

EdgeView Service Control Center (SCC)

User Guide

Release 14.1.0

U.S. Headquarters:

Edgewater Networks, Inc.
5225 Hellyer Ave. #100
San Jose, California 95138

Phone: 408.351.7200
Fax: 408.727.6430

edgewaternetworks.com

© 2016, Edgewater Networks, Inc.

Edgewater Networks, All Rights Reserved.

Trademarks

EDGEWATER NETWORKS EDGEMARC®, EDGEPROTECT®, and EDGECONNECT® are registered trademarks of Edgewater Networks, Inc. EDGEWATER NETWORKS™ and EDGEVIEW™ are trademarks of Edgewater Networks, Inc. Any other trademarks appearing in this manual are owned by their respective companies.

Copyright

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Edgewater Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement of the implied warranties of merchantability or fitness for a particular purpose.

Export Notice

You (Purchaser) acknowledge that these products are subject to the U.S. Export Administration Regulations (the “EAR”) and that you will comply with the EAR. You are not located in Cuba, Iran, North Korea, Sudan, and Syria. You will not export or re-export this product, directly or indirectly, to: (1) any countries that are subject to US export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan, and Syria); (2) any end user who you know or have reason to know will utilize them in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, and sounding rockets, or unmanned air vehicle systems; or (3) any end user who has been prohibited from participating in US export transactions by any federal agency of the US government. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use these products.

Licensing

Use of this product is subject to Edgewater Networks Software License Agreement.

Portions of this product include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE.

See the www.edgewaternetworks.com/licensing for more information regarding licenses.

Warranty

Product warranty does not apply to damage caused by lightning, power surges, or wrong voltage usage.

Typographical Errors

This publication could include technical inaccuracies or typographical errors, for which Edgewater Networks never can or shall be held liable. Changes are made periodically to the information herein; these changes will be incorporated in new releases of this publication. Edgewater Networks may make improvements or changes in the product or products described in this publication at any time, without prior notice.

Document Release Date

7/26/16

Contents

Preface

About this Guide 1
Typographic Conventions 2
Edgewater Networks Knowledgebase 3
Contact and Support Information 3

1 EdgeView Overview and Features

EdgeView Overview 5
EdgeMarc and Node Management 7
VoIP Analysis and Troubleshooting 7
Status and Notifications 7
Plug & Dial 7
EdgeView Reports 8
VoIP Traffic Capture Signaling and RTP Media 9
On-Demand Signaling Ladder 10
Integrated VoIP Test Agent 10
EdgeView Graphical User Interface 11
Context-Sensitive Help 13

2 Getting Started

Starting EdgeView 15
EdgeView Security Change Notification Page 17
Installing the EdgeView Product License and Support License Keys 17
Managing Passwords in EdgeView 18
Changing Your Password and User Profile 18
EdgeView Quick Tour 19
Icon Bar 20
Device Tree 22
Menu Bar 23

3 Basic EdgeMarc Management

Adding an EdgeMarc 25
Adding an EdgeMarc via Auto-Discovery 26
Configuring Auto-Discovery in EdgeView 26
Configuring Auto-Discovery Settings on the EdgeMarc 27
Manually Adding an EdgeMarc 29
Testing EdgeMarc Connectivity 33
Changing Polling and Discovery Settings 33
Setting the Matching Criteria for Auto-Discovery 34
Editing EdgeMarc Attributes 35
Adding an Additional IP Address 37
Deleting an EdgeMarc from EdgeView 37

© 2016 Edgewater Networks. All Rights Reserved.

Deleting Multiple EdgeMarcs 38
Launching the EdgeMarc GUI from EdgeView 38
Creating a Collection of EdgeMarcs 39
Most EdgeMarc node operations and node configuration can be performed on an EdgeMarc collection. By creating an EdgeMarc collection, a single task can be performed on multiple EdgeMarcs rather than individually. 39
Manually Selecting EdgeMarcs to Include in a Collection 39
Using Rule Filters to Add EdgeMarcs to a Collection 41
Creating an EdgeMarc Collection in an XML File 42
Uploading an EdgeMarc Collection XML File to EdgeView 43
Rebooting an EdgeMarc 45
Changing the EdgeMarc Password. 46
Displaying Decrypted Passwords in the EdgeView GUI 48
Marking a Device for RMA 49
Pre-Provisioning an EdgeMarc 49
Backing Up and Restoring an EdgeMarc Configuration 51
Backing Up an EdgeMarc (On-Demand) 52
Backing Up an EdgeMarc Configuration (Scheduled) 53
Scheduling a Daily Backup of All EdgeMarcs (Tenant or Group Level). 53
Backing Up an EdgeMarc Configuration (Group Level). 56
Managing EdgeMarc Backup Files 57
Moving a Backup File to the Archived Backup File List 58
Deleting an Archived Backup File. 58
Comparing EdgeView Configuration Backup Files 58
Restoring the EdgeMarc Configuration 59
Upgrading the EdgeMarc VOS Firmware 60
Upgrading the Firmware for an EdgeMarc. 60
Upgrading the Firmware for an EdgeMarc Group 64
Automatically Upgrading the Firmware for an EdgeMarc Group 66
Limiting the Time of Day for EdgeMarc Upgrades 68
Debugging EdgeMarc Upgrade 71
Managing License Keys 72
Pushing a License Key to an EdgeMarc 72
Pushing a License Key to a Group of EdgeMarcs 76
Creating a CSV File for the License Key 76
Uploading and Pushing the License Key CSV File. 77

4 Basic Group, Node, and User Management

Understanding the EdgeView Hierarchy 81
Tenant and Group Attributes 82
Limiting/Enabling User Access to EdgeView 82
Device Tree Hierarchy 82
Managing Tenants 84
Adding a Tenant. 84
Adding Tenant Attributes 85
Editing Global Tenant Attributes 89
Deleting a Tenant. 92
Managing Groups 93

© 2016 Edgewater Networks. All Rights Reserved.

Adding a Group . . . 93
Assigning Group Attributes . . . 95
Deleting a Group . . . 98
Assigning a Group to a Different Parent Group . . . 98
Moving an EdgeMarc from the Unassigned Group . . . 99
Moving Multiple EdgeMarcs to a Different Group . . . 100
Managing Node Settings . . . 101
Adding an EdgeMarc . . . 102
Adding a Third-Party Node . . . 102
Adding an SNMP-based Node . . . 104
Editing Node Settings . . . 105
Deleting a Node . . . 106
Moving a Node Between Groups . . . 106
Managing Users . . . 107
Adding a User . . . 108
Deleting a User . . . 110
Editing a User . . . 110
Assigning Specific Rights to a User . . . 111
Verifying User Access to EdgeView . . . 116
Managing Passwords . . . 117
Enforcing Strict Passwords . . . 118

5 Managing EdgeView System Settings

Configuring EdgeView System Settings . . . 121
Configuring SNMP Network Management Settings . . . 123
Default SNMP Settings in EdgeView . . . 123
Setting Warning Thresholds . . . 124
Warning on RX Errors . . . 124
Warning on TX Errors . . . 124
Warning on MOS Below . . . 124
Configuring Polling and Discovery Settings . . . 125
SSH Polling with EdgeView . . . 126
SNMP Polling with EdgeView . . . 126
Understanding Polling on EdgeView . . . 126
Configuring the EdgeMarc for SNMP Polling . . . 127
Changing the Node Polling Interval . . . 130
Enabling/Disabling Auto-Discovery . . . 130
Specifying Matching Criteria for Auto-Discovery . . . 130
Enabling Reverse DNS Lookup Settings . . . 131
Setting the EdgeView GUI Timeout Value . . . 132
Customizing the Device Tree Display . . . 132
Configuring Password Settings . . . 133
Enforcing Strict Passwords . . . 133
Showing Decrypted Passwords . . . 134
Forcing Users to Change Their Password . . . 134
Setting Up HTTPS for EdgeView . . . 135
Capturing Phone MOS Scores . . . 137
Setting Up and Scheduling Daily System Health Checks . . . 138
Setting a Message of the Day . . . 139
Configuring EdgeView System Security Settings . . . 140

© 2016 Edgewater Networks. All Rights Reserved.

