access Point Name (APN) reported on external interfaces. The customized APN is used in the Called-Station-ID AVP in messages in the external interfaces ***Note:*** *The APN Reporting value configured at the interface level overrides the APN Reporting value configured for the Control Profile. If the APN Reporting value is not configured at the interface level, the Called-Station-ID AVP and User-Name AVP will be filled based on the APN Reporting value configured for the Control Profile.* ***Note:*** *Offline charging APN Reporting at the interface-level is only supported for PGW.*
Protocol Type	Service Node: ■ Diameter ■ GTPP ■ Local
Report Epcqos in Kbps	Specifies whether the EPC QoS Information fields in CDRs should report values in Kilobits-per-second (Kbps). ■ enabled – The EPC QoS information fields in CDRs are filled as follows: – Sets the current (non-extended) bit rates in Kbps. – Sets the extended bit rates in Kbps if the current bit rates are greater than 2^32-1. ■ disabled – The EPC QoS information fields in CDRs are filled as follows: – Sets the current (non-extended) bit rates in bps. For bandwidth values greater than 2^32-1, sets the value to 2^32-1. – Sets the extended bit rates in Kbps if the current bit rates are greater than 2^32-1. ***Note:*** *Applies to Protocol Local and GTPP only.*
Server Group	Service Profile for the selected streaming protocol ***Note:*** *Applies to Protocol Type GTPP and Diameter only.*

Table 10-158 Offline Charging Parameters

Parameter	Description
CDR File Type	File type for streaming CDR record locally: ■ core files ■ data record ■ event log ■ other ***Note:*** *Applies to Protocol Local only.*
CDR File Name	Filename for streaming CDR record locally ***Note:*** *Applies to Protocol Local only.*
Error CDR File Name	File name for streaming ASN.1 CDRs locally when the CDR is categorized as an error CDR.
Invalid CDR File Name	File name for streaming ASN.1 CDRs locally when the CDR is categorized as an invalid CDR.
Encode Format	Specifies the format in which encoded CDRs are saved to the local diskformat: ■ csv ■ asn1 ■ both ***Note:*** *Applies to Protocol Local only.*
Custom Format	Specifies the format for GGSN local CDRs: ■ 3gpp ■ custom ***Note:*** *Applies to Protocol Local only.*
Start Template	Specifies the Start data record template name for CDRs in CSV format.
Interim Template	Specifies the Interim data record template name for CDRs in CSV format.
Stop Template	Specifies the Stop data record template name for CDRs in CSV format.
Event Template	Specifies the Event data record template name for CDRs in CSV format. ***Note:*** *Applies to Protocol Diameter and Local only.*
Interim Template ASN1	Specifies the interim (partial) data record template name for ASN.1 encoded CDRs. ***Note:*** *Applies to Encode Format asn1 or both.*
Stop Template ASN1	Specifies the stop (final) data record template name for ASN.1 encoded CDRs. ***Note:*** *Applies to Encode Format asn1 or both.*

Table 10-158 Offline Charging Parameters

Parameter	Description
ASN1 CDR Version	Specifies the 3GPP 32.298 version used to format ASN.1 local CDR fields in Interim and Stop data records: ■ **6.0** – Fields generated in local Interim and Stop data records are partially compliant to the ASN.1 syntax specified in 3GPP 32.298 version 6.0. The GPRSCallEventRecord value is set to 28 and the CallEventRecordType is set to 70, as per 3GPP 32.298 version 6.0. ■ **8.4** – Fields generated in local Interim and Stop data records are compliant to the ASN.1 syntax specified in 3GPP 32.298 version 8.4. ■ **9.0** – Fields generated in local Interim and Stop data records are compliant to the ASN.1 syntax specified in 3GPP 32.298 version 9.0. If using a 3GPP 32.298 version beyond 9.0 to format local CDR fields, select 9.0 and then configure the Interim and Stop data record templates to conform to the ASN.1 definitions specified in the desired 3GPP TS 32.298 release. Note the following: ■ The 3GPP 32.298 version configured for local CDR fields and the version configured for GTPP CDR fields do not need to match. ■ If a version is not configured for ASN.1 local CDR fields, local Interim and Stop data records will be compliant to the 3GPP 32.298 version configured for GTPP CDR fields. ■ If a version is not configured for either ASN.1 local CDR fields or ASN.1 GTPP CDR fields, local and GTPP Interim and Stop data records will be compliant to 3GPP 32.298 version 9.0. ***Note:*** *Applies to Protocol Local only.* ***Note:*** *Applies to Encode Format asn1 or both.*
Retransmit Count	Maximum number of times the gateway transmits the ACR to the offline charging server (OFCS). ***Note:*** *Applies to Protocol Type Diameter only.*
Retransmit Timeout	Time interval before retransmit, in milliseconds, before the system retransmits the ACR to the OFCS. ***Note:*** *Applies to Protocol Type Diameter only.*

Table 10-158 Offline Charging Parameters

Parameter	Description
Write Cdr To Disk On Failure	Specifies whether to enable or disable the Gz/Rf SGW CDR file storage functionality used to store CDRs when the remote server is unavailable. ■ enabled – When the remote server is unavailable, Gz/Rf SGW CDRs are stored in a predefined file and format based on the configuration. Once servers become available, an OFCS pulls the stored SGW CDRs using SFTP from the predefined file path. ■ disabled – When the remote server is unavailable, the system stores Gz/Rf SGW CDRs and sends (pushes) the pending CDRs to the billing server when the remote server becomes available. The predefined file and format does not apply in this case. ***Note:*** *Applies to Gz/Rf SGW CDRs generated on a standalone SGW only.*
Gz Cdr Encode Format	Specifies the format in which to encode the Gz/Rf SGW CDRs in the file. ■ custom1 – Gz/Rf SGW CDRs are stored according to the custom1 format. ***Note:*** *Applies only when the* ***Write Cdr To Disk On Failure*** *parameter is set to* ***enabled****.*
Gz Cdr File Profile	Specifies the filename used to store Gz/Rf SGW CDRs records in the event of a failure. ***Note:*** *Applies only when the* ***Write Cdr To Disk On Failure*** *parameter is set to* ***enabled****.*
Suppress No Interim Zero Traffic Asn1 Stop CDR	Suppress zero-volume Stop CDRs for short-lived sessions for which there is no Interim CDR generated. ■ enabled – The MCC suppresses Stop CDRs for short-lived sessions with zero-volume service data containers (SDCs) for which there is no Interim CDR generated. ■ disabled – (default) The MCC generates Stop CDRs for short-lived sessions even if there is no traffic data to report (zero-volume SDCs). ***Note:*** *Applies to SGW/PGW local ASN.1 and GTPP CDRs.*

Table 10-158 Offline Charging Parameters

Parameter	Description
Report Time Usage on Zero Traffic	Specifies whether the Time First Usage, Time Last Usage, and Time Usage CDR subfields should be set in Service Data Containers even if there is no data to be reported: ■ enabled – If there is no traffic data to report, the Time First Usage and the Time Last Usage subfields are set to the Time of Container Report and the Time Usage subfield is set to 0 in Stop and Interim PGW local ASN.1 and GTPP CDRs. ■ disabled – (default) If there is no traffic data to report, the Time First Usage, Time Last Usage, and Time Usage subfields are not included in Stop and Interim PGW local ASN.1 and GTPP CDRs. ***Note:*** *Applies to ASN.1 local and GTPP PGW CDRs only.* ***Note:*** *These CDR subfields are contained within the List of Traffic Data Volumes field, which is known as Change of Charging Condition in ASN.1 format.*
PDP PDN Type Prefix	Specifies the prefix used to fill in the spare bits of the PDP/PDN Type field in local ASN.1 and GTPP CDRs. Previously, the prefix for the PDP/PDN Type field was hard-coded to 0xF, as specified by 3GPP. This feature adds the ability to configure the PDP/PDN Type prefix. ***Note:*** *Applies to local ASN.1 and GTPP CDRs only.*
Populate PDN Type In PDP Type	Specifies whether to customize the values of the PDP/PDN Type field in local ASN.1 and GTPP CDRs. Previously, the PDP/PDN Type field was populated only with 3G PDP types, irrespective of whether the session was 3G or 4G. Operators can now specify whether to populate the PDP/PDN Type field with PDN type values for 4G sessions: ■ enabled ■ disabled When enabled, the following PDN type values are defined: ■ IPv4 – 0x01 ■ IPv6 – 0x02 ■ IPv4/IPv6 – 0x03 ***Note:*** *Applies to local ASN.1 and GTPP CDRs only*
Record Sequence Number Include Only if Interim Was Sent	Specifies whether to include the record sequence number in local ASN.1 and GTPP Stop CDRs. If enabled, the record sequence number will only be included in local ASN.1 and GTPP Stop CDRs if at least one Interim CDR was sent prior to the Stop CDR: ■ enabled ■ disabled ***Note:*** *Applies to local ASN.1 and GTPP CDRs only.*

Table 10-158 Offline Charging Parameters

Parameter	Description
Record Sequence Number Start Record Sequence Number from Zero	Specifies whether to set the record sequence number of the first record to zero in local ASN.1 and GTPP CDRs: ■ enabled – The record sequence number in local ASN.1/GTPP CDRs (whichever is generated first) starts with 0. ■ disabled – The record sequence number in local ASN.1/GTPP CDRs (whichever is generated first) starts with 1. ***Note:*** *Applies to local ASN.1 and GTPP CDRs only*.
APN Ni Format Per 3GPP	Specifies the ASN.1 encoding format for the Access Point Name Network Identifier (APN NI) ASN.1 CDR field. ■ enabled – The APN NI ASN.1 CDR field is encoded as defined in 3GPP 23.003. The APN NI may contain multiple labels and each label is coded as a one octet length field followed by that number of octets coded as 8-bit ASCII characters. ■ disabled – The APN NI ASN.1 CDR field is encoded with all the labels in ASCII characters and each label is separated by a dot (.). ***Note:*** *Applies to local ASN.1 and GTPP CDRs only*.
Served Imeisv Allow Zero Value	Specifies whether MCC sends the IMEISV with a value of 0 within Served IMEISV CDR on the Ga (GTPP), and local (ASN.1) interfaces. ■ enabled ■ disabled ***Note:*** *Applies to local ASN.1 and GTPP CDRs only*.
User Equipment Info Imeisv Allow Zero Value	Specifies whether MCC sends the IMEISV with a value of 0 within User-Equipment-Info AVP on the Gz/Rf interface: ■ enabled ■ disabled ***Note:*** *Applies to SGW and PGW and Protocol Type Diameter only*
3gpp Imeisv Allow Zero Value	Specifies whether MCC sends the IMEISV with a value of 0 within 3GPP-IMEISV AVP on the Gz/Rf interface: ■ enabled ■ disabled ***Note:*** *Applies to SGW and PGW and Protocol Type Diameter only*

5 Click the **Save** icon.

Interface: Online Charging

Use this object to configure an Online Charging Interface Profile.

To add an Online Charging Interface Profile:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **Online Charging**.
4. Configure the parameters as follows:

Table 10-159 Online Charging Parameters

Parameter	Description
Name	Online Charging interface profile name
Admin State	Admin state of Online Charging interface: ■ Enabled ■ Disabled
Interface Compliance	Interface compliance: ■ 3gpp ■ rfc4006 ■ vodafone ■ vodafoneCustom ■ vodafone21Version ■ 3gppVersion2 ■ 3gppCustom1
Service Context ID	Service Context ID content (Maximum length 64 characters)
Credit Control Session Failover Support	Support for Credit Control Session Failover: ■ Enabled ■ Disabled
Credit Control Failure Support	Credit Control Failure Support handling: ■ TERMINATE – The subscriber session is terminated whenever a Diameter transaction to the OCS server fails. ■ RETRY AND TERMINATE – The failed Diameter transaction is retried multiple times and terminates the session if no retry succeeds. ■ CONTINUE – The session continues even if the Diameter transaction fails. Note that the subscriber session is allowed to pass traffic without OCS server intervention, which could cause loss to the Operator revenue.
Retransmit Count	Maximum number of retransmit attempts to the server.
Retransmit Timeout	Time interval before retransmit, in milliseconds.

Table 10-159 Online Charging Parameters

Parameter	Description
Suppress Invalid ULI	Specifies whether to enable or disable the check for the invalid User Location Information (ULI) of 01 ff ff ff ff ff ff ff provided by the MME/SGSN and to suppress it over the Gx/Gy interfaces. ULI changes from valid to invalid and vice versa are considered valid ULI changes and are reported for offline/PCRF/OCS event-triggers. ■ true ■ false
Gy Action per Result Code	Specifies whether to enable or disable the command-level or MSCC-level result code policy lists. ■ enabled – The result code returned in the CCA message is compared to the configured result code list, and if there is a match, the PGW/GGSN applies the configured action. ■ disabled – The result code list functionality is not used. At the command level, if the OCS responds with a temporary failure (result code 3xxx), the message is retransmitted and the default quota may be applied and the Gy rejoin timer started based on the configuration. For all other CCA error messages (result code other than 2001), the system terminates the session. At the MSCC level, if the OCS returns a CCA error message (result code other than 2001), the gateway executes the action indicated in the FUA AVP if set to REDIRECT or RESTRICT-ACCESS. If the FUA is set to TERMINATE or the CCA does not contain the FUA AVP, then all traffic for the rating group is blocked.
Command Level Result Code List	Specifies the name of command-level result code list. The Command Level Result Code List must already exist. See Diameter Result Code Policy List. ***Note:*** *The Command Level Result Code List overrides the Mscc Level Result Code List.*
Mscc Level Result Code List	Specifies the name of MSCC-level result code list. The Mscc Level Result Code List must already exist. See Diameter Result Code Policy List. ***Note:*** *The Mscc Level Result Code List is only considered when the command-level result code is 2001.*

Table 10-159 Online Charging Parameters

Parameter	Description
Multi CRBN Allowed in CCR	Specifies whether to include multiple Charging-Rule-Base-Name AVPs (within PS-Information AVP) in CCR-I/CCR-U messages towards the OCS: ■ true - The PGW/GGSN includes multiple Charging-Rule-Base-Name AVPs (within the PS-Information AVP) in CCR-I/CCR-U messages towards the OCS. The value of the Charging-Rule-Base-Name AVPs correspond to both the locally configured charging instance from the Workfow Data Profile (Workflow > Data Profile > Charging) and all locally configured charginginstances from the PCRF-installed CRBN profiles (Services > CRBN Profile > Charging Instance). ***Note:*** *The MCC gateway will only include multiple Charging-Rule-Base-Name AVPs (within the PS-Information AVP) on the Gy interface if the charging-instances in the data-profile and crbn-profiles are different from each other.* ■ false - The PGW/GGSN includes a single Charging-Rule-Base-Name AVP (within the PS-Information AVP) in CCR-I/CCR-U messages towards the OCS. The value of the Charging-Rule-Base-Name AVP corresponds to the locally configured charging-instance from the data-profile on the MCC gateway (Workflow > Data Profile > Charging). ***Note:*** *This parameter is supported only when the Online Charging > Interface Compliance is set to 3gpp or 3GPPVersion2 and the Pcrf Charging > Crbn Mode is set to crbn-profile.*
OCS Down Default Gy Call Setup	Specifies whether to enable or disable the Default Gy feature. ■ enabled – When no OCS is available (not online or no response) or if the OCS returns a temporary failure (result code 3xxx), the GGSN/PGW sets up an online charging session and applies the default quota to the session. ■ disabled (default) – The GGSN/PGW does not set up an online charging session and does not apply the default quota to a session when no OCS is available (not online or no response) or if the OCS returns a temporary failure (result code 3xxx).
OCS Down Default Gy Quota	Specifies the maximum number of credits, in bytes, that the PGW allocates to a new or existing online charging session in the event of an OCS failure. The default of 10485760 is equivalent to 10 MB.

Table 10-159 Online Charging Parameters

Parameter	Description
OCS Down Gy Rejoin	Specifies whether to enable or disable Gy Rejoin: ■ enabled – If the default quota, used for an online charging session, is consumed or if the **OCS Down Gy Rejoin Time** expires, the PGW tries to rejoin the OCS. ■ disabled (default) – The PGW does not try to rejoin the OCS even if the OCS comes back up in the case where the default quota is applied to a session. If the OCS is down when a CCR-Update is attempted, the session is terminated.
OCS Down Gy Rejoin Time	Specifies the number of seconds to wait before attempting to connect to the non-responsive OCS.
OCS Down Gy Replay	Specifies whether to enable or disable Gy Replay: ■ enabled – If all OCS servers go down after the Gy session is already established and the session using the default quota is terminated before the OCS comes back up, the GGSN/PGW caches the USU based on the OCS GSU and replays the cached session information with the OCS becomes available. ■ disabled (default) – The session usage consumed based on the OCS grant is not cached and replayed to the OCS.
Send Final In Update	Controls whether the MCC GGSN/PGW sends a CCR-Update message to the OCS with a Reporting-Reason AVP (at the MSCC level) value of FINAL in response to a CCA message with result code DIAMTER_CREDIT_LIMIT-REACHED (4012): ■ true ■ false ***Note:*** *Applies to 3GPP variants only.*
Send RSU in Update	Set to true to configure the MCC GGSN/PGW to always include and populate the Requested-Service-Unit (RSU) AVP (at the MSCC level) in the CCR-Update message: ■ true ■ false ***Note:*** *Applies to 3GPP variants only.*
CCA Error Send Terminate	Controls whether the MCC GGSN/PGW sends the OCS a CCR-Terminate message upon receipt of a CCA-Update message with a permanent failure (Result Code 5xxx): ■ true ■ false ***Note:*** *Applies to 3GPP variants only.*

Table 10-159 Online Charging Parameters

Parameter	Description
Gy Async	Controls whether to enable Gy Async: ■ enabled – The PGW completes the PDN session setup by sending the Create Session Response and sets up the online charging session with the OCS asynchronously (not as part of the PDN session setup). ■ disabled (default) – The PGW completes the PDN session setup after establishing the online charging session with the OCS. ***Note:*** *Is configurable only when* ***Interface Compliance*** *is set to* ***3GPPVersion2****. By default,* ***Gy Async*** *is disabled for all other interfaces.*
Rating Group Initial Quota	Specifies the maximum number of credits, in bytes, that the PGW can allow per Rating Group before establishing the Gy session and receiving the granted quota from the OCS. If the initial quota is consumed before the PGW receives the granted quota from the OCS, traffic for this session is blocked. Default 0 (disabled) indicates that traffic is blocked until the granted quota is received from the OCS.
Charge Rating Group Initial Quota	Controls whether to charge for the traffic passed using the initial quota grant per Rating Group. ■ true ■ false (Default) ***Note:*** *All traffic, including the initial quota traffic, is included in offline CDRs regardless of whether charging is enabled for the initial quota.*
Override Destination Realm	Realm name to override the peer realm in the Destination-Realm AVP sent in CCR-Initial messages on the Gy interface.
PCRF Charging Info Avp Usage	Specifies how the destination host/realm extracted from the Charging-Information AVP (received from the PCRF) is used during Gy session setup: ■ peerSelection - The extracted destination host is used for selecting the OCS peer ■ overrideDestHostRealm - The extracted host/realm is used for the Destination-Host AVP and the Destination-Realm AVP in the CCR-I message sent to the OCS.
PCRF Num Labels Destination Realm	Number of labels to extract from the Charging-Information AVP for the destination-realm. The Charging-Information AVP contains a single FQDN value (with one or more labels separated with dots) for each primary and secondary OCS but does not indicate which part of the FQDN belongs to the parent realm. Default: 0 (Disabled), indicates that the destination-realm is not extracted from the Charging-Information AVP. ***Note:*** *Applies only when PCRF Charging Info Avp Usage is set to overrideDestHostRealm.*

Table 10-159 Online Charging Parameters

Parameter	Description
Send Called Station Id At Command Level	Configures the Gy interface to include the Called-Station-Id AVP at the command level (instead of inside the Service- Info AVP) for 3GPP CCR messages: ■ true ■ false ***Note:*** *Applies only when* ***Interface Compliance*** *is set to 3GPP, 3GPPVersion2, 3GPPCustom1, or RFC4006.*
User Name Type	Gy User Name Type(format) to be used if not present in PCO: ■ apn ■ default-username ■ imsi ■ imsi-plus-apn ■ imsi-plus-apnnionly ■ msisdn ■ msisdn-plus-apn ■ msisdn-plus-apnnionly ■ imsi-nai-prefix-0 ■ imsi-nai-no-prefix ■ none This setting overrides the **user name type** present at the APN level. However, if this User Name Type parameter is set to **none**, the APN level **user name type** is used.
Subscriptionid Imsi Format Non 3gpp Access	IMSI format to be sent in Subscription Id for non-3gpp access: ■ imsiformat ■ msinaiprefix0format
Reauth Response Success Result Code	Specifies which Diameter Result Code the PGW sends in RAA messages to the OCS to indicate the RAR was successfully processed: ■ success_2001: The PGW sends the DIAMETER_SUCCESS (2001) result code ■ Limited_success_2002: The PGW sends the DIAMETER_LIMITED_SUCCESS (2002) result code
Offline CDR for Gy Event	Specifies whether to generate offline charging Service-Data-Container/CDR on Gy reporting events on the Gy online charging interface: ■ Enabled ■ Disabled

Table 10-159 Online Charging Parameters

Parameter	Description
OCS Down Max Num Default Quota	Maximum number of times a session can be assigned default Gy quota while OCS server is down. If the user exceeds the maximum number of default quota allocations, the session is terminated. Value **0** allows for an unlimited number of default quota allocations.
OCS Down Session Terminate Timer	Time (in seconds) to terminate a session when default quota is exhausted. Value zero disables this timer. ***Note:*** *Applies only when Gy Rejoin (Ocs Down Gy Rejoin) is disabled and the Default Gy Quota (Ocs Down Default Gy Call Setup) is enabled.*
Report All Usage On Rejoin	Specifies whether to report all interim usage (including all default quota allocations) in a CCR-Update message when the PGW rejoins the OCS in the event of an OCS failure. ■ Enabled ■ Disabled
Restart on Session Not Found	Specifies whether the MCC PGW initiates a new Gy session if the OCS returns a 5002 result code when the PGW attempts to rejoin the OCS. If enabled, the PGW sends the CCR-I to initiate a new Gy session followed by the CCR-U to report the usage. ■ Enabled ■ Disabled
Write Records to Disk File on Call Termination	Specifies whether to enable the Gy CCR-T file storage functionality used to store session usage information when the OCS is unavailable. ■ Enabled – When the OCS is unavailable, Gy CCR-T records are stored in a predefined file and format based on the configuration. The stored CCR-T records are available for retrieval using SFTP. ■ Disabled – When the remote server is unavailable, the system does not store Gy CCR-T records in a file.
Gy CDR Encode Format	Specifies the format to encode the Gy CCR-T records in the file: ■ custom1 – Gy CCR-T records are stored according to the custom1 format. ***Note:*** *Applies only when Write Records to Disk File on Call Termination is set to enabled.*
Gy CDR File Type	Specifies the type of record file. In this case, select Gy-Record. ***Note:*** *Applies only when Write Records to Disk File on Call Termination is set to enabled.*
Gy CDR File	Specifies the file name to store CCR-T records in case of failure. ***Note:*** *Applies only when Write Records to Disk File on Call Termination is set to enabled.*

Table 10-159 Online Charging Parameters

Parameter	Description
Gy Close Time for Online Disable on LTE Wifi Handover	Specifies a Gy close timer (in seconds) to the Gy online charging interface to support dynamic Gy session termination when the PCRF disables all online service rules during interface-access handovers (LTE <–>Wi-Fi handovers). This feature helps to avoid unnecessary Gy session termination/setup procedures with multiple charging rule updates from the PCRF during inter-access handovers. When the PCRF disables all online service rules during inter-access handovers, the PGW sends a CCR-U to the OCS to report the final usage for online rating groups and starts the Gy close timer. If the Gy close timer expires before the PCRF installs new online service rules, the PGW terminates the Gy session. However, if the PCRF installs new online service rules before the Gy close timer expires, the PGW resumes the Gy session by sending a CCR-U to the OCS requesting a new grant for the required rating groups.
Terminate Gy if No Active Online Rule	Specifies whether a CCR-T or a CCR-U is sent when no active online rules exist: ■ true – MCC sends a CCR-T ■ false – MCC sends a CCR-U
Send Zero USU On No Grant	Specifies whether to report Used-Service-Units (USU) as zero for the rating group in CCR-U/CCR-T to the OCS when the PGW receives a CCA with no grant (no GSU AVP) in the MSCC: ■ true ■ false
Delete Session On FUI Terminate	Specifies whether to terminate the session when the FUI AVP is set to TERMINATE, irrespective of whether a grant is available for other online rating groups. By default, this parameter is set to false, indicating the session will not be terminated: ■ true – the session will be terminated ■ false – the session will not be terminated

Table 10-159 Online Charging Parameters

Parameter	Description
Defer Gy Session Until First Sdf Packet	Option to defer Gy session until the first service data flow packet (If not configured, default is not to defer Gy setup): ■ home-subscriber – For home subscribers, the PGW/GGSN establishes the online-charging session and requests quota with the OCS (MSCC AVP in the CCR-I) upon receiving the first service data flow packet. ■ roaming-subscriber – For roaming subscribers, the PGW/GGSN establishes the online-charging session requests quota with the OCS (MSCC AVP in the CCR-I) upon receiving the first service data flow packet. ■ both – For both home and roaming subscriber sessions, the PGW/GGSN establishes the online-charging session and requests quota with the OCS (MSCC AVP in the CCR-I) upon receiving the first service data flow packet. Note the following restrictions when using this feature: ■ This parameter applies only when all online rating groups have the **Credit Authorization Event** parameter set to firstSdfPkt. ■ Modifications to this parameter only apply to new sessions created after the configuration change. ■ For the set of subscribers for which the online charging session setup is not deferred and is setup along with the PDN sessions, Gy Async is applicable.
Apn Reporting	APN to use when reporting APN to external devices: ■ original — Initial APN ■ mapped — Final / current APN ■ prior-mapped — APN mapped prior to the mapped (final / current) APN. This setting allows APN Reporting to continue to be based on the previously-mapped APN (even following a remap to a final APN) ■ custom — Customized Access Point Name (APN) reported on external interfaces. The customized APN is used in the Called-Station-ID AVP in messages in the external interfaces ***Note:*** *The APN Reporting value configured at the interface level overrides the APN Reporting value configured for the Control Profile. If the APN Reporting value is not configured at the interface level, the Called-Station-ID AVP and User-Name AVP will be filled based on the APN Reporting value configured for the Control Profile.*
Service Node	Service Node: ■ GGSN - Gateway GPRS Support Node ■ PGW - Packet Data Network Gateway
Interface Trigger Template	***Note:*** *Deprecated: use Event Trigger Template instead.*

Table 10-159 Online Charging Parameters

Parameter	Description
Event Trigger Template	Event Trigger Template to use. The Event Trigger Template must already exist. See Event Trigger Template.
Proto Type	Proto Type: ■ Diameter
Server Group	Service Profile for the selected streaming protocol
Start Template	Start Record Template
Interim Template	Interim Record Template
Stop Template	Stop Record Template
Event Template	Event Record Template
CCA Initial	Template to apply to Credit-Control-Answer initial message
CCA Update	Template to apply to Credit-Control-Answer update message
CCA Final	Template to apply to Credit-Control-Answer final message
CCA Event	Template to apply to Credit-Control-Answer event message
AVP Customization User Equipment Info Imeisv Format Tbcd	The IMEISV sent within the User-Equipment-Info AVP in the CCR message on the Gy interface is encoded in Octet String format, by default. This parameter specifies whether to encode the IMEISV in Telephony Binary Coded Decimal (TBCD) format. Changes to this parameter take effect immediately. ■ enabled – The IMEISV sent within the User-Equipment-Info AVP in the CCR message on the Gy interface is encoded in TBCD format. ■ disabled – The IMEISV sent within the User-Equipment-Info AVP in the CCR message on the Gy interface is encoded in Octet String format.
AVP Customization User Equipment Info Imeisv Allow Zero Value	Specifies whether MCC sends the IMEISV with a value of 0 within User-Equipment-Info AVP on the Gy interface: ■ enabled ■ disabled
AVP Customization 3gpp Imeisv Allow Zero Value	Specifies whether MCC sends the IMEISV with a value of 0 within 3GPP-IMEISV AVP on the Gy interface: ■ enabled ■ disabled

5 Click the **Save** icon.

Interface: PCRF Charging

Use this object to configure a PCRF Charging Interface Profile.

To add an PCRF Charging Interface Profile:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **PCRF Charging**.
4. Configure the parameters as follows:

Table 10-160 PCRF Charging Parameters

Parameter	Description
Name	PCRF Charging interface name
Admin State	Admin state of PCRF Charging interface: ■ Enabled ■ Disabled
Retransmit Count	Maximum number of CCR retransmit attempts to the PCRF.
Retransmit Timeout	Time interval, in milliseconds, before the system retransmits the CCR to the PCRF.
Cer Auth Application ID	Specifies the Auth-Application-ID to be used in Capabilities-Exchange-Request (CER) messages within the Vendor-Specific-Application-Id AVP. The 3GPP Gx Auth-Application-Id (16777238) is mandatory in CER messages. This parameter is used to add an additional Auth-Application-Id to be used within the Vendor-Specific-Application-Id AVP in CER messages.
Default Gx Setup per Cause Code	Specifies whether to enable or disable session set up using the default Gx policy based on the result code received in the CCA error response. ■ enabled – The result code returned in the CCA error message is compared to the configured result code list, and if there is a match, the session is set up using the default Gx policy. ■ disabled – (default) The result code list functionality is not used to set up the session with the default Gx policy. However, if the result code returned in the CCA error message is a 3xxx error, the default Gx policy is used to set up the session.
Default Gx Cause Code List	Cause Code List for PCRF call setup. The Cause Code List must already exist. See Diameter Result Code Policy List.

Table 10-160 PCRF Charging Parameters

Parameter	Description
PCRF Down Default Gx Call Setup	The Default Gx Policy feature helps to avoid a disruption in service to subscribers by allowing the MCC GGSN/PGW to set up a session when no PCRF is available. When this parameter is enabled and no PCRF is available, new sessions are automatically processed in Default Gx Policy mode, where the GGSN/PGW uses the information in the locally configured workflow data profile to set up the subscriber session. PCRF down default Gx call setup admin state: ■ Enabled ■ Disabled
PCRF Down Gx Rejoin	Gx Rejoin/Replay helps to ensure session continuity in the event of a PCRF failure during an active session when no secondary PCRF is available. When this parameter is enabled and the GGSN/PGW detects a PCRF failure during an active session, the GGSN/PGW caches subscriber usage information locally and replays the cached session information via CCR-Update messages to the same PCRF that set up the session (once it becomes available). PCRF down Gx Rejoin admin state: ■ Enabled ■ Disabled
PCRF Down Tethering Entitlement	Specifies whether tethering should be applied to a session if the PCRF is down during session setup: ■ Enabled – If the PCRF is down during session setup, the MCC enables tethering for the session. ■ Disabled – If the PCRF is down during session setup, the MCC does not enable tethering for the session and uses the configured qos-flow. **Notes:** Once tethering is applied to the session and if the PCRF fails during the session, the previously applied tethering entitlement remains valid. If tethering entitlement is disabled during the session, MCC disables tethering entitlement for all active connections of the session and marks the connections as non-tethered-entitlement connections. Also the following counters *are not* incremented: ■ tethering-entitled-uplink-packets/downlink-packets ■ tethering-entitled-uplink-bytes/downlink-bytes For example, if a session initially has 5 active connection and tethering entitlement is enabled, MCC increments both counters for each and every packet. When tethering entitlement is disabled for the session, MCC disables tethering entitlement for all the 5 active connections and stops incrementing the respective counters.

Table 10-160 PCRF Charging Parameters

Parameter	Description
PCRF Down Rejoin Time	Number of seconds to wait before attempting to connect to the non-responsive PCRF.
PCRF Down Gx Replay	Gx Replay is used if all PCRF servers go down after the Gx session is already established and the session using the default policy is terminated before the PCRF comes back up. In this case, if Gx Replay is enabled, the GGSN/PGW replays the cached session information via a CCR-Terminate message. PCRF down Gx Replay admin state: ■ Enabled ■ Disabled
PCRF CCA Error Send Terminate	Controls whether the MCC GGSN/PGW sends the PCRF a CCR-Terminate message upon receipt of a CCA-Update message with a permanent failure (Result Code 5xxx): ■ true ■ false
PCRF Send Usage Update Always	Controls whether the PCEF sends usage monitoring information without a PCRF trigger: ■ true ■ false
PCRF 3GPP Release Compliance	PCRF 3GPP Release Compliance: ■ Release-10 - The PCRF is compliant with 3GPP TS 29.212 Release 10 or earlier. The PCEF receives and reports the USAGE_REPORT event-trigger with code 26. ■ Release-10-plus - The PCRF is compliant with 3GPP TS 29.212 Release 11 or later. The PCEF receives and reports the USAGE_REPORT event-trigger with code 33.
PCRF Send CRR in RAA	Controls whether the PGW includes the Charging-Rule-Report AVP in the Re-Auth-Answer (RAA) message upon receiving a Re-Auth-Request (RAR) message from the PCRF containing the Charging-Rule-Install AVP or Charging-Rule-Remove AVP: ■ true (default) – The PGW sends the Charging-Rule-Report AVP in the corresponding RAA message after processing the charging rules. ■ false – The PGW immediately sends the RAA message without the Charging-Rule-Report AVP. The PGW sends the Charging-Rule-Report AVP in a separate CCR-Update message after processing the charging rules.

Table 10-160 PCRF Charging Parameters

Parameter	Description
PCRF Override PLMNID	Specifies whether to override the PLMNID from PCRF if received in CCA-I/U/RAR: ■ enabled – The PLMN-ID received from the PCRF overrides the PLMN-ID received in GTP-C messages and is used in subsequent messages to the OCS and in local PGW CDRs (CSV and ASN.1 formats) and GTPP PGW CDRs (Ga interface). ■ disabled – The GGSN/PGW ignores the PLMN-ID received from PCRF and uses the PLMN-ID sent in GTP-C messages.
Subscriptionid Imsi Format Non 3gpp Access	IMSI format to be sent in Subscription Id for non-3gpp access: ■ imsiformat| ■ msinaiprefix0format
Diameter Pending Transaction	Specifies whether to enable parallel processing handling in Gx interface: ■ Enabled ■ Disabled When enabled, the MCC GGSN/PGW processes Diameter messages in parallel on the Gx interface to avoid possible race conditions in which the PCEF (GGSN/PGW) receives a PCRF-initiated message (for example, RAR) while a PCEF-initiated message (for example, CCR-U) is still pending a response (CCA-U) from the PCRF.

Table 10-160 PCRF Charging Parameters

Parameter	Description
CRBN Mode	Specifies how to interpret the Charging-Rule-Base-Name AVP received on the Gx interface: ■ data-profile – The value of the Charging-Rule-Base-Name AVP corresponds to the locally configured Workflow Data Profile on the MCC gateway. In this case, the MCC allows only one predefined group of PCC rules to be activated/deactivated on an MCC gateway using the Charging-Rule-Base-Name AVP within the Charging-Rule-Install AVP. If the MCC gateway receives more than one Charging-Rule-Base-Name AVP within the Charging-Rule-Install AVP, the system installs the first one, discards the remaining ones and logs the error. ■ crbn-profile – The value of the Charging-Rule-Base-Name AVP corresponds to the locally configured CRBN Profile on the MCC Gateway. In this case, the MCC supports the receipt of a Charging-Rule-Install AVP containing multiple Charging-Rule-Base-Name AVPs and allows for multiple predefined groups of PCC rules to be activated/deactivated on an MCC gateway. Note the following guidelines when activating/deactivating a CRBN profile: – All Rating Groups and Service Rules associated with a CRBN Profile should have the **Service Activation** set to **always on**. – The QoS Flow associated with CRBN Profile should have the bearer-control parameter configured as default-bearer. – There should be only one Billing Plan under the Charging Instance associated with the CRBN Profile, and it must have wildcard charging characteristics. – If the same Service Rule is part of multiple CRBN Profiles, the Service Rule is deactivated only after all the CRBN Profiles referring to it are deactivated. – A static Service Rule that is activated as part of a CRBN Profile will not be deactivated when the CRBN Profile referring to it is deactivated.
Send Qos Info in All CCR	Specifies whether to include the QoS-Information AVP in all CCR messages (Initial/Update/Terminate) towards the PCRF: ■ enabled – The MCC gateway includes the QoS-Information AVP in all CCR messages (Initial/Update/Terminate) towards the PCRF. ■ disabled – (default) The MCC gateway includes the QoS-Information AVP in the CCR-Initial message towards the PCRF. ***Note:*** *To use this feature, the QoS-Information AVP* `presentFlag` *setting must be set to* `yes` *or* `conditional` *in the Gx CCR data record templates (start/interim/stop).*

Table 10-160 PCRF Charging Parameters

Parameter	Description
Suppress Invalid ULI	Specifies whether to enable or disable the check for the invalid User Location Information (ULI) of 01 ff ff ff ff ff ff ff provided by the MME/SGSN and to suppress it over the Gx/Gy interfaces. ULI changes from valid to invalid and vice versa are considered valid ULI changes and are reported for offline/PCRF/OCS event-triggers. ■ true ■ false
Default Bearer QoS Change Indication	Specifies whether to enable event trigger of QCI/ARP change for default bearer if PCRF is not subscribed: ■ enabled – When the corresponding event occurs, such as a change in QCI or ARP, the PGW reports the event in a CCR-U to the PCRF, even if the event-trigger has not been provisioned by the PCRF in the CCA-I. ■ disabled – When the corresponding event occurs, such as a change in QCI or ARP, the PGW only reports the event in a CCR-U to the PCRF if the event-trigger has been provisioned by the PCRF in the CCA-I.
QoS Change Indication	Specifies whether to enable event trigger of APN/AMBR change for bearer if PCRF is not subscribed: ■ enabled – When the corresponding event occurs, such as a change in APN-AMBR, the PGW reports the event in a CCR-U to the PCRF, even if the event-trigger has not been provisioned by the PCRF in the CCA-I. ■ disabled – When the corresponding event occurs, such as a change in APN-AMBR, the PGW only reports the event in a CCR-U to the PCRF if the event-trigger has been provisioned by the PCRF in the CCA-I.
Apn Reporting	APN to use when reporting APN to external devices: ■ original — Initial APN ■ mapped — Final / current APN ■ prior-mapped — APN mapped prior to the mapped (final / current) APN. This setting allows APN Reporting to continue to be based on the previously-mapped APN (even following a remap to a final APN) ■ custom — Customized Access Point Name (APN) reported on external interfaces. The customized APN is used in the Called-Station-ID AVP in messages in the external interfaces ***Note:*** *The APN Reporting value configured at the interface level overrides the APN Reporting value configured for the Control Profile. If the APN Reporting value is not configured at the interface level, the Called-Station-ID AVP and User-Name AVP will be filled based on the APN Reporting value configured for the Control Profile.*

Table 10-160 PCRF Charging Parameters

Parameter	Description
User Name Type	Gx User Name Type(format) to be used if not present in PCO: ■ apn ■ default-username ■ imsi ■ imsi-plus-apn ■ imsi-plus-apnnionly ■ msisdn ■ msisdn-plus-apn ■ msisdn-plus-apnnionly ■ imsi-nai-prefix-0 ■ imsi-nai-no-prefix ■ none
Service Node	Service Node: ■ GGSN - Gateway GPRS Support Node ■ PGW - Packet Data Network Gateway
Proto Type	Proto Type: ■ Diameter
Server Group	Service Profile for the selected streaming protocol
Start Template	Start Record Template
Interim Template	Interim Record Template
Stop Template	Stop Record Template
CCA Initial	Template to apply to Credit-Control-Answer initial message
CCA Update	Template to apply to Credit-Control-Answer update message
CCA Final	Template to apply to Credit-Control-Answer final message
RAA Template	RAA Record Template
AVP Customization User Equipment Info Imeisv Allow Zero Value	Specifies whether MCC sends the IMEISV with a value of 0 within User-Equipment-Info AVP on the Gx interface: ■ enabled ■ disabled

5 Click the **Save** icon.

Interface: Policy Server Interface

Use this object to configure a policy server interface.

To add a Policy Server Interface:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **Policy Server Interface**.
4. Configure the parameters as follows:

Table 10-161 Policy Server Interface Parameters

Parameter	Description
Name	Server IP Address
Admin State	Admin state: ■ enabled ■ disable

5. Click the **Save** icon.

Interface: Port NBR Service

Use this object to configure a port NAT binding record (NBR) interface service profile. NAT Binding Records track the association between the source address/port of a connection/flow initiated by a subscriber in one address space and its translated source address/port in another address space.

To add a Port NBR Service:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **Port NBR Service**.
4. Configure the parameters as follows:
   - **Name**: Port NBR interface profile name
5. Click the **Save** icon.
6. Expand the port NBR service you added.
7. Expand **Service Node**.
8. Click **Local**.
9. Configure the parameters as follows:

Table 10-162 Port NBR Local Parameters

Parameter	Description
NBR File Type	NBR file type: ■ event log ■ data record ■ core files ■ RAM Data Profile ■ other
NBR File Name	NBR filename
Encode Format	Format to be used for encoding NAT binding records: ■ csv
Port NBR Template	Port NBR template The Port NBR template must already exist. Create it at Service Construct > Data Record Template > Port NBR > Local > NBR.

10. Click the **Save** icon.

Interface: Rx Interface

Use this object to specify the Rx interface.

To specify the Rx interface:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **Rx Interface**.
4. Configure the parameters as follows:

Table 10-163 Rx Interface Parameters

Parameter	Description
Name	Rx interface name
Admin State	Admin state of Rx interface: ■ Enabled ■ Disabled
Server Group	Service Profile for the selected streaming protocol
AAR Template	AAR Template
AAA Template	AAA Record Template
RAR Template	RAR Template
RAA Template	RAA Record Template

5. Click the **Save** icon.

Interface: S6b Interface

Use this object to specify the S6b interface.

To specify the S6b interface:

1. Expand **Service Construct** in the tree.
2. Expand **Interface**.
3. Click **S6b Interface**.
4. Configure the parameters as follows:

Table 10-164 S6b Interface Parameters

Parameter	Description
Name	S6b interface name

Table 10-164 S6b Interface Parameters

Parameter	Description
Admin State	Admin state of S6b interface: ■ Enabled ■ Disabled
Retransmit Count	Maximum number of retransmit attempts to the server.
Retransmit Timeout	Time interval before retransmit, in milliseconds.
Auth Application ID	Auth Application ID to be used
Access Type	Applicable Access Type for S6b interface: ■ non-3gpp-only ■ both-non3gpp-and-3gpp|
PGW Triggered Reauthorization	Specifies whether to enable Gateway-initiated reauthorization procedure on the S6b interface: ■ Enabled ■ Disabled
Authorization Lifetime	Time interval before the PGW initiates the reauthorization procedure on the S6b interface, in minutes. The PGW starts the authorization-lifetime timer upon receiving the AA-Answer (AAA) message.
Authorization Grace Period	Time interval before the PGW initiates the final reauthorization attempt on the S6b interface, in minutes. This timer starts when the PGW sends the AAR message following the expiration of the authorization-lifetime timer and the AAA message returns an error or the PGW is unable to send the AAR

5 Click the **Save** icon.

6 To configure the PGW Diameter interface, expand the S6B interface you added.

7 Expand **Service Node**, **PGW**, and **Prototype**.

8 Click **Diameter**.

9 Configure the parameters as follows:

Table 10-165 Diameter Interface Parameters

Parameter	Description
Server Group	Service Profile for the selected streaming protocol
AAR Template	AAR template
AAA Template	AAA record template
RAR Template	RAR template

Table 10-165 Diameter Interface Parameters

Parameter	Description
RAA Template	RAA record template
Mip6 Agent Info Type	Controls sending PGW information in the MIP6-Agent-Info AVP: ■ mip-home-agent-address specifies to send the PGW IP address. ■ mip-home-agent-host specifies to send the PGW's fully-qualified domain name (FQDN). In this case, the following fields also appear: ■ mip-home-agent-destination-host - Specifies the home agent destination host name in the FQDN. ■ mip-home-agent-destination-realm - Specifies the home agent destination realm name in the FQDN. ***Note:*** *If the mip-home-agent-destination-host name and/or mip-home-agent-destination-realm name are modified during a session, the subsequent AA-Requests (AARs) will include the modified PGW FQDN.*
STR Template	STR record template
STA Template	STA record template
ASR Template	ASR record template
ASA Template	ASA record template

10 Click the **Save** icon.

IP List

Use this object to configure an IP Address List.

To add an IP Address List:

1. Expand **Service Construct** in the tree.
2. Click **IP List**.
3. Configure the parameters as follows:

Table 10-166 IP List Parameters

Parameter	Description
Name	IP Address list name
User Description	IP Address list Description

4. Click the **Save** icon.
5. Expand the IP Address List you added.
6. To configure the specific IP address, click **IP Address**.
7. Configure the parameters as follows:

Table 10-167 IP Address Parameters

Parameter	Description
Address	IP Address (v4) or prefix (v4/v6)
User Description	IP Address description

8. Click the **Save** icon.
9. To configure an IP address range, click **IP Range**.
10. Configure the parameters as follows:

Table 10-168 IP Range Parameters

Parameter	Description
Start Address	Start IP Address (v4) or prefix (v4/v6)
End Address	End IP Address (v4) or prefix (v4/v6)
User Description	IP Address range description

11. Click the **Save** icon.

LDAP

Use this object to configure the Lightweight Directory Access Protocol (LDAP) services.

- Feature Group – Enable and configure LDAP feature group attributes such as the action to take if a match appears in the blacklist, define a list of LDAP attributes, and define enforcement rules.
- Remote Server – A list of configured remove servers with the same or different priority.
- Profile – Enable and configure LDAP profile attributes such as the default action to take if LDAP failure occurs, feature groups for this profile, network context for the LDAP server, priority, and the remote LDAP servers for this profile.

The Lightweight Directory Access Protocol (LDAP) is an application protocol for reading and writing directories over an IP network. It uses TCP/IP port 389 and UDP port 389. It is used to query and update an X.500 directory. LDAP is specified in a series of IETFs and RFCs, using the description language ASN.1. Affirmed Networks supports the latest specification, RFC 4511, Version 3.

LDAP Remote Server

To add an LDAP Remote Server:

1. Expand **Service Construct** in the tree.
2. Expand **Ldap**.
3. Click **Remote Server**.
4. Configure the parameters as follows:

Table 10-169 LDAP Remote Server Parameters

Parameter	Description
Name	LDAP server name.
Admin State	Admin state: ■ enabled ■ disable
Password	LDAP server bind password
Address	LDAP server IP address
Port	LDAP server port
Timeout	LDAP server timeout value, in seconds
Base DN	LDAP server base distinguished name string.
Bind Retry	LDAP Server bind retry

Table 10-169 LDAP Remote Server Parameters

Parameter	Description
Bind DN	LDAP Server bind distinguished name string
Idle Timeout	LDAP server connection idle timeout (in seconds) used to ping the server. If no activity occurs on this server connection for more than this idle timeout value, a abandon message is sent to the server serving as a ping. The response from server is to reset the timer on monitoring this connection. Otherwise, the connection is closed.
Version	LDAP Server version

5 Click the **Save** icon.

LDAP Feature Group

To add an LDAP Feature Group:

1 Expand **Service Construct** in the tree.

2 Expand **Ldap**.

3 Click **Feature Group**.

4 Configure the parameters as follows:

Table 10-170 LDAP Feature Group Parameters

Parameter	Description
Name	LDAP Feature Group name.
Admin State	Admin state: ■ enabled ■ disable
Enforce	Mark the checkbox to have the attributes checked, even in cases of parameter error.
Action	LDAP action to take if attribute list and MMS blacklist matches: ■ Allow ■ Block
Fields when Action is set to Block:	
SMS Notification	SMS Notification text
MMS Response	MMS Error Response

Table 10-170 LDAP Feature Group Parameters

Parameter	Description
Attributes List of LDAP attributes to be checked upon LDAP response. To add additional attributes, click the **Create** icon.	
Attribute Name	Specify the Attribute Name
Priority	Specify the Attribute priority
Attr Value	Specify the attribute type and its value: ■ String value: Specify the LDAP attribute value string to be checked against its value in the LDAP response ■ Date value: Specifies to check LDAP attribute value in the LDAP response against the current date ■ Destination Regex: Specify the Regular Expression to be checked against the destination address ■ MMS Blacklist: Select the MMS Blacklist to be checked against the destination address

5 Click the **Save** icon.

LDAP Profile

If the priority of the servers is the same in a given profile, the LDAP agent performs round-robin load balancing. If the priority of the servers differs, the LDAP agent uses priority-based load balancing.

The LDAP agent performs the following actions based on the priority of the servers in a given profile.

LDAP Agent Action	Same Priority	Different Priority	Mix of Priorities
Tries the next active client connection for each LDAP search request in a round-robin fashion. ■ If no active client connections exist, the LDAP agent reverts to the current active client server connection. ■ If all client connections are inactive in a given priority, the LDAP agent tries the next priority servers in the server configuration.	X		X
If all client connections are inactive in entire profile, the LDAP agent retries the servers from the server configuration Entry Index order since priority is same for all servers).	X		
Tries the same active client connection for each LDAP search request as long the server connection is in service and no other server client connections are active in that priority group.		X	X
If the current client connection is inactive, the LDAP agent tries the next priority active client connections.		X	X
If all client connections are inactive, the LDAP agent retries the servers from priority order.		X	X

To add an LDAP Profile:

1. Expand **Service Construct** in the tree.
2. Expand **Ldap**.
3. Click **Profile**.
4. Configure the parameters as follows:

Table 10-171 LDAP Profile Parameters

Parameter	Description
Name	LDAP Profile name.

Table 10-171 LDAP Profile Parameters

Parameter	Description
Admin State	Admin state: ■ enabled ■ disable
Network Context	Network Context to use to connect to the LDAP remote server
Loopback IP	Select the Loopback IP Address from the configured Network Context to be used as the local address, when connecting to the servers. Because a server may be used by different profiles, the same Loopback IP Address must be used in all profiles that use the same Network Context, configured or not. The Loopback IP Address must already exist. Create it at Network Context > *name* > Loopback IP.
The LDAP agent applications (that is, GW/HTTP Proxy) set the LDAP query key values based on the Lookup Key Type and Lookup Key String	
Lookup Key String	Enter the LDAP lookup key string
Lookup Key Type	Select the lookup key type: ■ ue-msisdn ■ ue-ip-address
Sort Attribute Name	Enter the LDAP attribute name to use to sort the search results. If not specified, the results are given in the order in which they are received from LDAP server.
Sort Order	Sort order to be used to sort multiple entries in the response from the server, based on the configured Sort Attribute Name. The entries are sorted as follows: ■ all (default) – MCC selects all attributes (up to 100) from matching entries in the order in which they are received. If no Sort Attribute Name is configured, all entries are matching entries. ■ ascending-first – MCC selects the first matching entry after all entries are sorted in ascending order based on the Sort Attribute Name. ■ descending-first – MCC selects the first matching entry after all entries are sorted in descending order based on the Sort Attribute Name. ■ first – MCC selects the first server that has a matching attribute based on the Sort Attribute Name.
Default Action	Action to take in case of permanent LDAP failure: ■ Allow ■ Block
Fields when Action is set to Block:	
SMS Notification	SMS Notification text

Table 10-171 LDAP Profile Parameters

Parameter	Description
MMS Response	MMS Error Response
Feature Group List of LDAP Feature Groups for the profile. To add additional LDAP Feature Groups, click the **Create** icon.	
Name	LDAP Feature Group name. The LDAP Feature Group must already exist. See LDAP Feature Group.
Priority	Unique priority for the LDAP Feature Group
Remote Server List of LDAP Remote Servers for the profile. To add additional LDAP Remote Servers, click the **Create** icon.	
Name	LDAP remote servers for the profile. The LDAP remote server must already exist. See LDAP Remote Server.
Priority	Priority for the LDAP remote servers: ■ If the priority of the specified servers differs, the LDAP agent uses priority-based load balancing. ■ If the priority of the specifies servers is the same, the LDAP agent performs round-robin load balancing.

5 Click the **Save** icon.

Loopback IP List

Use this object to configure a loopback IP list.

To add a Loopback IP List:

1. Expand **Service Construct** in the tree.
2. Click **Loopback IP List**.
3. Configure the parameters as follows:
   - **Name**: Loopback IP List name
4. Click the **Save** icon.
5. Expand the Loopback IP List you added.
6. Click **Network Context**.
7. Configure the parameters as follows:
   - **Name**: Select the Network Context that contains the loopback IP addresses.
8. Click the **Save** icon.
9. Expand the Network Context you specified.
10. Click **Loopback IP**.
11. Configure the parameters as follows:
    - **Name**: Select the loopback IP address. The Loopback IP address must already exist. Create it at Network Context > *name* > Loopback IP.
12. Click the **Save** icon.
13. Repeat step 10 through step 12 to add as many Looback IP addresses as needed.

Multimedia Messaging Service

Use this object to configure a Multimedia Messaging Service (MMS). MMS provides messaging capabilities for delivery of multimedia messages, composed of text, audio, graphics, photographs, and other media types on a network.

MMS packets can be routed among a pool of configured Multimedia Messaging Service Centers, based on:

- MMS originator and destination address
- MMS Short code value, range, and Regular Expression
- MMSC Load balance suffix range (Round-Robin)
- MMSC Message ID suffix
- Default MMSC in the group
- Backup MMSC

MMSCs are evaluated based on priority.

The MCA20 supports routing of all MM1, MM3, and MM4 PDUs to/from the MMSCs application server.

Supported MIME Types

Video Input and Output

- video/mp4
- video/3gpp
- video/3gpp2
- video/quicktime
- video/mpeg
- application/vnd.rn-realmedia
- application/shockwave-flash
- video/flv
- video/avi
- video/x-ms-asf
- video/ogg (input only, copy to output)
- video/matroska (input only, copy to output)
- video/webm (input only, copy to output)

Acoustic Audio Input and Output

- audio/aiff
- audio/amr
- audio/amr-wb (input only, copy to output)
- audio/mpeg
- audio/mp3
- audio/ac3
- audio/au
- audio/x-pn-realaudio
- audio/mp4
- audio/3gpp
- audio/3gpp2
- audio/quicktime
- audio/aac
- audio/flac
- audio/wav
- audio/avi
- audio/x-ms-wma
- audio/ogg
- audio/matroska
- audio/webm

Synthesized Audio Input and Output

- application/vnd.smaf
- audio/midi
- audio/sp-midi
- audio/mobile-xmf
- audio/x-nokia-rng
- audio/iMelody

Image Input and Output

- image/jpeg
- image/pjpeg
- image/gif
- image/png
- image/jp2
- image/tiff
- image/bmp
- image/wbmp
- image/svg+xml (input only, copy to output)
- application/pdf (input only, copy to output)

Text Input and Output

- text/plain
- text/x-c
- text/html
- text/css
- text/x-javascript
- application/vnd.symbian.install (input only, copy to output)
- application/xml
- text/vnd.wap.wml
- text/x-vCard
- text/x-vNote
- text/x-vCalendar

Text Input and Output Character Set Types

- US-ASCII
- UTF-7
- UTF-8
- UTF-16
- UTF-16BE
- UTF-16LE
- UTF-32
- UTF-32BE
- UTF-32LE
- UCS-2
- UCS-2BE
- UCS-2LE
- UCS-4
- UCS-4BE
- UCS-4LE
- ISO-8859-1 ... ISO-8859-10
- WINDOWS-1250 ... WINDOWS-1258
- KOI8-R
- KOI8-U
- GBK
- GB18030
- GB2312
- BIG5
- ISO-2022-JP
- ISO-2022-JP-1
- ISO-2022-JP-2
- ISO-2022-CN
- ISO-2022-CN-EXT
- ISO-2022-KR
- SHIFT-JIS

Multimedia Messaging Service Center

To add a Multimedia Messaging Service Center:

1. Expand **Service Construct** in the tree.
2. Expand **Mms**.
3. Click **Mmsc**.
4. Configure the parameters as follows:

Table 10-172 Multimedia Messaging Service Center Parameters

Parameter	Description
Name	Multimedia Messaging Service Center name.
Priority	Multimedia Messaging Service Center priority.
URL	Multimedia Messaging Service Center's URL. The current URL is replaced with this URL.
Transcode	Mark the checkbox to enable message transcoding for this MMSC. When an MMS message is downloaded, transcode it according to the UA Profile. See UA Profile.
Message ID Suffix	Message ID suffix for the MMSC.
Fall Back MMSC	Select the backup MMSC.
Host	MMSC hostname (for example, mms.era.pl)
Address	IP Address for the MMSC, can be IP v4 or IP v6.

Table 10-172 Multimedia Messaging Service Center Parameters

Parameter	Description
Port	Port for the MMSC.
Load Balance Suffix	Enter the Start Value and End Value that represents the Load Balance Suffix range. To add additional ranges, click the **Create** icon.
Max Message Size	Maximum message size, in KB.
Error Response	Enter the error response when the maximum message size is exceeded
Max Number Recipients	Maximum number of recipients
Error Response	Enter the error response when the maximum number of recipients is exceeded
Short Code	Enter the Start Value and End Value that represents the Short Code range used to route MMS packets. To add additional ranges, click the **Create** icon.
Regex	Enter the Short Code Regular Expression. To add additional Regular Expressions, click the **Create** icon.
Value	Enter the Short Code value. To add additional values, click the **Create** icon.

5 Click the **Save** icon.

Multimedia Messaging Service Center Group

To configure a group of MMSCs:

1. Click **Mmsc Group**.
2. Configure the parameters as follows:
   - **Name**: Multimedia Messaging Service Center group name
   - **Reject Invalid MMS Requests**: Mark the checkbox to reject GET requests if the host does not match MMSC host configuraiton.
3. Click the **Save** icon.
4. Expand the MMSC group you added.
5. Click **Mmsc**.
6. Configure the parameters as follows:
   - **Name**: Select the Multimedia Messaging Service Center to add to the group
   - **Default**: Mark the checkbox to set it as the default MMSC in the group.
7. Click the **Save** icon.

MM3 Profile

The MM3 interface allows the MMSC to exchange messages with external servers such as E-mail servers and SMSCs. The interface is typically based on IP-based E-mail protocols (such as SNMP).

To configure an MM3 interface:

1. Click **Mm3 Profile**.
2. Configure the parameters as follows:

Table 10-173 MM3 Profile Parameters

Parameter	Description
Name	MM3 Profile name
SMTP Server Name	SMTP Server domain name
SMTP Server Port	SMTP Server Port

3. Click the **Save** icon.
4. Expand the MM3 profile you added.
5. Click **PC Profile Filename**.

6 Configure the parameters as follows:

- **Filename**: Enter the PC Profile filename to be used for transcoding.

7 Click the **Save** icon.

MMS Error Response

Use this object to configure error response status and text in case of rejected MM requests:

To configure MMS error response:

1 Click **Error Response**.

2 Configure the parameters as follows:

- **Name**: Enter the error response Name.

3 In **Default Error Response**, configure the parameters as follows:

Table 10-174 Default Error Response Parameters

Parameter	Description
User Agent Prefix	Select the User Agent Prefix
Response Status	Select the Response status
Response Text	Enter the Response text

4 In **User Agent Prefix**, configure the parameters as follows:

Table 10-175 User Agent Prefix Parameters

Parameter	Description
User Agent Prefix	Enter the User Agent Prefix
Response Status	Select the Response status
Response Text	Enter the Response text

5 Click the **Save** icon.

STI Profile

To configure Standard Transcoder Interface profile:

1. Click **STI Profile**.
2. Configure the parameters as follows:

Table 10-176 STI Profile Parameters

Parameter	Description
Name	STI Profile Name
URI	STI Profile URI

3. Click the **Save** icon.

MMS Blacklist

Use this object to configure a list of destination addresses to match in To/Cc/Bcc.

To configure an MMS destination address blacklist:

1. Click **Blacklist**.
2. Configure the parameters as follows:
   - **Name**: Blacklist name
   - **LDAP in Use**: Mark the checkbox to specify that LDAP query is in use
3. Click the **Save** icon.
4. Expand the Blacklist you added.
5. Click **Destination Address**.
6. Configure the parameters as follows:
   - **Regex**: Regular expression to match the destination address, such as ^900[0-9][0-9][0-9]$
7. Click the **Save** icon.

Network Profile

Use this object to configure a minimum of one network profile for each of the network interface types and specify its network context.

To add a Network Profile:

1. Expand **Service Construct** in the tree.
2. Click **Network Profile**.
3. Configure the parameters as follows:

Table 10-177 Network Profile Parameters

Parameter	Description
Name	Enter a profile name.
Interface Type	Select an interface type: ■ s1u-gtpu ■ s5s8-gtpu-sgw ■ s5s8-gtpu-pgw ■ lawful-intercept
Network Context	Select a network context.

4. Click the **Save** icon.

Packet Filter

The Packet Filter construct defines the packet filter or service data flow configuration identified by:

- User Equipment IP address range
- Network IP address range
- User Equipment port range
- Network port range
- IP Protocol
- Flow initiator

To add a Packet Filter:

1. Expand **Service Construct** in the tree.
2. Click **Packet Filter**.
3. Configure the parameters as follows:

Table 10-178 Packet Filter Parameters

Parameter	Description
Name	Packet Filter name
IP Version	IP Version: ■ V4 only ■ V6 only ■ V4 or V6
UE IP Address Start	User equipment IPv4 address range start (inclusive)
Network IP Address Start	Network equipment IPv4 address range start (inclusive)
UE IP V6 Address Start	User equipment IPv6 address range start (inclusive)
Network IP V6 Address Start	Network equipment IPv6 address range start (inclusive)
UE Port Start	User equipment port range start value (valid for protocol TCP (6), UDP (17), SCTP (132) only)
UE Port End	User equipment port range end value (valid for protocol TCP (6), UDP (17), SCTP (132) only)
Network Port Start	Network equipment port range start value (valid for protocol TCP (6), UDP (17), SCTP (132) only)
Network Port End	Network equipment port range end value (valid for protocol TCP (6), UDP (17), SCTP (132) only)

Table 10-178 Packet Filter Parameters

Parameter	Description
Protocol	IP Protocol values, defined in usr/include/netinet/in.h
Initiator	Initiator of the connection: ■ UE: User equipment ■ Network ■ Both
UE IP Address End	User equipment IPv4 address range end (inclusive)
Network IP Address End	Network equipment IPv4 address range end (inclusive)
UE IP V6 Address End	User equipment IPv6 address range end (inclusive)
Network IP V6 Address End	Network equipment IPv6 address range end (inclusive)
Min Uplink TTL	Minimum value of the connection Time to Live. This setting enables Operators to differentiate charging based on minimum TTL values by configuring different charging groups with different service rules containing packet filters with TTL values to treat connections with different TTL differently.
Max Uplink TTL	Maximum value of the connection Time to Live. This setting enables Operators to differentiate charging based on maximum TTL values by configuring different charging groups with different service rules containing packet filters with TTL values to treat connections with different TTL differently.

4 Click the **Save** icon.

PLMN ID List

The PLMN ID List configures home and roaming (visiting) subscribers.

To add a subscriber to the PLMNID list:

1. Expand **Service Construct** in the tree.
2. Expand **Plmnid List**.
3. To add a subscriber to the home list, expand **home-list**.
4. Click **Plmnid**.
5. Configure the parameters as follows:

Table 10-179 Home List Parameters

Parameter	Description
Value	Specific PLMNID value
User Description	PLMNID list Description

6. Click the **Save** icon.
7. To add a subscriber to the roaming list, expand **roaming-list**.
8. Click **Plmnid**.
9. Configure the parameters as follows:

Table 10-180 Roaming List Parameters

Parameter	Description
Value	Specific PLMNID value
User Description	PLMNID list Description

10. Click the **Save** icon.

Protocol Application Rule Group (8.4 and later MCC version)

The Protocol Application Rule Group defines layer 7 applications and protocols for Signature Analysis by detecting deterministic and/or heuristic patterns in bidirectional packet flow. Signature Analysis is the key technology that enables Workflow to control application of advanced services on subscriber traffic (such as charging, per-application filtering, QoS, and so on).

Use the Protocol Application Rule Group to configure rules that match on the following connection attributes:

- Applications
- Flow attributes
- Protocols
- Protocol attributes
- Operating system
- Tethering

The following are the rules for matching with a Protocol Application Rule Group rule:

- If an application is specified, it must match.
- If a protocol is specified, it must match.
- If one or more protocol attributes are specified, all of them must match
- If one or more flow attributes are specified, all of them must match.
- If the subscriber operating system is specified, then it must match.
- If the flow operating system is specified, then it must match.
- If the subscriber tethering status is specified, then it must match.
- If the flow tethering status is specified, then it must match.

To add a Protocol Application Rule Group:

1. Expand **Service Construct** in the tree.
2. Click **Protocol Application Rule Group**.
3. Configure the parameters as follows:
   - **Name** – Enter a Protocol Application Rule Group name.
4. In Rule, Configure the parameters as follows:

Table 10-181 Protocol Application Rule Group Parameters

Parameter	Description
Name	Enter a rule name
Application Group:	
Name	Select the Application Group to include in the Protocol Application Rule Group: ■ Business ■ Conference ■ Database ■ E-Commerce ■ File Transfer ■ Gaming ■ Generic ■ Industrial ■ Mail ■ Messaging ■ Mobile ■ Network Management ■ Peer to Peer ■ Remote Control ■ Sharehosting ■ Social ■ Streaming ■ Tunnel ■ Voice Over IP ■ Web
Application Name	Select the Application to include in the Protocol Application Rule Group. The applications available are filtered based on the specified Application Group Name.

Table 10-181 Protocol Application Rule Group Parameters

Parameter	Description
Flow Attribute	Select the Flow Attribute(s) to include in the Protocol Application Rule Group: ■ amazon-cloud ■ android ■ apache ■ audio ■ blackberry ■ chat ■ chrome ■ ddl ■ encrypted ■ file-transfer ■ google ■ ios ■ mail ■ mariadb-server ■ microsoft-windows ■ mysql-server ■ none ■ ntlm ■ out ■ outlook_web_access ■ picture ■ stream ■ video ■ web ■ windows-mobile If you specify multiple Flow Attributes, a connection must match all the specified attributes for it to match the rule.

Table 10-181 Protocol Application Rule Group Parameters

Parameter	Description
Subscriber:	
Operating System *(Operating system of the user equipment device)*	Select the Subscriber Operating System to include in the Protocol Application Rule Group: ■ Android ■ Blackberry ■ Chrome ■ Darwin ■ Linux ■ OS X ■ Other ■ Symbian ■ Windows ■ WindowsMobile ■ WindowsPhone ■ iOS
Tethered	Specify whether there are tethered devices behind this subscriber: ■ true ■ false
Flow:	
Operating System *(Operating system of the individual flow. May differ from the subscriber operating system if from a tethered device)*	Select the Subscriber Operating System to include in the Protocol Application Rule Group: ■ Android ■ Blackberry ■ Chrome ■ Darwin ■ Linux ■ OS X ■ Other ■ Symbian ■ Windows ■ WindowsMobile ■ WindowsPhone ■ iOS
Tethered	Specify whether there are tethered devices behind this flow: ■ true ■ false

Table 10-181 Protocol Application Rule Group Parameters

Parameter	Description
Protocol Group:	
Name	Select the Protocol Group to include in the Protocol Application Rule Group: ■ Business ■ Conference ■ Database ■ E-Commerce ■ File Transfer ■ Gaming ■ Generic ■ Industrial ■ Mail ■ Messaging ■ Mobile ■ Network Management ■ Peer to Peer ■ Remote Control ■ Sharehosting ■ Social ■ Streaming ■ Tunnel ■ Voice Over IP ■ Web
Protocol Name	Select the Protocol to include in the Protocol Application Rule Group. The protocols available are filtered based on the specified Protocol.
Protocol Attribute Name	Select the Protocol Attribute(s) to include in the Protocol Application Rule Group. The protocols attributes available are filtered based on the specified Protocol Name. If you specify multiple Protocol Attributes, a connection must match all the specified attributes for it to match the rule.
To add additional rules, click the **Create** icon.	

5 Click the **Save** icon.

Quality of Service

QoS configures default and network Quality of Service characteristics associated with subscribers.

To add a QoS:

1. Expand **Service Construct** in the tree.
2. Click **Quality of Service**.
3. Configure the parameters as follows:

Table 10-182 Quality of Service Parameters

Parameter	Description
Name	QoS name
Rate Measurement Units	Rate Measurement units: ■ Kbps ■ Mbps ■ Gbps
Apn Uplink Ambr	Uplink Access Point Name Aggregate Maximum Bit Rate
Apn Downlink Ambr	Downlink Access Point Name Aggregate Maximum Bit Rate
Uplink Burst Size	Uplink Burst Size, in Kbytes
Downlink Burst Size	Downlink Burst Size, in Kbytes
QCI	QoS Class Identifier: ■ 1: Operator controlled Voice Calling ■ 2: Operator controlled Video Calling ■ 3: Operator controlled Real-time Gaming ■ 4: Operator controlled Streaming of Pre-recorded Video ■ 5: Signaling for Operator controlled applications ■ 6: Websites prioritized by Operator ■ 7: Operator controlled Live Video Streaming or Interactive Gaming ■ 8: All other traffic for premium subscriber ■ 9: All other traffic for regular subscriber
ARP	Allocation and Retention Policy

4. Click the **Save** icon.

RADIUS Mapping Template

The RADIUS Attribute Mapping template allows Operators to customize incoming and outgoing RADIUS authentication messages transmitted between the MCC TWAG and RADIUS server. Operators can customize the contents of certain RADIUS attributes and exclude certain attributes in the messages.

See the *Affirmed Networks TWAG/TWAP Administration Guide* for more information.

To add a RADIUS Mapping Template:

1. Expand **Service Construct** in the tree.
2. Expand **Radius Mapping**.
3. Click **Template**.
4. Configure the parameter as follows:
   - **Name** – Radius Mapping Template name.
5. Click the **Save** icon.
6. To add Radius attribute, expand the RADIUS Mapping Template you added.
7. Click **Attribute**.
8. Configure the parameters as follows:

Table 10-183 Attribute Parameters

Parameter	Description
Name	The name of the RADIUS attribute to be modified: ■ calledstationid ■ callingstationid ■ chargeableuserid ■ dhcpopt82 ■ dhcpopt82circuitid ■ dhcpopt82remoteid ■ nasportid ■ username

Table 10-183 Attribute Parameters

Parameter	Description
From	The value of the specified session data item will replace the value of the outgoing RADIUS attribute: ■ apnname ■ imei ■ imsi ■ macaddr ■ macaddr_1colon ■ macaddr_2colon ■ macaddr_colon ■ macaddr_hyphen ■ msisdn ■ nai ■ nil – Use to exclude an attribute from an outgoing or incoming RADIUS message. ■ tunnellocalip ■ tunnelremoteip ■ user1, user2, user3, user4, user5, user6, user7, user8, user9, user10 Use **user1**, **user2**, **user3**, **user4**, **user5**, **user6**, **user7**, **user8**, **user9**, or **user10** to allow an incoming template to save a value from an attribute and pass it on to an attribute in an outgoing template.
From Format	Specifies a substitution string to replace the value of the specified session data in the outgoing RADIUS attribute into a text string. Use "$*item*" to identify the session data item. In special cases, you can use "$$" to substitute a "$" character. Use the form "${item}" to identify the session data item if "$item" is followed by alphanumeric text. Enclose the substitution string in double quotation marks. Example: **From Format** `"imsi=$imsi,user=$nai"` This example substitutes the session IMSI and NAI with the resulting value. If the IMSI is "12345678901234" and the NAI is "foo@mytest.org", the resulting value of the attribute would be "imsi=12345678901234,user=foo@mytest.org".

Table 10-183 Attribute Parameters

Parameter	Description
To	The value of the specified session data item will be set using the value from the incoming RADIUS attribute: ■ apnname ■ imei ■ imsi ■ macaddr ■ msisdn ■ nai ■ nil – Use to exclude an attribute from an outgoing or incoming RADIUS message. ■ tunnellocalip ■ tunnelremoteip ■ user1, user2, user3, user4, user5, user6, user7, user8, user9, user10 Use **user1**, **user2**, **user3**, **user4**, **user5**, **user6**, **user7**, **user8**, **user9**, or **user10** to allow an incoming template to save a value from an attribute and pass it on to an attribute in an outgoing template.
To Format	Specifies the regular expression (PCRE) pattern to match against the incoming RADIUS attribute. The regular expression must have match groups surrounded by parentheses to select the text to be extracted from the incoming RADIUS attribute. Each match group is set in the session data items specified in the **To List** parameter in the order listed. Enclose the regular expression in double quotation marks. Example: **To Format** `“imsi=(.*),user=(.*)”`
To List	Specifies the name of the session data items in which to store the extracted values. If more than one data item is listed, the session data names must be contained within square brackets. Each match group specified in the `to-format` parameter is set in the session data items in the order listed in the **To List**. Example: **To Format** `“imsi=(.*),user=(.*)”` **To List** `[imsi nai]` The system takes the incoming attribute value of “imsi=12345678901234,user=foo@mytest.org” and stores the IMSI value of 12345678901234 and NAI value of “foo@mytest.org in the session’s data. ***Note:*** *If the number of match groups found does not equal the number of items in the* **To List** *parameter, the system does not modify the session data for the specified RADIUS attribute.*

9 Click the **Save** icon.

If the **From** or **From Format** setting fails, the attribute is removed from the outgoing RADIUS message.

If the **To** or **To Format**/**To List** setting fails, the system records the failure in the statistics.

Once you have configured the RADIUS Attribute Mapping template, you need to associate the template with a Session Learner interface (TWAG RADIUS Client or RADIUS Proxy) and a RADIUS message type.

The TWAG RADIUS Client interface has one set of templates and the RADIUS Proxy interface has templates for both the client and server sides of the session.

RADIUS Attribute Mapping Template Statistics

To view RADIUS Attribute Mapping Template statistics:

1 Expand **Service Construct** in the tree.

2 Expand **Radius Mapping**.

3 Expand **Statistics**.

4 Click an instance.

The following statistics are available:

Num Outgoing Replacements	Total number of outgoing replacements
Num Outgoing Removals	Total number of outgoing attributes removed (from nil)
Num Outgoing Format Substitutions	Number of outgoing substitutions using from-format
Num Outgoing Replacement Failures	Number of outgoing replacement failures
Num Incoming Replacements	Total number of incoming replacements
Num Incoming Removals	Total number of incoming attributes removed (to nil)
Num Incoming Matches	Number of incoming matches using to-format
Num Incoming Match Failures	Number of match failures using to-format
Num Incoming Replacement Failures	Number of incoming replacement failures

Realm List

The Realm List configures the Realm/Username@realm list.

To add a Realm List:

1. Expand **Service Construct** in the tree.
2. Click **Realm List**.
3. Configure the parameters as follows:

Table 10-184 Realm List Parameters

Parameter	Description
Name	Realm list name
User Description	Realm list description

4. Click the **Save** icon.
5. To add a username or realm to the Realm list, expand the Realm list you added.
6. Click **Realm**.
7. Configure the parameters as follows:

Table 10-185 Realm Parameters

Parameter	Description
Value	Specific username or realm value
User Description	Description of the specific username or realm

8. Click the **Save** icon.

SCTP Profile

Use this object to configure an SCTP (Stream Control Transmission Protocol) Profile.

To add an SCTP Profile:

1. Expand **Service Construct** in the tree.
2. Click **SCTP Profile**.
3. Configure the parameters as follows:

Table 10-186 SCTP Profile Parameters

Parameter	Description
Name	Service Rule name
Init Retry	Max number of attempts to retransmit the init message after which the attempted association is terminated.
Heartbeat Interval	Periodic time interval (in msecs) at which the SCTP heart beat message are sent. Value zero disables SCTP heart beats.
Path Max Retransmit	Maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive.
RTO Initial	Initial retransmission time out value (in msecs). Subsequent SCTP RTO will be recomputed starting from this value.
RTO Min	Minimum RTO value (in msecs) that any subsequent recomputed RTO may never go below.
RTO Max	Maximum RTO value (in msecs) that any subsequent recomputed RTO may never exceed.
Max In Streams	Number of inbound streams advertised in INIT.
Max Out Streams	Number of outbound streams advertised in INIT.
Cookie Life	Maximum lifespan of the SCTP cookie sent in an INIT ACK chunk, in 100 milliseconds units
Sack Period	Selective ACK period, in milliseconds. Value 0 disables the delay value.
Path MTU	Maximum transmission unit (MTU) size for SCTP streams, in bytes. Value 0 enables auto-discovery of the path MTU.

4. Click the **Save** icon.

Service Rule

The Service Rule is associated with a specific Service Data Flow, protocol analyzer, HTTP rule group, Protocol Application Rule Group, and/or Time of Day rule group. Service Rules are referenced in other services. Each rule has a unique service data flow identifier and an optional (non-unique) Correlation Identifier to be logged in CDR/EDR.

For a Service Rule to match, all of the following filters (if specified) must match:

- At least one Packet Filter
- At least one Time of Day Rule
- At least one HTTP Content Rule
- At least one Protocol Application Rule Group Rule. If multiple rules are specified in a rule group, at least one of the rules in the rule group must match.

Service Rules support the following separate categorization of traffic:

- TCP control traffic – Defined as TCP packets with IP total length equal to the IP header plus the TCP header.
- TCP data traffic and non-TCP traffic

This feature requires Service Rules to be paired to account for both types of traffic; one is the TCP Control Service Rule, one is the TCP Data Control Service Rule.

To add a Service Rule:

1. Expand **Service Construct** in the tree.
2. Click **Service Rule**.
3. Configure the parameters as follows:

Table 10-187 Service Rule Parameters

Parameter	Description
Name	Service Rule name
Admin State	Admin state: ■ enabled ■ disable

Table 10-187 Service Rule Parameters

Parameter	Description
Priority	Service Rule priority Allows service flows to select a service rule from a list of service rules based on priority. ***Note:*** *It is recommended that a Service Rule containing a Protocol Application Rule Group have a higher Priority than other Service Rules (containing Domain Rule Group, Session Rule Group, for example).*
Correlation ID	Non-unique numerical identifier for the Service Rule
Service Data Flow ID	Numerical identifier for the Service Rule The identifier does not have to be unique. Operators can configure multiple Service Rules with the same Service Data Flow ID so that multiple PCC rules can map to one service ID. When generating CDRs, MCC creates a separate service container for each service ID so associating multiple PCC rules (Service Rules) with the same service ID (SDF ID) reduces the number of service containers created in each CDR.
Time of Day Rule Group	Select the Time of Day Rule Group to specify the days and times for service rule activation. The Time of Day Rule Group must already exist. See Time of Day Rule Group.
Protocol Application Rule Group	Select the Protocol Application Rule Group to bind with the Service Rule. The Protocol Application Rule Group must already exist. See Protocol Application Rule Group (8.4 and later MCC version). ***Note:*** *If the Service Rule specifies both a Protocol Application Rule Group and an HTTP rule group, and the Protocol Application Rule Group specifies a protocol, it must be protocol HTTP. Or you can leave the protocol unspecified and configure an application instead.*
HTTP Rule Group	HTTP rule group (L7 HTTP Header based filter) to bind with the Service Rule (Optional) The HTTP rule group must already exist. See HTTP Rule Group.
TCP Filter	Specifies the TCP accounting category of the Service Rule: ■ all: accounts for all traffic ■ data: accounts for TCP data traffic and non-TCP traffic ■ control: accounts for TCP control traffic (packets with IP total length equal to the IP header plus the TCP header) When set to Data or All, the Service Rule may specify Packet Filter(s), a Time of Day Rule Group, a Protocol Application Rule Group, and an HTTP Rule Group. When set to Control, the Service Rule cannot have child objects. Multiple TCP Data Service Rules can link to the same TCP Control Service Rule.

Table 10-187 Service Rule Parameters

Parameter	Description
TCP Control Service Rule	When **TCP Filter** is set to Data, specifies the linked TCP Control Service Rule for accounting (required).
Service Activation	Specifies when to use or skip the service flow for packet classification: ■ always on - always use this service flow for classification ■ external activation - use the activation state of the service flow to determine whether to use or skip the service flow for packet classification.
TLS Rule Group	The TLS Rule Group for matching on SNI (Server Name Indication) and Server certificate CN (Common Name) fields of a TLS handshake. The TLS Rule Group must already exist. See TLS Rule Group.
Domain Rule Group	Optional Domain name rules. The Domain Rule Group must already exist. See Domain Rule Group.
Session Rule Group	Optional Session name rules. The Session Rule Group must already exist. See Session Rule Group.
PCC Rule Name	Applies when **Service Activation** is set to **external activation**. The Charging Rule name from PCRF to support service rule grouping. This option allows for multiple service rules with the same name but with different priorities and different correlation IDs. For example, you can apply the same PCC Rule Name to a set of service rules (some with Packet Filters, some with HTTP Rule Groups, and some with TLS Groups), all of which can be activated by a single Charging Rule Name installation from the PCRF. You can activate a list of service rules that share the same PCC Rule Name and apply the configuration to the following objects: ■ Online/offline rating group ■ Metering rating group ■ QoS flow You can associate a maximum of 32 service rules with one Service Rule Group.
Install Default Bearer Packet Filters on UE	Specifies whether the TFT defined in the charging action should be sent to the UE: ■ enabled ■ disable When enabled, the PGW does not send packet filters included in the service rule to UE.

Table 10-187 Service Rule Parameters

Parameter	Description
Include Service Data Flow ID in Offline SDC	Specifies whether to include the service data flow ID in service data containers (SDCs): ■ enabled – When generating CDRs, the MCC includes the service data flow ID in SDCs. ■ disabled – When generating CDRs, the MCC excludes the service data flow ID in SDCs. When disabled, the following guidelines apply: ■ Applies to static and predefined service rules only, which are pre-configured on the MCC. ■ Applies to Gz/Rf, Ga (GTPP), and local (CSV/ASN.1) CDRs. ■ Offline Charging **CDR Report Level** must be set to **bearer**. ■ Rating Group **Reporting Level** must be set to **Service Rule**. ■ Configure the same **Service Data Flow ID** for all Service Rules under each Rating Group that does not need the service data flow ID reported in SDCs. Only the Rating Group will be included in the SDC along with the usage information for all Service Rules associated with that Rating Group. However, the service data flow ID will not be included in the SDC. ■ Ensure the **Service Data Flow ID** for Service Rules configured with this parameter set to **disabled** does not overlap with another service rule that has the this parameter set to **enabled**. ■ Suppress the Service-Identifier AVP under the Multiple-Services-Credit-Control AVP in Gy interface data record templates.
TDF Application ID	Application ID to use in Application-Detection-Information AVP for Application Start/Stop notifications
Packet Filter	Select the packet filter(s) to bind with the Service Rule. This packet filter must already exist. See Packet Filter. To add additional packet filters, click the **Create** icon.

4 Click the **Save** icon.

Session Rule Group

Use this object to configure a list of rule groups that can be configured for RAT type, MBR matching, and/or device characteristics.

Video adaptation and video pacing use a Service Rule to match a Serving Policy. When HTTP proxy receives an HTTP response from the origin server, MCC adjusts the video adaptation QoE or video-pacing attributes based on the UE RAT type or bandwidth. MCC supports dynamic video adaption and video pacing adjustment according to the RAT type IE in the RADIUS accounting start message and the UE real-time throughput.

And, Operators can use device characteristics to configure differentiated rate-limiting bit rates based on device-type or device screen size.

To add a Session Rule Group:

1. Expand **Service Construct** in the tree.
2. Click **Session Rule Group**.
3. Configure the parameter as follows:
   - **Name** – Enter a Session Rule Group name.
4. In **Rule**, configure the parameters as follows:

Table 10-188 Rule Condition Parameters

Parameter	Description
Name	Rule name
RAT Type	RAT (Radio Technology) used by the mobile device: ■ E-UTRAN ■ GAN ■ GERAN ■ HSPA-EV ■ NON-3GPP ■ UTRAN ■ VIRTUAL ■ WLAN ■ NBIOT-EUTRAN

Table 10-188 Rule Condition Parameters

Parameter	Description
Device Type	Device type from the device database list: ■ HANDHELD ■ FEATURE-PHONE ■ SMART-PHONE ■ MODEM ■ DONGLE ■ TABLET ■ VEHICLE ■ CONNECTED-DEVICE ■ ROUTER ■ MODULE ■ EBOOK ■ FEMTO-AP
Max Screen Height	Maximum screen height of the device
Max Screen Width	Maximum screen width of the device
Min Screen Height	Minimum screen height of the device
Min Screen Width	Minimum screen width of the device
Congestion Level	Congestion level for applying optimization: ■ Mild ■ Moderate ■ Severe
Downlink MBR	Downlink Maximum Bit Rate range, in Kbps. Specify a start and end value.
Device Make	String to match against the device name: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

Table 10-188 Rule Condition Parameters

Parameter	Description
Device Model	String to match against the device model: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

To add additional Rules, click the **Create** icon.

5 Click the **Save** icon.

Short Message Service

Use this object to configure a Short Message Service.

Short Message Service Center Profile

To add a Short Message Service Center Profile:

1 Expand **Service Construct** in the tree.

2 Expand **Sms**.

3 Click **Smsc Profile**.

4 Configure the parameters as follows:

Table 10-189 Short Message Service Center Profile Parameters

Parameter	Description
Name	Short Message Service Center name.
User	User name to log onto the Short Message Service Center.
Password	Password to log onto the Short Message Service Center.
Address	Short Message Service Center IP address
Port	Short Message Service Center port

5 Click the **Save** icon.

Short Message Service Center Group

To configure a group of SMSCs:

1. Click **Smsc Group**.
2. Configure the parameters as follows:
   - **Name**: Short Message Service Center group name
   - **Network Context**: Network Context to use
3. Click the **Save** icon.
4. Expand the SMSC group you added.
5. Click **Smsc Profile**.
6. Configure the parameters as follows:
   - **Name**: Select the Short Message Service Profile to add to the group.
7. Click the **Save** icon.
8. Click **Looback IP**.
9. Configure the parameters as follows:

   Name: Select the Loopback IP Address to add to the group. The Loopback IP Address must already exist. Create it at Network Context > *name* > Loopback IP.
10. Click the **Save** icon.

Short Message Service Notification

To configure SMS notification text messages:

1. Click **SMS Notification**.
2. Configure the parameters as follows:

Table 10-190 Short Message Service Notification Parameters

Parameter	Description
Cause	Message cause
Brand	Brand/Market Segment
SMS Text	SMS text

3. Click the **Save** icon.

Static DNS Map

Use this object to configure a static DNS map for DNS lookups in HTTP Proxy. The static DNS map configures a set of IP addresses and a host to avoid performing a DNS lookup through configured DNS server(s). When an HTTP Proxy service specifies a static DNS map, it uses the map's configured IP Address list to open server connections for HTTP request.

Static DNS Map

To add a Static DNS Map:

1. Expand **Service Construct** in the tree.
2. Click **Static DNS Map**.
3. Configure the parameter as follows:

Table 10-191 Static DNS Map Parameters

Parameter	Description
Name	Static DNS map name
Network Context	Network Context associated with the static map
Returned Addr Order	Specifies how the returned host address list is constructed: ■ static ■ round-robin

4. Click the **Save** icon.
5. Expand the Static DNS map you added.
6. Click **Host**.
7. Configure the parameters as follows:

Table 10-192 Host Parameters

Parameter	Description
Host	Static DNS map host
IP Address	Host IP Address List You can specify up to 5 IPv4 addresses and 5 IPv6 addresses To add additional IP addresses, click the **Create** icon.

8. Click the **Save** icon.

Subscriber Group

A Subscriber Group is a group of subscribers whose traffic is rate-limited to a configured aggregate QoS Policy. When the aggregate usage of all the users in the group exceeds the configured limits, the packets from these users are dropped.

To add a Subscriber Group:

1. Expand **Service Construct** in the tree.
2. Click **Subscriber Group**.
3. Configure the parameters as follows:

Table 10-193 Subscriber Group Parameters

Parameter	Description
Name	Subscriber Group name
File Name	File name containing Subscriber IDs.
Subscriber ID Type	Username

4. Click the **Save** icon.

TCP Optimization Profile

TCP Optimization Profile specifies changes to the TCP/IP stack targeted to improve throughput and user experience in the mobile network.

To add a TCP Optimization Profile:

1. Expand **Service Construct** in the tree.
2. Click **TCP Optimization Profile**.
3. Configure the parameters as follows:
   - **Name** – Enter a TCP Optimization Profile name.
4. Click the **Save** icon.
5. Expand **TCP Optimization Profile**.
6. Expand the TCP Optimization Profile you added.
7. Click **TCP**.
8. Configure the parameters as follows:

Table 10-194 TCP Optimization Profile Parameters

Parameter	Description
Receive Mss	TCP received maximum segment size, in bytes
Fast Retransmit Dupacks	TCP number of duplicate acknowledgments to trigger the fast retransmit algorithm.
Congestion Control	TCP Congestion Control algorithm: ■ bic ■ cubic ■ highspeed ■ htcp ■ hybla ■ illinois ■ lp ■ reno ■ scalable ■ vegas ■ veno ■ westwood ■ yeah
Send Buffer Size	TCP send buffer size, in bytes
Recv Buffer Size	TCP receive buffer size, in bytes

Table 10-194 TCP Optimization Profile Parameters

Parameter	Description
Initial Congestion Window	TCP initial congestion window, in bytes. This feature prevents the congestion control algorithm from activating prematurely for wireless links with higher latency.
Initial Receive Window	Initial TCP receive window, in bytes
Window Size	TCP window size, in bytes
Slow Start	TCP Slow Start After Idle option: ■ enabled ■ disabled Disabling this feature causes the congestion window to time out after an idle period, preventing slow start algorithm for persistent connections
Nagle Algorithm	TCP Nagle Algorithm option: ■ enabled ■ disabled Enabling this feature reduces the overhead in the wireless link and allows combining small packets at the source.
Recv Buffer Auto Tuning	TCP Receive Buffer Auto-Tuning option (enable or disable auto-tuning of TCP window): ■ enabled ■ disabled This feature is tunable for each subscriber TCP flow. Set to enabled to use auto-tuning. Set to disabled to manually configure the Recv Buffer Size or Send Buffer Size.

9 Click the **Save** icon.

Time of Day Rule Group

The Time of Day Rule Group defines a layer 7 time of day rule group. The Time of Day Group contains Time of Day filters, each keyed by Day, Start Time, and End Time. If one of the Time of Day filters matches, then the Time of Day Specification is matched.

To add a Time of Day Rule Group:

1. Expand **Service Construct** in the tree.
2. Click **Time of Day Rule Group**.
3. Configure the parameters as follows:

Table 10-195 Time of Day Rule Group Parameters

Parameter	Description
Name	Time of Day Rule Group name
Day	Select the day.
Start Time	Enter the start time.
End Time	Enter the end time.

To add additional Time of Day Rules, click the **Create** icon.

4. Click the **Save** icon.

TLS Rule Group

The TLS Rule Group defines a set of rules for matching on SNI (Server Name Indication) and Server certificate CN (Common Name) fields of a TLS handshake. When a match is found, specific actions or service(s) can be applied, based on where the Service Rule is used, such as QoS and charging policies for HTTPS traffic.

Within a rule, you can specify SNI or Common Name matching or both. If you specify both, each must match for the rule to be considered a match.

To add a TLS Rule Group:

1. Expand **Service Construct** in the tree.
2. Click **TLS Rule Group**.
3. Configure the parameters as follows:
   - **Name** – Enter a TLS Rule Group name.
4. In **Rule**, configure the parameters as follows:

Table 10-196 Rule Condition Parameters

Parameter	Description
Name	Rule Condition name
SNI URL List	URL List to match against the incoming Server Name Indication.
Server Common Name	String to match against the incoming Common Name: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.
SNI	String to match against the incoming Server Name Indication: ■ begins-with ■ ends-with ■ contains ■ regex: Regular Expression ■ exact Enter the Match value.

To add additional Rule Conditions, click the **Create** icon.

5. Click the **Save** icon.

TLS Termination Policy

The TLS Termination Policy configures policies for terminating TLS connections on behalf of Operator's or Operator Partners' servers. The policy is applied when TLS connection's destination IP address matches the network context and one of the configured server addresses in the TLS Termination Policy.

The policy must also include server's certificate and private key that authenticate TLS connections on behalf of the server. If the private key is password-protected (recommended) a key passphrase must also be configured.

Server certificates and private keys configured in the TLS Termination Policy must be present in the /public/content/tls/servercerts/ folder on the MCM.

To add a TLS Termination Policy:

1. Expand **Service Construct** in the tree.
2. Click **TLS Termination Policy**.
3. Configure the parameters as follows:

Table 10-197 TLS Termination Policy Parameters

Parameter	Description
Name	TLS Termination Policy name
Network Context	Network Context through which the TLS server is reachable.

4. Click the **Save** icon.
5. In **IP Address**, configure the TLS server IP address list.

   To add additional IP Addresses, click the **Create** icon.
6. In **Sites**, configure the TLS server name list:

Table 10-198 Sites Parameters

Parameter	Description
Name	TLS server virtual name
Certificate	TLS server certificate filename.
Key	TLS server key filename.
Key Passphrase	TLS server key file passphrase.
Default	Mark the checkbox to set this site as the default site.

To add additional associations, click the **Create** icon.

7 Click the **Save** icon.

UA Profile

Use this object to configure a User Agent Profile.

To add a User Agent Profile:

1 Expand **Service Construct** in the tree.

2 Click **UA Profile**.

3 Configure the parameters as follows:

- **Name**: UA Profile name

4 In **User Agent Key**, configure the association between the User Agent and the UA Profile file:

Table 10-199 User Agent Key Parameters

Parameter	Description
User Agent Key	User Agent Key
UA Profile Filename	UA Profile Filename

To add additional associations, click the **Create** icon.

5 To configure the association between the Default User Agent and UA Profile file, expand the UA Profile you added.

6 In **UA Profile Default**, configure the association between the Default User Agent and UA Profile file:

Table 10-200 UA Profile Default Parameters

Parameter	Description
User Agent Key	Select the User Agent Key
UA Profile Filename	UA Profile Filename

To add additional associations, click the **Create** icon.

7 Click the **Save** icon.

URL List

URL List defines a list of URLs. This object is referred to by HTTP Rule Group and used as rules to match HTTP Request's URL.

The following guidelines apply to the URL List file format:

- The file used to configure the URL List must be a text file.
- The filter database is built when the URL List is configured and the file exists at designated location on MCC. Operators may import the file from the remote server or from local file. If the file is imported from the local file, the file is uploaded to the directory /public/content/policylists/url/userlists/ on the MCC. For import instructions, see Import Command.
- If you make changes to the file, you must import the file from the CLI (using the content-filter import debug command) to rebuild the database for the new file to take effect.
- The file should have a Fully Qualified Domain Name (FQDN) for each line for HTTP request URL prefix or exact-match:
  - The protocol schema is ignored and anything before "//" and including "//" is skipped. Only the URL following "//" is used.
  - If line contains a star "*", the entry is added in the database using the string before "*" for URL prefix-match. Otherwise, the entry is added in the database for URL exact-match.

To add a URL List:

1. Expand **Service Construct** in the tree.
2. Click **URL List**.
3. Configure the parameters as follows:

Table 10-201 URL List Parameters

Parameter	Description
Name	URL list name
Import as URL Prefixes	Specifies whether to treat URLs in the list as URL prefixes, rather than exact match URLs.

Table 10-201 URL List Parameters

Parameter	Description
Import From	Specifies to import from: ■ **Import from server**: references a file to be imported from a file server and configures a rule for importing the file. ■ **Import from local file**: references a file name for importing the file on local directory: */public/content/policylists/url/userlists/* The URL List database is built after an import action. The file contains a list of URLs in the following format. In the file, each URL is a string in the following format: http[s]://<*domain-name*>[:<*port*>]/[<*url-path*>][/*] The *port*, *url-path*, and terminating /* are optional. If /* is used, the URL is treated as an URL prefix rather than the exact-match URL. If you make changes to the file, you must import the file to rebuild the database for the new file to take effect. For import instructions, see Import Command.
Filename	Filename containing the URL list (such as folder/file-${DATE:yyyymmdd}.txt)
File Download Profile	Select the File Download Profile that defines parameters for importing the list from a file server. The File Download Profile must already exist. See File Download Profile.

4 Click the **Save** icon.

Import Command

To manually import the URL List:

1. Click the URL list you added.
2. Configure the parameters as follows:
   - **URL List Command** – Select **Import** and click **Select**.
3. Mark the checkboxes to disable alarm notification and/or a log entry if the import fails and click **Execute**.

URL List Statistics

To view URL List statistics:

1. Expand **Service Construct** in the tree.
2. Click **URL List Stats**.
3. In **URL List Commands**, select **Show Detail** and click **Select**.
   - In **Name**, enter a URL list name.
   - In **Url**, specify a pattern in URL.
   - To select only accepted entries, mark the **Accepted only** checkbox.
   - To select only rejected entries, mark the **Rejected only** checkbox.
4. Click **Execute**.

   Acuitas lists the URL list detail, including:
   - URL list name
   - Entry URL
   - Entry Status (Accepted or Rejected)
   - Reject Reason
   - Entry Rejected Reason
5. Expand **URL List Stats**.
6. Click **Summary**.

   Acuitas lists the download Summary for each URL list, including:
   - URL list name
   - Last Import Time
   - Last Import Result: Success or N/A
   - Last Import Type: manual or scheduled
   - Last Import Number
   - Last Import File Size
   - Next Scheduled Server Import Time

- Number of Accepted Entries
- Number of Rejected Entries
- Import File Name

7 Expand **Import History**.

8 Click the URL list.

Acuitas lists the Import History for all the retained URL list downloads, including:

- URL list name
- Server Import Time
- Server Import Result: Success or File does not exist on server
- Server Import File Size
- Number of Accepted Entries
- Number of Rejected Entries
- Import File Name
- Import Type: manual or scheduled

Workflow Data Stats

To view Workflow Data statistics:

1 Expand **Service Construct** in the tree.

2 Click **Workflow Data Stats**.

Acuitas lists the workflow data statistics, including:

- Local Gi received packets
- Local Gi received bytes
- Local Gi transmitted packets
- Local Gi transmitted bytes
- Local Gi tunnel received packets
- Local Gi tunnel received bytes
- Local Gi error packets
- Local Gi error bytes
- Local Gn received packets
- Local Gn received bytes
- Local Gn transmitted packets
- Local Gn transmitted bytes
- Local Gn tunnel received packets

- Local Gn tunnel received bytes
- Local Gn error packets
- Local Gn error bytes
- Fabric Gi received packets
- Fabric Gi received bytes
- Fabric Gi transmitted packets
- Fabric Gi transmitted bytes
- Fabric Gi tunnel received packets
- Fabric Gi tunnel received bytes
- Fabric Gi error packets
- Fabric Gi error bytes
- Fabric Gn received packets
- Fabric Gn received bytes
- Fabric Gn transmitted packets
- Fabric Gn transmitted bytes
- Fabric Gn tunnel received packets
- Fabric Gn tunnel received bytes
- Fabric Gn error packets
- Fabric Gn error bytes
- TND received packets
- TND received bytes
- TND transmitted packets
- TND transmitted bytes
- TND error transmitted packets
- TND error transmitted bytes
- Force Drops
- UE router upstream subnet received packets
- UE router TCP MSS adjusted packets
- Gi session lookup
- Gn session lookup
- Gn bearer lookup
- TND session lookup
- Discard Packets

Services

Create *service instances* for various services used in workflow. Workflow defines the treatment of a service flow across various services.

Table 10-202 Services

Service	Description
ACL	Defines Access Control List service
Affirmed Apps > Fair Bandwidth Usage	Normalizes bandwidth use then monthly subscription levels are breached
Charging > Rating Group	Defines the basis for charging service data flows
Charging > Billing Plan	Defines the charging method to be applied to list of Rating Groups
Charging > Charging Instance	Binds one or more billing plans
Charging > Service Data Flow	Lists each service data flow that is evaluated on each billing plan during flow classification, in order of evaluation.
Content Cache	Defines the behavior of the web and video cache
Content Filter > Instance	Defines the filtering capability for a subscriber workflow
Content Filter > Static Category	Is used by a content filter *instance* to either allow (white list) or deny (black list) content requests to a specific list of domains or URLs.
Content Filter > Content Categorization	Categorizes content into one or more categories. The Content Filtering Service applies configured actions (block, terminate, allow, redirect) to user HTTP transactions based on the category determined.
CRBN Profile	Configures a Changing Rule Base Name profile to specify the CRBN names that can be received from the PCRF.
DNS Proxy > Cache	Lists Cache display
DNS Proxy > Cache Stats	Lists Cache statistics
DNS Proxy > Domain Tunnel Age Time	Configures inactive blocking domain age time for DNS tunnel detection
DNS Proxy > DNS IP Flow	Configures a DNS Proxy IP Flow
DNS Proxy > DNS Policy	Defines DNS Policy
DNS Proxy > DNS Reverse Cache	Defines DNS Reverse Cache
DNS Proxy > Instance	Configures DNS Proxy Service instance

Table 10-202 Services

Service	Description
DNS Proxy > Module Stats	Lists DNS Proxy module statistics
DNS Proxy > DNS Proxy Service	Configures a DNS Proxy Service
DNS Proxy > Domain Clean Time	Configures global blocking domain clean time for DNS tunnel detection.
DNS Proxy > Tunnel Detection Profile	Configures settings to detect and block DNS tunneling transactions and receive notification of those actions.
Health Check	Confiigures a Health Check of external systems
Multi Protocol Proxy > ABR Optimization Profile	Configures an ABR Rate Limiting Optimization Profile
Multi Protocol Proxy > Back End Forwarding	Defines forwarding of HTTP requests between CSM modules
Multi Protocol Proxy > Client Connections	Defines Multi Protocol Proxy client connection parameters
Multi Protocol Proxy > Encryption Profile	Defines the Encryption Profile
Multi Protocol Proxy > Explicit Proxy Profile	Defines Explicit Proxy Address Profile
Multi Protocol Proxy > Fraud Detection Profile	Defines Fraud Detection Profile
Multi Protocol Proxy > HTTP IP Flow	Defines HTTP IP Layer 3 service flow
Multi Protocol Proxy > HTTP Request Policy	Defines HTTP Request Policy
Multi Protocol Proxy > HTTP Response Policy	Defines HTTP Response Policy
Multi Protocol Proxy > HTTP Transaction Record Profile	Defines HTTPS Transaction Record Profile
Multi Protocol Proxy > HTTPS Profile	Defines HTTPS Policy
Multi Protocol Proxy > Instance	Defines HTTP Proxy Service instance
Multi Protocol Proxy > LTMI	Defines a Long Term Mobile ID (LTMI)
Multi Protocol Proxy > Minify	Configures minification of Javascript/CSS/HTML
Multi Protocol Proxy > Optimization Overload Control	Configures optimization CPU overload control

Table 10-202 Services

Service	Description
Multi Protocol Proxy > Preemptive DNS	Replaces URLs in the response with the IP address of one of the Affirmed Networks Gi local loopback addresses and configured DNS Token before sending to the client.
Multi Protocol Proxy > Server Connections	Defines Multi Protocol Proxy server connections
Multi Protocol Proxy > Service Data Flow	Lists each service data flow that is evaluated on each Multi Protocol Proxy during flow classification, in order of evaluation.
Multi Protocol Proxy > Steering Group	Configures group of steering destinations
Multi Protocol Proxy > TCP Splicing Policy	Defines TCP Splicing policy
Multi Protocol Proxy > Toll Free Profile	Defines profile for toll free data traffic
Multi Protocol Proxy > Traffic Control Profile	Defines profile for handling splicing traffic
Multi Protocol Proxy > UDP	Defines profile for handling UDP Proxy
Multi Protocol Proxy > UDP Policy	Defines a UDP Policy
Multi Protocol Proxy > Video Pacing	Enable/Disable video pacing
Multi Protocol Proxy > Web Image Optimization Profile	Configures an HTTP Web Image Optimization Profile
HTTP Server > Entitlement Service	Configures an Entitlement Service mapping
HTTP Server > Instance	Configures an HTTP Server Instance
HTTP Server > HTTP Server Policy	Configures an HTTP Server Policy
Metering Service > Geographic Redundancy Group	Defines the Geographic Redundancy Groups to associate with the Metering Service instance
Metering Service > Metering Instance	Defines the Metering Service instance to operate in parallel to the charging service to convey the usage counts to the gateway
Metering Service > Service Data Flow	Lists each service data flow that is evaluated on each metering service during flow classification, in order of evaluation.
Quality of Service > QoS Flow	Allows for service data flow-level rate enforcement

Table 10-202 Services

Service	Description
Quality of Service > QoS Policy	Defines the QoS to be given to a list of QoS Flows
Quality of Service > Service Data Flow	Lists each service data flow that is evaluated on each QoS policy during flow classification, in order of evaluation.
Rate Limiting Subscriber Group	Configures a rate-limiting Subscriber Group
SMTP Proxy > Instance	Configures a Simple Mail Transfer Protocol Proxy instance
Steering > Service Data Flow	Lists each service data flow that is evaluated on each steering policy during flow classification, in order of evaluation.
Steering > Steering Flow	Configures a Layer 3 Steering Flow
Steering > Steering Policy	Configures a Layer 3 Steering Policy
Subscriber Firewall > Service Data Flow	Lists each service data flow that is evaluated on each subscriber firewall policy during flow classification, in order of evaluation.
Subscriber Firewall > Subscriber Firewall Flow	Defines Network Address and Port Translation treatment of multiple classified traffic flows
Subscriber Firewall > Subscriber Firewall Policy	Binds one or more (prioritized) Subscriber Firewall Flows and defines the NAT treatment to be applied when associated with a workflow data profile (or service flow)
Video Adaptation > Instance	Configures video adaptation instance
Video Adaptation > Offline Serving Policy	Configures offline serving policy
Video Adaptation > Offline Transcoding Policy	Configures offline transcoding policy
Video Adaptation > Online Transcoding Policy	Configures online transcoding policy
Video Adaptation > Target Media Profile	Defines the set of media encoding parameters to be applied for transcoding a cached object.
Video Adaptation > Transcoding Map	Configures a list of source > target map entries to be used in the online transcoding policy
Video Adaptation > Transcoding Rule	Configures rule to be eligible for transcoding
Video Adaptation > Service	Configures video adaptation service

Table 10-202 Services

Service	Description
WAP Gateway > Instance	Configures a Wireless Application Protocol Gateway Service instance
WAP Gateway > Service Data Flow	Lists each service data flow that is evaluated on each WAP Gateway during flow classification, in order of evaluation.
WAP Gateway > WAP IP Flow	Configure a Wireless Application Protocol Gateway Service IP Flow
WAP Gateway > WTLS	Configure a Wireless Transport Layer Security

Note: *As an alternative procedure, use the Affirmed Open Workflow application to define services. For instructions, see Affirmed Open Workflow.*

ACL

Operators can apply access control list (ACL) filtering to incoming control traffic to restrict or permit access to MCC interfaces. ACLs are applied on a network context basis, where access control filters apply to all interfaces within a specified network context.

To add an ACL service:

1. Expand **Services** in the tree.
2. Expand **ACL**.
3. Click **ACL Network Context**.
4. Configure the parameters as follows:

Table 10-203 ACL Network Context Parameters

Parameter	Description
Name	Select the Network Context
ACL List	The ACL List to use. The ACL List must already exist. See ACL List.

5. Click the **Save** icon.

Charging: Rating Group

The Rating Group defines the basis for charging the service data flows. It defines the mapping between usage units (octets, time, or event) and cost. Quota management can occur at the rating group level or at a higher shared credit-pool level.

When a billing plan is applied to a session, the MCC performs the following memory allocation:

- Allocates memory for all rating groups that have at least one service rule configured with the Service Activation parameter set to always-on.
- Does not allocate memory for rating groups that only have service rules configured with the Service Activation parameter set to external-activation.

When applying the billing plan for a Charging-Rule-Base-Name (CRBN) profile, the MCC only allocates memory for rating groups that have at least one service rule configured with the Service Activation parameter set to always-on or that have a service rule that is part of the CRBN service rule list.

Note: *MCC does not deallocate memory for a rating group within a billing plan even if the last service rule is removed from that rating group*

The Service Rule supports the following separate categorization of traffic, which can be used for charging:

- TCP control traffic – Defined as TCP packets with IP total length equal to the IP header plus the TCP header.
- TCP data traffic and non-TCP traffic

This feature requires Service Rules to be paired to account for both types of traffic; one is the TCP Control Service Rule, one is the TCP Data Control Service Rule. For more information, see Service Rule.

To add a Rating Group:

1. Expand **Services** in the tree.
2. Expand **Charging**.
3. Click **Rating Group**.
4. Configure the parameters as follows:

Table 10-204 Rating Group Parameters

Parameter	Description
Name	Rating Group name

Table 10-204 Rating Group Parameters

Parameter	Description
Charging Method	Charging Method: ■ online - prepaid/closed-loop ■ offline - postpaid/open-loop ■ local ■ no charge - subscriber traffic that uses this rating group is either not charged or CDRs are not generated for this rating group. This feature is useful when an Operator wants to exclude certain flows such as DNS requests or portal requests used to charge subscribers. ■ metering ■ no metering ■ afind - AF Indication for SDF detection
Quota ID	Unique Rating Group ID
Priority	Rating Group priority Priority resolves conflicts in the case of a multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object. Thus, Rating Group priority takes precedence over the associated service rule priority.
Admin State	Admin State: ■ enabled ■ disabled
Advice of Charge	Advice of Charge The Advice of Charge must already exist. See Advice of Charge
Multiplier	Multiplier applied to volume and event charging
Measurement Method	Measurement method: ■ time ■ volume ■ both: time and volume ■ event (applies only when Charging Method is set to offline or local)
Volume Measurement Count	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Volume measurement count: ■ total octets ■ input octets ■ output octets

Table 10-204 Rating Group Parameters

Parameter	Description
Volume Measurement Layer	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Volume measurement layer: ■ layer3: counts the entire IP datagram ■ layer4: excludes the IP header ■ layer7: excludes the IP header and the UDP/TCP/SCTP header
TCP Retransmission	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Inclusion or exclusion of TCP retransmissions in volume counts.
Credit Pool ID	***Note:*** *Applies when Charging Method is set to Online.* Credit pool used to grant credit blocks. ***Note:*** *Enter 0 if no credit pool is used.*
Quota Hold Time	Hold time after inactivity, in seconds.
Reporting Level	Policy control reporting level: ■ rating group ■ service rule ■ ratingGroupAndQci - enables the MCC PGW to generate service data containers at the rating group and QoS Class Identifier (QCI) level for session-level Gz/Rf CDR reporting
Quota Consumption Time	***Note:*** *Applies when Measurement Method is set to Time or Time and Volume.* Inactivity timeout for time-based accounting, in seconds.
Time Threshold	***Note:*** *Applies when Measurement Method is set to Time or Time and Volume.* Time threshold, in seconds ***Note:*** *Enter 0 if thresholding not desired*
Volume Threshold	***Note:*** *Applies when Measurement Method is set to Volume or Time and Volume.* Volume threshold, in bytes ***Note:*** *Enter 0 if thresholding not desired*
Event Threshold	***Note:*** *Applies when Measurement Method is set to Event.* Event threshold. ***Note:*** *Enter 0 if thresholding not desired*
Credit Authorization Event	***Note:*** *Applies when Charging Method is set to Online.* Credit authorization beginning stage: ■ bearerSetup: first control signaling packet ■ firstSdfPkt: first data packet

Table 10-204 Rating Group Parameters

Parameter	Description
Quota Black List Timer	***Note:*** *Applies when Charging Method is set to Online.* Quota Black List Timer, in minutes. Specifies how frequently to send grant requests after termination or suspension for this Rating Group.
Service Type	Service type: ■ data ■ mms-mo (inbound, mobile originated) ■ mms-mt (outbound, mobile termination)
Home Subscriber Charging	Specifies whether to use the rating group for home subscriber charging: ■ enabled ■ disabled
Roamer Subscriber Charging	Specifies whether to use the rating group for roaming subscriber charging: ■ enabled ■ disabled
CDR Interim Time	***Note:*** *Applies when Charging Method is set to Offline.* Interim for interim CDR generation, in seconds.
Monitor Key	***Note:*** *Applies when Charging Method is set to Metering.* Monitor Key associated with the PCRF. When the PCRF requests usage monitoring via Gx messaging, the Gateway uses the monitoring key to locate and activate the corresponding rating group.
Service Activation	Specifies when to use or skip the service flow for packet classification: ■ always on - always use this service flow for classification ■ external activation - use the activation state of the service flow to determine whether to use or skip the service flow for packet classification. This setting allows the Gateway to dynamically activate/deactivate Rating Groups.
MMS MT OCS Size	***Note:*** *Applies when Service Type is set to mms-mt.* Message size (in bytes) to be used for MMS-MT charging.
Enable Local CDR	***Note:*** *Applies when Charging Method is set to Online.* Specifies whether to enable local CDRs for the rating group: ■ enabled ■ disabled

Table 10-204 Rating Group Parameters

Parameter	Description
OCS Response Grace Period	***Note:*** *Applies when Charging Method is set to Online.* Number of seconds to pass traffic while waiting for an OCS response.
Requested Unit Value	Requested unit value for this rating group
SDF Inactivity Time	***Note:*** *Applies when Charging Method is set to Afind.* Inactivity time of SDF for AF Notification (in seconds). SDF is disabled upon the timer expiry.

5 In **Service Rule**, configure the parameters as follows:

Name — Select the service rule to link with the Rating Group. The Service Rule must already exist. See Service Rule.

To add additional Service Rules, click the **Create** icon.

6 Click the **Save** icon.

Charging: Billing Plan

The Billing Plan defines the charging method to be applied to list of Rating Groups. Multiple billing plans can be used to charge differently for home-area, roaming, preferential-roaming, fraudulent activity, and so on.

To add a Billing Plan:

1 Expand **Services** in the tree.

2 Expand **Charging**.

3 Click **Billing Plan**.

4 Configure the parameters as follows:

Table 10-205 Billing Plan Parameters

Parameter	Description
Name	Billing Plan name

5 In **Rating Group**, configure the parameters as follows:

- **Name** — Select the Rating Group to link with the Billing Plan. The Rating Group must already exist. See Charging: Rating Group.
- **Fraud Charging** — Set to true to designate this Rating Group for charging of fraudulent activity within this Billing Plan.

To add additional Rating Groups, click the **Create** icon.

6 In **Service Rule**, select only service rules used by this Billing Plan's Rating Groups:

Table 10-206 Service Rule Parameters

Parameter	Description
Name	Service Rule The Service Rule must already exist. See Service Rule.
Priority	Service Rule Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Weight	This setting allows you to apply a scaling factor to a service rule that is also associated with a rating group. For example, you could have different scaling factors for the same rating groups, depending on the billing plan.
Priority Override	Priority to override the Service Rule's priority when used with this billing plan.

To add additional Service Rules, click the **Create** icon.

7 Click the **Save** icon.

Charging: Charging Instance

The Charging Instance is made up of multiple billing plans. Billing plan selection is based on charging characteristics.

To add a Charging Instance:

1 Expand **Services** in the tree.

2 Expand **Charging**.

3 Click **Charging Instance**.

4 Configure the parameters as follows:

- **Name** – Enter a Charging Instance name.
- **State** – Set the Admin State to enabled or disabled.

Table 10-207 Charging Instance Parameters

Parameter	Description
Name	Enter a Charging Instance name.

Table 10-207 Charging Instance Parameters

Parameter	Description
State	Charging administrative state: ■ enabled ■ disabled
Priority Evaluation Mode	Priority Evaluation Mode when classifying traffic: ■ flat - Use Service Rule priority (ignore Rating Group priority). To make a match, examine all of the Service Rules on all of the Rating Groups for best priority. ■ flat-with-pcc-rule-precedence - Any PCC rules in effect have their precedence values compared with the Service Rule priority values, and the PCC rule or Service Rule with the highest priority (lowest numerical value) is selected. ■ hierarchical - Use Rating Group priority and Service Rule priority hierarchically. To make a match, examine the Rating Group in priority order and within each of them, examine the Service Rules in priority order.

5 In **Billing Plan Map**, configure the parameters as follows:

Table 10-208 Billing Plan Parameters

Parameter	Description
Name	Select the Billing Plan. The Billing Plan must already exist. See Charging: Billing Plan.
Charging Characteristic	Enter the Charging Characteristic. This number could be one provisioned in each user's subscription data, per-APN, or for the entire profile at HSS. It is significant inside the user's home network. It can be used by the Operator to specify data as CDF address, OCS address, interim reporting interval/volume for on-line charging, tariff times, and so on. It is attached to the billing plan as a method to associate the charging profile to a particular subscriber.

To add additional Billing Plans, click the **Create** icon.

6 In **Geo Redundant Group**, configure the parameters as follows:

- **Name** – Select the Geographic Redundancy Group to associate with the Charging Instance.

  The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.

To add additional Geographic Redundancy Groups, click the **Create** icon.

7 Click the **Save** icon.

Charging: Service Data Flow

Use this object to view each service data flow that is evaluated on each billing plan during flow classification, in order of evaluation.

To view service data flow:

1 Expand **Services** in the tree.

2 Expand **Charging**.

3 Expand **Service Data Flow**.

4 Click an instance.

Service data flow parameters are:

- Charging Instance
- Billing Plan
- Rating Group Priority
- Service Rule Priority
- Rating Group
- Service Rule
- Rating Group Id
- Service Rule Id

Content Cache

Content Cache Service

The Content Cache service configures the behavior of the web and video cache on the system. The system provides the ability to store cached content at the edge of the network for mobile delivery, resulting in reduced Internet bandwidth consumption and reduced latency.

To add a Content Cache Service:

1 Expand **Services** in the tree.

2 Click **Content Cache**.

3 Configure the parameters as follows:

Table 10-209 Content Cache Service Parameters

Parameter	Description
Admin State	Content cache administrative state: ■ enabled ■ disabled ***Note:*** *HTTP Proxy Admin State must be enabled before Content Cache Admin State can be enabled.*
Cache YouTube	Mark the checkbox to enable caching of YouTube videos.
Cache Metacafe	Mark the checkbox to enable caching of Metacafe videos.
Cache Dailymotion	Mark the checkbox to enable caching of Dailymotion videos.
Eviction Policy	Configure cache eviction policy: ■ LRU ■ LFU
Max Cache Life	Maximum cache lifetime, in seconds
Max Object Size Memory	Maximum object size (in bytes) that can be cached in memory. The proxy checks the maximum size of data that can be cached in the disk to avoid running out of cache buffers.
Max Object Size Disk	Maximum object size that can be cached on disk (multiple of 4K)
Min Hit Cache	Minimum number of hits to cache object.

4 Click the **Save** icon.

Eviction Threshold Disk

Use this object to configure the threshold to evict content from disk (when percent of disk usage is between minimum and maximum).

To add an Eviction Threshold Disk:

1 Expand **Services** in the tree.

2 Expand **Content Cache**.

3 Click **Eviction Threshold Disk**.

4 Configure the parameters as follows:

Table 10-210 Eviction Threshold Disk Parameters

Parameter	Description
Min	Configure minimum percent usage

Table 10-210 Eviction Threshold Disk Parameters

Parameter	Description
Max	Configure maximum percent usage

5 Click the **Save** icon.

Eviction Threshold Memory

Use this object to configure the threshold to evict content from memory (when percent of memory usage is between minimum and maximum).

To add an Eviction Threshold Memory:

1 Expand **Services** in the tree.

2 Expand **Content Cache**.

3 Click **Eviction Threshold Memory**.

4 Configure the parameters as follows:

Table 10-211 Eviction Threshold Memory Parameters

Parameter	Description
Min	Minimum percent usage
Max	Maximum percent usage

5 Click the **Save** icon.

Content Cache Instance

To add a Content Cache Instance:

1 Expand **Services** in the tree.

2 Expand **Content Cache**.

3 Click **Instance**.

4 Configure the parameters as follows:

- **Name** – Enter a Content Cache instance name.

5 In **Service Rule**, configure the parameters as follows:

Table 10-212 Service Rule Parameters

Parameter	Description
Name	Service Rule The Service Rule must already exist. See Service Rule. ***Note:*** *The Service Rule must contain an HTTP Rule Group.*
Priority	Service Rule Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Cache Bypass	Enable/Disable serving from cache: ■ disabled ■ enabled
Cache Server Response	Enable/Disable caching the response from the server: ■ disabled ■ enabled

To add additional Service Rules, click the **Create** icon.

6 Click the **Save** icon.

Content Filter

The Content Filter configures the filtering capability for a subscriber workflow. The user's HTTP transactions can be filtered using the following filter types:

- Blacklist
- Whitelist
- Static Category
- Service Rule
- Online Category Group
- Malware Category Group
- Phishing Category
- IWF Category

For each of these filter types, the Operator can specify the corresponding filtering action (allow, block, redirect, terminate) for a matching HTTP request.

The filter types Online Category Group, Malware Category Group, Phishing Category and IWF Category require configuration of the Content Categorization. Content Categorization uses third party databases for categorization of user requests. User requests are categorized to one or more of well-known Online Categories, Malware categories, the Phishing category or the IWF category.

These well-known categories are maintained online by a third party. The the Affirmed Networks system updates the databases periodically, as often as every hour.

Operators can also filter web search engine results for the Bing, Google, and YouTube search engines using the Safe Search feature.

To enable a Content Filter, the HTTP Proxy service must be enabled.

Global Content Filters

Global content filters include:

- Content Filter Blacklist — Deny files that contain a list of domains or URLs to block/terminate/redirect. For a global content filter, the Operator can configure up to ten Blacklist files.
- Content Filter Whitelist — Files that contain a list of domains or URLs to allow. For a global content filter, the Operator can configure up to ten Whitelist files.

If a global filter is not configured, HTTP traffic is filtered at the instance level. The following content-filtering guidelines apply to the file format:

- Must be a text file.
- The file must be uploaded through Acuitas and located on the MCC when the Content Filter is configured. For import instructions, see HTTP Filter File Management.
- If you make changes to the file, you must import the file to rebuild the database for the new file to take effect.
- When the File Type is domain, the file should have a Fully Qualified Domain Name (FQDN) for each line for HTTP request HOST exact-match:
  - The protocol schema is ignored and anything before "//" and including "//" is skipped. Only the domain name following "//" is used.
  - If line contains only the domain (without the forward slash), only the domain is added to the database for HOST exact-match.
  - If line contains a URL (with a forward slash), only the domain name is added in the database for HOST exact-match.
  - If line contains a star "*", the line is ignored.
- When the File Type is url, the file should have a Fully Qualified Domain Name (FQDN) for each line for HTTP request HOST or URL exact-match:
  - The protocol schema is ignored and anything before "//" and including "//" is skipped. Only the URL following "//" is used.
  - If line contains only the domain (without the forward slash), the entry is added to the database for HOST exact-match.
  - If line contains a URL (with a forward slash), the entry is added in the database for URL exact-match.
  - If line contains a star "*", the line is ignored.

Content Filter Static Category Filters

Operators can define Static Content Categories for matching user traffic. The Static Category is initialized with a list of URLs or domains (host names) specified in an Operator defined file.

For a Content Filter instance, the Operator can configure up to 16 Static Category filters, each with the action (allow/block/terminate/redirect) to be applied.

Content Filter Service Rule Filters

Operators can also specify a Service Rule that contains the HTTP rule groups to be matched with a request.

The HTTP rules can specify criteria for matching user requests against HTTP request fields including:

- Request Method
- Request URI
- URL List
- Response Status Code
- Accept Header
- Content-Type Header
- Host Header
- Referer Header
- User-Agent Header

For a global content filter, the Operator can configure one Service Rule with action block/terminate/redirect.

Content Filter Online Category Group Filters

With content categorization configured, user requests can be categorized to one or more well-known Online Categories.

Operators can group a set of the well-known Online Categories using the Online Category Group configuration object. For each Online Category Group, the Operator can define a filter with action block, terminate, redirect, or allow.

Online Categories are listed in the following table:

Table 10-213 Online Categories

Name	Sites that...
abortion	Provide information or arguments in favor of or against abortion; describe abortion procedures; offer help in obtaining or avoiding abortion; provide testimonials on the physical, social, mental, moral, or emotional effects of abortion.
advertising	Provide Internet advertising services.
alcohol	Promote or sell alcoholic beverages; supply recipes or paraphernalia to make alcoholic beverages; glorify, tout, or otherwise encourage alcohol consumption or intoxication.
alcohol kids	Include the promotion, glamorization, or encouragement of drinking alcohol to excess that is aimed at children or that may have a significant appeal to children.

Table 10-213 Online Categories

Name	Sites that...
anonymizer	Offer anonymous access to websites through a PHP or CGI proxy, allowing users to gain access to websites blocked by corporate and school proxies as well as parental control filtering solutions.
art-and-museums	Include art galleries, artists, and museums. Includes all types of visual arts such as performing arts, theater, painting, drawing, sculpture, photography, natural history, science, and children's museums.
art-nudes	Contain non-pornographic, tasteful, and artful display of the naked body.
automated-web-application	Allow a computer to automatically open an http connection for reasons such as checking for operating system or application updates.
automotive	Relate to motor vehicles, dealers, sales and clubs.
bikini	Offer the sale of bikinis, mico-kinis, mono-kinis, and thongs marketed as beachwear rather than swimwear. Also sites that feature galleries and/or videos of models in bikinis.
blogging	Contain blogs.
business	Are sponsored by or devoted to individual businesses not covered by any other categories.
cash-gambling	Involve the wagering and exchange of money online.
chat	Offer users the ability to chat online.
content-delivery-service	Are content delivery/distribution networks (CDN) designed to accelerate the delivery of content rich Internet pages or large files to end users.
criminal-skills	Provide instruction for threatening or violating the security of property or the privacy of people; and how to avoid complying with legally mandated duties and obligations.
cults	Feature well-known, organized new religious movements and sects regarded as exploitative or unorthodox.
cyberbullying	Contain targeted, deliberate, and slanderous or offensive content about other people with the intent to torment, threaten, humiliate or defame them. Content is often sexual, malicious or hostile in nature and is submitted via interactive digital technology. Examples include malicious gossip; inappropriate photos posted without consent
drugs	Promote, offer, sell, supply, encourage or otherwise advocate the recreational or illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
dynamic	Contain both appropriate and inappropriate user-generated content like social networking or blogging sites. Also, sites in which the page content changes based how the user interacts with it (for example, an Internet search).
education	Represent schools or other educational facilities, faculty, or alumni groups.
energy	Represent companies involved with the production and distribution of energy.
enterprise-webmail	Provide online e-mail services.
entertainment	Relate to personal entertainment as well as the entertainment industry.

Table 10-213 Online Categories

Name	Sites that...
filesharing	Make files available for other users to download over the Internet or private networks.
finance-and-investing	Provide the opportunity to establish, plan, research, or manage personal finances and investments.
food-and-restaurants	Provide information about food, recipes, specialty food shops, catering, food delivery, and restaurants.
forums-and-messageboards	Provide a web application enabling users to participate in the discussion of numerous topics, often in conjunction with online communities.
freeware-and-shareware	Offer online software download.
gambling	Allow users to place bets or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing bets; receive instructions, assistance or training on participating in games of chance.
gaming	Sites related to computer or video games, game downloads, and online game sites.
glamour	Emphasize, promote, or provide information on how to achieve physical attractiveness, allure, charm, beauty, or style with respect to personal appearance.
gore	Display graphic violence and/or the infliction of pain or injuries. Gross violence towards humans or animals, such as scenes of dismemberment, torture, massive blood and gore, sadism, and other types of excessive violence.
government	Sites sponsored by government branches or agencies.
hacking	Promote or provide the means to practice illegal or unauthorized acts of computer crime using technology or computer-programming skills.
hate	Advocate hostility or aggression toward individuals or groups on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics; sites that denigrate others on the basis of those characteristics or justifies inequality on the basis of those characteristics; sites that purport to use scientific or other commonly accredited methods to justify said aggression, hostility, or denigration.
health	Provide information or advice on personal health or medical services, health insurance, procedures, or devices; sites that include information on diets, nutrition, therapies, and counseling services.
hobby	Provide information on private pastimes.
hosting	Provide individuals or organizations with online systems for storing images, video, or any content accessible via the Web.
internet-telephony	Enable users to make telephone calls via the Internet or obtain information or software for that purpose.
job-search	Provide assistance or tools to help to find employment.
kids	Provide a safe and interesting Internet experience for children under 12 years of age.
law	Offer legal content and services.

Table 10-213 Online Categories

Name	Sites that...
lifestyles	Contain general material relevant to sexual orientation.
mature-content	Contain sexually explicit information that is not of a medical or scientific nature.
military	Are sponsored by military branches or agencies as well as official and personal sites related to military history, ideology, or specific branches of the military.
mobile-entertainment	Offer a range of add-ons for handheld devices, such as ringtones, wallpapers, games, and videos.
music	Are related to the music industry.
news	Report, inform, or comment, on current events or contemporary issues of the day, including sports, weather, editorials, and human interest news.
non-profit	Are owned by non-profit organizations.
obscene	Contain obscene material.
occult	Promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, or supernatural beings.
online-backup-and-storage	Provide the ability to backup or upload data files to the Internet providing long term storage, access from other computers or locations, or the ability to share data files with other users.
peer-to-peer	Provide centralized peer-to-peer networks.
personals-and-dating	Promote or provide opportunity for establishing or continuing romantic relationships.
pets	Are related to the care, maintenance, purchase, rescue, or breeding of any animal for companionship and enjoyment.
photography	Are related to taking, sharing, printing, studying, or manipulating photos at all skill levels, whether casual, amateur or professional.
placeholder	Are owned by domain name registrars, domain brokers, or Internet advertising publishers. They usually display dynamically generated content with the intent to monetize on traffic through linked advertising listings.
plagiarism	Are primarily designed to allow students to cheat at school by taking the work or ideas of someone else and pass it off as their own.
politics	Are related to politicians, election campaigns, political organizations, and publications. Includes official homepages of politicians and political parties and personal sites about politics and grass-root movements.
pornography	Contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
portal	Offer a broad array of resources and services, such as email, forums, search engines, and on-line shopping malls.
real-estate	Are involved in the real estate business.
reference	Serve as a general resource to the public and feature factual information produced by authoritative and trusted sources.

Table 10-213 Online Categories

Name	Sites that...
religion	Are about religion or any set of beliefs and practices that have the function of addressing the fundamental questions of human identity, ethics, death, and the existence of the Divine.
remote-access	Offer software/services that allow a computer or portable device to remotely control or monitor another computer or device via the Internet or another network.
science	Provide research materials in the natural and life sciences.
search	Support searching the Internet, news groups, or indexes and directories.
self-harm	Describe or discuss ways in which to self harm including eating disorders and self-injury.
sexual-education	Provide educational information on reproduction and sexual development, sexually transmitted disease, contraception, safe sexual practices, sexuality, and sexual orientation
shopping	Provide the means to purchase products or services online.
sports	Promote or provide information about spectator sports.
streaming-media	Host streaming media like television, movies, video, radio, or other media.
suicide	Describe or promote suicide.
technology-and-telecommunication	Provide information pertaining to computers, the Internet, and telecommunication.
tobacco	Encourage, promote, offer for sale or otherwise encourage the consumption of tobacco.
tobacco kids	Include the promotion, glamorization, or encouragement of smoking that is aimed at children or that may have a significant appeal to children.
travel	Promote or provide opportunity for travel planning in a general sense, particularly finding and making travel reservations.
violence	Advocate or provide instructions for causing physical harm to people or property through use of weapons, explosives, pranks, or other types of violence.
virtual-community	Offer a variety of tools and mechanisms to enable a group of people to communicate and interact via the Internet.
weapons	Describe or offer for sale weapons including guns, ammunition, firearm accessories, knives, and martial arts.
webmail	Provide free, web-based email services, accessible through any Internet browser.
wedding	Are related to the traditions, customs, planning, and products involved in a marriage, commitment ceremony, or civil unions.
Note: *The following categories are for sites formatted for small format browsers like WML and xHTML:*	
wireless-business	Are sponsored by or devoted to individual businesses not covered by any other categories.
wireless-chat-sms	Offer users the ability to chat online.

Table 10-213 Online Categories

Name	Sites that...
wireless-dynamic	Contain both appropriate and inappropriate user-generated content like social networking or blogging sites. Also, sites in which the page content changes based how the user interacts with it (for example, an Internet search).
wireless-entertainment	Offer a range of add-ons for handheld devices, such as ringtones, wallpapers, games, and videos.
wireless-finance	Provide the opportunity to establish, plan, research, or manage personal finances.
wireless-gambling	Allow users to place bets or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing bets; receive instructions, assistance or training on participating in games of chance.
wireless-news	Primarily report, inform, or comment, on current events or contemporary issues of the day. Includes sports, weather, editorials, and human interest news.
wireless-personals-and-dating	Promote or provide opportunity for establishing or continuing romantic relationships.
wireless-pornography	Contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
wireless-sports	Promote or provide information about spectator sports.
wireless-travel	Promote or provide opportunity for travel planning in a general sense, particularly finding and making travel reservations.
unknown	Are unknown to the category database.

Content Filter Malware Category Group Filters

With content categorization configured, user requests can be categorized to one or more well-known malware categories:

- malware-attack-botnet – Sites associated with malware that causes a system to perform automated tasks over the Internet.
- malware-domain – Sites where the domain was found to either contain malware or take advantage of other exploits to deliver adware, spyware, or malware.
- malware-object – Sites that contain direct links to malware file downloads (such as . exe, .dll, .ocx, and others). These URLs are generally highly malicious.
- malware-spyware – Sites of domains associated with vendors and distributors of spyware, adware, greyware, and other potentially unwanted advertising software. Some may run exploits to facilitate the installation of this unwanted software.
- potential-malware-victim – Sites that click fraud and adware components use when “phoning home” that could signal a device is infected with spyware or adware. This category should be used only for reporting, not for blocking as the target URLs can be legitimate sites.

A set of the well-known malware categories can be grouped using the Malware Category Group configuration object. For each Malware Category Group, the Operator can define a filter with action block, terminate, redirect, or allow.

Content Filter IWF Category Filters

With content categorization configured, user requests can be categorized to a well-known Internet Watch Foundation category. The IWF category contains web sites hosting illegal child abuse images and content anywhere in the world.

The category is sourced from the list maintained by the Internet Watch Foundation at http://www.iwf.org.uk

For the IWF category, the Operator can define a filter with action block, terminate, redirect, or allow.

Content Filter Service

To add a Content Filter Service:

1. Expand **Services** in the tree.
2. Click **Content Filter**.
3. Configure the parameters as follows:
   - **Content Filter Commands** –
     - To trigger an update of the online categorization database, select **import** and click **Select**. Select the database and click **Execute**.
     - To purge the online categorization database, select **purge** and click **Select**. Select the categorization database and click **Execute**.
     - To categorize a URL using the online categorization database, select **categorize** and click **Select**. Enter the URL string and click **Execute**.
   - **Admin State** – Select the filter administrative state.
4. Click the **Save** icon.

Static Category Source

Category is used by a content filter *instance* to either allow (white list) or deny (black list) content requests to a specific list of domains or URLs.

To add a Category:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Expand **Category Source**.
4. Click **Static Category**.
5. Configure the parameters as follows:

Table 10-214 Static Category Parameters

Parameter	Description
Name	Category name
File Type	Address types in the file: ■ Domain ■ URL
File Name	Name of the category file

6. Click the **Save** icon.

To specify that the category be used by a content filter to either allow (white list) or deny (black list) content requests to a specific list of domains or URLs, see Content Filter Instance.

Content Categorization

Content Categorization uses online category databases to categorize content (URLs, received content) into one or more categories. The Content Filtering Service applies configured actions (block, terminate, allow, redirect) to user HTTP transactions based on the category determined.

To add a Content Categorization:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Click **Content Categorization**.

4 Configure the database parameters as follows:

Table 10-215 Content Categorization Parameters

Parameter	Description
Admin State	Select enabled to enable the service.
Customer ID	Customer identification string
Network Context	The Network Context to use when connecting to third-party server to update category databases
URL Categorization	Enable/Disable URL Categorization: ■ Enabled ■ Disabled
Malware Categorization	Enable/Disable Malware categorization: ■ Enabled ■ Disabled When enabled, the content filter categorizes requests to the categories: malware-all, malware-domain, malware-object, malware-spyware, malware-victim.
Phishing Categorization	Enable/Disable Phishing categorization: ■ Enabled ■ Disabled When enabled, the content filter categorizes requests to the phishing category.
IWF Categorization	Enable/Disable IWF child abuse categorization: ■ Enabled ■ Disabled When enabled, the content filter categorizes requests to the IWF child abuse category.
Real Time Categorization	Enable/Disable real-time categorization of web pages containing dynamic or unknown content: ■ Enabled ■ Disabled When enabled and a page with dynamic content (that is, search engine or social networking page) is accessed, the content filter categorizes the page using real-time categorization engine. When dynamic categorization is disabled, the content filter categorizes the page as a dynamic category. ***Note:*** *Enabling this option can impact performance.*
Categorization Log Level	Set the categorization log level.
Database Update Interval	Database update interval, in hours.

5 Click the **Save** icon.

6 Expand **Content Categorization**.

7 To configure a content filter using a list of online categories, click **Online Category Group**.

8 Configure the parameters as follows:

- **Name** – Enter an online category group name.

9 Click the **Save** icon.

10 Expand the Online Category Group you added.

11 Click **Online Category**.

12 Configure the parameters as follows:

- **Name** – Select an Online Category name.

For a list of Online Categories, see Table 10-213.

13 Click the **Save** icon.

14 To configure a content filter using a list of Malware categories, click **Malware Category Group**.

15 Configure the parameters as follows:

- **Name** – Enter an Malware category group name.

16 Click the **Save** icon.

17 Expand the Malware Category Group you added.

18 Click **Malware Category**.

19 Configure the parameters as follows:

Table 10-216 Malware Category Parameters

Parameter	Description
Name	Malware category name: malware-domain, malware-attack-botnet, malware-spyware, malware-object, potential-malware-victim

20 Click the **Save** icon.

Filter Database Size

MCC can block or allow traffic by comparing a URL received from the UE with a filter database.

Use this object to configure maximum filter entry sizes for different filter types.

To add Filter Database Sizes:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Click **Filter Database Size**.
4. Configure the database parameters as follows:

Table 10-217 Filter Database Size Parameters

Parameter	Description
URL List	Set the URL-based filter total entry size. This setting requires a slot reboot on the CSM and SSM.
Static Filter	Set the static filter-based filter total entry size (includes blacklist, whitelist, and static-category) This setting requires a slot reboot on the CSM.
Filter Hash List	Set the filter hash list-based filter total entry size. This setting requires a slot reboot on the CSM.

5. Click the **Save** icon.

Content Filter Import History

Use this object to view content filter import history.

To view content filter import history:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Expand **Category Database Import History**.
4. Click **all**.

Content filter import history parameters are:

- Server Import Time:
- Server Import Result: Success or error
- Server Import File Size:
- Number of Entries:

- Import Type: manual or scheduled

Content Database Summary

Use this object to view content database summary.

To view content database summary:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Expand **Category Database Summary**.
4. Click the database type you want to view or click **all**.

   Acuitas lists the category database Summary, including:

   - Database Name
   - Last Import Time
   - Last Import Result: Success or error
   - Last Import Type: manual or scheduled
   - Last Import Number
   - Last Import File Size (in KB)
   - Last Database Import Total Entries
   - Current Database Version
   - Number of Entries in Database
   - Next Scheduled Database Import Time

Black List

Black List is used by a *global* content filter to deny content requests to a specific list of domains or URLs.

To add a black list:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Expand **Global**.
4. Click **Blacklist File**.
5. Configure the parameters as follows:

Table 10-218 Black List Parameters

Parameter	Description
Name	Black List name

Table 10-218 Black List Parameters

Parameter	Description
File Type	Address types in the file: ■ Domain ■ URL
HTTPS Action	HTTPS service action on match: ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	Allows the configuration of the original requested URL as part of the redirect URL for content filter features. If an action is redirect, MCC responds to the UE with a configured redirection page URL. The redirection URL may contain the original URL (blocked URL) in the following format: **`http://213.14.227.50/landpage?ms=${ORIGINAL_URL}`**
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307

6 Click the **Save** icon.

White List

White List is used by a *global* content filter to allow content requests to a specific list of domains or URLs.

Note: *White list URLs and domains are accessible to all subscribers, regardless of any other filtering rules present in workflows.*

To add a white list:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Expand **Global**.
4. Click **Whitelist File**.
5. Configure the parameters as follows:

Table 10-219 White List Parameters

Parameter	Description
Name	White List name
File Type	Address types in the file: ■ Domain ■ URL

6. Click the **Save** icon.

Service Rule

Service Rule is used by a *global* content filter to deny content requests to a specific list of domains or URLs.

To add a service rule:

1. Expand **Services** in the tree.
2. Expand **Content Filter**.
3. Expand **Global**.
4. Click **Service Rule**.
5. Configure the parameters as follows:

Table 10-220 Black List Parameters

Parameter	Description
Name	Service rule name. The Service Rule must already exist. See Service Rule.
HTTPS Action	HTTPS service action on match: ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message

6 Click the **Save** icon.

Content Filter Instance

To add a Content Filter instance:

1 Expand **Services** in the tree.

2 Expand **Content Filter**.

3 Click **Instance**.

4 Configure the parameters as follows:

- **Name** – Enter a Content Filter name.
- **Global Content Filter** – Set to **enabled** if this Content Filter is a Global Content Filter Service. Set to **disabled** if this Content Filter is a Content Filtering Instance (non-global).

5 In **IWF Category**, configure the content filter for the IWF category:

Table 10-221 Category Parameters

Parameter	Description
Priority	IWF category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Allow ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307

6 In **Malware Category Group**, configure a content filter using a malware category group that takes effect only for the enabled Content Categorization in the Content Filter Instance. Configure the parameters as follows:

Table 10-222 Malware Category Parameters

Parameter	Description
Name	Malware category that specifies a list of domains or URLs. The malware category must already exist. See Content Categorization.

Table 10-222 Malware Category Parameters

Parameter	Description
Priority	Content category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Allow ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

To add additional Online Categories, click the **Create** icon.

7 In **Online Category Group**, configure a content filter using an online category group that takes effect only for the enabled Content Categorization in the Content Filter Instance. Configure the parameters as follows:

Table 10-223 Online Category Parameters

Parameter	Description
Name	Online category that specifies a list of domains or URLs. The online category must already exist. See Content Categorization.
Priority	Content category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Allow ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

To add additional Online Categories, click the **Create** icon.

8 In **Phishing Category**, configure the content filter for the Phishing category:

Table 10-224 Phishing Parameters

Parameter	Description
Priority	Phishing category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Allow ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307

9 In **Service Rule**, configure the parameters as follows:

Table 10-225 Service Rule Map Parameters

Parameter	Description
Name	Service Rule The Service Rule must already exist. See Service Rule. ***Note:*** *The Service Rule must contain an HTTP Rule Group.*

Table 10-225 Service Rule Map Parameters

Parameter	Description
Priority	Service Rule Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Allow ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL The following variables can be used as part of redirect URL: ■ $(IMEI) ■ $(MSISDN) ■ $(IMSI) ■ $(UEIPADDR) ■ $(TIMESTAMP) – milliseconds since Epoch ■ $(RANDOM) – 16 random octets ■ $(ORIGINALURL) ■ $(SHA256[]) - base64 encoded hash of information (different macros or plain text) inside the square brackets
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307

Table 10-225 Service Rule Map Parameters

Parameter	Description
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

To add additional Service Rules, click the **Create** icon.

10 In **Static Category**, configure the parameters as follows:

Table 10-226 Static Category Parameters

Parameter	Description
Name	Static category that specifies a list of domains or URLs. The Static category must already exist. See Static Category Source.
Priority	Static category Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Allow ■ Terminate ■ Block
Fields when Action is set to Block:	
Block Notification Message	HTTP Request Block Notification Message
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL

Table 10-226 Static Category Parameters

Parameter	Description
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

To add additional Static Categories, click the **Create** icon.

11 In **Filter Hash List**, configure a content filter using a Filter Hash List. Configure the parameters as follows:

Table 10-227 Filter Hash List Parameters

Parameter	Description
Name	Name of the Filter Hash List. The Filter Hash List already exist. See Filter Hash List.
Priority	Filter Hash List Priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
HTTPS Action	HTTPS service action on match: ■ Allow ■ Terminate ■ Block
HTTP Action	HTTP service action on match: ■ Allow ■ Terminate ■ Block ■ Redirect
QUIC Action	QUIC service action on match (for UDP flows): ■ Allow ■ Terminate ■ Block
Fields when Action is set to Block:	

Table 10-227 Filter Hash List Parameters

Parameter	Description
Block Notification Message	HTTP Request Block Notification Message to include in the 403 status code in the response body
Fields when Action is set to Redirect:	
Redirect URL	HTTP Request Redirect URL
Redirect Code	HTTP Request Redirect Code: ■ 301 ■ 302 ■ 307
Redirect Interval	Restricts the frequency of redirection during a defined period for a service rule. For example, if a service rule specifies a redirect to a URL, MCC caps the redirection at one during this specified redirect interval. Configure a Redirect Interval (in seconds) for which the action is applied only once.

To add Filter Hash Lists, click the **Create** icon.

12 In **Geo Redundant Group**, configure the parameters as follows:

- **Name** – Select the Geographic Redundancy Group to associate with the Content Filter.

  The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.

To add additional Geographic Redundancy Groups, click the **Create** icon.

13 In **Safe Search**, enable Safe Search filtering capability. Search engines such Bing, Google, and YouTube provide a safe-search filtering mechanism that acts as an automated filter of inappropriate content. When configured for a specific subscriber, the system enforces Safe Search even if an attempt is made to disable it from the UE. The system content filter supports the capability to enforce safe-search per search engine and per subscriber.

Configure the parameters as follows:

Table 10-228 Safe Search Parameters

Parameter	Description
Google	Enable/disable Google Safe Search filtering capability, which removes sites that contain inappropriate content from search results: ■ Enabled ■ Disabled

Table 10-228 Safe Search Parameters

Parameter	Description
Bing	Enable/disable Bing Safe Search filtering capability, which removes sites that contain inappropriate content from search results: ■ Enabled ■ Disabled
Youtube	Enable/disable YouTube Safe Search filtering capability, which removes sites that contain inappropriate content from search results: ■ Enabled ■ Disabled
Service Rule	Configure Safe Search using a Service Rule. The Service Rule must already exist. See Service Rule.

14 In **Protocol Filtering**, enable this filter instance for different protocols:

- **HTTP** – Select enabled to enable this filter for HTTP protocol service.
- **HTTPS** – Select enabled to enable this filter for HTTPS protocol service.
- **QUIC** – Select enabled to enable this filter for QUIC protocol service.

15 Click the **Save** icon.

CRBN Profile

Use this object to configure a Changing Rule Base Name profile to specify the CRBN names that can be received from the PCRF. In this case, the Charging-Rule-Base-Name AVP corresponds to the locally configured CRBN Profile. When the CRBN Profile is enabled, multiple CRBN names can be received in the same PCRF message, all of which will be applied to the subscriber.

This feature allows for multiple predefined groups of PCC rules to be activated/deactivated on an MCC gateway using the Charging-Rule-Base Name AVP within the Charing-Rule-Install/Charging-Rule-Remove AVP sent via the Gx interface.

When Charging-Rule-Base-Name (CRBN) profile names are received in the Charging-Rule-Base Name AVP from the PCRF, the GGSN/PGW checks the CRBN Profile configuration and matches the name. If a matching profile configuration is found, all the Rating Groups and Service Rules inside the related Charging Instance are activated.

Note the following guidelines:

- All Rating Groups and Service Rules associated with a CRBN Profile should have the **Service Activation** parameter set to **always on**.
- The QoS Flow associated with CRBN Profile should have the **Bearer Control** parameter configured as **Default Bearer**.
- There should be only one Billing Plan under the Charging Instance associated with the CRBN Profile, and it must have wildcard charging characteristics.
- If the same Service Rule is part of multiple CRBN Profiles, the Service Rule is deactivated only after all the CRBN Profiles referring to it are deactivated.
- A static Service Rule that is activated as part of a CRBN Profile *is not* deactivated when the CRBN Profile referring to it is deactivated.

When the PCRF requests usage monitoring, the MCC gateway compares the metering instance received in the Monitoring-Key AVP (included within the Usage-Monitoring-Information (UMI) AVP) with all the rating groups configured under the metering instance associated with active CRBN profiles.

If a matching metering instance is found under an active CRBN profile, the MCC gateway activates usage monitoring services accordingly:

- Monitors all the rating groups configured under the metering instance of an active CRBN profile with the **Service Activation** set to **external activation**.
- Monitors all the service rules configured under the metering rating groups with the **Service Activation** set to **always on**. The service rules configured under the metering rating groups with the **Service Activation** set to **external activation** are monitored only when they are part of the CRBN service rule list.

To add a CRBN profile:

1 Expand **Services** in the tree.

2 Click **CRBN profile**.

3 Configure the parameters as follows:

Table 10-229 CRBN Profile Parameters

Parameter	Description
Name	CRBN profile name
Charging Instance	Charging Instance associated with this CRBN Profile. The Charging instance must already exist. See Charging: Charging Instance.
QoS Policy	QoS Policy associated with this CRBN Profile. The QoS Policy must already exist. See QoS Policy.
Metering	Metering service instance associated with this CRBN Profile. The Metering service instance must already exist. See Metering Service.
Multi Protocol Proxy	Multi Protocol Proxy instance associated with this CRBN Profile. The Multi Protocol Proxy instance must already exist. See Multi Protocol Proxy Instance.
Content Filter	Content Filter instance associated with this CRBN Profile. The Content Filter instance must already exist. See Content Filter Instance.

4 Click the **Save** icon.

5 To specify a CRBN service rule list, expand the CRBN Profile you added.

6 Click **Service Rule**.

7 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the CRBN service rule list.

  The Service Rule must already exist. See Service Rule.

  The Service Rules in the CRBN list must be linked with a Rating Group associated with the same CRBN profile and they must have the **Service Activation** set to **external activation**. You can configure a maximum of 128 service rules in the CRBN service rule list.

8 Click the **Save** icon.

DNS Proxy

Use this object to configure a DNS proxy and caching service.

The DNS caching service is used to reduce the amount of DNS message traffic towards an Operator's DNS servers. When enabled, the DNS caching service caches DNS response traffic, allowing subsequent DNS lookup requests for the same domains to be served locally from the DNS cache. Separate caches are maintained per network context, and the DNS caching service observes the time-to-live (TTL) contained in each DNS response to age out individual cache entries.

Additional cache-control configuration parameters allow the Operator to:

- Enable/disable the entire DNS cache
- Enable/disable the caching of DNS response data on a per-DNS server basis
- Override the TTL values that are used to age DNS cache entries

The DNS caching service also supports a configurable static host mapping table, allowing Operators to associate up to five IP addresses to a domain name. This configuration table is loaded into the DNS cache, and any request for a domain that is statically mapped is served directly by the MCC without any further exchange with an Operator's DNS servers. Each static mapping table can also be associated with a network context, allowing different IP addresses to be returned, based on the network context in which a UE resides.

To add a DNS Proxy service:

1. Expand **Services** in the tree.
2. Click **DNS Proxy**.
3. Configure the parameters as follows:

Table 10-230 DNS Proxy Parameters

Parameter	Description
Admin State	DNS Proxy administrative state: ■ enabled ■ disabled
Pending Request Timeout	Time in seconds to retain pending DNS request cache entries.
Max Cache Entries	Maximum number of cache entries for each DNS cache.
Positive Response TTL Override	TTL Override in seconds for caching positive DNS responses.
Negative Response TTL Override	TTL Override in seconds for caching negative DNS responses.
Static Map Entry TTL	TTL to return in any response for a static DNS entry.

4 Click the **Save** icon.

DNS IP Flow

Configure one or more DNS IP Flows to be processed by DNS Proxy.

To add a DNS IP Flow:

1 Expand **Services** in the tree.

2 Expand **DNS Proxy**.

3 Click **DNS IP Flow**.

4 Configure the parameters as follows:

Table 10-231 DNS IP Flow Parameters

Parameter	Description
Name	DNS IP Flow name
Admin State	Enable/Disable DNS IP Flow: ■ disabled ■ enabled
Priority	DNS IP Flow priority
Tunnel Detection Profile	DNS tunnel detection profile associated with this proxy instance. The Tunnel Detection Profile must already exist. See Tunnel Detection Profile.
DNS Policy	Select the DNS Policies to associate with the DNS IP flow. The DNS Policy must already exist. See DNS Policy. To add additional DNS Policies, click the **Create** icon.
Service Rule	Select the Service Rule to associate with the DNS IP flow. The Service Rule must already exist. See Service Rule. To add additional Service Rules, click the **Create** icon.

5 Click the **Save** icon.

DNS Policy

DNS Proxy supports the DNS whitelisting capability. This feature allows Operators to only allow DNS queries to trusted DNS servers. This feature prevents any DNS fraud where the user may have configured the IP address of a rogue DNS server.

To add a DNS Policy:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Click **DNS Policy**.
4. Configure the parameters as follows:

Table 10-232 DNS Policy Parameters

Parameter	Description
Name	DNS policy name
Admin State	Enable/Disable DNS policy: ■ disabled ■ enabled
Priority	DNS policy priority
Cache Control	DNS response cache control action for this policy: ■ cache-all ■ cache-none
Action	DNS request action for this policy: ■ allow ■ block ■ redirect The action dictates how the DNS server handles DNS requests. Configuration guidelines for each action are outlined in Table 10-233.
Redirect IP List	Select the DNS Redirect IP list. ***Note:*** *The IP list must not use IP address ranges.* The IP list must already exist. See IP List.

5. Click the **Save** icon.

Table 10-233 Configuration Guidelines for Policy Action

Action	DNS Server Response	Configuration Guidelines
allow	Allow DNS queries to Operator-hosted DNS servers (designated DNS servers in the network) Allow DNS queries to other trusted DNS servers (for example Google DNS)	**1** Configure a set of service-construct packet-filter objects for all Operator-hosted and other trusted DNS servers. **2** Configure services dns-proxy dns-ip-flow and associate it with the packet-filter for the trusted DNS servers. **3** Optionally, associate the dns-ip-flow with a dns-policy with action set to **`allow`** (default). The DNS-proxy based on the configuration above matches the DNS query with one of the packet-filters and the dns-ip-flow. Since the dns-ip-flow has a dns-policy with action set to **`allow`**, the dns packet is forwarded unaltered to the trusted DNS server.
block	Block DNS queries to untrusted DNS servers	**1** Configure a catch-all service-construct packet-filter object for all other (untrusted) DNS servers. **2** Configure services dns-proxy dns-ip-flow with a lower priority and associate it with the packet-filter for the untrusted DNS servers. **3** Associate the dns-ip-flow with a dns-policy with action set to **`block`**.
redirect	Redirect DNS queries to untrusted DNS servers to a set of designated DNS servers	**1** Configure a catch-all service-construct packet-filter object for all other (untrusted) DNS servers. **2** Configure services dns-proxy dns-ip-flow” with a lower priority and associate it with the packet-filter for the untrusted DNS servers. **3** Associate the dns-ip-flow with a dns-policy with action set to **`redirect`**. **4** Set the dns-policy redirect-ip-list to refer to a service-construct ip-list containing a list of IP addresses of trusted DNS servers.

DNS Reverse Cache

DNS reverse cache is a database to look up an IP address (IPv4 or IPv6) and return a list of host names that resolve to that IP address. This database is generated with information extracted from DNS responses by the DNS proxy. DNS reverse cache supports two modes:

- If the number of Domain Rule Groups is large and Regular Expression is expensive, all DNS responses are reverse cached.
- If the number of Domain Rule Groups is small and Regular Expression matching is relatively less expensive, only the Regular Expression matching DNS responses are reverse cached.

DNS reverse cache is used by a Domain Rule Group. See Domain Rule Group.

To add a DNS Reverse Cache:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Click **DNS Reverse Cache**.
4. Configure the parameters as follows:

Table 10-234 DNS Reverse Cache Parameters

Parameter	Description
Admin State	Enable/Disable DNS Reverse Cache: ■ disabled ■ enabled
Domain Rule Group Filtering	Enable/Disable Domain Rule Group filtering: ■ disabled ■ enabled
Max Cache Entries	Maximum number of reverse cache entries for each DNS cache.
Cache Full Alarm Threshold	Percent of the cache size that, when full, signals an alarm.
TTL Override	In Type, specify the a TTL override type: ■ add: Specify the value to add. ■ multiply-by: Specify the value to multiple by. ■ set: Specify the value to set.

5. Click the **Save** icon.

DNS Proxy Instance

To add a DNS Proxy Instance:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Click **Instance**.
4. Configure the parameters as follows:

Table 10-235 DNS Proxy Instance Parameters

Parameter	Description
Name	DNS Proxy Instance name
Admin State	Enable/Disable DNS Proxy instance: ■ disabled ■ enabled
DNS IP Flow	Select the DNS IP Flow(s) The DNS IP Flow must already exist. See DNS IP Flow. To add additional DNS IP Flows, click the **Create** icon.

5. Click the **Save** icon.

Cache Display

Use this object to view cache data.

To view cache data:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Expand **Cache**.
4. Click an instance.

Cache display parameters are:

- Node ID from which to display cache data
- Network Context name associated with this DNS cache
- Network Context ID
- Current number of entries in this DNS cache

Cache Statistics

Use this object to view DNS proxy cache statistics.

To view DNS Proxy cache statistics:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Expand **Cache Stats**.
4. Click an instance.

Cache statistics are:

- Node ID from which to gather module statistics
- Network Context name associated with this DNS cache
- Network Context ID
- Total number of DNS results added to the cache
- Total number of DNS results deleted from the cache
- Total number of DNS cache hits
- Total number of DNS cache misses

Module Statistics

Use this object to view DNS proxy module statistics.

To view DNS Proxy module statistics:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Expand **Module Stats**.
4. Click an instance.

Module statistics are:

- Node ID from which to gather module statistics
- Total number of DNS packets that have been processed
- Total number of upstream DNS packets that have been processed
- Total number of downstream DNS packets that have been processed
- Total number of DNS packets that have been ignored
- Total number of DNS requests that have been allowed
- Total number of DNS requests that have been blocked
- Total number of DNS requests that have been redirected
- Total number of DNS requests that have been examined by tunnel detection

- Total number of DNS requests that have been blocked by tunnel detection
- Total number of DNS internal errors
- Current number of domains blocked by tunnel detection

Domain Clean Time

Use this object to configure global blocking domain clean time for DNS tunnel detection.

To add a Domain Clean Time:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Click **Domain Clean Time**.
4. Configure the parameters as follows:

Table 10-236 Domain Clean Time Parameters

Parameter	Description
DNS Tunnel Age Time	Inactive blocking domain age time for DNS tunnel detection
DNS Tunnel Age Time Units	Age time units: ■ seconds ■ minutes ■ hours ■ days

5. Click the **Save** icon.

Tunnel Detection Profile

Use this object to detect and block DNS tunneling transactions and receive notification of those actions. These settings reduce the possibility of DNS packets being sent to a fraud domain.

To add a Tunnel Detection Profile:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Click **Tunnel Detection Profile**.
4. Configure the parameters as follows:

Table 10-237 Tunnel Detection Profile Parameters

Parameter	Description
Admin State	Tunnel Detection administrative state: ■ enabled ■ disabled
Domain Cache Size	Number of the recent domains to monitor
Refresh Rate	Refresh rate for monitor interval, in seconds
Domain Penalty Time	Penalty time for blocked domain, in seconds
Clean Time	Time to turn off detail monitoring after the total hit is under threshold and there is no blocked domain, in seconds
Single Domain Threshold	Threshold for hitting rate of one singe domain in detail monitoring mode
Total DNS Hit Threshold	Threshold for overall DNS traffic rate to turn on detail monitoring mode

5. Click the **Save** icon.

Tunnel Blocked Domain

Use this object to view domains blocked by DNS tunnel detection.

To view tunnel blocked display:

1. Expand **Services** in the tree.
2. Expand **DNS Proxy**.
3. Click **Tunnel Blocked Domain**.
4. Click an instance.

Fair Bandwidth Usage

Fair Bandwidth Usage Management is a category of services aimed at normalizing bandwidth use when monthly subscription levels are breached. Typically, when monthly volumes are breached, the user is rate limited at a throughput defined by the carrier until the end of the subscription period. At the beginning of a new subscription period, the service is restored to the subscribed throughput rate.

To add a Fair Bandwidth Usage:

1. Expand **Services** in the tree.
2. Expand **Affirmed Apps**.
3. Click **Fair Bandwidth Usage Service Profile**.
4. Configure the parameters as follows:

Table 10-238 Fair Bandwidth Usage Parameters

Parameter	Description
Name	Fair Bandwidth Usage name
Measurement Units	Measurement unit: ■ kB ■ mB ■ gB
Reset Interval	Reset timeout interval that triggers fallback to default parameters
Minor Volume Threshold	The usage threshold at which to transition the session to utilize the **Minor QOS Profile Id**.
Minor QoS Profile Id	The Minor QoS Profile to use when the **Minor Volume Threshold** is reached. The QoS Profile must already exist. See Quality of Service.

5. Click the **Save** icon.

Health Check

Use this object to configure a health check of external systems.

To add a Health Check:

1. Expand **Services** in the tree.
2. Click **Health Check**.
3. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable the Health Check.
4. Click the **Save** icon.

Statistics

Use this object to view the Health Check statistics.

To view Health Check Statistics:

1. Expand **Services** in the tree.
2. Expand **Health Check**.
3. Expand **Statistics**.
4. Expand **Cluster Level**.
5. Expand **Summary**.
6. Click an instance.

Server Plugin statistics are:

- Parent — Parent Health Check Destination
- Destination — Health Check Destination
- Network Context — Network Context of Destination
- Current State — Current State of the Destination
- Successes— Number of Successes
- Failures — Number of Failures
- Details — State Detail if applicable

HTTP Proxy (MCC versions prior to 8.4)

Acuitas does not support this object for MCC 8.4 and later releases. It has been replaced by Multi Protocol Proxy. See Protocol Application Rule Group (8.4 and later MCC version).

HTTP Proxy acts as an intermediary for requests from clients seeking resources from other servers. The HTTP Proxy is an intercepting forward proxy that acts like the server to the UE and acts like a client to the origin server.

The HTTP Proxy function supports:

- Separate Request Policy and Response Policy to allow the Operator to specify the actions separately for request phase and response phase.
- Request Policy to notify the origin servers of the private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
- On-the-fly HTTP compression for supported client requests or all client requests.
- Setting the global compression level.
- Fraud Detection handling – HTTP Proxy performs DNS validation and Header consistency checks to determine if a request is destined for a legitimate domain or destined for a rogue proxy. If the destination IP address is not within the defined range or domain returned by the DNS lookup, the system determines if a free browsing proxy is in use and enforces a specified action (allow the traffic and charge for it and/or reduce its QoS to a specified level).
- HTTP Proxy latency – HTTP Proxy forwards HTTP request and response data as soon as possible. Fragments of request/response body are received, processed, and immediately streamed, ensuring low forwarding latencies. Typical request and response forwarding latency is within several tens of milliseconds.

  However, the HTTP Proxy transaction latency may increase when:

  – Client or server socket back-pressure due to network congestion, QoS bandwidth, or burst limits.
  – Optimization features are applied (such as compression, minification, web image optimization, preemptive, DNS, and so on).
  – Request store-and-forward-limit option is used (applies to requests using the option. The added latency depends on the request size and client uplink speed).
  – Response buffering-limit option is used (applies to responses using the option. The added latency depends on response size and client downlink speed).
  – Large objects are served from disk cache on a system with rotational media.
  – Back-End Forwarding is enabled in the system.

The HTTP Proxy service retrieves the following VSAs from the PCRF via the Gx interface and distributes these VSAs to the HTTP Proxy. MCC uses these VSAs to customize HTTP Proxy services for a particular subscriber.

- VsaEntitlement – Indicates the type of service to which the subscriber is entitled.
- VsaPaymentType – Indicates subscriber payment type. Possible values include:
  - PO – Postpaid subscriber.
  - PR – Prepaid subscriber.
  - SL
- VsaSubId – Indicates the subscriber ID.
- VsaHttpPolicy – Customize HTTP Proxy services. Possible values include:
  - NOPRXY – HTTP Proxy is disabled for the subscriber.
  - NOGZIP – Gzip compression is disabled for the subscriber.
  - NOTFD – No Toll Free Data (TFD).
  - NOVIDEO – Video optimization is disabled for the subscriber.
- VsaResellerId – Indicates the subscriber's reseller ID.
- VsaMiDial – Indicates whether the subscriber opted out from Long Term Mobile ID (LTMI) header enrichment or opted for static trusted ID in LTMI header enrichment.

Service VSAs received by the PGW are listed in Subscriber > PDN Session.

The HTTP Proxy service allows users to load unoptimized content using shortcut keys from web browsers. The shortcut keys trigger a no-cache HTTP request header to disable the following HTTP optimization features:

- DNS Preemption
- Minification
- Web image optimization
- Zip compression
- Video adaptation online transcoding

Table 10-239 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
F5	All	Refreshes a page with If-Modified-Since header, but no no-cache header

Table 10-239 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
<Ctrl>F5	Internet Explorer10 Chrome Firefox	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>F5	Chrome	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>Reload	Safari	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache

HTTP Proxy Service

To add an HTTP Proxy Service:

1 Expand **Services** in the tree.

2 Click **HTTP Proxy**.

3 Configure the parameters as follows:

Table 10-240 HTTP Proxy Parameters

Parameter	Description
Admin State	HTTP Proxy administrative state: ■ enabled ■ disabled
Client Idle Timeout	Client idle timeout, in seconds
Compress Level	Global compression level: ■ default-compression ■ best-compression ■ best-speed
Static DNS Map	Static DNS map to use to avoid doing DNS lookup through configured DNS server(s). The HTTP Proxy service uses the map's IP Address list to open server connections for HTTP request. The Static DNS map must already exist. See Static DNS Map.

4 Click the **Save** icon.

HTTP Request Policy

To add an HTTP Request Policy:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **HTTP Request Policy**.
4. Configure the parameters as follows:

Table 10-241 HTTP Request Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
HTTP Protocol	Protocol used towards origin server: ■ ue-http-protocol: preserves original UE protocol ■ http ■ https
Steering Group	Steering Group to use for the HTTP requests. The Steering Group must already exist. See Steering Group.
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for server connections. The Loopback IP List must already exist. See Loopback IP List.
Store Forward Buffer Limit	Maximum data to store before forwarding request to server, in KB. When the HTTP Request Policy is applied, the server connection is not opened until the received request buffer size reaches this value or entire request is received. If zero, request is immediately forwarded.
Bypass HTTP Proxy	Specifies whether to bypass HTTP proxy for this policy: ■ disabled ■ enabled When enabled, the request is TCP spliced.
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds the specified HTTP headers/cookies to the HTTP request header. The Header Enrichment Profile must already exist. See HTTP Header Enrichment.

Table 10-241 HTTP Request Policy Parameters

Parameter	Description
Content Insertion Profile	Select the Content Insertion Profile. The Content Insertion Profile must already exist. See Content Insertion Profile.
URL Rewrite Profile	Select the HTTP URL Rewrite profile. The HTTP URL Rewrite profile must already exist. See HTTP URL Rewrite.
DNS Resolution	Specify whether to use DNS resolution to look up destination.
Forced Cache Access Notification	Enable/Disable Forced Cache Object Access Notification to the origin server: ■ disabled ■ enabled When enabled, HTTP request policy notifies the origin servers of private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
Compress Force	Specify whether to force on-the-fly HTTP compression for all client requests.
Compress Inline	Specify whether to enable on-the-fly HTTP compression for supported client requests.
Preemptive DNS	Specify whether to apply HTTP Proxy service level preemptive DNS for this policy: ■ enabled ■ disabled
Compress Min Size	Minimum response size in bytes required for compression to take effect
Web Image Optimization	Select the Web Image Optimization to use for HTTP requests. The Web Image Optimization must already exist. See Web Image Optimization Profile.
Server TCP Optimization Profile	Select the TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.

5 In **Compression**, configure the parameters as follows:

- **Compress Max Size** – Enter the maximum response size in bytes allowed for compression to take effect.

6 In **Minify**, configure the parameters as follows:

Table 10-242 Minify Parameters

Parameter	Description
Minify Javascript	Mark the checkbox to minify JavaScript (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify HTML	Mark the checkbox to minify HTML (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify Min Size	The minimum response size in bytes required for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Max Size	The maximum response size in bytes allowed for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Css Choice	Select minify-css to minify CSS (to remove unnecessary characters such as blank characters and new line characters from source code)

7 In **Service Rule**, configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the HTTP Request Policy.

  The Service Rule must already exist. See Service Rule.

  The Service Rule must contain an HTTP Rule Group.

To add additional Service Rules, click the **Create** icon.

HTTP Response Policy

To add an HTTP Response Policy:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **HTTP Response Policy**.

4 Click the **Create** icon.

5 Configure the parameters as follows:

Table 10-243 HTTP Response Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds the specified HTTP headers/cookies to the HTTP response header. The Header Enrichment Profile must already exist. See HTTP Header Enrichment.
Video Pacing Burst Time	Video Pacing burst time, in seconds. Represents the time for which the video data should be sent at a burst.
Video Pacing Factor	Video Pacing factor (scale factor 1/100) at which the video should be paced. Set to zero to disable pacing. For example, setting a Video Pacing Burst Time of 20s and a Video Pacing Factor of 100 specifies to send the initial 20 seconds of video at the maximum possible rate and to pace the video by a factor of 100 (that is, 1* bit-rate of the video).
Rate Limiting Burst Size	Rate limiting burst size, in bytes
Rate Limiting Bit Rate	Rate limiting bit rate, in bps
Buffering Limit	Maximum data to store when processing response from origin server, in KB. When the HTTP Response Policy is applied, HTTP Proxy uses this value to determine the biggest response data size to be stored while sending the response to client. When the limit is reached, HTTP Proxy stops reading from the server socket until space is freed after some data sent to client.

6 Click the **Save** icon.

7 Expand **HTTP Response Policy**.

8 Expand the HTTP Response Policy you added.

9 Click **Service Rule**.

10 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the HTTP Response Policy.

  The Service Rule must already exist. See Service Rule.

  The Service Rule must contain an HTTP Rule Group.

11 Click the **Save** icon.

12 Repeat step 9 through step 11 to add as many Service Rules as needed.

HTTP IP Flow

Configure one or more HTTP IP Flows to be processed by HTTP Proxy.

To steer traffic destined to an explicit proxy address, configured the HTTP IP Flow with a Service Rule containing a Packet Filter with matching destination IP and destination port values.

To add an HTTP Proxy IP Flow:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **HTTP IP Flow**.

4 Configure the parameters as follows:

Table 10-244 HTTP Proxy IP Flow Parameters

Parameter	Description
Name	HTTP Proxy IP Flow name
Admin State	Enable/Disable HTTP Proxy IP Flow: ■ disabled ■ enabled
Priority	HTTP Proxy IP Flow priority

Table 10-244 HTTP Proxy IP Flow Parameters

Parameter	Description
Protocol	HTTP transport protocol for the IP Flow: ■ HTTP ■ HTTPS ■ TCP ■ UDP TCP splicing provides the ability to enable TCP optimization for TCP-based protocols such as SFTP, FTP and HTTPS. The TCP splicing stitches the client and server TCP connections, enabling the Operator to configure the TCP parameters to be used for the client connections separately. MCC can be configured as a TCP splicing and support the following: ■ Terminate a TCP connection from the client and apply a set of TCP optimization parameters. ■ Originate a TCP connection to the server and apply a set of TCP optimization parameters. ■ Forward TCP traffic between the client and server TCP connections without parsing or disturbing the packets. ■ Teardown the TCP connections when the peer closes the sockets or idle exceeded timeou.t
IP Transparency	Enable/Disable IP Transparency for the IP Flow: ■ disabled ■ enabled When IP Transparency is enabled, HTTP requests forwarded by the HTTP Proxy to origin servers contain the UE's original IP address as the source TCP/IP address in the IP packet. IP transparent proxy is an HTTP proxy mode of operation where HTTP client IP addresses (UE addresses) are used as a source when originating network-side connections to Web origin servers. HTTP proxy, using the client addresses, hides its own network identity and becomes IP transparent to Internet origin servers. When IP transparency is used, origin servers are able to determine the identity of Web clients based on the source IP addresses of the HTTP/HTTPS connections. In non-IP Transparent mode, HTTP proxy uses MCC IP loopback addresses when originating network-side connections.
HTTP Request Policy	Select the HTTP Request Policies to bind to the IP flow. The HTTP Request Policy must already exist. See HTTP Request Policy. To add additional HTTP Request Policies, click the **Create** icon.

Table 10-244 HTTP Proxy IP Flow Parameters

Parameter	Description
HTTP Response Policy	Select the HTTP Response Policies to bind to the IP flow. The HTTP Response Policy must already exist. See HTTP Response Policy. To add additional HTTP Response Policies, click the **Create** icon.
Service Rule	Select the Service Rule The Service Rule must already exist. See Service Rule. ***Note:*** *The Service Rule cannot contain an HTTP Rule Group.* To add additional Service Rules, click the **Create** icon.
TCP Splicing Policy	Select the TCP Splicing Policy The TCP Splicing Policy must already exist. See TCP Splicing Policy. To add additional TCP Splicing Policies, click the **Create** icon.
UDP Policy	Select the UDP Policy The UDP Policy must already exist. See UDP Policy. To add additional UDP Policies, click the **Create** icon.

5 Click the **Save** icon.

HTTP Proxy Instance

To add an HTTP Proxy Instance:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **Instance**.

4 Configure the parameters as follows:

Table 10-245 HTTP Proxy Instance Parameters

Parameter	Description
Name	HTTP Proxy Instance name
Admin State	Enable/Disable HTTP Proxy instance: ■ disabled ■ enabled

Table 10-245 HTTP Proxy Instance Parameters

Parameter	Description
TCP Optimization Service	Select the TCP optimization service The TCP optimization service must already exist. See TCP Optimization Profile.
Encryption Profile	Select the Encryption Profile The Encryption Profile must already exist. See Encryption Profile.
MMSC Group	Select the Multimedia Messaging Service Center group. The MMSC group must already exist. See Multimedia Messaging Service Center Group.
SMSC Group	Select the Short Message Service group. The SMSC group must already exist. See Short Message Service Center Group.
LDAP Profile	Select the LDAP Profile. The LDAP Profile must already exist. See LDAP Profile.
UA Profile	Select the User Agent Profile. The UA Profile must already exist. See UA Profile.
Fraud Detection Profile	Select the Fraud Detection Profile. The Fraud Detection Profile must already exist. See Fraud Detection Profile.
Explicit Proxy Profile	Select the Explicit Proxy Profile. The Explicit Proxy Profile must already exist. See Explicit Proxy Profile.
ABR Opting Mode	Specifies the ABR opting modes for the subscriber: ■ opt-out – HTTP/HTTPS/QUIC ABR video rate limiting is applied unless the NOABR string is received in the acwhttppolicy Vendor-Specific Attribute (VSA) from the PCRF Gx interface. ■ opt-in – HTTP/HTTPS/QUIC ABR video rate limiting is not applied unless the ABR string is received in the acwhttppolicy Vendor-Specific Attribute (VSA) from the PCRF Gx interface.
HTTPS Profile	Select the HTTPS Profile. The HTTPS Profile must already exist. See HTTPS Profile.
TCP Traffic Control Profile	Select the TCP Traffic Control Profile. The Traffic Control Profile must already exist. See Traffic Control Profile.

Table 10-245 HTTP Proxy Instance Parameters

Parameter	Description
HTTP Transaction Record Profile	Select the HTTP Transaction Record Profile The HTTP Transaction Record Profile must already exist. See HTTP Transaction Record Profile.
Toll Free Profile	Select the Toll Free Profile The Toll Free Profile must already exist. See Toll Free Profile.
ABR Optimization Profile	Select the ABR Optimization Profile The ABR Optimization Profile must already exist. See ABR Optimization Profile.
UDP Traffic Control Profile	Select the UDP Traffic Control Profile. The Traffic Control Profile must already exist. See Traffic Control Profile.
TCP Measurement:	
Admin State	Enable/Disable TCP measurement: ■ disabled ■ enabled - MCC calculates the TCP performance parameters for the specified sampling frequency for both uplink and downlink connections
Sampling Interval	TCP measurement sampling interval, in milliseconds
Mild Congestion Level	Mild congestion level for applying optimization (throughput in kbps)
Moderate Congestion Level	Moderate congestion level for applying optimization (throughput in kbps)
Severe Congestion Level	Severe congestion level for applying optimization (throughput in kbps)
Server Connections:	
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by the gateway subsystem.
TCP Optimization Profile	TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.
Loopback IP List	Loopback IP List for server connections. The Loopback IP List must already exist. See Loopback IP List.

Table 10-245 HTTP Proxy Instance Parameters

Parameter	Description
Loopback Selection Algorithm	Specifies the loopback selection algorithm: ■ round-robin – HTTP Proxy selects a loopback IP from a Loopback IP List in a round-robin fashion for connections initiated to HTTP origin servers ■ session sticky – HTTP Proxy uses the same loopback IP for all connections for a given session
IP Family Preference	Specifies the preferred server connection IP family: ■ IPv4 – HTTP proxy requests both IPv4 and IPv6 server addresses and uses the IPv4 address unless it is unavailable. ■ IPv6 – HTTP proxy requests both IPv4 and IPv6 server addresses and uses the IPv6 address unless it is unavailable. ■ client-ip-family – HTTP proxy requests both IPv4 and IPv6 server addresses and uses the client-ip-family address unless it is unavailable.
HTTP IP Flow	Select the HTTP IP Flow(s) The HTTP IP Flow must already exist. See HTTP IP Flow. To add additional HTTP IP Flows, click the **Create** icon.