Configuring a Blacklist . . . 142
Configuring a Whitelist . . . 143
Enabling Anonymous FTP . . . 145
EdgeView Licenses . . . 145
Starting an SSH Session in EdgeView via CLI . . . 146
Using Maintenance Mode . . . 146
Using EdgeView Administrator Tools . . . 148
EdgeView Database Administration Tools . . . 149
Testing and Saving Database Configuration Settings . . . 150
Checking the Status of EdgeView Database Tables . . . 151
Managing EdgeView Historical Data with mysql Partitioning . . . 151
Backing Up the EdgeView Database . . . 152
Deleting a Scheduled Backup . . . 155
Restoring the Database . . . 156
Deleting a Database Backup File from the EdgeView Database . . . 157
EdgeView Signal Capture File Cleanup Configurable Storage . . . 157
SCP Support for EdgeView Database Backup and Restore . . . 158
EdgeView Disk Cleanup Tool . . . 159
Viewing EdgeView Log Files . . . 160
Viewing EdgeView Process and System Information . . . 160
Viewing EdgeView Tasks . . . 161
Setting Up EdgeView Hard Disk Automated Cleanup . . . 162
Performing a Password Security Scan . . . 163
Viewing Active Troubleshooting Jobs . . . 164
Viewing the Current Software Version and Patches Installed on EdgeView . . . 165

6 Status and Notifications

Viewing Status in EdgeView . . . 167
Viewing General EdgeMarc Status . . . 168
Storing and Graphing Memory Usage on the EdgeMarc . . . 169
Viewing the Phone Numbers Managed by EdgeView . . . 173
Viewing the Endpoint Client List Snapshot . . . 173
Manually Initiating a Call . . . 174
Viewing Node Status with EdgeView . . . 174
Customizing the Status Table . . . 175
Viewing Global EdgeMarc Status . . . 176
Secondary State Warnings . . . 176
Using the Search Function . . . 176
Viewing EdgeMarc Node Status . . . 177
Changing the Number of EdgeMarcs Displayed . . . 177
Specifying a Refresh Interval . . . 177
Viewing Group Status . . . 177
Viewing the Status of Other Nodes . . . 178
Viewing IP Phone Status . . . 179
Viewing EdgeConnect Status . . . 179
Sending UP/DOWN Status Notifications at the Tenant, Group and Node Level 180
Setting Node UP/DOWN Status Notifications at the Tenant Level . . . 181
Setting Node UP/DOWN Status Notifications at the Group Level . . . 181
Setting Node UP/DOWN Status Notifications for an EdgeMarc Node . . . 182
Viewing Inventory . . . 183

© 2016 Edgewater Networks. All Rights Reserved.

Viewing CSV Inventory Output . . . 184
Configuring Email Status Notifications . . . 185
Configuring General System Notifications . . . 187
Sending MOS Alert Notifications . . . 189
Adding/Editing a MOS Alert . . . 190
Deleting a MOS Alert . . . 192
Sending MOS Alerts on CAC Exceeded Events . . . 192
Sending MOS Alerts on Survivability Changes . . . 192
Sending SNMP Traps for MOS Alerts . . . 192
Enabling Live MOS Capture . . . 193
Testing MOS Notification Alert Settings . . . 193
Creating a Polling Notification Profile . . . 194
Editing a Polling Notification Profile . . . 197
Deleting a Polling Notification . . . 197
Sending SNMP Trap Notifications . . . 198
Deleting an SNMP Trap Notification . . . 198
Sending Notifications When the SIP Server Status Changes . . . 198
Configuring the Email Notification Template . . . 199
Sample MOS Notification Email . . . 201
Executing a Script and Sending Notifications on a Syslog Match . . . 201
Viewing Notification Alert History . . . 203

7 Using Templates

EdgeMarc Configuration Templates . . . 207
Generating a Template . . . 208
Editing Variables for an EdgeMarc Configuration Template . . . 210
Making Copies of a Template . . . 211
Renaming a Template . . . 212
Deleting a Template . . . 213
Exporting a Template to an XML-based File . . . 213
Importing an XML-based Template File . . . 214
Updating the EdgeMarc Configuration on a Global, Group, or Individual Node Level 215
Configuration Template Editor . . . 215
Managing Endpoint Templates . . . 216
Configuring Broadsoft Device Manager . . . 218
Configuring Script Manager . . . 218

8 MOS Analysis and Troubleshooting

Viewing the Syslog . . . 220
Viewing Syslog Messages . . . 220
Syslog Display for High Availability . . . 220
Configuring Syslog Settings . . . 221
Downloading the Syslog to a Local File . . . 222
Viewing Average Mean Opinion Score (MOS) Data . . . 223
Viewing MOS Data for the Last 10 Calls . . . 224
Viewing MOS Statistics for Call Legs . . . 224
Understanding MOS Scores . . . 228
Overview of Important MOS Statistics . . . 229

© 2016 Edgewater Networks. All Rights Reserved.

Call Quality Measurement Using EdgeView MOS Analysis 230
Accessing Call Analysis Options 230
Importing a File for MOS Analysis 234
Performing a MOS Analysis by Snapshot 235
Working with Snapshot Files 235
Troubleshooting MOS Collection Data 236
Viewing SNMP Traffic Graphs 237
Viewing Traffic Graphs for MOS Statistics 239
Sending MOS Alert Notifications 239
SIP Analytics 240
Configuring VoIP Protocol and System Analytics 240
Managing VoIP Protocol and System Analytics 241
Signaling Capture and Analysis 252
Configuring Signaling Capture Settings 253
Tips for Configuring Signal Capture Settings 254
Performing a Signal Capture 255
Analyzing the Signaling Capture 256
Downloading a Signaling Capture PCAP File 258
Deleting Signaling Capture Files 258
Performing an Active Line Test to Verify EdgeMarc Connectivity 259
Performing a Bulk Line Test 261
Setting Up a Bulk Line Test 262
Initiating a Bulk Line Test 264
Bulk Line Test Output 264
Initiating a Bulk Line Test via HTTPS Commands 266
EdgeView Troubleshooting Tools 267
Running an EdgeMarc Device Script 267
Device Script Termination Methods 269
Viewing Active Device Script Jobs 270
Remote Phone GUI Access Support 270
Testing for SSH 270
Configuring a Phone on an EdgeMarc: 272
Running a Shell Script on an EdgeMarc 273
Creating a Script 274
Editing, Copying, Renaming, and Deleting a Script 277
Executing a Script on an EdgeMarc 277
Viewing the Script Results 281
Running a Script Using Previous Settings 282
Executing a Script on a Pre-Provisioned EdgeMarc 283
Web Services to Support Running a Shell Script on the EdgeMarc 285
Automatic Trigger Diagnostics Support 286
Signaling Capture Support 289
Auto Populate for Signal Captures 289
Generating mandctl Logs 290

9 EdgeView Upgrade

Performing a Minor or Patch Upgrade 291
Verifying the Current EdgeView Software Version and Patches 291
Starting a Minor or Patch Upgrade 292

© 2016 Edgewater Networks. All Rights Reserved.

Downloading the Patch Files to a Local Computer 294
Manually Uploading a Software Patch 294
Which method should you use? 294
Manually Installing a Minor Upgrade or Patch via Direct Upload 295
Manually Installing a Minor Upgrade or Patch Using a Browser 296
Performing a Full Upgrade 299

10 Licensing
Overview 301
Installing EdgeView License Keys the First Time 301
Installing the EdgeView Product License Key 302
Viewing the Number of Licensed Nodes 304
Installing or Updating the Support License Key 305

11 EdgeView Reports
Overview 307
EdgeView Reporting Dashboard 308
Refreshing the Dashboard 312
Changing the Refresh Interval 313
What Can You Do With EdgeView Reports? 314
Registering the EdgeView Reports Server With EdgeView 315
Editing an EdgeView Reports Server Entry 316
Deleting an EdgeView Reports Server Entry 317

12 EdgeView Recommended Ports

Glossary

© 2016 Edgewater Networks. All Rights Reserved.

© 2016 Edgewater Networks. All Rights Reserved.

Preface

This document describes how to use EdgeView to centrally manage, monitor, and analyze statistics for Edgewater Networks' EdgeMarc™ and EdgeConnect™ Enterprise Session Border Controllers (ESBCs), third-party and SNMP-based devices, and IP phone endpoints in your network.

Audience

This guide is written for network installers, network operators, and network security officers who are responsible for implementing and maintaining network configurations.