5 Click the **Save** icon.

ABR Optimization Profile

Use this object to configure an ABR rate limiting optimization profile.

To add an ABR Optimization Profile:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **ABR Optimization Profile**.

4 Configure the parameters as follows:

Table 10-246 ABR Optimization Profile Parameters

Parameter	Description
Name	Optimization Profile name
Admin State	Enable/Disable the Profile: ■ disabled ■ enabled
Burst Size	Rate limiting burst size

Table 10-246 ABR Optimization Profile Parameters

Parameter	Description
Burst Size Unit	Burst size unit : ■ bytes ■ kbytes ■ mbytes ■ gbytes
Secondary Segment Threshold	Minimum segment threshold for bypassing secondary rate-limiting
Secondary Segment Threshold Unit	Secondary segment threshold unit: ■ bytes ■ kbytes ■ mbytes
Bitrate	Rate limiting bitrate
Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Secondary Segment Bitrate	Rate limiting bitrate (bits per second) for secondary segments.
Secondary Segment Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Savings Estimation Admin State	Enable/Disable estimation of optimization byte savings attributed to ABR pacing. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on content: ■ disabled ■ enabled
Sampling Interval	Sampling interval for savings estimation
Sampling Interval Unit	Sampling interval unit: ■ min ■ hr

5 Click the **Save** icon.

Client Connections

Use this object to configure HTTP Proxy client connection parameters.

To configure client connections:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Client Connections**.
4. Configure the parameters as follows:

   Request Wait Time – Configure the client connection HTTP request wait time in milliseconds (value 0 indicates forever). Reverse hand-off is implemented and if the HTTP request is found, it is handed back to the HTTP proxy and continues to process as HTTP traffic.

5. Click the **Save** icon.

Back End Forwarding

Use this object to enable forwarding of HTTP requests between CSM modules. Back end forwarding uses content cache in a distributed mode to achieve better cache hit rates.

To enable/disable back end forwarding:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Back End Forwarding**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable back end forwarding.
   - **Max Idle Connections** – Configure the maximum number of idle connections per back end proxy.
5. Click the **Save** icon.

Encryption Profile

The Encryption Profile is used in HHE to determine the algorithm and keys to be used for header encryption.

The Encryption Profile stores encryption algorithm information and keys depending on the algorithm configured by the Operator. MCC generates a random IV and includes this as an extra header in each encrypted header. MCC supports a key in hex format (without spaces).

MCC supports the AES-128/192/256-CBC encryption algorithm and Base64 and Hex encoding for the encrypted value.

To add an Encryption Profile:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click Encryption **Profile**.
4. Configure the parameters as follows:

Table 10-247 Encryption Profile Parameters

Parameter	Description
Name	Encryption Profile name
Admin State	Enable/Disable Encryption Profile: ■ disabled ■ enabled
Public Key Filename	The name of the public key file to be used for MSISDN encryption. The file should be placed in /tosdb/content/publickeys.
Type	Type of public key file: ■ PEM ■ DER ■ X509

5. Click the **Save** icon.

Explicit Proxy Profile

Use this object to configure an explicit proxy address profile.

To add an Explicit Proxy Address Profile:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Explicit Proxy Profile**.
4. Configure the parameters as follows:
   - **Name** – Specify an explicit proxy profile name.
5. Click the **Save** icon.
6. Expand the Explicit Proxy Profile you added.
7. To configure the network context and address list, click **Explicit Proxy Networkcontext**.
8. Configure the parameters as follows:
   - **Network Context** – Specify the network context to use for the explicit proxy address list.
9. Click the **Save** icon.
10. Expand the network context you specified.
11. Click **Explicit Proxy Address**.
12. Configure the parameters as follows:

Table 10-248 Explicit Proxy Address Parameters

Parameter	Description
Name	Name of the explicit proxy address list
IP Address	IP Address
Port	Port

13. Click the **Save** icon.

Fraud Detection Profile

Use this object to enable the gateway to detect and take a configured action on subscriber devices attempting data connections through fraudulent use of a web proxy. For example, the system can detect fraudulent users utilizing rogue HTTP proxies to spoof HTTP URLs for free rated sites, such as those the Carrier assigns for browsing promotions and partnerships.

To configure Fraud Detection Profile:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Fraud Detection Profile**.
4. Configure the parameters as follows:

Table 10-249 Fraud Detection Profile Parameters

Parameter	Description
Name	Fraud Detection Profile name.
Admin State	Enable/disable the Fraud Detection service: ■ enabled ■ disabled
Action	Action to take when fraud is detected: ■ allow ■ block
Block Notification Message	*Applies when Action is set to block:* HTTP Request Block Message used in the '403 forbidden' response sent to the client.
Service Rule	Service Rule to apply to the Fraud Detection Profile. The Service Rule specifies which requests to subject to the fraud check. For example, to apply the fraud check only to free rated websites for browsing promotions and partnerships, configure the Service Rule with the list of free-rated domains. If the fraud detection Service Rule is not configured, fraud checks are performed for *all* HTTP requests. The Service Rule must already exist. See Service Rule. To add additional Service Rules, click the **Create** icon.
Whitelist	Whitelist to apply to the Fraud Detection Profile. The Whitelist contains the IP addresses that represent legitimate proxies. The Whitelist must already exist. See Host List. To add additional Whitelists, click the **Create** icon.

5 Click the **Save** icon.

HTTP Transaction Record Profile

HTTP Transaction Data Records provides information about each HTTP transaction that traverses the NE. The data is represented in comma-separated values format (CSV) and written as a string of CSV values.

The HTTP Transaction Data record can include such information as:

- Time information: Request timestamp and latency information
- Subscriber information: IMSI, MSISDN, etc.
- Connection information: Network context, source and destination address, etc.
- Request information: HTTP request information
- Response information: HTTP response information
- Compression information: Compression and bytes saved, if compression is applied
- Web image Optimization information: Information about web image optimization and bytes saved, if applied.
- Video information: Information about any video served and bytes saved, if applied.
- Minification information: Information about minification and bytes saved, if applied.

The Operator can customize the records in certain positions and can include or omit certain records. Configure the following values in the Service Construct > Data Record Template > HTTP Proxy > HTTP Transaction:

- *Present Flag* – Indicates whether to include the data field in the CDR. By default, this value is set to conditional for all data fields, indicating that the data field will be filled in CDRs when available.
- *Position Index* – Location of the data field in the CDR. A pre-defined order exists for each data field if positionIndex is not configured.
- *Format Type* – The format for the data field. If not configured, the format type uses the default.
- *Length* – The fixed length of the data field. The length defaults to zero indicating the data field is written out as it is.

- *Alignment* – The alignment of the data field. If not configured, the alignment defaults to left aligned.
- *Padding* – The character used for padding when the field has a fixed length.

HTTP Transaction Data Records information can be used to:

- Calculate details, such as bandwidth savings when features like Web Image Optimization and video adaptation are enabled.
- Provide the basis for charging
- Measure analytics

Specify the HTTP transaction record profile in an HTTP Proxy instance tied to the workflow for it to take effect.

To configure HTTP Transaction Record Profile:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **HTTP Transaction Record Profile**.
4. Configure the parameters as follows:

Table 10-250 HTTP Transaction Record Profile Parameters

Parameter	Description
Name	HTTP Transaction Data Record profile name
File Type	File type for streaming HTDR record locally: ■ Event Log ■ Data Record ■ Core Files ■ RAM Disk-Storage ■ Storage ■ Ext-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming HTDR record locally
Encode Format	Format type: ■ CSV
Record URL Length	Length to which the URL field should be truncated in the record

Table 10-250 HTTP Transaction Record Profile Parameters

Parameter	Description
Transaction Template	HTTP Transaction Record Template. Configure at Service Construct > Data Record Template > HTTP Proxy > HTTP Transaction

5 Click the **Save** icon.

HTTPS Profile

Use this object to enable HTTP Proxy support for HTTPS (HTTP Secure) - an HTTP protocol variant that uses secure TLS, rather than TCP, connections for communication with clients and/or servers.

MCC HTTP Proxy supports the following HTTPS features:

- HTTPS termination of client TLS connections
- HTTPS origination of TLS connections to HTTPS servers
- HTTPS pass-through

When HTTP Proxy is used to terminate clients' TLS connections to HTTPS servers, the HTTPS Profile must include TLS Termination Policies for the servers. Once terminated, HTTP Proxy decrypts and processes user HTTPS requests and applies enabled content features.

When HTTP Proxy is used to originate HTTPS server connections, server authentication is performed using a list of trusted CA certificates configured in the HTTPS Profile.

HTTPS traffic for which no TLS Termination Policy is configured bypasses HTTP Proxy logic and is passed-through between the client and server. Because the HTTPS pass-through traffic is not processed by HTTP-Proxy, content features are not applied to HTTP requests on these connections. However, connection-level features such as TCP Optimization are supported.

To add an HTTPS Profile:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **HTTPS Profile**.

4 Configure the parameters as follows:

Table 10-251 HTTPS Profile Parameters

Parameter	Description
Name	HTTPS Profile name
Admin State	Admin state: ■ enabled ■ disable
Ca Certificate List	HTTPS Origination CA certificate list The Ca Certificate List must already exist. See CA Certificate List.
TLS Protocol Logging	Enable debug logging for openssl when this HTTPS Profile is used: ■ enabled ■ disable

5 Click the **Save** icon.

6 Expand **HTTPS Profile**.

7 Expand the HTTPS Profile you added.

8 Click **TLS Termination Policy**.

9 Configure the parameters as follows:

- **Name** – Enter the TLS Termination Policy name. The TLS Termination Policy must already exist. See TLS Termination Policy.

10 Click the **Save** icon.

11 Repeat step 8 through step 10 to add as many TLS Termination Policy as needed.

Long Term Mobile ID

Use this object to configure a Long Term Mobile ID (LTMI). It supports insertion of encrypted subscriber ID in an HTTP request header to allow the subscriber ID to be communicated to origin server in a secure manner.

MCC supports the following levels of encoding/encryption formats:

- Plain Text
- LTMI Static Trusted
- LTMI dynamic Trusted
- LTMI External

Operators can opt out of the LTMI feature using the Opt Out String and Static Trusted ID String.

MCC supports the following text string VSAs used to generate LTMI and the reseller ID header. The VSAs are retrieved from the PCRF when a call is established, and delivered to the HTTP Proxy when an HTTP request header is processed.

- subID
- miDial
- resellerID

Using HTTPS, the MCC periodically downloads encryption keys from a key server. The keys can be manually imported using import LTMI key or automatically imported from the key server by configuring the minute interval using key-import-interval.

To add a long term mobile ID:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **LTMI**.
4. Configure the parameters as follows:

Table 10-252 LTMI Parameters

Parameter	Description
The following parameters control the key import (download) from the key server using HTTPS:	
Key Import Interval	Key import interval, in minutes, zero turns off key import
Key Server URL	Network Context used for non-HTTP connections. It overrides the Network Context selected by a higher-level object.
Key Server Username	Key Server username for basic authentication.

Table 10-252 LTMI Parameters

Parameter	Description
Key Server Password	Key Server password for basic authentication.
Key Server Network Context	Key server network context
Loopback IP List	Key Server Loopback IP List. The Loopback IP List must already exist. Create it at Network Context > Loopback IP List. LTMI download chooses the loopback from Loopback IP List if it is configured.
The following parameters control if and how the LTMI ID is generated:	
ID Gen Admin State	Enable/Disable LTMI ID generation: ■ enabled ■ disable
Trusted ID Divisor	Number of minutes for trusted ID rotation interval (for example, 6 months rotation = 259,200 minutes)
External ID Divisor	Number of minutes for external ID rotation interval (for example, 24 hour rotation = 1440 minutes.
Network Carrier Code	Code used in dynamic mobile IDs to identify the carrier.
Opt Out String	String used to search the opt out value to see if a subscriber has opted out of Dynamic Mobile ID. When a subscriber opts out this feature, no LTMI is inserted in the HTTP request header. If the miDial string exactly matches the Opt Out String, then the subscriber completely opts out of LTMI.
Static Trusted ID String	Ending of the search string used to identify opt out value for static trusted ID. If the miDial string ends with the Static Trusted ID String, then the Static Trusted ID is used instead of the Dynamic Trusted ID. For example, if the Static Trusted ID String is configured as "#" and the miDail string is "xyz#" (ending with "#"), then the Static Trusted ID is used instead of the Dynamic Trusted ID.
Extra Curl Option	Passes additional option to the curl command used to download the LTMI key.

5 Click the **Save** icon.

LTMI Import History

Use this object to view import history of long term mobile ID keys.

To view LTMI import history:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Expand **LTMI Key**.
4. Expand **Import History**.
5. Click an instance.

LTMI import history parameters are:

- Import Time
- Import Result: Success or N/A
- Import File Size
- Number Of Accepted Entries
- Number Of Rejected Entries
- Import File Name
- Import Type: manual or scheduled

LTMI Key Status

Use this object to view status of long term mobile ID keys.

To view LTMI key status:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Expand **LTMI Key**.
4. Expand **Status**.
5. Click an instance.

LTMI key status parameters are:

- Last Import Time
- Last Import Result
- Last Import Type
- Last Import Number
- Last Import File Size (Bytes)
- Next Scheduled Import Time
- Number Of Entries

- Accepted Entries
- Import URL

Minify

Use this object to enable minification for Javascript, CSS, or HTML. Minification removes unnecessary characters (such as blank characters and new line characters) from source code, thereby reducing the amount of data that needs to be transferred.

To enable Minification:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Minify**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable minification.
5. Click the **Save** icon.

Optimization Overload Control

Use this object to enable Proxy Optimization Overload Control that adds logic to a proxy task to bypass some images or videos to prevent the system from being overloaded.

To enable Optimization Overload Control:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Optimization Overload Control**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable Optimization Overload Control.
5. Click the **Save** icon.

Preemptive DNS

Use this object to replace the URLs in the response with the IP address of one of the Affirmed Networks Gi local loopback addresses and configured DNS Token before sending to the client.

To configure HTTP preemptive DNS:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.

3 Click **Preemptive DNS**.

4 Configure the parameters as follows:

Table 10-253 Preemptive DNS Parameters

Parameter	Description
Admin State	Admin state: ■ enabled ■ disable
Token	String token used to replace URLs in HTTP Response.
Network Context	Network Context used to select Loopback IP address
Loopback IP v4	v4 loopback IP address to be used to replace URLs in HTTP response
Loopback IP v6	v6 loopback IP address to be used to replace URLs in HTTP response

5 Click the **Save** icon.

Server Connections

To configure HTTP Proxy server connections:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **Server Connections**.

4 Configure the parameters as follows:

Table 10-254 Server Connections Parameters

Parameter	Description
Idle Timeout	Server connection idle timeout, in seconds.
Max Server Idle	Maximum number of idle connections per server.
Max Total Idle	Total maximum number of idle server connections. Value 0 disables keeping idle connections.
HTTP Fast Open	Mark the checkbox to enable HTTP Fast Open. When enabled, the MCC proxy opens a server connection during the client connection handshake, which reduces the HTTP transaction time by approximately one Round Trip Time (RTT) between the UE and MCC proxy.

5 Click the **Save** icon.

Steering Group

Use this object to configure a group of Steering Destinations.

To add a Steering Group:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Steering Group**.
4. Configure the parameters as follows:
   - **Name**: Steering Group name.
   - **Health Check Profile**: Health Check Profile for the Steering Destination. The Health Check Profile must already exist. See Health Check Profile.
5. Click the **Save** icon.
6. To configure a steering destination for the group, expand the Steering Group you added.
7. Click **Steering Destination**.
8. Configure the parameters as follows:

Table 10-255 Steering Destination Parameters

Parameter	Description
Name	HTTP Steering Destination Name
IP Address	IP address for Steering Destination
Port	Port for Steering Destination Port
Host Name	Host Name (FQDN) of the Steering Destination
Network Context Override	Configure Network Context to use for Steering Destination
Priority	Configure Steering priority

9. Click the **Save** icon.
10. Repeat step 7 through step 9 to add as many steering destinations as needed.

TCP Splicing

Use this object to configure HTTPS Fast Open. When enabled, the MCC proxy opens a server connection during the client connection handshake, which reduces the HTTPS transaction time by approximately one Round Trip Time (RTT) between the UE and MCC proxy.

To configure HTTPS Fast Open:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **TCP Splicing**.
4. Configure the parameters as follows:
   - **Server Connection Fast Open** – Mark the checkbox to turn on TCP server connection fast open.
5. Click the **Save** icon.

TCP Splicing Policy

Use this object to configure a policy that controls the behavior of the TCP connections that match an HTTP IP Flow. The matched traffic is forwarded to a TCP splicing component and spliced to the server.

To configure a TCP Splicing Policy:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **TCP Splicing Policy**.
4. Configure the parameters as follows:

Table 10-256 TCP Splicing Policy Parameters

Parameter	Description
Name	Content TCP Splicing Policy Name
Priority	Priority of the TCP Splicing Policy, must be unique
Traffic Control Profile	Traffic Control Profile associated with this policy. The Traffic Control Profile must already exist. See Traffic Control Profile.

5. Click the **Save** icon.
6. Expand the policy you added.
7. Click **Service Rule**.
8. Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the TCP Splicing Policy.

  The Service Rule must already exist. See Service Rule.

9 Click the **Save** icon.

Toll Free Profile

Use this object to configure a toll free profile to support Toll Free Data (TFD). TFD is a feature in which a third-party (content provider) pays for a subscriber's data usage when the subscriber is downloading or using the third-party company's Apps, Websites, and services. If a toll free profile is enabled, TFD is turned on for that proxy instance.

To configure a toll free profile:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **Toll Free Profile**.

4 Configure the parameters as follows:

- **Name** – Enter a profile name.
- **Admin State** – Select Enabled to enable the profile.

5 Click the **Save** icon.

6 To configure a certificate server, expand the profile you added.

7 Click **Certificate Server**.

8 Configure the parameters as follows:

Table 10-257 Certificate Server Parameters

Parameter	Description
CA Certificate List	CA root certificate. The CA certificate must first be placed in */public/content/tls/cacerts* before it can be configured. The Ca Certificate List must already exist. See CA Certificate List.
Certificate URL	URL prefix for certificates (for example, http://certificateserver/)
Certificate File Extension	Certificate file extension

Table 10-257 Certificate Server Parameters

Parameter	Description
CRL URL	URL for Certificate Revocation List (string starting with http://) When toll-free-data manifest is received before Certificate Revocation List (CRL) is available to the MCC, the manifest is processed. After parsing and signature verification, the manifest is installed into the subscriber service profile. The manifest, using revoked content provider certificate, is only removed when the UE triggers a manifest refresh (re-downloads the manifest again).
Network Context	Network context for accessing the certificate server
Loopback IP	Loopback interface for accessing the certificate server

9 Click the **Save** icon.

10 To configure a data record, click **Data Record Configuration**.

11 Configure the parameters as follows:

Table 10-258 Data Record Configuration Parameters

Parameter	Description
File Type	File type for streaming the Toll Free Data record locally: ■ Event Log ■ Data Record ■ Cores Files ■ Storage ■ Ext-Storage ■ RAM Disk-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming the Toll Free Data record locally The file must already exist. Create it at Infrastructure > File Management > Profile (of type datarecord).
TFD Template	Toll Free Data record template The record template must already exist. Create it at Service Construct > Data Record Template > HTTP Proxy > Toll Free Data.

12 Click the **Save** icon.

13 To configure toll free header names, click **TF Header Names**.

14 Configure the parameters as follows:

Table 10-259 TF Header Names Parameters

Parameter	Description
TF Manifest Indication	Header name for toll free manifest indication
TF Manifest ID	Header name for toll free manifest ID
TF Eligible	Header name for toll free eligible
TF Access	Header name for toll free access
TF Status	Header name for toll free status
TF SID	Header name for toll free sponsor ID
TF Callback URL	Header name for toll free callback URL

15 Click the **Save** icon.

Traffic Control Profile

Use this object to configure a profile for handling of splicing traffic (data forwarding between client and server TCP connections).

HTTP proxy supports forwarding of non-HTTP traffic received on port 80. The TCP splicing component of HTTP proxy is responsible for handling of non-HTTP traffic. The component maintains a pair of client-side and server-side connections and forwards data between these connections.

To configure a Traffic Control Profile:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **Traffic Control Profile**.

4 Configure the parameters as follows:

Table 10-260 Traffic Control Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Network Context Override	Network Context used for the Traffic Control Profile. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for splicing server connections

Table 10-260 Traffic Control Profile Parameters

Parameter	Description
Steering Group	Configure the Steering Destinations to use for this profile. The Steering Group allows the UDP flow to be steered to the destination configured within itself, when the profile is selected. In the packet processing, after UDP policies are evaluated, the associated traffic-control-profile is selected. The steering group within the profile can have multiple steering-destinations. A round-robin approach is used between destinations. In case of a single steering-destination, the current UDP flow is steered to that destination. The Steering Destinations must already exist. See Steering Group.
Toll Free Data	Mark the checkbox to indicate that toll free data applies for this profile.
Upstream Buffering Limit	Maximum data to store when processing upstream data, in KB.
Downstream Buffering Limit	Maximum data to store when processing downstream data, in KB.
Segment Threshold	Segment threshold in bytes for bypassing rate-limiting.
Rate Limiting:	
Admin State	Admin state: ■ enabled ■ disable
Burst Size	Burst size
Burst Size Units	Burst size units: ■ bytes ■ kbytes ■ mbytes ■ gbytes
Bitrate	Bitrate
Bitrate Units	Bitrate units: ■ bps ■ kbps ■ mbps ■ gbps

Table 10-260 Traffic Control Profile Parameters

Parameter	Description
Savings Estimation:	
Admin State	Admin state: estimation of optimization byte savings attributed to rate-limited HTTPS video traffic. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on video sessions: ■ enabled ■ disable
Sampling Interval	Sampling interval for savings estimation
Sampling Interval Unit	Unit for sampling interval for savings estimation: ■ min ■ hr

5 Click the **Save** icon.

UDP

Use this object to configure a profile for handling UDP Proxy. It enables Operators to selectively apply rate limiting to Quick UDP Internet Connection (QUIC) protocol flows. This feature complies with Google's Quic Version 39.

To configure a UDP:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Click **UDP**.

4 Configure the parameters as follows:

Table 10-261 UDP Parameters

Parameter	Description
Quic Rate Limiting	Specifies whether to enable QUIC rate limiting ■ enabled ■ disable
Idle Timeout	UDP Splicing idle timeout, in seconds.
Quic Reset Timeout	QUIC reset timeout, in seconds.

5 Click the **Save** icon.

UDP Policy

Use this object to configure a UDP Policy.

To configure a UDP Policy:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **UDP Policy**.
4. Configure the parameters as follows:

Table 10-262 UDP Policy Parameters

Parameter	Description
Name	UDP Policy name
Priority	Priority of the UDP policy, must be unique
Traffic Control Profile	Traffic Control Profile associated with this policy. The Traffic Control Profile must already exist. See Traffic Control Profile.
Congestion Control	Type of Congestion Control: ■ head-drop ■ tail-drop

5. Click the **Save** icon.

Video Pacing

Use this object to configure video pacing. Video pacing is sending video data to the client at a restricted rate. The video is not completely streamed at the fastest possible rate, instead it is throttled.

To configure video pacing:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Video Pacing**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable video pacing.
5. Click the **Save** icon.

In addition, configure the following parameters in the HTTP Response Policy (see HTTP Response Policy):

- **Video Pacing Burst Time** represents the time for which the video data should be sent at a burst.
- **Video Pacing Factor** represents the factor at which the video should be paced.

Web Image Optimization Profile

Use this object to configure an HTTP Proxy Web Image Optimization Profile that defines image compression and transcoding to produce a large gain in bandwidth savings for the Operator.

The profile specifies image conversion parameters such as re-compression, metadata, quality, percentage, and size. For example, you can configure the predicted size savings percentage threshold that can be optimized, such as a target JPEG quality between 0 (coarsest) and 100 (finest quantization). You associate a Web Image Optimization Profile with an HTTP Request Policy.

To add a Web Image Optimization Profile:

1. Expand **Services** in the tree.
2. Expand **HTTP Proxy**.
3. Click **Web Image Optimization**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable web image optimization.
5. Click the **Save** icon.
6. Expand **Web Image Optimization**.
7. Click **Profile**.
8. Configure the parameters as follows:

Table 10-263 Web Image Optimization Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Convert PNG to JPEG	Mark the checkbox to allow conversion of PNG to JPEG.
Convert GIF to PNG	Mark the checkbox to allow conversion of GIF to PNG.
Convert GIF to JPEG	Mark the checkbox to allow conversion of GIF to JPEG.
Sample JPEG to 420	Mark the checkbox to allow 4:2:0 chroma subsampling of JPEG.
Interlace Image	Mark the checkbox to allow interlace image
Quantize Image	Mark the checkbox to allow requantization of palettized image.
Resize Image	Mark the checkbox to allow resizing of image.

Table 10-263 Web Image Optimization Profile Parameters

Parameter	Description
Remove Metadata	Mark the checkbox to allow removal of image metadata.
Target JPEG Quality	Target JPEG quality, with 0 being the coarsest quantization, and 100 being the finest quantization.
Target Max Size	Target maximum size (in KB) that can be optimized.
Source Min Size	Source minimum size (in KB) that can be optimized.
Size Saving Threshold	Predicted size saving percentage threshold that can be optimized.
Source Max Size	Source maximum size (in KB) that can be optimized.

9 Click the **Save** icon.

Service Data Flow

Use this object to view each service data flow that is evaluated on each HTTP Proxy during flow classification, in order of evaluation.

To view service data flow:

1 Expand **Services** in the tree.

2 Expand **HTTP Proxy**.

3 Expand **Service Data Flow**.

4 Click an instance.

Service data flow parameters are:

- Http Proxy
- Http Ip Flow Priority
- Service Rule Priority
- Http Ip Flow
- Service Rule
- Http Ip Flow Id
- Service Rule Id

HTTP Server

User this object to configure a Content HTTP Server Service.

HTTP Server Service Instance

Use this object to configure an HTTP Server Service instance associated with an MMS STI service.

To add an HTTP Server Service instance:

1. Expand **Services** in the tree.
2. Expand **HTTP Server**.
3. Click **Instance**.
4. Configure the parameters as follows:

Table 10-264 HTTP Server Service Instance Parameters

Parameter	Description
Name	Content HTTP Server Service instance name
Admin State	Admin state: ■ enabled ■ disable
Mms Sti	MMS STI profile associated with the HTTP Server Instance. The MMS STI profile already exist. See STI Profile.
UA Profile	User Agent database associated with this HTTP Server Service. The UA Profile must already exist. See UA Profile.

5. Click the **Save** icon.
6. To configure the Network Context and Loopback address to use for the HTTP Server instance, expand **Instance**.
7. Expand the Instance you added.
8. Click **Network Context**.
9. Configure the parameters as follows:

Table 10-265 Network Context Parameters

Parameter	Description
Network Context	Select the Network Context.
Loopback IP	Loopback IP Address.
Loopback Port	Loopback IP Port

10 Click the **Save** icon.

11 To configure the HTTP Server Policies to use for the HTTP Server instance, expand **Instance**.

12 Expand the Instance you added.

13 Click **HTTP Server Policy**.

14 Configure the parameters as follows:

- **Name** – Select the HTTP Server Policy to associate with the HTTP Server instance.

  The HTTP Server Policy must already exist. See HTTP Server Policy.

15 Click the **Save** icon.

16 To configure the content insertion to use for the HTTP Server instance, expand **Instance**.

17 Expand the Instance you added.

18 Click **Content Insertion**.

19 Configure the parameters as follows:

Table 10-266 Content Insertion Parameters

Parameter	Description
Admin State	Admin state: ■ enabled ■ disable
Loopback IP List	Loopback IP Address list used for content insertion. The Loopback IP List must already exist. See Loopback IP List.

20 Click the **Save** icon.

21 To configure the content insertion profile to use for the HTTP Server instance, expand the content insertion you added.

22 Click **Content Insertion Profile**.

23 Configure the parameters as follows:

- **Name** – Select the Content Insertion Profile to associate with the HTTP Server instance.

  The Content Insertion Profile must already exist. See Content Insertion Profile.

24 Click the **Save** icon.

Entitlement Service

Use this object to configure an Entitlement Service mapping.

The entitlement server is used by subscriber mobile devices to obtain information as to which services a subscriber is entitled. The entitlement server provides the ability for the UE to query and determine if a subscriber is entitled to certain services. The entitlement server is also used to obtain a signed MSISDN that is used with the registration server.

The entitlement server supports two types of entitlement:

- *Simple (http)* – Uses GET requests with no security. The simple entitlement protocol flow is as follows:
  - Subscriber device sends HTTP GET request to entitlement server; the URL contains service name
  - Entitlement server responds with HTTP status code (success or disallowed) for the queried service
- *Secure (https)* – Uses POST method and the body is in JSON format. The entitlement.py script contains the certificates to chain back to the Trusted Certificate Authority.

  The secure entitlement protocol flow is as follows:
  - PGW obtains a list of services to which the subscriber is entitled. The Gx interface contains a set of Vendor Specific Attributes (VSAs)
  - Subscriber Device sends HTTPS POST request to Entitlement Server; the payload used JSON formatting and gzip compression
  - Entitlement Server responds with subscriber status code (success or disallowed) for each queried service
  - Entitlement Server responds with MSISDN and signature of the nonce+MSIDSN for the MSISDN query
  - HTTP response is sent in the gzipped JSON format

An Entitlement Service global configuration specifies the mapping between the URI and the internal VSA name. MCC implements the entitlement server using a server plugin method that uses this mapping to determine whether the service exists in the Vendor Specific Attributes (VSAs) coming in from the service-metadata.

To add an Entitlement Service:

1. Expand **Services** in the tree.
2. Expand **HTTP Server**.
3. Expand **Entitlement**.
4. Click **Entitlement Service**.
5. Configure the parameters as follows:

Table 10-267 Entitlement Service Parameters

Parameter	Description
Name	Entitlement service name.
URI	URI of the service. If configured, the URI must be unique.
Entitlement VSA Value	Entitlement Vendor Specific Attribute Value

6 Click the **Save** icon.

HTTP Server Policy

For an entitlement server, associate two HTTP Server Policies with the instance: simple and secure entitlement. The policies reference a server plugin script that is responsible for processing the request and generating a response and a Service Rule to match the request to a policy. Associate this policy with a Service Rule.

To add an HTTP Server Policy:

1 Expand **Services** in the tree.

2 Expand **HTTP Server**.

3 Click **HTTP Server Policy**.

4 Configure the parameters as follows:

Table 10-268 HTTP Server Parameters

Parameter	Description
Name	HTTP Server Policy name
Priority	Priority of the http-server-policy, must be unique This value resolves conflicts in the case of multiple policies. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Server Plugin	Server plugin associated to this policy

5 Click the **Save** icon.

6 To configure the Service Rule to use, expand **HTTP Server Policy**.

7 Expand the HTTP server policy you added.

8 Click **Service Rule**.

9 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the HTTP Server Policy.

The Service Rule must already exist. See Service Rule.

10 Click the **Save** icon.

Statistics

Use this object to view the Server Plugin statistics.

To view Server Plugin Statistics:

1 Expand **Services** in the tree.

2 Expand **HTTP Server**.

3 Expand **Statistics**.

4 Expand **Cluster Level** or **Node Level**.

5 Expand **Server Plugin**.

6 Expand **Plugin Entry**.

7 Click a plugin entry instance.

Server Plugin statistics are:

- Server Plugin Summary Attempts: Total number of plugin attempts
- Server Plugin Summary Successes: Total number of plugin successes
- Server Plugin Summary Failures: Total number of plugin failures
- Server Plugin Detail HTTP Error Responses: Total number of plugin HTTP error responses
- Server Plugin Detail HTTP OK Responses: Total number of plugin HTTP OK responses
- Server Plugin Failures Internal Failures: Total number of plugin internal failures
- Server Plugin Failures Invalid Request: Total number of invalid requests sent to plugin

Metering Service

Use this object to configure a Metering Service to operate in parallel to the charging service. The metering service instance contains a set of metering rating groups to convey the usage counts to the gateway. Each metering rating group has a configurable threshold and an optional AOC landing page URL.

To add a Metering Service instance:

1. Expand **Services** in the tree.
2. Expand **Metering**.
3. Click **Metering Instance**.
4. Configure the parameters as follows:

Table 10-269 Metering Service Instance Parameters

Parameter	Description
Name	Metering Service instance name
State	Admin state: ■ enabled ■ disable

5. Click the **Save** icon.
6. To configure the Rating Groups to use, expand **Metering Instance**.
7. Expand the Metering Instance you added.
8. Click **Rating Group**.
9. Configure the parameters as follows:
   - **Name** – Select the Rating Group to associate with the Metering Instance.

     The Rating Group must already exist. See Charging: Rating Group.
10. Click the **Save** icon.
11. To associate Geographic Redundancy Groups with this Metering Instance, click **Geo Redundant Group**.
12. Configure the parameters as follows:
    - **Name** – Select the Geographic Redundancy Group to associate with the Metering Instance.

      The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.
13. Click the **Save** icon.

Service Data Flow

Use this object to view each service data flow that is evaluated on each metering service during flow classification, in order of evaluation.

To view service data flow:

1. Expand **Services** in the tree.
2. Expand **Metering**.
3. Expand **Service Data Flow**.
4. Click an instance.

Service data flow parameters are:

- Metering Service
- Rating Group Priority
- Service Rule Priority
- Rating Group
- Service Rule
- Rating Group Id
- Service Rule Id

Multi Protocol Proxy (8.4 and later MCC versions)

Multi Protocol Proxy acts as an intermediary for requests from clients seeking resources from other servers. The Multi Protocol Proxy is an intercepting forward proxy that acts like the server to the UE and acts like a client to the origin server.

The Multi Protocol Proxy function supports:

- Separate Request Policy and Response Policy to allow the Operator to specify the actions separately for request phase and response phase.
- Request Policy to notify the origin servers of the private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
- On-the-fly HTTP compression for supported client requests or all client requests.
- Setting the global compression level.
- Fraud Detection handling – Multi Protocol Proxy performs DNS validation and Header consistency checks to determine if a request is destined for a legitimate domain or destined for a rogue proxy. If the destination IP address is not within the defined range or domain returned by the DNS lookup, the system determines if a free browsing proxy is in use and enforces a specified action (allow the traffic and charge for it and/or reduce its QoS to a specified level).
- Multi Protocol Proxy latency – Multi Protocol Proxy forwards HTTP request and response data as soon as possible. Fragments of request/response body are received, processed, and immediately streamed, ensuring low forwarding latencies. Typical request and response forwarding latency is within several tens of milliseconds.

  However, the Multi Protocol Proxy transaction latency may increase when:

  – Client or server socket back-pressure due to network congestion, QoS bandwidth, or burst limits.
  – Optimization features are applied (such as compression, minification, web image optimization, preemptive, DNS, and so on).
  – Request store-and-forward-limit option is used (applies to requests using the option. The added latency depends on the request size and client uplink speed).
  – Response buffering-limit option is used (applies to responses using the option. The added latency depends on response size and client downlink speed).
  – Large objects are served from disk cache on a system with rotational media.
  – Back-End Forwarding is enabled in the system.

The Multi Protocol Proxy service retrieves the following VSAs from the PCRF via the Gx interface and distributes these VSAs to the Multi Protocol Proxy. MCC uses these VSAs to customize Multi Protocol Proxy services for a particular subscriber.

- VsaEntitlement – Indicates the type of service to which the subscriber is entitled.
- VsaPaymentType – Indicates subscriber payment type. Possible values include:
  - PO – Postpaid subscriber.
  - PR – Prepaid subscriber.
  - SL
- VsaSubId – Indicates the subscriber ID.
- VsaHttpPolicy – Customize Multi Protocol Proxy services. Possible values include:
  - NOPRXY – Multi Protocol Proxy is disabled for the subscriber.
  - NOGZIP – Gzip compression is disabled for the subscriber.
  - NOTFD – No Toll Free Data (TFD).
  - NOVIDEO – Video optimization is disabled for the subscriber.
- VsaResellerId – Indicates the subscriber's reseller ID.
- VsaMiDial – Indicates whether the subscriber opted out from Long Term Mobile ID (LTMI) header enrichment or opted for static trusted ID in LTMI header enrichment.

Service VSAs received by the PGW are listed in Subscriber > PDN Session.

The Multi Protocol Proxy service allows users to load unoptimized content using shortcut keys from web browsers. The shortcut keys trigger a no-cache HTTP request header to disable the following HTTP optimization features:

- DNS Preemption
- Minification
- Web image optimization
- Zip compression
- Video adaptation online transcoding

Table 10-270 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
F5	All	Refreshes a page with If-Modified-Since header, but no no-cache header

Table 10-270 Shortcut Keys to Load Unoptimized Content

Key	Browsers	Action
<Ctrl>F5	Internet Explorer10 Chrome Firefox	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>F5	Chrome	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache
<Shift>Reload	Safari	Refreshes a page with one or both of the HTTP headers to ignore cached response: ■ Cache-Control: no-cache ■ Pragma: no-cache

Multi Protocol Proxy Service

To add a Multi Protocol Proxy Service:

1 Expand **Services** in the tree.

2 Click **Multi Protocol Proxy**.

3 Configure the parameters as follows:

Table 10-271 Multi Protocol Proxy Parameters

Parameter	Description
Admin State	Multi Protocol Proxy administrative state: ■ enabled ■ disabled
Client Idle Timeout	Client idle timeout, in seconds
Compress Level	Global compression level: ■ default-compression ■ best-compression ■ best-speed
Static DNS Map	Static DNS map to use to avoid doing DNS lookup through configured DNS server(s). The Multi Protocol Proxy service uses the map's IP Address list to open server connections for HTTP request. The Static DNS map must already exist. See Static DNS Map.

4 Click the **Save** icon.

HTTP Request Policy

To add an HTTP Request Policy:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **HTTP Request Policy**.
4. Configure the parameters as follows:

Table 10-272 HTTP Request Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
HTTP Protocol	Protocol used towards origin server: ■ ue-http-protocol: preserves original UE protocol ■ http ■ https
Steering Group	Steering Group to use for the HTTP requests. The Steering Group must already exist. See Steering Group.
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for server connections. The Loopback IP List must already exist. See Loopback IP List.
Store Forward Buffer Limit	Maximum data to store before forwarding request to server, in KB. When the HTTP Request Policy is applied, the server connection is not opened until the received request buffer size reaches this value or entire request is received. If zero, request is immediately forwarded.
Bypass HTTP Proxy	Specifies whether to bypass HTTP proxy for this policy: ■ disabled ■ enabled When enabled, the request is TCP spliced.
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds the specified HTTP headers/cookies to the HTTP request header. The Header Enrichment Profile must already exist. See HTTP Header Enrichment.

Table 10-272 HTTP Request Policy Parameters

Parameter	Description
Content Insertion Profile	Select the Content Insertion Profile. The Content Insertion Profile must already exist. See Content Insertion Profile.
URL Rewrite Profile	Select the HTTP URL Rewrite profile. The HTTP URL Rewrite profile must already exist. See HTTP URL Rewrite.
DNS Resolution	Specify whether to use DNS resolution to look up destination.
Forced Cache Access Notification	Enable/Disable Forced Cache Object Access Notification to the origin server: ■ disabled ■ enabled When enabled, HTTP request policy notifies the origin servers of private-cacheable video objects access by sending a HTTP HEAD request to the origin server for each client access.
Compress Force	Specify whether to force on-the-fly HTTP compression for all client requests.
Compress Inline	Specify whether to enable on-the-fly HTTP compression for supported client requests.
Preemptive DNS	Specify whether to apply HTTP Proxy service level preemptive DNS for this policy: ■ enabled ■ disabled
Compress Min Size	Minimum response size in bytes required for compression to take effect
Web Image Optimization	Select the Web Image Optimization to use for HTTP requests. The Web Image Optimization must already exist. See Web Image Optimization Profile.
Server TCP Optimization Profile	Select the TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.

5 In **Compression**, configure the parameters as follows:

- **Compress Max Size** – Enter the maximum response size in bytes allowed for compression to take effect.

6 In **Minify**, configure the parameters as follows:

Table 10-273 Minify Parameters

Parameter	Description
Minify Javascript	Mark the checkbox to minify JavaScript (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify HTML	Mark the checkbox to minify HTML (to remove unnecessary characters such as blank characters and new line characters from source code)
Minify Min Size	The minimum response size in bytes required for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Max Size	The maximum response size in bytes allowed for minification to take effect. When a response exceeds this limit, the HTTP proxy bypasses minification. In addition, if the HTTP proxy is in a minor, major, or critical overload state, the HTTP proxy bypasses minification.
Minify Css Choice	Select minify-css to minify CSS (to remove unnecessary characters such as blank characters and new line characters from source code)

7 In **Service Rule**, configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the HTTP Request Policy.

  The Service Rule must already exist. See Service Rule.

  The Service Rule must contain an HTTP Rule Group.

To add additional Service Rules, click the **Create** icon.

HTTP Response Policy

To add an HTTP Response Policy:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **HTTP Response Policy**.

4 Click the **Create** icon.

5 Configure the parameters as follows:

Table 10-274 HTTP Response Policy Parameters

Parameter	Description
Name	Content HTTP Policy name
Priority	HTTP Policy priority
Header Enrichment Profile	Specified the Header Enrichment Profile to apply on service rule match. For example, if the Service Rule specifies an HTTP Rule Group of match type URL, upon a match, the HTTP Policy adds the specified HTTP headers/cookies to the HTTP response header. The Header Enrichment Profile must already exist. See HTTP Header Enrichment.
Video Pacing Burst Time	Video Pacing burst time, in seconds. Represents the time for which the video data should be sent at a burst.
Video Pacing Factor	Video Pacing factor (scale factor 1/100) at which the video should be paced. Set to zero to disable pacing. For example, setting a Video Pacing Burst Time of 20s and a Video Pacing Factor of 100 specifies to send the initial 20 seconds of video at the maximum possible rate and to pace the video by a factor of 100 (that is, 1* bit-rate of the video).
Rate Limiting Burst Size	Rate limiting burst size, in bytes
Rate Limiting Bit Rate	Rate limiting bit rate, in bps
Buffering Limit	Maximum data to store when processing response from origin server, in KB. When the HTTP Response Policy is applied, HTTP Proxy uses this value to determine the biggest response data size to be stored while sending the response to client. When the limit is reached, HTTP Proxy stops reading from the server socket until space is freed after some data sent to client.

6 Click the **Save** icon.

7 Expand **HTTP Response Policy**.

8 Expand the HTTP Response Policy you added.

9 Click **Service Rule**.

10 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the HTTP Response Policy.

  The Service Rule must already exist. See Service Rule.

  The Service Rule must contain an HTTP Rule Group.

11 Click the **Save** icon.

12 Repeat step 9 through step 11 to add as many Service Rules as needed.

IP Flow

Configure one or more IP Flows to be processed by Multi Protocol Proxy.

To steer traffic destined to an explicit proxy address, configured the HTTP IP Flow with a Service Rule containing a Packet Filter with matching destination IP and destination port values.

To add an Multi Protocol Proxy IP Flow:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **IP Flow**.

4 Configure the parameters as follows:

Table 10-275 IP Flow Parameters

Parameter	Description
Name	IP Flow name
Admin State	Enable/Disable IP Flow: ■ disabled ■ enabled
Priority	IP Flow priority

Table 10-275 IP Flow Parameters

Parameter	Description
Protocol	HTTP transport protocol for the IP Flow: ■ HTTP ■ HTTPS ■ TCP ■ UDP TCP splicing provides the ability to enable TCP optimization for TCP-based protocols such as SFTP, FTP and HTTPS. The TCP splicing stitches the client and server TCP connections, enabling the Operator to configure the TCP parameters to be used for the client connections separately. MCC can be configured as a TCP splicing and support the following: ■ Terminate a TCP connection from the client and apply a set of TCP optimization parameters. ■ Originate a TCP connection to the server and apply a set of TCP optimization parameters. ■ Forward TCP traffic between the client and server TCP connections without parsing or disturbing the packets. ■ Teardown the TCP connections when the peer closes the sockets or idle exceeded timeou.t
IP Transparency	Enable/Disable IP Transparency for the IP Flow: ■ disabled ■ enabled When IP Transparency is enabled, HTTP requests forwarded by the HTTP Proxy to origin servers contain the UE's original IP address as the source TCP/IP address in the IP packet. IP transparent proxy is an HTTP proxy mode of operation where HTTP client IP addresses (UE addresses) are used as a source when originating network-side connections to Web origin servers. HTTP proxy, using the client addresses, hides its own network identity and becomes IP transparent to Internet origin servers. When IP transparency is used, origin servers are able to determine the identity of Web clients based on the source IP addresses of the HTTP/HTTPS connections. In non-IP Transparent mode, HTTP proxy uses MCC IP loopback addresses when originating network-side connections.
Application Detection	Enable/Disable Application Detection for the IP Flow: ■ disabled ■ enabled

Table 10-275 IP Flow Parameters

Parameter	Description
Proxy Bypass	Enable/Disable proxy bypass for the IP Flow: ■ disabled ■ enabled Configure the bypassed IP Flow object with a higher priority than the non-bypassed IP Flow object.
HTTP Request Policy	Select the HTTP Request Policies to bind to the IP flow. The HTTP Request Policy must already exist. See HTTP Request Policy. To add additional HTTP Request Policies, click the **Create** icon.
HTTP Response Policy	Select the HTTP Response Policies to bind to the IP flow. The HTTP Response Policy must already exist. See HTTP Response Policy. To add additional HTTP Response Policies, click the **Create** icon.
Service Rule	Select the Service Rule The Service Rule must already exist. See Service Rule. **Notes:** The Service Rule *cannot* contain an HTTP Rule Group. The Service Rule *cannot* contain a Protocol Application Rule Group, if the protocol is configured as HTTP. Protocol Application Rule Group applies to TCP and UDP traffic only and is not supported for HTTP. The Service Rule *can* contain an Domain Rule Group. Such a configuration could use DNS proxy reverse cache to match up an incoming IP with the hostname, and only divert transactions for certain hostname to proxy. To add additional Service Rules, click the **Create** icon.
TCP Splicing Policy	Select the TCP Splicing Policy The TCP Splicing Policy must already exist. See TCP Splicing Policy. To add additional TCP Splicing Policies, click the **Create** icon.
UDP Policy	Select the UDP Policy The UDP Policy must already exist. See UDP Policy. To add additional UDP Policies, click the **Create** icon.

5 Click the **Save** icon.

Multi Protocol Proxy Instance

To add a Multi Protocol Proxy Instance:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **Instance**.

4 Configure the parameters as follows:

Table 10-276 Multi Protocol Proxy Instance Parameters

Parameter	Description
Name	Multi Protocol Proxy Instance name
Admin State	Enable/Disable Multi Protocol Proxy instance: ■ disabled ■ enabled
TCP Optimization Service	Select the TCP optimization service The TCP optimization service must already exist. See TCP Optimization Profile.
Encryption Profile	Select the Encryption Profile The Encryption Profile must already exist. See Encryption Profile.
MMSC Group	Select the Multimedia Messaging Service Center group. The MMSC group must already exist. See Multimedia Messaging Service Center Group.
SMSC Group	Select the Short Message Service group. The SMSC group must already exist. See Short Message Service Center Group.
LDAP Profile	Select the LDAP Profile. The LDAP Profile must already exist. See LDAP Profile.
UA Profile	Select the User Agent Profile. The UA Profile must already exist. See UA Profile.
Fraud Detection Profile	Select the Fraud Detection Profile. The Fraud Detection Profile must already exist. See Fraud Detection Profile.
Explicit Proxy Profile	Select the Explicit Proxy Profile. The Explicit Proxy Profile must already exist. See Explicit Proxy Profile.

Table 10-276 Multi Protocol Proxy Instance Parameters

Parameter	Description
ABR Opting Mode	Specifies the ABR opting modes for the subscriber: ■ opt-out – HTTP/HTTPS/QUIC ABR video rate limiting is applied unless the NOABR string is received in the acwhttppolicy Vendor-Specific Attribute (VSA) from the PCRF Gx interface. ■ opt-in – HTTP/HTTPS/QUIC ABR video rate limiting is not applied unless the ABR string is received in the acwhttppolicy Vendor-Specific Attribute (VSA) from the PCRF Gx interface.
HTTPS Profile	Select the HTTPS Profile. The HTTPS Profile must already exist. See HTTPS Profile.
TCP Traffic Control Profile	Select the TCP Traffic Control Profile. The Traffic Control Profile must already exist. See Traffic Control Profile.
HTTP Transaction Record Profile	Select the HTTP Transaction Record Profile The HTTP Transaction Record Profile must already exist. See HTTP Transaction Record Profile.
Toll Free Profile	Select the Toll Free Profile The Toll Free Profile must already exist. See Toll Free Profile.
ABR Optimization Profile	Select the ABR Optimization Profile The ABR Optimization Profile must already exist. See ABR Optimization Profile.
UDP Traffic Control Profile	Select the UDP Traffic Control Profile. The Traffic Control Profile must already exist. See Traffic Control Profile.
TCP Measurement:	
Admin State	Enable/Disable TCP measurement: ■ disabled ■ enabled - MCC calculates the TCP performance parameters for the specified sampling frequency for both uplink and downlink connections
Sampling Interval	TCP measurement sampling interval, in milliseconds
Mild Congestion Level	Mild congestion level for applying optimization (throughput in kbps)
Moderate Congestion Level	Moderate congestion level for applying optimization (throughput in kbps)
Severe Congestion Level	Severe congestion level for applying optimization (throughput in kbps)

Table 10-276 Multi Protocol Proxy Instance Parameters

Parameter	Description
Server Connections:	
Network Context Override	Network Context used for server connections. It overrides the Network Context selected by the gateway subsystem.
TCP Optimization Profile	TCP Optimization Profile to use for server connections. The TCP Optimization Profile must already exist. See TCP Optimization Profile.
Loopback IP List	Loopback IP List for server connections. The Loopback IP List must already exist. See Loopback IP List.
Loopback Selection Algorithm	Specifies the loopback selection algorithm: ■ round-robin – Selects a loopback IP from a Loopback IP List in a round-robin fashion for connections initiated to HTTP origin servers ■ session sticky – Uses the same loopback IP for all connections for a given session
IP Family Preference	Specifies the preferred server connection IP family: ■ IPv4 – Requests both IPv4 and IPv6 server addresses and uses the IPv4 address unless it is unavailable. ■ IPv6 – Rquests both IPv4 and IPv6 server addresses and uses the IPv6 address unless it is unavailable. ■ client-ip-family – Requests both IPv4 and IPv6 server addresses and uses the client-ip-family address unless it is unavailable.
IP Flow	Select the IP Flow(s) The IP Flow must already exist. See IP Flow. To add additional IP Flows, click the **Create** icon.

5 Click the **Save** icon.

ABR Optimization Profile

Use this object to configure an ABR rate limiting optimization profile.

To add an ABR Optimization Profile:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **ABR Optimization Profile**.

4 Configure the parameters as follows:

Table 10-277 ABR Optimization Profile Parameters

Parameter	Description
Name	Optimization Profile name
Admin State	Enable/Disable the Profile: ■ disabled ■ enabled
Burst Size	Rate limiting burst size
Burst Size Unit	Burst size unit : ■ bytes ■ kbytes ■ mbytes ■ gbytes
Secondary Segment Threshold	Minimum segment threshold for bypassing secondary rate-limiting
Secondary Segment Threshold Unit	Secondary segment threshold unit: ■ bytes ■ kbytes ■ mbytes
Bitrate	Rate limiting bitrate
Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Secondary Segment Bitrate	Rate limiting bitrate (bits per second) for secondary segments.
Secondary Segment Bitrate Unit	Bitrate unit: ■ bps ■ kbps ■ mbps ■ gbps
Savings Estimation Admin State	Enable/Disable estimation of optimization byte savings attributed to ABR pacing. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on content: ■ disabled ■ enabled
Sampling Interval	Sampling interval for savings estimation

Table 10-277 ABR Optimization Profile Parameters

Parameter	Description
Sampling Interval Unit	Sampling interval unit: ■ min ■ hr

5 Click the **Save** icon.

Client Connections

Use this object to configure Multi Protocol Proxy client connection parameters.

To configure client connections:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **Client Connections**.

4 Configure the parameters as follows:

Request Wait Time – Configure the client connection HTTP request wait time in milliseconds (value 0 indicates forever). Reverse hand-off is implemented and if the HTTP request is found, it is handed back to the Multi Protocol Proxy and continues to process as HTTP traffic.

5 Click the **Save** icon.

Back End Forwarding

Use this object to enable forwarding of HTTP requests between CSM modules. Back end forwarding uses content cache in a distributed mode to achieve better cache hit rates.

To enable/disable back end forwarding:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **Back End Forwarding**.

4 Configure the parameters as follows:

- **Admin State** – Select Enabled to enable back end forwarding.
- **Max Idle Connections** – Configure the maximum number of idle connections per back end proxy.

5 Click the **Save** icon.

Encryption Profile

The Encryption Profile is used in HHE to determine the algorithm and keys to be used for header encryption.

The Encryption Profile stores encryption algorithm information and keys depending on the algorithm configured by the Operator. MCC generates a random IV and includes this as an extra header in each encrypted header. MCC supports a key in hex format (without spaces).

MCC supports the AES-128/192/256-CBC encryption algorithm and Base64 and Hex encoding for the encrypted value.

To add an Encryption Profile:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click Encryption **Profile**.
4. Configure the parameters as follows:

Table 10-278 Encryption Profile Parameters

Parameter	Description
Name	Encryption Profile name
Admin State	Enable/Disable Encryption Profile: ■ disabled ■ enabled
Public Key Filename	The name of the public key file to be used for MSISDN encryption. The file should be placed in /tosdb/content/publickeys.
Type	Type of public key file: ■ PEM ■ DER ■ X509

5. Click the **Save** icon.

Explicit Proxy Profile

Use this object to configure an explicit proxy address profile.

To add an Explicit Proxy Address Profile:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **Explicit Proxy Profile**.
4. Configure the parameters as follows:
   - **Name** – Specify an explicit proxy profile name.
5. Click the **Save** icon.
6. Expand the Explicit Proxy Profile you added.
7. To configure the network context and address list, click **Explicit Proxy Networkcontext**.
8. Configure the parameters as follows:
   - **Network Context** – Specify the network context to use for the explicit proxy address list.
9. Click the **Save** icon.
10. Expand the network context you specified.
11. Click **Explicit Proxy Address**.
12. Configure the parameters as follows:

Table 10-279 Explicit Proxy Address Parameters

Parameter	Description
Name	Name of the explicit proxy address list
IP Address	IP Address
Port	Port

13. Click the **Save** icon.

Fraud Detection Profile

Use this object to enable the gateway to detect and take a configured action on subscriber devices attempting data connections through fraudulent use of a web proxy. For example, the system can detect fraudulent users utilizing rogue HTTP proxies to spoof HTTP URLs for free rated sites, such as those the Carrier assigns for browsing promotions and partnerships.

To configure Fraud Detection Profile:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **Fraud Detection Profile**.
4. Configure the parameters as follows:

Table 10-280 Fraud Detection Profile Parameters

Parameter	Description
Name	Fraud Detection Profile name.
Admin State	Enable/disable the Fraud Detection service: ■ enabled ■ disabled
Action	Action to take when fraud is detected: ■ allow ■ block
Block Notification Message	*Applies when Action is set to block:* HTTP Request Block Message used in the '403 forbidden' response sent to the client.
Service Rule	Service Rule to apply to the Fraud Detection Profile. The Service Rule specifies which requests to subject to the fraud check. For example, to apply the fraud check only to free rated websites for browsing promotions and partnerships, configure the Service Rule with the list of free-rated domains. If the fraud detection Service Rule is not configured, fraud checks are performed for *all* HTTP requests. The Service Rule must already exist. See Service Rule. To add additional Service Rules, click the **Create** icon.
Whitelist	Whitelist to apply to the Fraud Detection Profile. The Whitelist contains the IP addresses that represent legitimate proxies. The Whitelist must already exist. See Host List. To add additional Whitelists, click the **Create** icon.

5 Click the **Save** icon.

HTTP Transaction Record Profile

HTTP Transaction Data Records provides information about each HTTP transaction that traverses the NE. The data is represented in comma-separated values format (CSV) and written as a string of CSV values.

The HTTP Transaction Data record can include such information as:

- Time information: Request timestamp and latency information
- Subscriber information: IMSI, MSISDN, etc.
- Connection information: Network context, source and destination address, etc.
- Request information: HTTP request information
- Response information: HTTP response information
- Compression information: Compression and bytes saved, if compression is applied
- Web image Optimization information: Information about web image optimization and bytes saved, if applied.
- Video information: Information about any video served and bytes saved, if applied.
- Minification information: Information about minification and bytes saved, if applied.

The Operator can customize the records in certain positions and can include or omit certain records. Configure the following values in the Service Construct > Data Record Template > Multi Protocol Proxy > HTTP Transaction:

- *Present Flag* – Indicates whether to include the data field in the CDR. By default, this value is set to conditional for all data fields, indicating that the data field will be filled in CDRs when available.
- *Position Index* – Location of the data field in the CDR. A pre-defined order exists for each data field if positionIndex is not configured.
- *Format Type* – The format for the data field. If not configured, the format type uses the default.
- *Length* – The fixed length of the data field. The length defaults to zero indicating the data field is written out as it is.

- *Alignment* – The alignment of the data field. If not configured, the alignment defaults to left aligned.
- *Padding* – The character used for padding when the field has a fixed length.

HTTP Transaction Data Records information can be used to:

- Calculate details, such as bandwidth savings when features like Web Image Optimization and video adaptation are enabled.
- Provide the basis for charging
- Measure analytics

Specify the HTTP transaction record profile in an Multi Protocol Proxy instance tied to the workflow for it to take effect.

To configure HTTP Transaction Record Profile:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **HTTP Transaction Record Profile**.
4. Configure the parameters as follows:

Table 10-281 HTTP Transaction Record Profile Parameters

Parameter	Description
Name	HTTP Transaction Data Record profile name
File Type	File type for streaming HTDR record locally: ■ Event Log ■ Data Record ■ Core Files ■ RAM Disk-Storage ■ Storage ■ Ext-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming HTDR record locally
Encode Format	Format type: ■ CSV
Record URL Length	Length to which the URL field should be truncated in the record

Table 10-281 HTTP Transaction Record Profile Parameters

Parameter	Description
Transaction Template	HTTP Transaction Record Template. Configure at Service Construct > Data Record Template > Multi Protocol Proxy > HTTP Transaction

5 Click the **Save** icon.

HTTPS Profile

Use this object to enable HTTP Proxy support for HTTPS (HTTP Secure) - an HTTP protocol variant that uses secure TLS, rather than TCP, connections for communication with clients and/or servers.

MCC HTTP Proxy supports the following HTTPS features:

- HTTPS termination of client TLS connections
- HTTPS origination of TLS connections to HTTPS servers
- HTTPS pass-through

When HTTP Proxy is used to terminate clients' TLS connections to HTTPS servers, the HTTPS Profile must include TLS Termination Policies for the servers. Once terminated, HTTP Proxy decrypts and processes user HTTPS requests and applies enabled content features.

When HTTP Proxy is used to originate HTTPS server connections, server authentication is performed using a list of trusted CA certificates configured in the HTTPS Profile.

HTTPS traffic for which no TLS Termination Policy is configured bypasses HTTP Proxy logic and is passed-through between the client and server. Because the HTTPS pass-through traffic is not processed by HTTP-Proxy, content features are not applied to HTTP requests on these connections. However, connection-level features such as TCP Optimization are supported.

To add an HTTPS Profile:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **HTTPS Profile**.

4 Configure the parameters as follows:

Table 10-282 HTTPS Profile Parameters

Parameter	Description
Name	HTTPS Profile name
Admin State	Admin state: ■ enabled ■ disable
Ca Certificate List	HTTPS Origination CA certificate list The Ca Certificate List must already exist. See CA Certificate List.
TLS Protocol Logging	Enable debug logging for openssl when this HTTPS Profile is used: ■ enabled ■ disable

5 Click the **Save** icon.

6 Expand **HTTPS Profile**.

7 Expand the HTTPS Profile you added.

8 Click **TLS Termination Policy**.

9 Configure the parameters as follows:

- **Name** – Enter the TLS Termination Policy name. The TLS Termination Policy must already exist. See TLS Termination Policy.

10 Click the **Save** icon.

11 Repeat step 8 through step 10 to add as many TLS Termination Policy as needed.

Long Term Mobile ID

Use this object to configure a Long Term Mobile ID (LTMI). It supports insertion of encrypted subscriber ID in an HTTP request header to allow the subscriber ID to be communicated to origin server in a secure manner.

MCC supports the following levels of encoding/encryption formats:

- Plain Text
- LTMI Static Trusted
- LTMI dynamic Trusted
- LTMI External

Operators can opt out of the LTMI feature using the Opt Out String and Static Trusted ID String.

MCC supports the following text string VSAs used to generate LTMI and the reseller ID header. The VSAs are retrieved from the PCRF when a call is established, and delivered to the HTTP Proxy when an HTTP request header is processed.

- subID
- miDial
- resellerID

Using HTTPS, the MCC periodically downloads encryption keys from a key server. The keys can be manually imported using import LTMI key or automatically imported from the key server by configuring the minute interval using key-import-interval.

To add a long term mobile ID:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **LTMI**.
4. Configure the parameters as follows:

Table 10-283 LTMI Parameters

Parameter	Description
The following parameters control the key import (download) from the key server using HTTPS:	
Key Import Interval	Key import interval, in minutes, zero turns off key import
Key Server URL	Network Context used for non-HTTP connections. It overrides the Network Context selected by a higher-level object.
Key Server Username	Key Server username for basic authentication.

Table 10-283 LTMI Parameters

Parameter	Description
Key Server Password	Key Server password for basic authentication.
Key Server Network Context	Key server network context
Loopback IP List	Key Server Loopback IP List. The Loopback IP List must already exist. Create it at Network Context > Loopback IP List. LTMI download chooses the loopback from Loopback IP List if it is configured.
The following parameters control if and how the LTMI ID is generated:	
ID Gen Admin State	Enable/Disable LTMI ID generation: ■ enabled ■ disable
Trusted ID Divisor	Number of minutes for trusted ID rotation interval (for example, 6 months rotation = 259,200 minutes)
External ID Divisor	Number of minutes for external ID rotation interval (for example, 24 hour rotation = 1440 minutes.
Network Carrier Code	Code used in dynamic mobile IDs to identify the carrier.
Opt Out String	String used to search the opt out value to see if a subscriber has opted out of Dynamic Mobile ID. When a subscriber opts out this feature, no LTMI is inserted in the HTTP request header. If the miDial string exactly matches the Opt Out String, then the subscriber completely opts out of LTMI.
Static Trusted ID String	Ending of the search string used to identify opt out value for static trusted ID. If the miDial string ends with the Static Trusted ID String, then the Static Trusted ID is used instead of the Dynamic Trusted ID. For example, if the Static Trusted ID String is configured as "#" and the miDail string is "xyz#" (ending with "#"), then the Static Trusted ID is used instead of the Dynamic Trusted ID.
Extra Curl Option	Passes additional option to the curl command used to download the LTMI key.

5 Click the **Save** icon.

LTMI Import History

Use this object to view import history of long term mobile ID keys.

To view LTMI import history:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Expand **LTMI Key**.
4. Expand **Import History**.
5. Click an instance.

LTMI import history parameters are:

- Import Time
- Import Result: Success or N/A
- Import File Size
- Number Of Accepted Entries
- Number Of Rejected Entries
- Import File Name
- Import Type: manual or scheduled

LTMI Key Status

Use this object to view status of long term mobile ID keys.

To view LTMI key status:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Expand **LTMI Key**.
4. Expand **Status**.
5. Click an instance.

LTMI key status parameters are:

- Last Import Time
- Last Import Result
- Last Import Type
- Last Import Number
- Last Import File Size (Bytes)
- Next Scheduled Import Time
- Number Of Entries

- Accepted Entries
- Import URL

Minify

Use this object to enable minification for Javascript, CSS, or HTML. Minification removes unnecessary characters (such as blank characters and new line characters) from source code, thereby reducing the amount of data that needs to be transferred.

To enable Minification:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **Minify**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable minification.
5. Click the **Save** icon.

Optimization Overload Control

Use this object to enable Proxy Optimization Overload Control that adds logic to a proxy task to bypass some images or videos to prevent the system from being overloaded.

To enable Optimization Overload Control:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **Optimization Overload Control**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable Optimization Overload Control.
5. Click the **Save** icon.

Preemptive DNS

Use this object to replace the URLs in the response with the IP address of one of the Affirmed Networks Gi local loopback addresses and configured DNS Token before sending to the client.

To configure HTTP preemptive DNS:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.

3 Click **Preemptive DNS**.

4 Configure the parameters as follows:

Table 10-284 Preemptive DNS Parameters

Parameter	Description
Admin State	Admin state: ■ enabled ■ disable
Token	String token used to replace URLs in HTTP Response.
Network Context	Network Context used to select Loopback IP address
Loopback IP v4	v4 loopback IP address to be used to replace URLs in HTTP response
Loopback IP v6	v6 loopback IP address to be used to replace URLs in HTTP response

5 Click the **Save** icon.

Server Connections

To configure Multi Protocol Proxy server connections:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **Server Connections**.

4 Configure the parameters as follows:

Table 10-285 Server Connections Parameters

Parameter	Description
Idle Timeout	Server connection idle timeout, in seconds.
Max Server Idle	Maximum number of idle connections per server.
Max Total Idle	Total maximum number of idle server connections. Value 0 disables keeping idle connections.
HTTP Fast Open	Mark the checkbox to enable HTTP Fast Open. When enabled, the MCC proxy opens a server connection during the client connection handshake, which reduces the HTTP transaction time by approximately one Round Trip Time (RTT) between the UE and MCC proxy.

5 Click the **Save** icon.

Steering Group

Use this object to configure a group of Steering Destinations.

To add a Steering Group:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **Steering Group**.
4. Configure the parameters as follows:
   - **Name**: Steering Group name.
   - **Health Check Profile**: Health Check Profile for the Steering Destination. The Health Check Profile must already exist. See Health Check Profile.
5. Click the **Save** icon.
6. To configure a steering destination for the group, expand the Steering Group you added.
7. Click **Steering Destination**.
8. Configure the parameters as follows:

Table 10-286 Steering Destination Parameters

Parameter	Description
Name	HTTP Steering Destination Name
IP Address	IP address for Steering Destination
Port	Port for Steering Destination Port
Host Name	Host Name (FQDN) of the Steering Destination
Network Context Override	Configure Network Context to use for Steering Destination
Priority	Configure Steering priority

9. Click the **Save** icon.
10. Repeat step 7 through step 9 to add as many steering destinations as needed.

TCP Splicing

Use this object to configure HTTPS Fast Open. When enabled, the MCC proxy opens a server connection during the client connection handshake, which reduces the HTTPS transaction time by approximately one Round Trip Time (RTT) between the UE and MCC proxy.

To configure HTTPS Fast Open:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **TCP Splicing**.
4. Configure the parameters as follows:
   - **Server Connection Fast Open** – Mark the checkbox to turn on TCP server connection fast open.
5. Click the **Save** icon.

TCP Splicing Policy

Use this object to configure a policy that controls the behavior of the TCP connections that match an HTTP IP Flow. The matched traffic is forwarded to a TCP splicing component and spliced to the server.

To configure a TCP Splicing Policy:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **TCP Splicing Policy**.
4. Configure the parameters as follows:

Table 10-287 TCP Splicing Policy Parameters

Parameter	Description
Name	Content TCP Splicing Policy Name
Priority	Priority of the TCP Splicing Policy, must be unique
Traffic Control Profile	Traffic Control Profile associated with this policy. The Traffic Control Profile must already exist. See Traffic Control Profile.

5. Click the **Save** icon.
6. Expand the policy you added.
7. Click **Service Rule**.
8. Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the TCP Splicing Policy.

  The Service Rule must already exist. See Service Rule.

9 Click the **Save** icon.

Toll Free Profile

Use this object to configure a toll free profile to support Toll Free Data (TFD). TFD is a feature in which a third-party (content provider) pays for a subscriber's data usage when the subscriber is downloading or using the third-party company's Apps, Websites, and services. If a toll free profile is enabled, TFD is turned on for that proxy instance.

To configure a toll free profile:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **Toll Free Profile**.

4 Configure the parameters as follows:

- **Name** – Enter a profile name.
- **Admin State** – Select Enabled to enable the profile.

5 Click the **Save** icon.

6 To configure a certificate server, expand the profile you added.

7 Click **Certificate Server**.

8 Configure the parameters as follows:

Table 10-288 Certificate Server Parameters

Parameter	Description
CA Certificate List	CA root certificate. The CA certificate must first be placed in */public/content/tls/cacerts* before it can be configured. The Ca Certificate List must already exist. See CA Certificate List.
Certificate URL	URL prefix for certificates (for example, http://certificateserver/)
Certificate File Extension	Certificate file extension

Table 10-288 Certificate Server Parameters

Parameter	Description
CRL URL	URL for Certificate Revocation List (string starting with http://) When toll-free-data manifest is received before Certificate Revocation List (CRL) is available to the MCC, the manifest is processed. After parsing and signature verification, the manifest is installed into the subscriber service profile. The manifest, using revoked content provider certificate, is only removed when the UE triggers a manifest refresh (re-downloads the manifest again).
Network Context	Network context for accessing the certificate server
Loopback IP	Loopback interface for accessing the certificate server

9 Click the **Save** icon.

10 To configure a data record, click **Data Record Configuration**.

11 Configure the parameters as follows:

Table 10-289 Data Record Configuration Parameters

Parameter	Description
File Type	File type for streaming the Toll Free Data record locally: ■ Event Log ■ Data Record ■ Cores Files ■ Storage ■ Ext-Storage ■ RAM Disk-Storage ■ PSM ■ Tech-Support ■ Other
File Name	File name for streaming the Toll Free Data record locally The file must already exist. Create it at Infrastructure > File Management > Profile (of type datarecord).
TFD Template	Toll Free Data record template The record template must already exist. Create it at Service Construct > Data Record Template > Multi Protocol Proxy > Toll Free Data.

12 Click the **Save** icon.

13 To configure toll free header names, click **TF Header Names**.

14 Configure the parameters as follows:

Table 10-290 TF Header Names Parameters

Parameter	Description
TF Manifest Indication	Header name for toll free manifest indication
TF Manifest ID	Header name for toll free manifest ID
TF Eligible	Header name for toll free eligible
TF Access	Header name for toll free access
TF Status	Header name for toll free status
TF SID	Header name for toll free sponsor ID
TF Callback URL	Header name for toll free callback URL

15 Click the **Save** icon.

Traffic Control Profile

Use this object to configure a profile for handling of splicing traffic (data forwarding between client and server TCP connections).

Multi Protocol Proxy supports forwarding of non-HTTP traffic received on port 80. The TCP splicing component of Multi Protocol Proxy is responsible for handling of non-HTTP traffic. The component maintains a pair of client-side and server-side connections and forwards data between these connections.

To configure a Traffic Control Profile:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **Traffic Control Profile**.

4 Configure the parameters as follows:

Table 10-291 Traffic Control Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Network Context Override	Network Context used for the Traffic Control Profile. It overrides the Network Context selected by a higher-level object.
Loopback IP List	Loopback IP list for splicing server connections

Table 10-291 Traffic Control Profile Parameters

Parameter	Description
Steering Group	Configure the Steering Destinations to use for this profile. The Steering Group allows the UDP flow to be steered to the destination configured within itself, when the profile is selected. In the packet processing, after UDP policies are evaluated, the associated traffic-control-profile is selected. The steering group within the profile can have multiple steering-destinations. A round-robin approach is used between destinations. In case of a single steering-destination, the current UDP flow is steered to that destination. The Steering Destinations must already exist. See Steering Group.
Toll Free Data	Mark the checkbox to indicate that toll free data applies for this profile.
Upstream Buffering Limit	Maximum data to store when processing upstream data, in KB.
Downstream Buffering Limit	Maximum data to store when processing downstream data, in KB.
Segment Threshold	Segment threshold in bytes for bypassing rate-limiting.
Rate Limiting:	
Admin State	Admin state: ■ enabled ■ disable
Burst Size	Burst size
Burst Size Units	Burst size units: ■ bytes ■ kbytes ■ mbytes ■ gbytes
Bitrate	Bitrate
Bitrate Units	Bitrate units: ■ bps ■ kbps ■ mbps ■ gbps

Table 10-291 Traffic Control Profile Parameters

Parameter	Description
Savings Estimation:	
Admin State	Admin state: estimation of optimization byte savings attributed to rate-limited HTTPS video traffic. When enabled, MCC logs performance statistics and provides an estimate of savings obtained by enforcing rate-limiting on video sessions: ■ enabled ■ disable
Sampling Interval	Sampling interval for savings estimation
Sampling Interval Unit	Unit for sampling interval for savings estimation: ■ min ■ hr

5 Click the **Save** icon.

UDP

Use this object to configure a profile for handling UDP Proxy. It enables Operators to selectively apply rate limiting to Quick UDP Internet Connection (QUIC) protocol flows. This feature complies with Google's Quic Version 39.

To configure a UDP:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Click **UDP**.

4 Configure the parameters as follows:

Table 10-292 UDP Parameters

Parameter	Description
Quic Rate Limiting	Specifies whether to enable QUIC rate limiting ■ enabled ■ disable
Idle Timeout	UDP Splicing idle timeout, in seconds.
Quic Reset Timeout	QUIC reset timeout, in seconds.

5 Click the **Save** icon.

UDP Policy

Use this object to configure a UDP Policy.

To configure a UDP Policy:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **UDP Policy**.
4. Configure the parameters as follows:

Table 10-293 UDP Policy Parameters

Parameter	Description
Name	UDP Policy name
Priority	Priority of the UDP policy, must be unique
Traffic Control Profile	Traffic Control Profile associated with this policy. The Traffic Control Profile must already exist. See Traffic Control Profile.
Congestion Control	Type of Congestion Control: ■ head-drop ■ tail-drop

5. Click the **Save** icon.

Video Pacing

Use this object to configure video pacing. Video pacing is sending video data to the client at a restricted rate. The video is not completely streamed at the fastest possible rate, instead it is throttled.

To configure video pacing:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **Video Pacing**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable video pacing.
5. Click the **Save** icon.

In addition, configure the following parameters in the HTTP Response Policy (see HTTP Response Policy):

- **Video Pacing Burst Time** represents the time for which the video data should be sent at a burst.
- **Video Pacing Factor** represents the factor at which the video should be paced.

Web Image Optimization Profile

Use this object to configure an Multi Protocol Proxy Web Image Optimization Profile that defines image compression and transcoding to produce a large gain in bandwidth savings for the Operator.

The profile specifies image conversion parameters such as re-compression, metadata, quality, percentage, and size. For example, you can configure the predicted size savings percentage threshold that can be optimized, such as a target JPEG quality between 0 (coarsest) and 100 (finest quantization). You associate a Web Image Optimization Profile with an HTTP Request Policy.

To add a Web Image Optimization Profile:

1. Expand **Services** in the tree.
2. Expand **Multi Protocol Proxy**.
3. Click **Web Image Optimization**.
4. Configure the parameters as follows:
   - **Admin State** – Select Enabled to enable web image optimization.
5. Click the **Save** icon.
6. Expand **Web Image Optimization**.
7. Click **Profile**.
8. Configure the parameters as follows:

Table 10-294 Web Image Optimization Profile Parameters

Parameter	Description
Name	Web Image Optimization Profile name
Convert PNG to JPEG	Mark the checkbox to allow conversion of PNG to JPEG.
Convert GIF to PNG	Mark the checkbox to allow conversion of GIF to PNG.
Convert GIF to JPEG	Mark the checkbox to allow conversion of GIF to JPEG.
Sample JPEG to 420	Mark the checkbox to allow 4:2:0 chroma subsampling of JPEG.
Interlace Image	Mark the checkbox to allow interlace image
Quantize Image	Mark the checkbox to allow requantization of palettized image.
Resize Image	Mark the checkbox to allow resizing of image.

Table 10-294 Web Image Optimization Profile Parameters

Parameter	Description
Remove Metadata	Mark the checkbox to allow removal of image metadata.
Target JPEG Quality	Target JPEG quality, with 0 being the coarsest quantization, and 100 being the finest quantization.
Target Max Size	Target maximum size (in KB) that can be optimized.
Source Min Size	Source minimum size (in KB) that can be optimized.
Size Saving Threshold	Predicted size saving percentage threshold that can be optimized.
Source Max Size	Source maximum size (in KB) that can be optimized.

9 Click the **Save** icon.

Service Data Flow

Use this object to view each service data flow that is evaluated on each Multi Protocol Proxy during flow classification, in order of evaluation.

To view service data flow:

1 Expand **Services** in the tree.

2 Expand **Multi Protocol Proxy**.

3 Expand **Service Data Flow**.

4 Click an instance.

Service data flow parameters are:

- Multi Protocol Proxy
- Http Ip Flow Priority
- Service Rule Priority
- Http Ip Flow
- Service Rule
- Http Ip Flow Id
- Service Rule Id

Quality of Service

QoS Flow

The QoS Flow service allows for service data flow-level rate enforcement. You can link service rule(s) to the QoS Flow to specify the actions to take on traffic that matches at least one of its service rules. For example, you can limit the amount of ICMP traffic to specified uplink and/or downlink rates. QCI/ARP values are compared to the default bearer to determine if a dedicated bearer is required.

To add a QoS Flow:

1. Expand **Services** in the tree.
2. Expand **Quality of Service**.
3. Click **QoS Flow**.
4. Configure the parameters as follows:

Table 10-295 QoS Flow Parameters

Parameter	Description
Name	QoS Flow name
Admin State	Admin State: ■ enabled ■ disabled
Rate Measurement Units	Measurement Unit: ■ kbps ■ mbps ■ gbps
Uplink MBR	Uplink Maximum Bit Rate
Downlink MBR	Downlink Maximum Bit Rate
Uplink GBR	Uplink Guaranteed Bit Rate
Downlink GBR	Downlink Guaranteed Bit Rate
Uplink Max Burst	Uplink Max Burst, in Kbytes
Uplink Guaranteed Burst	Uplink Guaranteed Burst, in Kbytes
Downlink Max Burst	Downlink Max Burst, in Kbytes
Downlink Guaranteed Burst	Downlink Guaranteed Burst, in Kbytes

Table 10-295 QoS Flow Parameters

Parameter	Description
Qci	***Note:*** *Applies when Bearer Control is set to Network Initiated or User Initiated.* QoS Class Identifier: ■ 1: Operator controlled Voice Calling ■ 2: Operator controlled Video Calling ■ 3: Operator controlled Real-time Gaming ■ 4: Operator controlled Streaming of Pre-recorded Video ■ 5: Signaling for Operator controlled applications ■ 6: Websites prioritized by Operator ■ 7: Operator controlled Live Video Streaming or Interactive Gaming ■ 8: All other traffic for premium subscriber ■ 9: All other traffic for regular subscribe
Arp	***Note:*** *Applies when Bearer Control is set to Network Initiated or User Initiated.* Allocation and Retention Policy Higher values are preferred.
Gate	Gate: ■ Block ■ Pass ■ Pass Upstream ■ Pass Downstream
Priority	QoS Flow Priority. This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Bearer Control	Specifies the Bearer Control: ■ Network Initiated ■ User Initiated ■ Default Bearer
DSCP	Optional flow-level override to bearer QCI/DSCP mapping (the DSCP derived from the bearer QCI).

Table 10-295 QoS Flow Parameters

Parameter	Description
Service Activation	Specifies when to use or skip the service flow for packet classification: ■ always on - always use this service flow for classification ■ external activation - use the activation state of the service flow to determine whether to use or skip the service flow for packet classification. This setting allows the Gateway to dynamically activate/deactivate Rating Groups.
Aggregate QoS Flow	Specifies whether this QoS Flow is an aggregate flow: ■ true ■ false

5 In **Service Rule**, configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the QoS Flow.

  The Service Rule must already exist. See Service Rule.

To add additional Service Rules, click the **Create** icon.

6 Click the **Save** icon.

QoS Policy

The QoS Policy defines the QoS to be given to a list of QoS Flows, each of which can be prioritized.

To add a QoS Policy:

1 Expand **Services** in the tree.

2 Expand **Quality of Service**.

3 Click **QoS Policy**.

4 Configure the parameters as follows:

Table 10-296 QoS Policy Parameters

Parameter	Description
Name	QoS Policy name
Admin State	Admin State: ■ enabled ■ disabled
Package Id	Policy instance in the AAA server

Table 10-296 QoS Policy Parameters

Parameter	Description
Priority Evaluation Mode	Priority Evaluation Mode: ■ flat - Use Service Rule priority (ignore QoS Flow priority). To make a match, examine all of the Service Rules on all of the QoS Flows for best priority. ■ flat-with-pcc-rule-precedence - Any PCC rules in effect have their precedence values compared with the Service Rule priority values, and the PCC rule or Service Rule with the highest priority (lowest numerical value) is selected. ■ hierarchical - Use QoS Flow priority and Service Rule priority hierarchically. To make a match, examine the QoS Flows in priority order and within each of them, examine the Service Rules in priority order.
Dscp Replacement Mode	Allows the mapping of the DSCP value in the IPv4/6 header of an egress packet to a configurable 802.1Q VLAN priority. The DSCP value can be replaced in either the outer IP header or in both the inner and outer IP header: ■ outer: replaces the dscp value in only the outer IP header ■ both: replaces the dscp value in both the inner and outer IP header
Aggregate QoS Policy	Specifies whether this QoS Policy is an aggregate policy: ■ true ■ false

5 In **Geo Redundant Group**, configure the parameters as follows:

- **Name** – Select the Geographic Redundancy Group to associate with the QoS Policy.

  The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.

To add additional Geographic Redundancy Groups, click the **Create** icon.

6 In **Qci Dscp Map**, configure the parameters as follows:

Table 10-297 Qci Dscp Map Parameters

Parameter	Description
Qci	QoS Class Identifier: ■ 1: Operator controlled Voice Calling ■ 2: Operator controlled Video Calling ■ 3: Operator controlled Real-time Gaming ■ 4: Operator controlled Streaming of Pre-recorded Video ■ 5: Signaling for Operator controlled applications ■ 6: Websites prioritized by Operator ■ 7: Operator controlled Live Video Streaming or Interactive Gaming ■ 8: All other traffic for premium subscriber ■ 9: All other traffic for regular subscriber
Dscp	Select the Differentiated Services Code Point Map.

To add additional Qci Dscp Maps, click the **Create** icon.

7 In **Qos Flow**, configure the parameters as follows:

- **Name** – Select the QoS Flow to associate with the QoS Policy.

  The QoS Flow must already exist. See QoS Flow.

- **Fraud QoS** — Set to true to designate this QoS Flow for handling of fraudulent activity within this QoS Policy.

To add additional QoS Flows, click the **Create** icon.

8 Click the **Save** icon.

Service Data Flow

Use this object to view each service data flow that is evaluated on each QoS policy during flow classification, in order of evaluation.

To view service data flow:

1 Expand **Services** in the tree.

2 Expand **Quality of Service**.

3 Expand **Service Data Flow**.

4 Click an instance.

Service data flow parameters are:

- Qos Policy
- Qos Flow Priority
- Service Rule Priority
- Qos Flow
- Service Rule
- Qos Flow Id
- Service Rule Id

Rate Limiting Subscriber Group

Use this object to configure a group of subscribers whose traffic is rate-limited to a configured aggregate QoS Policy. When the aggregate usage of all the users in the group exceeds the configured limits, the packets from these users are dropped.

To add a Rate Limiting Subscriber Group:

1. Expand **Services** in the tree.
2. Click **Rate Limiting Subscriber Group**.
3. Configure the parameters as follows:

Table 10-298 Rate Limiting Subscriber Group Parameters

Parameter	Description
Subscriber Group	Subscriber Group. The Subscriber Group must already exist. Configure it Subscriber Group.
QoS Policy	The QoS policy to associate with the Subscriber Group. The QoS Policy must already exist with **Aggregate QoS Policy** set to true. Configure it at QoS Policy.

4. Click the **Save** icon.

SMTP Proxy

Use this object to configure an Simple Mail Transfer Protocol proxy instance for handling SMTP traffic.

To add a SMTP Proxy instance:

1. Expand **Services** in the tree.
2. Expand **SMTP Proxy**.
3. Click **Instance**.
4. Configure the parameters as follows:

Table 10-299 SMTP Proxy Instance Parameters

Parameter	Description
Name	Content SMTP Proxy instance name
Admin State	Admin state: ■ enabled ■ disable
Mms Mm3	MMS MM3 Instance associated with the HTTP Server Instance. The MMS MM3 instance must already exist. See MM3 Profile.

5. Click the **Save** icon.
6. To configure the Network Context and Loopback address to use for SMTP Proxy instance, expand **Instance**.
7. Expand the Instance you added.
8. Click **Network Context**.
9. Configure the parameters as follows:

Table 10-300 Network Context Parameters

Parameter	Description
Network Context	Select the Network Context.
Loopback IP	Loopback IP Address
Loopback Port	Loopback IP Port

10. Click the **Save** icon.

Steering Service

The Steering Service allows the normal routing of a packet to be overridden for upstream subscriber traffic based on the configured Steering Policy.

Steering allows upstream subscriber traffic to be force-routed to a specific next hop or into a specific tunnel. Steering is compatible with NAT, as an upstream packet can be source NAT'd and steered. Steering is subservient to the Multi Protocol Proxy and its dependent services – if the packet is to be proxied, steering is ignored.

Steering can be based on any of the inputs present on the Service Rule:

- L3/4 Packet Filter
- Time of Day Rule Group
- DPI Protocol Application Rule Group
- L7 HTTP Rule Group

Note: *The Steering Service does not support steering into IPSec tunnels.*

Steering Flow

The Steering Flow service allows for upstream subscriber traffic steering. You can link service rule(s) to the Steering Flow to specify the actions to take on traffic that matches at least one of its service rules.

To add a Steering Flow:

1. Expand **Services** in the tree.
2. Expand **Steering Service**.
3. Click **Steering Flow**.
4. Configure the parameters as follows:

Table 10-301 Steering Flow Parameters

Parameter	Description
Name	Steering Flow name
Admin State	Admin State: ■ enabled ■ disabled

Table 10-301 Steering Flow Parameters

Parameter	Description
Priority	Steering Flow Priority. This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
Network Context	***Note:*** *Applies when* ***Action*** *is set to Steering.* Network Context of the tunnel or next hop on which upstream traffic is to be sent.
Tunnel	***Note:*** *Applies when* ***Action*** *is set to Steering.* Name of the tunnel or next hop on which upstream traffic is to be sent.
Action	Action to take for this steering flow: ■ steering ■ no steering ■ nc-steering: Steers traffic to an auxiliary network context.

5 Click the **Save** icon.

6 Expand the Steering Flow you added.

7 Click **Service Rule**.

8 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the Steering Flow.

  The Service Rule must already exist. See Service Rule.

9 Click the **Save** icon.

10 Repeat step 7 through step 9 to add as many Service Rules as needed.

Steering Policy

To add a Steering Policy:

1. Expand **Services** in the tree.
2. Expand **Steering Service**.
3. Click **Steering Policy**.
4. Configure the parameters as follows:

Table 10-302 Steering Policy Parameters

Parameter	Description
Name	Steering Policy name
Admin State	Admin State: ■ enabled ■ disabled

5. In **Steering Flow**, configure the parameters as follows:
   - **Name** – Select the Steering Flow to associate with the Steering Policy.

     The Steering Flow must already exist. See Steering Flow.

   To add additional Steering Flows, click the **Create** icon.
6. Click the **Save** icon.

Service Data Flow

Use this object to view each service data flow that is evaluated on each steering policy during flow classification, in order of evaluation.

To view service data flow:

1. Expand **Services** in the tree.
2. Expand **Steering**.
3. Expand **Service Data Flow**.
4. Click an instance.

   Service data flow parameters are:

   - Steering Policy
   - Steering Flow Priority
   - Service Rule Priority
   - Steering Flow

- Service Rule
- Steering Flow Id
- Service Rule Id

Subscriber Firewall

Subscriber Firewall Flow

The Subscriber Firewall flow allows differentiated Network Address and Port Translation treatment of multiple classified traffic flows. Network Address and Port Translation is used to map private UE IP addresses to a limited pool of public IP addresses. For example, certain traffic can be mapped to public addresses from one particular NAT pool, other traffic may be mapped to another NAT pool, and some traffic may not be mapped at all.