Before You Begin

This guide assumes you have already installed the EdgeView Service Control Center (SCC) according to the instructions in the *SCC Installation Guide* and the Release Notes available in the Edgewater Networks Knowledgebase: www.edgewaternetworks.com/kb

About this Guide

Chapter	Description
Chapter 1, EdgeView Overview and Features	Provides an overview of the EdgeView Service Control Center (SCC) features.
Chapter 2, Getting Started	Provides instructions for logging in to EdgeView, entering the product and support license keys and configuring security settings. Also provides a quick tour of the user interface.
Chapter 3, Basic EdgeMarc Management	Provides instructions for adding, pre-provisioning, and auto-discovering EdgeMarcs, backing up, restoring, and updating EdgeMarc configurations, and resetting the EdgeMarc password.
Chapter 4, Basic Group, Node, and User Management	Describes how to create a hierarchal view of your network by adding Tenants, groups, nodes, and users in EdgeView. Also describes how to limit user access to selected EdgeView menus and features globally and at the node level.
Chapter 5, Managing EdgeView System Settings	Provides instructions for how to use the many EdgeView system tools to view and configure EdgeView system and security settings and to manage the database and database settings. It also covers how to start an SSH Session in EdgeView via CLI and how to activate EdgeView product and support licenses.
Chapter 6, Status and Notifications	Provides instructions for viewing node and group status and configuring notification settings in EdgeView.
Chapter 7, Using Templates	Describes how to create and generate EdgeMarc Configuration Templates which can be re-used by EdgeMarcs globally at the tenant or group level and locally at the EdgeMarc node level.

Chapter	Description
Chapter 8, MOS Analysis and Troubleshooting	Describes how to use EdgeView to analyze and diagnose problems on the network using mean opinion score (MOS) statistics for EdgeMarcs, groups and EdgeView sub-groups. Also covers how to analyze the EdgeMarc signaling processes and display the results in a PCAP file.
Chapter 9, EdgeView Upgrade	Provides instructions for upgrading the EdgeView system.
Chapter 10, Licensing	Provides important information about how to activate the different types of licenses for EdgeView.
Chapter 11, EdgeView Reports	Provides instructions for using the EdgeView Reporting Dashboard. Also provides an introduction to the EdgeView Reports application.
Chapter 12, EdgeView Recommended Ports	Lists available and recommended ports.

Typographic Conventions

User input is displayed in **boldface** type and can represent either keyboard input or mouse selections in a browser window, depending on the context.

Command Line Interface (CLI) text is shown in `courier font`.



Note

Notes highlight information that is important or that has special interest.



Tip

Tips provide additional information that is helpful in performing a particular task but is not mandatory to perform the task.



Caution

Cautions alert you of actions or events that may cause system damage or loss of data.



Warning

Warnings alert you of actions or events that may cause bodily harm.

Edgewater Networks Knowledgebase

The Edgewater Networks KnowledgeBase provides a central repository for information that includes:

- Configuration guides
- Data sheets
- Frequently asked questions (FAQs)
- Hardware and software installation guides
- Release notes
- Troubleshooting guides
- White papers

Visit the Knowledgebase: www.edgewaternetworks.com/kb

For further information, contact Edgewater Networks: info@edgewaternetworks.com

Contact and Support Information

Edgewater Networks, Inc.

U.S. Headquarters:

Edgewater Networks, Inc.
5225 Hellyer Ave. #100
San Jose, California 95138

Phone: 408.351.7200
Fax: 408.727.6430

edgewaternetworks.com

General: info@edgwaternetworks.com
Sales: sales@edgewaternetworks.com

Edgewater Networks, Inc. - Technical Assistance Center
Phone: 408-351-7255
Support@edgewaternetworks.com

1

EdgeView Overview and Features

This section provides an overview of the many features provided by the EdgeView Service Control Center including:

- EdgeView Overview
- EdgeMarc and Node Management
- VoIP Analysis and Troubleshooting
- Status and Notifications
- Plug & Dial
- EdgeView Reports
- VoIP Traffic Capture Signaling and RTP Media
- Integrated VoIP Test Agent
- EdgeView Graphical User Interface

EdgeView Overview

EdgeView Service Control Center enables remote configuration and central management of Edgewater Networks Enterprise Session Border Controllers (ESBCs) and auto-provisioning of VoIP phones without the overhead of running a complex software stack on separate hardware. Using the EdgeView software running on EdgeView, enterprises and service providers can monitor, and troubleshoot VoIP performance statistics from a central location, thus enhancing the support services provided to their customers. As a virtual appliance, EdgeView offers an excellent alternative to single-purpose hardware appliances, enabling high performance, agile and cost-effective WANs which can act as solid foundations for those enterprises and managed service providers considering virtualization and cloud computing.

EdgeView can manage networks of all sizes. It can be installed as a standalone system or in a redundant high-availability configuration for carrier-grade environments.

Figure 1-1 illustrates the EdgeView Service Control Center platform.

Figure 1-1 EdgeView Service Control Center Platform

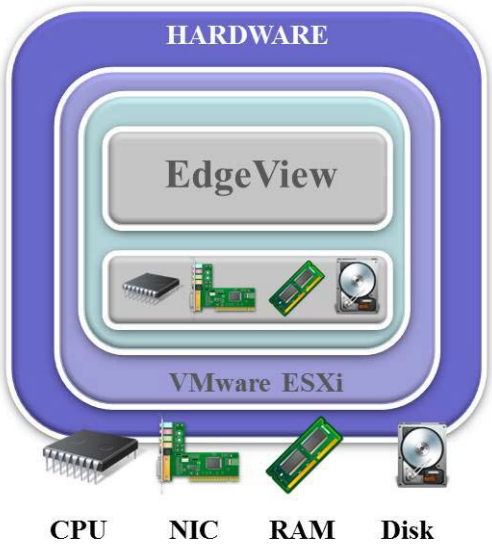
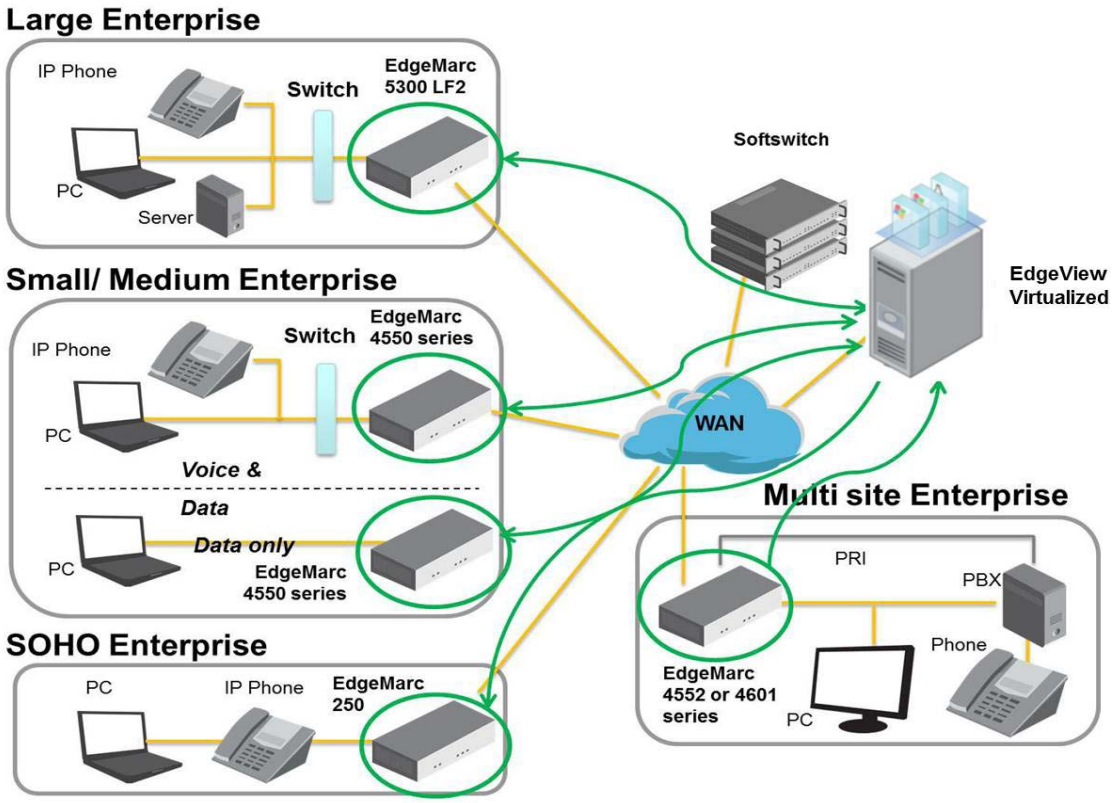


Figure 1-2 illustrates typical EdgeView deployment scenarios for large, small/medium and SOHO enterprises.

Figure 1-2 Typical EdgeView Deployment Scenarios



EdgeMarc and Node Management

EdgeView provides many capabilities for managing and monitoring the EdgeMarcs, third-party devices, and SNMP-based nodes on your network. With EdgeView, you can remotely monitor and control EdgeMarcs, including firmware upgrades, configuration changes, backups and restores, and passwords. The EdgeView auto-discovery feature enables auto configuration of EdgeMarcs and IP phones globally and at the group and node level. Third-party devices (for example, any device which can be reached via SSH protocol) and SNMP-based devices can be also be monitored with EdgeView.