To add a Subscriber Firewall Flow:

1. Expand **Services** in the tree.
2. Expand **Subscriber Firewall**.
3. Click **Subscriber Firewall Flow**.
4. Configure the parameters as follows:

Table 10-303 Subscriber Firewall Flow Parameters

Parameter	Description
Name	Subscriber Firewall Flow name
Admin State	Admin state: ■ enabled ■ disable
Priority	Subscriber Firewall Flow priority This value resolves conflicts in the case of multiple service instances. Priority is hierarchical: the priority of the higher-level object takes precedence over the lower-level object.
NAT Pool	NAT Pool associated with this Subscriber Firewall Flow. The NAT pool must already exist. Create it at Network Context > *name* > Nat Pool.
Action	Action to apply: ■ NAT: Apply Network Address and Port Translation treatment (default) ■ Pass ■ Drop

Table 10-303 Subscriber Firewall Flow Parameters

Parameter	Description
ALG	ALG application: ■ FTP ■ RTCP ■ SIP ■ TFTP
Flow Auth	Enables flow authorization on the subscriber firewall flow: ■ enabled ■ disable Applies only when **Action** is set to NAT.
NAT Flow Filter Mode	NAT Flow Filter Mode: ■ address-dependent – Filtering mode wherein downlink traffic from [A:*] on nat [ip:port] is accepted if UE has active uplink connection to [A:*] via [ip:port] ■ address-port-dependent – Filtering mode wherein downlink traffic from [A:a] on nat [ip:port] is accepted if UE has active uplink connection to [A:a] via [ip:port] ■ endpoint-independent – Filtering mode wherein downlink traffic from [*:*] on nat [ip:port] is accepted if UE has active uplink connection to any [*:*] via [ip:port] ■ not-set ***Note:*** *By default, the filtering mode configured on the NAT Pool is applied for this flow. If this parameter is set, it overrides the NAT Pool setting. Set this parameter only to use a different filtering mode for this flow.*
NAT Flow Binding Time	Timer (in seconds) to persist NAT address/port bindings even after connection close is initiated. ***Note:*** *MCC keeps the address mapping binding (NAT'ed IP) persistent for this timer period by keeping the connection object alive even after the data connection is deleted. This helps in reusing the same NAT'ed IP for the connections, if the connection returns within the nat-binding-time period. However, setting this timer puts strain on resources.*

5 Click the **Save** icon.

6 Expand **Subscriber Firewall Flow**.

7 Expand the Subscriber Firewall Flow you added.

8 Click **Service Rule**.

9 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the Subscriber Firewall Flow.

  The Service Rule must already exist. See Service Rule.

10 Click the **Save** icon.

11 Repeat step 8 through step 10 to add as many Service Rules as needed.

Subscriber Firewall Policy

Subscriber Firewall Policy binds one or more (prioritized) Subscriber Firewall flows and defines the NAT treatment to be applied when associated with a workflow data profile (or service flow).

To add a Subscriber Firewall Policy:

1 Expand **Services** in the tree.

2 Expand **Subscriber Firewall**.

3 Click **Subscriber Firewall Policy**.

4 Configure the parameters as follows:

Table 10-304 Subscriber Firewall Policy Parameters

Parameter	Description
Name	Subscriber Firewall Policy name
Admin State	Admin state: ■ enabled ■ disable
Subscriber Firewall Flow	Select the Subscriber Firewall Flow(s) to bind with the Subscriber Firewall Policy The Subscriber Firewall Flow must already exist. See Subscriber Firewall Flow. To add additional Subscriber Firewall Flows, click the **Create** icon.

5 Click the **Save** icon.

Service Data Flow

Use this object to view each service data flow that is evaluated on each subscriber firewall policy during flow classification, in order of evaluation.

To view service data flow:

1 Expand **Services** in the tree.

2 Expand **Subscriber Firewall**.

3 Expand **Service Data Flow**.

4 Click an instance.

Service data flow parameters are:

- Subscriber Firewall Policy
- Subscriber Firewall Flow Policy
- Service Rule Priority
- Subscriber Firewall Flow
- Service Rule
- Subscriber Firewall Flow Id
- Service Rule Id

ALG Packet Statistics

Use this object to view the number of control packets processed by each ALG.

To view ALG Packet Statistics:

1. Expand **Services** in the tree.
2. Expand **Subscriber Firewall**.
3. Expand **ALG Packet Statistics**.
4. Click an ALG instance.

ALG Packet statistics are:

- NAT ALG Upstream Packets: Number of Upstream NAT packets classified as ALG
- NAT ALG Downstream Packets: Number of Downstream NAT packets classified as ALG
- Pass ALG Upstream Packets: Number of Upstream packets classified as ALG
- Pass ALG Downstream Packets: Number of Downstream packets classified as ALG

Video Adaptation (MCC versions prior to 8.2)

Acuitas does not support this object for MCC 8.2 and later releases.

Video Adaptation Service

Use this object to configure video adaptation services.

To enable a video adaptation service, the HTTP Proxy service must be enabled.

A video adaptation service is applied to HTTP traffic for a subscriber workflow when the following conditions are met:

- Subscriber workflow has an associated video adaptation instance
- Content is video
- Content Cache service is enabled

The system supports the following target container types and source <=> target combinations.

Offline Transcoding	Online Transcoding
■ MP4 <=> FLV ■ MP4 => MP4 ■ FLV => FLV ■ WebM => WebM	■ MP4 => MP4 ■ FLV => FLV ■ WebM => WebM

Note: *Video pacing and online and offline transcoding is not supported for range requests, including those received from the server categorized as follows:*

HTTP Response status 206 “Partial Content”
HTTP Response status 200 “OK” that includes a “Range” header
HTTP Response status 200 “OK” to an HTTP Request that includes a range specification in the URI

The system supports five QoE grades and resolutions per container type. It supports the following video-adaptation profiles for MP4, FLV, and WebM container types:

Supported Container Type	Media Container	Values					
MP4, FLV, WebM	QoE Grade	0	1	2	3	4	5
MP4, FLV, WebM	Max Video Height	180	240	360	480	720	1080
MP4, FLV, WebM	Max Video Width	320	428	640	854	1280	1920
MP4, FLV, WebM	Max Video Frame Rate	30	30	30	30	30	30
MP4, FLV, WebM	Pref Video Bitrate Type	333	442	748	1179	2407	5172
MP4, FLV	Pref Video Codec	h264	h264	h264	h264	h264	h264
WebM		vp8	vp8	vp8	vp8	vp8	vp8
MP4, FLV	Video Profile	main	main	main	main	main	main
WebM		N/A	N/A	N/A	N/A	N/A	N/A

To add a Video Adaptation Service:

1. Expand **Services** in the tree.
2. Click **Video Adaptation**.
3. Configure the parameters as follows:

Table 10-305 Video Adaptation Service Parameters

Parameter	Description
Admin State	Admin State of the Video Adaptation service for both offline and online transcoding: ■ enabled ■ disabled

4. Click the **Save** icon.

Video Adaptation Instance

Use this object to specify the video adaptation instance.

The following instance guidelines apply:

- Each instance has a maximum QoE. The system uses the QoE under the serving policy if there is a match instead of the QoE under instance.
- The instance supports a transcoding policy for online transcoding. Multiple service rules can be configured to the policy.
- If the optional media container is not specified, the system uses the original content type.
- For offline transcoding:
  - If no service rule is configured under the serving policy, the system uses the original content.
  - If the requested container type does not exist in the cache, the system uses the original content from the origin server or cache.

To add a Video Adaptation Instance:

1. Expand **Services** in the tree.
2. Expand **Video Adaptation**.
3. Click **Instance**.
4. Configure the parameters as follows:
   - **Name** – Enter a Video Adaptation name.
   - **Max Qoe Grade** – Enter the maximum quality of experience grade allowed for both offline and online transcoding (0-5).

     Streaming bitrates for Quality of Experience (QoE) are as follows:
     - QoE 0: Less than 333 kbps
     - QoE 1: From 333 to 442 kbps
     - QoE 2: From 442 to 748 kbps
     - QoE 3: From 748 to 1179 kbps
     - QoE 4: From 1179 to 2407 kbps
     - QoE 5: From 2407 to 5179 kbps

5 In **Offline Transcoding**, configure the parameters as follows:

Table 10-306 Offline Transcoding Parameters

Parameter	Description
Admin State	Enable/Disable Video Adaptation Service Offline Transcoding: ■ enabled ■ disable
Serving Policy	Select the Offline Serving Policy used to serve adapted videos to clients. The Offline Serving Policy must already exist. See Offline Transcoding Policy. To add additional Offline Serving Policies, click the **Create** icon.

6 In **Online Transcoding**, configure the parameters as follows:

Table 10-307 Online Transcoding Parameters

Parameter	Description
Admin State	Enable/Disable Video Adaptation Service Offline Transcoding: ■ enabled ■ disable
Transcoding Policy	Select the Online Transcoding Policy. The Transcoding Policy must already exist. See Online Transcoding Policy. To add additional Online Transcoding Policies, click the **Create** icon.

7 Click the **Save** icon.

Offline Transcoding Policy

Offline transcoding caches the original video from the origin server and transcodes the video into different QoE grades and multiple container types. The system serves the video to the user from the cache when subsequent requests are made for the same video. Transcoded videos are served as they are completed, rather than waiting for all QoE grades to complete.

To add an Offline Transcoding Policy:

1 Expand **Services** in the tree.

2 Expand **Video Adaptation**.

3 Click **Offline Transcoding**.

4 Configure the parameters as follows:

Table 10-308 Offline Transcoding Parameters

Parameter	Description
Cache Min Hit	Minimum number of hits for a cached object to be eligible for transcoding.
Cache Min Lifetime	Minimum remaining lifetime of a cached object to be eligible for transcoding, in seconds.

5 Click the **Save** icon.

6 To configure the Serving Policy used to serve adapted videos to clients, expand **Offline Transcoding**.

7 Click **Serving Policy**.

8 Configure the parameters as follows:

Table 10-309 Serving Policy Parameters

Parameter	Description
Name	Serving Policy name
Admin State	Enable/Disable Serving Policy: ■ enabled ■ disable
Priority	Enter the Priority
Container Type	Select the target media container type serving to clients: ■ FLV ■ MP4 ■ WebM
QoE Grade	Select the serving quality of experience grade (0-5).

9 Click the **Save** icon.

10 To configure the service rule associated with this Serving Policy, expand the Serving Policy you added.

11 Click **Service Rule**.

12 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the Serving Policy.

  The Service Rule must already exist. See Service Rule.

13 Click the **Save** icon.

14 To configure the offline Transcoding Policy used to transcode cached videos, click **Transcoding Policy**.

15 Configure the parameters as follows:

Table 10-310 Transcoding Policy Parameters

Parameter	Description
Name	Transcoding Policy name
Admin State	Enable/Disable Offline Transcoding Policy: ■ enabled ■ disable
Priority	Enter the Priority
Transcoding Rule	Select the Transcoding Rule. The Transcoding Rule must already exist. See Transcoding Rule.
Target Container Types	You can configure up to three target container types. Select the target container type: ■ FLV ■ MP4 ■ WebM

16 Click the **Save** icon.

Online Transcoding Policy

Online transcoding is used to compress video contents in real-time when video is playing back from a user's device. The original data is decoded and then encoded into a target format with a lower QoE grade.

To add an Online Transcoding Policy:

1 Expand **Services** in the tree.

2 Expand **Video Adaptation**.

3 Expand **Online Transcoding**.

4 Click **Transcoding Policy**.

5 Configure the parameters as follows:

Table 10-311 Transcoding Policy Parameters

Parameter	Description
Name	Serving Policy name

Table 10-311 Transcoding Policy Parameters

Parameter	Description
Admin State	Enable/Disable Online Transcoding Policy: ■ enabled ■ disable
Priority	Enter the Priority
Max QoE Grade	Select the maximum quality of experience grade allowed (0-5).
Transcoding Rule	Select the Transcoding Rule. The Transcoding Rule must already exist. See Transcoding Rule.
Speed Level	Select the transcoding speed level: ■ Slow ■ Medium ■ Fast
Transcoding Map	The transcoding map associated with this policy. The Transcoding Map must already exist. See Transcoding Map.

6 Click the **Save** icon.

7 To configure the service rule associated with this Transcoding Policy, expand the Transcoding Policy you added.

8 Click **Service Rule**.

9 Configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the Transcoding Policy.

  The Service Rule must already exist. See Service Rule.

10 Click the **Save** icon.

Target Media Profile

This object defines the set of media encoding parameters to be applied for transcoding a cached object. Video adaptation service can be provisioned to support up to 18 Target Media Profiles.

Note: *In this release, profiles are pre-configured and cannot be modified.*

To view a Target Media Profile:

1 Expand **Services** in the tree.

2 Expand **Video Adaptation**.

3 Expand **Target Media Profile**.

4 Click a profile.

Target Media Profile parameters are listed in the following table:

Target Media Profile Parameters

Parameter	Description
Media Container	Video adaptation media profile media container
QoE Grade	Maximum quality of experience grade allowed
Max Video Height	Maximum video resolution height
Max Video Width	Maximum video resolution width
Max Video Frame Rate	Maximum video frames per second
Target Data Rate	Target A/V media data rate (kbps)
Pref Video Codec	Preferred target video codec
Pref Audio Codec	Preferred target audio codec
Pref Video Bitrate Type	Preferred Video Bitrate Type: ■ CBR ■ VBR
GOP Duration	Group of pictures duration, in seconds

Transcoding Map

The transcoding map enables Operators to adjust the parameters of the target video based on the characteristics of the source video. When the transcoding map is configured, it is used by OTF (on-the-fly) video transcoder instead of the QoE profile. The transcoding map is passed from the HTTP proxy layer to the intermediate OTF library. The OTF library is responsible for communicating with the lower-level streaming transcoder layer that uses these abstract parameters to derive a set of tangible parameters for use in the transcoding process.

Note: *If the transcoding instance has both transcoding map and QoE defined, transcoding map takes priority and QoE is used if the source mapping does not match.*

To add a Transcoding Map:

1. Expand **Services** in the tree.
2. Expand **Video Adaptation**.
3. Click **Transcoding Map**.
4. Configure the parameters as follows:
   - **Name** – Enter a name for the Transcoding Map.
5. Click the **Save** icon.
6. Expand the Transcoding Map you added.
7. Click **Entry**.
8. Configure the parameters as follows:

Table 10-312 Transcoding Map Entry Parameters

Parameter	Description
Name	Transcoding Map entry name
Priority	Enter the Priority. Must be unique.
Container Types	Source containers on which the matching is performed. You can configure up to three source container types. Select the target container type: ■ FLV ■ MP4 ■ WebM
Source Audio Sampling Rate in KHz	
Min	Min value of the source audio sampling rate in KHz. Configuring only the minimum value indicates that any value greater than or equal to that rate would match.
Max	Max value of the source audio sampling rate in KHz.
Source Bitrate in bits-per-second	
Min	Min bitrate value in bits per second. Configuring only the minimum value indicates that any value greater than or equal to that rate would match.
Max	Max bitrate value in bits per second.
Source Frame Rate	
Min	Lower bound value. Configuring only the lower bound value indicates that any value greater than or equal to that rate would match.
Max	Upper bound value.

Table 10-312 Transcoding Map Entry Parameters

Parameter	Description
Resolution	
Max Width	Maximum width value for resolution
Max Height	Maximum height value for resolution
Min Width	Minimum width value for resolution
Min Height	Minimum height value for resolution
Target: target parameters to which to transcode. *Configure the target parameters as percentages of the source parameters. The lower layers use the percentage value to compute the actual used values. The target parameters define the maximum allowable values. The actual value may be the maximum value or lower.*	
Max Audio Sampling Rate	Maximum target (less than or equal to) value for audio sampling rate in KHz.
Min Audio Channel Count	Maximum number of allowed audio channels in the target video. ■ monoaural ■ stereo
Bypass	Bypasses transcoding: ■ True: all other parameters are ignored and source parameter transcoding is bypassed ■ False
Target Bitrate of the target video	
Max or Percentage	Bitrate as maximum or percentage: ■ max-bitrate: Maximum (Lesser than or equal to) value for bitrate in bits-per-second. Configure as a maximum value indicating that the target bitrate does not exceed the given amount. ■ percentage-bitrate: Target bitrate as a percentage (of the source) values. Configure as a percentage value, indicating the percentage of the source bitrate.
Bitrate Value	Maximum or percentage value
Target Frame Rate of the target video	

Table 10-312 Transcoding Map Entry Parameters

Parameter	Description
Max or Percentage	Bitrate as maximum or percentage: ■ max-framerate: Maximum value for frame rate. Configure as a maximum value indicating that the target framerate does not exceed the given amount. If the target frame rate is not configured or exceeds the origianl frame rate, the original frame rate is used. ■ percentage-framerate: Target frame rate as a percentage (of the source) frame rate. Configure as a percentage value, indicating the percentage of the source framerate. If the target frame rate is not configured, the original frame rate is used.
Frame Rate Value	Maximum or percentage value
Target Resolution of the target video	
Max or Percentage	Resolution as maximum or percentage: ■ max: Maximum height/width value ■ percentage-resolution: Target resolution as a percentage (of the source) resolution.
Max Width	Maximum (Lesser than or equal to) width value for resolution
Max Height	Maximum (Lesser than or equal to) height value for resolution
Percentage Resolution	Target resolution as a percentage (of the source) resolution

9 Click the **Save** icon.

Transcoding Rule

Use this object to configure a rule to be eligible for transcoding.

To add a Transcoding Rule:

1 Expand **Services** in the tree.

2 Expand **Video Adaptation**.

3 Click **Transcoding Rule**.

4 Configure the parameters as follows:

Table 10-313 Transcoding Rule Parameters

Parameter	Description
Name	Transcoding rule name
Max Object Size	Maximum object size to be eligible for transcoding, in kbytes.

Table 10-313 Transcoding Rule Parameters

Parameter	Description
Min Object Size	Minimum object size to be eligible for transcoding, in kbytes.
Max Duration	Maximum duration to be eligible for transcoding, in seconds.
Min Duration	Minimum duration to be eligible for transcoding, in seconds.
Max Bitrate	Maximum bitrate to be eligible for transcoding, in bits per second.
Max Framerate	Maximum frame rate to be eligible for transcoding.
Source Container Types	You can configure up to three source container types. Select the target container type: ■ FLV ■ MP4 ■ WebM
Min Savings Threshold	Minimum saving s bitrate threshold to be elible for transcoding, in percentage.

5 Click the **Save** icon.

WAP Gateway

WAP Gateway Service Instance

Use this object to configure a Wireless Application Protocol Gateway Service instance. The WAP Gateway processes WAP requests and translates them to HTTP requests.

Note: *The WAP Gateway includes software developed by the Kannel Group (http://www.kannel.org/).*
==========
The Kannel Software License, Version 1.0

Copyright (c) 2001-2012 Kannel Group
Copyright (c) 1998-2001 WapIT Ltd.
All rights reserved.

To add a WAP Gateway Service Instance:

1 Expand **Services** in the tree.

2 Expand **WAP Gateway**.

3 Click **Instance**.

4 Configure the parameters as follows:

Table 10-314 WAP Gateway Instance Parameters

Parameter	Description
Name	WAP Gateway Service instance name
Admin State	Admin state: ■ enabled ■ disable

5 In **WAP IP Flow**, configure the parameters as follows:

- **Name** – Select the WAP IP Flow to associate with the WAP Gateway.

  The WAP IP Flow must already exist. See WAP Gateway IP Flow.

  To add additional WAP IP Flows, click the **Create** icon.

6 To configure Wireless Transport Layer Security, in **WTLS**, configure the parameters as follows:

Table 10-315 WTLS Parameters

Parameter	Description
Admin State	Admin state: ■ enabled ■ disable
Gateway Certificate	Enter the gateway certificate file name
Gateway Key	Enter the gateway private key file name

7 Click the **Save** icon.

WAP Gateway IP Flow

Use this object to configure a Wireless Application Protocol Gateway Service IP Flow.

To add a WAP Gateway IP Flow:

1 Expand **Services** in the tree.

2 Expand **WAP Gateway**.

3 Click **WAP IP Flow**.

4 Configure the parameters as follows:

Table 10-316 WAP IP Flow Parameters

Parameter	Description
Name	WAP IP Flow name
Admin State	Admin state: ■ enabled ■ disable
Priority	WAP IP Flow priority This value resolves conflicts in the case of multiple service instances.

5 In **Service Rule**, configure the parameters as follows:

- **Name** – Select the Service Rule to associate with the WAP IP Flow.

  The Service Rule must already exist. See Service Rule.

  To add additional Service Rules, click the **Create** icon.

6 Click the **Save** icon.

Service Data Flow

Use this object to view each service data flow that is evaluated on each WAP Gateway during flow classification, in order of evaluation.

To view service data flow:

1 Expand **Services** in the tree.

2 Expand **WAP Gateway**.

3 Expand **Service Data Flow**.

4 Click an instance.

Service data flow parameters are:

- Wap Gateway
- Wap IP Flow Priority
- Service Rule Priority
- Wap Ip Flow
- Service Rule
- Wap Ip Flow Id
- Service Rule Id

SNMP

Use this object to configure Simple Network Management Protocol configuration.

To configure SNMP:

1. Expand **SNMP** in the tree.
2. Click **Community String**.
3. Configure the parameters as follows:
   - **Name**: SNMP community string.
4. Click the **Save** icon.
5. Click **Trap Target**.
6. Configure the parameters as follows:
   - **Name**: SNMP trap target.
7. Click the **Save** icon.

Use this object to configure user name and encryption policies for SNMPv3:

To configure user name and encryption policies for SNMPv3:

1. Expand **SNMP** in the tree.
2. Expand **V3**.
3. Expand **Community Entry**.
4. Click the community entry.
5. Configure the parameters as follows:

Table 10-317 Community Entry Parameters

Parameter	Description
Name	SNMP community string
Engine ID	SNMP entity

6. Click the **Save** icon.
7. Expand the community entry you added.
8. Click **User**.

9 Configure the parameters as follows:

Table 10-318 User Parameters

Parameter	Description
Security Name	SNMP security name
Security Password	SNMP security password
Security Type	Security Type: ■ noAuthnoPriv - Communication without authentication and privacy. ■ authNoPriv - Communication with authentication and without privacy. Protocols supported for Authentication are MD5 and SHA. ■ authPriv - Communication with authentication and privacy. Protocols supported for Authentication are MD5 and SHA. Protocols supported for Privacy are DES and AES.
Security Authentication Protocol	Security Authentication Protocol: ■ none ■ md5 ■ sha Value none is valid only when Security Type is noAuthnoPriv.
Security Privacy Protocol	Security Privacy Protocol: ■ none ■ des ■ aes Value none is valid only when Security Type is noAuthnoPriv or authNoPriv.

10 Click the **Save** icon.

System

To view system uptime:

1 Expand **System** in the tree.

2 Expand **Uptime**.

3 Click the system instance to display the system uptime in seconds.

TAM

Traffic Anchoring Mode (TAM) is a feature supported on existing VM types, specifically the Subscriber Services Module (SSM) and Integrated Services Module (ISM). This feature applies only to SSM/ISM VM personalities where I/O and workflow services are co-located. This feature adds TAM functionality to the MCC and CUPS platforms. TAM is used to reduce East-West traffic within an MCC or U-Plane cluster for SAEGW traffic. TAM is supported on a standalone PGW, standalone SGW, co-located PGW/SGW, and GGSN.

To configure TAM:

1. Expand **TAM** in the tree.
2. Click **Policy**.
3. Configure the parameters as follows:

Table 10-319 TAM Parameters

Object	Description
Mode	Configure cluster-wide TAM behavior. Options include: ■ disabled – Deactivate Traffic Anchoring Mode (TAM) on all SSMs/ISMs. ■ enabled-for-cluster – Activate Traffic Anchoring Mode (TAM) on all SSMS/ISMs with TAM profiles. TAM is active cluster-wide. The system rejects any session create request that does not map to the resources in one of the entries in the profile list. Only anchored traffic is supported. ***Note:*** *Changing the mode triggers an immediate cluster reboot.*

4. Click the **Save** icon.
5. Click **Profile**.
6. Configure the parameters as follows:

Table 10-320 TAM Profile Parameters

Object	Description
Cluster Id	The cluster where this profile will be anchored.
Node Slot	The node where this profile will be anchored. This is a reference to an SSM or ISM node object used to identify the VM in which traffic associated with the profile is anchored. The node must be unique across all profile rows. That is, a node can only be referenced by one profile.

7. Click the **Save** icon.

8 To configure a list of Loopback IP addresses anchored by this profile, expand the TAM Profile you added.

9 Click **Loopback IP**.

10 Configure the parameters as follows:

Table 10-321 Loopback IP Parameters

Object	Description
Network Context	Network Context containing the Loopback IP
Loopback IP	List of loopback IP addresses anchored by this profile. The Loopback IP must already exist. Create it at Network Context > *name* > Loopback IP.

11 Click the **Save** icon.

12 To configure a list of IP subpools anchored by this profile, expand the TAM Profile you added.

13 Click **IP Subpool**.

14 Configure the parameters as follows:

Table 10-322 TIP Subpool Parameters

Object	Description
Network Context	Network Context containing the IP subpool
IP Subpool	List of every IP Subpool that is anchored to the node. Adding or removing an IP Subpool when TAM is active immediately results in routing changes. The Loopback IP must already exist. Create it at Network Context > *name* > IP Sub Pool.

15 Click the **Save** icon.

16 To view the TAM statistics, expand **TAM Data Stats**.

17 Click an instance.

User Access

Use this object to use Terminal Access Controller Access Control System Plus (TACACS+) as an external authentication, authorization, and accounting server to manage user access to MCC devices. When users log in to MCC devices, an authentication request is sent to the TACACS+ server and the server either accepts or rejects the request based on information in its user database.

Upon successful authentication, the MCC device sends an authorization request to which the server responds with the user's group assignment (used to determine the commands to which the user has access). After the session is established, the system sends user accounting messages to the TACACS+ server, including session termination.

The MCC supports the following general TACACS+ features and functions when the Admin State is enabled:

- Supports the configuration of up to eight TACACS+ servers.
  - Network Elements are capable of specifying individual timeouts for each configured Access Control Server.
  - A global timeout value may be specified as a default when individual timeout values are not configurable for each Access Control Server.
- Supports TACACS+ server connection failure switchover after a fixed number of attempts.
- Supports a local authentication mechanism as fallback if no configured TACACS+ servers are accessible. The MCC supports the TACACS+ method as the primary method. When that method is unavailable, MCC uses local authentication.

In addition, you can issue a User Access command to enable users to disable CLI confirmation prompts (Default: enabled). This command applies only to the user that issues the command, and only disables prompts for the current session. It does not affect other users with the same username. Prompts are automatically re-enabled when the CLI session terminates.

To enable/disable confirmation prompts:

1. Click **User Access** in the tree.
2. Under **User Access Commands**, select **prompt-ackowledgement**.
3. Click **Select**.
4. Select the mode:
   - enabled
   - disabled
5. Click **Execute**.

To configure TACACS+ Management:

1. Expand **User Access** in the tree.
2. Expand **AAA**.
3. To configure a customized login banner, click **Admin**.
4. Configure the parameters as follows:
   - **Login Banner**: Enter the customized login banner to be displayed prior to displaying the password prompt.
5. Click the **Save** icon.
6. Expand **TACACS Plus**.
7. Click **Admin**.
8. Configure the parameters as follows:

Table 10-323 Admin Parameters

Parameter	Description
Admin State	Admin State of the TACACS+ service: ■ Enabled ■ Disabled
Failure Limit	Maximum number of failures before a server is skipped automatically. It limits the number of failed attempts (unreachable) before the server is considered down or unreachable. If a server is declared unreachable, the MCC does not attempt another AAA operation until the reattempt time has expired (see **Timers**).

9. Click the **Save** icon.
10. Click **Server**.
11. Configure the parameters as follows:

Table 10-324 TACACS+ Server Parameters

Parameter	Description
Priority	Priority of TACACS+ server to identify the order of authentication.
IP Address	IP address of the external TACACS+ server.
Port	You can configure up to eight TACACS+ servers to authenticate MCC users. Specify the priority of each server to identify the order of authentication.

Table 10-324 TACACS+ Server Parameters

Parameter	Description
Secret Key	The shared secret text string (secret key) used to authenticate the MCC device to a specific TACACS+ server. Specify a separate secret key for each TACACS+ server configured to use with MCC devices.
Timeout	Timeout for authentication
Authen Type	Authentication Type: ■ PAP ■ ASCII

12 Click the **Save** icon.

13 To configure accounting, click **Accounting**.

14 Configure the parameters as follows:

- **Mode**: Select local or remote.

15 Click the **Save** icon.

16 To filter accounting commands and groups, expand **Accounting**.

17 Click **Remote Exclude**.

18 The parameters are as follows:

Table 10-325 Remote Exclude Parameters

Parameter	Description
Groups	Groups to exclude from remote accounting: ■ admin ■ calea ■ content ■ readonly ■ user3g ■ user4g
Commands	Commands to exclude from remote accounting: ■ configure ■ show

19 To configure authentication, expand **Authentication**.

20 Click **Allow Local**.

21 Configure the parameters as follows:

Table 10-326 Allow Local Parameters

Parameter	Description
CLI Users	Local CLI users authentication mode: ■ fallback: local users are permitted to log in to the MCC if the TACACS+ server is configured and unreachable. A local account can be duplicated on the TACACS+ server but authentication is performed and decided by the remote server if it is reachable. If the remote server rejects the authentication, then the login fails. ■ always: local authentication is always attempted if the remote authentication fails.
Maint Users	Local maint users authentication mode: ■ fallback: local users are permitted to log in to the MCC if the TACACS+ server is configured and unreachable. A local account can be duplicated on the TACACS+ server but authentication is performed and decided by the remote server if it is reachable. If the remote server rejects the authentication, then the login fails. ■ always: local authentication is always attempted if the remote authentication fails.

22 Click the **Save** icon.

23 To configure accounting, click **Authorization**.

24 Configure the parameters as follows:

- **Mode**: Select local or remote.

25 Click the **Save** icon.

26 To filter authorization commands and groups, expand **Authorization**.

27 Click **Remote Exclude**.

28 The parameters are as follows:

Table 10-327 Remote Exclude Parameters

Parameter	Description
Groups	Groups to exclude from remote authorization: ■ admin ■ calea ■ content ■ readonly ■ user3g ■ user4g

Table 10-327 Remote Exclude Parameters

Parameter	Description
Commands	Commands to exclude from remote authorization: ■ configure ■ show

29 To configure re-attempt timers, click **Timers**.

30 Configure the parameters as follows:

Table 10-328 Timers Parameters

Parameter	Description
Reattempt Primary Aaa	Time (in seconds) to wait before the primary AAA method (TACACS+ if configured) is reattempted if it is considered down. MCC uses local authentication as a fallback until the timer expires. The TACACS+ service is considered down if none of the remote servers are reachable and the wait time is intended to prevent network thrashing until the issue is resolved. The MCC tries all the remote servers in a round-robin sequence based on priority.
Reattempt Server	Time (in seconds) before an individual timer is retried if it is down. After a server crosses the failure limit, it is considered down and is removed from the list of servers. The server is not retired until the reattempt time has elapsed.
Reattempt Primary Server	Time (in seconds) before the primary server is reattempted.

31 Click the **Save** icon.

32 To view the current status of the TACACS+ Servers, expand **Status**.

33 Click an instance.

vTap

Use this object to configure a subscriber vTap to replicate subscriber traffic for monitoring. The vTap specifies the subscriber session(s) that require a data tap. When a subscriber vTap is configured, all workflow sessions for the subscriber(s) are marked for tapping, and all the data traffic processed for that session are tapped.

To configure a subscriber vTap:

1. Expand **vTap** in the tree.
2. Click **Sink Config**.
3. Configure the parameters as follows:

Table 10-329 Sink Config Parameters

Parameter	Description
Name	Sink name
Type	Sink type: ■ GRE
Network Context	Network Context of the tunnel interface
Tunnel Name	Tunnel name

4. Click the **Save** icon.
5. To configure the fields to be included in the packet metadata sent to the destination, expand the sink you added.
6. Click **Packet Metadata**.
7. Configure the parameters as follows:

Table 10-330 Packet Metadata Parameters

Parameter	Description
Include IMSI	Specifies whether to include the IMSI in the packet metadata: ■ true ■ false
Include Timestamp	Specifies whether to include the timestamp in the packet metadata: ■ true ■ false

Table 10-330 Packet Metadata Parameters

Parameter	Description
Include EBI	Specifies whether to include the EBI in the packet metadata (if available): ■ true ■ false

8 Click the **Save** icon.

9 To configure a subscriber filter that defines the set of subscribers whose traffic is to be replicated, click **Subscriber Filter**.

10 Configure the parameters as follows:

- **Name**: Enter the subscriber filter name.

11 Click the **Save** icon.

12 To configure a list of analyzed keys, expand the subscriber filter you added.

13 Click **Key**. A key can have multiple attributes and all attributes specified in the key must match for a key to be considered matching. If any one key matches, the subscriber filter is considered matching:

14 Configure the parameters as follows:

Table 10-331 Key Parameters

Parameter	Description
Name	Keys name.
APN Name	APN name
IMSI List	List of International Mobile Subscriber Identity
MAC Address List	List of MAC addresses in common notation (with or without - or :)
NAI List	List of NAIs (Network Address Identifiers). Matching is performed after stripping any decoration (preceding a ! or :) from the received NAI
NAI Realm List	List of Network Address Identifier realms. Matches only the realm portion (after the @) of received NAIs. Provides a group matching capability like the IMSI range filter.

15 Click the **Save** icon.

16 To configure Key attributes, expand the Key you added.

17 Click the range you want to specify (**IMEI Range**, **IMSI Range**, **UE IP Range**).

18 Configure the parameters as follows:

Table 10-332 Range Parameters

Parameter	Description
Low	User equipment identifier or IP address start value
High	User equipment identifier or IP address end value

19 Click the **Save** icon.

20 To configure a subscriber vTap that specifies one or more subscriber filters, sinks, and reference points, click **Subscriber Tap Config**.

- When multiple subscriber filters are configured, a packet matches the subscriber vTap if it belongs to one of the sessions that match the configured filters.
- When multiple sinks are configured, the system replicates the matching packet and send to each sink.
- When multiple reference points are configured, the system copies the packet and sends it for each reference point.

21 Configure the parameters as follows:

Table 10-333 Subscriber Tap Parameters

Parameter	Description
Name	Subscriber vTap name
Admin State	Admin state of the subscriber vTap: ■ enabled ■ disabled
Requires External Activation	Specifies whether the subscriber vTap can be externally activated or deactivated by the **`vtap start`** and **`vtap stop`** commands: ■ yes ■ no The Admin State of a subscriber vTap must be enabled for this setting to take effect.

Table 10-333 Subscriber Tap Parameters

Parameter	Description
Reference Point	Reference point that specifies where to take a snapshot of the received subscriber packet: ■ access: Corresponds to the following interfaces: – S1-U interface in collated SGW/PGW deployments – S5/S8 interface for standalone PGW deployment – Gn interface for GGSN deployments ■ core: Corresponds to the following interfaces: – Sgi interface for standalone PGW or collocated SGW/PGW deployments – Gi interface for GGSN deployments ■ intermediate: Corresponds to the interface between gateway and proxy in deployments that use value-added services such as Multi Protocol Proxy or content filtering. ■ encrypted-access: Specifies that MCC should take a snapshot of the received subscriber packets before they are decrypted on ingress and after they are encrypted on egress. Corresponds to the following interface: – SWu interface in ePDG deployments To add additional Reference Points, click the **Create** icon.
Sink	vTap sink object To add additional Sinks, click the **Create** icon.
Subscriber Filter Set	vTap subscriber filter object To add additional Subscriber Filter Sets, click the **Create** icon.

22 Click the **Save** icon.

23 To view the sink statistics, expand **Sink Statistics**.

24 Click an instance.

25 To view the subscriber Tap statistics, expand **Subscriber Tap Statistics**.

26 Click an instance.

Workflow

Create a workflow that includes:

- **APN Mapping List** – Create an APN mapping list to provide additional granularity to Access Point Name mapping. It contains a list of APN values to be mapped to, based upon user-specific criteria. For example, it could use PAP username criteria to select a specific APN to use for the specific subscriber.
- **Control Profile** – Create a workflow control profile. Specify the back-end interfaces for charging, PCRF, authentication, and accounting.
- **Data Profile** – Create a workflow data profile that specifies the services to provide for the PDN session and controls resource utilization by the session. When the workflow is established, each associated subscriber's traffic flow is steered to the collection of associated services.
- **Data Profile Reselection Trigger Template** – Create a workflow data profile reselection trigger template that triggers a data profile switch and associates the template from the control profile. MCC switches the data profile by applying the subscriber analyzer selection based on RAT type. This feature supports switching of a data profile with and without PCRF on RAT change: This feature also supports 3GPP to non-3GPP handover and vice versa.
- **Subscriber Analyzer** – Bind the subscriber analyzer to the workflow control profile and to the workflow data profile.

Figure 10-12 Workflow Components

Note: *As an alternative procedure, use the Affirmed Open Workflow application to define workflow components. For instructions, see Affirmed Open Workflow.*

APN Mapping List

Use this object to provide additional granularity to APN mapping. It contains a list of APN values to be mapped to, based upon user-specific criteria. For example, it could use PAP username criteria to select a specific APN to use for the specific subscriber.

Note: *APN mapping is not supported for emergency APNs.*

To add an APN Mapping List:

1. Expand **Workflow** in the tree.
2. Click **Apn Mapping List**.
3. Configure the parameters as follows:

Table 10-334 APN Mapping List Parameters

Parameter	Description
Name	APN Mapping List name
User Description	Description of APN Mapping List

4. Click the **Save** icon.
5. Expand the APN Mapping List you added.
6. Click **Apn Mapping**.
7. Configure the parameters as follows:

Table 10-335 APN Mapping Parameters

Parameter	Description
Value	Specify to perform the classification using user@realm or just realm. For example, user1@internet.net or internet.net
User Description	Description of the specific APN Mapping.
Mapped Apn Name	The mapped APN to use. The APN must already exist. Create it at Zone > *name* > Gateway > APN.

8. Click the **Save** icon.

Control Profile

The Control Profile specifies the back-end interfaces for charging, PCRF, authentication, and accounting to be used for the workflow.

Note: *Dynamic selection of a Charging Instance via a RADIUS interface takes precedence over any Charging Instance specified in the Data Profile and Control Profile. For static selection of a Charging Instance, the Charging Instance specified in the Workflow Data Profile takes precedence over the Charging Instances specified in the Control Profile.*

To add a Control Profile:

1. Expand **Workflow** in the tree.
2. Click **Control Profile**.
3. Configure the parameters as follows:

Table 10-336 Workflow Control Profile Parameters

Parameter	Description
Name	Workflow Control Profile name
Default Accounting Interface	Default accounting interface (RADIUS/Diameter) ***Note:*** *Only accounting interfaces designated with an interface type of primary can be selected.*
Default Offline Interface 1	Default Offline Interface 1 (local/diameter)
Default Offline Interface 2	Default Offline Interface 2 (local/diameter)
Default Online Interface	Default Online Interface (local/diameter)
Default PCRF Interface	Default Policy and Charging and Rules Function interface.
Default Auth Interface	Default authorization interface.
Mapped APN Name	Mapped Access Point Name Use this parameter to map the generic APN to a specified APN so that external entities such as policy and charging servers can provide differentiated treatments. The APN must already exist. Create it at Zone > *name* > Gateway > APN.
Default Home Post Paid Charging Instance	Default postpaid charging service for the home PLMN. This charging instance must already exist. See Charging: Charging Instance.

Table 10-336 Workflow Control Profile Parameters

Parameter	Description
Default Roaming Post Paid Charging Instance	Default postpaid charging service for the visited PLMN. This charging instance must already exist. See Charging: Charging Instance.
Default Roaming Pre Paid Charging Instance	Default prepaid charging service for the visited PLMN. This charging instance must already exist. See Charging: Charging Instance.
Default Home Pre Paid Charging Instance	Default prepaid charging service for the home PLMN. This charging instance must already exist. See Charging: Charging Instance. ***Note:*** *Dynamic selection of a Charging Instance via a RADIUS interface takes precedence over this Charging Instance.*
Charging Characteristic	Charging characteristic per subscriber. This number could be one provisioned in each user's subscription data, per-APN, or for the entire profile at HSS. It is significant inside the user's home network. It can be used by the Operator to specify data as CDF address, OCS address, interim reporting interval/volume for on-line charging, tariff times, and so on.
Is OCS Enabled	Online charging enabled per subscriber: ■ true ■ false
Apn Reporting	APN to use when reporting APN to external devices: ■ original — Initial APN ■ mapped — Final / current APN ■ prior-mapped — APN mapped prior to the mapped (final / current) APN. This setting allows APN Reporting to continue to be based on the previously-mapped APN (even following a remap to a final APN) ■ custom — Customized Access Point Name (APN) reported on external interfaces. The customized APN is used in the Called-Station-ID AVP in messages in the external interfaces ***Note:*** *The APN Reporting value configured at the interface level overrides the APN Reporting value configured for the Control Profile. If the APN Reporting value is not configured at the interface level, the Called-Station-ID AVP and User-Name AVP will be filled based on the APN Reporting value configured for the Control Profile.*

Table 10-336 Workflow Control Profile Parameters

Parameter	Description
Custom Reporting APN Name	Customized APN sent in Called-Station-ID AVP in the external interfaces: ■ Access-Request on RADIUS interfaces ■ Accounting-Request on Gz and RADIUS interfaces ■ Credit-Control-Request (CCR) on Gx and Gy interface For Ga (GTPP) and local interfaces, the customized APN-reporting value is filled in the Access Point Name Network Identifier CDR field. Applies only when **APN Reporting** is set to custom.
Allow Dedicated Bearers	Controls whether subscribers can have dedicated bearers or secondary PDP contexts: ■ true ■ false
Default Tunnel Configuration	Default Tunnel configuration to use to bypass routing of egress traffic and force upstream packet into a pre-configured GRE tunnel referenced by a tunnel interface. The Tunnel must already exist. Create it at Network Context > *name* > Tunnel.
Ldap Interface Profile	LDAP Interface Profile to use. The LDAP Interface Profile must already exist. See LDAP Profile.
Apn Mapping List	APN list to use. The APN List must already exist. See APN Mapping List.
Apn Mapping Control	Control for mapping APN: ■ none – No APN mapping. Incoming APN is used. ■ explicit – Map to the APN specified by the **Mapped APN Name** field. ■ PAP username exclusive – Map APN using the Password Authentication Protocol (PAP) username received in PCO and **Apn Mapping List**. If it does not match, reject the call. ■ PAP username or explicit – Map APN using the Password Authentication Protocol (PAP) username received in PCO and **Apn Mapping List**, if possible. If it does not match, use to APN specified by the **Mapped APN Name** field. ■ External – Map APN using value received from external source (such as RADIUS or in mvnoId in case of Gx)
Apn Mapping Failure Behavior	GW behavior if APN remapping fails: ■ Use original – Allow the call using the original APN value ■ reject – Reject the call

Table 10-336 Workflow Control Profile Parameters

Parameter	Description
UE IP Allocation Mode	UE IP Allocation Mode: ■ Local-ue-ip-allocation – The UE IP assignment is managed locally on the system using local pools. ■ Radius-ue-ip-allocation – The UE IP allocation is managed from an external server (for both Framed IP behavior as well as for pool name based assignment) ■ Dhcp-relay-ue-ip-allocation – The UE IP is assigned/managed using a DHCP relay – with the UE acting as the DHCP client and the system learning the IP that the UE finally selects. The system manages a 'remote' UE pool to keep track of the DHCP assigned UE addresses. ■ Dhcp-client-ue-ip-allocation – The UE IP is assigned by the external DHCP server, however the system acts as a DHCP client and does the DHCP negotiation on behalf of the UE. ■ Lns-ip-allocation – The UE IP is assigned by LNS (L2TP Network Server) ■ S6-3gpp-aaa-ue-ip-allocation UE IP address allocation is managed as Framed-Pool, Framed-Ipv6-Pool, or Served-Party-Ip-Address allocation
Dhcp Local Server Admin Mode	DHCP local server admin mode (applies when **UE IP Allocation Mode** is set to local-ue-ip-allocation): ■ enabled ■ disabled
Dhcp Local Server Profile	DHCP local server to use (applies when **UE IP Allocation Mode** is set to local-ue-ip-allocation). The DHCP local Server Profile must already exist. See DHCP Local Server Profile.
Remote IP Alloc Fallback Option	Fallback Option to use if the RADIUS server does not allocate an IP address to a user requesting access (applies when **UE IP Allocation Mode** specifies to use RADIUS): ■ alloc-none – If the RADIUS server fails to send the Framed-Ip-Address attribute or IPv4/IPv6 pool names in the Access-Accept message, the GGSN/PGW rejects the call. ■ alloc-local-pool – If the RADIUS server fails to send the Framed-Ip-Address attribute or IPv4/IPv6 pool names in the Access-Accept message, the GGSN/PGW allocates the UE IP address from the local pool. ■ alloc-remote-pool – If the RADIUS server fails to send the Framed-Ip-Address attribute or IPv4/IPv6 pool names in the Access-Accept message, the GGSN/PGW allocates the UE IP address from the remote pool.
DHCP Service Profile	External DHCP server(s) to use (applies when **UE IP Allocation Mode** specifies to use a DHCP Relay Agent or DHCP client. The DHCP Server Profile must already exist. See DHCP Service Profile.

Table 10-336 Workflow Control Profile Parameters

Parameter	Description
Default Advice of Charge	Default Advice of Charge to use. The Advice of Charge must already exist. See Advice of Charge.
Allow Mapped APN Based Sub Analyzer	Allows mapped APN based Subscriber Analyzer to be applied to the subscriber: ■ true: Applies the Subscriber Analyzer rules associated with the APN received in the Called-Station-Id attribute to the subscriber ■ false ***Note:*** *Only one APN redirection is allowed per subscriber.*
V4v6 Hybrid Allocation State	The policy to use for hybrid v4v6 UE IP allocation, where one IP address is managed externally (RADIUS) and the second IP address is managed internally by the MCC (applies when **UE IP Allocation Mode** specifies to use RADIUS): ■ v4v6-hybrid-allocation-disabled – Hybrid UE IP allocation is disabled. In the event that RADIUS returns only one of the IP addresses, the session setup request is rejected. ■ v4v6-hybrid-allocation-local-pool – If RADIUS allocates one of the IP addresses, MCC attempts to allocate the other IP address from one of the local IP sub pools. ■ v4v6-hybrid-allocation-remote-pool – If RADIUS allocates one of the IP addresses, MCC attempts to allocate the other IP address from one of the remote IP sub pools. This configuration applies only in the case where the UE is requesting a v4v6 IP address and RADIUS allocates only a v4 or a v6 IP address. If the RADIUS does not assign any UE IP address, hybrid allocation mode does not apply. Actions are dependent on the **Remote IP Alloc Fallback Option**.
Duplicate IP Reserve Request Handling	Controls the subscriber session setup during a duplicate IP assignment (for example, when an external server (such as RADIUS) assigns a UE IP to a subscriber that is already assigned to a different subscriber). Applies when **UE IP Allocation Mode** *is not* set to local-ue-ip-allocation. Values: ■ reject-new-session – Reject the new subscriber session setup and keep the old session. ■ delete-existing-session – Close the existing session and accept the new session creation request with the duplicate IP assignment.

Table 10-336 Workflow Control Profile Parameters

Parameter	Description
Allow Mapped APN Based Sub Analyser	Specifies whether to allow mapped APN-based sub-analyzer to be applied to the subscriber: ■ true – Maps the generic APN to the specified mapped APN and applies the Subscriber Analyzer rules associated with the mapped APN to the subscriber. ■ false – Maps the generic APN to the specified mapped APN so that external entities, such as RADIUS and policy and charging servers, can provide differentiated treatments.
Default Port NBR Interface	The default Port NAT binding record interface. The Port NAT binding record interface must already exist. See Interface: Port NBR Service.
Default Rx Interface	The default Rx interface. The Rx interface must already exist. See Interface: Rx Interface.
User Subscription Charging Type	User Subscription Charging Type: ■ no-subscription: No Subscription Type. MCC sends online and offline AVP as enabled ■ postpaid-subscription: Postpaid User Type. MCC sends online AVP disabled and offline AVP as enabled ■ prepaid-subscription: Prepaid User Type. MCC sends online AVP enabled and offline AVP as disabled
Initial User Unknown Error Handling	Initial Diameter user unknown error result code handling: ■ reject-session ■ redirect-session
Redirect on Creation	Specifies whether to redirect the session upon creation: ■ true: If a redirect URL is provisioned, session is redirected to the URL immediately ■ false
MVNO Profile	The Mobile Virtual Network Operator profile for sessions associated with an MVNO and using this Control Profile. The MVNO Profile must already exist. Create it at Zone > *name* > Gateway > Profile > MVNO Profile.
Default S6b Interface	The default S6b interface to use. The S6b interface must already exist. See Interface: S6b Interface.
EDR Interface	The Event Data Record Interface Profile to use. The EDR Interface Profile must already exist. See EDR Interface Profile.

Table 10-336 Workflow Control Profile Parameters

Parameter	Description
Update Prior Mapped Apn	Specifies whether to update the prior mapped APN when APN mapping is performed: ■ false – If APN mapping is configured on this control profile, the APN mapped prior to the current APN is not populated in the prior mapped APN. ■ true – (default) If APN mapping is configured on this control profile, the APN mapped prior to the current APN is populated in the prior mapped APN.
Flow Authorization Interface	Specifies the flow authorization interface to use. The flow authorization interface must already exist. See Interface: Flow Authorization Interface.
Allocate Delegated Prefix from Local Pool	Allocate the delegated IPv6 prefix from the local IP subpools: ■ enabled ■ disabled
Data Profile Reselection Trigger Template	Select the Data Profile Reselection Trigger Template to use. The Data Profile Reselection Trigger Template must already exist. See Data Profile Reselection Trigger Template.
Profile Type	The QoS Profile to use to provide AMBR and burst sizes for the default bearer: ■ Network QoS Profile: the AMBR unconditionally overrides the user equipment's AMBR request. ■ Default QoS Profile: The AMBR is used only if the user equipment does not request a particular bandwidth (AMBR request is 0).
Field when Profile Type is set to Default QoS Profile	
Default QoS Profile	The default QoS Profile to use if the user equipment does not request a particular bandwidth. The QoS Profile must already exist. See Quality of Service.
Field when Profile Type is set to Network QoS Profile	
Network QoS Profile	Network QoS Profile to use to override UE signaled AMBR. The QoS Profile must already exist. See Quality of Service.

4 In **Mirrored Accounting Interface List**, select the accounting interface on which the mirrored accounting messages are to be sent.

Only accounting interfaces designated with an interface type of mirrored can be selected. This parameter is only available when a primary accounting interface is configured.

To add additional Mirrored Accounting Interfaces, click the **Create** icon.

5 In **Delegated Prefix List**, specify the prefix length of the delegated IPv6 prefix to be assigned from local IP subpools:

- **prefixlength**
- **priority** - priority to choose the Delegated IPv6 Prefix to be assigned from local IP subpools.

To add additional Delegated Prefix Lengths, click the **Create** icon.

6 Click the **Save** icon.

Data Profile

Use this object to specify the services to provide for the PDN session and controls resource utilization by the session.

To add a Data Profile:

1. Expand **Workflow** in the tree.
2. Click **Data Profile**.
3. Configure the parameters as follows:

Table 10-337 Data Profile Parameters

Parameter	Description
Name	Enter a Data Profile name.
Max Connections	Enter the maximum number of allowed connections.
Force Packet Drop	Specifies whether to force all the packets to drop both on the access and core side after workflow processing. Set to true when the system is acting as a probe, and you want it to analyze the data and drop the packets: ■ true ■ false
Fair Bandwidth Usage	The Fair Bandwidth Usage Profile to add to the Data Profile. The Fair Bandwidth Usage Profile must already exist. See Fair Bandwidth Usage.
Multi Protocol Proxy	The Multi Protocol Proxy instance to add to the Data Profile. The Multi Protocol Proxy instance must already exist. See Multi Protocol Proxy Instance.
Content Filter	The Content Filter service to add to the Data Profile. The Content Filter must already exist. See Content Filter.
Content Cache	The Content Cache service to add to the Data Profile. The Content Cache must already exist. See Content Cache.
Video Adaptation	The Video Adaptation service to add in the Data Profile. The Video Adaptation must already exist. See Video Adaptation (MCC versions prior to 8.2).
QoS Service	The QoS Policy to add in the Data Profile. The QoS Policy must already exist. See QoS Policy.
Subscriber Firewall	The Subscriber Firewall Policy to add in the Data Profile. The Subscriber Firewall Policy must already exist. See Subscriber Firewall Policy.

Table 10-337 Data Profile Parameters

Parameter	Description
Charging	The Charging instance to add in the Data Profile. The Charging instance must already exist. See Charging: Charging Instance. ***Note:*** *Dynamic selection of a Charging Instance via a RADIUS interface takes precedence over any Charging Instance specified in the Workflow Data Profile and the Workflow Control Profile. For static selection of a Charging Instance, the Charging Instance specified in the Workflow Data Profile takes precedence over the Charging Instances specified in the Control Profile.*
WAP Gateway	The WAP Gateway Service Instance to add theData Profile. The WAP Gateway Service Instance must already exist. See WAP Gateway Service Instance.
Steering Policy	The Layer 3 route Steering Policy to add the Data Profile. The Steering Policy must already exist. See Steering Policy.
DNS Policy	The DNS Policy to add the Data Profile. The DNS Policy must already exist. See DNS Policy.
HTTP Server	The HTTP Server instance to add to the Data Profile. The HTTP Server instance must already exist. See HTTP Server Service Instance.
Priority Evaluation Mode	Priority Evaluation Mode when classifying traffic: ■ flat - Use Service Rule priority (ignore Service Flow priority). To make a match, examine all of the Service Rules on all of the Service Flows for best priority. ■ flat-with-pcc-rule-precedence - Any PCC rules in effect have their precedence values compared with the Service Rule priority values, and the PCC rule or Service Rule with the highest priority (lowest numerical value) is selected. ■ hierarchical - Use Service Flow priority and Service Rule priority hierarchically. To make a match, examine the Service Flow in priority order and within each of them, examine the Service Rules in priority order.
DPI Pre Detection Max Pkts	DPI pre-detection allows DPI to identify the protocol or application by default. Specifies the maximum number of packets for DPI pre-protocol and application detection.
DPI Pre Detection Max Bytes	DPI pre-detection allows DPI to identify the protocol or application by default. Specifies the maximum number of bytes for DPI pre-protocol and application detection.

Table 10-337 Data Profile Parameters

Parameter	Description
Default CRBN Profile	The default CRBN profile to be used when the PCRF is unreachable and the PGW uses the default Gx policy to set up the session. If the PCRF in unreachable during the session setup and the default Gx policy is enabled, the default CRBN profile is activated for a subscriber. Once the PCRF comes back up and the PGW receives a CCA-I from the PCRF, the default CRBN is deactivated for the subscriber. Applies only when the CRBN Mode is set to CRBN Profile in the PCRF Charging Interface Profile. The CRBN Profile must already exist. See CRBN Profile.
First Packet Over Volume Quota	Behavior for first packet to exceed volume quota: ■ allow ■ disallow
Flow Idle Timeout Profile	Flow idle timeout profile bound to the data profile. The flow idle timeout profile must already exist. See Flow Idle Timeout Profile.
Network QoS Profile	Network QoS Profile to overrides the user equipment's signalled AMBR request.
Metering Service	Select the Metering Service. The Metering Service must already exist. See Metering Service. To add additional Metering Services, click the **Create** icon.
Geo Redundant Group	Select the Geo Redundant Group. To add additional Geo Redundant Groups, click the **Create** icon.

4 Click the **Save** icon.

Data Profile Switching

MCC supports switching workflow data profiles, whereby any services can be switched to a new service.

For example, in the following scenarios, MCC switches the workflow data profile to match the corresponding new plan dynamically without terminating the subscriber:

- When a subscriber's plan quota runs out
- When a subscriber purchases optional plan packages

- When a subscriber upgrades/downgrades a package
- When a policy changes in the network

When workflow data profile switching occurs, the system reclassifies traffic and applies all referenced services supported by the new workflow data profile:

- Some services (such as charging instance and QoS Policy) immediately take effect for the next packet. Existing connections are mapped to different QoS flows or rating groups, based on the new workflow data profile.
- Other services (such as Multi Protocol Proxy and steering service) take effect only for new transactions. Current transactions continue to use the previous data profile information.

When switching to a new charging instance, all referenced rating groups present in both the previous and new data profile are reauthorized for grants from the OCS server. Rating groups present in the previous data profile but not in the new data profile are closed by sending the FINAL reporting reason to the OCS server with current usage information. These rating groups are deleted from the subscriber and the subscriber data traffic is reclassified and assigned to the new rating groups.

Data Profile Reselection Trigger Template

Use this object to trigger a data profile switch and associate the template from the control profile. MCC switches the data profile by applying the subscriber analyzer selection based on RAT type. This feature supports switching of a data profile with and without PCRF on RAT change: This feature also supports 3GPP to non-3GPP handover and vice versa.

To add a Date Profile Reselection Trigger Template:

1. Expand **Workflow** in the tree.
2. Click **Data Profile Reselction Trigger Template**.
3. Configure the parameters as follows:

Table 10-338 Data Profile Reselection Trigger Template Parameters

Parameter	Description
Name	Enter a Data Profile Reselection Trigger Template name.
RAT Change	Specifies whether to enable reselection of a data profile on RAT change: ■ enabled ■ disabled

4. Click the **Save** icon.

Subscriber Analyzer

Use this object to define the rules that dictate whether to apply a specific service flow to a subscriber.

To add a Subscriber Analyzer:

1. Expand **Workflow** in the tree.
2. Click **Subscriber Analyzer**.
3. Configure the parameters as follows:

Table 10-339 Subscriber Analyzer Parameters

Parameter	Description
Name	Enter a workflow name.
Analyzer Type	Workflow Analyzer type. ■ Peer Selector ■ Workflow Profile ■ User Plane Selector: Specifies that a session is a CPF/CUPS session as opposed to a regular integrated non-CUPS session. This configuration applies to both the collocated and standalone PGW service, as well as standalone SGW service.
Peer List	***Note:*** *Applies when Analyzer Type is Peer Selector.* GTP Peer list. The GTP Peer list must already exist. Configure it at Zone > *name* > Gateway > Epdg *name* > Gtp Peer List.
Priority	Enter a workflow priority (value must be unique)
Geo Redundant Group	The Geographic Redundancy Group. In a CUPS deployment, this Geographic Redundancy Group is the one referenced by the UE Pools in the IP Subpools that are associated with the specified User Plane Profile. The Geographic Redundancy Group must already exist. See Geographic Redundancy Manager.
Event	Specify whether to associate the workflow with: ■ Bearer Setup
Action	
Data Profile	Select the Workflow Data Profile to statically bind a service flow to the workflow. Omit the Workflow Data Profile to dynamically obtain the services that have been programmed on the system. The Workflow Data Profile must already exist. See Data Profile.
Control Profile	Select the Workflow Control Profile identifying the external identity providing the workflow data profile. The Workflow Control Profile must already exist. See Control Profile.

Table 10-339 Subscriber Analyzer Parameters

Parameter	Description
User Plane Profile	Select the User Plane Profile identifying the user plane providing the network profile and PFCP Peer. The User Plane Profile must already exist. Configure it at Zone > *name* > Gateway > User Plane Profile. To add additional User Plane Profiles, click the **Create** icon.

4 You can configure multiple keys, each identified by name. If any key matches, the subscriber analyzer is selected. A key can specify multiple triggers, all of which must match for a key to match. If no keys are configured or the keys have no attributes, the subscriber analyzer is ignored and is not part of the selection process during session setup.

In **Key**, configure the parameters as follows:

Table 10-340 Key Parameters

Parameter	Description
Name	Key set name
UE Capabilities	Mark the checkbox to select User Plane or Workflow Profile based on UE's support for Dual Connectivity New Radio (DCNR) ***Note:*** *UE Capabilities is supported for Workflow Subscriber Analyzer of Analyzer Type User Plane Selector and Workflow Profile.*
APN Name	Select the Access Point Name.
GTP Proxy Name	Select the GTP Proxy service name.
PGW Name	Select the Packet Data Network Gateway.
SGW Name	Select the Serving Gateway.
GGSN Name	Select the Gateway GPRS Support Node.
MCC Name	Select the MCC Gi Gateway.
UE IP Address	Enter User Equipment IP Address.

Table 10-340 Key Parameters

Parameter	Description
RAT Type	Select the Radio Access Type: ■ UTRAN ■ GERAN ■ WLAN ■ GAN ■ HSPA Evolution ■ EUTRAN ■ Virtual ■ NBIOT EUTRAN
PDN Type	Select the PDN Type: ■ IP ■ Non-IP Using this key, subscribers with IP and non-IP PDN types can use the same APN but different services based on the workflow control profile. Options include: IPv4, IPv6, IPv4v6, and non-IP
Home PLMNID	Enter the Subscriber's Home PLMNID, 5 or 6 digits.
Serving NW PLMNID	Enter the Serving Network's PLMN ID, 5 or 6 digits. The RADIUS AVP 3GPP-SGSN-Address is received in the Accounting Request and retrieves the serving-nw-plmnid (plmn-id-mcc and plmn-id-mnc) from the SigInfo table. If this serving-nw-plmnid is configured as key for any of the Subscriber Analyzers, then that Subscriber Analyzer is selected for the session. In GiGW, this key is matched against the 3GPP-SGSN-MCC-MNC AVP.
Serving NW MCC	Enter the Serving Network's Mobile Country Code The GTP Proxy service can select any PGW based on a UE’s location or classification type. This facilitates topology hiding, simplifies deploying or adding more PGWs, and streamlines the billing-data information required for supporting multiple countries with multiple operators.
Charging Characteristics	Enter the Charging Characteristics information
MVNO Identifier	Enter the MVNO name or Identifier
MVNO Sub Identifier	Enter the MVNO sub name or sub Identifier
Roaming User	Specify whether the user is a roaming user: ■ true ■ false

Table 10-340 Key Parameters

Parameter	Description
Signalling Priority LAPI	Specifies whether to use signalling priority indication LAPI. ■ true ■ false This key is used to define criteria for the subscriber analyzer selection and configure rules to differentiate the treatment for LAPI PDNs.
Credit Control Group	Enter the Credit Control group value.
Gigw Unknown Subscriber Profile	Specify whether the subscriber analyzer is intended for SA-GIGW unknown subscribers: ■ true ■ false
WAG Name	Select the Wireless Access Gateway. The Wireless Access Gateway must already exist. Create it at Zone > *name* > Gateway > WAG.
ePDG Name	Select the ePDG. The ePDG must already exist. Create it at Zone > *name* > Gateway > ePDG.
User Name Prefix	Prefix of the username to match
Realm Name	Domain name portion of the username
IMEI Range	Enter the International Mobile Equipment Identity range.
IMSI Range	Enter the International Mobile Subscriber Identity range.
Cell Global ID	Enter the following values: ■ Cell Global ID PLMNID, 5 or 6 digits. ■ Tracking Area Code ■ Cell Identifier
Service Area ID	Enter the following values: ■ Service Area ID PLMN ID, 5 or 6 digits. ■ Location Area Code ■ Service Area Code
Routing Area ID	Enter the following values: ■ Routing Area ID PLMNID, 5 or 6 digits. ■ Location Area Code ■ Routing Area Code
Tracking Area ID	Enter the following values: ■ Tracking Area ID PLMN ID, 5 or 6 digits. ■ Tracking Area Code

Table 10-340 Key Parameters

Parameter	Description
E-Utran Cell Global ID	Enter the following values: ■ E-Utran Cell Global ID PLMNID, 5 or 6 digits. ■ E-Utran Cell Identifier
MSISDN Range	Enter the Mobile Subscriber Integrated Services Digital Network-Number range.
APN Name List	Enter multiple APN names to match: ■ Values ■ Match Type: – match-any – match-none
Serving NW PLMNID List	Enter multiple Serving NW PLMNID to match

To add additional Keys, click the **Create** icon.

5 Click the **Save** icon.

Zone

Use the Zone object to partition resources.

Zone child objects are listed in the following table:

Table 10-341 Zone Child Objects

Parent	Child	Description
Content	Congestion Control	Configures Content Services congestion control
	Statistics	Lists content statistics
	Threshold	Lists threshold statistics for HTTP Proxy
	Threshold History	Lists threshold crossing history
Deep Packet Inspection	Statistics	Lists DPI statistics
Gateway	Apn	Configures Access Point Name
	Congestion Control	Configures Gateway service congestion control
	Connectivity Check	Generate calls to the gateway Device Under Test (DUT) to verify that all internal and external configurations and interfaces are working properly.
	Control Plane Block Management Statistics	Lists Control Plane Block Management statistics
	Debug Stats	Lists Gateway debug statistics
	Dns Global Cache	Lists global DNS cache
	Dns GW Cache	Lists gateway DNS cache
	Dynamic PCC Rule	Lists dynamic PCC rule information
	Enhanced Features List	Enables/Disables list of enhance features
	Epdg	Configures Evolved Packet Data Gateway (ePDG) service
	Filter ID Pco Action Association Table	Configures a list of Filter ID to PCO Action associations
	Ggsn	Configures GGSN service
	Gtp Peer	Configures the GTP Peer with which the SGW, PGW, or GGSN communicates
	Gtp Peer Status	Lists GTP Peer information for gateway instances
	Gtp Proxy	Configures GTP Proxy service
	Instance Apn Status	Lists APN status of Gateway Service Instances

Table 10-341 Zone Child Objects

Parent	Child	Description
(Continued)	Instance Apn Status	Lists gateway service instance APN status table
	Instance Status	Lists gateway service instance status table
	Mcc Gigw	Mobile Content Cloud (MCC) Gi Gateway Service Configuration
	Pcscf Table	Configures P-CSCF addresses
	Pdn Bearer	Lists status and statistics of a PDN bearer
	Pdn Service Data Flow	Lists status and statistics of a PDN service data flow
	Pdn Session	Lists status and statistics of a PDN session
	Peer Selection	Lists peer selection information
	Pfcp Peer	Configures that PFCP peer that the SGW, PGW, or User Plane communicates with
	Pfcp Peer Status	Lists the PFCP peer information for gateway services
	Pgw	Configures PGW service
	Procedure Duration Stats	Gateway Procedure Duration Histogram
	Profile	Configures the following profiles: ■ Common Gateway Profile (timers/counts and configuration settings) ■ Service Profile for GTP-U path management ■ Default Peer Overload Control profile used by gateway instances
	SBM Control Plane Block Table	Lists control plane block number distribution across services (PGW/SGW, GGSN/IMSIMGR)
	SBM User Plane Block Table	Lists user plane block number distribution across services (PGW/SGW, GGSN/IMSIMGR)
	Service Rule Pco Action Association Table	Configures a list of Service Rule to PCO Action associations
	Service Status	Lists status of the Gateway service
	Session Blockid Management	Session Block ID Management configuration
	Session Load Balancer	Configures Session Load Balancer parameters
	Sgw	Configures SGW service
	Sig Info Table	Configures a GTPv1 signaling information table containing default values for the RAT Type, serving network PLMN ID (RAI), and the MS Time Zone on an IP/Subnet basis (SGSN IP).

Table 10-341 Zone Child Objects

Parent	Child	Description
(Continued)	Slb Load Status	Lists load distribution status across GWs (PGW/SGW/GGSN)
	Statistics	Lists gateway statistics
	Subscriber	Lists a count of subscribers based upon IMSI range (inclusive) or a count of subscribers using a specific APN. Can also be used to clear subscribers based upon IMSI range (inclusive) or clear subscribers using a specific APN
	Subscriber Trace	Configures subscriber trace
	Task Instance Status	Lists task instance status table
	Threshold	Lists threshold statistics for call performance
	Threshold History	Lists threshold crossing history
	User Plane Block Management Statistics	Lists User Plane Block Management statistics
	User Plane Profile	Configures User Plane Profile
	User Plane Service	Configures User Plane Service
	WAG	Configures WLAN Access Gateway Service
Policy Server	PCRF List	Configures PCRF service
	Roaming List	Configures Roaming profile
Statistics Framework	Service Status	Lists operational status, operational reason, number of table requests sent, number of table responses received, number of tables tracked, and number of statistics agent instances.
System	Congestion Control	Configures system congestion control
	Statistics	Lists system statistics
	Threshold	Lists threshold statistics for system CPU and system memory
	Threshold History	Lists threshold crossing history

Chapter 11

Network Element

This topic provides information about using Acuitas to monitor and manage the network element.

It includes the following topics:

- Log Viewer
- Save Tech Support Information
- Device Audit Trail
- Rate Limiting Subscriber Group File Management
- Accessing Siemens SPCRF EMS
- Accessing HPE HSS EMS EMS
- Accessing Device Gateway Application

Log Viewer

From Acuitas, you can view the following network element logs:

- Event Log – Each contains a history of the activities on the network element, which is useful for monitoring the health of the network element and the history of events that have occurred. A Protocol Log is a type of event log that contains the control packets for a specific protocol (for example, GTP-C, RADIUS, and so on) or a specific interface (for example, S11, S2, and so on).
- Messages – Each contains logs from the Linux subsystem, kernel, and other services/daemons running on the system.
- Fault Files – Each contains a core dump file in binary format, which is useful to Affirmed Networks Engineering and TAC for diagnosing and resolving the failure.

- Trace Files – Contains UE trace output, cell trace output, and UE trace PCAP output for subscriber trace sessions.

In addition, you can view the following MCC MME logs:

- Console Files – Contains the console output of an EPC process.
- Support Tarball – Contains all log information, which is useful to Affirmed Networks Engineering and TAC for diagnosing and resolving failures.

In addition, you can view the following SSF logs:

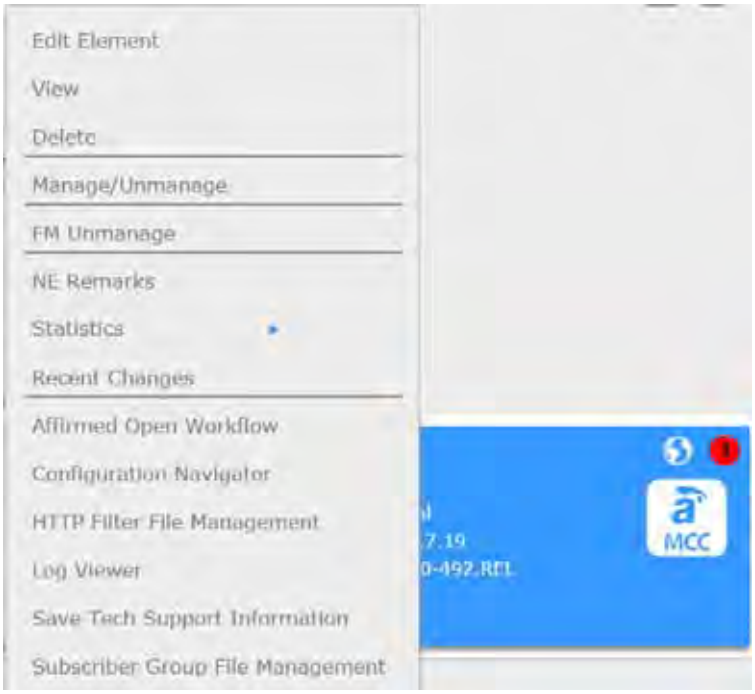
- Support Tarball – Contains all log information, which is useful to Affirmed Networks Engineering and TAC for diagnosing and resolving failures.
- Alarm Files – Contains a stream of set/clr alarms in syslog form
- Developer Files – Contains debug logs for developers

Note: *To view network element logs, you must have either Configuration > MCC Configuration > System Configuration > Read or Admin security group permissions. For instructions, see* *Specifying Permissions by Security Group**.*

To view logs:

1 Right-click an NE and select **Log Viewer**.

Figure 11-1 Log Viewer



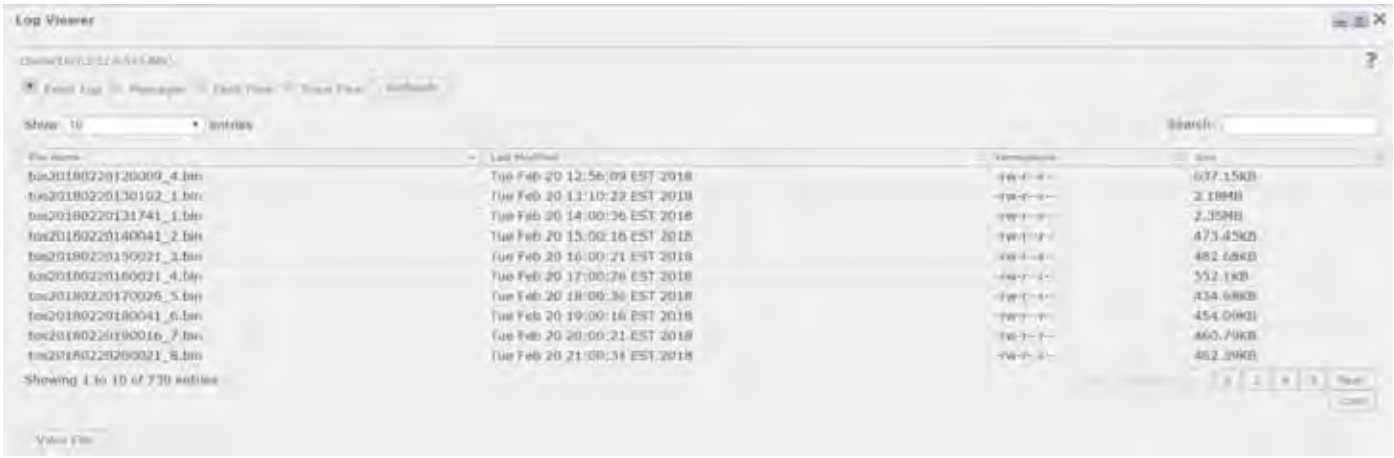
Acuitas displays the **Log Viewer** window.

2 Mark the radio button to select the log you want to view:

- Event Log
- Messages
- Fault Files
- Trace Files
- Console Files (*MME only*)
- Support Tarball (*MME and SSF only*)
- Alarm Files (*SSF only*)
- Developer Files (*SSF only*)

Acuitas lists the specific log files for the selected network element.

Figure 11-2 Sample Event Log Files



In the case of a large number of files, Acuitas displays them over multiple pages. The current page and entry count are listed at the bottom of the window.

To specify how many files you want displayed per page, select the value in the Show Entries box.

Click **First**, **Previous**, **Next**, or **Last** to navigate over multiple pages. To navigate to a specific page, click the page number.

Use the **Search** text box at the top on the window to search for a particular file based on its name, permissions, or size.

Click **Refresh** to refresh the list.

Event Logs

Each Event Log contains a history of the activities on the network element, which is useful for monitoring the health of the network element and the history of events that have occurred. Event logs are in ASCII format. You can either save an Event Log file to the Acuitas client machine or view it using a text viewer.

A Protocol Log is a type of event log that contains the control packets for a specific protocol (for example, GTP-C, RADIUS, and so on) and/or a specific interface (for example, S11, S2, and so on). Protocol Logs have the .pcap-ng extension. For instructions on viewing or saving a Protocol Log, see Protocol Logs.

To view an Event Log file:

1. Select the event log and click **View File**.
2. At the Firefox prompt, click **Open with** and specify the application to use to open it.
3. Click **OK**.

To save an Event Log file:

1. Select the event log and click **View File**.
2. At the Firefox prompt, click **Save File**.
3. Click **OK**.

Protocol Logs

You can save a Protocol Log to the Acuitas client machine or open it using software that decodes files in pcap-ng format (such as Wireshark or TShark) to view it.

Configuring Protocol Logs on the NE

The Protocol Log must already exist on the network element. Configure it in the Configuration Navigator:

To configure the Protocol Log:

1. Expand **Infrastructure** in the tree.
2. Expand **Logging**.
3. Expand **Event Log**.
4. Click **Policy**.
5. Configure the parameters as follows:
   - **Name** – Enter a log name.
   - **Log Type** – Set to **protocol**.
6. Click the **Save** icon.
7. Expand the Policy you added.

8 Click **Protocol Logging Filter Field**.

9 Configure the parameters as follows:

- **Filter Field** – Specify the field on which to filter. To filter on a specific protocol, set to **protocol**.

10 Click the **Save** icon.

11 Expand **protocol**.

12 Click **Filter Value**.

13 Configure the parameters as follows:

- **Value** – Specify a protocol (RADIUS, Diameter, GTPv0, GTPv1, GTPv2, GTPP).

14 Click the **Save** icon.

15 Expand the protocol you added.

16 Click **Filter Field**.

17 Configure the parameters as follows:

- **Filter Field** – To specify a specific interface, set to **interface**.

18 Click the **Save** icon.

19 Expand **interface**.

20 Click **Filter Value**.

21 Configure the parameters as follows:

- **Value** – Specify the interface to use.
- **Exclude** – Specify whether to exclude logs with the filter value.

22 Click the **Save** icon.

Viewing Protocol Logs with Packet Analyzers

MCC performs protocol logging using application software that receives only Application Layer Packets (not Layer3 or Layer4 packet header information). To view Protocol Logs with packet analyzers, it is recommended that you configure the analyzer to ignore Layer3 and Layer4 header fields, otherwise the tool may incorrectly analyze those layers.

For example, in Wireshark:

1 Select **Edit** > **Preferences** > **Protocol**.

2 Select an individual protocol, such as TCP.

3 Unmark the checkbox that specifies to analyze that data.

4 Click **Apply**.

5 Repeat step 2 through step 4 for the other protocols.

To view a Protocol Log, first set the association between the *.pcap-ng file and the Wireshark or TShark application.

To set the application between file and application:

1. Select the Protocol Log and click **View File**.
2. At the Firefox prompt, click **Save File**.
3. Click **OK**.
4. Right-click the saved file and click **Open**.
5. At the prompt, select **Select a program from a list of installed programs** and click **OK**.
6. From the file browser, select the Wireshark or TShark application and choose **Always use the selected program to open this kind of file**. Click **OK**.

Once you set the association between the *.pcap-ng file and the application, you can view Protocol Logs, as follows:

To view a Protocol Log:

1. Select the log and click **View File**.

To save a Protocol Log:

1. Select the log and click **View Log**.
2. At the Firefox prompt, click **Save File**.
3. Click **OK**.

Messages

Each Messages file contain logs from the Linux subsystem, kernel, and other services/daemons running on the system.

The two most recent message files (the one currently being written to and the most recent rotated file) are in ASCII format. Each older file is stored as a compressed (zipped) file. You can either save the two most recent message files to the Acuitas client machine or view them using a text viewer. You can save an older message file to the Acuitas client machine or open it using unzipping software (such as 7-zip or pkunzip) to view it.

To view a Message file:

1. Select the message file and click **View File**.
2. At the Firefox prompt, click **Open with** and specify the application to use to open it.
3. Click **OK**.

To save a Message file:

1. Select the message file and click **View Log**.
2. At the Firefox prompt, click **Save File**.
3. Click **OK**.

Fault Files

Each Fault File contains a core dump file in binary format, which is useful to Affirmed Networks Engineering and TAC for diagnosing and resolving the failure. You can save a Fault file to the Acuitas client machine and make it available to Affirmed Networks personnel for analysis.

To save a Fault file:

1. Select the core file and click **Download File**.
2. At the Firefox prompt, click **Save File**.
3. Click **OK**.

Console Files

Each Console File contains the console output of an EPC process of an MME.

To view a Console file:

1. Select the console file and click **View File**.
2. Click the downloaded file to open it.

Trace Files

Trace File contains UE trace output, cell trace output, and UE trace PCAP output for subscriber trace sessions.

To download a Trace file:

1. Select the Trace file and click **Download File**.
2. Click the downloaded file.
3. Click **Open**.

Viewing Trace File with Wireshark

You can open trace files with Wireshark, which decodes the files in PCAP format.

Prerequisites

Perform the following prerequisites:

- Install Wireshark on the client machine.
- Set up the environment for Wireshark and browser.
- Download the decryption key files to the Acuitas user's local machine in the Wireshark's user preferences directory.

To setup the environment for Wireshark and browser:

1 Set up the browser to always prompt where to save downloaded files:

In Firefox:

a In the toolbar, click the **Open Menu** icon.

b Click **Options**.

c Under **Downloads**, mark the **Always ask me where to save file** radio button.

In Chrome:

a In the toolbar, click the **Customize** icon and select **Settings**.

b Click **Show advanced settings**.

c Under **Downloads**, mark the **Ask where to save each file before downloading** checkbox.

MCC generates the following PCAP files located in /var/log/eventlog directory:

- PCAP files: .pcap .pcapng
- ESP Decryption keys: esp_saXXXXXXXX.txt
- IKEv2 Decryption table: ikev2_decryption_tableXXXXXXXX.txt

You need to download the decryption key files to the Acuitas user's local machine in the Wireshark's user preferences directory (such as %AppData%/Roaming/Wireshark).

To download the encryption key files:

1 Right-click an NE and select **Log Viewer**.

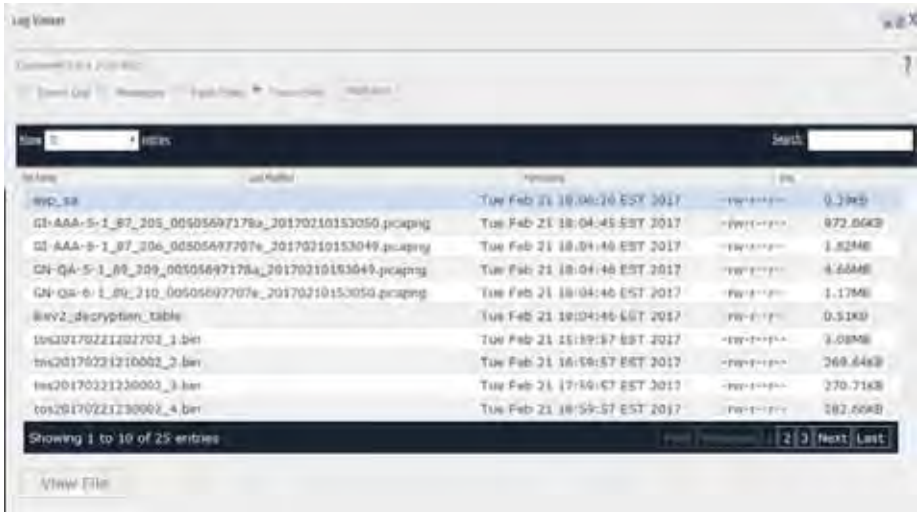
Acuitas displays the **Log Viewer** window.

2 Mark the **Trace Files** radio button.

3 Select one of the following decryption key files from the list:

- esp_sa
- ikev1_decryption_table
- ikev2_decryption_table

Figure 11-3 Sample Trace Files



4 Click **View File**.

5 Specify where you want the file saved and click **Save**.

6 Do not change the filename. Save the file to the Wireshark preferences folder.

Note: To determine the Wireshark preferences folder:

a From Wireshark, select **Help** > **About**.

b Click the **Folders** tab.

c The preference folder is listed in the **Personal** configuration line.

d click **OK**.

7 Click **Save**.

8 Repeat step 3 through step 7 to download the other decryption key files.

Wireshark can now open the PCAP file and use the decryption keys from the default folder to decrypt the encrypted data.

Using Wireshark to View PCAP Files

To view PCAP files:

1. Right-click an NE and select **Log Viewer**.

   Acuitas displays the **Log Viewer** window.

2. Mark the **Trace Files** radio button.
3. Select the file and click **View File**.
4. Mark the **Open with** radio button and select Wireshark from the dropdown list.
5. Click **OK**.

   Wireshark opens the PCAP file, displaying the decrypted data.

Support Tarball

Each Support Tarball contains all log information of an MME, which is useful to Affirmed Networks Engineering and TAC for diagnosing and resolving failures.

Support Tarball files are generated only when you issue the following system operational command to specify the desired level of support information:

```
request system support information level [min | medium | max]
```

To download a support tarball:

1. Select the support tarball file and click **Download File**.
2. Click the downloaded file to open it.

Save Tech Support Information

The Save Tech Support Information command collects detailed debugging information about a Network Element (such as fault files and logs), which is useful to Affirmed Networks Engineering and TAC for diagnosing and resolving failures.

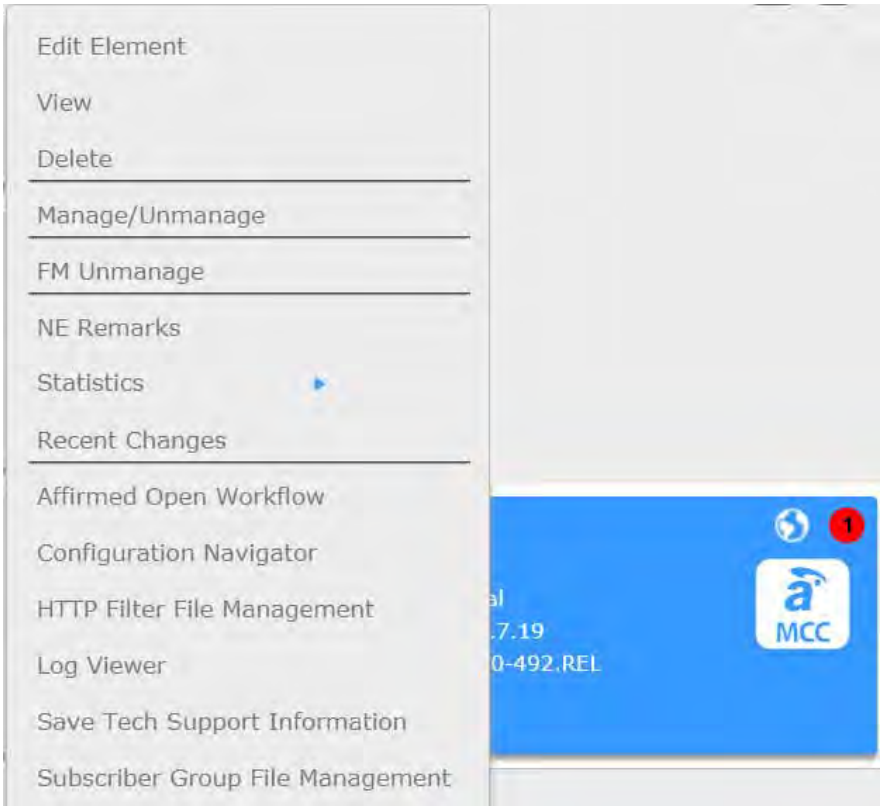
The command packages the information into an individual tar.gz file and an individual MD5 file, and compresses them into a single zip file. In the case of a georedundant pair, you can specify whether to collect information for both nodes, whereby the command creates a tar.gz file and an MD5 file for both the active MCM and the peer MCM and compresses them into a single zip file.

The Network Element must be reachable and managed.

To save Tech Support Information:

1 Right-click an NE and select **Save Tech Support Information**.

Figure 11-4 Save Tech Support Information



Acuitas displays the **Save Tech Support Information** window, listing the options of the command.

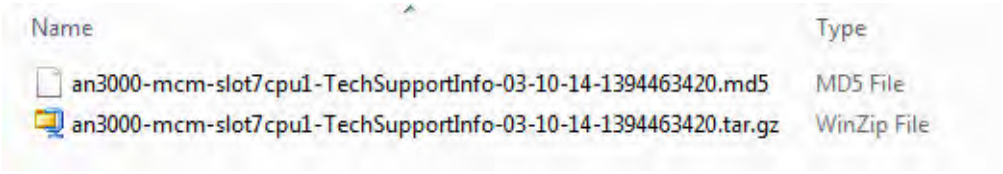
2 Mark the options checkboxes and click **Invoke**:

- **Run Local Only** – Collect the information only on the active node in a georedundant pair (not on the peer).
- **No Log Files** – Do not collect log files.
- **No Fault Files** – Do not collect fault files.
- **No Routing Info** – Do not collect routing-related command outputs.
- **Include Datarecord Files** – Collect datarecord files.
- **Include PSM Files** – Collect PSM (bulk statistics) files.
- **Number of Days** – Collect files that have been modified in the last number of days.
- **Number of Hours** – Collect files that have been modified in the last number of hours.

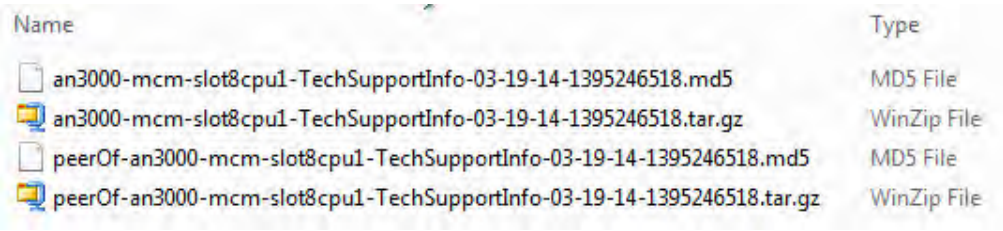
3 The command can take several minutes to complete. When prompted, specify whether to open the file or save it to the Acuitas client machine.