See Chapter 3, *Basic EdgeMarc Management* and Chapter 4, *Basic Group, Node, and User Management* for more details.

VoIP Analysis and Troubleshooting

To help you analyze and diagnose VoIP problems on the network, EdgeView provides mean opinion score (MOS) statistics for EdgeMarcs and other managed nodes in your network. EdgeView can also analyze the VoIP signaling processes running on an EdgeMarc and display flow results in an on-demand signaling ladder. You can enter a date and time range for MOS analysis and for signaling captures to help you narrow the results to the estimated time when an issue occurred for root cause analysis and correlation. Other customizations are also available.

See Chapter 8, *MOS Analysis and Troubleshooting* for more details.

Status and Notifications

To help you monitor the devices on your network, EdgeView offers many options for viewing status, viewing alerts, and sending email notifications for the status of managed nodes and devices.

Chapter 6, *Status and Notifications* for guidelines on viewing node and group status and configuring notification settings in EdgeView.

Plug & Dial

The EdgeView “Plug & Dial” feature automates the process of provisioning SIP phones, dramatically reducing installation times from hours to minutes.



Note

Plug & Dial is a licensed feature.

When Plug & Dial is deployed in a hosted PBX or IP Centrex environment, users plug in their IP phone to the LAN and then follow voice prompts which guide them through how to configure their phone settings. This information is used by EdgeView to seamlessly and securely authenticate the user with a feature server/softswitch. Upon successful authentication, the EdgeView system generates the appropriate phone configuration files, installs them on the EdgeMarc which pushes them to the IP phones, reboots the phones and then sends notifications to upstream OSS systems.

Refer to Chapter 11, *Plug & Dial* for details on how to provision Plug & Dial.

EdgeView Reports

EdgeView offers comprehensive reporting features via the Reporting Dashboard and the add-on EdgeView Reports (EdgeView Reports) module.



Note

EdgeView Reports is a licensed feature.

EdgeView Reporting Dashboard provides a graphical snapshot of the current system status using graphs and charts which show a summary of the statistics gathered by EdgeView over the past 24 hours. The pie charts, bar charts, and graphs on the Dashboard display real-time call quality performance metrics including minimum, maximum, and average Mean Opinion Scores (MOS), MOS polling and reporting statistics, below threshold count (BTC) alerts and more. You can view more detailed data for a particular device by clicking an area in the pie chart or graph.

In addition to the Reporting Dashboard, EdgeView integrates with the EdgeView Reports add-on module which provides valuable VoIP performance information about the interaction between EdgeView and the EdgeMarc(s) and other nodes managed by EdgeView. With EdgeView Reports, you can immediately see a graphical snapshot of the current system status and retrieve detailed call quality performance statistics on-demand or on a schedule. The EdgeView Reports user interface offers a real-time “Dashboard” view with high-level dynamic reporting and a comprehensive library of reports that can be adapted to your needs, then printed or saved in a range of useful formats.

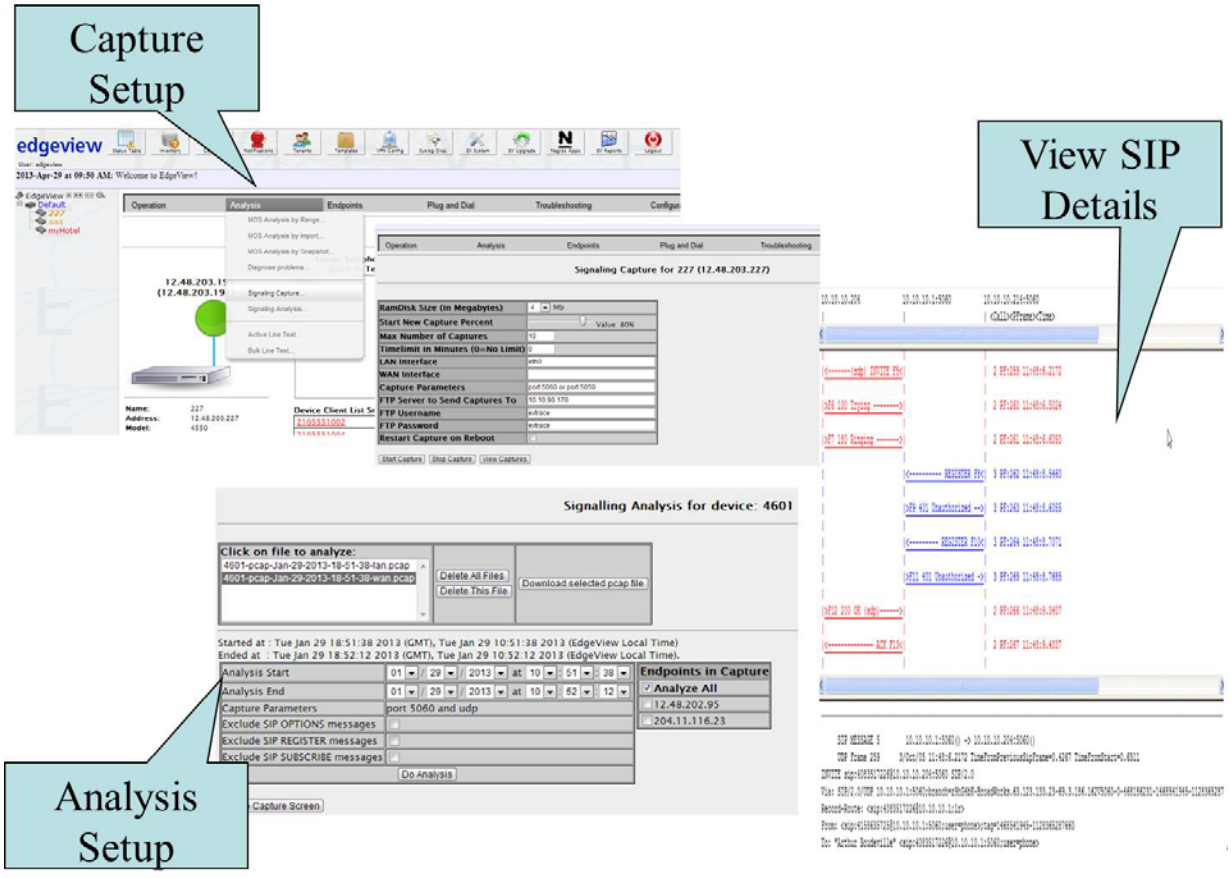
Refer to Chapter 11, *EdgeView Reports* for details about using the Dashboard and an overview of the many reports and statistics provided by EdgeView Reports.

For more details on using EdgeView Reports, refer to the EdgeView Reports documentation in the Edgewater Networks Knowledgebase: www.edgewaternetworks.com/kb

VoIP Traffic Capture Signaling and RTP Media

EdgeView can capture, store, view, and analyze VoIP traffic, signaling, and Real Time Protocol (RTP) media. You can set filters to capture only the data of interest to you and then store the file in the EdgeView database. For example, you can filter on a time frame, IP address, or special SIP messages. The capture file can be viewed in EdgeView or downloaded to your local drive in a number of formats for analysis with your favorite packet analyzer.