Each zip file contains a tar.gz file and an MD5 sum file for each node.

Sample Files from One Node:



Sample Files from Both Nodes in a Georedundant Pair:



Device Audit Trail

Device Audit Trail logs audit trails from all modules (including Configuration, Performance, and Topology) associated with a selected MCC, MME, or SSF device or EMS Server.

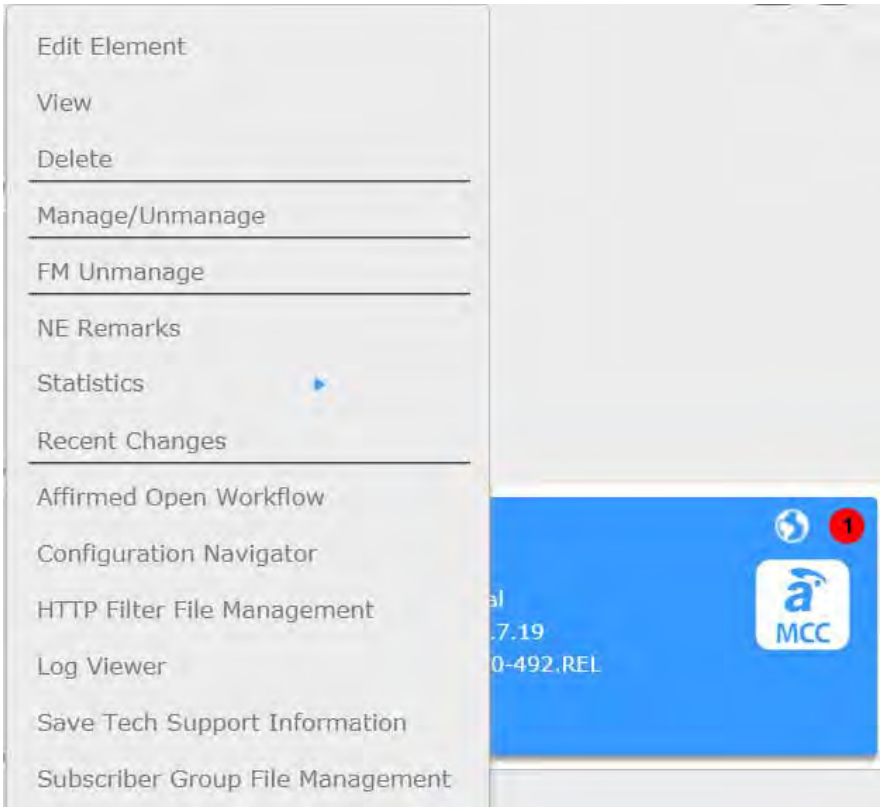
Viewing the Device Audit Trail

Note: *To view the Device Audit Trail, you must have the Configuration > Config Audit Trails > View Config Audit Trails security group permission. For instructions, see* *Specifying Permissions by Security Group**.*

To view the Device Audit Trail:

1 Right-click an NE and select **Recent Changes**.

Figure 11-5 Recent Changes



Acuitas displays the **View Recent Changes** window, listing the following information:

- Element Name
- Component Name

- Module
- Operations
- Date/Time
- Status

2 Click **Close** to close the window.

Exporting Device Audit Trail

You can export the Device Audit Trail to a CSV/PDF/XLS/XML/HTML file.

Note: *To export the Device Audit Trail, you must have the Configuration > Config Audit Trails > Export Config Audit Trails security group permission. For instructions, see Specifying Permissions by Security Group.*

To export the Device Audit Trail:

1 Right-click an NE and select **Recent Changes**.

Acuitas displays the **View Recent Changes** window.

2 If desired, use the Filter Manager or Quick Filter to filter the data displayed in the window.

3 Click the **Export** icon.

Acuitas displays the **Configure Export Parameters** window.

4 Configure the parameters as follows:

- **File Type**: Select the required file format (CSV, PDF, XLS, XML, HTML).
- **Column Configuration**: Select the columns you want exported (Visible Column or All Columns)
- **Export Type**: Select the export type (Whole Data, Current View, Selected Data)
- **Use Current Filter**: Mark the checkbox to restrict data based on the existing filter conditions.

5 Click **Apply**.

Acuitas displays the **Download Files** window.

6 Click **Download Exported File**.

7 From the **Download File**s window, click **Close**.

Rate Limiting Subscriber Group File Management

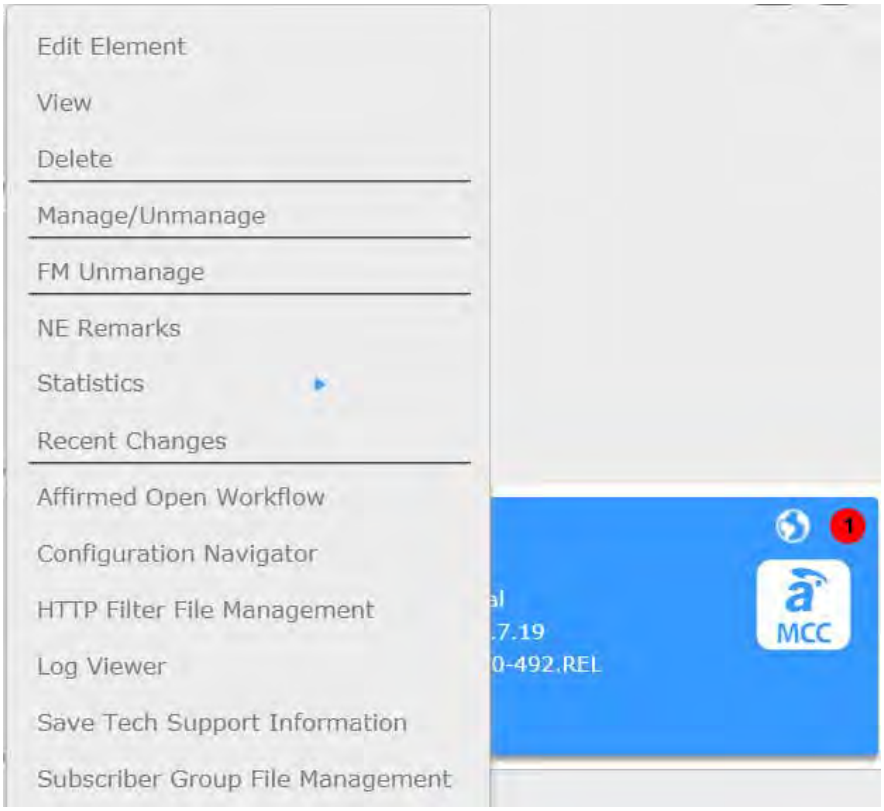
You can configure a group of subscribers whose traffic is rate-limited to a configured aggregate QoS Policy. When the aggregate usage of all the users in the group exceeds the configured limits, the packets from these users are dropped.

Note: *To use the Subscriber Group File Management application, you must have Configuration > MCC Configuration > Service Provisioning – Content > Admin security group permissions. For instructions, see* *Specifying Permissions by Security Group**.*

To manage Subscriber Group Files:

1 Right-click an NE and select **Subscriber Group File Management**.

Figure 11-6 Subscriber Group File Management



Acuitas lists the Subscriber Groups in the system.

Figure 11-7 Subscriber Groups

In the case of a large number of groups, Acuitas displays them over multiple pages. The current page and entry count are listed at the bottom of the window.

To specify how many groups you want displayed per page, select the value in the Show Entries box.

Click **First**, **Previous**, **Next**, or **Last** to navigate over multiple pages. To navigate to a specific page, click the page number.

Use the **Search** text box at the top on the window to search for a particular group by name.

Adding Subscriber Groups

Prerequisites

Before adding a Subscriber Group, create the following objects in the Configuration Navigator:

- Configure a QoS Flow service that allows for service data flow-level rate enforcement. Set **Aggregate QoS Flow** to true and configure the aggregate Uplink/Downlink maximum bit rate (MBR) and Uplink/Downlink maximum burst rate configured. See QoS Flow.
- Configure the QoS Policy that defines the QoS to be given to the QoS Flow. Set **Aggregate QoS Policy** to true. Select the QoS Flow to associate with the QoS Policy. See QoS Policy.

To add a Subscriber Group:

1. Right-click an NE and select **Subscriber Group File Management**.

   Acuitas lists the Subscriber Groups in the system.
2. Click **Create**.
3. In **Upload File**, click **Choose File** to upload a Subscriber ID file (text file of subscriber IDs) from the local machine to the MCC.
4. Select the text file and click **Upload**.

Acuitas pushes the file to the MCC in the directory /public/gateway/subscriber_group/import/. Acuitas returns a notification message when the file is successfully uploaded.

5 Once the file uploads, configure the parameters as follows:

Table 11-1 Subscriber Group Parameters

Parameter	Description
Name	Subscriber Group name
File Name	Auto-filled based on uploaded file name
Subscriber ID Type	Username
QoS Policy	The QoS policy to associate with the Subscriber Group. The QoS Policy must already exist with **Aggregate QoS Policy** set to true. The QoS Flow associated with the aggregate QoS Policy must have the **Aggregate QoS Flow** set to true and an aggregate Uplink/Downlink maximum bit rate (MBR) and Uplink/Downlink maximum burst rate configured.

6 Click **Create**.

The details of the creation task are logged in the configuration Audit Trail on success/failure.

Modifying or Deleting Subscriber Groups

To modify or delete a Subscriber Group:

1 Right-click an NE and select **Subscriber Group File Management**.

Acuitas lists the Subscriber Groups in the system.

2 Select the Subscriber Group and click **Modify**.

3 To modify the Subscriber Group, make the necessary changes and click **Update**:

Table 11-2 Subscriber Group Parameters

Parameter	Description
Upload File	1 Click **Choose File** to upload a Subscriber ID file (text file of subscriber IDs) from the local machine to the MCC. 2 Select the text file and click **Upload**. Acuitas pushes the file to the MCC in the directory /public/gateway/subscriber_group/import/. Acuitas displays a notification message when the file is successfully uploaded.
Name	Subscriber group name (*cannot be modified*)
File Name	Auto-filled based on uploaded file name

Table 11-2 Subscriber Group Parameters

Parameter	Description
Subscriber ID Type	Username
QoS Policy	The QoS policy to associate with the Subscriber Group. The QoS Policy must already exist with **Aggregate QoS Policy** set to true. The QoS Flow associated with the aggregate QoS Policy must have the **Aggregate QoS Flow** set to true and an aggregate Uplink/Downlink maximum bit rate (MBR) and Uplink/Downlink maximum burst rate configured.

To delete a Subscriber Group, click **Delete**.

The details of the modification or deletion task are logged in the configuration Audit Trail on success/failure.

Viewing the Contents of a Subscriber Group File

To view the contents of a Subscriber Group file:

1. Right-click an NE and select **Subscriber Group File Management**.

   Acuitas lists the Subscriber Groups in the system.
2. Select the Subscriber Group and click **View File**.
3. When prompted, specify how you want the file saved and click **Save**.
4. When you have finished, close the window.

Viewing Subscriber Group File List

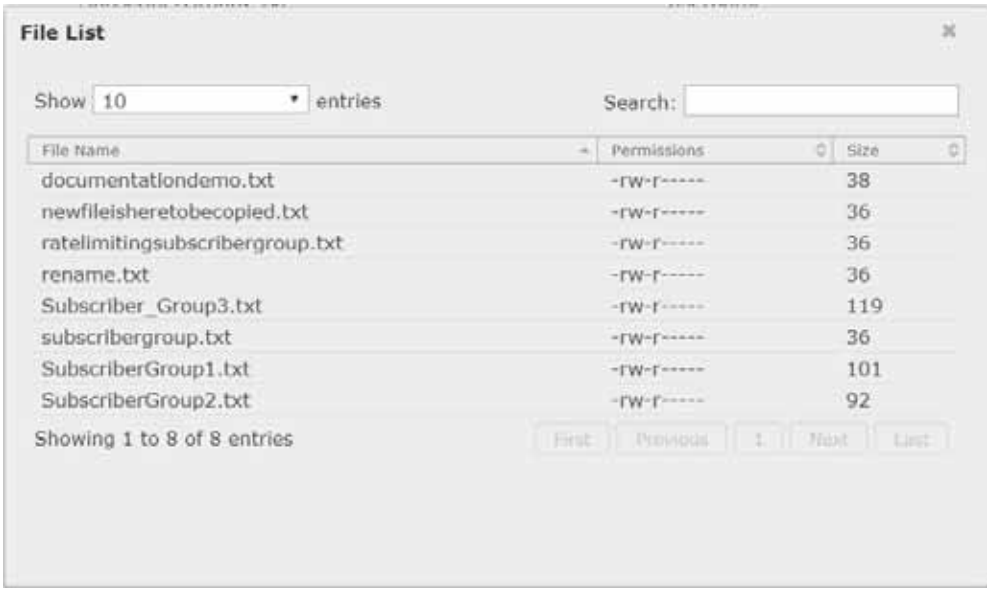
To view the list of a Subscriber Group files on the system:

1. Right-click an NE and select **Subscriber Group File Management**.

   Acuitas lists the Subscriber Groups in the system.
2. Click **View File List**.

Acuitas displays the **File List** window, listing the Subscriber Group files in the system.

Figure 11-8 File List



In the case of a large number of files, Acuitas displays them over multiple pages. The current page and entry count are listed at the bottom of the window.

To specify how many files you want displayed per page, select the value in the Show Entries box.

Click **First**, **Previous**, **Next**, or **Last** to navigate over multiple pages. To navigate to a specific page, click the page number.

Use the **Search** text box at the top on the window to search for a particular file by its name.

3 When you have finished, close the window.

Geographic Redundancy Considerations

Add an Aggregate QoS Policy to a Geographic Redundancy Group to replicate the policy and its associated Subscriber Group and Subscriber ID file from the active node to the standby node. For details, see Geographic Redundancy Manager.

However, if you later modify the Subscriber ID file content (such as change the subscriber IDs) but do not change the filename, Geographic Redundancy Manager does not replicate the updated file to the standby node.

As a workaround, perform the following steps on *both* the active node and the standby node of the Geographic Redundancy Group:

1. Right-click the NE and select **Subscriber Group File Management**.

   Acuitas lists the Subscriber Groups in the system.

2. Select the Subscriber Group and click **Modify**.
3. In **Upload File**, click **Choose File** to upload the modified Subscriber ID file (text file of subscriber IDs) from the local machine to the MCC.
4. Select the text file and click **Upload**.

   Acuitas pushes the file to the MCC in the directory /public/gateway/subscriber_group/import/. Acuitas returns a notification message when the file is successfully uploaded.

5. Click **Update**.

Accessing Siemens SPCRF EMS

You can access the Siemens SPCRF EMS through Acuitas.

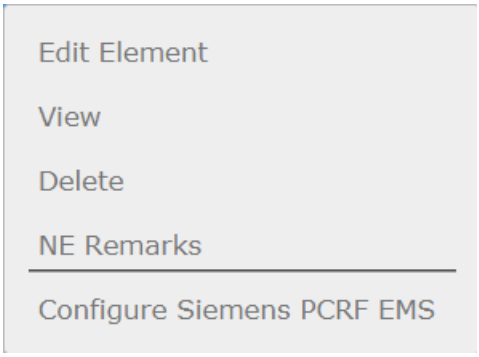
Create a Siemens SPCRF EMS network element:

1. Select **Topology => Add Element**.
2. In **Device Type**, select **Siemens SPCRF**.
3. In **IP Version**, select **IPv4** (*required*).
4. In **IP Address**, enter the IP address of the Siemens SPCRF EMS (*required*).
5. Enter the **Name**, **Description**, and **Location Details** (*optional*).
6. Click **Save**.
7. At the confirmation prompt, click **OK**.

Launch the Siemens SPCRF EMS:

1. Right-click the Siemens SPCRF EMS network element and click **Configure Siemens PCRF EMS**.

Figure 11-9 Configure Siemens SPCRF EMS



Acuitas launches the Siemens SPCRF EMS.

Accessing HPE HSS EMS EMS

You can access the HPE HSS EMS through Acuitas.

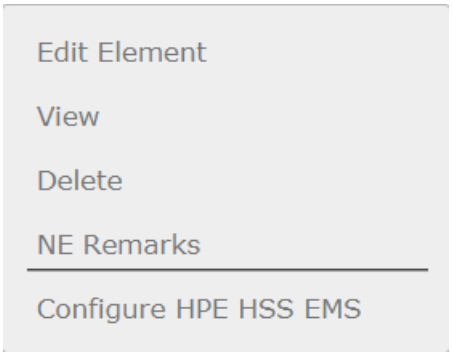
Create a HPE HSS EMS network element:

1. Select **Topology => Add Element**.
2. In **Device Type**, select **HPE HSS EMS**.
3. In **IP Version**, select **IPv4** (*required*).
4. In **IP Address**, enter the IP address of the HPE HSS EMS (*required*).
5. Enter the **Name**, **Description**, and **Location Details** (*optional*).
6. Click **Save**.
7. At the confirmation prompt, click **OK**.

Launch the HPE HSS EMS:

1. Right-click the HPE HSS EMS network element and click **Configure HPE HSS EMS**.

Figure 11-10 Configure HPE HSS EMS



Acuitas launches the HPE HSS EMS.

Accessing Device Gateway Application

You can access the Device Gateway application interface through Acuitas.

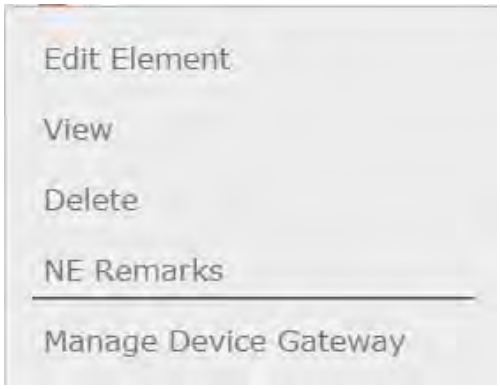
Create a Device Gateway network element:

1. Select **Topology => Add Element**.
2. In **Device Type**, select **Device Gateway**.
3. In **IP Version**, select **IPv4** (*required*).
4. In **IP Address**, enter the IP address of the Device Gateway (*required*).
5. Enter the **Name**, **Description**, and **Location Details** (*optional*).
6. Click **Save**.
7. At the confirmation prompt, click **OK**.

Launch the Device Gateway application interface:

1. Right-click the Device Gateway network element and click **Manage Device Gateway**.

Figure 11-11 Manage Device Gateway



Acuitas launches the Device Gateway application interface.

Appendix A

Interfacing with Northbound Interfaces

This appendix contains information about interfacing with northbound interfaces, such as to OSS systems.

It contains the following topics:

- Acuitas TACACS+ Authentication, Authorization, and Accounting
- Acuitas LDAP Authentication and Authorization
- Acuitas RADIUS Authentication and Authorization
- Acuitas Triggered Alarm Detail
- Acuitas Trap Format
- Exported Performance Management Data
- VNF Manager and Provisioning REST API
- Security REST API

Acuitas TACACS+ Authentication, Authorization, and Accounting

Overview

Terminal Access Controller Access Control System Plus (TACACS+) is a protocol based on a client-server model where the Acuitas server (an NAS entity) sends requests to and receives responses from the TACACS+ server.

When a user attempts to log into Acuitas, Acuitas sends an authentication request to the TACACS+ server and the server either accepts or rejects the request based on information in its user database.

Upon successful authentication, the Acuitas server sends an authorization request to which the TACACS+ server responds with the user's group assignment (used to determine the commands to which the user has access). The authorization information propagated from the TACACS+ server is via a custom attribute-value-pair in the form of group=<*user_group*>, where *user_group* is defined in Acuitas. Once the session is established, the system sends user accounting messages to the TACACS+ server, including session termination.

To use TACACS+ authentication and authorization, configure and enable TACACS+ authentication before starting the Acuitas Application.

Acuitas Security Module Authentication Order

The Acuitas Security Module performs Authentication and Authorization of users by implementing the enabled login modules in the following order:

1. TACACS+ login
2. LDAP login
3. RADIUS login
4. SANE login
5. DB login

Any user attempting login into Acuitas is authenticated using these enabled login modules. In case of any authentication failure in a module, the process proceeds to the next enabled login module. Modules are called in the order defined in the AuthenticationServer.xml file.

Note: *If DB Login is disabled, you must create the* `admin` *user in the* `Administrator` *user group in TACACS+.*

For any new non-DB login user (TACACS/LDAP/RADIUS) user, an equivalent DB user is created with TACACS/LDAP/RADIUS password on its initial successful login. However, the password of the DB users is not be updated on successive RADIUS/TACACS logins.

These DB users (automatically created in Acuitas through TACACS/LDAP/RADIUS) are listed in the Acuitas Security Manager > Security User Details window with Edit User and Change Password options. As a result, these DB users can have user details updated and passwords changed.

Authentication Configuration

To configure and enable TACACS+ Authentication:

1 Following an Acuitas installation and before starting the server, issue the following commands at the command prompt:

```
cd /opt/Affirmed/NMS/bin
configureserver.sh
```

Acuitas displays the **Configure Server Details** menu.

```
Configure Server Details
------------------------

1.DatabaseDetails

2.PortDetails

3.Authentication

4.ProtocolDetails

5.PurgeConfigurationDetails

6.Exit


        Please select your option from (1 | 2 | 3 | 4 | 5 | 6) [1] :
```

2 To configure the TACACS+ Authentication parameters, enter **3**.

```
Authentication Details
----------------------
Would you like to enable Primary TACACS+ Login? (Y | N) [N]:
```

3 To enable a primary TACACS+ login, enter **Y**.

```
AuthMethod [PAP]:

HostName [10.10.10.10]:

Port [49]:

SharedSecret [tacacs]:
```

4 When prompted, configure the following parameters to communicate with the TACACS+ server for authentication:

- TACACS+ Authentication Method
- TACACS+ Host Name
- TACACS+ Account Port
- RADIUS Shared Secret

```
Would you like to enable Secondary TACACS+ Login? (Y | N) [N]:
```

5 To enable a secondary TACACS+ login, enter **Y**.

```
AuthMethod [PAP]:

HostName [10.10.10.10]:

Port [49]:

SharedSecret [tacacs]:
```

6 When prompted, configure the following parameters to communicate with the TACACS+ server for authentication:

- TACACS+ Authentication Method
- TACACS+ Host Name
- TACACS+ Account Port
- RADIUS Shared Secret

```
Would you like to enable Active Directory/LDAP Login? (Y | N) [Y]:
```

7 Enter **N**.

```
Would you like to enable Primary RADIUS Login? (Y | N) [N]:
```

8 Enter **N**.

```
Would you like to enable Secondary RADIUS Login? (Y | N) [N]:
```

9 Enter **N**.

```
Would you like to enable DBLogin? (Y | N) [Y]:
```

10 To enable DB login, enter **Y**.

```
Would you like to save the changes (Y | N) [N]:
```

11 Enter **Y**.

```
Configure Server Details
------------------------

1.DatabaseDetails

2.PortDetails

3.Authentication

4.ProtocolDetails

5.PurgeConfigurationDetails

6.Exit


        Please select your option from (1 | 2 | 3 | 4 | 5 | 6) [1] :
```

12 To exit, enter **6**.

Acuitas LDAP Authentication and Authorization

Overview

The Acuitas Security Module can enable the LDAP login module and perform the following authentication and authorization:

- When a user attempts to log in, Acuitas connects with the LDAP server for authentication.
- Following successful authentication, Acuitas retrieves user-group mapping details from the LDAP Authentication response.
- Authentication creates a logical user details entry in the Acuitas database to handle user-specific Acuitas operations.

The following sections describe how the LDAP login module supports authentication and authorization in Acuitas.

Authentication

Acuitas authenticates users by checking the list of enabled login modules in the order in which they were configured. LDAP login is enabled in the following order:

1. LDAP login
2. DB login

When a user attempts authentication, the LDAP login module acts as standard LDAP client. The following high level actions are performed:

1. LDAP login module sends the user name and password to LDAP server and attempts to gain access to the user's LDAP context in the LDAP server.
2. LDAP server authenticates the user and provides access to the LDAP context.
3. Acuitas either creates the Acuitas user session or fails the user authentication based on the response from LDAP server.

Acuitas supports configuring primary and secondary LDAP servers. In the case where the primary LDAP server is not reachable, the secondary LDAP server can be used to authenticate the user.

Authorization

The Acuitas Security Module supports the following user authorization:

- In Acuitas, user operations have individual role permissions.
- Any created Acuitas user is associated with one or more a user groups.
- A set of role permissions is provided for each user group.

Separate user-group mapping and group-role mapping are stored in the Acuitas database.

Following successful authentication, Acuitas retrieves the user group and role mapping details from the Acuitas database. The Acuitas user is permitted to perform only the operations for which they have role permissions in their belonged user groups.

When LDAP based authorization is enabled:

- Following successful LDAP authentication, user-group mapping is expected from LDAP context access provided by the LDAP server.

  For example, once a LDAP user named *test* is authenticated in the LDAP server, its user-group mapping *test – Operators* must be provided as LDAP response.

- Acuitas creates a logical user entry in the Acuitas database to handle authorization internally upon new LDAP user authentication attempts. Acuitas updates the group associations with every LDAP login.

- Using the user-group mapping from LDAP and the group-role mapping in the Acuitas database, user authorization functions the same as the existing DB-based authorization.

Acuitas Security Module Authentication Order

The Acuitas Security Module performs Authentication and Authorization of users by implementing the enabled login modules in the following order:

1. TACACS+ login
2. LDAP login
3. RADIUS login
4. SANE login
5. DB login

Any user attempting login into Acuitas is authenticated using these enabled login modules. In case of any authentication failure in a module, the process proceeds to the next enabled login module. Modules are called in the order defined in the AuthenticationServer.xml file.

Note: *If DB Login is disabled, you must create the* `admin` *user in the* `Administrator` *user group in LDAP.*

For any new non-DB login user (TACACS/LDAP/RADIUS) user, an equivalent DB user is created with TACACS/LDAP/RADIUS password on its initial successful login. However, the password of the DB users is not be updated on successive RADIUS/TACACS logins.

These DB users (automatically created in Acuitas through TACACS/LDAP/RADIUS) are listed in the Acuitas Security Manager > Security User Details window with Edit User and Change Password options. As a result, these DB users can have user details updated and passwords changed. On Acuitas, the password change must follow the Acuitas password rules.

LDAP Authentication Configuration

To configure and enable LDAP Authentication:

1 Following an Acuitas installation and before starting the server, issue the following commands at the command prompt:

```
cd /opt/Affirmed/NMS/bin
configureserver.sh
```

Acuitas displays the **Configure Server Details** menu.

```
Configure Server Details
------------------------

1.DatabaseDetails

2.PortDetails

3.Authentication

4.ProtocolDetails

5.PurgeConfigurationDetails

6.Exit
```

```
Please select your option from (1 | 2 | 3 | 4 | 5 | 6) [1] :
```

2 To configure the LDAP Authentication parameters, enter **3**.

```
Authentication Details
----------------------
Would you like to enable Primary TACACS+ Login? (Y | N) [N]:
```

3 Enter **N**.

```
Would you like to enable Secondary TACACS+ Login? (Y | N) [N]:
```

4 Enter **N**.

```
Would you like to enable Active Directory/LDAP Login? (Y | N) [Y]:
```

5 To enable Active Directory/LDAP Login, enter **Y**.

```
IPAddress [192.168.27.160]:
Port [636]:
Realm [uid=#userName#,ou=Users,dc=affirmed,dc=com]:
GetGroupAttr [memberof]:
SSLEnabled [yes]:
Checking LDAP Server ( 192.168.27.160:636 ) connection..
 Success : LDAP Server ( 192.168.27.160:636 ) is reachable..
```

6 When prompted, configure the following parameters to communicate with the LDAP server for authentication:

Table A-1 LDAP Authentication Parameters

Parameter	Description
IPAddress	Server IP Address (IPv4 or IPv6) of the Directory Service running on the LDAP Server.
Port	Port number through which Acuitas accesses the LDAP server. By default, LDAP use port 389 and LDAPS use 636.
Realm	User account location in the Directory Service hierarchy of the LDAP server. If the users in the LDAP server are placed in Users under domain affirmed.com, Realm is uid=#userName#, ou=Users, dc=affirmed, dc=com, where #userName# provided in Realm is replaced by username during authentication. ***Note:*** *Provide uid=”#userName# section in Realm to perform LDAP authentication. #userName# is case-sensitive.*
GetGroupAttr	Attribute used to fetch the list of groups mapped to the user. MS Active Directory and most of the LDAP servers use attribute memberof (Acuitas default value) for this purpose. ***Note:*** *A memberof-like attribute is not available in openLDAP by default, so user should configure memberof overlay to use memberof search in openLDAP server.*

Table A-1 LDAP Authentication Parameters

Parameter	Description
SSLEnabled	Enables/disables LDAPS (LDAP over SSL). In LDAP simple protocol, data is transported in plain text. To avoid this situation, enable LDAPS.
Note: When LDAPS is enabled for a LDAP server, Acuitas expects its LDAP server certificate in keystore (configured in */opt/Affirmed/NMS/server/ems/resources/cloud.properties*) under alias having its IPAddress as alias name during actual authentication.	

```
Checking LDAP Server ( 192.168.27.160:636 ) connection..
Success : LDAP Server ( 192.168.27.160:636 ) is reachable..

Would you like to enable Primary RADIUS Login? (Y | N) [N]:
```

7 Enter **N**.

```
Would you like to enable Secondary RADIUS Login? (Y | N) [N]:
```

8 Enter **N**.

```
Would you like to enable DBLogin? (Y | N) [Y]:
```

9 To enable DB login, enter **Y**.

```
Would you like to save the changes (Y | N) [N]:
```

10 Enter **Y**.

```
Configure Server Details
------------------------

1.DatabaseDetails

2.PortDetails

3.Authentication

4.ProtocolDetails

5.PurgeConfigurationDetails

6.Exit


        Please select your option from (1 | 2 | 3 | 4 | 5 | 6) [1] :
```

11 To exit, enter **6**.

12 Restart the Acuitas server for the configuration to take effect.

Downloading Server (LDAP Server) Certificate

To download the LDAP Server Certificate:

1 Issue the following command to download the certificate file from the LDAP server:

```
echo -n | openssl s_client -connect <LDAP_SERVER_IP>:<PORT_636> | sed
-ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > ldapServer.pem
```

2 Issue the following command to convert the generated pem cert file to jks:

```
keytool -v -importcert -alias <AliasName[IPAddress]> -file
ldapServer.pem -keypass <KeyPassword> -keystore
/opt/Affirmed/NMS/server/ems/resources/.keystore -storepass
<StorePassword>
```

3 Issue the following command to view the list of keystore files:

```
keytool -list -v -keystore
/opt/Affirmed/NMS/server/ems/resources/.keystore -storepass
<StorePassword>
```

4 Issue the following command to view the keystore by AliasName:

```
keytool -list -v -alias primaryLDAP -keystore
/opt/Affirmed/NMS/server/ems/resources/.keystore -storepass
<StorePasswor>
```

The generated keystore with AliasName is used as Serve certificate during LDAPS connection.

Configuration Required on the LDAP Server

The following configuration is required on any LDAP server like MS Active Directory, Open LDAP, and so on:

- Create the set of users that require Acuitas login on the LDAP Server.
- Create the user groups on the LDAP Server.
- Associate the users with a desired set of user groups.
- Assign an attribute for mapping with `GetGroupAttr` to each user. Assign this attribute with the list of user groups associated with the user.

  Note: `memberof`-like attribute is not available in openLDAP server by default. Instead, configure `memberof` overlay to use `memberof` search in the openLDAP server:

  – LDAP server responds for Acuitas along with this `memberof` attribute in case of successful authentication. The Acuitas server treats this attribute value as a list of user groups.

  – User groups created in Acuitas that match with the `memberof` attribute value are assigned to the LDAP user for authorization.

For example, if a user is member of groups Administrators and *XXX* in the LDAP server, Acuitas checks for a group with those same names (Administrators and *XXX*). If they are available, the groups are associated with the LDAP user.

Any unmatched groups in `memberof` attribute are ignored.

If no group in `memberof` attribute is matched with user groups available in the Acuitas server, the LDAP user is associated with default user group (Operators).

- To perform LDAPS authentication, enable the secured LDAP in the LDAP server and configure the SSL server and client certificates (*optional*) in the LDAP server.

Note: Acuitas accepts only certificates for LDAPS connection as the JKS type. You can generate the certificate using openssl and keytool.

Acuitas RADIUS Authentication and Authorization

Overview

RADIUS (Remote Authentication Dial-In User Service) is a network protocol that provides centralized authentication and authorization support for an organization.

Acuitas supports RADIUS PAP (Password Authentication Protocol) based authentication and authorization. If the user name is found in the RADIUS database and the password is correct, the RADIUS server returns an Access-Accept response including pre-defined parameters (attribute-value pairs) that grant proper access to the user. These parameters are configured in RADIUS, including service type, protocol type, IP address to assign the user, an access control list (ACL), and other values.

By default, RADIUS based authentication is disabled. To use RADIUS authentication and authorization, configure the Authentication provider and other settings and enable it following Acuitas installation, before starting the Acuitas Application.

Note: *In addition, add the Acuitas server as an authorized client of the RADIUS server. Do so for all Acuitas servers in the HA or HA+DR cluster.*

Acuitas Security Module Authentication Order

The Acuitas Security Module performs Authentication and Authorization of users by implementing the enabled login modules in the following order:

1. TACACS+ login
2. LDAP login
3. RADIUS login
4. SANE login
5. DB login

Any user attempting login into Acuitas is authenticated using these enabled login modules. In case of any authentication failure in a module, the process proceeds to the next enabled login module. Modules are called in the order defined in the AuthenticationServer.xml file.

Note: *If DB Login is disabled, you must create the* `admin` *user in the* `Administrator` *user group in RADIUS.*

For any new non-DB login user (TACACS/LDAP/RADIUS) user, an equivalent DB user is created with TACACS/LDAP/RADIUS password on its initial successful login. However, the password of the DB users is not be updated on successive RADIUS/TACACS logins.

These DB users (automatically created in Acuitas through TACACS/LDAP/RADIUS) are listed in the Acuitas Security Manager > Security User Details window with Edit User and Change Password options. As a result, these DB users can have user details updated and passwords changed.

RADIUS Authentication Configuration

RADIUS Authorization Prerequisites

Acuitas supports RADIUS based authorization using the VSA (Vendor Specific Attribute). The following procedure is required before performing the RADIUS Authentication Procedure steps.

To configure RADIUS Authorization:

1 **RADIUS Configuration:** Create an affirmed-specific dictionary with the following vendor-specific attributes:

- Vendor `affirmed` with ID `37963`.
- Group `affirmedgroup` with ID `2` and type `string`.

RADIUS Authentication Procedure

To configure and enable RADIUS Authentication:

1 Following an Acuitas installation and before starting the server, issue the following commands at the command prompt:

```
cd /opt/Affirmed/NMS/bin
configureserver.sh
```

Acuitas displays the **Configure Server Details** menu.

```
Configure Server Details
------------------------

1.DatabaseDetails

2.PortDetails

3.Authentication

4.ProtocolDetails
```

```
5.PurgeConfigurationDetails

6.Exit


        Please select your option from (1 | 2 | 3 | 4 | 5 | 6) [1] :
```

2 To configure the RADIUS Authentication parameters, enter **3**.

```
Authentication Details
----------------------
Would you like to enable Primary TACACS+ Login? (Y | N) [N]:
```

3 Enter **N**.

```
Would you like to enable Secondary TACACS+ Login? (Y | N) [N]:
```

4 Enter **N**.

```
Would you like to enable Active Directory/LDAP Login? (Y | N) [Y]:
```

5 Enter **N**.

```
Would you like to enable Primary RADIUS Login? (Y | N) [N]:
```

6 To configure the Primary RADIUS Login module, enter **Y**.

```
AccountPort [1813]:

AuthMethod [PAP]:

AuthPort [1812]:

HostName [10.10.10.10]:

SharedSecret [radius]:
```

7 When prompted, configure the following parameters to communicate with the RADIUS server for authentication:

- RADIUS Account Port
- RADIUS Authentication Method
- RADIUS Authentication Port
- RADIUS Host Name

- RADIUS Shared Secret

```
Would you like to enable Secondary RADIUS Login? (Y | N) [N]:
```

8 To configure the Secondary RADIUS Login module, enter **Y**.

```
AccountPort [1813]:

AuthMethod [PAP]:

AuthPort [1812]:

HostName [10.10.10.10]:

SharedSecret [radius]:
```

9 When prompted, configure the following parameters to communicate with the RADIUS server for authentication:

- RADIUS Account Port
- RADIUS Authentication Method
- RADIUS Authentication Port
- RADIUS Host Name
- RADIUS Shared Secret

```
Would you like to enable DBLogin? (Y | N) [Y]:
```

10 To enable DB login, enter **Y**.

If both RADIUS Login and DB Login options are enabled, the Acuitas server performs login checks in both modules and authenticates the user if at least one module's login process is successful.

Note: *If DB Login is disabled, you must create the* `admin` *user in the* `Administrator` *user group in RADIUS.*

```
Would you like to save the changes (Y | N) [N]:
```

11 Enter **Y**.

```
Configure Server Details
------------------------
```

```
1.DatabaseDetails

2.PortDetails

3.Authentication

4.ProtocolDetails

5.PurgeConfigurationDetails

6.Exit


        Please select your option from (1 | 2 | 3 | 4 | 5 | 6) [1] :
```

12 To exit, enter **6**.

RADIUS Authorization Configuration

Acuitas supports RADIUS based authorization using the VSA (Vendor Specific Attribute). If a user is not defined in Acuitas but is defined in RADIUS server, upon successful authentication by RADIUS (using the group name returned from the RADIUS server), the user and group are added to Acuitas at login time.

In the following procedure, perform the **RADIUS Configuration** steps on the RADIUS server and perform the **Acuitas Configuration** steps on the Acuitas server.

To configure RADIUS Authorization:

1 **RADIUS Authorization Prerequisite:** Make sure that the prerequisite has be met (see RADIUS Authorization Prerequisites).

2 **Acuitas Configuration:** Add Acuitas Security group permissions to control group members access to specific types of objects and control the actions the members can perform on those objects. For details, see Adding Security Groups.

3 **RADIUS Configuration:** Assign the RADIUS users to the Acuitas security groups, using the `affirmedgroup` attribute. For example, to assign users to an Acuitas group “workflow_provisioners,” set each user’s `affirmedgroup` attribute to “workflow_provisioners.”

Acuitas Triggered Alarm Detail

This section lists the Acuitas triggered alarm detail in alphabetical order by alarm name.

Table A-2 Alarm Detail

Data Collection Failure	Description:	Data collection failed on the device.
	Status:	Current
	Severity:	Major
	Auto Clearing:	Yes
	Potential Impact:	Fail to retrieve the performance data from the device.
	Corrective Action:	
	Northbound Alarm Mapping:	dataCollectionFailure
Database Backup Command Execution Failed	Description:	User triggered or scheduled DB backup fails to create the backup file.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes — After next successful scheduled backup.
	Potential Impact:	Database backup not created.
	Corrective Action:	
	Northbound Alarm Mapping:	
Database Backup Upload Operation Failed	Description:	User triggered or scheduled DB backup file is created but fails to SFTP the backup file to the remote file server.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes — After next successful scheduled backup to remote server.
	Potential Impact:	Scheduled database backup not created.
	Corrective Action:	Verify SFTP account used is correct and has correct permissions for remote file server.
	Northbound Alarm Mapping:	

Table A-2 Alarm Detail

Delta Reached	Description:	
	Status:	
	Severity:	Defined by User
	Auto Clearing:	Yes
	Potential Impact:	
	Corrective Action:	
	Northbound Alarm Mapping:	
Device is not Reachable	Description:	Device is not reachable. Device is not SNMP reachable or you cannot ping the device.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	Device will be unreachable.
	Corrective Action:	
	Northbound Alarm Mapping:	networkElementNotReachable
Discovery — Component Added	Description:	
	Status:	Current
	Severity:	Intermediate
	Auto Clearing:	
	Potential Impact:	
	Corrective Action:	
	Northbound Alarm Mapping:	
Discovery — Component Removed	Description:	
	Status:	Current
	Severity:	Intermediate
	Auto Clearing:	
	Potential Impact:	
	Corrective Action:	
	Northbound Alarm Mapping:	

Table A-2 Alarm Detail

HA – Cluster Topology Update Alarm	Description:	Raises an alarm when a node is added to the cluster, removed from the cluster or the active/standby roles change.
	Status:	Current
	Severity:	Warning
	Auto Clearing:	No — User must manually clear the alarm
	Potential Impact:	If a server leaves the cluster the EMS is no longer redundant. Also can signify an HA switchover.
	Corrective Action:	Inspect the node that has left the cluster and bring up the EMS process.
	Northbound Alarm Mapping:	clusterTopologyUpdate
HA Status Change	Description:	Management Server will send this notification to its NB Clients (NMS / OSS) upon its detection of cluster status change.
	Status:	Current
	Severity:	Warning
	Auto Clearing:	No — User must clear
	Potential Impact:	The HA cluster may not be functioning correctly.
	Corrective Action:	Verify that both servers are running with correct active/standby roles.
	Northbound Alarm Mapping:	emsClusterStatusChangeNotification
MySQL Replication — Down	Description:	Database replication is down.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	Data lost after database switchover.
	Corrective Action:	
	Northbound Alarm Mapping:	

Table A-2 Alarm Detail

MySQL Replication — Lagging Behind	Description:	Database replication is lagging behind.
	Status:	Current
	Severity:	Lagging behind between the HA nodes: ■ Critical if replication is lagging behind by 5 minutes ■ Warning if replication is lagging behind by 5 seconds Lagging behind between the DR nodes: ■ Critical if replication is lagging behind by 5 minutes ■ Warning if replication is lagging behind by 30 seconds (between 30 seconds – 5 minutes)
	Auto Clearing:	Yes
	Potential Impact:	Data lost after database switchover.
	Corrective Action:	
	Northbound Alarm Mapping:	
Northbound — Email Publishing Failed	Description:	SMTP configuration or email destination is incorrect.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	No — User must clear
	Potential Impact:	Some alarms may not be sent to the email destination.
	Corrective Action:	Verify SMTP configuration and email destination is correct.
	Northbound Alarm Mapping:	alarmEmailNotificationFailure
Northbound — Trap Forwarding Failed	Description:	Warning – A trap is not supported for forwarding. Critical – The trap destination cannot be reached.
	Status:	Current
	Severity:	Warning/Critical
	Auto Clearing:	No — User must clear
	Potential Impact:	Some traps may not be sent to the trap destination.
	Corrective Action:	Verify trap destination is reachable and receiving alarms.
	Northbound Alarm Mapping:	

Table A-2 Alarm Detail

Security — Dormancy Period Exceeded	Description:	The configured dormancy period has passed and account is locked.
	Status:	Current
	Severity:	Major
	Auto Clearing:	No — Administrator much change user status to active.
	Potential Impact:	User cannot log into Acuitas.
	Corrective Action:	Administrator much change user status to active.
	Northbound Alarm Mapping:	alarmfromElementManagementSystem
Security — Max Login Failed	Description:	After three login failures, the account is locked.
	Status:	Current
	Severity:	Major
	Auto Clearing:	No — Administrator much change user status to active.
	Potential Impact:	User cannot log into Acuitas.
	Corrective Action:	Administrator much change user status to active.
	Northbound Alarm Mapping:	alarmfromElementManagementSystem
SNMP Agent is Down / SNMP Version is not Supported	Description:	The device is not SNMP reachable. The SNMP agent could be down or SNMP Version is not supported.
	Status:	Current
	Severity:	Major
	Auto Clearing:	Yes
	Potential Impact:	Device will be unreachable.
	Corrective Action:	Check if the device is SNMP reachable and enable the SNMP agent on the device.
	Northbound Alarm Mapping:	networkElementNotManageable

Table A-2 Alarm Detail

Threshold Crossing	Description:	Threshold defined by the user for the performance metric has been reached.
	Status:	Current
	Severity:	Defined by User — Minor, Major, Critical
	Auto Clearing:	Yes
	Potential Impact:	None
	Corrective Action:	
	Northbound Alarm Mapping:	Critical — mgmtServerPerfMetricCriticalTCA Major — mgmtServerPerfMetricMajorTCA Minor — mgmtServerPerfMetricMinorTCA
Virtualization – Scale In Failed	Description:	This alarm is generated when the deletion of the VM fails.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	None
	Corrective Action:	
	Northbound Alarm Mapping:	vnfScaleInAlarm
Virtualization – Scale Out Failed	Description:	This alarm is generated when the creation of the VM fails.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	None
	Corrective Action:	
	Northbound Alarm Mapping:	vnfScaleOutAlarm

Table A-2 Alarm Detail

Virtualization – Threshold – In Overload condition	Description:	The respective KPI is transitioned to the following states Overload condition.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	Service impacting because of the overload on the resources
	Corrective Action:	
	Northbound Alarm Mapping:	vnfScaleKpiMonitorAlarm
Virtualization – Threshold – Overload Threshold Crossed for 80% of the Duration (Virtualization)	Description:	Overload threshold crossed for 80% of the duration.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	Service impacting because of the overload on the resources.
	Corrective Action:	
	Northbound Alarm Mapping:	vnfScaleKpiMonitorAlarm
Virtualization – Threshold – Underload Condition	Description:	The respective KPI is transitioned to the following stateUnderload condition.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	Service impacting because of the overload on the resources.
	Corrective Action:	
	Northbound Alarm Mapping:	vnfScaleKpiMonitorAlarm
Virtualization – Threshold – Underload Threshold Crossed for 80% of the Duration (Virtualization)	Description:	Underload threshold crossed for 80% of the duration.
	Status:	Current
	Severity:	Critical
	Auto Clearing:	Yes
	Potential Impact:	Service impacting because of the overload on the resources.
	Corrective Action:	
	Northbound Alarm Mapping:	vnfScaleKpiMonitorAlarm

Acuitas Trap Format

For instructions on viewing alarms, see Viewing Alarms. For instructions on forwarding traps, see Configuring SNMP Alarm Forwarding.

The following Affirmed Networks SNMP Management Information Bases contain Acuitas-forwarded traps and notifications:

- AFFIRMED-TEMS-NOTIFICATION-MIB.mib
- AFFIRMED-TEMS-OBJECTS-MIB.mib
- AFFIRMED-TEMS-SNMP-MIB.mib
- AFFIRMED-TEMS-TC-MIB.mib

The MIBs are located in */opt/Affirmed/NMS/server/ems/mibs*.

You should have a basic understanding of the Simple Network Management Protocol (SNMP) and MIB files in order to read the MIB. The Affirmed Networks MIB is identified by the object identifier (OID) 1.3.6.1.4.1.37963. Each object in the Affirmed Networks MIB has a unique name.

Third-party Traps

Acuitas supports the following third-party traps.

HP Blade System Enclosure iLO Traps

Table A-3 HP Blade System Enclosure iLO Traps

SNMP Trap	Alarm
cpqRackServerBladeRemoved2	**Category:** BladePresence **Severity:** Critical **Source:** Blade[cpqRackServerBladeName] **Message:** `Server blade [cpqRackServerBladeName] removed from position [cpqRackServerBladeName], in enclosure [cpqRackServerBladeEnclosureName], in rack [cpqRackName].`
cpqRackServerBladeInserted2	**Category:** BladePresence **Severity:** Cleared **Source:** Blade[cpqRackServerBladeName] **Message:** `Server blade [cpqRackServerBladeName] inserted into position [cpqRackServerBladePosition], in enclosure [cpqRackServerBladeEnclosureName], in rack [cpqRackName].`
cpqRackEnclosureTempFailed	**Category:** EnclosureTemperature **Severity:** Critical **Source:** Sensor[cpqRackCommonEnclosureTempLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The temperature sensor [cpqRackCommonEnclosureTempLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been set to failed.` **Remedy:** Shutdown the enclosure and possibly the rack as soon as possible. Insure all fans are working properly and that air flow in the rack has not been blocked.

Table A-3 HP Blade System Enclosure iLO Traps

SNMP Trap	Alarm
cpqRackEnclosureTempDegraded	**Category:** EnclosureTemperature **Severity:** Major **Source:** Sensor[cpqRackCommonEnclosureTempLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The temperature sensor [cpqRackCommonEnclosureTempLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been set to failed.` **Remedy:** Shutdown the enclosure and possibly the rack as soon as possible. Insure all fans are working properly and that air flow in the rack has not been blocked.
cpqRackEnclosureTempOk	**Category:** EnclosureTemperature **Severity:** Cleared **Source:** Sensor[cpqRackCommonEnclosureTempLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The temperature sensor [cpqRackCommonEnclosureTempLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been set to ok.`
cpqRackEnclosureFanFailed	**Category:** EnclosureFan **Severity:** Critical **Source:** Fan[cpqRackCommonEnclosureFanLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The fan [cpqRackCommonEnclosureFanLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been set to failed.` **Remedy:** Replace the fan as soon as possible.
cpqRackEnclosureFanDegraded	**Category:** EnclosureFan **Severity:** Major **Source:** Fan[cpqRackCommonEnclosureFanLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The fan [cpqRackCommonEnclosureFanLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been set to degraded.` **Remedy:** Replace the fan as soon as possible.

Table A-3 HP Blade System Enclosure iLO Traps

SNMP Trap	Alarm
cpqRackEnclosureFanOk	**Category:** EnclosureFan **Severity:** Cleared **Source:** Fan[cpqRackCommonEnclosureFanLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The fan [cpqRackCommonEnclosureFanLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been set to ok.`
cpqRackEnclosureFanRemoved	**Category:** FanPresence **Severity:** Minor **Source:** Fan[cpqRackCommonEnclosureFanLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The fan [cpqRackCommonEnclosureFanLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been removed.`
cpqRackEnclosureFanInserted	**Category:** FanPresence **Severity:** Cleared **Source:** Fan[cpqRackCommonEnclosureFanLocation] Enclosure[cpqRackCommonEnclosureTempLocation] Rack[cpqRackName] **Message:** `The fan [cpqRackCommonEnclosureFanLocation] in enclosure [cpqRackCommonEnclosureName] in rack [cpqRackName] has been inserted.`
cpqRackPowerSupplyFailed	**Category:** PowerSupplyStatus **Severity:** Critical **Source:** Supply[cpqRackPowerSupplyPosition] Enclosure [cpqRackPowerSupplyEnclosureName] Rack[cpqRackName] **Message:** `The power supply [cpqRackPowerSupplyPosition] in enclosure [cpqRackPowerSupplyEnclosureName] in rack [cpqRackName] has been set to failed.` **Remedy:** Replace the power supply as soon as possible.

Table A-3 HP Blade System Enclosure iLO Traps

SNMP Trap	Alarm
cpqRackPowerSupplyDegraded	**Category:** PowerSupplyStatus **Severity:** Major **Source:** Supply[cpqRackPowerSupplyPosition] Enclosure [cpqRackPowerSupplyEnclosureName] Rack[cpqRackName] **Message:** `The power supply [cpqRackPowerSupplyPosition] in enclosure [cpqRackPowerSupplyEnclosureName] in rack [cpqRackName] has been set to degraded.` **Remedy:** Replace the power supply as soon as possible.
cpqRackPowerSupplyOk	**Category:** PowerSupplyStatus **Severity:** Cleared **Source:** Supply[cpqRackPowerSupplyPosition] Enclosure [cpqRackPowerSupplyEnclosureName] Rack[cpqRackName] **Message:** `The power supply [cpqRackPowerSupplyPosition] in enclosure [cpqRackPowerSupplyEnclosureName] in rack [cpqRackName] has been set to ok.`
cpqRackPowerSupplyRemoved	**Category:** PowerSupplyPresence **Severity:** Minor **Source:** Supply[cpqRackPowerSupplyPosition] Enclosure [cpqRackPowerSupplyEnclosureName] Rack[cpqRackName] **Message:** `The power supply [cpqRackPowerSupplyPosition] in enclosure [cpqRackPowerSupplyEnclosureName] in rack [cpqRackName] has been removed.`
cpqRackPowerSupplyInserted	**Category:** PowerSupplyPresence **Severity:** Cleared **Source:** Supply[cpqRackPowerSupplyPosition] Enclosure [cpqRackPowerSupplyEnclosureName] Rack[cpqRackName] **Message:** `The power supply [cpqRackPowerSupplyPosition] in enclosure [cpqRackPowerSupplyEnclosureName] in rack [cpqRackName] has been inserted.`

HP Blade iLO Traps

Table A-4 HP Blade iLO Traps

SNMP Trap	Alarm
cpqHe4FltTolPowerSupplyACpowerloss	**Category:** PowerSupplyStatus **Severity:** Critical **Source:** `Chassis`[cpqHeFltTolPowerSupplyChassis] `Bay`[cpqHeFltTolPowerSupplyBay] **Message:** `The Power Supply AC power loss in [cpqHeFltTolPowerSupplyChassis], Bay [cpqHeFltTolPowerSupplyBay], Status [cpqHeFltTolPowerSupplyStatus], Model [cpqHeFltTolPowerSupplyModel], Serial Num [cpqHeFltTolPowerSupplySerialNumber], Firmware [cpqHeFltTolPowerSupplyFirmwareRev].` **Remedy:** Check the power connection to the power supply.
cpqHe4FltTolPowerSupplyOk	**Category:** PowerSupplyStatus **Severity:** Cleared **Source:** `Chassis`[cpqHeFltTolPowerSupplyChassis] `Bay`[cpqHeFltTolPowerSupplyBay] **Message:** `The Power Supply is OK on Chassis [cpqHeFltTolPowerSupplyChassis], Bay [cpqHeFltTolPowerSupplyBay], Status [cpqHeFltTolPowerSupplyStatus], Model [cpqHeFltTolPowerSupplyModel], Serial Num [cpqHeFltTolPowerSupplySerialNumber], Firmware [cpqHeFltTolPowerSupplyFirmwareRev].`
cpqHe3FltTolPowerRedundancyLost	**Category:** PowerSupplyRedundancy **Severity:** Major **Source:** Chassis [cpqHeFltTolPowerSupplyChassis] **Message:** `The Power Supplies are no longer redundant on Chassis [cpqHeFltTolPowerSupplyChassis].`
cpqHe3FltTolPowerRedundancyRestore	**Category:** PowerSupplyRedundancy **Severity:** Cleared **Source:** Chassis [cpqHeFltTolPowerSupplyChassis] **Message:** `The Power Supplies are now redundant on Chassis [cpqHeFltTolPowerSupplyChassis].`

Table A-4 HP Blade iLO Traps

SNMP Trap	Alarm
cpqNic3ConnectivityLost	**Category:** Nic3Connectivity **Severity:** Critical **Source:** Slot[cpqNicIfPhysAdapterSlot] Port[cpqNicIfPhysAdapterPort] **Message:** `Connectivity lost for adapter in slot [cpqNicIfPhysAdapterSlot], port [cpqNicIfPhysAdapterPort].` **Remedy:** Check the cables to the adapter and the Hub or Switch. If no able problems are found, the adapter, Hub, or Switch may need replacement.
cpqNic3ConnectivityRestored	**Category:** Nic3Connectivity **Severity:** Cleared **Source:** Slot[cpqNicIfPhysAdapterSlot] Port[cpqNicIfPhysAdapterPort] **Message:** `Connectivity is restored for adapter in slot[cpqNicIfPhysAdapterSlot], port [cpqNicIfPhysAdapterPort].`
cpqDa6LogDrvStatusChange	**Category:** LogicalDriveStatusChange **Severity:** Critical **Source:** [cpqDaCntlrHwLocation] [cpqDaLogDrvIndex] **Message:** `Status is now [cpqDaLogDrvStatus]` **Remedy:** Is a self-clearing alarm. When the logical drive status changes to OK, CLEARING alarm is generated. All other states including recovering(5) state is also treated as CRITICAL.
cpqDa7PhyDrvStatusChange	**Category:** PhysicalDriveStatusChange **Severity:** Critical **Source:** [cpqDaCntlrHwLocation] [cpqDaPhyDrvIndex] [cpqDaPhyDrvLocationString] **Message:** `Physical Drive Status is now [cpqDaPhyDrvStatus].` **Remedy:** If the physical drive status is failed(3) or predictiveFailure(4), replace the drive. Is a self-clearing alarm. When the physical drive status changes to OK, CLEARING alarm is generated.
cpqDa6AccelStatusChange	**Category:** AcceleratorBoardStatusChange **Severity:** Critical **Source:** Slot[cpqDaCntlrSlot] **Message:** `Status is now [cpqDaAccelStatus].` **Remedy:** If the accelerator board status is permDisabled(5), you might need to replace the accelerator board. Is a self-clearing alarm. When the Cache Module Operation status changes to enabled, a CLEARING alarm is generated. All other states are treated as CRITICAL.

Table A-4 HP Blade iLO Traps

SNMP Trap	Alarm
cpqHe3PostError	**Category:** ServerStart **Severity:** Minor **Message:** `Errors occurred during server restart.` **Remedy:** Is created only when POST errors occur during reboots. It is not a self-clearing alarm. The Operator must manually clear this alarm.
cpqHo2GenericTrap	**Category:** Generic **Severity:** Informational **Message:** `[cpqHoTrapData]`
cpqSm2ServerPowerOn	**Category:** ServerPower **Severity:** Cleared **Message:** `The server has been powered on.`
cpqSm2ServerPowerOff	**Category:** ServerPower **Severity:** Critical **Message:** `The server has been powered off.`

VMware Traps

Table A-5 VMware Traps

SNMP Trap	Alarm
vmwVmPoweredOff	**Category:** VMOperation **Severity:** Major **Source:** [vmwDisplayName] **Message:** `Virtual machine is power off – [vmwVmConfigFilePath].`
vmwVmSuspended	**Category:** VMOperation **Source:** [vmwDisplayName] **Severity:** Warning **Message:** `Virtual Machine is suspended – [vmwVmConfigFilePath].`
vmwVmPoweredOn	**Category:** VMOperation **Severity:** Cleared **Source:** [vmwDisplayName] **Message:** `Virtual machine is power on – [vmwVmConfigFilePath].`

Table A-5 VMware Traps

SNMP Trap	Alarm
vmwVmHBLost	**Category:** Heartbeat **Severity:** Warning **Source:** [vmwDisplayName] **Message:** `Virtual Machine detects a loss in heartbeat.`
vmwVmHBDetected	**Category:** Heartbeat **Severity:** Cleared **Source:** [vmwDisplayName] **Message:** `Virtual Machine detects or regains the required number of guest heartbeats for a given period of time.`

Mapping of VMware ESXi Traps to Acuitas Alarms

The following table lists the VMware ESXi traps that are mapped to Acuitas alarms.

Table A-6 Mapped VMware ESXi Traps

Trap Name	Description
vmwESXEnvHardwareAlert	A hardware alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvBatteryAlert	A battery alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvChassisAlert	A chassis alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvThermalAlert	A cooling/thermal alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvDiskAlert	A disk drive alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvPowerAlert	A power supply alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvProcessorAlert	An IPMI processor alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvMemoryAlert	An IPMI memory alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvBIOSAlert	A BIOS System Event Log alert as received from the Common Infrastructure Management (CIM) subsystem on this system.

VMware ESXi traps use the variable bindings listed in the following table.

Table A-7 VMware ESXi Trap Variable Bindings

VMware ESXi Trap Variable Binding	Description
vmwDescription	Description
vmwEnvEventTime	Time and date the underlying event was first detected. Is set to NULL if the creating entity is unable to provide the information. This value is based on the local date and time of the Managed System Element generating it.
vmwEnvIndicationTime	Time and date that the indication received by the SNMP agent was created.
vmwEnvPerceivedSeverity	Perceived Severity: 1 – Other: Indicates that the Severity's value can be found in the Other Severity property. 2 – Informational: The Alert Indication's severity is informational 3 – Degraded/Warning: Is used to indicate that the user can decide if action is needed 4 – Minor: Is used to indicate that action is needed but is not considered serious 5 – Major: Is used to indicate that action is needed immediately 6 – Critical: Is used to indicate action is needed immediately and the scope is broad (such as, an imminent outage to a critical resource may result). 7 – Fatal/NonRecoverable: Is used to indicate an error occurred, but it is too late to take remedial action.

Table A-7 VMware ESXi Trap Variable Bindings

VMware ESXi Trap Variable Binding	Description
vmwEnvAlertType	Alert Types: 1 – Other: The alert type does not fit into any of the known categories 2 – Communications Alert: An Indication of this type is principally associated with the procedures and/or processes required conveying information from one point to another. 3 – Quality of Service Alert: An Indication of this type is principally associated with a degradation or errors in the performance or function of an entity. 4 – Processing Alert: An Indication of this type is principally associated with software or processing fault. 5 – Device Alert: An Indication of this type is principally associated with an equipment or hardware fault. 6 – Environmental Alert: An Indication of this type is principally associated with a condition relating to an enclosure in which the hardware resides, or other environmental considerations. 7 – Model Change: The Indication addresses changes in the Information Model. For example, it may embed a Lifecycle Indication to convey the specific model change being alerted. 8 – Security Alert: An Indication of this type is associated with security violations, detection of viruses, and similar issues.
vmwEnvSysCreationClassName	Scoping System's CreationClassName for the Provider generating this .
vmwEnvAlertingElement	Identifying information of the entity (the instance) for which this notification is generated. The property contains the CIM path of an CIM object instance, encoded as a string parameter - if the instance is modeled in the CIM Schema. If not a CIM instance, the property contains some identifying string that names the entity for which the Alert is generated. The path or identifying string is formatted per the AlertingElementFormat property.
vmwEnvAlertingFormat	Alerting Format Types: 0 – Unknown: The format is unknown or cannot be interpreted by the CIM client 1 – Other: The format is defined by the value of the OtherAlertingElementFormat property 2 – CIMObjectPath: The format is a CIMObjectPath, with format <NamespacePath>:<ClassName>.<Prop1>=<Value1>, Prop2>=<Value2>, .specifying an instance in the CIM Schema.
vmwEnvSystemName	Name of the system generating this alert.
vmwEnvProviderName	Name of the provider generating this alert.

As the VMware ESXi trap Variable Bindings differ from the fields listed in the Acuitas **Alarms** tab, Acuitas maps the information obtained from the VMWare trap MIBs to the information displayed in the Acuitas **Alarms** tab, as follows:

VMware ESXi Trap Variable Binding		Acuitas Alarms Tab Field
vmwEnvPerceivedSeverity	=>	Severity
vmwEnvAlertingElement	=>	Source ***Note:*** *If the hypervisor is added as a server group, the source field displays the bladindex followed by the value of* ***vmwEnvAlertingElement****. For example:* blade-2 : (vmwEnvAlertingElement)
vmwDescription	=>	Message
vmwEnvEventTime	=>	Updated time ***Note:*** *The time obtained from the VMWare traps (****vmwEnvEventTime****) is converted from hexadecimal notation to a string.*
vmwEnvAlertType	=>	Category ***Note:*** *To distinguish VMWare categories from Acuitas Alarms tab categories,* ***VMWARE*** *is prepended to the category name.*

As the VMware ESXi trap severities (vmwEnvPerceivedSeverity) differ from the values listed in the Acuitas **Alarms** tab, Acuitas maps the information obtained from the VMWare trap MIBs to the information displayed in the Acuitas **Alarms** tab, as follows:

Severity Number	VMware ESXi Trap Severity		Acuitas Alarms Tab Field
0	Unknown	=>	Warning(6)
1	Other	=>	Warning(6)
2	Information	=>	Info(7)
3	Warning	=>	Warning(6)
4	Minor	=>	Minor(5)

Severity Number	VMware ESXi Trap Severity		Acuitas Alarms Tab Field
5	Major	=>	Major(4)
6	Critical	=>	Critical(3)
7	Fatal	=>	Critical(3)

Siemens PCRF and AAA Traps

Siemens PCRF and AAA traps with the trap OID 1.3.6.1.4.1.10548.1.1.1.3.1.1 are mapped to Acuitas events. For a list of supported alarms, see the *Affirmed Networks AAA Alarm Guide*.

Forwarded Trap Mappings

Acuitas-forwarded traps are mapped to one of the traps in the following table.

Table A-8 Forwarded Traps

Trap Name	Description	Variable Bindings
networkElementNotReachable	Network Element Not Reachable Trap Severity: CRITICAL	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
networkElementNotManageable	Network Element Not Manageable Trap Severity: MAJOR	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
networkElementManageable	Network Element Manageable Trap Severity: CLEARED	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
unSupportedNetworkElement Version	Network Element Version Not Supported Trap Severity: CRITICAL	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **networkElementSoftwareVersion**: 1.3.6.1.4.1.37963.6.3.1.2.5 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
cliLoginFailed	CLI Login Failed Trap	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **cliUserName**: 1.3.6.1.4.1.37963.6.3.1.2.6 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
alarmEmailNotificationFailure	Email Notification Failure Trap	**notificationAddress**: 1.3.6.1.4.1.37963.6.3.1.2.7 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18

Table A-8 Forwarded Traps

Trap Name	Description	Variable Bindings
dataCollectionFailure	Data Collection Failure Trap Severity: MAJOR, CLEARED	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **temsServerPerfMetric**: 1.3.6.1.4.1.37963.6.2.1.4.1.1.2 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
temsServerPerfMetricCriticalTCA	Critical Threshold Crossing Alert Trap Severity: CRITICAL	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **temsServerPerfMetric**: 1.3.6.1.4.1.37963.6.2.1.4.1.1.2 **temsServerPerfMetricCollectedValue**: 1.3.6.1.4.1.37963.6.2.1.4.2.1.3 **perfMetricCriticalThreshold**: 1.3.6.1.4.1.37963.6.2.1.5.2.1.3 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
temsServerPerfMetricMajorTCA	Major Threshold Crossing Alert Trap Severity: MAJOR	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **temsServerPerfMetric**: 1.3.6.1.4.1.37963.6.2.1.4.1.1.2 **temsServerPerfMetricCollectedValue**: 1.3.6.1.4.1.37963.6.2.1.4.2.1.3 **perfMetricMajorThreshold**: 1.3.6.1.4.1.37963.6.2.1.5.2.1.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
temsServerPerfMetricMinorTCA	Minor Threshold Crossing Alert Trap Severity: MINOR	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **temsServerPerfMetric**: 1.3.6.1.4.1.37963.6.2.1.4.1.1.2 **temsServerPerfMetricCollectedValue**: 1.3.6.1.4.1.37963.6.2.1.4.2.1.3 **perfMetricMinorThreshold**: 1.3.6.1.4.1.37963.6.2.1.5.2.1.5 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18

Table A-8 Forwarded Traps

Trap Name	Description	Variable Bindings
temsServerPerfMetricClearTCA	Clear Threshold Crossing Alert Trap Severity: CLEARED	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **temsServerPerfMetric**: 1.3.6.1.4.1.37963.6.2.1.4.1.1.2 **temsServerPerfMetricCollectedValue**: 1.3.6.1.4.1.37963.6.2.1.4.2.1.3 **perfMetricClearThreshold**: 1.3.6.1.4.1.37963.6.2.1.5.2.1.9 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
alarmfromNetworkElement	Alarm from Network Element	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **alarmCategory**: 1.3.6.1.4.1.37963.6.3.1.2.9 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmRemedy:** 1.3.6.1.4.1.37963.6.3.1.2.15 **alarmAdditionalInfo**: 1.3.6.1.4.1.37963.6.3.1.2.16 **alarmTrapOID**: 1.3.6.1.4.1.37963.6.3.1.2.17 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
hotStandbyTakesOver	Switchover of the Management server from primary to Standby Server (when the Management Server is deployed in a Primary - HotStandBy mode) *Deprecated*	**alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1
primaryServerisRestored	Primary Management Server has been restored back in Service (when the Management Server is deployed in a Primary - HotStandBy mode) *Deprecated*	**alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1
alarmfromElementManagement System	Alarm from Element management system Severity: CRITICAL, CLEARED, MINOR	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **alarmCategory**: 1.3.6.1.4.1.37963.6.3.1.2.9 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18

Table A-8 Forwarded Traps

Trap Name	Description	Variable Bindings
georedundancyGroupMismatch	Geo Redundancy Mismatch Trap	**sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
vnfScaleKpiMonitorAlarm	Under load or Over load of Resources	**sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
vnfScaleOutAlarm	Adding a VM failed	**sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
vnfScaleInAlarm	Deleting a VM failed	**sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
emsClusterStatusChangeNotification	Cluster status changed	**emsNodeIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.10 **emsClusterChangeNotificationData**: 1.3.6.1.4.1.37963.6.3.1.2.11 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18

Table A-8 Forwarded Traps

Trap Name	Description	Variable Bindings
alarmFromVCenter	Alarm raised due to the occurrence of a trap from VCenter Server	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmCategory**: 1.3.6.1.4.1.37963.6.3.1.2.9 **vCenterTargetObjectType:** 1.3.6.1.4.1.37963.6.3.1.2.14 **vCenterOldStatus:** 1.3.6.1.4.1.37963.6.3.1.2.12 **vCenterNewStatus**:1.3.6.1.4.1.37963.6.3.1.2.13 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
cliLoginSuccess	CLI Login Success Trap	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **cliUserName**: 1.3.6.1.4.1.37963.6.3.1.2.6 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
cliTemplateConfigFailed	CLI Template Configuration Failed	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
cliTemplateConfigSuccess	CLI Template Configuration Success	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
alarmtriggeredCliTemplateConfig Failed	Alarm triggered CLI template configuration failed	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18

Table A-8 Forwarded Traps

Trap Name	Description	Variable Bindings
alarmtriggeredCliTemplateConfig Success	Alarm triggered CLI template configuration success	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
alarmSnmpNotificationFailure	SNMP Notification Failure *Deprecated*	**sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
masterSlaveStandbyNodeDown	Master slave standby node is down Severity: CRITICAL	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
masterSlaveStandbyNodeUp	Master slave standby node is up Severity: CLEARED	**networkElementIPAddress**: 1.3.6.1.4.1.37963.6.3.1.2.4 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18
NBHeartBeat	Management Server sends this notification to its INFORM supported northbound clients to verify the northbound client alive status	
alarmSnmpInformNotificationQueue Monitor	Dynamic SNMP INFORM notification queue monitoring alarms Severity: ■ WARNING when queue reaches WARN threshold limit ■ CRITICAL when queue reaches CRITICAL threshold limit ■ CLEARED when queue size is under control	**sourceComponent**: 1.3.6.1.4.1.37963.6.3.1.2.8 **alarmDiagnosticData**: 1.3.6.1.4.1.37963.6.3.1.2.3 **temsServerTimeStamp**: 1.3.6.1.4.1.37963.6.3.1.2.1 **alarmSeverity**: 1.3.6.1.4.1.37963.6.3.1.2.2 **elementHostName**: 1.3.6.1.4.1.37963.6.3.1.2.18

vCenter Traps

This section describes the categories of vCenter traps and how they are processed in Acuitas.

vpxdAlarmInfo

This notification is sent on entity alarm state change by the vCenter Server SNMP agent. Acuitas generates alarms for this trap based on severity. You can forward the alarms to a trap listener or to an e-mail listener. For instructions, see Forwarding Alarms.

The trap OID is 4.1.6876.4.3.0.203 and uses the varbinds listed in the following table.

Table A-9 vpxdAlarmInfo Trap Variable Bindings

Trap Variable Bindings	Description
vmwVpxdOldStatus	The old status in the notification (string)
vmwVpxdNewStatus	The new status in the notification (string). Trap severity is based on the value of this varbind
vmwVpxdObjValue	The current object value in the notification (string)
vmwVpxdTargetObj	The current object in the notification (string)
vmwVpxdTargetObjType	The alarm target object type (integer)

Acuitas maps the information obtained from this trap to the information displayed in the Acuitas **Alarms** tab, as follows:

Severity Number	vmwVpxdNewStatus Value		Acuitas Alarms Tab Field
1	Red	=>	Critical
2	Yellow	=>	Major
3	Green	=>	Cleared
4	Gray	=>	Intermediate
5	*Any other*	=>	Information

vpxdDiagnostic

This trap is saved only as an event in Acuitas; no alarm is generated. You can configure to forward the saved events toa northbound SNMP trap destination. No filtering is available, as the events are sent directly (without creating/correlating any alarms) to the northbound interface. A new northbound SNMP trap is created in the EMS NOTIFICATIONS for this trap.

To receive and process these vCenter traps, perfrom the procedure in Receiving vCenter Traps.

This trap uses the varbinds listed in the following table.

Table A-10 vCenter Trap Variable Bindings

Trap Variable Binding	Description
vpxdDiagnostic	This notification is sent upon starting or restarting vCenter Server, on requesting a test notification explicitly, and can also be configured to be sent periodically at a specified time interval via vCenter Server configuration by the vCenter Server SNMP agent.

Table A-10 vCenter Trap Variable Bindings

Trap Variable Binding	Description
alarmFromVCenter	Management Server sends this notification to its northbound Clients (NMS / OSS) to report an alarm raised due to the occurrence of a trap from vCenter Server. It provides the details of vCenter event details.

Northbound varbinds mappings to vCenter trap values / varbinds are as follows:

Varbind	**vCenter Event Value**
networkElementIPAddress	vCenterIP
alarmCategory	vCenterAlarm
vCenterTargetObjectType	vmwVpxdTargetObjType is the alarm target object type. Values: { unknown(1), host(2), vm(3), other(4)}
vCenterOldStatus	vmwVpxdOldStatus is the old status in the notification.
vCenterNewStatus	vmwVpxdNewStatus is the new status in the notification.
alarmDiagnosticData	vmwVpxdObjValue is the current object value in the notification. Only the first 2000 characters are included in the Acuitas event and northbound trap.
sourceComponent	vmwVpxdTargetObj is the current object in the notification. It may be one of ESXi host name, VM name, or other.
temsServerTimeStamp	Timestamp when Acuitas trap was received

Receiving vCenter Traps

To receive and process vCenter traps, perform this procedure.

To receive vCenter traps:

1 Use any of the following methods to add the vCenter device to a group:

Settings icon on the toolbar: Select **Topology => Add Element**.

Pop-up menu: Right-click an object in the tree and click **Add Element**.

Acuitas displays the **Add Network Element** window.

2 Configure the parameters as follows, using the values configured on vCenter:

Table A-11 Add Network Element Parameters

Parameter	Description
General Details	
IP Version	Select IPv4 or IPv6.
IP Address	Enter the vCenter IP address (which is the IP address for which Acuitas should collect traps).
Name	Enter the display name of the network element.
Description	Enter the description of the network element.
File Server	Select the file server.
CLI & NETCONF	
User Name	For an MME, enter `admin`. Enter `emsadmin`.
Password/Confirm Password	Enter the password for the user. Acuitas allows upper and lower case letters, numbers, and the following special characters for the CLI/NETCONF password: ([!@#$%^&*]) ***Note:*** *If you change the password on the network element, you must also change that account information here.*
Port	The default port is **2022**. For an MME, enter port 830.
CLI Time Out	Leave as default value.
SFTP	
User Name	Enter `admin`.
Password	Enter the password for the user.

Table A-11 Add Network Element Parameters

Parameter	Description
Port	Enter port 2222.
SNMP	
Read Community	The Read Community string used for sending SNMP requests for data collection from the device. This value must match the value on the network element. The default community string listed in the configuration screen is **affirmed**. Change the value to the vCenter's SNMP Read Community value. vCenter's default Read Community value is **public**.
Location Details Either the Address of the network element.	

3 Click **Save**.

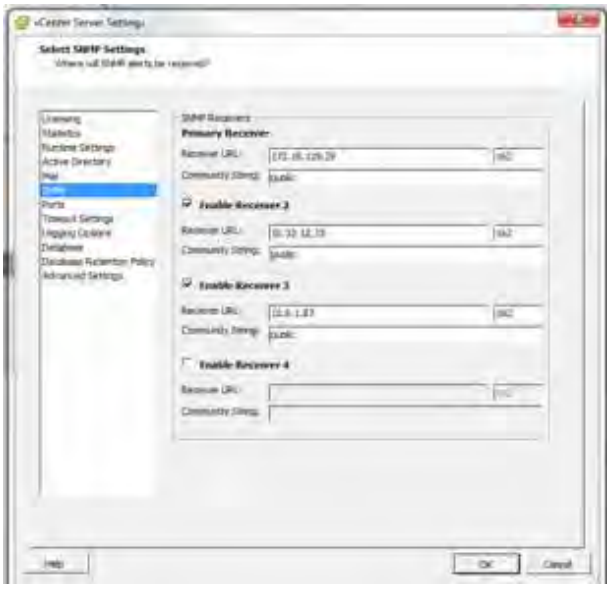
4 Set up the trap destination in vCenter:

a To start the vSphere client, select **Start** > **Programs** > **VMware** > **VMware vSphere Client**.

b Log in using the appropriate username/password.

c Under **Administration**, select **vCenter Server Settings**.

d Click **SNMP**.



e Enter the trap receiver information.

f Click **OK**.

HP 3PAR SAN Traps

The ThreeParMIB.mib contains the SNMPV2 notification alertNotify. On receiving the alertNotify trap from the device, Acuitas generates an alarm or event from the raw PDU.

The trap OID is 1.3.6.1.4.1.12925.1.8 and uses the varbinds listed in the following table.

Table A-12 alertNotify Trap Variable Bindings

3PAR SAN Trap Variable Binding	Description
component	Category
details	Message
severity	Severity: 0 - fatal: indicates an error occurred, but it's too late to take any actions. 1 - critical: an action is needed immediately and scope of the error is broad. 2 - major: an action is needed, the situation is serious. 3 - minor: an action is needed, but the situation is not serious. 4 - degraded/warning: the user decides whether to take an action. 5 - informational: indicates state change or status change, but it's not an error. 6 - debug: information that are logged for later analysis.
timeOccurred	Event time. Is used in event time field. Date time format as 2016-01-15 09:45:05 EST
id	Event ID
state	This field provides information about the state of the alert. new - new alert generated by the system acknowledged - an administrator has acknowledged the alert but may or may not have fixed it, depending on whether remedial action is necessary fixed - remedial action has been taken to fix the alert condition removed - the alert has been removed autofixed - the system has taken action to automatically resolve the alert condition. This varbind decides the alarm as outstanding or cleared. Acuitas clears the alarm based on the state value. When the acknowledged (2) state is received from the device for the existing alarm, Acuitas acknowledges the specific alarm and updates the acknowledged time (As event time from the device).

Acuitas handles the state obtained from this trap is as follows:

State Number	3PAR SAN State	Action
1	New	Raise alarm with severity mapping
2	Acknowledged	Raise or update alarm with severity mapping. The alarm may or may not be fixed.
3	Fixed	Clear the alarm
4	Removed	Update the alarm with description
5	Autofixed	Clear the alarm

Acuitas maps the severity obtained from this trap to the information displayed in the Acuitas **Alarms** or **Events** tab, as follows:

Severity Number	3PAR SAN Severity		Acuitas Alarms or Events Tab Field
0	Fatal	=>	Critical
1	Critical	=>	Critical
2	Major	=>	Major
3	Minor	=>	Minor
4	Degraded/ Warrning	=>	Warning
5	Informational	=>	Informational
6	Debug	=>	Informational

HPE HSS Traps

Acuitas supports the following HPE HSS traps.

Table A-13 HPE HHS Traps

HPE HSS Trap Type	Trap Name	Trap OID
SNMPv1	rtmsMessage	1.3.6.1.4.1.169.3.199.0.1
SNMPv2c/v3	rtmsMessage	1.3.6.1.4.1.169.3.199.0.1

These traps use the varbinds and event mappings listed in the following table.

Table A-14 RTMS Event Trap Variable Bindings and Event Mappings

Varbind Position	Name	Description	Varbind OID	Acuitas Event Mapping
1	trapSSID	Subsystem ID that generated the event	.1.0	Source
2	trapEventNumber	Event number of event	.2.0	Optional field
3	trapSeverity	Severity of the Event: ■ 0 - Informational ■ 1 - Minor ■ 2 - Major ■ 3 - Critical ■ 4 - Clearing	.3.0	Severity
4	trapProcess	Process name that generated the event	.4.0	Source
5	trapGenerationtime	GMT the event was generated, rendered as yyyy-mm-dd hh.mm.ss. Timestamp is system time	.5.0	Event time
6	trapText	The text expansion of the RTMS event	.6.0	Message

Acuitas combines the values of trapSSID and trapProcess varbinds and sets them as the Source in the **Events** tab. Acuitas sets the trap name from MIB as the Category in the **Events** tab.

Acuitas maps the severity obtained from these traps to the information displayed in the Acuitas **Events** tab, as follows:

Severity Number and HP HSS Severity		Acuitas Events Tab Field
0 - Informational	=>	7 - INFORMATIONAL
1 - Minor	=>	5 - MINOR
2 - Major	=>	4 - MAJOR
3 - Critical	=>	3 - CRITICAL
4 - Clearing	=>	1 - CLEARED

VERTICA Traps

Acuitas supports the following traps from Vertica database with trap OID (.1.3.6.1.4.1.31207.2.1.1).

Table A-15 VERTICA Traps

Event Name	Event Type	Description	Remedy
Low Disk Space	0	The database is running out of disk space or a disk is failing or there is an I/O hardware failure.	It is imperative that you add more disk space or replace the failing disk or hardware as soon as possible.
Read Only File System	1	The database does not have write access to the file system for the data or catalog paths. This can sometimes occur if Linux remounts a drive due to a kernel issue.	Modify the privileges on the file system to give the database write access.
Loss Of K Safety	2	The database is no longer K-Safe because there are insufficient nodes functioning within the cluster. Loss of K-safety causes the database to shut down. In a four-node cluster, for example, K-safety=1. If one node fails, the fault tolerance is at a critical level. If two nodes fail, the system loses K-safety.	If a system shuts down due to loss of K-safety, you need to recover the system.
Current Fault Tolerance at Critical Level	3	One or more nodes in the cluster have failed. If the database loses one more node, it is no longer K-Safe and it shuts down. (For example, a four- node cluster is no longer K-safe if two nodes fail.)	Restore any nodes that have failed or been shut down.
Too Many ROS Containers	4	Due to heavy data load conditions, there are too many ROS containers. This occurs when the Tuple Mover falls behind in performing merge out operations. The resulting excess number of ROS containers can exhaust all available system resources. To prevent this, Vertica automatically rolls back all transactions that would load data until the Tuple Mover has time to catch up.	
WOS Over Flow	5	The WOS cannot hold all the data that you are attempting to load. This means that the copy fails and the transaction rolls back.	
Node State Change	6	The node state has changed.	
Recovery Failure	7	The database was not restored to a functional state after hardware or software related failure.	

Table A-15 VERTICA Traps

Event Name	Event Type	Description	Remedy
Recovery Error	8	The database encountered an error while attempting to recover. If the number of recovery errors exceeds Max Tries, the Recovery Failure event is triggered.	
Recovery Lock Error	9	A recovering node could not obtain an S lock on the table. If you have a continuous stream of COPY commands in progress, recovery might not be able to obtain this lock even after multiple re-tries.	
Recovery Projection Retrieval Error	10	Vertica was unable to retrieve information about a projection.	
Refresh Error	11	The database encountered an error while attempting to refresh.	
Refresh Lock Error	12	The database encountered a locking error during refresh.	
Tuple Mover Error	13	The database encountered an error while attempting to move the contents of the Write Optimized Store (WOS) into the Read Optimized Store (ROS).	
Timer Service Task Error	14	An error occurred in an internal scheduled task.	
Stale Checkpoint	15	Data in the WOS has not been completely moved out in a timely manner. An UNSAFE shutdown could require reloading a significant amount of data.	
CRC Mismatch	16	The Cyclic Redundancy Check returned an error or errors while fetching data.	

These traps use the varbinds and event log mappings listed in the following table.

Table A-16 VERTICA Database Trap Variable Bindings and Event Log Mappings

Varbind Position	Varbind OID	VERTICA Database	Acuitas Event Mapping	Example
1	1.3.6.1.4.1.31207.1.1	Event Type		7
2	1.3.6.1.4.1.31207.1.2	Event OID		10001
3	1.3.6.1.4.1.31207.1.3	Event Time		2018-12-31 11:15:05:826715
4	1.3.6.1.4.1.31207.1.4	Event Severity	Severity .4 & .5	Debug(8) and open
5	1.3.6.1.4.1.31207.1.5	Event Status		
6	1.3.6.1.4.1.31207.1.6	Node name	Source .7[.6]	ems-10-32-0-37[v_vertica_viva_node0001]
7	1.3.6.1.4.1.31207.1.7	Host name		
8	1.3.6.1.4.1.31207.1.8	Description	Message	reported by snmp_trap_test() function
9	1.3.6.1.4.1.31207.1.9	Database Name		vertica_Viva
10	1.3.6.1.4.1.31207.1.10	Event Short Description	Category	Recovery Failure

Acuitas maps the severity obtained from these traps to the information displayed in the Acuitas Event log, as follows:

Severity Number and VERTICA Severity		Acuitas Events Log
1 - Emergency	=>	CRITICAL
2 - Alert	=>	CRITICAL
3 - Critical	=>	MAJOR
4 - Error	=>	MINOR
5 - Warning	=>	WARNING
6 - Notice	=>	INFORMATIONAL
7 - Info	=>	INFORMATIONAL
8 -Debug	=>	INFORMATIONAL

Exported Performance Management Data

Acuitas periodically exports the following data to files on the Acuitas server:

- Raw Performance Management data
- Calculated KPI data

The files are exported to the local Acuitas server. You can run a script to push the files from the local Acuitas server to any remote server. For details, see Copying Performance Management Statistics Files to Destination Server.

The export interval is tied to the collection interval, which is currently set to five minutes. By default, Acuitas purges any file older than one day. The purge value can be configured up to seven days. See File Purge Interval.

PerformanceConfiguration.properties

The PerformanceConfiguration.properties file contains configurable attributes to control handling of exported files. If you change any property value, restart the Acuitas server for the new value to take effect.

PerformanceConfiguration.properties is in the directory:

/opt/Affirmed/NMS/server/ems/resources

Export Schedule Interval

You can increase data collection into a shorter interval so that all the exported files are available within *x* minutes of the 5-minute interval. This setting makes exported CSV files available within a particular time period for retrieval by the OSS. The configuration serves the following purposes:

- Distributes collection from a large number of NEs more evenly within the interval to improve performance and scalability of the performance management functions.
- Manages exported PM CSV files for northbound OSS integration to make the files available for OSS at a more predictable time.

Configuration of the schedule interval directly impacts Acuitas performance. Therefore, consult with Affirmed Networks Technical Assistance Center (TAC) before making any changes.

The configurable attributes are:

```
# Randomize Window

DataCollection.schedule.interval.start.millis=15000

DataCollection.schedule.interval.end.millis=135000
```

The above default configuration allows PM collection to be scheduled any time between 30 seconds to 4 minutes of the 5-minute collection interval. The scheduling is performed once when the NE is registered. Therefore, any reconfiguration should be performed at the beginning of the deployment, before the NE's are registered and requires restart of the Acuitas server to take effect.

File Purge Interval

By default, the exported CSV files are purged after one day. If you want to retain the files for up to seven days, specify the number of days by modifying the following configurable attribute:

```
DataCollection.purge.retentionDays=1
```

For example:

```
DataCollection.purge.retentionDays=7
```

If you set a value greater than 7, the retention days is set to 7.

File Time Offset

By default, the CSV files are generated with GMT time. If you want to generate the CSV files with the local time zone, specify the offset from the GMT time by modifying the following configurable attribute:

```
DataCollection.pmstats.gmt.offset=0
```

Set the value in number of hours and minutes. The valid format is (+/-)hh:mm. The range is from -14:00 to +12:00.

For example:

```
DataCollection.pmstats.gmt.offset=-4:30
```

The generated CSV filenames contain the new time stamp and offset. For example:

```
WAGCALLPERFSTATSGRID-2017-09-15-09-54-59-0400.csv
WAGCALLPERFSTATSGRID-2017-09-15-09-54-59+0500.csv
```

Raw Performance Management Data

Acuitas exports raw Performance Management data to the directory:

/opt/Affirmed/NMS/server/ems/data/pm/<node name>

The export filename is <*PM stats table name*>-<*interval timestamp*>.csv, where *interval timestamp* represents the starting timestamp of the export interval.

For example, the following file contains SLOT_STATS for the interval from 19:45 to 19:50:

```
SLOT_STATS-2013-11-16-19-45-00.csv
```

The statistics file contains the following comma-delimited data in order:

- Time of Collection – Beginning interval timestamp in GMT
- Resource ID – Name of the device
- Indices of the PM stats – Such as Cluster ID, Stats Slot (Slot ID)
- Attributes of the PM stats – Such as cpuutil (CPU Utilization) and memutil (Memory Utilization).

The following table lists the statistics tables that do not directly map from any statistics table on the NE. They are generated by transforming the tables obtained from the NE.