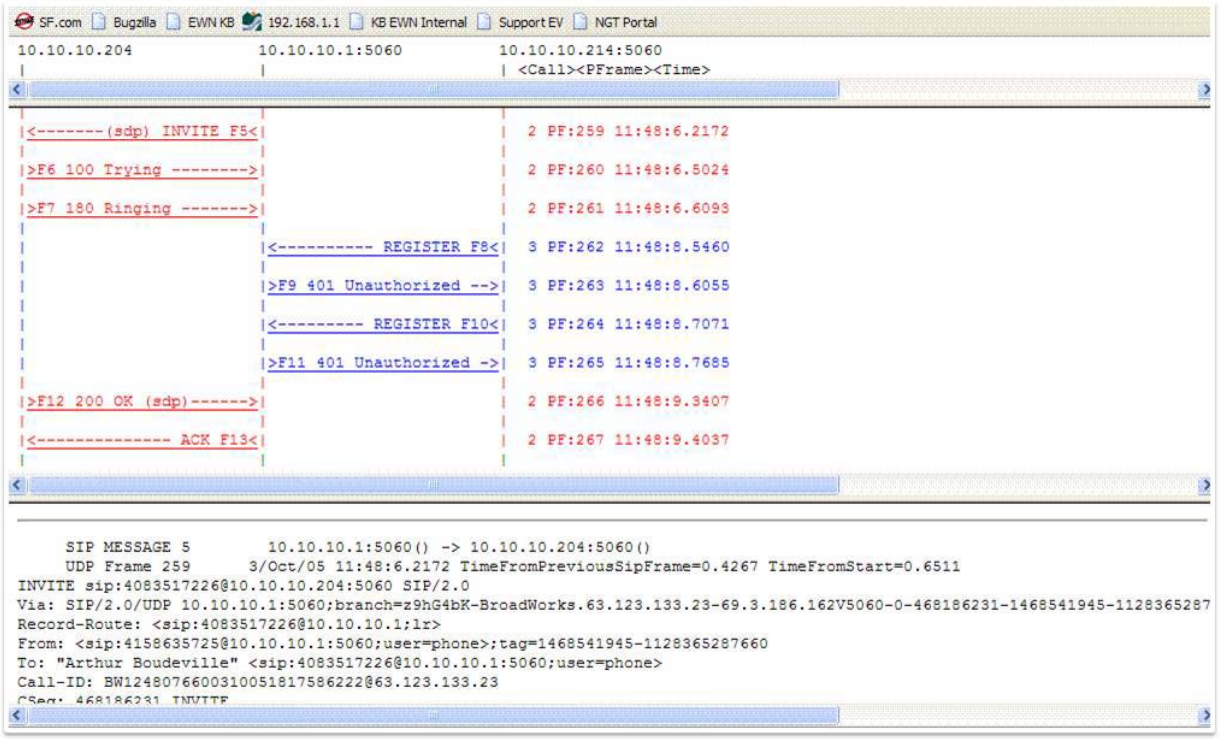
Figure 1-3 VoIP Traffic Capture Signaling and RTP Media



On-Demand Signaling Ladder

To help you investigate call flow issues, EdgeView can display an on-demand signaling ladder for a selected call leg (Figure 1-4). The signaling ladder shows the SIP call flow and highlights any signalization misbehavior.

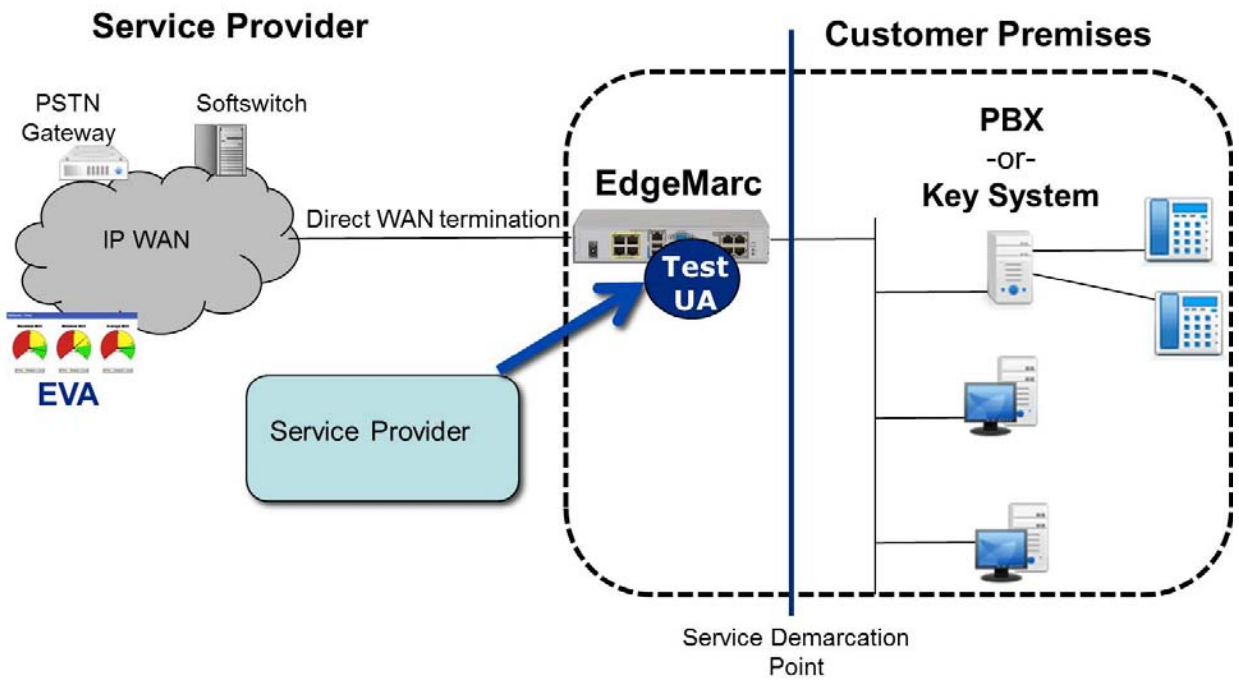
Figure 1-4 Signaling Ladder



Integrated VoIP Test Agent

As illustrated in Figure 1-5, EdgeView can place test VoIP calls to and from deployed EdgeMarcs and EdgeConnects without requiring remote assistance from end users. This allows service providers, network operators, and field technicians to remotely validate installations and troubleshoot problems without interaction from the end user.

Figure 1-5 Integrated VoIP Test Agent



EdgeView Graphical User Interface

EdgeView provides an intuitive, easy-to-use graphical user interface for centrally managing the EdgeMarcs, EdgeConnects, third-party devices, SNMP-based nodes, and IP phones on your network. Using EdgeView, you can create a hierarchical view of your network which displays color-coded status information for quick identification of service affecting problems. You can apply configuration settings globally at different levels in the hierarchy with a single operation, allowing you to automate many routine tasks. For example, you can upgrade a group of EdgeMarcs at one time rather than individually.

EdgeView provides graphical menus for capturing, viewing, and analyzing VoIP traffic, signaling, and call-related statistics. Using the many EdgeView reporting features, you can perform extensive trend analysis and reporting for items such as uptime, link utilization, and call quality. EdgeView provides context sensitive, online troubleshooting tips linked to the Edgewater Networks Knowledgebase for real-time problem resolution.

Figure 1-6 shows an example of the main EdgeMarc Status page for analyzing and viewing EdgeMarc and EdgeConnect status and call statistics. Figure 1-7 shows an example of the more detailed node level status collected by EdgeView.