Table A-17 Transformed Tables

Table Name	Transformed from these NE tables: *(these tables are not exported in CSV format)*
EMSDPIPROTOCOLSGRID	DPI<*PROTOCOL_CATEGORY*>PROTOCOLSGRID
EMSDPIAPPLICATIONSGRID	DPIAPPLICATIONSGRID
EMSDPIOPERATINGSYSTEMSGRID	DPIOPERATINGSYSTEMSGRID

Calculated KPI Data

Acuitas exports calculated KPI data to the directory:

/opt/Affirmed/NMS/server/ems/data/pm/<node name>

The export filename is <*KPI table name*>-<*interval timestamp*>.csv, where *interval timestamp* represents the starting timestamp of the export interval.

For example, the following file contains PGW KPIs for the interval from 16:15 to 16:20:

`PGW-2014-08-11-16-15-00.csv`

The statistics file contains the following comma-delimited data in order:

- Time of Collection – Beginning interval timestamp in GMT
- Resource ID – Name of the device
- Indices of the KPIs – Such as Zone, PGW
- KPIs

Exported KPIs are grouped into files based on the statistics table from which they are derived, as shown in the following table.

Table A-18 Exported KPI Filenames and Contents

Export Filename (Associated Statistics Table)	KPIs
SGW (SGWPROCEDUREGRID)	sgwEpsAttachSuccessRate, trackingAreaUpdateSuccessRateWithSgwRelocation, trackingAreaUpdateSuccessRateWithoutSgwRelocation, sgwNetworkInitiatedDedicatedBearerCreationRateHandler, sgwPagingSuccessRate, sgwUEInitiatedDedicatedBearerCreationSuccessRate, sgwInterSgwInterSystemHandoverSuccessRate, sgwIntraSgwHandoverSuccessRate ,sgwIntraSgwIntraMmeHandoverSuccessRate, sgwIntraSgwInterMmeHandoverSuccessRate, sgwIntraSgwIntraSgsnHandoverSuccessRate, sgwIntraSgwInterSgsnHandoverSuccessRate, sgwIntraSgwMmetoSgsnHandoverSuccessRate
SGWCALLPERF (SGWCALLPERFSTATSGRID)	sgwTotalNumberOf CurrentCalls, sgwTotalEpsBearerSetup
PGWPROCEDURE (PGWPROCEDUREGRID)	pgwEpsAttachSuccessRate
PGW (PGWCALLPERFSTATSGRID)	pgwNetworkInitiatedDedicatedBearerCreationRateHandler, pgwUEInitiatedDedicatedBearerCreationRateHandler, pgwTotalNumberOfCurrentCalls

Table A-18 Exported KPI Filenames and Contents

Export Filename (Associated Statistics Table)	KPIs
GGSN (GGSNCALLPERFSTATSGRID)	ggsnUmtPdpContextActivationSuccessRate, ggsnStatsCreatePdpContextAccepts, ggsnStatsCreatePdpContextRejects, ggsnStatsDeletePdpContextAccepts, ggsnStatsIdleSessionDurationExceededCloses, ggsnUpdatePdpContextSuccessRate, ggsnReceivedDeletePdpContextSuccessRate, ggsnTransDelPDPContextSuccRate, pgwTotalNumberOfCurrentCalls
CONTENTHTTPPROXYSUMMARY (CONTENTHTTPPROXYSUMMARY STATSGRID)	cacheObjectHitRatio, cacheByteHitRatio, httpProxyClientDownlinkThroughput, httpProxyClientUplinkThroughput, httpProxyServerDownlinkThroughput, httpProxyServerUplinkThroughput, httpProxyTPS, httpProxyTransSuccessRate
DPIGENERAL (DPIGENERALGRID)	dpiTrafficPercentage, dpiUnclassifiedPercentage, protocolNetworkUsagePercentage, applicationNetworkUsagePercentage, osNetworkUsagePercentage
EMSDPIPROTOCOLS (EMSDPIPROTOCOLSGRID)	protocolNetworkUsage, protocolNetworkUsagePercentage
EMSDPIAPPLICATIONS (EMSDPIAPPLICATIONSGRID)	applicationNetworkUsage, applicationNetworkUsagePercentage
GTP (GTPSTATSGRID	gtpTransactionsPerSecond
CONTENTMMSMM1SUMMARY (CONTENTMMSMM1SUMMARY STATSGRID)	mmsTrafficInSendRequests, mmsTrafficInNotifyResponseIndications, mmsTrafficInAcknowledgeIndications, mmsTrafficOutRetrieveConfirmations
EMSDPIOPERATINGSYSTEM EMSDPIOPERATINGSYSTEMGRID)	osNetworkUsage, osNetworkUsagePercentage
RADIUSPROCEDURE (RADIUSPROCEDURESTATS)	radiusAuthenticationSuccessRate
RADIUSPROCEDUREPEER (RADIUSPROCEDURESTATSPEER)	peerRadiusAccountSuccessRate
GWGTPMESSAGE (GWGTPMESSAGESTATS)	ggsnNodeUmtsPdpContextActivationSuccRate
APNCALLPERF (APNCALLPERFSTATSGRID)	apnUplinkPacketDropRate, apnDownlinkPacketDropRate, apnTotalGgsnInitDeletePdpContextReqSuccRate, apnTotalCreatePdpContextSuccessRate, apnTotalCreatePdpContextIpsuccrate, apnAvgDownlinkPacketSize, apnAvgUplinkPacketSize, apnPdpContextDownlinkDataRate, apnPdpContextUplinkDataRate

Copying Performance Management Statistics Files to Destination Server

You can run the configureRemoteServerForCsvPush.sh script to push the exported performance management files from the local Acuitas server to either a local or remote server.

The 5-minute interval CSV files are saved to the directory:

/opt/Affirmed/NMS/server/ems/archive

You can specify to save the daily-exported CSV files to an alternate directory either locally or on the remote server.

Prerequisites

Before you can run the script, follow this procedure to allow SSH access between the local Acuitas server and the remote server.

To configure SSH access for the root user:

Perform these steps on the local Acuitas server:

1. Log into the Acuitas server as the root user and issue the following command:

   ```
   #ssh-keygen –t rsa
   ```

2. Press **Enter** for each of the following prompts:

   ```
   Enter file in which to save the key (/opt/Affirmed/.ssh/id_rsa):
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   ```

   Note: *If the key file already exists, do not overwrite the file.*

3. Issue the following command on the Acuitas server:

   ```
   ssh-copy-id -i ~/.ssh/id_rsa.pub <username>@<remote-server-ip-address>
   Are you sure you want to continue connecting (yes/no)?
   ```

4. Enter **yes**.
5. When prompted, enter the user password.
6. Issue the following command to log into the remote server:

   ```
   ssh <username>@<remote-server-ip-address>
   ```

   Note: *In this case, you are not prompted for a password.*

7. Issue the following command to verify that no extra keys were added:

```
vi ~/.ssh/authorized_keys
```

Note: *If the host keys are later changed, you must perform this procedure again to allow SSH access between the systems.*

Initial Set Up

Before running the script, follow this procedure to specify:

- NEs for which you want to collect data for transfer to the server
- CSV files you want to transfer to the server. (By default, all files are transferred)

To specify the NEs and CSV files:

1. Edit the file /opt/Affirmed/NMS/bin/pm/mcc.nodes.txt (in an HA scenario, edit the file on the active server):

   ```
   $ vi  opt/Affirmed/NMS/conf/pm/mcc.nodes.txt
   ```

2. Add entries (one per line) for the NEs for which you want to collect data. Enter the resource name used when the NE was registered in Acuitas.

   For example:

   ```
   Cluster39
   Cluster24
   ```

3. Save the file.
4. Edit the file /opt/Affirmed/NMS/bin/pm/mcc.files.txt (in an HA scenario, edit the file on the active server):

   ```
   $ vi  opt/Affirmed/NMS/conf/pm/mcc.files.txt
   ```

5. Specify the CSV files you want to transfer. You can use the * character as a wildcard symbol in any position and multiple times. (To transfer all CSV files, skip this step.)

   For example:

   ```
   APNCALLPERFSTATSGRID-*
   ```

   This entry transfers only the APNCALLPERFSTATSGRID files.

6. Save the file.

After the initial setup, you can later modify the list of NEs and CSV files. The next time the cron job runs the script, it picks up the new values from the mcc.nodes.txt and mcc.files.txt files.

Running the Script

Use /opt/Affirmed/NMS/bin/configureRemoteServerForCsvPush.sh to push the exported Performance Management files from the local Acuitas server to either a local or remote server. Run the script individually for each server. In an HA scenario, run the script in the current active server. The script automatically pushes the configuration files to the standby server.

The script performs the following actions:

- Reads mcc.nodes.txt to identify the NEs for which the files are to be copied (in an HA scenario, the script copies the file from the active server to the standby server)
- Reads mcc.files.txt to identify the CSV files to be copied (in an HA scenario, the script copies the file from the active server to the standby server)
- Sets up the cron job to transfer CSV files to the server with a specified time interval (Default: 15 minutes)
- In the case of a local destination server, backs up the CSV files for a specified number of days
- Uses rsync to transfer files to the server

Command Syntax

```
sh configureRemoteServerForCsvPush.sh [ -s ] [ -d ] [ -u ][ -t ] [ -l ]
[ -b ] [ -r ] [ -a ]
```

Argument	Description
-s	serverIpAddress – IP address of the remote server
-d	destinationFolder – Location on the remote server where to copy the 5-minute interval CSV files
-u	username – Username used to log into the remote server
-t	timeInterval – Frequency to run the cron job to copy files, in minutes (Default:15)
-l	localBackupLocation – Location on the local server where to copy the CSV files
-b	localBackupDays – Number of days to back up the CSV files on the local server
-r	archiveBackupFolder – Location on the remote server where to copy the daily-exported CSV files
-a	localArchiveBackupFolder – Location on the local server where to copy the daily-exported CSV files

For example:

```
sh configureRemoteServerForCsvPush.sh -d aapvm11 -d /data -u root -t 20
```

By default, the CSV files are generated with GMT time. To generate the CSV files with the local time zone, specify the offset from the GMT time in the DataCollection.pmstats.gmt.offset property in /opt/Affirmed/NMS/server/ems/resources/PerformanceConfiguration.properties. For details, see File Time Offset.

By default, the backed up CSV files on the local Acuitas server are purged after one day. To retain the files for up to seven days, specify the number of days in the DataCollection.purge.retentionDays property in PerformanceConfiguration.properties file. For details, see File Purge Interval.

VNF Manager and Provisioning REST API

The VNF Manager and Provisioning API provides a northbound Application Programming Interface (API) for use by Network Function Virtualization Orchestrator (NFVO) to control and monitor virtualized MCC and MCC MME clusters in real-time. The API:

- Exposes necessary VIM information for constructing cluster configurations
- Manages cluster configurations as the basis for cluster lifecycle management
- Provides lifecycle management of MCC MCC and MCC MME clusters
- Supports dynamic scaling of MCC MCC and MCC MME clusters
- Supports MCC MCC and MCC MME configuration

The VNF Manager and Provisioning API is a representational state transfer (REST)-based API over HTTPS.

The VNF Manager and Provisioning API supports the following APIs:

- VIM Management APIs
- Cluster Configuration Management APIs
- Lifecycle Management APIs
- Dynamic Scaling APIs
- MCC Configuration APIs
- Network Configuration APIs

Authentication and Authorization

The VNF Manager and Provisioning API uses the HTTP basic authentication and grants access only to users with Tools > Northbound API security group permission.

Note: *For information on the Tools > Northbound API security group permission, see Specifying Permissions by Security Group.*

Accept Request Header (Optional)

The VNF Manager and Provisioning API client can optionally supply an Accept header. If it is supplied by the client, the VNF Manager and Provisioning API requires its value to be application/json, otherwise the client will receive a 406 (Not Acceptable) error.

Error Handling

The VNF Manager and Provisioning APIs use the HTTP status code 500 to report errors.

Response Parameters

Parameter	Type	Description
method	xsd:string	HTTP method
url	xsd:string	URL
code	xsd:int	Application error code (1=error)
description	xsd:string	Error condition description
timestamp	xsd:long	Timestamp (in milliseconds since Epoch time)

Sample Response

```
{
       "method": "POST",
       "code": 1,
       "url": "/rest/vnfm/clusters/cluster-15",
       "description": "Cluster not found",
       "timestamp": 1458235583156
}
```

Audit Log

Access to VNF Manager and Provisioning APIs is logged to the following audit log:

/opt/Affirmed/NMS/server/ems/log/nbapi.log

Sample Log

The following sample log is for the API user `admin`.

```
2016-03-17 13:57:18,284 [api.audit]  - admin: VnfmService: begin -
listClusters
2016-03-17 13:57:18,292 [api.audit]  - admin: VnfmService:   end -
listClusters: done
2016-03-17 13:57:24,476 [api.audit]  - admin: VnfmService: begin -
getCluster: clusterName=cluster-125
2016-03-17 13:57:24,483 [api.audit]  - admin: VnfmService:   end -
getCluster: done
```

Each API operation that causes change to Acuitas or MCC clusters is logged in the Acuitas configuration audit log.

VIM Management APIs

The following table lists the VIM Management APIs:

Table A-19 VIM Management APIs

Functionality	Method	URL	Comment
List VIM instances	GET	/nbapi/rest/vnfm/vims	Returns the list of VIMs managed by VNFM.
List OVA instances	GET	/nbapi/rest/vnfm/vims/{vimId}/ovas	For vCenter: Returns the list of onboard a vCenter {vimId} for MCC deployment. The name must start with “an-”.
List host instances	GET	/nbapi/rest/vnfm/vims/{vimId}/hosts	For vCenter: Returns the list of managed hosts for a vCenter {vimId} for MCC deployment.
Get host details	GET	/nbapi/rest/vnfm/vims/{vimId}/hosts/{hostId}	For vCenter: Returns the list of managed hosts for a vCenter {vimId} for MCC deployment.
List image instances	GET	/nbapi/rest/vnfm/vims/{vimId}/images	For OpenStack: Returns the list of images onboard an OpenStack Controller {vimId} for MCC deployment. The names must start with “an-”.
List network instances	GET	/nbapi/rest/vnfm/vims/{vimId}/networks	For OpenStack: Returns the list of networks configured in OpenStack {vimId} for MCC deployment. The network names must start with “AN”.
List availability zone instances	GET	/nbapi/rest/vnfm/vims/{vimId}/availability-zones	For OpenStack: Returns the list of managed Availability Zone instances configured in OpenStack {vimId} for MCC deployment.
List server group instances	GET	/nbapi/rest/vnfm/vims/{vimId}/server-groups	For OpenStack: Returns the list of Server Group instances configured in OpenStack {vimId} for MCC deployment. The names must start with “an“.
List flavor instances	GET	/nbapi/rest/vnfm/vims/{vimId}/flavors	For OpenStack: Returns the list of flavors configured in OpenStack {vimId} for MCC deployment. The names must start with “AN-“.

The following sections describe the details of each API.

List VIMs

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
vims	xsd:list		List of VIM objects
id	xsd:long		VIM ID
name	xsd:string	max-length: 50	VIM name
type	xsd:string	enum: ■ vcenter ■ openstack	VIM type
ipAddr	xsd:string	max-length: 39	VIM IP address

Sample Response

```
{
       "vims": [{
          "id": 2,
          "name": "VC-5.5",
          "type": "vcenter",
          "ipAddr": "10.32.2.144"
       }, {
          "id": 3,
```

```
            "name": "VC-6.0",
            "type": "vcenter",
            "ipAddr": "10.32.6.146"
        }, {
            "id": 4,
            "name": "OS-ubuntu-liberty",
            "type": "openstack",
            "ipAddr": "10.32.9.170"
        }, {
            "id": 5,
            "name": "OS-redhat-juno",
            "type": "openstack",
            "ipAddr": "10.33.0.225"
        }]
}
```


List OVAs

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/ovas

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
ovas	xsd:list		List of OVA objects
id	xsd:long		OVA ID
name	xsd:string	max-length: 255	OVA name

Parameter	Type	Constraint	Description
type	xsd:string	enum: ■ mcm ■ ccm ■ ssm	OVA type
version	xsd:string	max-length: 50	OVA version

Sample Response

```
{
       "ovas": [{
           "id": 1,
           "name": "an-6.3.0.0-310.REL_CSM-C8.M32768-props.ova",
           "type": "csm",
           "version": "6.3.0.0"
       }, {
           "id": 2,
           "name": "an-6.3.0.0-310.REL_MCM-C8.M8192-props.ova",
           "type": "mcm",
           "version": "6.3.0.0"
       }, {
           "id": 3,
           "name": "an-6.3.0.0-310.REL_SSM-C7.M32768-props.ova",
           "type": "ssm",
           "version": "6.3.0.0"
       }]
}
```

List Hosts

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/hosts

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
hosts	xsd:list		List of Host objects
id	xsd:long		Host ID
name	xsd:string	max-length: 64	Host name

Sample Response

```
{
       "hosts": [{
          "id": 3,
          "name": "10.32.0.159"
       }, {
          "id": 4,
          "name": "10.32.0.151"
       }, {
          "id": 6,
          "name": "10.33.10.126"
       }]
}
```

Get Host Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/hosts/{hostId}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
hosts	xsd:list		List of Host objects
id	xsd:long		Host ID
name	xsd:string	max-length: 64	Host name
datastore	xsd:string	max-length: 64	Datastore name
mgmt	xsd:string	max-length: 64	Management network
base1	xsd:string	max-length: 64	Base 1 network
base2	xsd:string	max-length: 64	Base 2 network
ew1	xsd:string	max-length: 64	East/West 1 network
ew2	xsd:string	max-length: 64	East/West 2 network
ns1	xsd:string	max-length: 64	North/South 1 network
ns2	xsd:string	max-length: 64	North/South 2 network

Sample Response


```
{
       "id": 3,
       "name": "10.32.0.159",
       "datastore": "local_10_32_0_159_datastore",
       "mgmtNw": "AN Management 1 Network",
       "base1Nw": "AN Base 1 Network",
       "base2Nw": "AN Base 2 Network",
       "ew1Nw": "AN East-West 1 Network",
       "ew2Nw": "AN East-West 2 Network",
       "ns1Nw": "AN North-South 1 Network",
       "ns2Nw": "AN North-South 2 Network"
}
```

List Images

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/images

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
images	xsd:list		List of Image objects
name	xsd:string	max-length: 64	Image name
type	xsd:string	enum: ■ controller ■ payload	Image type

Sample Response

```
{
       "images": [{
          "name": "an-6.1.2.0-110.REL-controller",
          "type": "controller"
       }, {
          "name": "an-6.1.2.0-110.REL-payload",
          "type": "payload"
       }]
}
```

List Networks

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/networks

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
networks	xsd:list		List of Network objects
name	xsd:string	max-length: 64	Network name

Sample Response

```
{
       "networks": [{
           "name": "AN Base 1 Network"
       }, {
           "name": "AN EW 1 Network PF"
       }, {
           "name": "AN MGMT Network"
       }, {
           "name": "AN NS 1 Network PF"
       }, {
           "name": "AN NS 2 Network PF"
       }]
}
```

List Availability Zones

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/availability-zones

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
availabilityZones	xsd:list		List of Availability Zone objects
id	xsd:long		Availability Zone ID
name	xsd:string	max-length: 64	Availability Zone name

Sample Response

```
{
       "availabilityZones": [{
          "id": 17,
          "name": "an-zone-1"
       }, {
          "id": 18,
          "name": "an-zone-2"
       }]
}
```

List Server Groups

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/server-groups

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
serverGroups	xsd:list		List of Server Group objects
name	xsd:string	max-length: 64	Server group name

Sample Response

```
{
       "serverGroups": [{
           "name": "an-mcc-csm-anti-affinity"
       }, {
           "name": "an-mcc-mcm-anti-affinity"
       }, {
           "name": "an-mcc-ssm-anti-affinity"
       }]
}
```

List Flavors

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/flavors

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
flavors	xsd:list		List of Flavor objects
name	xsd:string	max-length: 64	Flavor name

Sample Response

```
{
       "flavors": [{
           "name": "AN-CCM"
       }, {
           "name": "AN-DCM"
       }, {
           "name": "AN-IOM"
       }, {
           "name": "AN-MCM"
       }, {
           "name": "AN-WSM"
       }]
}
```

Cluster Configuration Management APIs

The following table lists the Cluster Configuration Management APIs:

Table A-20 Cluster Configuration Management APIs

Functionality	Method	URL	Comment
List Cluster Configuration	GET	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs	Returns the list of Cluster Configuration instances managed by VIM {vimId}.
Put Cluster Configuration	PUT	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs	Puts a Cluster Configuration instance for VIM {vimId}.
Put Cluster OVA Configuration	PUT	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusterConfigId} /ovas	For vCenter: Puts OVAs for a Cluster Configuration instance {clusterConfigId} managed by VIM {vimId}.
Put Cluster Image Configuration	PUT	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusterConfigId} /images	For OpenStack: Puts images for a Cluster Configuration instance {clusterConfigId} managed by VIM {vimId}.
GET Cluster Configuration Details	GET	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusterConfigId}	Returns the Cluster Configuration instance identified by {clusterConfigId} managed by VIM {vimId}.
List Node Configurations	GET	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusteConfigId}/ node-configs	Returns the list of Node Configuration instances contained by Cluster Configuration {clusterConfigId} managed by VIM {vimId}.
Put Node Configuration	PUT	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusterConfigId} /node-configs	Puts a Node Configuration instance for a Cluster Configuration {clusterConfigId} managed by VIM {vimId}.
Get Node Configuration Details	GET	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusterConfigId} /node-configs/{nodeConfigId}	Returns the Node Configuration instance for a Node Configuration {nodeConfigId} in a Cluster Configuration {clusterConfigId} managed by VIM {vimId}.
Delete Node Configuration	DELETE	nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusterConfigId} /node-configs/{nodeConfigId}	Removes a Node Configuration with {nodeConfigId} for a Cluster Configuration {clusterConfigId} managed by VIM {vimId}.

Table A-20 Cluster Configuration Management APIs

Functionality	Method	URL	Comment
Delete Cluster Configuration	DELETE	/nbapi/rest/vnfm/vims/{vimId}/ cluster-configs/{clusterConfigId}	Removes a Cluster Configuration {clusterConfigId} managed by VIM {vimId}.

The following table lists the cluster configuration attributes that apply to the corresponding VIM and cluster types (MCC, MCC MME).

Table A-21 Cluster Configuration Attributes (R = Required, A = Applicable)

Attribute	MCC			MCC MME
	vCenter	OpenStack	vCloudDirector	OpenStack
id	**R (for updates)**	**R (for updates)**		**R (for updates)**
clusterId	**R**	**R**		**R**
name	**R**	**R**		**R**
strategy	**R**	**R**		
sriovConfig	**R**	**R**		
ewRedundant	**R**	**R**		
ewVlanAEdp				**R (for EDP SR-IOV)**
ewVlanBEdp				**R (for EDP SR-IOV)**
baseVlanA	**R**	**R**		**A**
baseVlanB	**R**	**R**		
ewVlanA	**R**	**R**		**A**
ewVlanB	**R**	**R**		
diskFormat	**R**			
logicalIp	**R**	**R**		**R**
ntpIp	**R**	**R**		**R**
enableRootSshAccess	**R**	**R**		
enablePasswordAging				

Table A-21 Cluster Configuration Attributes (R = Required, A = Applicable)

Attribute	MCC			MCC MME
	vCenter	OpenStack	vCloudDirector	OpenStack
enableMultipleSession	**R**	**R**		
enableTelnetAccess				
vimId	**R**	**R**		**R**
mcmTemplateId	**R**			
csmTemplateId	**R**			
ssmTemplateId	**R**			
controllerImage		**R**		**R**
payloadImage		**R**		
mgmtNw		**R**		**R**
base1Nw		**R**		**R**
base2Nw		**A**		
ew1Nw		**R**		**R**
ew2Nw		**A**		
ew1NwEdp				**R (for EDP deployment)**
ew2NwEdp				**R (for EDP deployment)**
ns1Nw		**R**		**R**
ns2Nw		**R**		**R**
ns3Nw		**A**		**A**
ns4Nw		**A**		**A**
ns5Nw		**A**		**A**
ns6Nw		**A**		**A**
ns7Nw		**A**		**A**
ns8Nw		**A**		**A**
ns9Nw		**A**		**A**
ns10Nw		**A**		**A**

Table A-21 Cluster Configuration Attributes (R = Required, A = Applicable)

Attribute	MCC			MCC MME
	vCenter	OpenStack	vCloudDirector	OpenStack
ns11Nw		A		A
ns12Nw		A		A
ns13Nw		A		A
ns14Nw		A		A
ns15Nw		A		A
ns16Nw		A		A
ns17Nw		A		A
ns18Nw		A		A
ns19Nw		A		A
ns20Nw		A		A
ns21Nw		A		A
ns22Nw		A		A
ns23Nw		A		A
ns24Nw		A		A
vlanStrippingEnabled		R		
controllerBootSize		R		R
payloadBootSize		R		
mcmVappTemplate				
csmVappTemplate				
ssmVappTemplate				
clusterType	R	R		R
mgmt2Nw				R
cinderEnabled		A		R
controllerEphSize				R
payloadEphSize				R
securityGroup		A		R

The following table lists the node configuration attributes that apply to the corresponding VIM and cluster types (MCC, MCC MME).

Table A-22 Node Configuration Attributes (R = Required, A = Applicable)

Attribute	MCC			MCC MME
	vCenter	OpenStack	vCloudDirector	OpenStack
id	**R (for updates)**	**R (for updates)**		**R (for updates)**
nodeId	**R**	**R**		
name	**R**	**R**		**R**
instantiationOrder	**A**	**A**		**A**
nodeType	**R**	**R**		**R**
nodePersonality	**R**	**R**		
containerId	**R**	**R**		**R**
reserved	**R**	**R**		**R**
cpu	**R**			
cpuAffinity	**R**			
memory	**R**			
flavor		**R**		**R**
serverGroup		**A**		**A**
mgmtIp	**R**	**R**		**R**
gatewayIp	**R**	**R**		**R**
mgmtVlan	**R**	**R**		**R**
netmask	**R**	**R**		**R**
ns1Nw		**A**		**R (for EDP SR-IOV enabled node)**
ns2Nw		**A**		**R (for EDP SR-IOV enabled node)**
ns3Nw		**A**		**A**
ns4Nw		**A**		**A**

Table A-22 Node Configuration Attributes (R = Required, A = Applicable)

Attribute	MCC			MCC MME
	vCenter	OpenStack	vCloudDirector	OpenStack
ns5Nw		A		A
ns6Nw		A		A
ns7Nw		A		A
ns8Nw		A		A
ns9Nw		A		A
ns10Nw		A		A
ns11Nw		A		A
ns12Nw		A		A
ns13Nw		A		A
ns14Nw		A		A
ns15Nw		A		A
ns16Nw		A		A
ns17Nw		A		A
ns18Nw		A		A
ns19Nw		A		A
ns20Nw		A		A
ns21Nw		A		A
ns22Nw		A		A
ns23Nw		A		A
ns24Nw		A		A
disk		A		
vappName				
serviceRole				R
ns1Ip		A		R (for LB, DATA, MSM, and EDP nodes)

Table A-22 Node Configuration Attributes (R = Required, A = Applicable)

Attribute	MCC			MCC MME
	vCenter	OpenStack	vCloudDirector	OpenStack
ns2Ip		A		R (for LB, DATA, MSM, and EDP nodes)
ns3Ip		A		A
ns4Ip		A		A
ns5Ip		A		A
ns6Ip		A		A
ns7Ip		A		A
ns8Ip		A		A
ns9Ip		A		A
ns10Ip		A		A
ns11Ip		A		A
ns12Ip		A		A
ns13Ip		A		A
ns14Ip		A		A
ns15Ip		A		A
ns16Ip		A		A
ns17Ip		A		A
ns18Ip		A		A
ns19Ip		A		A
ns20Ip		A		A
ns21Ip		A		A
ns22Ip		A		A
ns23Ip		A		A
ns24Ip		A		A

The following sections describe the details of each API.

List Cluster Configurations

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
clusterConfigs	xsd:list		List of Cluster Configuration objects
id	xsd:long		Cluster configuration id
name	xsd:string	max-length: 50	Cluster configuration name
clusterId	xsd:long	range: 1-127	Cluster ID
active	xsd:boolean		Indicator whether the cluster configuration is being used by an instantiated cluster. If the cluster configuration is active, no modification to it is allowed except the images.

Sample Response

```
{
       "clusterConfigs": [{
           "id": 2,
           "name": "cluster-7",
           "clusterId": 7,
           "active": true
       }, {
           "id": 7,
           "name": "cluster-23",
           "clusterId": 23,
           "active": false
       }]
}
```

Put Cluster Configurations

Request Method

PUT

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
id	xsd:long		ID of the cluster configuration object. **Important**: When creating a new cluster configuration, the ID must be null, because it is internally created by the VNF Manager. When updating an existing cluster configuration, you must supply the ID.
name	xsd:string	max-length: 50	Cluster configuration name
clusterId	xsd:long	range: 1-127	Cluster ID

Parameter	Type	Constraint	Description
strategy	xsd:string	enum: ■ compact ■ advanced-services-separation ■ control-services-separation ■ specialized	Building block strategy
sriovConfig	xsd:string	enum: ■ none ■ ew_ns ■ ew_ns_base_mgmt (OpenStack only)	Specify the networks supporting SR-IOV
ewRedundant	xsd:boolean		Indicator whether to enable East/West network redundancy
baseVlanA	xsd:int		Base network VLAN ID A
baseVlanB	xsd:int		Base network VLAN ID B
ewVlanA	xsd:int		East/West network VLAN ID A
ewVlanB	xsd:int		East/West network VLAN ID B
epdEwVlanA	xsd:int		OpenStack only: EDP East/West network VLAN ID A
epdEwVlanB	xsd:int		OpenStack only: EDP East/West network VLAN ID B
diskFormat	xsd:string	enum: ■ thin ■ eagerZeroedThick	vCenter only: Disk format
logicalIp	xsd:string	max-length: 39	Logical IP address
ntpIp	xsd:string	max-length: 39	NTP IP address
enableRootSshAccess	xsd:boolean		Indicator whether to enable root ssh access
enablePasswordAging	xsd:boolean		Indicator whether to enable password aging
enableMultipleSession	xsd:boolean		Indicator whether to enable multiple sessions
enableTelnetAccess	xsd:boolean		Indicator whether to enable telnet access
vimId	xsd:long		The vimId of the managing VIM

Parameter	Type	Constraint	Description
mcmTemplateId	xsd:long		vCenter only: OVA template ID for MCM node type
csmTemplateId	xsd:long		vCenter only: OVA template ID for CSM node type
ssmTemplateId	xsd:long		vCenter only: OVA template ID for SSM node type
controllerImage	xsd:string	max-length: 64	OpenStack only: Controller image name for MCM node type
payloadImage	xsd:string	max-length: 64	OpenStack only: Payload image image name for CSM and SSM node types
mgmtNw	xsd:string	max-length: 64	OpenStack only: Management network name
base1Nw	xsd:string	max-length: 64	OpenStack only: Base 1 network name
base2Nw	xsd:string	max-length: 64	OpenStack only: Base 2 network name
ew1Nw	xsd:string	max-length: 64	OpenStack only: East/West 1 network name
ew2Nw	xsd:string	max-length: 64	OpenStack only: East/West 2 network name
ew1NwEpd	xsd:string	max-length: 64	OpenStack only: The East/West 1 network name for EDP deployment
ew2NwEpd	xsd:string	max-length: 64	OpenStack only: The East/West 2 network name for EDP deployment
ns1Nw	xsd:string	max-length: 64	OpenStack only: North/South 1 network name
ns2Nw	xsd:string	max-length: 64	OpenStack only: North/South 2 network name
ns3Nw	xsd:string	max-length: 64	OpenStack only: North/South 3 network name
ns4Nw	xsd:string	max-length: 64	OpenStack only: North/South 4 network name
ns5Nw	xsd:string	max-length: 64	OpenStack only: North/South 5 network name
ns6Nw	xsd:string	max-length: 64	OpenStack only: North/South 6 network name

Parameter	Type	Constraint	Description
ns7Nw	xsd:string	max-length: 64	OpenStack only: North/South 7 network name
ns8Nw	xsd:string	max-length: 64	OpenStack only: North/South 8 network name
ns9Nw	xsd:string	max-length: 64	OpenStack only: North/South 9 network name
ns10Nw	xsd:string	max-length: 64	OpenStack only: North/South 10 network name
ns11Nw	xsd:string	max-length: 64	OpenStack only: North/South 11 network name
ns12Nw	xsd:string	max-length: 64	OpenStack only: North/South 12 network name
ns13Nw	xsd:string	max-length: 64	OpenStack only: North/South 13 network name
ns14Nw	xsd:string	max-length: 64	OpenStack only: North/South 14 network name
ns15Nw	xsd:string	max-length: 64	OpenStack only: North/South 15 network name
ns16Nw	xsd:string	max-length: 64	OpenStack only: North/South 16 network name
ns17Nw	xsd:string	max-length: 64	OpenStack only: North/South 17 network name
ns18Nw	xsd:string	max-length: 64	OpenStack only: North/South 18 network name
ns19Nw	xsd:string	max-length: 64	OpenStack only: North/South 19 network name
ns20Nw	xsd:string	max-length: 64	OpenStack only: North/South 20 network name
ns21Nw	xsd:string	max-length: 64	OpenStack only: North/South 21 network name
ns22Nw	xsd:string	max-length: 64	OpenStack only: North/South 22 network name
ns23Nw	xsd:string	max-length: 64	OpenStack only: North/South 23 network name
ns24Nw	xsd:string	max-length: 64	OpenStack only: North/South 24 network name

Parameter	Type	Constraint	Description
vlanStrippingEnabled	xsd:boolean		Enables VLAN stripping. Set to True for OpenStack deployments that do not allow Flat Networks and instead manage VLAN tagged traffic before the traffic arrives at the MCC. In these cases, network interfaces within the MCC must be configured as untagged. Untagged packets sent from the MCC are tagged by the OpenStack controller.
controllerBootSize	xsd:int		Controller boot size
payloadBootSize	xsd:int		Payload boot size
mcmVappTemplate	xsd:string	max-length: 64	VCenter only: vAPP template for mcm node type
csmVappTemplate	xsd:string	max-length: 64	VCenter only: The vAPP template for csmnode type
ssmVappTemplate	xsd:string	max-length: 64	VCenter only: The vAPP template for ssm node type
clusterType	xsd:string	max-length: 64	Cluster type (MCC or MCC MME)
mgmt2Nw	xsd:string	max-length: 64	OpenStack only: The management 2 network name
cinderEnabled	xsd:boolean		Indicator whether to enable cinder
controllerEphSize	xsd:int		Controller Ephemera size
payloadEphSize	xsd:int		Payload Ephemera size
securityGroup	xsd:string	max-length: 64	Security group

Sample Request

```
{
        "name":"mme-90",
        "clusterId":90,
        "strategy":"na",
        "sriovConfig":none,
        "ewRedundant":false,
        "vlanStrippingEnabled":false,
        "baseVlanA":0,
        "baseVlanB":0,
        "ewVlanA":0,
        "ewVlanB":0,
```

```
"ewVlanAEdp": 0,
"ewVlanBEdp": 0,
"diskFormat":"thin",
"logicalIp":"10.168.200.70",
"ntpIp":"172.162.39.2",
"enableRootSshAccess":false,
"enableMultipleSession":false,
"vimId":4,
"mcmTemplateId":"",
"csmTemplateId":"",
"ssmTemplateId":"",
"controllerImage":"epc-11.0.09-fixes",
"payloadImage":"",
"mgmtNw":"epc-oam-vlan361",
"base1Nw":"vmc090-base",
"base2Nw":"",
"ew1Nw":"vmc090-eastwest",
"ew2Nw":"",
"ew1NwEdp": "saegw016-eastwest1",
"ew2NwEdp": "saegw016-eastwest2",
"ns1Nw":"epc-access-vlan305",
"ns2Nw":"epc-core-vlan325",
"ns3Nw":"",
"ns4Nw":"",
"ns5Nw":"",
"ns6Nw":"",
"ns7Nw":"",
"ns8Nw":"",
"ns9Nw":"",
"ns10Nw":"",
"ns11Nw":"",
"ns12Nw":"",
"ns13Nw":"",
"ns14Nw":"",
"ns15Nw":"",
"ns16Nw":"",
"ns17Nw":"",
"ns18Nw":"",
"ns19Nw":"",
"ns20Nw":"",
"ns21Nw":"",
"ns22Nw":"",
"ns23Nw":"",
```

```
        "ns24Nw":"",
        "enablePasswordAging":false,
        "enableTelnetAccess":false,
        "controllerBootSize":0,
        "payloadBootSize":0,
        "mcmVappTemplate":"",
        "csmVappTemplate":"",
        "ssmVappTemplate":"",
        "clusterType":"",
        "mgmt2Nw":"",
        "cinderEnabled":false,
        "controllerEphSize":0,
        "payloadEphSize":0,
        "securityGroup":""
}
```


Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Cluster configuration ID
name	xsd:string	max-length: 64	Cluster configuration name

Sample Response


```
{
        "id": 23,
        "name": "mme-90"
}
```

Put Cluster OVA Configuration

Request Method

PUT

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}/ovas

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
mcmTemplateId	xsd:long		OVA template ID for MCM node type
csmTemplateId	xsd:long		OVA template ID for CSM node type
ssmTemplateId	xsd:long		OVA template ID for SSM node type

Sample Request

```
{
       "mcmTemplateId": 2,
       "csmTemplateId": 1,
       "ssmTemplateId": 3,
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Cluster configuration ID
name	xsd:string	max-length: 50	Cluster configuration name

Sample Response

```
{
       "id": 2,
       "name": "cluster-7"
}
```

Put Cluster Image Configuration

Request Method

PUT

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}/images

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
controllerImage	xsd:string	max-length: 64	Controller image name for MCM node type
payloadImage	xsd:string	max-length: 64	Payload image name for CSM and SSM node types

Sample Request

```
{
        "controllerImage": "an-6.1.2.0-110.REL-controller",
        "payloadImage": "an-6.1.2.0-110.REL-payload"
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Cluster configuration ID
name	xsd:string	max-length: 50	Cluster configuration name

Sample Response

```
{
       "id": 4,
       "name": "cluster-125"
}
```

Get Cluster Configuration Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Cluster configuration ID
name	xsd:string	max-length: 50	Cluster configuration name
clusterId	xsd:long	range: 1-127	Cluster ID

Parameter	Type	Constraint	Description
strategy	xsd:string	enum: ■ compact ■ advanced-services-separation ■ control-services-separation ■ specialized	Building block strategy
sriovConfig	xsd:string	enum: ■ none ■ ew_ns ■ ew_ns_base_mgmt (OpenStack only)	Networks supporting SR-IOV
ewRedundant	xsd:boolean		Indicator whether to enable East/West network redundancy
baseVlanA	xsd:int		Base network VLAN ID A
baseVlanB	xsd:int		Base network VLAN ID B
ewVlanA	xsd:int		East/West network VLAN ID A
ewVlanB	xsd:int		East/West network VLAN ID B
epdEwVlanA	xsd:int		EDP East/West network VLAN ID A
epdEwVlanB	xsd:int		EDP East/West network VLAN ID B
diskFormat	xsd:string	enum: ■ thin ■ eagerZeroedThick	vCenter only: Disk format
logicalIp	xsd:string	max-length: 39	Logical IP address
ntpIp	xsd:string	max-length: 39	NTP IP address
enableRootSshAccess	xsd:boolean		Indicator whether to enable root ssh access
enablePasswordAging	xsd:boolean		Indicator whether to enable password aging
enableMultipleSession	xsd:boolean		Indicator whether to enable multiple session
enableTelnetAccess	xsd:boolean		Indicator whether to enable telnet access

Parameter	Type	Constraint	Description
vimId	xsd:long		ID of the managing VIM
mcmTemplateId	xsd:long		vCenter only: OVA template ID for MCM node type
csmTemplateId	xsd:long		vCenter only: OVA template ID for CSM node type
ssmTemplateId	xsd:long		vCenter only: OVA template ID for SSM node type
controllerImage	xsd:string	max-length: 64	OpenStack only: Controller image name for MCM node type
payloadImage	xsd:string	max-length: 64	OpenStack only: Payload image name for CSM and SSM node types
mgmtNw	xsd:string	max-length: 64	OpenStack only: Management network name
base1Nw	xsd:string	max-length: 64	OpenStack only: Base 1 network name
base2Nw	xsd:string	max-length: 64	OpenStack only: Base 2 network name
ew1Nw	xsd:string	max-length: 64	OpenStack only: East/West 1 network name
ew2Nw	xsd:string	max-length: 64	OpenStack only: East/West 2 network name
ew1NwEpd	xsd:string	max-length: 64	OpenStack only: The East/West 1 network name for EDP deployment
ew2NwEpd	xsd:string	max-length: 64	OpenStack only: The East/West 2 network name for EDP deployment
ns1Nw	xsd:string	max-length: 64	OpenStack only: North/South 1 network name
ns2Nw	xsd:string	max-length: 64	OpenStack only: North/South 2 network name
ns3Nw	xsd:string	max-length: 64	OpenStack only: North/South 3 network name
ns4Nw	xsd:string	max-length: 64	OpenStack only: North/South 4 network name
ns5Nw	xsd:string	max-length: 64	OpenStack only: North/South 5 network name

Parameter	Type	Constraint	Description
ns6Nw	xsd:string	max-length: 64	OpenStack only: North/South 6 network name
ns7Nw	xsd:string	max-length: 64	OpenStack only: North/South 7 network name
ns8Nw	xsd:string	max-length: 64	OpenStack only: North/South 8 network name
ns9Nw	xsd:string	max-length: 64	OpenStack only: North/South 9 network name
ns10Nw	xsd:string	max-length: 64	OpenStack only: North/South 10 network name
ns11Nw	xsd:string	max-length: 64	OpenStack only: North/South 11 network name
ns12Nw	xsd:string	max-length: 64	OpenStack only: North/South 12 network name
ns13Nw	xsd:string	max-length: 64	OpenStack only: North/South 13 network name
ns14Nw	xsd:string	max-length: 64	OpenStack only: North/South 14 network name
ns15Nw	xsd:string	max-length: 64	OpenStack only: North/South 15 network name
ns16Nw	xsd:string	max-length: 64	OpenStack only: North/South 16 network name
ns17Nw	xsd:string	max-length: 64	OpenStack only: North/South 17 network name
ns18Nw	xsd:string	max-length: 64	OpenStack only: North/South 18 network name
ns19Nw	xsd:string	max-length: 64	OpenStack only: North/South 19 network name
ns20Nw	xsd:string	max-length: 64	OpenStack only: North/South 20 network name
ns21Nw	xsd:string	max-length: 64	OpenStack only: North/South 21 network name
ns22Nw	xsd:string	max-length: 64	OpenStack only: North/South 22 network name
ns23Nw	xsd:string	max-length: 64	OpenStack only: North/South 23 network name
ns24Nw	xsd:string	max-length: 64	OpenStack only: North/South 24 network name

Parameter	Type	Constraint	Description
vlanStrippingEnabled	xsd:boolean		Enables VLAN stripping. Set to True for OpenStack deployments that do not allow Flat Networks and instead manage VLAN tagged traffic before the traffic arrives at the MCC. In these cases, network interfaces within the MCC must be configured as untagged. Untagged packets sent from the MCC are tagged by the OpenStack controller.
controllerBootSize	xsd:int		Controller boot size
payloadBootSize	xsd:int		Payload boot size
mcmVappTemplate	xsd:string	max-length: 64	VCenter only: vAPP template for mcm node type
csmVappTemplate	xsd:string	max-length: 64	VCenter only: The vAPP template for csm node type
ssmVappTemplate	xsd:string	max-length: 64	VCenter only: The vAPP template for ssm node type
clusterType	xsd:string	max-length: 64	Cluster type (MCC or MCC MME)
mgmt2Nw	xsd:string	max-length: 64	OpenStack only: The management 2 network name
cinderEnabled	xsd:boolean		Indicator whether to enable cinder
controllerEphSize	xsd:int		Controller Ephemera size
payloadEphSize	xsd:int		Payload Ephemera size
securityGroup	xsd:string	max-length: 64	Security group

Sample Response


```
{
    "base1Nw": "vmc085-base",
    "base2Nw": "",
    "baseVlanA": 0,
    "baseVlanB": 0,
    "cinderEnabled": false,
    "clusterId": 85,
```

```
"clusterType": "MME",
"controllerBootSize": 0,
"controllerEphSize": 0,
"controllerImage": "epc-11.1.14",
"csmTemplateId": null,
"csmVappTemplate": null,
"diskFormat": "thin",
"enableMultipleSession": false,
"enablePasswordAging": false,
"enableRootSshAccess": false,
"enableTelnetAccess": false,
"ew1Nw": "vmc085-eastwest",
"ew1NwEdp": "saegw016-eastwest1",
"ew2Nw": "",
"ew2NwEdp": "saegw013-eastwest2",
"ewRedundant": false,
"ewVlanA": 0,
"ewVlanAEdp": 0,
"ewVlanB": 0,
"ewVlanBEdp": 0,
"id": 140,
"logicalIp": "10.168.201.152",
"mcmTemplateId": null,
"mcmVappTemplate": null,
"mgmt2Nw": null,
"mgmtNw": "epc-oam-vlan361",
"name": "mme-85",
"ns10Nw": "",
"ns11Nw": "",
"ns12Nw": "",
"ns13Nw": "",
"ns14Nw": "",
"ns15Nw": "",
"ns16Nw": "",
"ns17Nw": "",
"ns18Nw": "",
"ns19Nw": "",
"ns1Nw": "",
"ns20Nw": "",
"ns21Nw": "",
"ns22Nw": "",
"ns23Nw": "",
"ns24Nw": "",
```

```
    "ns2Nw": "",
    "ns3Nw": "",
    "ns4Nw": "",
    "ns5Nw": "",
    "ns6Nw": "",
    "ns7Nw": "",
    "ns8Nw": "",
    "ns9Nw": "",
    "ntpIp": "172.16.239.2",
    "payloadBootSize": 0,
    "payloadEphSize": 0,
    "payloadImage": "",
    "securityGroup": null,
    "sriovConfig": ew_ns_base_mgmt,
    "ssmTemplateId": null,
    "ssmVappTemplate": null,
    "strategy": "specialized",
    "vimId": 8,
    "vlanStrippingEnabled": false
}
```


List Node Configurations

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}/node-configs

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
nodeConfigs	xsd:list		List of Node Configuration objects for Cluster Configuration {clusterConfigId}
id	xsd:long		Node configuration ID
name	xsd:string	max-length: 24	Node configuration name
nodeId	xsd:long		Node ID
reserved	xsd:boolean		Indicator whether the node configuration is reserved for dynamic expansion.
active	xsd:boolean		Indicator whether the node configuration is being used by an instantiated cluster. If the node configuration is active, no modification to it is allowed.
serviceRole	xsd:string		Service role (*MCC MME cluster type only*)

Sample Response


```
{
    "nodeConfigs": [
        {
            "active": true,
            "clusterConfigName": "mme-90",
            "id": 353,
            "name": "vmc090-mgmt-0",
            "nodeId": 1,
            "reserved": false,
            "serviceRole": "mgmt-0"
        },
        {
            "active": true,
            "clusterConfigName": "mme-90",
            "id": 354,
            "name": "vmc090-mgmt-1",
            "nodeId": 2,
            "reserved": false,
            "serviceRole": "mgmt-1"
        },
```

```
            {
                "active": true,
                "clusterConfigName": "mme-90",
                "id": 355,
                "name": "vmc090-rm-0",
                "nodeId": 5,
                "reserved": false,
                "serviceRole": "rm-0"
            },
            {
                "active": false,
                "clusterConfigName": "mme-90",
                "id": 356,
                "name": "vmc090-callp0-0",
                "nodeId": 10,
                "reserved": true,
                "serviceRole": "callp0-0"
        },
            {
                "active": true,
                "clusterConfigName": "mme-90",
                "id": 357,
                "name": "vmc090-callp0-1",
                "nodeId": 11,
                "reserved": false,
                "serviceRole": "callp0-1"
            },
            {
                "active": true,
                "clusterConfigName": "mme-90",
                "id": 359,
                "name": "vmc090-sig-0",
                "nodeId": 60,
                "reserved": false,
                "serviceRole": "sig-0"
            }
        ]
    }
```

Put Node Configuration

Request Method

PUT

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}/node-configs

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
id	xsd:long		ID of the node configuration object. **Important**: When creating a new cluster configuration, the ID must be null because it is internally created by the VNF Manager. When updating an existing cluster configuration, you must supply the ID.
name	xsd:string	max-length: 24	Node configuration name
nodeId	xsd:long		Node ID
instantiationOrder	xsd:int		VM instantiation order to be applied during cluster instantiation. If no instantiation order specified, VNF Manager instantiates VMS by ascending node type ID: mcm (1), ssm (2), csm (3), mgmt (10), rm (11), callp (12), sig (13), lb (14), data (15), edp (16), mrm (17), msm (18) If some VMs in a cluster have instantiation order specified, VNF Manager first instantiates those VMs according to instantiation order, then instantiates the other VMs according to ascending node type ID.
nodeType	xsd:string	enum: ■ mcm ■ csm ■ ssm	Node type

Parameter	Type	Constraint	Description
nodePersonality	xsd:string	enum: ■ NA ■ DCM ■ ASM ■ WSM ■ CCM ■ IOM ■ CPM	Node personality
containerId	xsd:long		Container ID: For vCenter: Host ID For OpenStack: Availability zone ID
reserved	xsd:boolean		Indicator whether the node is reserved for dynamic scaling.
cpu	xsd:int		vCenter only: Number of CPUs
cpuAffinity	xsd:string	max-length: 64	vCenter only: CPU affinity configuration
memory	xsd:int		vCenter only: Memory size in KB
flavor	xsd:string	max-length: 64	OpenStack only: VM flavor for the node
serverGroup	xsd:string	max-length: 64	OpenStack only: Server group for the node (*optional*)
mgmtIp	xsd:string	max-length: 39	Node Management IP address
gatewayIp	xsd:string	max-length: 39	Node Gateway IP address
mgmtVlan	xsd:int		Management VLAN ID
netmask	xsd:int		Netmask length
ns1Nw	xsd:string	max-length: 64	OpenStack only: The North/South 1 network name. Required for EDP SR-IOV enabled node.
ns2Nw	xsd:string	max-length: 64	OpenStack only: The North/South 2 network name. Required for EDP SR-IOV enabled node.
ns3Nw	xsd:string	max-length: 64	OpenStack only: The North/South 3 network name
ns4Nw	xsd:string	max-length: 64	OpenStack only: The North/South 4 network name
ns5Nw	xsd:string	max-length: 64	OpenStack only: The North/South 5 network name

Parameter	Type	Constraint	Description
ns6Nw	xsd:string	max-length: 64	OpenStack only: The North/South 6 network name
ns7Nw	xsd:string	max-length: 64	OpenStack only: The North/South 7 network name
ns8Nw	xsd:string	max-length: 64	OpenStack only: The North/South 8 network name
ns9Nw	xsd:string	max-length: 64	OpenStack only: The North/South 9 network name
n10Nw	xsd:string	max-length: 64	OpenStack only: The North/South 10 network name
ns11Nw	xsd:string	max-length: 64	OpenStack only: The North/South 11 network name
ns12Nw	xsd:string	max-length: 64	OpenStack only: The North/South 12 network name
ns13Nw	xsd:string	max-length: 64	OpenStack only: The North/South 13 network name
ns14Nw	xsd:string	max-length: 64	OpenStack only: The North/South 14 network name
ns15Nw	xsd:string	max-length: 64	OpenStack only: The North/South 15 network name
ns16Nw	xsd:string	max-length: 64	OpenStack only: The North/South 16 network name
ns17Nw	xsd:string	max-length: 64	OpenStack only: The North/South 17 network name
ns18Nw	xsd:string	max-length: 64	OpenStack only: The North/South 18 network name
ns19Nw	xsd:string	max-length: 64	OpenStack only: The North/South 19 network name
ns20Nw	xsd:string	max-length: 64	OpenStack only: The North/South 20 network name
ns21Nw	xsd:string	max-length: 64	OpenStack only: The North/South 21 network name
ns22Nw	xsd:string	max-length: 64	OpenStack only: The North/South 22 network name
ns23Nw	xsd:string	max-length: 64	OpenStack only: The North/South 23 network name
ns24Nw	xsd:string	max-length: 64	OpenStack only: The North/South 24 network name

Parameter	Type	Constraint	Description
diskFormat	xsd:string	enum: ■ Thin ■ eagerZeroed Thick	VCenter only: disk format
vappName	xsd:string	max-length: 64	
serviceRole	xsd:string	max-length: 64	Service role (*MCC MME cluster type only*)
ns1Ip	xsd:string	max-length: 64	OpenStack only: The North/South 1 IP. Required for LB, DATA, MSM, and EDP nodes.
ns2Ip	xsd:string	max-length: 64	OpenStack only: The North/South 2 IP. Required for LB, DATA, MSM, and EDP nodes.
ns3Ip	xsd:string	max-length: 64	OpenStack only: The North/South 3 IP
ns4Ip	xsd:string	max-length: 64	OpenStack only: The North/South 4 IP
ns5Ip	xsd:string	max-length: 64	OpenStack only: The North/South 5 IP
ns6Ip	xsd:string	max-length: 64	OpenStack only: The North/South 6 IP
ns7Ip	xsd:string	max-length: 64	OpenStack only: The North/South 7 IP
ns8Ip	xsd:string	max-length: 64	OpenStack only: The North/South 8 IP
ns9Ip	xsd:string	max-length: 64	OpenStack only: The North/South 9 IP
ns10Ip	xsd:string	max-length: 64	OpenStack only: The North/South 10 IP
ns11Ip	xsd:string	max-length: 64	OpenStack only: The North/South 11 IP
ns12Ip	xsd:string	max-length: 64	OpenStack only: The North/South 12 IP
ns13Ip	xsd:string	max-length: 64	OpenStack only: The North/South 13 IP
ns14Ip	xsd:string	max-length: 64	OpenStack only: The North/South 14 IP

Parameter	Type	Constraint	Description
ns15Ip	xsd:string	max-length: 64	OpenStack only: The North/South 15 IP
ns16Ip	xsd:string	max-length: 64	OpenStack only: The North/South 16 IP
ns17Ip	xsd:string	max-length: 64	OpenStack only: The North/South 17 IP
ns18Ip	xsd:string	max-length: 64	OpenStack only: The North/South 18 IP
ns19Ip	xsd:string	max-length: 64	OpenStack only: The North/South 19 IP
ns20Ip	xsd:string	max-length: 64	OpenStack only: The North/South 20 IP
ns21Ip	xsd:string	max-length: 64	OpenStack only: The North/South 21 IP
ns22Ip	xsd:string	max-length: 64	OpenStack only: The North/South 22 IP
ns23Ip	xsd:string	max-length: 64	OpenStack only: The North/South 23 IP
ns24Ip	xsd:string	max-length: 64	OpenStack only: The North/South 24 IP

Sample Request

```
{
        "nodeId":1,
        "name":"vmc090-mgmt-0",
        "instantiationOrder":3,
        "nodeType":"mgmt",
        "nodePersonality":"NA",
        "containerId":3,
        "reserved":false,
        "flavor":"mgmt-vmc090",
        "mgmtIp":"10.168.200.71",
        "gatewayIp":"10.168.200.1",
        "mgmtVlan":0,
        "netmask":24,
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Node configuration ID
name	xsd:string	max-length: 24	Node configuration ID

Sample Response

```
{
       "id": 1,
       "name": "vmc090-mgmt-0"
}
```

Get Node Configuration Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}/node-configs/{nodeConfigId}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Node configuration ID
name	xsd:string	max-length: 24	Node configuration name

Parameter	Type	Constraint	Description
nodeId	xsd:long		Node ID
instantiationOrder	xsd:int		VM instantiation order to be applied during cluster instantiation
nodeType	xsd:string	enum: ■ mcm ■ csm ■ ssm	Node type
nodePersonality	xsd:string	enum: ■ NA ■ DCM ■ ASM ■ WSM ■ CCM ■ IOM ■ CPM	Node personality
containerId	xsd:long		The container ID ■ For vCenter: Host ID ■ For OpenStack: Availability zone ID
reserved	xsd:boolean		Indicator whether the node is reserved for dynamic scaling.
cpu	xsd:int		vCenter only: Number of CPUs
cpuAffinity	xsd:string	max-length: 64	vCenter only: CPU affinity configuration
memory	xsd:int		vCenter only: Memory size in KB
flavor	xsd:string	max-length: 64	OpenStack only: Node VM flavor
serverGroup	xsd:string	max-length: 64	OpenStack only: Node server group for the node (*optional*)
mgmtIp	xsd:string	max-length: 39	Node management IP address
gatewayIp	xsd:string	max-length: 39	Node gateway IP address
mgmtVlan	xsd:int		Management VLAN ID
netmask	xsd:int		Netmask length
ns1Nw	xsd:string	max-length: 64	OpenStack only: The North/South 1 network name. Required for SR-IOV EDP node.

Parameter	Type	Constraint	Description
ns2Nw	xsd:string	max-length: 64	OpenStack only: The North/South 2 network name. Required for SR-IOV EDP node.
ns3Nw	xsd:string	max-length: 64	OpenStack only: The North/South 3 network name
ns4Nw	xsd:string	max-length: 64	OpenStack only: The North/South 4 network name
ns5Nw	xsd:string	max-length: 64	OpenStack only: The North/South 5 network name
ns6Nw	xsd:string	max-length: 64	OpenStack only: The North/South 6 network name
ns7Nw	xsd:string	max-length: 64	OpenStack only: The North/South 7 network name
ns8Nw	xsd:string	max-length: 64	OpenStack only: The North/South 8 network name
ns9Nw	xsd:string	max-length: 64	OpenStack only: The North/South 9 network name
n10Nw	xsd:string	max-length: 64	OpenStack only: The North/South 10 network name
ns11Nw	xsd:string	max-length: 64	OpenStack only: The North/South 11 network name
ns12Nw	xsd:string	max-length: 64	OpenStack only: The North/South 12 network name
ns13Nw	xsd:string	max-length: 64	OpenStack only: The North/South 13 network name
ns14Nw	xsd:string	max-length: 64	OpenStack only: The North/South 14 network name
ns15Nw	xsd:string	max-length: 64	OpenStack only: The North/South 15 network name
ns16Nw	xsd:string	max-length: 64	OpenStack only: The North/South 16 network name
ns17Nw	xsd:string	max-length: 64	OpenStack only: The North/South 17 network name
ns18Nw	xsd:string	max-length: 64	OpenStack only: The North/South 18 network name
ns19Nw	xsd:string	max-length: 64	OpenStack only: The North/South 19 network name

Parameter	Type	Constraint	Description
ns20Nw	xsd:string	max-length: 64	OpenStack only: The North/South 20 network name
ns21Nw	xsd:string	max-length: 64	OpenStack only: The North/South 21 network name
ns22Nw	xsd:string	max-length: 64	OpenStack only: The North/South 22 network name
ns23Nw	xsd:string	max-length: 64	OpenStack only: The North/South 23 network name
ns24Nw	xsd:string	max-length: 64	OpenStack only: The North/South 24 network name
diskFormat	xsd:string	enum: ■ Thin ■ eagerZeroed Thick	VCenter only: disk format
vappName	xsd:string	max-length: 64	
serviceRole	xsd:string	max-length: 64	Service role (*MCC MME cluster type only*)
ns1Ip	xsd:string	max-length: 64	OpenStack only: The North/South 1 IP. Required for LB, DATA, MSM, and EDP nodes.
ns2Ip	xsd:string	max-length: 64	OpenStack only: The North/South 2 IP. Required for LB, DATA, MSM, and EDP nodes.
ns3Ip	xsd:string	max-length: 64	OpenStack only: The North/South 3 IP
ns4Ip	xsd:string	max-length: 64	OpenStack only: The North/South 4 IP
ns5Ip	xsd:string	max-length: 64	OpenStack only: The North/South 5 IP
ns6Ip	xsd:string	max-length: 64	OpenStack only: The North/South 6 IP
ns7Ip	xsd:string	max-length: 64	OpenStack only: The North/South 7 IP
ns8Ip	xsd:string	max-length: 64	OpenStack only: The North/South 8 IP
ns9Ip	xsd:string	max-length: 64	OpenStack only: The North/South 9 IP

Parameter	Type	Constraint	Description
ns10Ip	xsd:string	max-length: 64	OpenStack only: The North/South 10 IP
ns11Ip	xsd:string	max-length: 64	OpenStack only: The North/South 11 IP
ns12Ip	xsd:string	max-length: 64	OpenStack only: The North/South 12 IP
ns13Ip	xsd:string	max-length: 64	OpenStack only: The North/South 13 IP
ns14Ip	xsd:string	max-length: 64	OpenStack only: The North/South 14 IP
ns15Ip	xsd:string	max-length: 64	OpenStack only: The North/South 15 IP
ns16Ip	xsd:string	max-length: 64	OpenStack only: The North/South 16 IP
ns17Ip	xsd:string	max-length: 64	OpenStack only: The North/South 17 IP
ns18Ip	xsd:string	max-length: 64	OpenStack only: The North/South 18 IP
ns19Ip	xsd:string	max-length: 64	OpenStack only: The North/South 19 IP
ns20Ip	xsd:string	max-length: 64	OpenStack only: The North/South 20 IP
ns21Ip	xsd:string	max-length: 64	OpenStack only: The North/South 21 IP
ns22Ip	xsd:string	max-length: 64	OpenStack only: The North/South 22 IP
ns23Ip	xsd:string	max-length: 64	OpenStack only: The North/South 23 IP
ns24Ip	xsd:string	max-length: 64	OpenStack only: The North/South 24 IP

Sample Response


```
{
    "containerId": 9,
    "cpu": null,
    "cpuAffinity": null,
    "disk": null,
    "flavor": "mgmt-vmc090",
    "gatewayIp": "10.168.200.1",
```

```
"id": 353,
"memory": null,
"mgmtIp": "10.168.200.71",
"mgmtVlan": 0,
"name": "vmc090-mgmt-0",
"netmask": 24,
"nodeId": 1,
"nodePersonality": "NA",
"nodeType": "mgmt",
"ns10Ip": null,
"ns10Nw": null,
"ns11Ip": null,
"ns11Nw": null,
"ns12Ip": null,
"ns12Nw": null,
"ns13Ip": null,
"ns13Nw": null,
"ns14Ip": null,
"ns14Nw": null,
"ns15Ip": null,
"ns15Nw": null,
"ns16Ip": null,
"ns16Nw": null,
"ns17Ip": null,
"ns17Nw": null,
"ns18Ip": null,
"ns18Nw": null,
"ns19Ip": null,
"ns19Nw": null,
"ns1Ip": "",
"ns1Nw": "epc-access-vlan305",
"ns20Ip": null,
"ns20Nw": null,
"ns21Ip": null,
"ns21Nw": null,
"ns22Ip": null,
"ns22Nw": null,
"ns23Ip": null,
"ns23Nw": null,
"ns24Ip": null,
"ns24Nw": null,
"ns2Ip": null,
"ns2Nw": "epc-core-vlan325",
```

```
    "ns3Ip": null,
    "ns3Nw": null,
    "ns4Ip": null,
    "ns4Nw": null,
    "ns5Ip": null,
    "ns5Nw": null,
    "ns6Ip": null,
    "ns6Nw": null,
    "ns7Ip": null,
    "ns7Nw": null,
    "ns8Ip": null,
    "ns8Nw": null,
    "ns9Ip": null,
    "ns9Nw": null,
    "reserved": false,
    "serverGroup": "",
    "serviceRole": "mgmt-0",
    "vappName": null
}
```


Delete Node Configuration

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}/node-configs/{nodeConfigId}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response

```
{
    "method": "DELETE",
    "code": 0,
    "description": "Node configuration deleted",
    "url": "/rest/vnfm/vims/4/cluster-configs/23/node-configs/77",
    "timestamp": 1496344330240
}
```

Delete Cluster Configuration

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/vnfm/vims/{vimId}/cluster-configs/{clusterConfigId}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response

```
{
    "method": "DELETE",
    "code": 0,
    "description": "Cluster cluster deleted",
    "url": "/rest/vnfm/vims/4/cluster-configs/23",
    "timestamp": 1496344338989
}
```

Lifecycle Management APIs

The following table lists the Lifecycle Management APIs:

Table A-23 Lifecycle Management APIs

Functionality	Method	URL	Comment
Instantiate Cluster	POST	/nbapi/rest/vnfm/clusters/{clusterName}	Instantiates an MCC/MCC MME cluster with Cluster Configuration {clusterName}. Non-reserved nodes are created.
Scale Out Cluster	POST	/nbapi/rest/vnfm/clusters/{clusterName}/nodes	Scales out only the non-reserved nodes for an MCC/MCC MME cluster with Cluster Configuration {clusterName}
Scale Out Node	POST	/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeList}	Scales out one or multiple reserved/non-reserved nodes {nodeLIst} for Cluster {clusterName} Cluster type MCC, {nodeList} is the nodeId for a Node instance, or comma-separated nodeIds for multiple node instances. Cluster type MCC MME, {nodeList} is service role for a Node instance, or comma-separated service roles for multiple Node Instances.
Scale In Node	DELETE	/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeList}	Scales in one or multiple reserved/non-reserved nodes {nodeList} for Cluster {clusterName} Cluster type MCC, {nodeList} is the nodeId for a Node instance, or comma-separated nodeIds for multiple Node instances. Cluster type MCC MME, {nodeList} is service role for a Node instance, or comma-separated service roles for multiple Node Instances.
Terminate Cluster	DELETE	/nbapi/rest/vnfm/clusters/{clusterName}	Terminates Cluster {clusterName}.
List Clusters	GET	/nbapi/rest/vnfm/clusters	Returns the list of Cluster instances
GET Cluster Details	GET	/nbapi/rest/vnfm/clusters/{clusterName}	Returns the Cluster instance identified by {clusterName}.

Table A-23 Lifecycle Management APIs

Functionality	Method	URL	Comment
List Nodes	GET	/nbapi/rest/vnfm/clusters/{clusterName}/nodes	Returns the list of Nodes for a Cluster instance identified by {clusterName}.
Get Node Details	GET	/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeId}	Returns a Node instance identified by {nodeId} for Cluster {clusterName}. Cluster type MCC, {nodeId} is the nodeId for a Node instance. Cluster type MCC MME, {nodeId} is the service role for a Node instance.
Validate Cluster Configuration	GET	/nbapi/rest/vnfm/cluster-config/{clusterName}/validate	Validates cluster/node configurations and relevant values against references. Returns `Cluster configuration is valid` or error.
Heal Node	POST	/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeId}/heal	Heals a failed MCC node or MCC MME node by removing the failed node and instantiating it to either the same host or a new host. The process ensures that the node configuration remains intact to avoid impacting services. Cluster type MCC, {nodeId} is the nodeId for a Node instance. Cluster type MCC MME, {nodeId} is the service role for a Node instance.

The following sections describe the details of each API.

Instantiate Cluster

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response

```
{
    "method": "POST",
    "code": 0,
    "description": "Instantiate cluster submitted.",
    "url": "/rest/vnfm/clusters/mme-90",
    "timestamp": 1495481481120
}
```

Scale Out Cluster

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/nodes

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response

```
{
    "method": "POST",
    "code": 0,
    "description": "Cluster scale out submitted.",
    "url": "/rest/vnfm/clusters/mme-90/nodes",
    "timestamp": 1495481481120
}
```

Scale Out Node

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeList}

For cluster type MCC, {nodeList} is the nodeId for a Node instance, or comma-separated nodeIds for multiple node instances.

For cluster type MCC MME, {nodeList} is service role for a Node instance, or comma-separated service roles for multiple Node Instances.

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response

```
{
    "method": "POST",
    "code": 0,
    "description": "Node scale out submitted.",
    "url": "/rest/vnfm/clusters/mme-90/nodes/11",
    "timestamp": 1495484156972
}
```

Scale In Node

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeList}

For cluster type MCC, {nodeList} is the nodeId for a Node instance, or comma-separated nodeIds for multiple Node instances.

For cluster type MCC MME, {nodeList} is service role for a Node instance, or comma-separated service roles for multiple Node Instances.

Request Content Type

application/json

Request Parameters (Optional)

Parameter	Type	Constraint	Description
dryupTimeoutInSec	xsd:long		Dryup timeout period, in seconds. If the request parameter is not set, VNF Manager uses the default value (300 seconds).

Sample Request

```
{
        "dryupTimeoutInSec": 120
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response

```
{
    "method": "DELETE",
    "code": 0,
    "description": "Node scale in submitted.",
    "url": "/rest/vnfm/clusters/mme-90/nodes/11",
    "timestamp": 1495484065934
}
```

Terminate Cluster

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response

```
{
    "method": "DELETE",
    "code": 0,
    "description": "Terminate cluster submitted.",
    "url": "/rest/vnfm/clusters/mme-90/nodes/11",
    "timestamp": 1495484065934
}
```

List Clusters

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
name	xsd:string		Cluster name
clusterId	xsd:long		Cluster ID

state	xsd:string	enum: ■ na ■ instantiate_cms_deploy_started ■ instantiate_cms_deploy_failed ■ instantiate_cms_deploy_done ■ instantiate_cms_config_started ■ instantiate_cms_config_failed ■ instantiate_cms_config_done ■ instantiate_cms_poweron_started ■ instantiate_cms_poweron_failed ■ instantiate_cms_poweron_done ■ instantiate_mcc_config_cluster_started ■ instantiate_mcc_config_cluster_failed ■ instantiate_mcc_config_cluster_done ■ instantiate_mcc_create_started ■ instantiate_mcc_create_failed ■ instantiate_mcc_create_done ■ instantiate_mcc_config_started ■ instantiate_mcc_config_failed ■ instantiate_mcc_config_done ■ instantiate_cms_config_host_started ■ instantiate_cms_config_host_failed ■ instantiate_cms_config_host_done ■ instantiate_cms_config_nictype_started ■ instantiate_cms_config_nictype_failed ■ instantiate_cms_config_nictype_done ■ scaleout_cms_deploy_started ■ scaleout_cms_deploy_failed ■ scaleout_cms_deploy_done	Cluster state

state ***(Continued)***		■ scaleout_cms_config_started ■ scaleout_cms_config_failed ■ scaleout_cms_config_done ■ scaleout_cms_poweron_started ■ scaleout_cms_poweron_failed ■ scaleout_cms_poweron_done ■ scaleout_mcc_create_started ■ scaleout_mcc_create_failed ■ scaleout_mcc_create_done ■ scaleout_mcc_config_started ■ scaleout_mcc_config_failed ■ scaleout_mcc_config_done ■ scaleout_cms_config_host_started ■ scaleout_cms_config_host_failed ■ scaleout_cms_config_host_done ■ scaleout_cms_config_nictype_started ■ scaleout_cms_config_nictype_failed ■ scaleout_cms_config_nictype_done ■ scalein_mcc_dryup_started ■ scalein_mcc_dryup_failed ■ scalein_mcc_dryup_done ■ scalein_mcc_disable_started ■ scalein_mcc_disable_failed ■ scalein_mcc_disable_done ■ scalein_mcc_delete_started ■ scalein_mcc_delete_failed ■ scalein_mcc_delete_done ■ scalein_cms_poweroff_started ■ scalein_cms_poweroff_failed ■ scalein_cms_poweroff_done ■ scalein_cms_delete_started ■ scalein_cms_delete_failed ■ scalein_cms_delete_done ■ scalein_cms_config_host_started ■ scalein_cms_config_host_failed ■ scalein_cms_config_host_done ■ scalein_cms_config_nictype_started ■ scalein_cms_config_nictype_failed ■ scalein_cms_config_nictype_done ■ terminate_cms_poweroff_started ■ terminate_cms_poweroff_failed	

state ***(Continued)***		■ terminate_cms_poweroff_done ■ terminate_cms_delete_started ■ terminate_cms_delete_failed ■ terminate_cms_delete_done	
stateTimestamp	xsd:long		Timestamp (in milliseconds since Epoch time) for the state

Sample Response

```
{
       "clusters": [{
           "name": "cluster-125",
           "clusterId": 125,
           "state": "instantiate_mcc_config_done",
           "stateTimestamp": 1458139270000
       }, {
           "name ": "cluster-7",
           "clusterId": 7,
           "state": "instantiate_mcc_config_done",
           "stateTimestamp": 1458129270000
       }]
}
```

GET Cluster Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Cluster object ID
name	xsd:string	max-length: 50	Cluster name
clusterId	xsd:long		Cluster ID
version	xsd:string	max-length: 32	Cluster version
strategy	xsd:string	enum: ■ compact ■ advanced-services-separation ■ control-services-separation ■ specialized	Building block strategy
logicalIp	xsd:string	max-length: 39	Logical IP address of the cluster
policyName	xsd:string	max-length: 16	Name of the policy assigned to the cluster

state	xsd:string	enum: ■ na ■ instantiate_cms_deploy_started ■ instantiate_cms_deploy_failed ■ instantiate_cms_deploy_done ■ instantiate_cms_config_started ■ instantiate_cms_config_failed ■ instantiate_cms_config_done ■ instantiate_cms_poweron_started ■ instantiate_cms_poweron_failed ■ instantiate_cms_poweron_done ■ instantiate_mcc_config_cluster_started ■ instantiate_mcc_config_cluster_failed ■ instantiate_mcc_config_cluster_done ■ instantiate_mcc_create_started ■ instantiate_mcc_create_failed ■ instantiate_mcc_create_done ■ instantiate_mcc_config_started ■ instantiate_mcc_config_failed ■ instantiate_mcc_config_done ■ instantiate_cms_config_host_started ■ instantiate_cms_config_host_failed ■ instantiate_cms_config_host_done ■ instantiate_cms_config_nictype_started ■ instantiate_cms_config_nictype_failed	Cluster state

state ***(Continued)***		■ instantiate_cms_config_nictype_done ■ scaleout_cms_deploy_started ■ scaleout_cms_deploy_failed ■ scaleout_cms_deploy_done ■ scaleout_cms_config_started ■ scaleout_cms_config_failed ■ scaleout_cms_config_done ■ scaleout_cms_poweron_started ■ scaleout_cms_poweron_failed ■ scaleout_cms_poweron_done ■ scaleout_mcc_create_started ■ scaleout_mcc_create_failed ■ scaleout_mcc_create_done ■ scaleout_mcc_config_started ■ scaleout_mcc_config_failed ■ scaleout_mcc_config_done ■ scaleout_cms_config_host_started ■ scaleout_cms_config_host_failed ■ scaleout_cms_config_host_done ■ scaleout_cms_config_nictype_started ■ scaleout_cms_config_nictype_failed ■ scaleout_cms_config_nictype_done ■ scalein_mcc_dryup_started ■ scalein_mcc_dryup_failed ■ scalein_mcc_dryup_done ■ scalein_mcc_disable_started ■ scalein_mcc_disable_failed ■ scalein_mcc_disable_done ■ scalein_mcc_delete_started ■ scalein_mcc_delete_failed ■ scalein_mcc_delete_done ■ scalein_cms_poweroff_started ■ scalein_cms_poweroff_failed ■ scalein_cms_poweroff_done ■ scalein_cms_delete_started ■ scalein_cms_delete_failed ■ scalein_cms_delete_done ■ scalein_cms_config_host_started ■ scalein_cms_config_host_failed ■ scalein_cms_config_host_done ■ scalein_cms_config_nictype_started ■ scalein_cms_config_nictype_failed	

state ***(Continued)***		■ scalein_cms_config_nictype_done ■ terminate_cms_poweroff_started ■ terminate_cms_poweroff_failed ■ terminate_cms_poweroff_done ■ terminate_cms_delete_started ■ terminate_cms_delete_failed ■ terminate_cms_delete_done	
stateTimestamp	xsd:long		Timestamp (in milliseconds since Epoch time) for the state

Sample Response

```
{
       "name": "cluster-125",
       "version": "6.1.2.0-110.REL",
       "strategy": "specialized",
       "clusterId": 125,
       "policyName": null,
       "logicalIp": "10.33.15.125",
       "state": "instantiate_mcc_config_done",
       "stateTimestamp": 1458139270000
}
```

List Nodes

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/nodes

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
id	xsd:long		Node object ID
clusterName	xsd:string	max-length: 50	Cluster name
name	xsd:string	max-length: 24	Node name
nodeId	xsd:long		Node ID
state	xsd:string	enum: ■ na ■ cms_create_started ■ cms_create_failed ■ cms_create_done ■ mcc_create_started ■ mcc_create_failed ■ mcc_create_done ■ mcc_config_started ■ mcc_config_failed ■ mcc_config_done ■ mcc_dryup_started ■ mcc_dryup_failed ■ mcc_dryup_done ■ mcc_disable_started ■ mcc_disable_failed ■ mcc_disable_done ■ mcc_delete_started ■ mcc_delete_failed ■ mcc_delete_done ■ cms_delete_started ■ cms_delete_failed ■ cms_delete_done ■ cms_deploy_started ■ cms_deploy_failed ■ cms_deploy_done ■ cms_config_started ■ cms_config_failed ■ cms_config_done ■ cms_poweron_started ■ cms_poweron_failed ■ cms_poweron_done	Cluster state

state ***(Continued)***		■ cms_poweroff_started ■ cms_poweroff_failed ■ cms_poweroff_done ■ cms_config_nictype_started ■ cms_config_nictype_failed ■ cms_config_nictype_done	
stateTimestamp	xsd:long		Timestamp (in milliseconds since Epoch time) for the state
serviceRole	xsd:string		Service role (*MCC MME cluster type only*)

Sample Response


```
{
    "nodes": [
        {
            "clusterName": "mme-90",
            "name": "vmc090-mgmt-0",
            "nodeId": 1,
            "serviceRole": "mgmt-0",
            "state": "mcc_config_done",
            "stateTimestamp": 1498745340000
        },
        {
            "clusterName": "mme-90",
            "name": "vmc090-mgmt-1",
            "nodeId": 2,
            "serviceRole": "mgmt-1",
            "state": "mcc_config_done",
            "stateTimestamp": 1498745340000
        },
        {
            "clusterName": "mme-90",
            "name": "vmc090-rm-0",
            "nodeId": 5,
            "serviceRole": "rm-0",
            "state": "mcc_config_done",
            "stateTimestamp": 1498745340000
        },
        {
            "clusterName": "mme-90",
            "name": "vmc090-callp0-1",
            "nodeId": 11,
```

```
            "serviceRole": "callp0-1",
            "state": "mcc_config_done",
            "stateTimestamp": 1498745340000
        },
        {
            "clusterName": "mme-90",
            "name": "vmc090-sig-0",
            "nodeId": 60,
            "serviceRole": "sig-0",
            "state": "mcc_config_done",
            "stateTimestamp": 1498745340000
        }
    ]
}
```


Get Node Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeId}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
clusterName	xsd:string	max-length: 50	Cluster name
name	xsd:string	max-length: 24	Node name
nodeId	xsd:long		Node ID

instantiationOrder	xsd:int		VM instantiation order to be applied during cluster instantiation
nodeType	xsd:string	enum: ■ mcm ■ csm ■ ssm	Node type
nodePersonality	xsd:string	enum: ■ NA ■ DCM ■ ASM ■ WSM ■ CCM ■ IOM ■ CPM	Node personality
hostIp	xsd:string	max-length: 39	Host IP address
mgmtIp	xsd:string	max-length: 39	Management IP address

state	xsd:string	enum: ■ na ■ cms_create_started ■ cms_create_failed ■ cms_create_done ■ mcc_create_started ■ mcc_create_failed ■ mcc_create_done ■ mcc_config_started ■ mcc_config_failed ■ mcc_config_done ■ mcc_dryup_started ■ mcc_dryup_failed ■ mcc_dryup_done ■ mcc_disable_started ■ mcc_disable_failed ■ mcc_disable_done ■ mcc_delete_started ■ mcc_delete_failed ■ mcc_delete_done ■ cms_delete_started ■ cms_delete_failed ■ cms_delete_done ■ cms_deploy_started ■ cms_deploy_failed ■ cms_deploy_done ■ cms_config_started ■ cms_config_failed ■ cms_config_done ■ cms_poweron_started ■ cms_poweron_failed ■ cms_poweron_done ■ cms_poweroff_started ■ cms_poweroff_failed ■ cms_poweroff_done ■ cms_config_nictype_started ■ cms_config_nictype_failed ■ cms_config_nictype_done	The node state
stateTimestamp	xsd:long		Timestamp (in milliseconds since Epoch time) for the state
service Role	xsd:string		Service role (*MCC MME cluster type only*)

Sample Response


```
{
    "clusterName": "mme-90",
    "hostIp": "172.18.253.22",
    "mgmtIp": "10.168.200.71",
    "name": "vmc090-mgmt-0",
    "nodeId": 1,
    "nodePersonality": "NA",
    "nodeType": "mgmt",
    "serviceRole": "mgmt-0",
    "state": "mcc_config_done",
    "stateTimestamp": 1498745340000
}
```


Heal Node

Heals a failed MCC node or MCC MME node by removing the failed node and instantiating it to either the same host or a new host. The process ensures that the node configuration remains intact to avoid impacting services. Must be manually initiated by an Operator.

- For MCC nodes, healing is supported in OpenStack and vCenter deployments. To support healing of MCMs, the MCC must be deployed with two MCM nodes.

  For MCC nodes, {nodeId} is the nodeId for a Node instance.

- For MCC MME nodes, healing is supported in OpenStack deployments. To support healing of mcms, the MCC MME must be deployed with two mgmt nodes.

  For MCC MME nodes, {nodeId} is the service role for a Node instance.

Healing operations are logged in the Acuitas configuration audit log.

Request Method

POST

Request URL

/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeId}/heal

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
containerId	xsd:long		Container ID: ■ For vCenter: Host ID ■ For OpenStack: Availability Zone ID If you omit the containerId, healing is targeted to the existing host/Availability Zone

Sample Request

```
{
        "containerId":3
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Response

```
{
    "method": "POST",
    "code": 0,
    "description": "Heal submitted",
    "url": "/rest/vnfm/clusters/mcc-125/nodes/2",
    "timestamp": 1528744927295
}
```

Scale In Node

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/nodes/{nodeList}

For cluster type MCC, {nodeList} is the nodeId for a Node instance, or comma-separated nodeIds for multiple Node instances.

For cluster type MCC MME, {nodeList} is service role for a Node instance, or comma-separated service roles for multiple Node Instances.

Request Content Type

application/json

Request Parameters (Optional)

Parameter	Type	Constraint	Description
dryupTimeoutInSec	xsd:long		Dryup timeout period, in seconds. If the request parameter is not set, VNF Manager uses the default value (300 seconds).