Figure 1-6 Main EdgeMarc Status Page

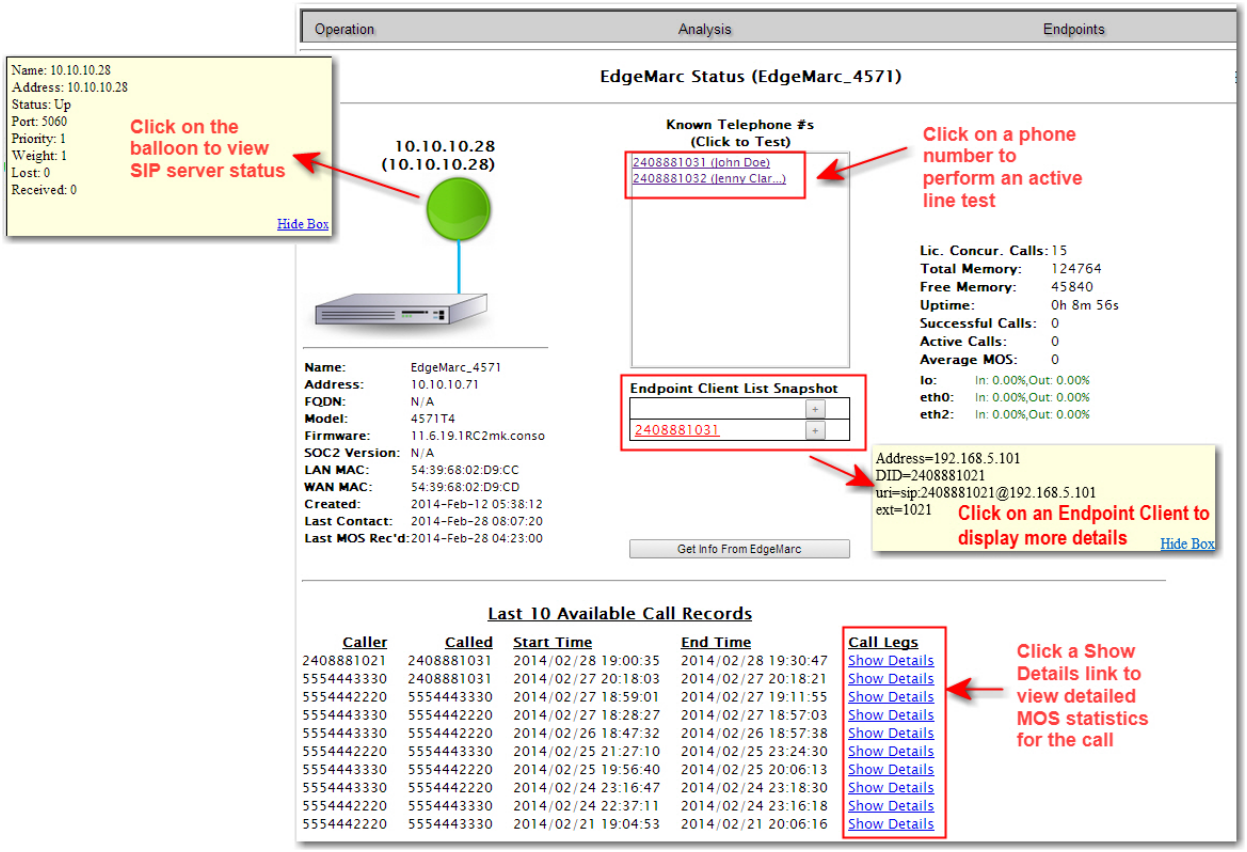
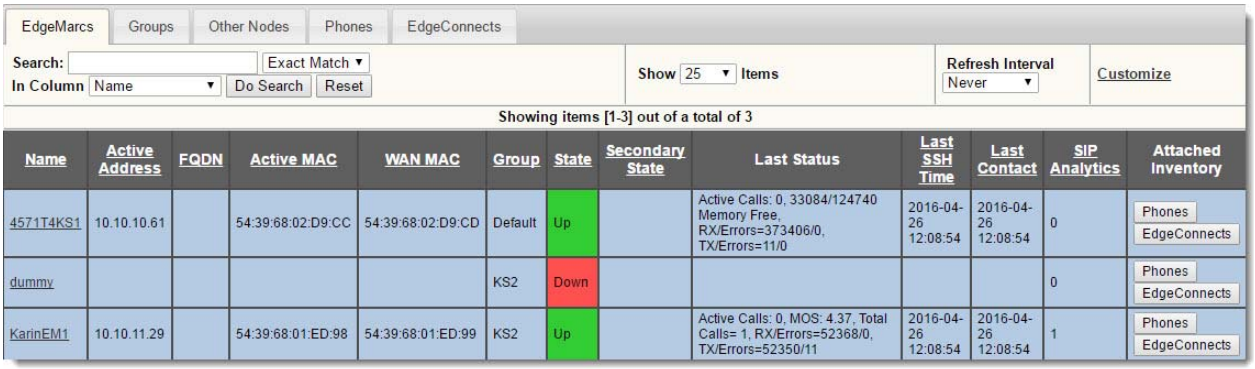


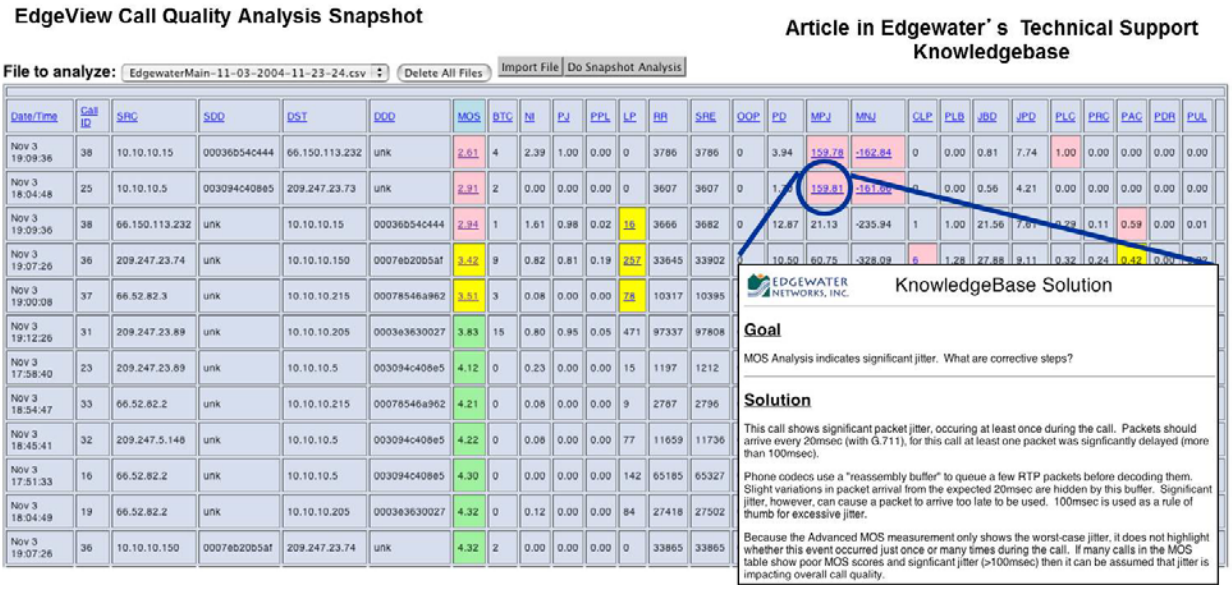
Figure 1-7 Viewing Node Level Status



Context-Sensitive Help

To simplify problem resolution, EdgeView displays context-sensitive help. For example, when you are viewing and analyzing call quality statistics, you can click the underlined text in a column to view a topical article in the Edgewater Networks Knowledgebase (Figure 1-8). The article provides details about the statistic to help you better understand the meaning, as well as steps you can take to resolve the problem.

Figure 1-8 EdgeView Context Sensitive Help



2

Getting Started

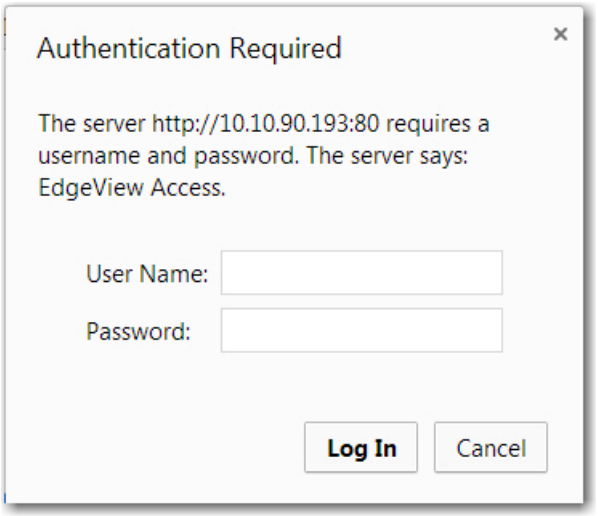
This section provides instructions for logging in to EdgeView, installing the product and support license keys, and managing passwords. It also includes a quick tour of the EdgeView user interface.

- Starting EdgeView
- Installing the EdgeView Product License and Support License Keys
- Managing Passwords in EdgeView
- EdgeView Quick Tour

Starting EdgeView

1. Open a browser window and enter the IP address or fully qualified domain name (FQDN) of EdgeView in the address bar. The EdgeView Login page displays (Figure 2-1).

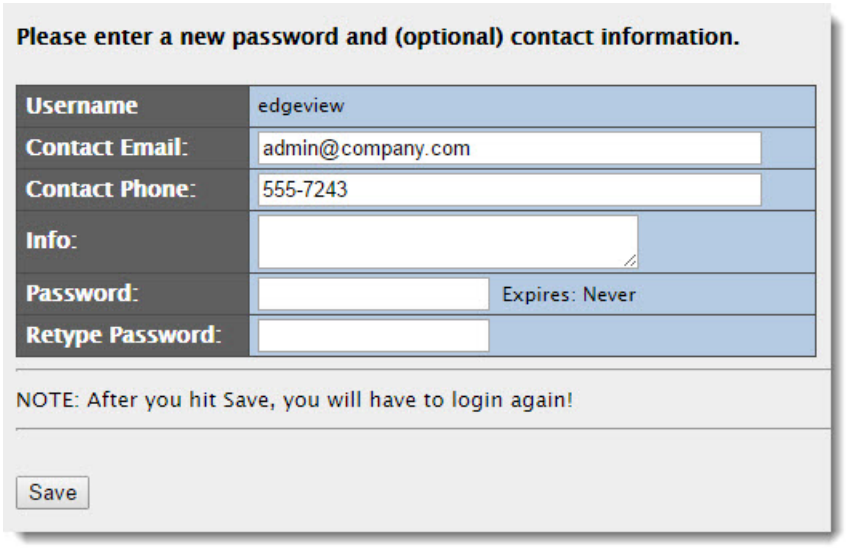
Figure 2-1 EdgeView Login Page



2. Log in with the default login credentials:
   - Name—**edgeview**
   - Password—**edgeview**
3. Click **Log In**.

You will immediately be prompted to change the global login credentials (Figure 2-2).

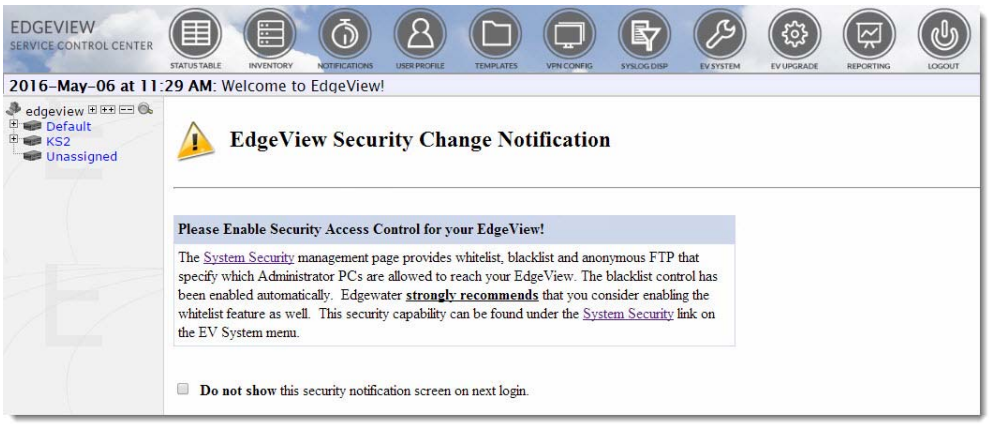
Figure 2-2 Changing Global Password Settings



4. Enter a new password and optional contact information. If your system administrator has enabled the strict password setting, the password will be required to have 6-8 characters, two or more character types, and no dictionary words. Character types include lowercase letters, uppercase letters, digits and the rest of the allowed characters.
5. Click **Save**. The login screen will re-display.

   If you are logging in to EdgeView for the first time, you will need to install the Product and Support license keys. Refer to Installing the EdgeView Product License and Support License Keys.
6. Once you have changed your password, the EdgeView Security Change Notification page displays (Figure 2-3).

Figure 2-3 EdgeView Security Change Notification Page



EdgeView Security Change Notification Page

When you log in to EdgeView the first time, the EdgeView Security Change Notification page displays. This screen reminds you to configure security settings to restrict and enable access through the firewall. For details on how to configure security settings, refer to Configuring EdgeView System Security Settings in Chapter 5, *Managing EdgeView System Settings*.

If you prefer not to see the EdgeView Security Notification screen upon login, select the checkbox:



You can also disable this setting on the EdgeView Security Configuration screen: **EV System** > **System Settings** > **Security Settings**

The next time you log in, the Advanced Directory of Tenants will be the first screen displayed in EdgeView.

Figure 2-4 Directory of Tenants



Installing the EdgeView Product License and Support License Keys

The first time you log in to EdgeView, you will immediately be prompted to change the global login credentials. Once you have changed the login credentials, the EdgeView License Key screen displays for you to install the EdgeView Product License key and Support License key. These keys are sent in email when you purchase an EdgeView and a Support License. The email includes the MAC address, license key, and URL to the location of the OVA file. Refer to Chapter 10, *Licensing* for instructions.

Managing Passwords in EdgeView

If you are an Administrator user, you can change the EdgeView login password and assign unique login passwords to users once they have been added in EdgeView. Additionally, you can force users to change their password according to a set time interval and enforce users to enter strict passwords. Strict passwords require 6-8 characters, two or more character types, and no dictionary words. Character types include lowercase letters, uppercase letters, digits and the rest of the allowed characters. The password restrictions are enforced when the user changes their password the first time they log in to EdgeView and when an EdgeMarc is added or changed in EdgeView. Strict passwords are disabled by default.

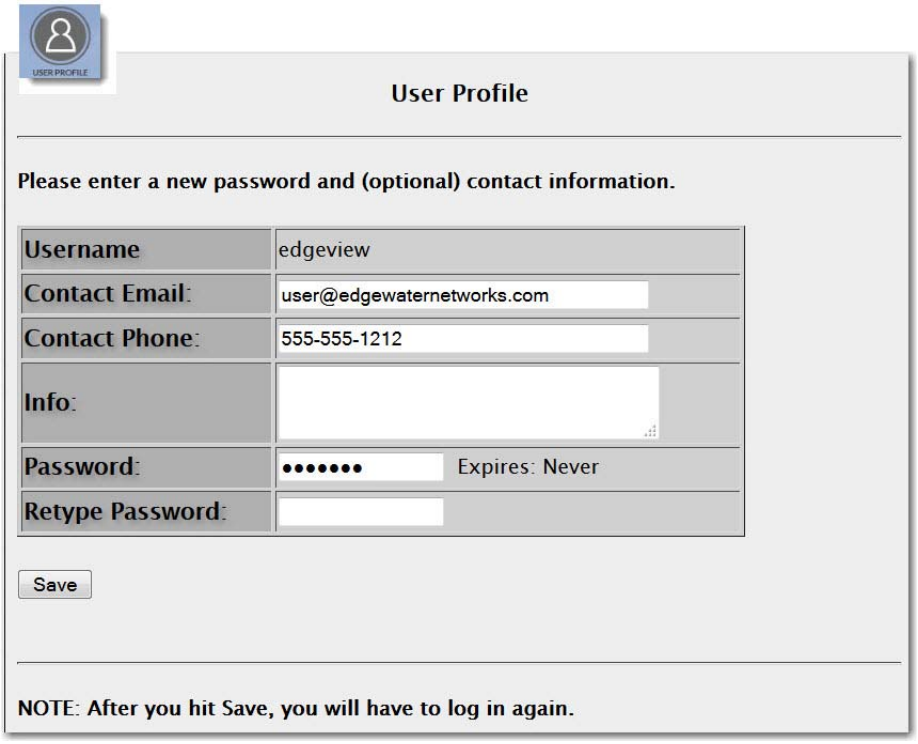
For more details about managing passwords, see Chapter 5, *Managing EdgeView System Settings*.

Changing Your Password and User Profile

Any user can change their password and contact information at any time by selecting the **Profile** icon from the EdgeView icon bar.

1. If you are a user without administrator rights, click **Profile** in the icon bar.
2. If you are a user with administrator rights, click **User Profiles** in the icon bar. Figure 2-5 shows the Admin User Profiles page.

Figure 2-5 User Profile Screen



3. Review the contact information and change if appropriate.
4. Enter a new password.
5. Retype the password.
6. Click **Save**.

Note

After you click **Save**, you will need to log in again.

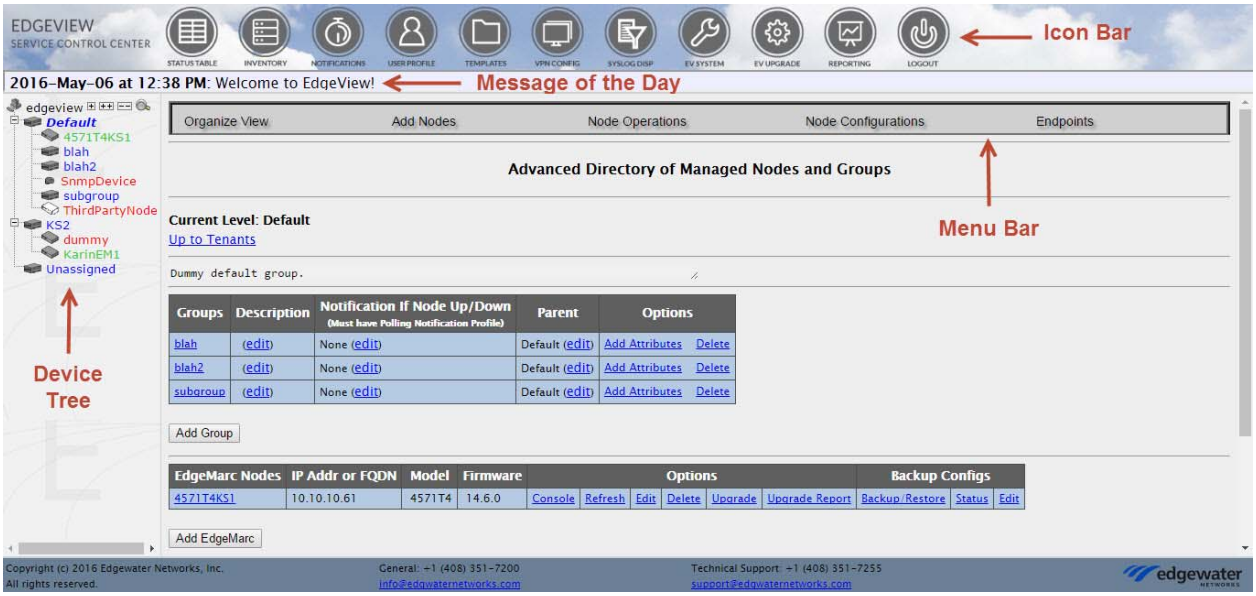
EdgeView Quick Tour

As illustrated in Figure 2-6, the general page layout of the EdgeView interface is comprised of the following components:

- **Icon Bar**—Provides access to the general EdgeView functions.
- **Message Bar**—Displays the currently logged in EdgeView user and the Message of the Day.
- **Device Tree**—Shows hierarchical, collapsible lists of the groups, EdgeMarcs, IP phones, third-party nodes and other SNMP-based nodes managed by EdgeView.