Sample Request

```
{
        "dryupTimeoutInSec": 120
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
method	xsd:string	max-length: 16	Request method
code	xsd:int		Application status code (0=success, 1=error)
description	xsd:string		Status
url	xsd:string		URL path
timestamp	xsd:long		Task submitted timestamp (in milliseconds since Epoch time)

Sample Response


```
{
    "method": "DELETE",
    "code": 0,
    "description": "Node scale in submitted.",
    "url": "/rest/vnfm/clusters/mme-90/nodes/11",
    "timestamp": 1495484065934
}
```

Dynamic Scaling APIs

The following table lists the Dynamic Scaling APIs:

Table A-24 Dynamic Scaling APIs

Functionality	Method	URL	Comment
List Policies	GET	/nbapi/rest/vnfm/policies	Returns the list of Policy instances. Not applicable for cluster type MCC MME.
Get Policy Details	GET	/nbapi/rest/vnfm/policies/{policyName}	Returns a Policy instance identified by {policyName}. Not applicable for cluster type MCC MME.
Associate Policy	PUT	/nbapi/rest/vnfm/clusters/{clusterName}/policies/{policyName}	Assigns Policy {policyName} to Cluster {clusterName}. Not applicable for cluster type MCC MME.
Disassociate Policy	DELETE	/nbapi/rest/vnfm/clusters/{clusterName}/policies	Removes policy from Cluster {clusterName}. Not applicable for cluster type MCC MME.

The following sections describe the details of each API.

List Policies

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/policies

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
name	xsd:string	max-length: 16	Policy name
adminState	xsd:string	enum: ■ enabled ■ disabled	Admin state

Sample Response

```
{
       "policys": [{
          "name": "policy-101",
          "adminState": "disabled"
       }, {
          "name": "policy-trap-only",
          "adminState": "enabled"
       }]
}
```

Get Policy Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/vnfm/policies/{policyName}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description

name	xsd:string	max-length: 16	Policy name
adminState	xsd:string	enum: ■ enable ■ disabled	Admin state: enabled|disabled
expansionCap	xsd:int		Maximum number of nodes for a cluster assigned with the policy
throttleTime	xsd:long		Throttle time (in minutes) between scale out/in operations
scaleInTimeout	xsd:long		Dryup time out (in minutes) during dynamic scale in
forceShutdown	xsd:string	enum: ■ enable ■ disabled	Whether to enable force shutdown if dryup does not complete with the scaleInTimeout during scale in: enabled|disabled
description	xsd:string		Description
rules:type	xsd:string	enum: ■ DCM ■ ASM ■ WSM	Personality of nodes to which the rule applies
rules:adminState	xsd:string	enum: ■ enable ■ disabled	Admin state
condition:type	xsd:string	enum: ■ Overload ■ Underload	Type of condition to trigger action
condition:duration	xsd:long		Duration (in seconds) of condition
threshold:target	xsd:string	enum: ■ DCMSession ■ WSMSession ■ ASMConn ■ ASMThruput	Monitoring utilization target
threshold:value	xsd:int		Utilization percentage value
action:type	xsd:string	enum: ■ Notify ■ Createdcm ■ Removed ■ Createwsm ■ Removewsm ■ Createasm ■ removeasm	Action type

Sample Response


```
{
       "name": "policy-101",
       "expansionCap": 48,
       "throttleTime": 15,
       "scaleInTimeout": 5,
       "forceShutdown": "disabled",
       "adminState": "disabled",
       "description": "this is a test",
       "rules": [{
          "type": "DCM",
          "adminState": "enabled",
          "condition": {
             "type": "Overload",
             "duration": 60,
             "thresholds": [{
                "target": "DCMSession",
                "value": 75
             }]
          },
          "actions": [{
             "type": "createdcm",
             "adminState": "enabled"
          }]
       }, {
          "type": "DCM",
          "adminState": "enabled",
          "condition": {
             "type": "Underload",
             "duration": 60,
             "thresholds": [{
                "target": "DCMSession",
                "value": 25
             }]
          },
          "actions": [{
             "type": "removedcm",
             "adminState": "enabled"
          }]
       }, {
          "type": "WSM",
          "adminState": "enabled",
```

```
        "condition": {
            "type": "Overload",
            "duration": 60,
            "thresholds": [{
                "target": "WSMSession",
                "value": 75
            }]
        },
        "actions": [{
            "type": "createwsm",
            "adminState": "disabled"
        }]
    }, {
        "type": "WSM",
        "adminState": "enabled",
        "condition": {
            "type": "Underload",
            "duration": 60,
            "thresholds": [{
                "target": "WSMSession",
                "value": 25
            }]
        },
        "actions": [{
            "type": "removewsm",
            "adminState": "disabled"
        }]
    }, {
        "type": "ASM",
        "adminState": "disabled",
        "condition": {
            "type": "Overload",
            "duration": 60,
            "thresholds": [{
                "target": "ASMConn",
                "value": 75
            }, {
                "target": "ASMThruput",
                "value": 75
            }]
        },
        "actions": [{
            "type": "createasm",
```

```
            "adminState": "disabled"
        }]
    }, {
        "type": "ASM",
        "adminState": "disabled",
        "condition": {
            "type": "Underload",
            "duration": 60,
            "thresholds": [{
                "target": "ASMConn",
                "value": 25
            }, {
                "target": "ASMThruput",
                "value": 25
            }]
        },
        "actions": [{
            "type": "removeasm",
            "adminState": "disabled"
        }]
    }]
}
```

Associate Policy

Request Method

PUT

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/policies/{policyName}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Disassociate Policy

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/policies

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

MCC Configuration APIs

The following table lists the MCC configuration APIs:

Table A-25 MCC Configuration APIs

Functionality	Method	URL	Comment
Execute EMS Template	POST	/nbapi/rest/vnfm/clusters/{clusterName}/executeEmsTemplate	Executes an EMS Template with input parameter in request body. Supported for cluster type MCC MME only for version 11.0.x or higher
Execute Template	POST	/nbapi/rest/vnfm/clusters/{clusterName}/executeTemplate	Executes a Template in the input of request body. Supported for cluster type MCC MME only for version 11.0.x or higher

The following sections describe the details of each API.

Execute EMS Template

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/executeEmsTemplate

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
name	xsd:string	max-length: 100	Name of the EMS template
paramValuePairs	xsd:list		List of parameter value pairs
name	xsd:string	max-length: 32	Parameter name
value	xsd:string	max-length: 32	Parameter value

Sample Request

```
{
        "name": "show-summary",
        "paramValuePairs": [{
                "name": "clusterId",
                "value": "125"
        }]
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
clusterName	xsd:string	max-length: 50	Cluster name
templateName	xsd:string	max-length: 100	Template name
starttime	xsd:long		Execution start timestamp (in milliseconds since Epoch time)
finishtime	xsd:long		Execution finish timestamp (in milliseconds since Epoch time)
status	xsd:string	enum: ■ success ■ failure	Execution status
description	xsd:string		Output collected from execution

Sample Response


```
{
       "clusterName": "cluster-125",
       "templateName": "show-summary",
       "starttime": 1458148823130,
       "finishtime": 1458148823464,
       "status": "success",
       "description": "cmd[0]: show cluster 125 summary\nrsp[0]:
summary 1 1\r\n Type        v-csm\r\n Personality CCM\r\n Model
vCSM\r\n Admin State enabled\r\n HA State    active\r\n CPU State
up\r\n CPU Uptime  \"D:000 H:02 M:37 S:34\"\r\n Release
6.1.2.0-110.REL\r\nsummary 2 1\r\n Type        v-csm\r\n Personality
DCM\r\n Model       vCSM\r\n Admin State enabled\r\n HA State
active\r\n CPU State   up\r\n CPU Uptime  \"D:000 H:02 M:37 S:33\"\r\n
Release     6.1.2.0-110.REL\r\nsummary 5 1\r\n Type        v-ssm\r\n
Personality IOM\r\n Model       vSSM\r\n Admin State enabled\r\n HA
State    active\r\n CPU State   up\r\n CPU Uptime  \"D:000 H:02 M:37
S:34\"\r\n Release     6.1.2.0-110.REL\r\nsummary 6 1\r\n Type
v-ssm\r\n Personality WSM\r\n Model       vSSM\r\n Admin State
enabled\r\n HA State    active\r\n CPU State   up\r\n CPU Uptime
\"D:000 H:02 M:37 S:14\"\r\n Release     6.1.2.0-110.REL\r\nsummary 7
1\r\n Type        v-mcm\r\n Personality MCM\r\n Model       vMCM\r\n
Admin State enabled\r\n HA State    active\r\n CPU State   up\r\n CPU
Uptime  \"D:000 H:02 M:40 S:32\"\r\n Release
6.1.2.0-110.REL\r\nsummary 8 1\r\n Type        v-mcm\r\n Personality
MCM\r\n Model       vMCM\r\n Admin State enabled\r\n HA State
standby\r\n CPU State   up\r\n CPU Uptime  \"D:000 H:02 M:40 S:15\"\r\n
Release     6.1.2.0-110.REL\n"
}
```


Execute Template

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/{clusterName}/executeTemplate

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
name	xsd:string	max-length: 50	Cluster name
commands	xsd:list		List of commands

Sample Request

```
{
        "name": "t-test",
        "commands": ["who", "pwd"]
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
clusterName	xsd:string		Cluster name
templateName	xsd:string		Template name
starttime	xsd:long		Execution start timestamp (in milliseconds since Epoch time)
finishtime	xsd:long		Execution finish timestamp (in milliseconds since Epoch time)
status	xsd:string	enum: ■ success ■ failure	Execution status
description	xsd:string		Output collected from execution

Sample Response

```
{
       "clusterName": "cluster-125",
       "templateName": "t-test",
       "starttime": 1458148267379,
       "finishtime": 1458148267620,
       "status": "success",
       "description": "cmd[0]: who\nrsp[0]: Session User     Context
From       Proto Date     Mode       \r\n*275    emsadmin cli
10.6.1.246 ssh   17:11:06 operational\r\n 274    affirmed snmp
10.6.1.246 udp   17:11:04 operational\r\n 267    emsadmin netconf
10.6.1.246 ssh   17:06:09 operational\ncmd[1]: pwd\nrsp[1]: At top
level\n"
}
```

Network Configuration APIs

Network configuration requests from the client are executed against all the active MCC clusters managed by Acuitas.

The following table lists the Network configuration APIs:

Table A-26 Network Configuration APIs

Functionality	Method	URL	Comment
Execute EMS Template	POST	/nbapi/rest/vnfm/clusters/executeEmsTemplate	Executes an EMS Template with input parameter in request body.
Execute Template	POST	/nbapi/rest/vnfm/clusters/executeTemplate	Executes a Template in the input of request body.

The following sections describe the details of each API.

Execute EMS Template

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/executeEmsTemplate

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
name	xsd:string	max-length: 100	Name of the EMS template
paramValuePairs	xsd:list		List of parameter value pairs
name	xsd:string	max-length: 32	Parameter name
value	xsd:string	max-length: 32	Parameter value

Sample Request

```
{
    "name": "enableVtapSubFilter",
    "paramValuePairs": [
        {
        "name": "filterName",
        "value": "vtap_sf_1"
        },
        {
        "name": "imsiLow",
        "value": "226041000001"
        },
        {
        "name": "imsiHigh",
        "value": "226041000002"
        }
    ]
}
```

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
clusterName	xsd:string	max-length: 50	Cluster name
templateName	xsd:string	max-length: 100	Template name
starttime	xsd:long		Execution start timestamp (in milliseconds since Epoch time)
finishtime	xsd:long		Execution finish timestamp (in milliseconds since Epoch time)
status	xsd:string	enum: ■ success ■ failure	Execution status

description	xsd:string		Output collected from execution
additionalInfo	xsd:string		Output from the MCC when applicable
taskStatus	xsd:string	enum: ■ success: Template is executed successfully against the specified MCC. ■ error_node_unmanaged: Failed to execute the template because the MCC is unmanaged administratively. ■ error_io: Failed to communicate with the MCC. ■ error_login: Failed to login to the MCC because of invalid username/password. ■ error_cli: Failed to execute a CLI command. ■ error_commit: Failed to commit changes. ■ error_cli_timeout: Failed to obtain CLI response from the MCC in time. ■ error_task_timeout: Failed to execute all CLI commands in time. ■ error_general: Failed to execute the template. ■ error_internal: Failed to execute the template because of a system internal error.	
taskStatusDescription	xsd:string		Error description for the MCC

Sample Response

```
{
    "description": "success@Cluster-19 success@Cluster-39",
    "finishtime": 1469213171790,
    "starttime": 1469213171324,
    "status": "success",
    "taskStatusList": [
        {
            "additionalInfo": "cmd[0]: config\nrsp[0]: Entering
configuration mode terminal\ncmd[1]: vtap subscriber-filter
vtap_sf_1\nrsp[1]: \ncmd[2]: key key1 imsi-range low 226041000001 high
226041000002\nrsp[2]: \ncmd[3]: commit\nrsp[3]: Commit complete.\n",
            "clusterName": "Cluster-19",
            "taskStatus ": "success",
            "taskStatusDescription": null
        },
        {
```

```
            "additionalInfo": "cmd[0]: config\nrsp[0]: Entering
configuration mode terminal\ncmd[1]: vtap subscriber-filter
vtap_sf_1\nrsp[1]: \ncmd[2]: key key1 imsi-range low 226041000001 high
226041000002\nrsp[2]: \ncmd[3]: commit\nrsp[3]: Commit complete.\n",
            "clusterName": "Cluster-39",
            "taskStatus": "success",
            "taskStatusDescription": null
        }
    ],
    "templateName": "enableVtapSubFilter"
}
```


Execute Template

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/vnfm/clusters/executeTemplate

Request Content Type

application/json

Request Parameters

Parameter	Type	Constraint	Description
name	xsd:string	max-length: 50	Cluster name
commands	xsd:list		List of commands

Sample Request


```
{
    "name": "showVtapSubFilter",
    "commands": ["show running-config vtap subscriber-filter"]
}
```


Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
clusterName	xsd:string		Cluster name
templateName	xsd:string		Template name
starttime	xsd:long		Execution start timestamp (in milliseconds since Epoch time)
finishtime	xsd:long		Execution finish timestamp (in milliseconds since Epoch time)
status	xsd:string	enum: ■ success ■ failure	Execution status
description	xsd:string		Output collected from execution
additionalInfo	xsd:string		Output from the MCC when applicable
taskStatus	xsd:string	enum: ■ success: Template is executed successfully against the specified MCC. ■ error_node_unmanaged: Failed to execute the template because the MCC is unmanaged administratively. ■ error_io: Failed to communicate with the MCC. ■ error_login: Failed to login to the MCC because of invalid username/password. ■ error_cli: Failed to execute a CLI command. ■ error_commit: Failed to commit changes. ■ error_cli_timeout: Failed to obtain CLI response from the MCC in time. ■ error_task_timeout: Failed to execute all CLI commands in time. ■ error_general: Failed to execute the template. ■ error_internal: Failed to execute the template because of a system internal error.	
taskStatusDescription	xsd:string		Error description for the MCC

Sample Response


```
{
    "description": "failure@cluster-125 success@Cluster-19
success@Cluster-39",
    "finishtime": 1469653967878,
    "starttime": 1469653964840,
    "status": "failure",
    "taskStatusList": [
        {
            "additionalInfo": "",
            "clusterName": "cluster-125",
            "taskStatus ": "error_io",
            "taskStatusDescription": "There was a problem while
connecting to 10.33.15.125:22"
        },
        {
            "additionalInfo": "cmd[0]: show running-config vtap
sink\nrsp[0]: % No entries found.\ncmd[1]: show running-config vtap
subscriber-tap\nrsp[1]: % No entries found.\ncmd[2]: show
running-config vtap subscriber-filter\nrsp[2]: % No entries found.\n",

            "clusterName": "Cluster-19",
            "taskStatus": "success",
            "taskStatusDescription": null
        },
        {
            "additionalInfo": "cmd[0]: show running-config vtap
sink\nrsp[0]: % No entries found.\ncmd[1]: show running-config vtap
subscriber-tap\nrsp[1]: % No entries found.\ncmd[2]: show
running-config vtap subscriber-filter\nrsp[2]: % No entries found.\n",

            "clusterName": "Cluster-39",
            "taskStatus ": "success",
            "taskStatusDescription": null
        }
    ],
    "templateName": "showVtapSubFilter"
}
```

Use Cases

The following use cases demonstrate how to use the REST APIs with the aid of curl, which is a Linux-based command line tool for HTTP communications.

Create Cluster Configuration

The following command creates a cluster configuration:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/vims/3/cluster-configs" -X PUT -H
"Content-Type: application/json" -d @cluster-config-125.input.json |
/usr/bin/python -m json.tool
```

The cluster-config-125.input.json follows:

```
{
    "base1Nw": "AN Base 1 Network",
    "base2Nw": null,
    "baseVlanA": 0,
    "baseVlanB": 0,
    "clusterId": 125,
    "controllerImage": "an-6.1.2.0-110.REL-controller",
    "csmTemplateId": null,
    "diskFormat": "thin",
    "enableMultipleSession": true,
    "enableRootSshAccess": true,
    "ew1Nw": "AN EW 1 Network PF",
    "ew2Nw": null,
    "ewRedundant": false,
    "ewVlanA": 0,
    "ewVlanB": 0,
    "logicalIp": "10.33.15.125",
    "mcmTemplateId": null,
    "mgmtNw": "AN MGMT Network",
    "name": "cluster-125",
    "ns1Nw": "AN NS 1 Network PF",
    "ns2Nw": "AN NS 2 Network PF",
    "ns3Nw": null,
    "ns4Nw": null,
    "ns5Nw": null,
    "ns6Nw": null,
    "ns7Nw": null,
    "ns8Nw": null,
    "ntpIp": "10.32.0.254",
    "payloadImage": "an-6.1.2.0-110.REL-payload",
```

```
    "sriovConfig": ew_ns_base_mgmt,
    "ssmTemplateId": null,
    "strategy": "specialized",
    "vimId": 3
}
```

The response contains the ID for the created cluster configuration:

```
{
    "id": 4,
    "name": "cluster-125"
}
```

Create Node Configuration

The following command creates a node configuration:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/vims/3/cluster-configs/4/node-conf
igs" -X PUT -H "Content-Type: application/json" -d
@node-config-7.input.json | /usr/bin/python -m json.tool
```

The node-config-7.input.json follows:

```
{
    "containerId": 3,
    "cpu": null,
    "cpuAffinity": null,
    "flavor": "AN-MCM",
    "gatewayIp": "10.33.0.1",
    "memory": null,
    "mgmtIp": "10.33.7.125",
    "mgmtVlan": 0,
    "name": "MCM-125-7",
    "netmask": 20,
    "nodeId": 7,
    "nodePersonality": "NA",
    "nodeType": "mcm",
    "reserved": false,
    "serverGroup": null
}
```

The response contains the ID for the created node configuration:

```
{
    "id": 26,
    "name": "MCM-125-7"
}
```

Instantiate MCC Cluster

The following command instantiates a cluster:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125" -X POST
```

The instantiation process can be monitored with:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125" -X GET |
/usr/bin/python -m json.tool
```

The response contains the state for the cluster:

```
{
    "clusterId": 125,
    "logicalIp": "10.33.15.125",
    "name": "cluster-125",
    "policyName": null,
    "state": "instantiate_mcc_config_done",
    "stateTimestamp": 1458847214000,
    "strategy": "specialized",
    "version": "6.1.2.0-110.REL"
}
```

Scale Out a Node for MCC Cluster

The following command scales out a node for a cluster:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125/nodes/4" -X
POST
```

The scale out process can be monitored with:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125/nodes/4" -X
GET | /usr/bin/python -m json.tool
```

The response contains the state for the node:

```
{
    "clusterName": "cluster-125",
    "hostIp": "10.33.0.125",
    "mgmtIp": "10.33.3.125",
    "name": "DCM-125-3",
    "nodeId": 3,
    "nodePersonality": "DCM",
    "nodeType": "csm",
    "state": "mcc_create_done",
    "stateTimestamp": 1458846667000
}
```

Scale In a Node for MCC Cluster

The following command scales in a node for a cluster:

```
curl -k --user {username}:{password} -X DELETE
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125/nodes/4" -H
"Content-Type: application/json" -d @scalein.input.json
```

The scalein.input.json follows:

```
{
        "dryupTimeoutInSec": 120
}
```

The scale in process can be monitored with:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125/nodes/4" -X
GET | /usr/bin/python -m json.tool
```

The response contains the state for the node:

```
{
    "clusterName": "cluster-125",
    "hostIp": "10.33.0.125",
    "mgmtIp": "10.33.3.125",
    "name": "DCM-125-3",
    "nodeId": 3,
    "nodePersonality": "DCM",
    "nodeType": "csm",
    "state": "mcc_create_done",
    "stateTimestamp": 1458846667000
}
```

Terminate MCC Cluster

The following command terminates for a cluster:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125" -X DELETE
```

The instantiation process can be monitored with:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/clusters/cluster-125" -X GET |
/usr/bin/python -m json.tool
```

The response contains the state for the cluster:

```
{
    "clusterId": 125,
    "logicalIp": "10.33.15.125",
    "name": "cluster-125",
    "policyName": null,
    "state": "instantiate_mcc_config_done",
    "stateTimestamp": 1458847214000,
    "strategy": "specialized",
    "version": "6.1.2.0-110.REL"
}
```

Remove Cluster Configuration

The following command removes a cluster configuration with its node-configuration objects:

```
curl -k --user {username}:{password}
"https://10.6.1.246/nbapi/rest/vnfm/vims/3/cluster-configs/4" -X
DELETE
```

Security REST API

The Security API provides a northbound Application Programming Interface (API) for Acuitas user and group security management functions. The API allows Operators to integrate Acuitas Service with another Network Management System and script interactions with the Acuitas server.

The Security API is a representational state transfer (REST)-based API over HTTPS.

The Security API supports the following APIs:

- Security Group APIs
- Security User APIs

Authentication and Authorization

The Security API uses the HTTP basic authentication and grants access only to users with the following security group permissions:

- Tools > Northbound API
- All permissions under the following group permissions:
  - Security Manager > Security Group Details
  - Security Manager > Security User Details
  - Security Manager > Change Password

Note: *For information on these security group permissions, see Specifying Permissions by Security Group.*

Accept Request Header (Optional)

The Security API client can optionally supply an Accept header. If it is supplied by the client, the Security API requires its value to be application/json or application/xml. If no Accept header is given, the default is application/json.

Error Handling

The Security APIs use the HTTP status code 500 to report errors.

Response Parameters

Parameter	Type	Description
method	xsd:string	HTTP method
url	xsd:string	URL
description	xsd:string	Error condition description
timestamp	xsd:long	Timestamp (in milliseconds since Epoch time)

Sample Response

```
{
       "method": "POST",
       "url": "/nbapi/rest/nms/security/user",
       "description": "User not found",
       "timestamp": 1458235583156
}
```

Security Group APIs

The following table lists the Security Group APIs:

Table A-27 Security Group APIs

Functionality	Method	URL	Comment
List all groups	GET	nbapi/rest/nms/security/group	Return the list of Groups
Get group details	GET	nbapi/rest/nms/security/group/{groupname}	Return the Group details
List all the roles	GET	nbapi/rest/nms/security/getrolenamelist	List all the roles with roleid, rolename and description
List all the roles in the tree hierarchy	GET	nbapi/rest/nms/security/getroles	List all the roles in the tree hierarchy
Create a group	POST	nbapi/rest/nms/security/addgroup	Create a new group
Clone a group	POST	nbapi/rest/nms/security/copygroup/{groupname}	Create a group by copy all the group parameters from an existing group
Modify a group	POST	nbapi/rest/nms/security/updategroup	Update the group
Add roles to a group	POST	nbapi/rest/nms/security/addrole	Add the permissions to the group
Remove roles from a group	POST	nbapi/rest/nms/security/removerole	Remove the permission from the group
Delete a group	DELETE	nbapi/rest/nms/security/group/{groupname}	Delete the group whose name is provided in {groupname}

The following sections describe the details of each API.

List Groups

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/security/group

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
groupid	xsd:long		Group ID. Group table's primary key
groupname	xsd:string	max-length:	Group name
description	xsd:string	max-length:	Description
assignedUsers	xsd:list	max-length:	List of users assigned to this group

Sample Response

```
{
       "group": [
        {
            "assignedUsers": {},
            "description": "Administrators",
            "groupid": 2,
            "groupname": "Administrators",
            "roles": null
        },
        {
            "assignedUsers": {},
            "description": "default user",
            "groupid": 1,
            "groupname": "Operators",
            "roles": null
       }
   ]
}
```

Get Group Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/security/group/{groupname}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
groupid	xsd:long		Group ID. Group table's primary key
groupname	xsd:string	max-length:	Group name
description	xsd:string	max-length:	Description
assignedUsers	xsd:list	max-length:	List of users assigned to this group

Sample Command

```
curl -k -u {username}:{password} -S -X GET -H Accept:application/json
https://10.6.1.134/nbapi/rest/nms/security/group/{Administrators}
```

Sample Response

```
{
       "group": [
        {
             "assignedUsers": {},
             "description": "Administrators",
             "groupid": 2,
             "groupname": "Administrators",
             "roles": {}
       }
   ]
}
```

List Roles

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/security/group/getrolenamelist

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
roleid	xsd:long		Role ID. Role table's primary key
rolename	xsd:string	max-length:	Role name
description	xsd:string	max-length:	Description
childRoles	xsd:list	max-length:	List of child roles

Sample Command

```
curl -k -u {username}:{password} -S -X GET -H Accept:application/json
https://10.6.1.134/nbapi/rest/nms/security/group/getrolenamelist
```

Sample Response


```
{
       "role": [
        {
            "childRoles": null,
            "description": "EMS Management",
            "roleid": 10000000,
            "rolename": "EMS_MGMT"
        },
        {
            "childRoles": null,
            "description": "Topology",
            "roleid": 12000000,
            "rolename": "TOPO"
        },
        {
            "childRoles": null,
            "description": "Element Details",
            "roleid": 12000001,
            "rolename": "DEV_VIEW_DETAILS"
        },
        .
        .
        .
       }
   ]
}
```


List Hierarchy Roles

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/security/group/getroles

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
roleid	xsd:long		Role ID. Role table's primary key.
rolename	xsd:string	max-length:	Role name
description	xsd:string	max-length:	Description
childRoles	xsd:list	max-length:	List of child roles

Sample Command

```
curl -k -u {username}:{password} -S -X GET -H Accept:application/json
https://10.6.1.134/nbapi/rest/nms/security/getroles
```

Create Group

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/addgroup

Request Parameters

Parameter	Type	Constraint	Description
groupname	xsd:string	Must be unique	Group name
description	xsd:string	max-length:	Description
assignedUsers	xd:list	max-length:	List of users assigned to this group.

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command creates the group DemoGroup with four roles:

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d @addgroup.xml
https://10.6.1.134/nbapi/rest/nms/security/addgroup
<group>
        <groupname>DemoGroup</groupname>
        <description>Group created by rest</description>
        <role>EMS_MGMT</role>
        <role>TOPO</role>
        <role>DEV_VIEW_DETAILS</role>
        <role>DEV_ADD</role>
        <user>
                 <username>restuser</username>
        </user>
        <user>
                  <username>test1</username>
        </user>
</group>
```

Copy Group

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/copygroup/{groupname}

where {groupname} is the name of the group you want to copy.

Request Parameters

Parameter	Type	Constraint	Description
groupname	xsd:string	Must be unique	New group's group name.
description	xsd:string	max-length:	Description

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command creates a new group CloneAdminGroup by copy the existing Administrator group:

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d copygroup.xml
https://10.6.1.134/nbapi/rest/nms/security/copygroup/{Administrator}
<group>
       <groupname>CloneAdminGroup</groupname>
             <description>Any description here</description>
</group>
```

Modify Group

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/updategroup

Request Parameters

Parameter	Type	Constraint	Description
groupid	xsd:long	max-length:	Group ID. Group table's primary key
groupname	xsd:string	max-length:	Group name.
description	xsd:string	max-length:	Description
assignedUsers	xd:list	max-length:	List of users assigned to this group.

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d updategroup.xml
https://10.6.1.134/nbapi/rest/nms/security/updategroup/{CloneAdminGrou
p]
<group>
       <groupname>CloneAdminGroup</groupname>
       <description>Your description here</description
       <role>TOPO</role>
       <role>DEV_VIEW_DETAILS</role>
       <role>DEV_ADD</role>
</group>
```

Add Roles (Permissions) to Group

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/addrole

Request Parameters

Parameter	Type	Constraint	Description
groupname	xsd:string	max-length:	Group name.
rolenames	xd:list	max-length:	List of roles to add to this group.

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command adds roles Topology and EMS_MGMT to the group TestGroup:

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d @addrole.xml
https://10.6.1.134/nbapi/rest/nms/security/addrole
<group>
       <groupname>TestGroup</groupname>
       <role>EMS_MGMT</role>
       <role>Topology</role>
</group>
```

Remove Roles (Permissions) from Group

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/removerole

Request Parameters

Parameter	Type	Constraint	Description
groupname	xsd:string	max-length:	Group name.
rolenames	xd:list	max-length:	List of roles to remove from the group.

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command removes roles Topology and EMS_MGMT to the group TestGroup:

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d @removerole.xml
https://10.6.1.134/nbapi/rest/nms/security/removerole
<group>
       <groupname>TestGroup</groupname>
       <role>EMS_MGMT</role>
       <role>Topology</role>
</group>
```

Delete Group

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/security/group/{groupname}

Request Parameters

Parameter	Type	Constraint	Description
groupname	xsd:string	max-length:	Group name.

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command deletes the group TestGroup:

```
curl -k -u {username}:{password} -S -X DELETE -H
Accept:application/json
https://10.6.1.134/nbapi/rest/nms/security/group/{TestGroup}
```

Security User APIs

The following table lists the Security User APIs:

Table A-28 Security User APIs

Functionality	Method	URL	Comment
List all users	GET	nbapi/rest/nms/security/user	Return the list of users
Get user details	GET	nbapi/rest/nms/security/{username}	Return the user details
Create a user	POST	nbapi/rest/nms/security/adduser	Create a new user
Modify a user	POST	nbapi/rest/nms/security/updateuser	Modify user details
Delete a user	DELETE	nbapi/rest/nms/security/user/{username}	Delete a user
Reset user password	POST	nbapi/rest/nms/security/resetpassword	Reset user password
Assign Groups to a user	POST	nbapi/rest/nms/security/assignGroupToUser	Assign Groups to a user
Remove Groups from user	POST	nbapi/rest/nms/security/unassignGroupFromuser	Remove Groups from user

The following sections describe the details of each API.

List All Users

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/security/user

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
uaerid	xsd:long		User ID.
username	xsd:string	max-length: 50	Unique userename
assignedGroups	xsd:string		List of users assigned to this group
idleTimeout	xsd:long		Number of minutes of idle time after which the user is logged out
passwordAge	xsd:long		Number of days from the first login after which the password expires.
acccountAge	xsd:long		Number of days from the first login after which the user account expires
status	xsd:string		User status: ■ Active: User is active and can log in. ■ Inactive: User is inactive and cannot log in ■ Blocked: User is blocked from logging in ■ Password Expired: Maximum password age has expired ■ Account Expired: Maximum Account Age has expired ■ Account Locked: User had consecutive failed logon attempts (default 6), so the user account is disabled and must be activated by the administrator. ■ Change Password on Login: User is forced to change password on next login ■ Dormancy Period Exceeded: User is locked out because the dormancy time was exceeded
emailaddress	xsd:string	max-length: 64	User account email address
mobile	xsd:string	max-length: 64	User account phone number
pager	xsd:string	max-length: 64	User account pager address, specified as <PAGERNUMBER>@<SERVICEPROVIDERDOMAIN>

Parameter	Type	Constraint	Description
supervisor	xsd:string		User's supervisor account (used to terminate the user's session, change the user's password, and control the user's status)
lastupdated	xsd:string		Date and time of last update of the account
description	xsd:string	max-length:	User description

Sample Command

The following command lists all users.

```
curl -k -u {username}:{password} -S -X GET -H Accept:application/json
https://10.6.1.134/nbapi/rest/nms/security/user
```

Sample Response


```
{
    "user": [
        {
            "accountAge": null,
            "assignGroup": null,
            "description": null,
            "emailaddress": "",
            "idleTimeout": null,
            "lastupdated": "1458341650562",
            "mobile": "",
            "newPassword": null,
            "pager": null,
            "password": null,
            "passwordAge": null,
            "passwordExpired": false,
            "passwordStatus": null,
            "status": null,
            "supervisor": null,
            "tenantid": null,
            "userid": 1,
            "username": "admin"
        },
        {
            "accountAge": null,
            "assignGroup": null,
            "description": null,
```

```
            "emailaddress": null,
            "idleTimeout": null,
            "lastupdated": "1462680000049",
            "mobile": null,
            "newPassword": null,
            "pager": null,
            "password": null,
            "passwordAge": null,
            "passwordExpired": false,
            "passwordStatus": null,
            "status": null,
            "supervisor": null,
            "tenantid": null,
            "userid": 10,
            "username": "affirmed_oper"
        }
    ]
}
```


Get User Details

Request Method

GET

Request URL

https://<*host*>/nbapi/rest/security/user/{username}

Request Parameters

none

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

Parameter	Type	Constraint	Description
uaerid	xsd:long		User ID.
username	xsd:string	max-length: 50	Unique userename
assignedGroups	xsd:string		List of users assigned to this group
idleTimeout	xsd:long		Number of minutes of idle time after which the user is logged out
passwordAge	xsd:long		Number of days from the first login after which the password expires.
acccountAge	xsd:long		Number of days from the first login after which the user account expires
status	xsd:string		User status: ■ Active: User is active and can log in. ■ Inactive: User is inactive and cannot log in ■ Blocked: User is blocked from logging in ■ Password Expired: Maximum password age has expired ■ Account Expired: Maximum Account Age has expired ■ Account Locked: User had consecutive failed logon attempts (default 6), so the user account is disabled and must be activated by the administrator. ■ Change Password on Login: User is forced to change password on next login ■ Dormancy Period Exceeded: User is locked out because the dormancy time was exceeded
emailaddress	xsd:string	max-length: 64	User account email address
mobile	xsd:string	max-length: 64	User account phone number
pager	xsd:string	max-length: 64	User account pager address, specified as <PAGERNUMBER>@<SERVICEPROVIDERDOMAIN>
supervisor	xsd:string		User's supervisor account (used to terminate the user's session, change the user's password, and control the user's status)

Parameter	Type	Constraint	Description
lastupdated	xsd:string		Date and time of last update of the account
description	xsd:string	max-length:	User description

Sample Command

The following command gets user details for the admin user.

```
curl -k -u {username}:{password} -S -X GET -H Accept:application/json
https://10.6.1.134/nbapi/rest/nms/security/user/{admin}
```

Sample Response


```
{
    "user": [
        {
            "accountAge": null,
            "assignGroup": null,
            "description": null,
            "emailaddress": "",
            "idleTimeout": null,
            "lastupdated": "1458341650562",
            "mobile": "",
            "newPassword": null,
            "pager": null,
            "password": null,
            "passwordAge": null,
            "passwordExpired": false,
            "passwordStatus": null,
            "status": null,
            "supervisor": null,
            "tenantid": null,
            "userid": 1,
            "username": "admin"
        }
    ]
}
```

Create User

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/adduser

Request Parameters

Parameter	Type	Constraint	Description
uaerid	xsd:long		User ID.
username	xsd:string	max-length: 50	Unique userename
assignedGroups	xsd:string		List of users assigned to this group
idleTimeout	xsd:long		Number of minutes of idle time after which the user is logged out
passwordAge	xsd:long		Number of days from the first login after which the password expires.
acccountAge	xsd:long		Number of days from the first login after which the user account expires
status	xsd:string		User status: ■ Active: User is active and can log in. ■ Inactive: User is inactive and cannot log in ■ Blocked: User is blocked from logging in ■ Password Expired: Maximum password age has expired ■ Account Expired: Maximum Account Age has expired ■ Account Locked: User had consecutive failed logon attempts (default 6), so the user account is disabled and must be activated by the administrator. ■ Change Password on Login: User is forced to change password on next login ■ Dormancy Period Exceeded: User is locked out because the dormancy time was exceeded
emailaddress	xsd:string	max-length: 64	User account email address

Parameter	Type	Constraint	Description
mobile	xsd:string	max-length: 64	User account phone number
pager	xsd:string	max-length: 64	User account pager address, specified as <PAGERNUMBER>@<SERVICEPROVIDERDOMAIN>
supervisor	xsd:string		User's supervisor account (used to terminate the user's session, change the user's password, and control the user's status)
lastupdated	xsd:string		Date and time of last update of the account
description	xsd:string	max-length:	User description

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command creates the user testUser:

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d @adduser.xml
https://10.6.1.134/nbapi/rest/nms/security/adduser
<user>
        <username>testUser</username>
        <password>Rest@123</password>
        <passwordAge>5</passwordAge>
        <accountAge>5</accountAge>
        <idleTimeout>10</idleTimeout>
        <emailaddress>xxx@gmail.com</emailaddress>
        <pager>123456</pager>
        <mobile>678932</mobile>
        <assignGroup>Administrators</assignGroup>
        <status>1</status>
        <supervisor>admin</supervisor>
```

```
</user>
```

Modify User

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/updateuser

Request Parameters

Parameter	Type	Constraint	Description
uaerid	xsd:long		User ID.
username	xsd:string	max-length: 50	Unique userename
assignedGroups	xsd:string		List of users assigned to this group
idleTimeout	xsd:long		Number of minutes of idle time after which the user is logged out
passwordAge	xsd:long		Number of days from the first login after which the password expires.
acccountAge	xsd:long		Number of days from the first login after which the user account expires

Parameter	Type	Constraint	Description
status	xsd:string		User status: ■ Active: User is active and can log in. ■ Inactive: User is inactive and cannot log in ■ Blocked: User is blocked from logging in ■ Password Expired: Maximum password age has expired ■ Account Expired: Maximum Account Age has expired ■ Account Locked: User had consecutive failed logon attempts (default 6), so the user account is disabled and must be activated by the administrator. ■ Change Password on Login: User is forced to change password on next login ■ Dormancy Period Exceeded: User is locked out because the dormancy time was exceeded
emailaddress	xsd:string	max-length: 64	User account email address
mobile	xsd:string	max-length: 64	User account phone number
pager	xsd:string	max-length: 64	User account pager address, specified as <PAGERNUMBER>@<SERVICEPROVIDERDOMAIN>
supervisor	xsd:string		User's supervisor account (used to terminate the user's session, change the user's password, and control the user's status)
lastupdated	xsd:string		Date and time of last update of the account
description	xsd:string	max-length:	User description

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command modifies the user testUser:

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d @modifyuser.xml
https://10.6.1.134/nbapi/rest/nms/security/updateuser
<user>
       <username>testUser</username>
       <passwordAge>30</passwordAge>
       <idleTimeout>10</idleTimeout>
       <assignGroup>Operators,TestGroup</assignGroup>
</user>
```

Delete User

Request Method

DELETE

Request URL

https://<*host*>/nbapi/rest/security/user/{username}

Request Parameters

Parameter	Type	Constraint	Description
username	xsd:string	max-length:	User name.

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command deletes the user testuser:

```
curl -k -u {username}:{password} -S -X DELETE -H
Accept:application/json
https://10.6.1.134/nbapi/rest/nms/security/user/{testuser}
```

Reset User Password

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/resetpassword

Request Parameters

Parameter	Type	Constraint	Description
username	xsd:string	max-length:	Username
newPassword	xsd:string	max-length:	User's new password.

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command resets the user testUser password:

```
curl -k -u {username}:{password} -S -X POST -H
'Content-Type:application/xml' -d @resetpassword.xml
https://10.6.1.134/nbapi/rest/nms/security/resetpassword

<user>
    <username>testUser</username>
    <newPassword>Rest@4321</newPassword>
</user>
```

Assign Groups to User

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/assignGroupToUser

Request Parameters

Parameter	Type	Constraint	Description
username	xsd:string	max-length:	Username
assignGroup	xsd:list	max-length:	Assign groups to the user

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command adds group testGrp1 and testGrp2 to user testuser:

```
curl -k -u {username}:{password} S -X POST -H
'Content-Type:application/xml' -d @assignGroup.xml
https://10.6.1.134/nbapi/rest/nms/security/assignGroupToUser


<user>
       <username>testuser</username>
       <assignGroup>testGrp1,testGrp2 </assignGroup>
</user>
```

Remove Groups from User

Request Method

POST

Request URL

https://<*host*>/nbapi/rest/security/unassignGroupFromuser

Request Parameters

Parameter	Type	Constraint	Description
username	xsd:string	max-length:	Username
assignGroup	xsd:list	max-length:	Groups to be unassigned to the user

Error Response Code

401 (Unauthorized), 403 (Forbidden), 500 (Internal Server Error)

Normal Response Code

200 (OK)

Response Parameters

none

Sample Command

The following command unassigns group testGrp1 and testGrp2 to user testuser:

```
curl -k -u {username}:{password} S -X POST -H
'Content-Type:application/xml' -d @unassignGroup.xml
https://10.6.1.134/nbapi/rest/nms/security/unassignGroup/fromuser


<user>
       <username>testuser</username>
       <assignGroup>testGrp1,testGrp2 </assignGroup>
</user>
```

Appendix B

Key Performance Indicators (KPIs) Metrics

KPI metrics are described in the following sections:

- Derived Metrics use KPI formulas of statistics
- Raw Metrics use individual statistics

For instructions on how to view Key Performance Indicators, see Viewing Key Performance Indicators.

Derived Metrics

Table B-1 Derived Metrics

Metric	KPI Formula
SGW KPIs:	
SGW - EPS Attach Success Rate	SGWPROCEDUREGRID.NumInitAttachSuccess / (SGWPROCEDUREGRID.NumInitAttachSuccess + SGWPROCEDUREGRID.NumInitAttachFail) * 100
SGW - Mobility Update Success Rate with SGW Relocation	(SGWPROCEDUREGRID.NumS1InterRatHandoverSgwChangeSuccess + SGWPROCEDUREGRID.NumTauRauHandoverSuccess) / (SGWPROCEDUREGRID.NumS1InterRatHandoverSgwChangeSuccess + SGWPROCEDUREGRID.NumS1InterRatHandoverSgwChangeFail + SGWPROCEDUREGRID.NumTauRauHandoverSuccess + SGWPROCEDUREGRID.NumTauRauHandoverFail) * 100
SGW - Mobility Update Success Rate without SGW Relocation	SGWPROCEDUREGRID.NumTauRauHandoverSuccess / (SGWPROCEDUREGRID.NumTauRauHandoverSuccess + SGWPROCEDUREGRID.NumTauRauHandoverFail) * 100
SGW - Network Initiated Dedicated Bearer Creation Success Rate	SGWPROCEDUREGRID.NumNWInitiatedCreateBearerSuccess / (SGWPROCEDUREGRID.NumNWInitiatedCreateBearerSuccess + SGWPROCEDUREGRID.NumNWInitiatedCreateBearerFail) * 100
SGW - Paging Success Rate	SGWPROCEDUREGRID.NumPagingSuccess / (SGWPROCEDUREGRID.NumPagingSuccess + SGWPROCEDUREGRID.NumPagingFail) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
SGW - UE Initiated Dedicated Bearer Creation Success Rate	SGWPROCEDUREGRID.NumUEInitiatedCreateBearerSuccess / (SGWPROCEDUREGRID.NumUEInitiatedCreateBearerSuccess + SGWPROCEDUREGRID.NumUEInitiatedCreateBearerFail) * 100
SGW - Inter SGW Inter System Handover Success Rate	(SGWPROCEDUREGRID.NumTauRauX2HandoverSgwChangeSuccess + SGWPROCEDUREGRID.NumS1InterRatHandoverSgwChangeSuccess) / (SGWPROCEDUREGRID.NumTauRauX2HandoverSgwChangeSuccess + SGWPROCEDUREGRID.NumTauRauX2HandoverSgwChangeFail + SGWPROCEDUREGRID.NumS1InterRatHandoverSgwChangeSuccess + SGWPROCEDUREGRID.NumS1InterRatHandoverSgwChangeFail) * 100
SGW - Intra SGW Handover Success Rate	SGWPROCEDUREGRID.NumTauRauHandoverSuccess / (SGWPROCEDUREGRID.NumTauRauHandoverSuccess + SGWPROCEDUREGRID.NumTauRauHandoverFail) * 100
SGW - Intra SGW Intra MME Handover Success Rate	SGWPROCEDUREGRID.NumIntraMmeIntraSgwHandoverSuccess / (SGWPROCEDUREGRID.NumIntraMmeIntraSgwHandoverSuccess + SGWPROCEDUREGRID.NumIntraMmeIntraSgwHandoverFail) * 100
SGW - Intra SGW Inter MME Handover Success Rate	SGWPROCEDUREGRID.NumInterMmeIntraSgwHandoverSuccess / (SGWPROCEDUREGRID.NumInterMmeIntraSgwHandoverSuccess + SGWPROCEDUREGRID.NumInterMmeIntraSgwHandoverFail) * 100
SGW - Intra SGW Intra SGSN Handover Success Rate	SGWPROCEDUREGRID.NumIntraSgsnIntraSgwHandoverSuccess / (SGWPROCEDUREGRID.NumIntraSgsnIntraSgwHandoverSuccess + SGWPROCEDUREGRID.NumIntraSgsnIntraSgwHandoverFail) * 100
SGW - Intra SGW Inter SGSN Handover Success Rate	SGWPROCEDUREGRID.NumInterSgsnIntraSgwHandoverSuccess / (SGWPROCEDUREGRID.NumInterSgsnIntraSgwHandoverSuccess + SGWPROCEDUREGRID.NumInterSgsnIntraSgwHandoverFail) * 100
SGW - Intra SGW MME to SGSN Handover Success Rate	SGWPROCEDUREGRID.NumMmeToSgsnIntraSgwHandoverSuccess / (SGWPROCEDUREGRID.NumMmeToSgsnIntraSgwHandoverSuccess + SGWPROCEDUREGRID.NumMmeToSgsnIntraSgwHandoverFail) * 100
SGWCALLPERF KPIs:	
SGW - Total EPS Bearer Setup	SGWCALLPERFSTATSGRID.NumTotalBearersSetupSuccess + SGWCALLPERFSTATSGRID.NumTotalBearersSetupFail
SAEGWSGW - Total Bearers Setup	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccess + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFail
SGW - Uplink Throughput(Mbps) †	SGWCALLPERFSTATSGRID.NumUplinkBytes * 8 / 1000000 / Interval
SGW - Downlink Throughput(Mbps) †	SGWCALLPERFSTATSGRID.NumDownlinkBytes * 8 / 1000000 / Interval
SAEGWSGW - Qci1 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci1 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci1
SAEGWSGW - Qci2 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci2 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci2

Table B-1 Derived Metrics

Metric	KPI Formula
SAEGWSGW - Qci3 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci3 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci3
SAEGWSGW - Qci4 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci4 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci4
SAEGWSGW - Qci5 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci5 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci5
SAEGWSGW - Qci6 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci6 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci6
SAEGWSGW - Qci7 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci7 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci7
SAEGWSGW - Qci8 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci8 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci8
SAEGWSGW - Qci9 - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci9 + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQci9
SAEGWSGW - Qci Other - Total EPS Bearer SetUp	SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupSuccessQci Other + SGWCALLPERFSTATSGRID.NumSaegwTotalBearersSetupFailQciOther
SGW - Current 2G/3G S4 Sessions	SGWCALLPERFSTATSGRID.NumPdnConnectionsS4Geran + SGWCALLPERFSTATSGRID.NumPdnConnectionsS4Utran
SGW - Current Co-located 2G/3G S4 Sessions	SGWCALLPERFSTATSGRID.NumSaegwPdnConnectionsS4Geran + SGWCALLPERFSTATSGRID.NumSaegwPdnConnectionsS4Utran
SGW - Current Standalone 2G/3G S4 Sessions	SGWCALLPERFSTATSGRID.NumPdnConnectionsS4Geran + SGWCALLPERFSTATSGRID.NumPdnConnectionsS4Utran - SGWCALLPERFSTATSGRID.NumSaegwPdnConnectionsS4Geran - SGWCALLPERFSTATSGRID.NumSaegwPdnConnectionsS4Utran
SGW - Current Standalone 4G Sessions	SGWCALLPERFSTATSGRID.NumPdnConnectionsEutran - SGWCALLPERFSTATSGRID.NumSaegwPdnConnectionsEutran
SGW - Modify Bearer Failure Ratio < 0.5 %	(1 - (SGWCALLPERFSTATSGRID.NumModifyBearerAccept + SGWCALLPERFSTATSGRID.NumUpdateBearerAccept) / (SGWCALLPERFSTATSGRID.NumModifyBearerReq + SGWCALLPERFSTATSGRID.NumUpdateBearerReq)) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
PGWPROCEDURE KPIs:	
PGW - EPS Attach Success Rate	PGWPROCEDUREGRID.NumCreateSessionSuccess / (PGWPROCEDUREGRID.NumCreateSessionSuccess + PGWPROCEDUREGRID.NumCreateSessionFail) * 100
PGW - Inter-SGSN Handover Success Rate	PGWPROCEDUREGRID.NumInterSgsnHandoverSuccess / (PGWPROCEDUREGRID.NumInterSgsnHandoverSuccess + PGWPROCEDUREGRID.NumInterSgsnHandoverFail) * 100
PGW - Inter-SGW Handover Success Rate	PGWPROCEDUREGRID.NumInterSgwHandoverSuccess / (PGWPROCEDUREGRID.NumInterSgwHandoverSuccess + PGWPROCEDUREGRID.NumInterSgwHandoverFail) * 100
PGW - Gn/Gp to LTE Handover Success Rate	PGWPROCEDUREGRID.NumGnGpToLteHandoverSuccess / (PGWPROCEDUREGRID.NumGnGpToLteHandoverSuccess + PGWPROCEDUREGRID.NumGnGpToLteHandoverFail) * 100
PGW - LTE to Gn/Gp Handover Success Rate	PGWPROCEDUREGRID.NumInterLteToGnGpSuccess / (PGWPROCEDUREGRID.NumInterLteToGnGpSuccess + PGWPROCEDUREGRID.NumInterLteToGnGpFail) * 100
PGW KPIs:	
PGW - Network Initiated Dedicated Bearer Creation Success Rate	PGWCALLPERFSTATSGRID.NumPGWInitDedBearerActAccept / PGWCALLPERFSTATSGRID.NumPGWInitDedBearerActAttempt * 100
PGW - UE Initiated Dedicated Bearer Creation Success Rate	PGWCALLPERFSTATSGRID.NumUEInitDedBearerActAccept / PGWCALLPERFSTATSGRID.NumUEInitDedBearerActAttempt * 100
PGW - EPS Bearer Activation Success Rate	PGWCALLPERFSTATSGRID.NumCreateSessionAccept / PGWCALLPERFSTATSGRID.NumCreateSessionAttempt * 100
PGW - Uplink Throughput(Mbps) †	PGWCALLPERFSTATSGRID.NumUplinkBytes * 8 / 1000000 / Interval
PGW - Downlink Throughout(Mbps) †	PGWCALLPERFSTATSGRID.NumDownlinkBytes * 8 / 1000000 / Interval
SAEGWPGW - Uplink Throughput(Mbps) †	PGWCALLPERFSTATSGRID.NumUplinkBytes * 8 / 1000000 / Interval
SAEGWPGW - Downlink Throughput(Mbps) †	PGWCALLPERFSTATSGRID.NumDownlinkBytes * 8 / 1000000 / Interval
PGW - UMTS PDP Context Activation Success Rate	PGWCALLPERFSTATSGRID.NumCreatePdpAccept + PGWCALLPERFSTATSGRID.NumUEInitSecPdpActAccept + PGWCALLPERFSTATSGRID.NumGGSNInitSecPdpActAccept) / (PGWCALLPERFSTATSGRID.NumCreatePdpAttempt + PGWCALLPERFSTATSGRID.NumUEInitSecPdpActAttempt + PGWCALLPERFSTATSGRID.NumGGSNInitSecPdpActAttempt) * 100
PGW - Create PDP Context Success Rate	PGWCALLPERFSTATSGRID.NumCreatePdpAccept / PGWCALLPERFSTATSGRID.NumCreatePdpAttempt * 100

Table B-1 Derived Metrics

Metric	KPI Formula
PGW - Create PDP Context Local Failure Rate	(PGWCALLPERFSTATSGRID.NumCreatePdpRejectRsrcUnavailable + PGWCALLPERFSTATSGRID.NumCreatePdpRejectSystemFailure) / PGWCALLPERFSTATSGRID.NumCreatePdpAttempt * 100
PGW - Create PDP Context Accepts per Second	PGWCALLPERFSTATSGRID.NumCreatePdpAccept / Interval
PGW - Create PDP Context Rejects per Second	PGWCALLPERFSTATSGRID.NumCreatePdpReject / Interval
PGW - Delete PDP Context Accepts per Second	PGWCALLPERFSTATSGRID.NumDeletePdpAccept / Interval
PGW - Delete PDP Context Rejects per Second	PGWCALLPERFSTATSGRID.NumDeletePdpReject / Interval
PGW - Idle Session Duration Exceeded Closes per Second	PGWCALLPERFSTATSGRID.NumIdleDurationExceededCloses / Interval
PGW - Update PDP Context Success Rate	(PGWCALLPERFSTATSGRID.NumSGSNInitUpdatePdpAccept + PGWCALLPERFSTATSGRID.NumGGSNInitUpdatePdpAccept) / (PGWCALLPERFSTATSGRID.NumSGSNInitUpdatePdpAttempt + PGWCALLPERFSTATSGRID.NumGGSNInitUpdatePdpAttempt) * 100
PGW - Received Delete PDP Context Success Rate	(PGWCALLPERFSTATSGRID.NumDeletePdpAccept + PGWCALLPERFSTATSGRID.NumUEInitSecPdpDeactAccept) / (PGWCALLPERFSTATSGRID.NumDeletePdpAttempt + PGWCALLPERFSTATSGRID.NumUEInitSecPdpDeactAttempt) * 100
PGW - Transmitted Delete PDP Context Success Rate	(PGWCALLPERFSTATSGRID.NumLocalCloseAttemptsAccepted + PGWCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAccept) / (PGWCALLPERFSTATSGRID.NumLocalCloseAttempts + PGWCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAttempt) * 100
PGW - Active Current Sessions Percentage	(PGWCALLPERFSTATSGRID.NumActiveCurrentSessions * 100) / (PGWCALLPERFSTATSGRID.NumActiveCurrentSessions + PGWCALLPERFSTATSGRID.NumIdleCurrentSessions)
PGW - CDR Success Rate	PGWCALLPERFSTATSGRID.NumGtppCdrRespSuccess / PGWCALLPERFSTATSGRID.NumGtppCdrSent * 100
PGW - Current Standalone Sessions	PGWCALLPERFSTATSGRID.NumCurrentSessions - PGWCALLPERFSTATSGRID.NumSaegwCurrentSessions
PGW - Current 2G/3G S5/S8 Sessions	PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran
PGW - Current Co-located 2G/3G S5/S8 Sessions	PGWCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8Geran + PGWCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8Utran
PGW - Current Standalone 2G/3G S5/S8 Sessions	PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran - PGWCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8Geran - PGWCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8Utran

Table B-1 Derived Metrics

Metric	KPI Formula
PGW - Current 2G/3G Gn/Gp Sessions	PGWCALLPERFSTATSGRID.NumCurrentSessionsGnGeran + PGWCALLPERFSTATSGRID.NumCurrentSessionsGnUtran
PGW - Current 2G/3G Sessions	PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran + PGWCALLPERFSTATSGRID.NumCurrentSessionsGnGeran + PGWCALLPERFSTATSGRID.NumCurrentSessionsGnUtran
PGW - Current Standalone 4G Sessions	PGWCALLPERFSTATSGRID.NumRatTypeEUtranSessions - PGWCALLPERFSTATSGRID.NumSaegwRatTypeEUtranSessions
PGW - Current Standalone 2G/3G Sessions	PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + PGWCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran + PGWCALLPERFSTATSGRID.NumCurrentSessionsGnGeran + PGWCALLPERFSTATSGRID.NumCurrentSessionsGnUtran - PGWCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8Geran - PGWCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8Utran
PGW – Uplink Packet Rate (pps)	PGWCALLPERFSTATSGRID.NumUplinkPackets / Interval
PGW – Downlink Packet Rate (pps)	PGWCALLPERFSTATSGRID.NumDownlinkPackets / Interval
PGW - S5 Deactivation Failure Ratio < 0.5 %	(1 - (PGWCALLPERFSTATSGRID.NumPGWInitDedBearerDeactAccept / PGWCALLPERFSTATSGRID.NumPGWInitDedBearerDeactAttempt))* 100
PGW - S5 Modify Bearer Failure Ratio < 0.5 %	(1 - (PGWCALLPERFSTATSGRID.NumModifyBearerAccept + PGWCALLPERFSTATSGRID.NumUpdateBearerAccept) / (PGWCALLPERFSTATSGRID.NumModifyBearerAttempt + PGWCALLPERFSTATSGRID.NumUpdateBearerAttempt)) * 100
PGW - Update Bearer Failure Ratio < 0.5 %	(1 - (PGWCALLPERFSTATSGRID.NumUpdateBearerAccept / PGWCALLPERFSTATSGRID.NumUpdateBearerAttempt))* 100
PROXYBUFFERSTATSSLOT KPIs:	
Proxy Buffer - Packet Buffer Utilization Percentage	PROXYBUFFERSTATSSLOT.pbuf-5min-peak / PROXYBUFFERSTATSSLOT.pbuf-total * 100
Proxy Buffer - 4KB Utilization Percentage	PROXYBUFFERSTATSSLOT.buffer-4k-5min-peak / PROXYBUFFERSTATSSLOT.buffer-4k-total * 100
Proxy Buffer - 8KB Utilization Percentage	PROXYBUFFERSTATSSLOT.buffer-8k-5min-peak / PROXYBUFFERSTATSSLOT.buffer-8k-total * 100
Proxy Buffer - 64KB Utilization Percentage	PROXYBUFFERSTATSSLOT.buffer-64k-5min-peak / PROXYBUFFERSTATSSLOT.buffer-64k-total * 100
Proxy Buffer - 128KB Utilization Percentage	PROXYBUFFERSTATSSLOT.buffer-128k-5min-peak / PROXYBUFFERSTATSSLOT.buffer-128k-total * 100
Proxy Buffer - 256KB Utilization Percentage	PROXYBUFFERSTATSSLOT.buffer-256k-5min-peak / PROXYBUFFERSTATSSLOT.buffer-256k-total * 100

Table B-1 Derived Metrics

Metric	KPI Formula
Proxy Buffer - 512KB Utilization Percentage	PROXYBUFFERSTATSSLOT.buffer-512k-5min-peak / PROXYBUFFERSTATSSLOT.buffer-512k-total * 100
GGSN KPIs:	
GGSN - UMTS PDP Context Activation Success Rate	GGSNCALLPERFSTATSGRID.NumCreatePdpAccept + GGSNCALLPERFSTATSGRID.NumUEInitSecPdpActAccept + GGSNCALLPERFSTATSGRID.NumGGSNInitSecPdpActAccept) / (GGSNCALLPERFSTATSGRID.NumCreatePdpAttempt + GGSNCALLPERFSTATSGRID.NumUEInitSecPdpActAttempt + GGSNCALLPERFSTATSGRID.NumGGSNInitSecPdpActAttempt) * 100
GGSN - Create PDP Context Accepts per Second	GGSNCALLPERFSTATSGRID.NumCreatePdpAccept / Interval
GGSN - Create PDP Context Rejects per Second	GGSNCALLPERFSTATSGRID.NumCreatePdpReject / Interval
GGSN - Delete PDP Context Accepts per Second	GGSNCALLPERFSTATSGRID.NumDeletePdpAccept / Interval
GGSN - Delete PDP Context Rejects per Second	GGSNCALLPERFSTATSGRID.NumDeletePdpReject / Interval
GGSN - Idle Session Duration Exceeded Closes per Second	GGSNCALLPERFSTATSGRID.NumIdleDurationExceededCloses / Interval
GGSN - Update PDP Context Success Rate	GGSNCALLPERFSTATSGRID.NumSGSNInitUpdatePdpAccept + GGSNCALLPERFSTATSGRID.NumGGSNInitUpdatePdpAccept) / (GGSNCALLPERFSTATSGRID.NumSGSNInitUpdatePdpAttempt + GGSNCALLPERFSTATSGRID.NumGGSNInitUpdatePdpAttempt) * 100
GGSN - Received Delete PDP Context Success Rate	(GGSNCALLPERFSTATSGRID.NumDeletePdpAccept + GGSNCALLPERFSTATSGRID.NumUEInitSecPdpDeactAccept) / (GGSNCALLPERFSTATSGRID.NumDeletePdpAttempt + GGSNCALLPERFSTATSGRID.NumUEInitSecPdpDeactAttempt) * 100
GGSN - Transmitted Delete PDP Context Success Rate	(GGSNCALLPERFSTATSGRID.NumLocalCloseAttemptsAccepted + GGSNCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAccept) / (GGSNCALLPERFSTATSGRID.NumLocalCloseAttempts + GGSNCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAttempt) * 100
GGSN - Create PDP Context Success Rate	GGSNCALLPERFSTATSGRID.NumCreatePdpAccept / GGSNCALLPERFSTATSGRID.NumCreatePdpAttempt * 100
GGSN - Create PDP Context Local Failure Rate	GGSNCALLPERFSTATSGRID.NumCreatePdpRejectRsrcUnavailable + GGSNCALLPERFSTATSGRID.NumCreatePdpRejectSystemFailure) / GGSNCALLPERFSTATSGRID.NumCreatePdpAttempt * 100
GGSN - CDR Success Rate	GGSNCALLPERFSTATSGRID.NumGtppCdrRespSuccess / GGSNCALLPERFSTATSGRID.NumGtppCdrSent * 100
GGSN - Current 2G/3G Sessions	GGSNCALLPERFSTATSGRID.NumCurrentSessionsGnGeran + GGSNCALLPERFSTATSGRID.NumCurrentSessionsGnUtran

Table B-1 Derived Metrics

Metric	KPI Formula
GWGTPMESSAGE KPIs:	
GGSN - Node - UMTS PDP Context Activation Success Rate	GWGTPMESSAGESTATS.numGtpv1ReqAcceptedTx / (GWGTPMESSAGESTATS.numTx - GWGTPMESSAGESTATS.numGtpv1AuthenticationFailureTx - GWGTPMESSAGESTATS.numGtpv1NoRsrcAvailTx - GWGTPMESSAGESTATS.numGtpv1MandatoryIeIncorrectTx - GWGTPMESSAGESTATS.numGtpv1OptionalIeIncorrectTx - GWGTPMESSAGESTATS.numGtpv1MandatoryIeMissingTx - GWGTPMESSAGESTATS.numGtpv1ServiceNotSupportedTx - GWGTPMESSAGESTATS.numGtpv1SysFailureTx) * 100
CONTENTCACHESUMMARYSTATS KPIs:	
Content Cache - Object Hit Ratio	CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_success / CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_total_client_requests * 100
Content Cache - Byte Hit Ratio	CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_bytes_memory + CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_bytes_disk) / CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_bytes_client_response * 100
CONTENTFILTERSUMMARYSTATS KPIs:	
Content-Filter - Safe-Searches Enforced	CONTENTFILTERSUMMARYSTATSCHASSIS.num_google_safe_search_enforced + CONTENTFILTERSUMMARYSTATSCHASSIS.num_bing_safe_search_enforced + CONTENTFILTERSUMMARYSTATSCHASSIS.num_youtube_safe_search_enforced
CONTENTHTTPPROXYSUMMARY KPIs:	
HTTP Proxy - Client Downlink Throughput (Mbps) †	CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_bytes_client_response * 8 / 1000000 / Interval
HTTP Proxy - Client Uplink Throughput (Mbps) †	CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_bytes_client_request * 8 / 1000000 / Interval
HTTP Proxy - Server Downlink Throughput (Mbps) †	CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_bytes_server_response * 8 / 1000000 / Interval
HTTP Proxy - Server Uplink Throughput (Mbps) †	CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_bytes_server_request * 8 / 1000000 / Interval

Table B-1 Derived Metrics

Metric	KPI Formula
HTTP Proxy - Transaction Success Percentage	delta(CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_total_client_requests - CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_invalid_client_requests - CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_proxy_service_failed - CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_failed - CONTENTFILTERSUMMARYSTATSCHASSIS.num_filter_service_failed - CONTENTHTTPSERVERSUMMARYSTATSCHASSIS.num_server_service_failed) / delta(CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_total_client_requests + CONTENTHTTPPROXYCONNECTIONSTATSCHASSIS.num_failures_client_connnections)
HTTP Proxy - Transaction Success Rate	CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_total_client_requests - CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_invalid_client_requests - CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_proxy_service_failed - CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_failed - CONTENTFILTERSUMMARYSTATSCHASSIS.num_filter_service_failed - CONTENTHTTPSERVERSUMMARYSTATSCHASSIS.num_server_service_failed) / Interval
HTTP Proxy - Transaction Failure Rate	delta(CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_invalid_client_requests + CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_proxy_service_failed + CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_failed + CONTENTFILTERSUMMARYSTATSCHASSIS.num_filter_service_failed + CONTENTHTTPSERVERSUMMARYSTATSCHASSIS.num_server_service_failed + CONTENTHTTPPROXYCONNECTIONSTATSCHASSIS.num_failures_client_connnections) /Interval
HTTP Proxy - Transaction Rate	CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_total_client_requests / Interval

Table B-1 Derived Metrics

Metric	KPI Formula
DPI KPIs are Historical metrics on DPI characteristics (traffic usage). It *is not* recommended to view the percentage based DPI metrics in a pie chart to display the breakdown of the applications/protocols/OS: ■ DPI - % Application Network Usage ■ DPI - % Protocol Network Usage ■ DPI - % OS network usage Instead, use the line and bar chart for these KPI's to get the percentages in a time series. Or, you can use the throughput DPI metrics in a pie chart, if you want a summary percentage breakdown of the applications/protocols/OS for the specified time frame: ■ DPI - Application Network Usage (Mbps) ■ DPI - Protocol Network Usage (Mbps) ■ DPI - OS Network Usage (Mbps)	
DPIGENERAL KPIs:	
DPI - % Traffic processed by DPI	DPIGENERALGRID.detectionTotalUlBytes + DPIGENERALGRID.detectionTotalDlBytes) / (DPIGENERALGRID.detectionTotalUlBytes + DPIGENERALGRID.detectionTotalDlBytes + DPIGENERALGRID.noDpiTotalUlBytes + DPIGENERALGRID.noDpiTotalDlBytes) * 100
DPI - % Unclassified Traffic out of DPI traffic	DPIGENERALGRID.protocolUndetectedUlBytes + DPIGENERALGRID.protocolUndetectedDlBytes) / (DPIGENERALGRID.detectionTotalUlBytes + DPIGENERALGRID.detectionTotalDlBytes) * 100
EMSDPIPROTOCOLS KPIs:	
DPI - % Protocol Network Usage	EMSDPIPROTOCOLSGRID.uplink-bytes + EMSDPIPROTOCOLSGRID.downlink-bytes) / (DPIGENERALGRID.detectionTotalUlBytes + DPIGENERALGRID.detectionTotalDlBytes) * 100
DPI - Protocol Network Usage (Mbps) †	EMSDPIPROTOCOLSGRID.uplink-bytes + EMSDPIPROTOCOLSGRID.downlink-bytes) * 8 / 1000000 / Interval
EMSDPIAPPLICATIONS KPIs:	
DPI - % Application Network Usage	EMSDPIAPPLICATIONSGRID.uplink-bytes + EMSDPIAPPLICATIONSGRID.downlink-bytes) / (DPIGENERALGRID.detectionTotalUlBytes + DPIGENERALGRID.detectionTotalDlBytes) * 100
DPI - Application Network Usage (Mbps) †	EMSDPIAPPLICATIONSGRID.uplink-bytes + EMSDPIAPPLICATIONSGRID.downlink-bytes) * 8 / 1000000 / Interval

Table B-1 Derived Metrics

Metric	KPI Formula
EMSDPIOPERATINGSYSTEMS KPIs:	
DPI - % OS Network Usage	EMSDPIOPERATINGSYSTEMSGRID.uplink-bytes + EMSDPIOPERATINGSYSTEMSGRID.downlink-bytes) / (DPIGENERALGRID.detectionTotalUlBytes + DPIGENERALGRID.detectionTotalDlBytes) * 100
DPI - OS Network Usage (Mbps) †	EMSDPIOPERATINGSYSTEMSGRID.uplink-bytes + EMSDPIOPERATINGSYSTEMSGRID.downlink-bytes) * 8 / 1000000 / Interval
CONTENTMMSMM1SUMMARY KPIs:	
MMS - Traffic In Send Request per Second	CONTENTMMSMM1SUMMARYSTATSGRID.num_mms_msg_type_send_req / Interval
MMS - Traffic In Notify Response Indications per Second	CONTENTMMSMM1SUMMARYSTATSGRID.num_mms_msg_type_notifyresp_ind / Interval
MMS - Traffic In Acknowledge Indications per Second	CONTENTMMSMM1SUMMARYSTATSGRID.num_mms_msg_type_acknowledge_ind / Interval
MMS - Traffic Out Retrieve Confirmations per Second	CONTENTMMSMM1SUMMARYSTATSGRID.num_mms_msg_type_retrieve_conf / Interval
RADIUSPROCEDURE KPIs:	
PDN GW - Radius Authentication Success Rate	RADIUSPROCEDURESTATS.numAccessAcceptRx / RADIUSPROCEDURESTATS.numAccessReqTx * 100
PDN GW - Radius Account Success Rate	RADIUSPROCEDURESTATS.numAccountRequestStartRespRx + RADIUSPROCEDURESTATS.numAccountRequestInterimUpdateRespRx + RADIUSPROCEDURESTATS.numAccountRequestStopRespRx) / (RADIUSPROCEDURESTATS.numAccountRequestStartTx + RADIUSPROCEDURESTATS.numAccountRequestInterimUpdateTx + RADIUSPROCEDURESTATS.numAccountRequestStopTx) * 100
Radius - Average Authentication/Accounting Latency(microsecond)	RADIUSPROCEDURESTATS.AverageLatency / RADIUSPROCEDURESTATS.LatencySamples
Radius - Average CoA Latency(microsecond)	RADIUSPROCEDURESTATS.AverageCoaLatency / RADIUSPROCEDURESTATS.CoaLatencySamples

Table B-1 Derived Metrics

Metric	KPI Formula
RADIUSPROCEDUREPEER KPIs:	
PDN GW - Peer - Radius Authentication Success Rate	RADIUSPROCEDURESTATSPEER.numAccessAcceptRx / RADIUSPROCEDURESTATSPEER.numAccessReqTx * 100
PDN GW - Peer - Radius Account Success Rate	RADIUSPROCEDURESTATSPEER.numAccountRequestStartRespRx + RADIUSPROCEDURESTATSPEER.numAccountRequestInterimUpdate RespRx + RADIUSPROCEDURESTATSPEER.numAccountRequestStopRespRx) / (RADIUSPROCEDURESTATSPEER.numAccountRequestStartTx + RADIUSPROCEDURESTATSPEER.numAccountRequestInterimUpdateTx + RADIUSPROCEDURESTATSPEER.numAccountRequestStopTx) * 100
Radius - Accounting Requests Timed Out	RADIUSPROCEDURESTATSPEER.numAccountRequestStartTimeout + RADIUSPROCEDURESTATSPEER.numAccountRequestInterimUpdate Timeout + RADIUSPROCEDURESTATSPEER.numAccountRequestStopTimeout
Radius Peer - Average Authentication/Accounting Latency(microsecond)	RADIUSPROCEDURESTATSPEER.AverageLatency / RADIUSPROCEDURESTATSPEER.LatencySamples
Radius Peer - Average CoA Latency(microsecond)	RADIUSPROCEDURESTATSPEER.AverageCoaLatency / RADIUSPROCEDURESTATSPEER.CoaLatencySamples
APNCALLPERF KPIs:	
APN - Uplink Packet Drop Rate	APNCALLPERFSTATSGRID.NumUplinkDropPackets / (APNCALLPERFSTATSGRID.NumUplinkPackets + APNCALLPERFSTATSGRID.NumUplinkDropPackets) * 100
APN - Downlink Packet Drop Rate	APNCALLPERFSTATSGRID.NumDownlinkDropPackets / (APNCALLPERFSTATSGRID.NumDownlinkPackets + APNCALLPERFSTATSGRID.NumDownlinkDropPackets) * 100
APN - Total GGSN Initiated Delete PDP Context Request Success Rate	APNCALLPERFSTATSGRID.NumLocalCloseAttemptsAccepted + APNCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAccept) / (APNCALLPERFSTATSGRID.NumLocalCloseAttempts + APNCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAttempt) * 100
APN - Total Create PDP Context Success Rate	(APNCALLPERFSTATSGRID.NumCreatePdpAccept + APNCALLPERFSTATSGRID.NumUEInitSecPdpActAccept + APNCALLPERFSTATSGRID.NumGGSNInitSecPdpActAccept) / (APNCALLPERFSTATSGRID.NumCreatePdpAttempt + APNCALLPERFSTATSGRID.NumUEInitSecPdpActAttempt + APNCALLPERFSTATSGRID.NumGGSNInitSecPdpActAttempt) * 100
APN - Total Create PDP Context Dynamic IP Success Rate	(APNCALLPERFSTATSGRID.NumLocalIPv4AllocSuccesses + APNCALLPERFSTATSGRID.NumLocalIPv6AllocSuccesses) / (APNCALLPERFSTATSGRID.NumLocalIPv4AllocSuccesses + APNCALLPERFSTATSGRID.NumLocalIPv4AllocFailures + APNCALLPERFSTATSGRID.NumLocalIPv6AllocSuccesses + APNCALLPERFSTATSGRID.NumLocalIPv6AllocFailures) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
APN - Average Uplink Packet Size (byte) †	APNCALLPERFSTATSGRID.NumUplinkBytes / APNCALLPERFSTATSGRID.NumUplinkPackets
APN - Average Downlink Packet Size (byte) †	APNCALLPERFSTATSGRID.NumDownlinkBytes / APNCALLPERFSTATSGRID.NumDownlinkPackets
APN - Pdp Context - Downlink Data Rate (Kbps) †	APNCALLPERFSTATSGRID.NumDownlinkBytes * 8 / APNCALLPERFSTATSGRID.NumBearers / 1000 / Interval
APN - Pdp Context - Uplink Data Rate (Kbps) †	APNCALLPERFSTATSGRID.NumUplinkBytes * 8 / APNCALLPERFSTATSGRID.NumBearers / 1000 / Interval
APN - Uplink Throughput(Mbps) †	APNCALLPERFSTATSGRID.NumUplinkBytes * 8 / 1000000 / Interval
APN - Downlink Throughput(Mbps) †	APNCALLPERFSTATSGRID.NumDownlinkBytes * 8 / 1000000 / Interval
APN - Total SGSN Initiated Delete PDP Context Request Success Rate	(APNCALLPERFSTATSGRID.NumDeletePdpAccept + APNCALLPERFSTATSGRID.NumUEInitSecPdpDeactAccept) / (APNCALLPERFSTATSGRID.NumDeletePdpAttempt + APNCALLPERFSTATSGRID.NumUEInitSecPdpDeactAttempt) * 100
APN - UE Requested IP Address Reservations Successful	APNCALLPERFSTATSGRID.NumUeAllocStaticIPv4ReserveSuccesses + APNCALLPERFSTATSGRID.NumUeAllocStaticIPv6ReserveSuccesses
APN - Radius AAA Server Allocated IP Address Reservations Successful	APNCALLPERFSTATSGRID.NumRadiusAllocIPv4ReserveSuccesses + APNCALLPERFSTATSGRID.NumRadiusAllocIPv6ReserveSuccesses
APN - Remote DHCP Server Allocated IP Address Reservations Successful	APNCALLPERFSTATSGRID.NumRemoteDhcpAllocIPv4Reserve Successes + APNCALLPERFSTATSGRID.NumRemoteDhcpAllocIPv6Reserve Successes
APN - DHCP Relay Allocated IP Address Reservations Successful	APNCALLPERFSTATSGRID.NumDhcpRelayAllocIPv4ReserveSuccesses + APNCALLPERFSTATSGRID.NumDhcpRelayAllocIPv6ReserveSuccesses
APN - Accounting Requests Timed Out	APNCALLPERFSTATSGRID.NumAcctStartReqTimeout + APNCALLPERFSTATSGRID.NumAcctInterimUpdReqTimeout + APNCALLPERFSTATSGRID.NumAcctStopReqTimeout
APN - Activation Rate	(APNCALLPERFSTATSGRID.NumCreateSessionAccept + APNCALLPERFSTATSGRID.NumCreatePdpAccept) / Interval
APN - Create Bearer Failure per APN Ratio < 0.5 %	(1 - (APNCALLPERFSTATSGRID.NumPGWInitDedBearerActAccept / APNCALLPERFSTATSGRID.NumPGWInitDedBearerActAttempt)) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
SAEGWSGWPROCEDURE KPIs:	
SAEGWSGW - Inter S-GW Inter System Handover Success Rate	(SAEGWSGWPROCEDUREGRID.NumTauRauX2HandoverSgwChange Success + SAEGWSGWPROCEDUREGRID.NumS1InterRatHandoverSgwChange Success) / (SAEGWSGWPROCEDUREGRID.NumTauRauX2HandoverSgwChange Success + SAEGWSGWPROCEDUREGRID.NumTauRauX2HandoverSgwChange Fail + SAEGWSGWPROCEDUREGRID.NumS1InterRatHandoverSgwChange Success + SAEGWSGWPROCEDUREGRID.NumS1InterRatHandoverSgwChange Fail) * 100
SAEGWSGW - Intra S-GW Intra MME Handover Success Rate	SAEGWSGWPROCEDUREGRID.NumIntraMmeIntraSgwHandover Success / (SAEGWSGWPROCEDUREGRID.NumIntraMmeIntraSgwHandover Success + SAEGWSGWPROCEDUREGRID.NumIntraMmeIntraSgwHandoverFail) * 100
SAEGWSGW - Intra S-GW Inter MME Handover Success Rate	SAEGWSGWPROCEDUREGRID.NumInterMmeIntraSgwHandover Success / (SAEGWSGWPROCEDUREGRID.NumInterMmeIntraSgwHandover Success + SAEGWSGWPROCEDUREGRID.NumInterMmeIntraSgwHandoverFail) * 100
SAEGWSGW - Intra S-GW Intra SGSN Handover Success Rate	SAEGWSGWPROCEDUREGRID.NumIntraSgsnIntraSgwHandover Success / (SAEGWSGWPROCEDUREGRID.NumIntraSgsnIntraSgwHandover Success + SAEGWSGWPROCEDUREGRID.NumIntraSgsnIntraSgwHandoverFail) * 100
SAEGWSGW - Intra S-GW Inter SGSN Handover Success Rate	SAEGWSGWPROCEDUREGRID.NumInterSgsnIntraSgwHandover Success / (SAEGWSGWPROCEDUREGRID.NumInterSgsnIntraSgwHandover Success + SAEGWSGWPROCEDUREGRID.NumInterSgsnIntraSgwHandoverFail) * 100
SAEGWSGW - Intra S-GW MME to SGSN Handover Success Rate	SAEGWSGWPROCEDUREGRID.NumMmeToSgsnIntraSgwHandover Success / (SAEGWSGWPROCEDUREGRID.NumMmeToSgsnIntraSgwHandover Success + SAEGWSGWPROCEDUREGRID.NumMmeToSgsnIntraSgwHandover Fail) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
SAEGWSGW - Intra S-GW SGSN to MME Handover Success Rate	SAEGWSGWPROCEDUREGRID.NumSgsnToMmeIntraSgwHandover Success / (SAEGWSGWPROCEDUREGRID.NumSgsnToMmeIntraSgwHandover Success + SAEGWSGWPROCEDUREGRID.NumSgsnToMmeIntraSgwHandover Fail) * 100
SAEGWPGWPROCEDURE KPIs:	
SAEGWPGW - Inter-SGSN Handover Success Rate	SAEGWPGWPROCEDUREGRID.NumInterSgsnHandoverSuccess / (SAEGWPGWPROCEDUREGRID.NumInterSgsnHandoverSuccess + SAEGWPGWPROCEDUREGRID.NumInterSgsnHandoverFail) * 100
SAEGWPGW - Inter-SGW Handover Success Rate	SAEGWPGWPROCEDUREGRID.NumInterSgwHandoverSuccess / (SAEGWPGWPROCEDUREGRID.NumInterSgwHandoverSuccess + SAEGWPGWPROCEDUREGRID.NumInterSgwHandoverFail) * 100
SAEGWPGW - Gn/Gp to LTE Handover Success Rate	SAEGWPGWPROCEDUREGRID.NumGnGpToLteHandoverSuccess / (SAEGWPGWPROCEDUREGRID.NumGnGpToLteHandoverSuccess + SAEGWPGWPROCEDUREGRID.NumGnGpToLteHandoverFail) * 100
SAEGWPGW - LTE to Gn/Gp Handover Success Rate	SAEGWPGWPROCEDUREGRID.NumInterLteToGnGpSuccess / (SAEGWPGWPROCEDUREGRID.NumInterLteToGnGpSuccess + SAEGWPGWPROCEDUREGRID.NumInterLteToGnGpFail) * 100
INTERFACESTATISTICS KPIs:	
System - Transmitted Throughput(Mbps) †	(INTERFACESTATISTICSGRID.numTxV4Bytes + INTERFACESTATISTICSGRID.numTxV6Bytes) * 8 / 1000000 / Interval
System - Received Throughput(Mbps) †	(INTERFACESTATISTICSGRID.numRxV4Bytes + INTERFACESTATISTICSGRID.numRxV6Bytes) * 8 / 1000000 / Interval
System - Transmitted Average Packet Size (byte) †	(INTERFACESTATISTICSGRID.numTxV4Bytes + INTERFACESTATISTICSGRID.numTxV6Bytes) / (INTERFACESTATISTICSGRID.numTxV4Pkts + INTERFACESTATISTICSGRID.numTxV6Pkts)
System - Received Average Packet Size (byte) †	(INTERFACESTATISTICSGRID.numRxV4Bytes + INTERFACESTATISTICSGRID.numRxV6Bytes) / (INTERFACESTATISTICSGRID.numRxV4Pkts + INTERFACESTATISTICSGRID.numRxV6Pkts)

Table B-1 Derived Metrics

Metric	KPI Formula
CONTENTHTTPPROXYCOMPRESSIONSTATS KPIs:	
HTTP Proxy - Compression Bytes Saved †	CONTENTHTTPPROXYCOMPRESSIONSTATSGRID.num_bytes_not_compressed_by_server - (CONTENTHTTPPROXYCOMPRESSIONSTATSGRID.num_bytes_compressed_by_proxy + CONTENTHTTPPROXYCOMPRESSIONSTATSGRID.num_bytes_forced_compress_by_proxy)
HTTP Proxy - Compression Saving Ratio	(CONTENTHTTPPROXYCOMPRESSIONSTATSGRID.num_bytes_not_compressed_by_server - (CONTENTHTTPPROXYCOMPRESSIONSTATSGRID.num_bytes_compressed_by_proxy + CONTENTHTTPPROXYCOMPRESSIONSTATSGRID.num_bytes_forced_compress_by_proxy)) / CONTENTHTTPPROXYCOMPRESSIONSTATSGRID.num_bytes_not_compressed_by_server * 100
C-SGN KPIs:	
C-SGN - CpCIot IP Bearer Activation Success Rate for Attach	100 * (LTESM_PROCEDURE.SM.ActDefaultCpCIoTIpBearerAttachSucc / LTESM_PROCEDURE.SM.ActDefaultCpCIoTIpBearerAttachAtt)
C-SGN - CpCIot IP Bearer Activation Success Rate for PDN	100 * (LTESM_PROCEDURE.SM.ActDefaultCpCIoTIpBearerPdnConnSucc / LTESM_PROCEDURE.SM.ActDefaultCpCIoTIpBearerPdnConnAtt)
C-SGN - CpCIot Non-IP Bearer Activation Success Rate for Attach	100 * (LTESM_PROCEDURE.SM.ActDefaultCpCIoTNonIpBearerAttachSucc / LTESM_PROCEDURE.SM.ActDefaultCpCIoTNonIpBearerAttachAtt)
C-SGN - CpCIot Non-IP Bearer Activation Success Rate for PDN	100 * (LTESM_PROCEDURE.SM.ActDefaultCpCIoTNonIpBearerPdnConnSucc / LTESM_PROCEDURE.SM.ActDefaultCpCIoTNonIpBearerPdnConnAtt)
C-SGN - Data Over NAS Downlink Throughput for S11 IP-Data (Kbps) †	((LTESM_DATATRANSPORT.SM.DataTransport.DL.IP.GW.DataOct * 8) / <*Sample Period, in seconds*>) / 1000
C-SGN - Data Over NAS Downlink Throughput for S11 Non-IP-Data (Kbps) †	((LTESM_DATATRANSPORT.SM.DataTransport.DL.NonIP.GW.DataOct * 8) / <*Sample Period, in seconds*>) / 1000
C-SGN - Data Over NAS Downlink Throughput for T6 (Kbps) †	((LTESM_DATATRANSPORT.SM.DataTransport.DL.NonIP.SCEF.DataOct * 8) / <*Sample Period, in seconds*>) / 1000
C-SGN - Data Over NAS Uplink Throughput for S11 IP-Data (Kbps) †	((LTESM_DATATRANSPORT.SM.DataTransport.UL.IP.GW.DataOct * 8) / <*Sample Period, in seconds*>) / 1000
C-SGN - Data Over NAS Uplink Throughput for S11 Non-IP-Data (Kbps) †	((LTESM_DATATRANSPORT.SM.DataTransport.UL.NonIP.GW.DataOct * 8) / <*Sample Period, in seconds*>s) / 1000
C-SGN - Data Over NAS Uplink Throughput for T6 (Kbps) †	((LTESM_DATATRANSPORT.SM.DataTransport.UL.NonIP.SCEF.DataOct * 8) / <*Sample Period, in seconds*>) / 1000

Table B-1 Derived Metrics

Metric	KPI Formula
C-SGN - LTE CP Service Request Success Rate (Uplink)	100 * (LTEMM_PROCEDURE.VS.MM.ControlPlaneServiceRequestSucc / (LTEMM_PROCEDURE.VS.MM.ControlPlaneServiceRequestAtt - (LTEMM_PROCEDURE.MM.PagingEpsAtt - LTEMM_PROCEDURE.MM.PagingEpsFail)))
C-SGN - No-PDN Attach Success Rate	100 * (LTEMM_ATTACH.VS.MM.AttachNoPdnSucc / LTEMM_ATTACH.VS.MM.AttachNoPdnAtt)
C-SGN - LTE SMS-Only Attach Success Rate	100 * (LTEMM_ATTACH.VS.MM.SmsOnlyAttachSucc / LTEMM_ATTACH.VS.MM.SmsOnlyAttachAtt)
LTE KPIs:	
LTE - Attach Success Rate Nodal	100 * ((LTEMM.PROCEDURE.MM.EpsAttachSucc.E) / (LTEMM.PROCEDURE.MM.EpsAttachSucc.E + LTEMM.ATTACHFAIL.MM.EpsAttachFail.Congestion_22.E - LTEMM.ATTACHFAIL.VS.MM.EpsAttachFail.Congestion_22.DCN.E - LTEMM.ATTACHFAIL. Congestion_22.AdmissionControl.E + LTEMM.ATTACHFAIL.NetworkFailure_17.MmeInternalError.E))
LTE - Bearer Activation Success Rate Nodal	100 * (LTESM_PROCEDURE.SM.ActDedicatedEpsBearerSucc) / (LTESM_PROCEDURE.SM.ActDedicatedEpsBearerSucc + LTESM_BEARERACTFAIL.InsfRscs_26.ControlPlaneFail + LTESM_BEARERACTFAIL.InsfRscs_26.MsgSendFail + LTESM_BEARERACTFAIL.ActRejUnspc_31.GrdTimerExpiry + LTESM_BEARERACTFAIL.InsfRscs_26.Overload))
LTE - Percentage of SAU in ECM-CONNECTED	100 * (LTEMM_GENERAL.MM.NbrEpsSubConnect / (LTEMM_GENERAL.MM.NbrEpsSubConnect + LTEMM_GENERAL.MM.NbrEpsSubIdle))
LTE - Session Activation Success Rate Nodal	100 * ((LTESM_PROCEDURE.SM.ActDefaultEpsBearerPdnConSucc + LTESM_PROCEDURE.SM.ActDefaultEpsBearerAttachSucc) / (LTESM_PROCEDURE.SM.ActDefaultEpsBearerPdnConSucc + LTESM_PROCEDURE.SM.ActDefaultEpsBearerAttachSucc + LTESM_SESSIONACTFAIL.InsfRscs_26.ControlPlaneFail + LTESM_SESSIONACTFAIL.InsfRscs_26.MsgSendFail + LTESM_SESSIONACTFAIL.ActRejUnspc_31.GrdTimerExpiry))

Table B-1 Derived Metrics

Metric	KPI Formula
CONTENTHTTPPROXYMINIFYSTATS KPIs:	
HTTP Proxy - Minification Bytes Saved †	(CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_not_minified - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_minified) + (CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_not_minified - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_minified) + (CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_not_minified - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_minified)
HTTP Proxy - Minification Saving Ratio	((CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_not_minified - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_minified) + (CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_not_minified - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_minified) + (CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_not_minified - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_minified)) / (CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_css_bytes_not_minified + CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_html_bytes_not_minified + CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_attempt - CONTENTHTTPPROXYMINIFYSTATSGRID.num_minify_js_bytes_not_minified) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATS KPIs:	
HTTP Proxy - Web Image Optimization Bytes Saved †	CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_attempt - CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_not_adapted - CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_adapted
HTTP Proxy - Web Image Optimization Saving Ratio	(CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_attempt - CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_not_adapted - CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_adapted) / (CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_attempt - CONTENTHTTPPROXYWEBIMAGEOPTSUMMARYSTATSGRID.num_web_image_opt_bytes_not_adapted) * 100
CONTENTFILTERSTATS KPIs:	
Content Filter - Safe Searches Enforced	CONTENTFILTERSTATSGRID.num_google_safe_search_enforced + CONTENTFILTERSTATSGRID.num_bing_safe_search_enforced + CONTENTFILTERSTATSGRID.num_yahoo_safe_search_enforced

Table B-1 Derived Metrics

Metric	KPI Formula
CONTENTVAOFFLINETRANSCODINGSUMMARYSTATS KPIs:	
Video Adaptation - Hit Ratio	((CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_flv_serving_success + CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_flv_serving_abort) + (CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_mp4_serving_success + CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_mp4_serving_abort) + (CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_webm_serving_success + CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_webm_serving_abort)) / ((CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_orig_serving_success + CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_orig_serving_abort) + (CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_flv_serving_success + CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_flv_serving_abort) + (CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_mp4_serving_success + CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_mp4_serving_abort) + (CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_webm_serving_success + CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_webm_serving_abort))
Video Adaptation - Offline Transcoding Bytes Saved †	CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_original_bytes - CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_adapted_bytes_served
Video Adaptation - Offline Transcoding Saving Ratio †	(CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_original_bytes - CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_adapted_bytes_served) / CONTENTVAOFFLINETRANSCODINGSUMMARYSTATSCHASSIS.num_offline_original_bytes * 100

Table B-1 Derived Metrics

Metric	KPI Formula
CONTENTVAONLINETRANSCODINGSUMMARYSTATS KPIs:	
Video Adaptation - Online Transcoding Bytes Saved	CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_attempt - CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_cancel - CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_adapted
Video Adaptation - Online Transcoding Saving Ratio	(CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_attempt - CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_cancel - CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_adapted) / (CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_attempt - CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_bytes_cancel) * 100
Video Adaptation - Online Transactions Processed Percentage	(CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_attempts - CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_failures) / CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS.num_otf_attempts * 100
VASOPTIMIZATIONSAVINGS KPIs:	
VAS - Bytes Saved †	HTTPPROXYOPTIMIZATIONSAVINGS.compression_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.minify_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.web_image_optimization_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.offline_video_xcoding_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.online_video_xcoding_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.video_pacing_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.abr_rate_limiting_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.tcp_rl_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.quic_rl_bytes_saved
VAS Server-side Bytes Saved †	HTTPPROXYOPTIMIZATIONSAVINGS.tcp_rl_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.abr_rate_limiting_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.video_pacing_total_bytes_saved + CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_bytes_disk + CONTENTCACHESUMMARYSTATSCHASSIS.num_cache_service_bytes_memory

Table B-1 Derived Metrics

Metric	KPI Formula
VAS - Saving Ratio	((HTTPPROXYOPTIMIZATIONSAVINGS.compression_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.minify_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.web_image_optimization_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.offline_video_xcoding_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.online_video_xcoding_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.video_pacing_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.abr_rate_limiting_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.tcp_rl_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.quic_rl_bytes_saved) / CONTENTHTTPPROXYSUMMARYSTATSCHASSIS.num_bytes_client_response + TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_client_connections_bytes_sent + UDPPROXYSTATSCONNECTIONCHASSIS.client-connections-bytes-sent + (HTTPPROXYOPTIMIZATIONSAVINGS.compression_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.minify_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.web_image_optimization_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.offline_video_xcoding_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.online_video_xcoding_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.video_pacing_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.abr_rate_limiting_total_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.tcp_rl_bytes_saved + HTTPPROXYOPTIMIZATIONSAVINGS.quic_rl_bytes_saved))* 100
DIAMETER KPIs:	
Diameter - 3xx Error Rate	(DIAMETERSTATSPEER.numCCAInitial3xxx + DIAMETERSTATSPEER.numCCAUpdate3xxx + DIAMETERSTATSPEER.numCCATerminate3xxx) / (DIAMETERSTATSPEER.numCCRInitialAttempted + DIAMETERSTATSPEER.numCCRUpdateAttempted + DIAMETERSTATSPEER.numCCRTerminateAttempted) * 100
Diameter - 4xx Error Rate	(DIAMETERSTATSPEER.numCCAInitial4xxx + DIAMETERSTATSPEER.numCCAUpdate4xxx + DIAMETERSTATSPEER.numCCATerminate4xxx) / (DIAMETERSTATSPEER.numCCRInitialAttempted + DIAMETERSTATSPEER.numCCRUpdateAttempted + DIAMETERSTATSPEER.numCCRTerminateAttempted) * 100
Diameter - 5xx Error Rate	(DIAMETERSTATSPEER.numCCAInitial5xxx + DIAMETERSTATSPEER.numCCAUpdate5xxx + DIAMETERSTATSPEER.numCCATerminate5xxx) / (DIAMETERSTATSPEER.numCCRInitialAttempted + DIAMETERSTATSPEER.numCCRUpdateAttempted + DIAMETERSTATSPEER.numCCRTerminateAttempted) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
Diameter - CCA Sessions Retried on Secondary Server Due to Session Failover	(DIAMETERSTATSPEER.numCCAInitial3xxx + DIAMETERSTATSPEER.numCCRInitialTimeout - DIAMETERSTATSPEER.numCCAInitialDelayedSuccess) + (DIAMETERSTATSPEER.numCCAUpdate3xxx + DIAMETERSTATSPEER.numCCRUpdateTimeout - DIAMETERSTATSPEER.numCCAUpdateDelayedSuccess) + (DIAMETERSTATSPEER.numCCATerminate3xxx + DIAMETERSTATSPEER.numCCRTerminateTimeout - DIAMETERSTATSPEER.numCCATerminateDelayedSuccess)
Diameter - SWm Diameter STR	(1 – DIAMETERSTATSPEER.NumSTRSuccess / DIAMETERSTATSPEER.NumSTRAttempted) * 100
NETWORKCONTEXTSTATISTICS KPIs:	
Networking - IPv4 Tx Pkts Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numTxV4Pkts / (NETWORKCONTEXTSTATISTICSGRID.numTxV4Pkts + NETWORKCONTEXTSTATISTICSGRID.numTxV4DropPkts)) * 100
Networking - IPv4 Tx Bytes Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numTxV4Bytes / (NETWORKCONTEXTSTATISTICSGRID.numTxV4Bytes + NETWORKCONTEXTSTATISTICSGRID.numTxV4DropBytes)) * 100
Networking - IPv4 Rx Pkts Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numRxV4Pkts / (NETWORKCONTEXTSTATISTICSGRID.numRxV4Pkts + NETWORKCONTEXTSTATISTICSGRID.numRxV4DropPkts)) * 100
Networking - IPv4 Rx Bytes Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numRxV4Bytes / (NETWORKCONTEXTSTATISTICSGRID.numRxV4Bytes + NETWORKCONTEXTSTATISTICSGRID.numRxV4DropBytes)) * 100
Networking - IPv6 Tx Pkts Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numTxV6Pkts / (NETWORKCONTEXTSTATISTICSGRID.numTxV6Pkts + NETWORKCONTEXTSTATISTICSGRID.numTxV6DropPkts)) * 100
Networking - IPv6 Tx Bytes Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numTxV6Bytes / (NETWORKCONTEXTSTATISTICSGRID.numTxV6Bytes + NETWORKCONTEXTSTATISTICSGRID.numTxV6DropBytes)) * 100
Networking - IPv6 Rx Pkts Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numRxV6Pkts / (NETWORKCONTEXTSTATISTICSGRID.numRxV6Pkts + NETWORKCONTEXTSTATISTICSGRID.numRxV6DropPkts)) * 100
Networking - IPv6 Rx Bytes Success Rate	(NETWORKCONTEXTSTATISTICSGRID.numRxV6Bytes / (NETWORKCONTEXTSTATISTICSGRID.numRxV6Bytes + NETWORKCONTEXTSTATISTICSGRID.numRxV6DropBytes)) * 100
Networking - Throughput(Mbps) †	((NETWORKCONTEXTSTATISTICSGRID.numTxV4Bytes + NETWORKCONTEXTSTATISTICSGRID.numRxV4Bytes + NETWORKCONTEXTSTATISTICSGRID.numTxV6Bytes + NETWORKCONTEXTSTATISTICSGRID.numRxV6Bytes) * 8 / Interval) / 1000000

Table B-1 Derived Metrics

Metric	KPI Formula
IPSECNETWORKCONTEXTSTATS KPIs:	
Networking - DPD	(IKEMESSAGESTATS.deadPeerDetections / IPSECNETWORKCONTEXTSTATS.totalIkeTunnels) * 100
Networking - Rekey	IPSECNETWORKCONTEXTSTATS.rekeyedTransforms / IPSECNETWORKCONTEXTSTATS.totalTransforms
EMSGWQCIARP KPIs:	
QCI/ARP - Downlink Throughput(Mbps) †	EMSGWQCIARPSTATS.NumDownlinkBytes * 8 / 1000000 / Interval
QCI/ARP - Uplink Throughput(Mbps) †	EMSGWQCIARPSTATS.NumUplinkBytes * 8 / 1000000 / Interval
QCI/ARP - Bearer Drop Rate	EMSGWQCIARPSTATS.NumTotalBearersAbnormalRelease / (EMSGWQCIARPSTATS.NumTotalBearersAbnormalRelease + EMSGWQCIARPSTATS.NumTotalBearersNormalRelease) * 100
QCI/ARP - Handover Success Rate	EMSGWQCIARPSTATS.NumTotalBearersHandoverSuccess / (EMSGWQCIARPSTATS.NumTotalBearersHandoverSuccess + EMSGWQCIARPSTATS.NumTotalBearersHandoverFailure) * 100
QCI/ARP - Bearer Retainability Rate	EMSGWQCIARPSTATS.NumTotalBearersNormalRelease / (EMSGWQCIARPSTATS.NumTotalBearersNormalRelease + EMSGWQCIARPSTATS.NumTotalBearersAbnormalRelease) * 100
EMSGWAPNQCIARP KPIs:	
QCI/ARP APN - Downlink Throughput(Mbps) †	EMSGWAPNQCIARPSTATS.NumDownlinkBytes * 8 / 1000000 / Interval
QCI/ARP APN - Uplink Throughput(Mbps) †	EMSGWAPNQCIARPSTATS.NumUplinkBytes * 8 / 1000000 / Interval
QCI/ARP APN - Bearer Drop Rate	EMSGWAPNQCIARPSTATS.NumTotalBearersAbnormalRelease / (EMSGWAPNQCIARPSTATS.NumTotalBearersAbnormalRelease + EMSGWAPNQCIARPSTATS.NumTotalBearersNormalRelease) * 100
QCI/ARP APN - Handover Success Rate	EMSGWAPNQCIARPSTATS.NumTotalBearersHandoverSuccess / (EMSGWAPNQCIARPSTATS.NumTotalBearersHandoverSuccess + EMSGWAPNQCIARPSTATS.NumTotalBearersHandoverFailure) * 100
QCI/ARP APN - Bearer Retainability Rate	EMSGWAPNQCIARPSTATS.NumTotalBearersNormalRelease / (EMSGWAPNQCIARPSTATS.NumTotalBearersNormalRelease + EMSGWAPNQCIARPSTATS.NumTotalBearersAbnormalRelease) * 100
EPDGAPNCALLPERFSTATS KPIs:	
EPDG APN - Average Uplink Packet Size †	EPDGAPNCALLPERFSTATSGRID.NumUplinkBytes / EPDGAPNCALLPERFSTATSGRID.NumUplinkPackets
EPDG APN - Average Downlink Packet Size †	EPDGAPNCALLPERFSTATSGRID.NumDownlinkBytes / EPDGAPNCALLPERFSTATSGRID.NumDownlinkPackets

Table B-1 Derived Metrics

Metric	KPI Formula
EPDG APN - Uplink Data Rate Per APN †	(EPDGAPNCALLPERFSTATSGRID.NumUplinkBytes * 8) / (EPDGAPNCALLPERFSTATSGRID.NumCreateSessionAccept * 1000)
EPDG APN - Downlink Data Rate Per APN †	(EPDGAPNCALLPERFSTATSGRID.NumDownlinkBytes * 8) / (EPDGAPNCALLPERFSTATSGRID.NumCreateSessionAccept * 1000)
EPDGCALLPERFSTATS KPIs:	
EPDG - Total Authentication Failures	EPDGCALLPERFSTATSGRID.NumEpdgAuthFailures + EPDGCALLPERFSTATSGRID.NumEpdgAAAReauthFailures
EPDG - IPv4 Subscriber Percentage	(EPDGCALLPERFSTATSGRID.NumIpv4Sessions * 100) / (EPDGCALLPERFSTATSGRID.NumIpv4Sessions + EPDGCALLPERFSTATSGRID.NumIpv6Sessions + EPDGCALLPERFSTATSGRID.NumIpv4v6Sessions)
EPDG - IPv6 Subscriber Percentage	(EPDGCALLPERFSTATSGRID.NumIpv6Sessions * 100) / (EPDGCALLPERFSTATSGRID.NumIpv4Sessions + EPDGCALLPERFSTATSGRID.NumIpv6Sessions + EPDGCALLPERFSTATSGRID.NumIpv4v6Sessions)
EPDG - IPv4v6 Subscriber Percentage	(EPDGCALLPERFSTATSGRID.NumIpv4v6Sessions * 100) / (EPDGCALLPERFSTATSGRID.NumIpv4Sessions + EPDGCALLPERFSTATSGRID.NumIpv6Sessions + EPDGCALLPERFSTATSGRID.NumIpv4v6Sessions)
EPDG - Active Current Sessions Percentage	(EPDGCALLPERFSTATSGRID.NumActiveCurrentSessions * 100) / (EPDGCALLPERFSTATSGRID.NumActiveCurrentSessions + EPDGCALLPERFSTATSGRID.NumIdleCurrentSessions)
EPDG - S2bC Create Bearer Failure Rate	(1 - EPDGCALLPERFSTATSGRID.NumCreateBearerAccept / EPDGCALLPERFSTATSGRID.NumCreateBearerReq) * 100
EPDG - S2bC Delete Session Failure Rate	(1 - EPDGCALLPERFSTATSGRID.NumDeleteSessionAcceptFromPgw / EPDGCALLPERFSTATSGRID.NumDeleteSessionReqToPgw) * 100
EPDG - S2bC Update Bearer Failure Rate	(1 - EPDGCALLPERFSTATSGRID.NumUpdateBearerAccept / EPDGCALLPERFSTATSGRID.NumUpdateBearerReq) * 100
EPDG - SWm EAP Failure Rate	(1 - EPDGCALLPERFSTATSGRID.NumEpdgEapSuccess / EPDGCALLPERFSTATSGRID.NumEpdgEapAttempts) * 100
EPDG - Average Rekeying Rate	EPDGCALLPERFSTATSGRID.NumIPSecRekey / EPDGCALLPERFSTATSGRID.NumCurrentSessions
TCPMEASUREMENTSSUMMARYSTATSCHASSIS KPIs:	
TCP Client-side - Downstream TCP Segments Retransmitted Percentage	(TCPMEASUREMENTSSUMMARYSTATSCHASSIS.num_total_segments_retrans_dl / TCPMEASUREMENTSSUMMARYTATSCHASSIS.num_total_estimated_segments_dl) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
TCPSPLICING KPIs:	
TCP-Splicing - Success Percentage	(TCPSPLICINGSTATSSUMMARYCHASSIS.num_tcp_splicing_summary_successes + TCPSPLICINGSTATSSUMMARYCHASSIS.num_tcp_splicing_summary_aborts) / (TCPSPLICINGSTATSSUMMARYCHASSIS.num_tcp_splicing_summary_attempts)
TCP-Splicing - Failure Percentage	(TCPSPLICINGSTATSSUMMARYCHASSIS.num_tcp_splicing_summary_failures) / (TCPSPLICINGSTATSSUMMARYCHASSIS.num_tcp_splicing_summary_attempts)
TCP-Splicing - Transaction Rate	(TCPSPLICINGSTATSSUMMARYCHASSIS.num_tcp_splicing_summary_attempts) / Interval
TCP-Splicing - Client Downlink Throughput (Mbps) †	(TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_client_connections_bytes_sent) * 8 / 1,000,000 / Interval
TCP-Splicing - Client Uplink Throughput (Mbps) †	(TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_client_connections_bytes_received) * 8 / 1,000,000 / Interval
TCP-Splicing - Server Downlink Throughput (Mbps) †	(TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_server_connections_bytes_received) * 8 / 1,000,000 / Interval
TCP-Splicing - Server Uplink Throughput (Mbps) †	(TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_server_connections_bytes_sent) * 8 / 1,000,000 / Interval
TCP-Splicing - Average Client Downlink Throughput (Mbps) †	(TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_client_connections_bytes_sent) * 8 / 1,000,000 / (TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_client_connections_total) / Interval
TCP-Splicing - Average Client Uplink Throughput (Mbps) †	(TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_client_connections_bytes_received) * 8 / 1,000,000 / (TCPSPLICINGSTATSCONNECTIONCHASSIS.num_tcp_splicing_client_connections_total) / Interval

Table B-1 Derived Metrics

Metric	KPI Formula
WAGCALLPERFSTATS KPIs:	
DHCP - Average DHCP Latency(microsecond)	WAGCALLPERFSTATSGRID.AverageDhcpClientLatency / WAGCALLPERFSTATSGRID.DhcpClientLatencySamples
WAG - IPv4 Subscriber Percentage	(WAGCALLPERFSTATSGRID.NumIpv4Sessions * 100) / (WAGCALLPERFSTATSGRID.NumIpv4Sessions + WAGCALLPERFSTATSGRID.NumIpv6Sessions + WAGCALLPERFSTATSGRID.NumIpv4v6Sessions)
WAG - IPv6 Subscriber Percentage	(WAGCALLPERFSTATSGRID.NumIpv6Sessions * 100) / (WAGCALLPERFSTATSGRID.NumIpv4Sessions + WAGCALLPERFSTATSGRID.NumIpv6Sessions + WAGCALLPERFSTATSGRID.NumIpv4v6Sessions)
WAG - IPv4v6 Subscriber Percentage	(WAGCALLPERFSTATSGRID.NumIpv4v6Sessions * 100) / (WAGCALLPERFSTATSGRID.NumIpv4Sessions + WAGCALLPERFSTATSGRID.NumIpv6Sessions + WAGCALLPERFSTATSGRID.NumIpv4v6Sessions)
WAG - Active Current Sessions Percentage	(WAGCALLPERFSTATSGRID.NumActiveCurrentSessions * 100) / (WAGCALLPERFSTATSGRID.NumActiveCurrentSessions + WAGCALLPERFSTATSGRID.NumIdleCurrentSessions)
WAGAPNCALLPERFSTATS KPIs:	
WAG APN - Average Uplink Packet Size †	WAGAPNCALLPERFSTATSGRID.NumUplinkBytes / WAGAPNCALLPERFSTATSGRID.NumUplinkPackets
WAG APN - Average Downlink Packet Size †	WAGAPNCALLPERFSTATSGRID.NumDownlinkBytes / WAGAPNCALLPERFSTATSGRID.NumDownlinkPackets
WAG APN - Uplink Data Rate Per APN †	(WAGAPNCALLPERFSTATSGRID.NumUplinkBytes * 8) / (WAGAPNCALLPERFSTATSGRID.NumCreateSessionAccept * 1000)
WAG APN - Downlink Data Rate Per APN †	(WAGAPNCALLPERFSTATSGRID.NumDownlinkBytes * 8) / (WAGAPNCALLPERFSTATSGRID.NumCreateSessionAccept * 1000)
DHCP APN - Average DHCP Latency(microsecond)	WAGAPNCALLPERFSTATSGRID.AverageDhcpClientLatency / WAGAPNCALLPERFSTATSGRID.DhcpClientLatencySamples
MME KPIs:	
SGSN - UMTS Attach Success Rate Nodal	100 * (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.U / (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Nodal.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Nodal.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.UPLMN.Nodal.U))
SGSN - UMTS Activation Success Rate Nodal	100 * (UMTSSM_PROCEDURE.SM.SuccActPdpContext.U / (UMTSSM_PROCEDURE.SM.SuccActPdpContext.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.Nodal.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.Nodal.U))

Table B-1 Derived Metrics

Metric	KPI Formula
SGSN - UMTS Uplink Throughput (Kbps) - Data VM †	((sd.relay.GTP.GtpuInDataOctIu * 8) / samplePeriodInSeconds) / 1000
SGSN - UMTS Downlink Throughput (Kbps) - Data VM †	((sd.relay.GTP.GtpuOutDataOctIu * 8) / samplePeriodInSeconds) / 1000
SGSN - UMTS Uplink Packet Throughput (Kpps) - Data VM	((sd.relay.GTP.GtpuInDataPktIu) / samplePeriodInSeconds) / 1000
SGSN - UMTS Downlink Packet Throughput (Kpps) - Data VM	((sd.relay.GTP.GtpuOutDataPktIu) / samplePeriodInSeconds) / 1000
SGSN - GPRS Attach Success Rate Nodal	100 * (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.G / (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Nodal.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Nodal.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.UPLMN.Nodal.G))
SGSN - GPRS Activation Success Rate Nodal	100 * (GPRSSM_PROCEDURE.SM.SuccActPdpContext.G / (GPRSSM_PROCEDURE.SM.SuccActPdpContext.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.Nodal.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.Nodal.G))
SGSN - GPRS Downlink Packet Throughput (Kpps) - Data VM †	(((sd.relay.VS.GTP.OutDataOctGn - sd.relay.GTP.GtpuInDataOctIu) * 8) / samplePeriodInSeconds) / 1000
SGSN - GPRS Downlink Throughput (Kbps) - Data VM †	(((sd.relay.VS.GTP.InDataOctGn - sd.relay.GTP.GtpuOutDataOctIu) * 8) / samplePeriodInSeconds) / 1000
SGSN - GPRS Uplink Packet Throughput (Kpps) - Data VM †	((sd.relay.VS.GTP.OutDataPktGn - sd.relay.GTP.GtpuInDataPktIu) / samplePeriodInSeconds) / 1000
SGSN - GPRS Downlink Packet Throughput (Kpps) - Data VM †	((sd.relay.VS.GTP.InDataPktGn - sd.relay.GTP.GtpuOutDataPktIu) / samplePeriodInSeconds) / 1000
SGSN - GPRS Page Success Rate	100 * (GPRSMM_MISC.MM.SuccPsPagingProcGb) / (GPRSMM_MISC.MM.AttPsPagingProcGb)
SGSN - UMTS Page Success Rate	100 * (UMTSMM_MISC.MM.SuccPsPagingProcIu) / (UMTSMM_MISC.MM.AttPsPagingProcIu)
SGSN - GPRS RAU Success Rate Network	100 * ((GPRSMM_PROCEDURE.MM.SuccIntraSgsnRaUpdate.G) / (GPRSMM_PROCEDURE.MM.SuccIntraSgsnRaUpdate.G + GPRSMM_RAUFAIL.VS.MM.FailIntraSgsnRaUpdate.MsgError.G + GPRSMM_RAUFAIL.MM.FailIntraSgsnRaUpdate.NetworkFailure_17.G + GPRSMM_RAUFAIL.MM.FailIntraSgsnRaUpdate.Congestion_22.G + GPRSMM_RAUFAIL.MsIdNotDerived_9.PtmsiCollision.G))

Table B-1 Derived Metrics

Metric	KPI Formula
SGSN - GPRS IRAU Success Rate Network	100 * GPRSMM_PROCEDURE.`MM.SuccInterSgsnRaUpdate.G` / (GPRSMM_PROCEDURE.`MM.SuccInterSgsnRaUpdate.G` + GPRSMM_IRAUFAIL.`VS.MM.FailInterSgsnRaUpdate.MsgError.G` + GPRSMM_IRAUFAIL.`MM.FailInterSgsnRaUpdate.NetworkFailure_17.G` - GPRSMM_IRAUFAIL.`NetworkFailure_17.UeSignalRate.G` + GPRSMM_IRAUFAIL.`MM.FailInterSgsnRaUpdate.Congestion_22.G` - GPRSMM_IRAUFAIL.`Congestion_22.UeSignalRate.G` + GPRSMM_IRAUFAIL.`MsIdNotDerived_9.PtmsiCollision.G`)
SGSN - UMTS RAU Success Rate Network	100 * ((UMTSMM_PROCEDURE.MM.SuccIntraSgsnRaUpdate.U) / (UMTSMM_PROCEDURE.MM.SuccIntraSgsnRaUpdate.U + UMTSMM_RAUFAIL.VS.MM.FailIntraSgsnRaUpdate.MsgError.U + UMTSMM_RAUFAIL.MM.FailIntraSgsnRaUpdate.NetworkFailure_17.U + UMTSMM_RAUFAIL.MM.FailIntraSgsnRaUpdate.Congestion_22.U + UMTSMM_RAUFAIL.MsIdNotDerived_9.PtmsiCollision.U))
SGSN - UMTS IRAU Success Rate Network	100 * UMTSMM_PROCEDURE.`MM.SuccInterSgsnRaUpdate.U` / (UMTSMM_PROCEDURE.`MM.SuccInterSgsnRaUpdate.U` + UMTSMM_IRAUFAIL.`VS.MM.FailInterSgsnRaUpdate.MsgError.U` + UMTSMM_IRAUFAIL.`MM.FailInterSgsnRaUpdate.MsIdNotDerived_9.U` + UMTSMM_IRAUFAIL.`MM.FailInterSgsnRaUpdate.NetworkFailure_17.U` - UMTSMM_IRAUFAIL.`NetworkFailure_17.UeSignalRate.U` + UMTSMM_IRAUFAIL.`MM.FailInterSgsnRaUpdate.Congestion_22.U` - UMTSMM_IRAUFAIL.`VS.MM.FailInterSgsnRaUpdate.UeSignalRate.U`)
MME - LTE Attach Success Rate Nodal	100 * (LTEMM_PROCEDURE.MM.EpsAttachSucc.E / (LTEMM_PROCEDURE.MM.EpsAttachSucc.E + LTEMM_PROCEDURE.MM.EpsAttachFail.VPLMN.Nodal.E + LTEMM_PROCEDURE.MM.EpsAttachFail.HPLMN.Nodal.E + LTEMM_PROCEDURE.MM.EpsAttachFail.UPLMN.Nodal.E))
MME - LTE Attach Success Rate Network	100 * (LTEMM_PROCEDURE.MM.EpsAttachSucc.E / (LTEMM_PROCEDURE.MM.EpsAttachSucc.E + LTEMM_PROCEDURE.MM.EpsAttachFail.VPLMN.Network.E + LTEMM_PROCEDURE.MM.EpsAttachFail.HPLMN.Network.E + LTEMM_PROCEDURE.MM.EpsAttachFail.UPLMN.Network.E))
MME - LTE Attach Success Rate HPLMN Nodal	100 * (LTEMM_PROCEDURE.MM.EpsAttachSucc.HPLMN.E / (LTEMM_PROCEDURE.MM.EpsAttachSucc.HPLMN.E + LTEMM_PROCEDURE.MM.EpsAttachFail.HPLMN.Nodal.E))
MME - LTE Attach Success Rate HPLMN Network	100 * (LTEMM_PROCEDURE.MM.EpsAttachSucc.HPLMN.E / (LTEMM_PROCEDURE.MM.EpsAttachSucc.HPLMN.E + LTEMM_PROCEDURE.MM.EpsAttachFail.HPLMN.Network.E))
MME - LTE Attach Success Rate VPLMN Nodal	100 * (LTEMM_PROCEDURE.MM.EpsAttachSucc.VPLMN.E / (LTEMM_PROCEDURE.MM.EpsAttachSucc.VPLMN.E + LTEMM_PROCEDURE.MM.EpsAttachFail.VPLMN.Nodal.E))
MME - LTE Attach Success Rate VPLMN Network	100 * (LTEMM_PROCEDURE.MM.EpsAttachSucc.VPLMN.E / (LTEMM_PROCEDURE.MM.EpsAttachSucc.VPLMN.E + LTEMM_PROCEDURE.MM.EpsAttachFail.VPLMN.Network.E))

Table B-1 Derived Metrics

Metric	KPI Formula
MME - LTE PDN Session Activation Success Rate Nodal	100 * (LTESM_PROCEDURE.`SM.ActDefaultEpsBearerPdnConSucc` + LTESM_PROCEDURE.`SM.ActDefaultEpsBearerAttachSucc`) / (LTESM_PROCEDURE.`SM.ActDefaultEpsBearerPdnConSucc` + LTESM_PROCEDURE.`SM.ActDefaultEpsBearerAttachSucc` + LTESM_SESSIONACTFAIL.`InsfRscs_26.ControlPlaneFail` + LTESM_SESSIONACTFAIL.`InsfRscs_26.MsgSendFail` + LTESM_SESSIONACTFAIL.`ActRejUnspc_31.GrdTimerExpiry`)
MME - LTE PDN Session Activation Success Rate Network	100 * (LTESM_PROCEDURE.`SM.ActDefaultEpsBearerPdnConSucc` + LTESM_PROCEDURE.`SM.ActDefaultEpsBearerAttachSucc`) / (LTESM_PROCEDURE.`SM.ActDefaultEpsBearerPdnConSucc` + LTESM_PROCEDURE.`SM.ActDefaultEpsBearerAttachSucc` + LTESM_SESSIONACTFAIL.`SM.ActDefaultEpsBearerFail.ActRejSgw OrPgw_30` + LTESM_SESSIONACTFAIL.`SM.ActDefaultEpsBearerFail.ActRejUnspc_ 31` + LTESM_SESSIONACTFAIL.`SM.ActDefaultEpsBearerFail.SrvcTempOutO fOrder_34` + LTESM_SESSIONACTFAIL.`SM.ActDefaultEpsBearerFail.NetworkFailure _38` + LTESM_SESSIONACTFAIL.`VS.SM.ActDefaultEpsBearerFail.MsgErr` + LTESM_SESSIONACTFAIL.`VS.SM.ActDefaultEpsBearerFail.UeTimeout ` + LTESM_SESSIONACTFAIL.`InsfRscs_26.ErabSetupFail` + LTESM_SESSIONACTFAIL.`InsfRscs_26.ControlPlaneFail` + LTESM_SESSIONACTFAIL.`InsfRscs_26.MsgSendFail`)
MME - LTE Bearer Activation Success Rate Nodal	100 * (LTESM_PROCEDURE.SM.ActDedicatedEpsBearerSucc / (LTESM_PROCEDURE.SM.ActDedicatedEpsBearerSucc + LTESM_PROCEDURE.SM.ActDedicatedEpsBearerFail.VPLMN.Nodal + LTESM_PROCEDURE.SM.ActDedicatedEpsBearerFail.HPLMN.Nodal))
MME - LTE Bearer Activation Success Rate Network	100 * (LTESM_PROCEDURE.SM.ActDedicatedEpsBearerSucc / (LTESM_PROCEDURE.SM.ActDedicatedEpsBearerSucc + LTESM_PROCEDURE.SM.ActDedicatedEpsBearerFail.VPLMN.Network + LTESM_PROCEDURE.SM.ActDedicatedEpsBearerFail.HPLMN.Network))
MME - TAU Success Rate Nodal	100 * (LTEMM_PROCEDURE.VS.MM.IntraMmeTauSucc + LTEMM_TAU.ISYSC.IntraNodeGsmEpsSucc + LTEMM_TAU.ISYSC.IntraNodeUmtsEpsSucc) / (LTEMM_PROCEDURE.VS.MM.IntraMmeTauAtt + LTEMM_TAU.ISYSC.IntraNodeGsmEpsAtt + LTEMM_TAU.ISYSC.IntraNodeUmtsEpsAtt - LTEMM_TAU.VS.MM.IntraMmeTauDcnReroute)

Table B-1 Derived Metrics

Metric	KPI Formula
MME - TAU Success Rate Network	100 * ((LTEMM_PROCEDURE.VS.MM.IntraMmeTauSucc + LTEMM_TAU.ISYSC.IntraNodeGsmEpsSucc + LTEMM_TAU.ISYSC.IntraNodeUmtsEpsSucc) / (LTEMM_PROCEDURE.VS.MM.IntraMmeTauSucc + LTEMM_TAU.ISYSC.IntraNodeGsmEpsSucc + LTEMM_TAU.ISYSC.IntraNodeUmtsEpsSucc + LTEMM_TAUFAIL.VS.MM.IntraMmeTauFail.NetworkFailure_17 + LTEMM_TAUFAIL.VS.MM.IntraMmeTauFail.EsmFailure_19 + LTEMM_TAUFAIL.VS.MM.IntraMmeTauFail.Congestion_22 + LTEMM_TAUFAIL.VS.MM.IntraMmeTauFail.MsgErr + LTEMM_TAUFAIL.VS.MM.IntraMmeTauFail.Other + LTEMM_TAUFAIL.VS.MM.TauReqIgn))
MME - ITAU Success Rate Nodal	100 * (LTEMM_PROCEDURE.VS.MM.InterMmeTauSucc + LTEMM_PROCEDURE.VS.MM.InterSgsnTauSucc) / (LTEMM_PROCEDURE.VS.MM.InterMmeTauAtt + LTEMM_PROCEDURE.VS.MM.InterSgsnTauAtt - LTEMM_ITAU.VS.MM.InterMmeTauDcnReroute - LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.Congestion_22.AdmissionControl - LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.UeSignalRate)
MME - ITAU Success Rate Network	100 * ((LTEMM_ITAU.VS.MM.InterMmeTauInterSgwSucc + LTEMM_ITAU.VS.MM.InterMmeTauIntraSgwSucc) / (LTEMM_ITAU.VS.MM.InterMmeTauInterSgwSucc + LTEMM_ITAU.VS.MM.InterMmeTauIntraSgwSucc + LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.NetworkFailure_17 - LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.NetworkFailure_17.UeSignalRate + LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.Congestion_22 - LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.Congestion_22.UeSignalRate + LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.MsgErr + LTEMM_ITAUFAIL.VS.MM.InterMmeTauFail.Other + LTEMM_ITAUFAIL.VS.MM.ItauReqIgn))
MME - Page Success Rate	100 * (LTEMM_PROCEDURE.MM.PagingEpsAtt - LTEMM_PROCEDURE.MM.PagingEpsFail) / (LTEMM_PROCEDURE.MM.PagingEpsAtt)
SGSN - UMTS Attach Success Rate Network	100 * (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.U / (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Network.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Network.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.UPLMN.Network.U))
SGSN - UMTS Attach Success Rate HPLMN Nodal	100 * (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.U / (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Nodal.U))
SGSN - UMTS Attach Success Rate HPLMN Network	100 * (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.U / (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Network.U))

Table B-1 Derived Metrics

Metric	KPI Formula
SGSN - UMTS Attach Success Rate VPLMN Nodal	100 * (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.U / (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Nodal.U))
SGSN - UMTS Attach Success Rate VPLMN Network	100 * (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.U / (UMTSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.U + UMTSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Network.U))
SGSN - UMTS Activation Success Rate Network	100 * (UMTSSM_PROCEDURE.SM.SuccActPdpContext.U / (UMTSSM_PROCEDURE.SM.SuccActPdpContext.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.Network.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.Network.U))
SGSN - UMTS Activation Success Rate HPLMN Nodal	100 * (UMTSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.U / (UMTSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.nodal.U))
SGSN - UMTS Activation Success Rate HPLMN Network	100 * (UMTSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.U / (UMTSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.network.U))
SGSN - UMTS Activation Success Rate VPLMN Nodal	100 * (UMTSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.U / (UMTSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.nodal.U))
SGSN - UMTS Activation Success Rate VPLMN Network	100 * (UMTSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.U / (UMTSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.U + UMTSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.network.U))
SGSN - GPRS Attach Success Rate Network	100 * (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.G / (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Nodal.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Nodal.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.UPLMN.Nodal.G))
SGSN - GPRS Attach Success Rate HPLMN Nodal	100 * (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.G / (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Nodal.G))
SGSN - GPRS Attach Success Rate HPLMN Network	100 * (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.G / (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.HPLMN.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.HPLMN.Network.G))
SGSN - GPRS Attach Success Rate VPLMN Nodal	100 * (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.G / (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Nodal.G))
SGSN - GPRS Attach Success Rate VPLMN Network	100 * (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.G / (GPRSMM_PROCEDURE.VS.MM.SuccMsAttach.VPLMN.G + GPRSMM_PROCEDURE.VS.MM.AttachRej.VPLMN.Network.G))

Table B-1 Derived Metrics

Metric	KPI Formula
SGSN - GPRS Activation Success Rate Network	100 * (GPRSSM_PROCEDURE.SM.SuccActPdpContext.G / (GPRSSM_PROCEDURE.SM.SuccActPdpContext.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.Network.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.Network.G))
SGSN - GPRS Activation Success Rate HPLMN Nodal	100 * (GPRSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.G / (GPRSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.nodal.G))
SGSN - GPRS Activation Success Rate HPLMN Network	100 * (GPRSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.G / (GPRSSM_PROCEDURE.SM.SuccActPdpContext.HPLMN.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.HPLMN.network.G))
SGSN - GPRS Activation Success Rate VPLMN Nodal	100 * (GPRSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.G / (GPRSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.nodal.G))
SGSN - GPRS Activation Success Rate VPLMN Network	100 * (GPRSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.G / (GPRSSM_PROCEDURE.SM.SuccActPdpContext.VPLMN.G + GPRSSM_PROCEDURE.SM.FailActPdpContext.VPLMN.network.G))
MME - LTE First Page Success Rate per Profile	100 * (1-(LTEMM_PAGINGPROFILE.MM.PagingEpsFirstRetryAtt / LTEMM_PAGINGPROFILE.MM.PagingEpsAtt))
MME - LTE Service Request Success Rate	100 * (LTEMM_PROCEDURE.MM.ServiceRequestSucc /LTEMM_PROCEDURE.MM.ServiceRequestAtt)
SSF KPIs:	
SSF - DNS External Query Success Rate	100 * (SSF_DNS_DNS.external-query-success / SSF_DNS_DNS.external-query-attempt)
SSF - DNS Internal Cache Hit Rate	100 * ((SSF_DNS_DNS.dynamic-cache-success + SSF_DNS_DNS.static-cache-success) / SSF_DNS_DNS.total-query-attempt)
SSF - GTP CSR Success Rate	100 * ((SSF_GTP_3GPP_TUNNEL.gtpv1-create-pdp-context-response-rx + SSF_GTP_3GPP_TUNNEL.gtpv2-create-session-response-rx - SSF_GTP_3GPP_TUNNEL.gtpv1-create-pdp-context-response-gw-failure-rx - SSF_GTP_3GPP_TUNNEL.gtpv2-create-session-response-gw-failure-rx) / (SSF_GTP_3GPP_TUNNEL.gtpv1-create-pdp-context-request-tx + SSF_GTP_3GPP_TUNNEL.gtpv2-create-session-request-tx))
SSF - GTP Transactions Per Second	(SSF_GTP_3GPP_TUNNEL.gtpv1-create-pdp-context-request-tx + SSF_GTP_3GPP_TUNNEL.gtpv2-create-session-request-tx) / (collection-interval-seconds=300)
SSF - LDAP Search Success Rate	100 * (SSF_LDAP_MSG.search-success / (SSF_LDAP_MSG.search-success + SSF_LDAP_MSG.search-fail-timeout + SSF_LDAP_MSG.search-fail-discard + SSF_LDAP_MSG.search-fail-other))
SSF - LDAP TPS	SSF_LDAP_MSG.search-result / (collection-interval-seconds=300)

Table B-1 Derived Metrics

Metric	KPI Formula
SSF - Packets Per Second	SSF_PLATFORM_NETWORK.outgoing-packets / (collection-interval-seconds=300)
SSF - REST Query Success Rate	100 * ((SSF_REST_MSG.http-response - SSF_REST_MSG.http-failure) / (SSF_REST_MSG.http-response + SSF_REST_MSG.http-request-discard))
SSF - EST TPS	SSF_REST_MSG.http-response / Interval
GTP V1 Left Side CSR Network Success Rate	100 * (SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx – SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx.resent – SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx.reject.ssf – SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx.reject.ggsn) / (SSF_GTP_3GPP_V1_LEFT.create-pdpc-request-rx – SSF_GTP_3GPP_V1_LEFT.create-pdpc-request-rx.resent – SSF_GTP_3GPP_V1_LEFT.create-pdpc-request-rx.passthru)
GTP V1 Left Side CSR Nodal Success Rate	100 * (SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx – SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx.resent - SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx.reject.ssf + SSF_GTP_3GPP_V1_LEFT.create-pdpc-response-tx.reject.ssf.procedure-timeout) / (SSF_GTP_3GPP_V1_LEFT.create-pdpc-request-rx – SSF_GTP_3GPP_V1_LEFT.create-pdpc-request-rx.resent – SSF_GTP_3GPP_V1_LEFT.create-pdpc-request-rx.passthru)
GTP V1 Right Side CSR Network Success Rate	100 * (SSF_GTP_3GPP_V1_RIGHT.create-pdpc-response-rx – SSF_GTP_3GPP_V1_RIGHT.create-pdpc-response-rx.resent – SSF_GTP_3GPP_V1_RIGHT.create-pdpc-response-rx.ignored – SSF_GTP_3GPP_V1_RIGHT.create-pdpc-response-rx.reject) / (SSF_GTP_3GPP_V1_RIGHT.create-pdpc-request-tx – SSF_GTP_3GPP_V1_RIGHT.create-pdpc-request-tx.resent – SSF_GTP_3GPP_V1_RIGHT.create-pdpc-request-tx.reselect.resent – SSF_GTP_3GPP_V1_RIGHT.create-pdpc-request-tx.passthru)
GTP V2 Left Side CSR Network Success Rate	100 * (SSF_GTP_3GPP_V2_LEFT.create-session-response-tx – SSF_GTP_3GPP_V2_LEFT.create-session-response-tx.resent – SSF_GTP_3GPP_V2_LEFT.create-session-response-tx.reject.ssf – SSF_GTP_3GPP_V2_LEFT.create-session-response-tx.reject.gw) / (SSF_GTP_3GPP_V2_LEFT.create-session-request-rx – SSF_GTP_3GPP_V2_LEFT.create-session-request-rx.resent– SSF_GTP_3GPP_V2_LEFT.create-session-request-rx.passthru)
GTP V2 Left Side CSR Nodal Success Rate	100 * (SSF_GTP_3GPP_V2_LEFT.create-session-response-tx – SSF_GTP_3GPP_V2_LEFT.create-session-response-tx.resent - SSF_GTP_3GPP_V2_LEFT.create-session-response-tx.reject.ssf + SSF_GTP_3GPP_V2_LEFT.create-session-response-tx.reject.ssf.procedure-timeout) / (SSF_GTP_3GPP_V2_LEFT.create-session-request-rx – SSF_GTP_3GPP_V2_LEFT.create-session-request-rx.resent – SSF_GTP_3GPP_V2_LEFT.create-session-request-rx.passthru)

Table B-1 Derived Metrics

Metric	KPI Formula
GTP V2 Right Side CSR Network Success Rate	100 * (SSF_GTP_3GPP_V2_RIGHT.create-session-response-rx – SSF_GTP_3GPP_V2_RIGHT.create-session-response-rx.resent – SSF_GTP_3GPP_V2_RIGHT.create-session-response-rx.ignored – SSF_GTP_3GPP_V2_RIGHT.create-session-response-rx.reject) / (SSF_GTP_3GPP_V2_RIGHT.create-session-request-tx – SSF_GTP_3GPP_V2_RIGHT.create-session-request-tx.resent – SSF_GTP_3GPP_V2_RIGHT.create-session-request-tx.reselect.resent – SSF_GTP_3GPP_V2_RIGHT.create-session-request-tx.passthru)
DIAMETER Transactions Per Second	SSF_DIAMETER_MSG.get-gateway-answer / SSF_DIAMETER_MSG.seconds-per-interval
DIAMETER Query Success Rate	100 * (SSF_DIAMETER_MSG.get-gateway-answer.success / SSF_DIAMETER_MSG.get-gateway-request)
GTP Proxy KPIs:	
GTP Proxy - Current 2G/3G Gn/Gp Sessions	GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsGnGeran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsGnUtran
GTP Proxy – Active Current Sessions Percentage	GTPPROXYCALLPERFSTATSGRID.NumActiveCurrentSessions / (GTPPROXYCALLPERFSTATSGRID.NumActiveCurrentSessions + GTPPROXYCALLPERFSTATSGRID.NumIdleCurrentSessions)
GTP Proxy – CDR Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumGtppCdrRespSuccess / GTPPROXYCALLPERFSTATSGRID.NumGtppCdrSent) * 100
GTP Proxy - Create PDP Context Accepts per Second	GTPPROXYCALLPERFSTATSGRID.NumCreatePdpAccept / Interval
GTP Proxy - Create PDP Context Local Failure Rate	(GTPPROXYCALLPERFSTATSGRID.NumCreatePdpRejectRsrc Unavailable + GTPPROXYCALLPERFSTATSGRID.NumCreatePdp RejectSystemFailure) / GTPPROXYCALLPERFSTATSGRID.NumCreatePdpAttempt * 100
GTP Proxy - Create PDP Context Rejects per Second	GTPPROXYCALLPERFSTATSGRID.NumCreatePdpReject / Interval
GTP Proxy - Create PDP Context Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumCreatePdpAccept / GTPPROXYCALLPERFSTATSGRID.NumCreatePdpAttempt) * 100
GTP Proxy - Current 2G/3G S5/S8 Sessions	GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran
GTP Proxy - Current 2G/3G Sessions	GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsGnGeran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsGnUtran
GTP Proxy - Current Co-located 2G/3G S5/S8 Sessions	GTPPROXYCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8 Geran + GTPPROXYCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8 Utran

Table B-1 Derived Metrics

Metric	KPI Formula
GTP Proxy - Current Standalone 2G/3G S5/S8 Sessions	GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran - GTPPROXYCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8 Geran - GTPPROXYCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8 Utran
GTP Proxy - Current Standalone 2G/3G Sessions	GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Geran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsS5S8Utran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsGnGeran + GTPPROXYCALLPERFSTATSGRID.NumCurrentSessionsGnUtran - GTPPROXYCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8 Geran - GTPPROXYCALLPERFSTATSGRID.NumSaegwCurrentSessionsS5S8 Utran
GTP Proxy - Current Standalone 4G Sessions	GTPPROXYCALLPERFSTATSGRID.NumRatTypeEUtranSessions - GTPPROXYCALLPERFSTATSGRID.NumSaegwRatTypeEUtranSessions
GTP Proxy - Current Standalone Sessions	GTPPROXYCALLPERFSTATSGRID.NumCurrentSessions - GTPPROXYCALLPERFSTATSGRID.NumSaegwCurrentSessions
GTP Proxy - Delete PDP Context Accepts per Second	GTPPROXYCALLPERFSTATSGRID.NumDeletePdpAccept / Interval
GTP Proxy - Delete PDP Context Rejects per Second	GTPPROXYCALLPERFSTATSGRID.NumDeletePdpReject / Interval
GTP Proxy – Downlink Packet Rate (pps)	GTPPROXYCALLPERFSTATSGRID.NumDownlinkPackets / Interval
GTP Proxy – Downlink Throughput (Mbps) †	GTPPROXYCALLPERFSTATSGRID.NumDownlinkBytes * 8 / Interval / 1000000
GTP Proxy - EPS Attach Success Rate	(GTPPROXYPROCEDUREGRID.NumCreateSessionSuccess) / (GTPPROXYPROCEDUREGRID.NumCreateSessionFail + GTPPROXYPROCEDUREGRID.NumCreateSessionSuccess) * 100
GTP Proxy - EPS Bearer Activation Success Rate	GTPPROXYCALLPERFSTATSGRID.NumCreateSessionAccept / GTPPROXYCALLPERFSTATSGRID.NumCreateSessionAttempt * 100
GTP Proxy - Gn/Gp to LTE Handover Success Rate	GTPPROXYPROCEDUREGRID.NumGnGpToLteHandoverSuccess / (GTPPROXYPROCEDUREGRID.NumGnGpToLteHandoverSuccess + GTPPROXYPROCEDUREGRID.NumGnGpToLteHandoverFail) * 100
GTP Proxy - Idle Session Duration Exceeded Closes per Second	GTPPROXYCALLPERFSTATSGRID.NumIdleDurationExceededCloses / Interval
GTP Proxy - Inter-SGSN Handover Success Rate	GTPPROXYPROCEDUREGRID.NumInterSgsnHandoverSuccess / (GTPPROXYPROCEDUREGRID.NumInterSgsnHandoverSuccess + GTPPROXYPROCEDUREGRID.NumInterSgsnHandoverFail) * 100
GTP Proxy - Inter-SGW Handover Success Rate	GTPPROXYPROCEDUREGRID.NumInterSgwHandoverSuccess / (GTPPROXYPROCEDUREGRID.NumInterSgwHandoverSuccess + GTPPROXYPROCEDUREGRID.NumInterSgwHandoverFail) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
GTP Proxy - LTE to Gn/Gp Handover Success Rate	GTPPROXYPROCEDUREGRID.NumInterLteToGnGpSuccess / (GTPPROXYPROCEDUREGRID.NumInterLteToGnGpSuccess + GTPPROXYPROCEDUREGRID.NumInterLteToGnGpFail) * 100
GTP Proxy - Network Initiated Dedicated Bearer Creation Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumPGWInitDedBearerActAccept / GTPPROXYCALLPERFSTATSGRID.NumPGWInitDedBearerActAttempt) * 100
GTP Proxy - Received Delete PDP Context Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumDeletePdpAccept + GTPPROXYCALLPERFSTATSGRID.NumUEInitSecPdpDeactAccept) / (GTPPROXYCALLPERFSTATSGRID.NumDeletePdpAttempt + GTPPROXYCALLPERFSTATSGRID.NumUEInitSecPdpDeactAttempt) * 100
GTP Proxy - Transmitted Delete PDP Context Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAccept + GTPPROXYCALLPERFSTATSGRID.NumLocalCloseAttemptsAccepted) / (GTPPROXYCALLPERFSTATSGRID.NumGGSNInitSecPdpDeactAttempt + GTPPROXYCALLPERFSTATSGRID.NumLocalCloseAttempts) * 100
GTP Proxy - UE Initiated Dedicated Bearer Creation Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumUEInitDedBearerActAccept / GTPPROXYCALLPERFSTATSGRID.NumUEInitDedBearerActAttempt) * 100
GTP Proxy - UMTS PDP Context Activation Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumCreatePdpAccept + GTPPROXYCALLPERFSTATSGRID.NumUEInitSecPdpActAccept + GTPPROXYCALLPERFSTATSGRID.NumGGSNInitSecPdpActAccept) / (GTPPROXYCALLPERFSTATSGRID.NumCreatePdpAttempt + GTPPROXYCALLPERFSTATSGRID.NumUEInitSecPdpActAttempt + GTPPROXYCALLPERFSTATSGRID.NumGGSNInitSecPdpActAttempt) * 100
GTP Proxy - Update PDP Context Success Rate	(GTPPROXYCALLPERFSTATSGRID.NumSGSNInitUpdatePdpAccept + GTPPROXYCALLPERFSTATSGRID.NumGGSNInitUpdatePdpAccept) / (GTPPROXYCALLPERFSTATSGRID.NumSGSNInitUpdatePdpAttempt + GTPPROXYCALLPERFSTATSGRID.NumGGSNInitUpdatePdpAttempt) * 100
GTP Proxy – Uplink Packet Rate (pps)	GTPPROXYCALLPERFSTATSGRID.NumUplinkPackets / Interval
GTP Proxy – Uplink Throughput (Mbps) †	GTPPROXYCALLPERFSTATSGRID.NumUplinkBytes * 8 / Interval / 1000000
GTP Proxy - S5 Deactivation Failure Ratio < 0.5 %	(1 - (GTPPROXYCALLPERFSTATSGRID.NumPGWInitDedBearerDeact Accept / GTPPROXYCALLPERFSTATSGRID.NumPGWInitDedBearerDeact Attempt))* 100
GTP Proxy - S5 Modify Bearer Failure Ratio < 0.5 %	(1 - (GTPPROXYCALLPERFSTATSGRID.NumModifyBearerAccept + GTPPROXYCALLPERFSTATSGRID.NumUpdateBearerAccept) / (GTPPROXYCALLPERFSTATSGRID.NumModifyBearerAttempt + GTPPROXYCALLPERFSTATSGRID.NumUpdateBearerAttempt)) * 100

Table B-1 Derived Metrics

Metric	KPI Formula
GTP Proxy - Update Bearer Failure Ratio < 0.5 %	(1 - (GTPPROXYCALLPERFSTATSGRID.NumUpdateBearerAccept / GTPPROXYCALLPERFSTATSGRID.NumUpdateBearerAttempt))* 100
UDP Proxy KPIs:	
UDP-Proxy - Transaction Rate	delta(UDPPROXYSTATSSUMMARYCHASSIS.num_udp_proxy_summary _attempts)/ delta(time)
UDP-Proxy - Transaction Success Percentage	(UDPPROXYSTATSSUMMARYCHASSIS.num_udp_proxy_summary_ successes + UDPPROXYSTATSSUMMARYCHASSIS.num_udp_proxy_summary_ aborts) / UDPPROXYSTATSSUMMARYCHASSIS.num_udp_proxy_summary_ attempts
UDP-Proxy - Upstream Throughput	delta (UDPPROXYSTATSCONNECTIONCHASSIS.num_udp_proxy_client_ connections_bytes_received)*8 / 1,000,000 / delta (time)
UDP-Proxy - Downstream Throughput	delta (UDPPROXYSTATSCONNECTIONCHASSIS.num_udp_proxy_server_ connections_bytes_received)*8 / 1,000,000 / delta (time)
UDP-Proxy - QUIC Transaction Rate	delta(UDPPROXYSTATSQUICCHASSIS.num_udp_proxy_quic_ connections)/ delta(time)
UDP-Proxy - QUIC Upstream Throughput †	delta (UDPPROXYSTATSQUICCHASSIS.num_udp_proxy_quic_bytes_ upstream)*8 / 1,000,000 / delta (time)
UDP-Proxy - QUIC Downstream Throughput †	delta (UDPPROXYSTATSQUICCHASSIS.num_udp_proxy_quic_bytes_ downstream)*8 / 1,000,000 / delta (time)
SCEF KPIs:	
NIDD configuration success rate	(SCEFCALLPERFSTATSGRID.NumNiddConfigSuccess / (SCEFCALLPERFSTATSGRID.NumNiddConfigSuccess + SCEFCALLPERFSTATSGRID.NumniddConfigFailures - SCEFCALLPERFSTATSGRID.NumNiddConfigError)) *100
NIDD configuration update success rate	(SCEFCALLPERFSTATSGRID.NumNiddConfigUpdateSuccess / (SCEFCALLPERFSTATSGRID.NumNiddConfigUpdateSuccess + SCEFCALLPERFSTATSGRID.NumNiddConfigUpdateFailures - SCEFCALLPERFSTATSGRID.NumNiddConfigUpdateError)) *100
NIDD configuration delete success rate	(SCEFCALLPERFSTATSGRID.NumNiddConfigDeleteSuccess / (SCEFCALLPERFSTATSGRID.NumNiddConfigDeleteSuccess + SCEFCALLPERFSTATSGRID.NumNiddConfigDeleteFailures - SCEFCALLPERFSTATSGRID.NumNiddConfigDeleteError)) *100
CMR connection establishment success rate	(SCEFCALLPERFSTATSGRID.NumCmrConnEstablishSuccess / (SCEFCALLPERFSTATSGRID.NumCmrConnEstablishSuccess + SCEFCALLPERFSTATSGRID.NumCmrConnEstablishFailures - SCEFCALLPERFSTATSGRID.NumCmrConnEstablishError)) *100

Table B-1 Derived Metrics

Metric	KPI Formula
CMR connection update success rate	(SCEFCALLPERFSTATSGRID.NumCmrConnUpdateSuccess / (SCEFCALLPERFSTATSGRID.NumCmrConnUpdateSuccess + SCEFCALLPERFSTATSGRID.NumCmrConnUpdateFailures - SCEFCALLPERFSTATSGRID.NumCmrConnUpdateError)) *100
MME initiated CMR connection release success rate	(SCEFCALLPERFSTATSGRID.NumCmrConnReleaseSuccess / (SCEFCALLPERFSTATSGRID.NumCmrConnReleaseSuccess + SCEFCALLPERFSTATSGRID.NumCmrConnReleaseFailures - SCEFCALLPERFSTATSGRID.NumCmrConnReleaseError)) *100
Downlink packet success rate	(SCEFCALLPERFSTATSGRID.NumNiddMtDataReqSuccess / (SCEFCALLPERFSTATSGRID.NumNiddDlPacketsReceived - SCEFCALLPERFSTATSGRID.NumNiddDlPacketsError)) *100
Uplink packet success rate	(SCEFCALLPERFSTATSGRID.NumNiddMoDataReqSuccess / (SCEFCALLPERFSTATSGRID.NumNiddMoDataReqSuccess + SCEFCALLPERFSTATSGRID.NumNiddMoDataReqFailures - SCEFCALLPERFSTATSGRID.NumNiddMoDataReqError)) *100
Downlink packet discard rate on PSM timer expiry	(SCEFCALLPERFSTATSGRID.NumNiddMtDataPacketsDiscardedPsm / (SCEFCALLPERFSTATSGRID.NumNiddDlPacketsReceived - SCEFCALLPERFSTATSGRID.NumNiddDlPacketsError)) *100
Downlink packet buffering rate	(SCEFCALLPERFSTATSGRID.NumNiddDlPacketsBuffered / (SCEFCALLPERFSTATSGRID.NumNiddDlPacketsReceived - SCEFCALLPERFSTATSGRID.NumNiddDlPacketsError)) *100
Downlink packet received bit rate (Mbps) †	((SCEFCALLPERFSTATSGRID.NumNiddDlBytesReceived - SCEFCALLPERFSTATSGRID.NumNiddDlBytesError)*8) / 1000000 / Interval
Uplink packet received bit rate (Mbps) †	((SCEFCALLPERFSTATSGRID.NumNiddMoDataBytesReceived - SCEFCALLPERFSTATSGRID.NumNiddMoDataBytesError) *8) / 1000000 / Interval
Downlink packet received rate	(SCEFCALLPERFSTATSGRID.NumNiddDlPacketsReceived - SCEFCALLPERFSTATSGRID.NumNiddDlPacketsError) / Interval
Uplink packet received rate	(SCEFCALLPERFSTATSGRID.NumNiddMoDataReqReceived - SCEFCALLPERFSTATSGRID.NumNiddMoDataReqError) / Interval
Downlink packet sent bit rate (Mbps) †	((SCEFCALLPERFSTATSGRID.NumNiddMtDataBytesSuccess) *8) / 1000000 / Interval
Uplink packet sent bit rate (Mbps) †	((SCEFCALLPERFSTATSGRID.NumNiddMoDataBytesSuccess) *8) / 1000000 / Interval
Downlink packet sent rate	(SCEFCALLPERFSTATSGRID.NumNiddMtDataReqSuccess) / Interval
Uplink packet sent rate	(SCEFCALLPERFSTATSGRID.NumNiddMoDataPacketsSuccess) / Interval

Table B-1 Derived Metrics

Metric	KPI Formula
Monitoring event configuration success rate	(SCEFCALLPERFSTATSGRID.NumMonteEventSubsSuccess / (SCEFCALLPERFSTATSGRID.NumMonteEventSubsSuccess + SCEFCALLPERFSTATSGRID.NumMonteEventSubsFailures - SCEFCALLPERFSTATSGRID.NumMonteEventSubsError)) *100
Monitoring event configuration update success rate	(SCEFCALLPERFSTATSGRID.NumMonteEventSubsUpdateSuccess / (SCEFCALLPERFSTATSGRID.NumMonteEventSubsUpdateSuccess + SCEFCALLPERFSTATSGRID.NumMonteEventSubsUpdateFailures - SCEFCALLPERFSTATSGRID.NumMonteEventSubsUpdateError)) *100
Monitoring event configuration delete success rate	(SCEFCALLPERFSTATSGRID.NumMonteEventSubsDeleteSuccess / (SCEFCALLPERFSTATSGRID.NumMonteEventSubsDeleteSuccess + SCEFCALLPERFSTATSGRID.NumMonteEventSubsDeleteFailures - SCEFCALLPERFSTATSGRID.NumMonteEventSubsDeleteError)) *100
Monitoring event reporting success rate	(SCEFCALLPERFSTATSGRID.NumMonteEventReportSuccess / (SCEFCALLPERFSTATSGRID.NumMonteEventReportSuccess + SCEFCALLPERFSTATSGRID.NumMonteEventReportFailures - SCEFCALLPERFSTATSGRID.NumMonteEventReportError)) *100

† denotes a metric that supports changing the data unit in the dashboard graph.

Raw Metrics

Table B-2 Raw Metrics

Metric	Statistic
ABRRATELIMITINGVIDEOSEGMENTSTATSCHASSIS KPIs:	
HTTP-Proxy - ABR Video Rate Limiting Segments	Video Segment - Total
ABRRATELIMITINGVIDEOSESSIONSTATSCHASSIS KPIs:	
HTTP-Proxy - ABR Video Rate Limiting Sessions	Video Session - Total
APNCALLPERFSTATSGRIP KPIs:	
APN - Authentication Requests Timed out	NumSprAuthReqTimeout
CONTENTFILTERSTATSGRID KPIs:	
Content Filter – Requests Allowed	Num Request Allowed
Content Filter – Requests Blocked	Num Request Blocked
Content Filter – Requests Redirected	Num Request Redirected
Content Filter – Requests Terminated	Num Request Terminated
CONTENTHTTPPROXYCONNECTIONSTATSGRID KPIs:	
HTTP Proxy – Client Connections	Num Current Client Connections
CONTENTHTTPPROXYPREMPTDNSSTATSGRID KPIs:	
HTTP Proxy – Preemptive-DNS URLs Updated	Num Prempt Dns Rsp Urlrw Total
CONTENTHTTPPROXYSUMMARYSTATSCHASSIS KPIs:	
HTTP Proxy – Request Latency Average	Latency Request Avg
HTTP Proxy – Response Latency Average	Latency Response Avg
HTTP Proxy – Transaction Latency Average	Latency Avg
HTTP Proxy – Average Service Time	Client HTTP Service Time Avg
CONTENTVAONLINETRANSCODINGSUMMARYSTATSCHASSIS KPIs:	
Online Transcoding - Current	Total number of Online Transcoding current
EMSGWAPNQCIARPSTATS KPIs:	
Interval Peak Bearers	IntervalPeakBearers
Number of Current Bearers	NumCurrentBearers
Number of Downlink Drop Bytes	NumDownlinkDropBytes

Table B-2 Raw Metrics

Metric	Statistic
Number of Downlink Drop Packets	NumDownlinkDropPackets
Number of Downlink Error Loss Packets	NumDownlinkErrorLossPackets
Number of Uplink Drop Bytes	NumDownlinkDropBytes
Number of Uplink Drop Packest	NumUplinkDropPackets
Number of Uplink Error Loss Packets	NumUplinkErrorLossPackets
QCI/ARP APN - Average Number of Rules	NumCurrentRules
QCI/ARP APN - Max Number of Rules	IntervalPeakRules
EMSGWQCIARPSTATS KPIs:	
Interval Peak Bearers	IntervalPeakBearers
Number of Current Bearers	NumCurrentBearers
Number of Downlink Drop Bytes	NumDownlinkDropBytes
Number of Downlink Drop Packets	NumDownlinkDropPackets
Number of Downlink Error Loss Packets	NumDownlinkErrorLossPackets
Number of Uplink Drop Bytes	NumDownlinkDropBytes
Number of Uplink Drop Packets	NumUplinkDropPackets
Number of Uplink Error Loss Packets	NumUplinkErrorLossPackets
QCI/ARP - Average Number of Rules	NumCurrentRules
QCI/ARP - Max Number of Rules	IntervalPeakRules
GGSNCALLPERFSTATSGRID KPIs:	
Peak Session Count	Interval Peak Current Sessions
HTTPPROXYOPTIMIZATIONSAVINGS KPIs:	
ABR Rate Limiting – Total Bytes Saved	abr_rate_limiting_total_bytes_saved
ABR Rate Limiting – HLS Bytes Saved	hls-bytes-saved
ABR Rate Limiting – DASH Bytes Saved	dash-bytes-saved
ABR Rate Limiting – HDS Bytes Saved	hds-bytes-save
Minify – CSS Bytes Saved	Minify - CSS Bytes Saved
Minify – HTML Bytes Saved	Minify - HTML Bytes Saved
Minify – JavaScript Bytes Saved	Minify - Javascript Bytes Saved

Table B-2 Raw Metrics

Metric	Statistic
Offline Video Transcoding – FLV Bytes Saved	Offline Video Transcoding - FLV Bytes Saved
Offline Video Transcoding – MP4 Bytes Saved	Offline Video Transcoding - MP4 Bytes Saved
Offline Video Transcoding – WEBM Bytes Saved	Offline Video Transcoding - WEBM Bytes Saved
Online Video Transcoding – FLV Bytes Saved	Online Video Transcoding - FLV Bytes Saved
Online Video Transcoding – MP4 Bytes Saved	Online Video Transcoding - MP4 Bytes Saved
Online Video Transcoding – WEBM Bytes Saved	Online Video Transcoding - WEBM Bytes Saved
TCP-Splicing Rate-Limiting Bytes Saved	tcp_rl_bytes_saved
Video Pacing – FLV Bytes Saved	Video Pacing - FLV Bytes Saved
Video Pacing – MP4 Bytes Saved	Video Pacing - MP4 Bytes Saved
Video Pacing – Total Bytes Saved	Video Pacing - Total Bytes Saved
Video Pacing – WEBM Bytes Saved	Video Pacing - WEBM Bytes Saved
Web Image Optimization – GIF Bytes Saved	Web Image Optimization - GIF Bytes Saved
Web Image Optimization – JPEG Bytes Saved	Web Image Optimization - JPEG Bytes Saved
Web Image Optimization – PNG Bytes Saved	Web Image Optimization - PNG Bytes Saved
UDP Proxy - QUIC Video Rate Limiting Bytes Saved	quic_rl_bytes_saved
LTEMM_GENERAL KPIs:	
Attached subscribers with no PDN	MM.RegisteredActNoPdnSubNbr
Attached subscribers registered for SMS	MM.RegisteredActSmsSubNbr
LTE - Total Simultaneous Attached Subscribers (SAU)	MM.RegisteredSubNbrMax
LTESM_GENERAL KPIs:	
LTE - Peak Number of Active Dedicated Bearers	SM.MaxNbrActDedicatedBearer
LTE - Peak Number of Active Default Bearers	SM.MaxNbrActDefaultEpsBearer
CpCIot IP Bearers	SM.NbrActDefaultCpCIoTIpBearer
CpCIot Non-IP Bearers	SM.NbrActDefaultCpCIoTNonIpBearer
MME KPIs:	
UMTS - Attached Subscribers	umtsMm.general.MM.MaxNbrAttachedSub.U
UMTS - PDP Contexts	umtsSm.general.VS.SM.MaxNbrPdpContexts.U
GPRS - Attached Subscribers	gprsMm.general.MM.MaxNbrAttachedSub.G

Table B-2 Raw Metrics

Metric	Statistic
GPRS - PDP Contexts	gprsSm.general.VS.SM.MaxNbrPdpContexts.G
NODAL_S1 KPIs:	
NB-IoT capable eNB connected	S1.CurrentNbrNbIoTCapableEnb
LTE - Total eNodeB Connected	S1.PeakNbrEnb
PLATFORM_RESOURCE KPIs:	
VM - Busiest CPU Usage	CpuUtilization.BusiestCore
VM - Memory Usage	MemoryUtilization
PGWCALLPERFSTATSGRID KPIs:	
PGW – Interval Peak Active Current Sessions	Interval Peak Active Current Sessions
Peak Session Count	Interval Peak Current Sessions
PGW – Current Sessions	NumCurrentSessions
PGW – Current 4GSessions	NumRatTypeEUtranSessions
PGW – Current Co-located Sessions	NumSaegwCurrentSessions
PGW – Current Co-located 4G Sessions	NumSaegwRatTypeEUtranSessions
RADIUSPROCEDURESTATSPEER KPIs:	
Radius - Authentication Requests Timed out	numAccessReqTimeout
S1_MSG KPIs:	
NAS Transport Uplink Message Count at S1	S1.IncUlNasTransport
NAS Transport Downlink Message Count at S1	S1.OutDlNasTransport
SGWCALLPERFSTATSGRID KPIs:	
Peak Session Count	IntervalPeakCurrentSessions
SGW – Current Sessions	NumPdnConnections
SGW – Current 4GSessions	NumPdnConnectionsEutran
SGW – Current Co-located Sessions	NumSaegwPdnConnections
SGW – Current Co-located 4G Sessions	NumSaegwPdnConnectionsEutran

Table B-2 Raw Metrics

Metric	Statistic
SLOT_STATS KPIs:	
System - CPU Utilization	CPU Utilization (%), by individual CPU
System - Memory Utilization	Memory Utilization (MB), by individual CPU
SSF KPIs:	
SSF - DNS total-query-attempt	SSF_DNS_DNS.total-query-attempt
SSF - RESOURCE cpu-utilization-busiest-core	SSF_PLATFORM_RESOURCE.cpu-utilization-busiest-core
SSF - RESOURCE memory-utilization	SSF_PLATFORM_RESOURCE.memory -utilization
SSF - FILESYSTEM utilization	SSF_PLATFORM_FILESYSTEM.utilization
TCPMEASUREMENTSSERVERSIDESTATSCHASSIS KPIs:	
TCP Server Side Measurement - Average Round Trip Time	avg_rtt
TCP Server Side Measurement - Number of Downstream Packets Retransmitted	num_retrans_in
TCP Server Side Measurement - Number of Downstream Packets Out of Order	num_ooo_in
TCPMEASUREMENTSSUMMARYSTATSCHASSIS KPIs:	
TCP Client-side Measurement - Average Available Downstream Connection Throughput (Kbps) †	avg_throughput_dl
TCP Client-side Measurement - Average Downstream CWND (Congestion Window)	avg_cwnd_dl
TCP Client-side Measurement - Average Downstream MSS (Max Segment	avg_mss_dl
TCP Client-side Measurement - Average Round Trip Time	avg_rtt
TCP Client-side Measurement - Downstream Segments Retransmitted	num_total_segments_retrans_dl
TCPSPLICINGSTATSCONNECTIONCHASSIS KPIs:	
TCP-Splicing - Transaction Latency Average	tcp_service_duration_avg
TCP-Splicing - Client Connections	num_total_client_connections
TCP-Splicing - Transaction Failure	num_total_connection_failures
TCP-Splicing Client Connections	num_tcp_splicing_client_connections_total

Table B-2 Raw Metrics

Metric	Statistic
TCPSPLICINGRATELIMITINGSTATSCHASSIS KPIs:	
TCP-Splicing - Rate-Limited Bytes	Total number of rate limiting bytes
TCP-Splicing - Rate-Limiting Disabled	Total number of rate limiting disabled
TCP-Splicing - Rate-Limiting Opted Out	Total number of rate limiting summary opted out by subscriber
TCP-Splicing - Rate-Limited Connections	Rate Limiting Summary - Successes
TCPSPLICINGSTATSSUMMARYCHASSIS KPIs:	
TCP-Splicing Transaction Duration Average	num_tcp_service_duration_avg
UDPPROXYRATELIMITINGSTATSCHASSIS KPIs:	
UDP-Proxy - QUIC Rate Limited Connections	num_udp_proxy_rate_limiting_bytes
UDP-Proxy - QUIC Rate Limited Bytes	num_udp_proxy_rate_limiting_summary_ successes
WAGAPNCALLPERFSTATSGRID KPIs:	
WAG APN - Current Number of Sessions in Captive(walled - garden) State	NumCaptiveCurrentSessions
WAG APN - Current Number of Sessions in Authenticated State	NumOpenCurrentSessions
WAGCALLPERFSTATSGRID KPIs:	
WAG - Current Number of Sessions in Captive(walled - garden) State	NumCaptiveCurrentSessions
WAG - Current Number of Sessions in Authenticated State	NumOpenCurrentSessions

Index

A

AAA interface group 10-265
ACL List construct 10-142
ACL service 10-382
Acuitas
  CUPS Manager 3-2
  description xlvii
  LDAP authentication and authorization A-6
  logging in 1-5
  logging out 1-13
  login failure 1-7
  NE configuration backup and restore 8-12
  Network configuration backup 8-9
  network element logs, viewing 11-1
  RADIUS authentication and authorization A-13
  TACACS+ authentication, authorization, and accounting A-2
  trap format A-25
  viewing product version number 1-10
  VNF Manager and Provisioning API 6-123
Advice of charge construct 9-66, 10-136, 10-144
Affirmed Open Workflow 9-1
Alarm Triggered Configuration
  about 3-61
  adding 3-61
  modifying 3-62
  use case 3-64
Alarms
  acknowledging 4-16
  assigning owner 4-16
  clearing 4-17
  configuring purge settings 4-29
  configuring SNMP alarm forwarding 4-30
  deleting 4-19
  detail A-18
  e-mail notification 4-34
  exporting 4-26
  filtering 4-12
  forwarding 4-20
  generating alarm report 4-28
  hiding cleared 4-18
  host system alarms, viewing 1-21
  identifying objects with 4-2
  printing 4-27
  purging cleared 4-18
  severity color settings, configuring 8-9
  showing cleared 4-18
  streaming to syslog 4-21
  view/edit details 4-14
  viewing 1-21, 4-8
  viewing statistics 4-23
Aoc hardware ID format construct 9-69, 10-146
APN Mapping List 9-71
Application rule group construct 9-72, 10-147
Associating a threshold with a PM collection task 5-31
Audit Trail 2-16
  about 3-76
  exporting 3-77
  exporting device audit trail 11-14
  exporting topology audit trail 2-17
  viewing 3-76, 7-39
  viewing device audit trail 11-13
  viewing topology audit trail 2-16

B

Back up configuration data for all NEs 8-9
Backup and restore NE configuration 8-12
Billing plan service 9-187, 10-387

C

Category

adding 9-350
modifying or deleting 9-351
viewing file contents 9-351
Charging instance service 9-188, 10-388
Cluster
nodes 10-21
objects 10-8
statistics 10-27
summary 10-27
TND peer statisitcs 10-28
TND total statisitcs 10-28
Cluster reports
about 6-99
Code mapping lists construct 10-177
Color settings for alarm severity 8-9
Column properties, setting 1-37
Configuration application 3-1
Configuration Navigator
AAA interface group 10-139, 10-265
about 10-1
ACL list 10-142
ACL service 10-382
advice of charge 10-144
advice of charge construct 10-136
aoc hardware ID format 10-146
APN mapping list 10-556
application rule group 10-147
authorization service 10-248
billing plan service 10-387
black list 10-407
charging instance service 10-388
cluster 10-8
cluster statistics 10-27
cluster summary 10-27
cluster TND peer statisitcs 10-28
cluster TND total statisitcs 10-28
code mapping lists 10-177
content cache service 10-390
content database import history 10-406
content database summary 10-407
content filter service 10-394
content insertion 10-178
control profile 10-557
CRBN profile 10-420
data path 10-29
data profile 10-565
data profile reselection trigger template 10-568
data record template 10-137, 10-181
data records 10-30
deep packet inspection construct 10-182
device database 10-183
DHCP local service profile 10-186
DHCP mapping template construct 10-187
DHCP service profile 10-195
Diameter Result Code Policy List 10-192
Diffserv profile 10-196
DNS IP flow 10-423
DNS policy 10-424
DNS proxy cache display 10-427
DNS proxy cache statistics 10-428
DNS proxy domain clean time 10-429
DNS proxy instance 10-427
DNS proxy module statistics 10-428
DNS proxy service 10-422
DNS reverse cache 10-426
DNS tunnel blocked domain 10-430
DNS tunnel detection profile 10-430
domain rule group 10-200
EDR flow network stats profile 10-201
EDR interface profile 10-202
EDR server profile 10-211
EDR session data stats profile 10-212
encryption profile 10-213, 10-447, 10-492
entering configuration values 10-6
event log configuration 10-55
event trigger template 10-215, 10-223
fair bandwidth usage service 10-431
fault management 10-31
file download profile 10-138, 10-217
filter database size 10-406
filter hash list 10-218
flow authorization interface 10-251
flow idle timeout filter 10-220
Flow idle timeout profile 10-32
gateway session learner 10-253
geo redundancy server 10-221
Geographic Redundancy Group 10-33
health check 10-432
health check profile 10-224
host list 10-225
HTTP Header Enrichment 10-138, 10-226
HTTP proxy instance 10-442
HTTP proxy IP flow 10-440
HTTP proxy service 10-435
HTTP request policy 10-436, 10-480
HTTP response policy 10-438, 10-482
HTTP rule group construct 10-139, 10-234
HTTP server 10-237, 10-470
HTTP server list 10-237
HTTP URL rewrite 10-139, 10-239
image management 10-36
image management card status 10-44
image management release modifier status 10-45
image management status 10-45
IMSI range 10-241
IMSI range list 10-242
infrastructure 10-47
infrastructure dynamic scaling 10-47
infrastructure EDR statistics 10-48
infrastructure export IP 10-48
infrastructure file management 10-49
infrastructure TOS Cgroup OOM 10-61
IP List 10-326
IP protocols 10-69
IPMS intreface 10-262
LDAP 10-327

Loopback IP list 10-333
metering service 10-475
MME 10-101
Multi protocol proxy instance 10-487
Multi protocol proxy IP flow 10-484
Multi protocol proxy service 10-479
Multimedia Messaging Service 10-334
neighbor discovery profile 10-109
network context 10-104
network profile construct 10-341
NTP server configuration 10-60
offline charging 10-139, 10-294
online charging 10-139, 10-304
packet filter construct 10-140, 10-342
paging and filtering object instances 10-4
PCRF charging 10-139, 10-314
performance statistics management 10-110
personalities 10-10
pki 10-111
PLMNID List construct 10-344
port NBR service 10-322
protocol application rule group 9-309, 10-345
protocol application rule group construct 10-140
QoS flow service 10-514
QoS policy 10-516
Quality of Service construct 10-141, 10-350
RADIUS content Server 10-321
Radius mapping template construct 10-351
rating group service 10-383
realm List construct 10-355
refreshing tree 10-4
Rx interface 10-323
S6b interface 10-323
SCTP profile construct 10-356
security 10-117
service constructs 10-136
service rule 10-409
service rule construct 10-141, 10-357
services 10-378
Session Rule Group 9-163, 10-361
Short Message Service 10-363
SMTP proxy 9-322
static category source 10-403
static DNS map 10-365
steering flow 10-521
steering policy 10-523
subscriber analyzer 10-569
subscriber firewall 10-524
subscriber firewall flow 10-524
subscriber firewall policy 10-526
subscriber group construct 10-366
system 10-543
system log configuration 10-59
TAM 10-544
TCP optimization profile construct 10-141, 10-367
time of day rule group construct 10-141, 10-369
time zone 10-68
TLS rule group construct 10-370
TLS termination policy construct 10-371
tree display 10-2
UA Profile construct 10-372
URL list 10-141, 10-373
user access 10-546
video adaptation service 10-528
view MME real time statisics 10-101
viewing alarms 10-7
virtual node 10-21
vTap 10-551
WAP gateway instance 10-539
WAP gateway IP flow 9-345, 10-540
white list 10-409
workflow 10-555
workflow data stats construct 10-376
zone 10-574
Configuration template
about 3-44
adding 3-44
copying 3-46
deleting 3-49
exporting 3-50
importing 3-51
modifying 3-47
setting obsolete 3-48
viewing 3-45
Configuring SNMP alarm forwarding 4-30
Content cache service 9-190, 10-390
Content Database Import History 10-406
Content Database Summary 10-407
Content filter service 9-193, 10-394
Content insertion construct 10-178
Control list configuration, definitions of terms 9-347
Conventions xciv
CRBN profile 10-420
CSV statistics recovery
about 5-38
deleting schedule 5-43
launching 5-38
viewing schedule details 5-40
viewing status 5-41

D

Data record template construct 10-137, 10-181
Database administration
about 8-2
adding backup 8-2
deleting backup 8-5
restoring from backup 8-6
scheduling backup 8-3
viewing backup details 8-3
viewing scheduled backup 8-4
Database backup
adding 8-2

deleting 8-5
restoring 8-6
scheduling 8-3
viewing 8-4
viewing details 8-3
Deep packet inspection construct 10-182
Device database construct 10-183
Device Gateway application, accessing 11-23
DHCP local server profile construct 9-105
DHCP local service profile construct 10-186
DHCP mapping template construct 10-187
DHCP service profile construct 9-106, 10-195
Diameter Result Code Policy List construct 10-192
Diffserv profile construct 10-196
Disaster Recovery
for Geographic Redundancy group 3-107
DNS IP flow 10-423
DNS policy 10-424
DNS proxy cache display 10-427
DNS proxy cache statistics 10-428
DNS proxy domain clean time 10-429
DNS proxy instance 10-427
DNS proxy module statistics 10-428
DNS proxy service 10-422
DNS reverse cache 10-426
DNS tunnel blocked domain 10-430
DNS tunnel detection profile 10-430
Domain rule group construct 9-112, 10-200

E

EDR flow network stats profile construct 10-201
EDR interface profile construct 10-202
EDR server profile construct 9-114, 10-211
EDR session data stats profile construct 10-212
Element details, viewing 1-20
E-mail notification, alarms 4-34
Encryption construct 9-115
Encryption profile 9-244, 9-285, 10-447, 10-492
Encryption profile construct 10-213
Evaluating workflow 9-40
Event logs
exporting 4-39
printing 4-38
purging 4-40
viewing 1-21, 4-36
Viewing details 4-37
Event Trigger Template 10-215, 10-223
Events
about 4-36
Export reports
configuring 5-21
configuring purge interval 5-23
triggering on demand 5-22
Exporting
alarms 4-26
audit trail 3-77
configuration template 3-50
device audit trail 11-14
event logs 4-39
historical statistics 5-17
KPI data 5-59
records 1-38
security groups 7-8
topology audit trail 2-17
user tasks scheduler 5-36
users 7-37

F

Fair bandwidth usage service 9-229, 10-431
Fault application 4-1
File download profile construct 9-116, 10-138, 10-217
File Server
about 3-78
adding 3-78
deleting 3-63, 3-80
modifying 3-62, 3-79
viewing 3-79
Filter database size 10-406
Filter database size construct 9-118
Filter hash list construct 10-218
Filters
applying 1-35
creating 1-33
deleting 1-36
modifying 1-35
Quick Filters 1-36
Flow idle timeout filter construct 10-220

G

Geo redundancy server construct 10-221
Geographic Redundancy
adding groups 3-85
comparing configurations 3-96
configuration for disaster recovery 3-107
deleting groups 3-105
modifying groups 3-91
overview 3-81
replicating configuration 3-98
switching over 3-101
troubleshooting problems 3-109
viewing chronological switchover log of Geo Redundancy Groups 3-104
viewing groups 3-84
viewing recent activities 3-102
Groups

about 2-2
adding 2-2
deleting 2-3
modifying 2-3

H

Header Enrichment construct 9-120, 10-138, 10-226
Health check 10-432
Health Check Profile 10-224
Help, using 1-11
Historical statistics
exporting 5-17
viewing 5-9
Host list construct 9-119, 10-225
HPE HSS EMS, accessing 11-22
HTTP Filter file management
adding category 9-350
adding URL list 9-348
control list configuration 9-347
modifying or deleting category 9-351
modifying or deleting URL list 9-349
viewing file contents 9-349, 9-351
viewing file list 9-352
HTTP proxy instance 9-245, 10-442
HTTP proxy IP flow 9-242, 10-440
HTTP proxy service 10-435
HTTP request policy 9-238, 9-279, 10-436, 10-480
HTTP response policy 9-241, 9-282, 10-438, 10-482
HTTP rule group construct 9-128, 10-139, 10-234
HTTP server 10-470
HTTP server construct 10-237
HTTP server list construct 10-237
HTTP URL rewrite construct 9-132, 10-139, 10-239

I

Icons, defined 1-22
Image management
card status 10-44
objects 10-36
release modifier status 10-45
status 10-45
Importing
configuration template 3-51
IMSI range construct 10-241
IMSI range list construct 10-242
Infrastructure
dynamic scaling 10-47
EDR statistics 10-48
event log configuration 10-55
Export IP 10-48
file management 10-49
NTP server configuration 10-60
objects 10-47
system log configuration 10-59
TOS Cgroup OOM 10-61
IP List 10-326
IP protocols 10-69

K

Key Performance Indicators
configuring dashboard 5-47
exporting data 5-59
metrics B-1
viewing 1-21, 5-44

L

LDAP authentication and authorization support for Acuitas A-6
LDAP construct 9-138, 10-327
Logging into Acuitas 1-5
Logging out of Acuitas 1-13
Login failure 1-7
Logs,viewing 11-1
Loopback IP list 10-333

M

Mail server, configuring 2-21
Message prompt on locked user accounts, configuring 2-23
Metering service 9-271, 10-475
MME 10-101
multi protocol proxy instance 9-286
multi protocol proxy IP flow 9-283, 10-484
multi protocol proxy service 10-479
Multimedia Messaging Service 10-334
Multimedia Messaging Service Center construct 9-146
Multiple records, navigating 1-38
mutil protocol instance 10-487

N

Navigating
through records 1-38
tree display 1-14
NE configuration backup and restore 8-12
adding user triggered backup 8-12
deleting backup 8-15

disabling schedule 8-19
downloading backup file 8-14
enabling schedule 8-19
exporting schedule 8-21
modifying schedued backup 8-18
purging backup files 8-14
Quick Start schedule 8-20
restoring backup file 8-15
scheduling backup 8-16
viewing backup details 8-13
viewing scheduled backup details 8-17
NE configuration backup and restore schedule
deleting schedule 8-22
Network configuration backup 8-9
Network Context 10-104
Network element
adding 2-4
adding remarks 2-14
deleting 2-14
managing 2-15
managing fault management state 4-4
modifying 2-8
unmanaging 2-15
viewing 2-8
Network filter construct 10-341
Network view 1-15
Node Configuration Manager
comparing configuration files 3-119
deleting configuration files 3-120
downloading configuration files 3-118
overview 3-116
saving configuration files 3-117
viewing configuration files 3-116

O

Offline charging 10-139, 10-294
Online charging 10-139, 10-304
Online Help, using 1-11
Outage reports
viewing 5-21

P

Packet filter construct 9-153, 10-140, 10-342
Paging and filtering instances in the Configuration Navigator tree 10-4
Password
changing 1-32, 7-38
PCRF charging 10-139, 10-314
Performance Management
application 5-1
disabling collections 5-3
enabling collections 5-3
exported data A-56
Performance reports
about 5-4
Performance statistics management 10-110
Personalities 10-10
PLMNID list construct 10-344
PM Dashboard
configuring dashboard 5-47
exporting data 5-59
viewing 5-44
Port NBR service 10-322
Printing
alarms 4-27
event logs 4-38
records 1-39
Product version number, viewing 1-10
Protocal application rule group construct 9-309, 10-345
Protocol application rule group construct 10-140

Q

QoS construct 9-155
QoS flow service 9-315, 10-514
QoS policy 9-318, 10-516
Quality of Service construct 10-141, 10-350

R

RADIUS authentication and authorization support for Acuitas A-13
RADIUS content server 10-321
Radius mapping template construct 10-351
Rate limiting subscriber group file management 11-15
Rating group service 9-183, 10-383
Real time statistics
viewing 5-18
Realm list construct 10-355
Records
exporting 1-38
printing 1-39
Refreshing Configuration Navigator tree 10-4
Refreshing screen 1-39
Remarks, adding 2-14

S

Screen background color, changing 1-31
Screen, refreshing 1-39
SCTP profile construct 9-157, 10-356
Security 10-117

Security application 7-1
Security groups
  about 7-2
  adding 7-4
  associating resources 7-5
  copying 7-7
  deleting 7-10
  exporting 7-8
  modifying 7-9
  viewing 7-6
Service flows 9-26
Service functions 9-59
Service instance 9-180
Service rule construct 9-158, 10-141, 10-357
Session Rule Group Service construct 9-163, 10-361
Short Message Service construct 9-165, 10-363
Siemens SPCRF EMS, accessing 11-21
SMTP proxy 9-322
SNMP settings, configuring 2-22
Software release
  about 3-22
  adding 3-22
  deleting 3-26
  modifying 3-25
  setting obsolete 3-26
  viewing 3-24
Software rollback
  about 3-40
  performing 3-40
  viewing 3-41
  viewing status 3-42
Software schedule
  about 3-32
  adding 3-32
  copying 3-36
  deleting 3-39
  disabling 3-37
  enabling 3-37
  modifying 3-38
  Quick Start 3-38
  viewing 3-34
Software schedule subtask
  viewing status 3-35
Sorting column data 1-37
Static DNS map 9-168
Static DNS map construct 10-365
Statistic data type
  configuring at the global level 5-4
Statistic unit conversion
  configuring at the global level 5-4
Steering flow 9-324, 10-521
Steering policy 9-325, 10-523
Subscriber firewall 10-524
Subscriber firewall flow 9-327, 10-524
Subscriber firewall policy 9-329, 10-526
Subscriber group construct 10-366
Subscriber group file
  viewing file contents 11-18
Subscriber group file management
  adding subscriber groups 11-16
  modifying or deleting subscriber groups 11-17
  viewing file contents 11-18
  viewing file list 11-18
Subscriber groups
  adding 11-16
  modifying or deleting 11-17
Synchronize/Compare workflow 9-58
System availability, viewing 1-21

T

Tabs 1-15
TACACS+ authentication, authorization, and accounting support for Acuitas A-2
TCP optimization profile construct 9-169, 10-141, 10-367
Technical Assistance Center xcv
Template schedule
  about 3-52
  adding 3-52
  copying 3-55
  deleting 3-60
  disabling 3-58
  enabling 3-58
  modifying 3-59
  Quick Start 3-59
  viewing 3-56
  viewing execution status 3-57
Theme, changing 1-31
Threshold
  about 5-24
  adding 5-24
  modifying 5-27
  viewing 5-26
Threshold, associating with a PM collection task 5-31
Time of day rule group construct 9-176, 10-141, 10-369
Time zone 10-68
TLS rule group construct 10-370
TLS termination policy construct 10-371
Tools application 8-1
Topology application 2-1
Tracing workflow 9-51
Traps
  format A-25
  forwarded trap mappings A-38
  third-party traps A-26
Tree display 1-14, 10-2
Troubleshooting problems with Geographic Redundancy groups 3-109

U

UA Profile construct 9-176, 10-372
URL list
  adding 9-348
  modifying or deleting 9-349
  viewing file contents 9-349
URL list construct 9-178, 10-141, 10-373
URL list files
  Auto-Push 3-123
  comparing 3-128
  editing 3-125
  marking as reviewed 3-128
  overwriting 3-127
  viewing 3-122
URL list maintenance
  about 3-121
URL list schedule
  about 3-130
  adding 3-130
  copying 3-133
  deleting 3-136
  disabling 3-134
  enabling 3-134
  modifying 3-135
  Quick Start 3-134
  viewing 3-131
URL list schedule subtask
  viewing status 3-132
User Tasks Scheduler
  about 5-30
  disabling 5-30
  enabling 5-30
  exporting 5-36
  modifying 5-31
  Quick Start 5-36
  viewing 5-30
User Tasks Template
  about 5-28
  modifying 5-28
  viewing 5-28
Users
  adding 7-33
  changing password 7-38
  deleting 7-46
  exporting 7-37
  managing sessions 7-45
  modifying 7-36
  unlocking 7-46
  viewing 7-34

V

Validating workflow 9-36
Video adaptation service 9-330, 10-528
Viewing MME real time statistics 10-101
VNF Manager and Provisioning API 6-123
VNF Manager application 6-1

W

WAP Gateway instance 9-344, 10-539
WAP Gateway IP flow 9-345, 10-540
Workflow
  about 9-1
  advice of charge construct 9-66
  Aoc hardware ID format construct 9-69
  APN Mapping List 10-556
  APN mapping list 9-71
  application rule group construct 9-72
  billing plan service 9-187
  build a workflow method 9-60
  build out functions method 9-59
  charging instance service 9-188
  configuration methods 9-2
  configuring control profile 9-16
  configuring data profile reselection trigger template 9-23
  configuring service flows 9-26
  configuring service functions 9-59
  configuring services 9-180
  configuring workflow 9-15
  content cache service 9-190
  content filter service 9-193
  data stats construct 10-376
  definition of terms 9-2
  DHCP local server profile 9-105
  DHCP service profile 9-106
  domain rule group construct 9-112
  EDR server profile construct 9-114
  encryption profile 9-244, 9-285
  encryption profile construct 9-115
  fair bandwidth usage service 9-229
  file download profile construct 9-116
  filter database size construct 9-118
  host list 9-119
  HTTP header enrichment 9-120
  HTTP proxy instance 9-245
  HTTP proxy IP flow 9-242
  HTTP request policy 9-238, 9-279
  HTTP response policy 9-241, 9-282
  HTTP rule group construct 9-128
  HTTP URL rewrite construct 9-132
  in Configuration Navigator 10-555
  LDAP construct 9-138
  metering service 9-271
  Multi protocol proxy instance 9-286
  Multi protocol proxy IP flow 9-283
  Multimedia Messaging Service Center construct 9-146

overview 9-2
packet filter construct 9-153
QoS construct 9-155
QoS flow service 9-315
QoS policy 9-318
rating group service 9-183
SCTP profile construct 9-157
server connections 9-248, 9-289
service evaluation 9-40
service flow switching 9-10
service rule construct 9-158
Short Message Service construct 9-165
Static DNS map 9-168
steering 9-324
steering policy 9-325
subscriber analyzer 10-569
subscriber firewall flow 9-327
subscriber firewall policy 9-329
synchronize/compare 9-58
TCP optimization profile construct 9-169
time of day rule group construct 9-176
tracing 9-51
UA profile construct 9-176
URL list construct 9-178
validating 9-36
video adaptation service 9-330
WAP gateway instance 9-344
workflow control profile 10-557
workflow data profile 10-565
workflow data profile reselection trigger template 10-568