- **Menu Bar**—Contains menu options for monitoring, provisioning, configuring and performing operations on the nodes managed by EdgeView. The menu bar options change depending on which level you are at in the device tree and the type of information you are viewing.

Figure 2-6 EdgeView Page Layout



Icon Bar

The icons at the top of the EdgeView main page provide access to GUI pages for configuring settings and viewing status of the nodes being managed by EdgeView. The user will see only the icons they have specific rights to access (Table 2-1).

Table 2-1 EdgeView Admin Navigation Buttons

Button	Available Functions
	Click the **Status Table** icon to view the Device Table which shows status for the EdgeMarcs, Phones, EdgeConnects, groups, and other nodes being monitored by EdgeView. Each tab in the Device Table displays status specific to the selected node type.
	Click the **Inventory** icon to view database information about the nodes being managed by EdgeView.

Table 2-1 EdgeView Admin Navigation Buttons

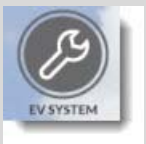
Button	Available Functions
	Click the **Notifications** icon to set which type of device notifications you want to monitor and to configure settings for automatically sending a notification to selected email addresses. The email notifications are triggered based on a certain event or events that are logged by the EdgeMarc or by EdgeView. You can also automatically send email notifications for MOS statistics.
	Click the **User Profiles** icon to administer user profiles and passwords.
	Click the **Templates** icon to show EdgeMarc templates, endpoint templates and scripts which contain configuration values to the EdgeMarc and phones.
	Click the **VPN Config** icon to view and edit VPN groups and VPN Policies.
	Click the **Syslog Disp** icon to display Syslog messages. You can filter the messages by EdgeMarc, group, date, and by the message receipt status (incoming, new, received). You can also save the Syslog to a file.
	Click the **EV System** icon to access the system and administration tools which allow you to perform various tasks related to database management, system settings, security, and licensing.

Table 2-1 EdgeView Admin Navigation Buttons

Button	Available Functions
	Click the **EV Upgrade** icon to perform full and partial system upgrades.
	Click the **Reporting** icon to access the EdgeView Reports Dashboard which provides a real-time graphical view of call quality performance metrics.
	Click the **Logout** icon to log out of EdgeView.

Device Tree

The EdgeView device tree shows a hierarchical view of your network with collapsible lists of the users, tenants, groups, nodes, and endpoints being managed by EdgeView. The device tree shows color-coded status information for quick identification of service affecting problems. Once you set up the device tree hierarchy, you can apply configuration settings globally at different levels in the hierarchy with a single operation, allowing you to automate many routine tasks. For example, you can upgrade a group of EdgeMarcs at one time rather than individually.

Refer to Figure 2-7 and Table 2-2.

Figure 2-7 EdgeView Device Tree

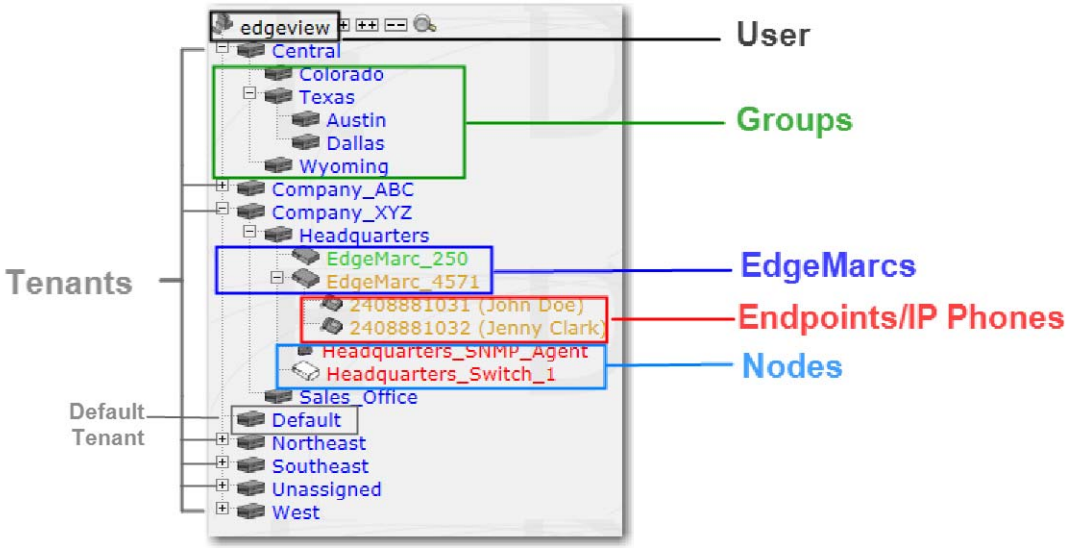


Table 2-2 Device Tree Descriptions

User	The currently logged in user. The user is the root of the device tree. Only the Tenants assigned to the user are shown in the device tree. The default user is ‘edgeview’.
Tenant	The highest level in the EdgeView hierarchy. Tenants contain groups and nodes.
Group	A collection of nodes which are grouped together to make them easier to manage. By grouping nodes, you can apply a single action to all nodes in the group at once which saves you from having to configure each node individually. Note that groups can also contain other groups (sub-groups).
Node	An EdgeMarc, EdgeConnect, third-party device, SNMP-based device, or Plug & Dial conduit.
Endpoint	An IP phone.

For more information about how to setup the device tree hierarchy, refer to Chapter 4, *Basic Group, Node, and User Management*. For more information about the node level status displayed for different types of nodes managed by EdgeView, refer to Chapter 6, *Status and Notifications*.

Menu Bar

The EdgeMarc Status menu bar provides access to menus for monitoring, provisioning, configuring and performing operations on EdgeMarcs, groups, nodes, and endpoints managed by EdgeView. The menu bar options change depending on your level in the device tree. The user will see only the menus they have specific rights to access.

3

Basic EdgeMarc Management

This section provides instructions for using EdgeView to remotely monitor and control EdgeMarcs including how to configure settings for the EdgeView auto-discovery feature so that EdgeView can automatically configure EdgeMarcs upon discovery.

- Adding an EdgeMarc
- Changing Polling and Discovery Settings
- Editing EdgeMarc Attributes
- Deleting an EdgeMarc from EdgeView
- Launching the EdgeMarc GUI from EdgeView
- Creating a Collection of EdgeMarcs
- Rebooting an EdgeMarc
- Changing the EdgeMarc Password
- Pre-Provisioning an EdgeMarc
- Backing Up and Restoring an EdgeMarc Configuration
- Upgrading the EdgeMarc VOS Firmware
- Managing License Keys

For instructions on how to create EdgeMarc groups, refer to Chapter 4, *Basic Group, Node, and User Management*.

Adding an EdgeMarc

To start managing EdgeMarcs in your network they must first be added to EdgeView manually or through auto-discovery (the default). You can also add EdgeMarcs using the EdgeView Web Services API.

Refer to the *EdgeView Web Services User Guide* available in the Edgewater Knowledgebase for details on adding EdgeMarcs using the EdgeView Web Services API: www.edgewaternetworks.com/kb

Note

Although the term “EdgeMarc” is used throughout the EdgeView GUI and in this guide, it also applies to all Edgewater Networks ESBCs in your network.

Adding an EdgeMarc via Auto-Discovery

By default, EdgeMarcs are auto-discovered by EdgeView when they come online. This requires some initial setup on both the EdgeMarc and EdgeView so EdgeView can “see” the EdgeMarc and automatically add it to the database. Minimally, enter the EdgeView IP address or FQDN in the EdgeMarc VOS user interface and then start EdgeView. Using the default settings, EdgeView will automatically discover the EdgeMarc, add it to the EdgeView database, and then add it to the device tree. EdgeView uses the EdgeMarc hostname as the name of the node. You can rename the node to whatever you like.

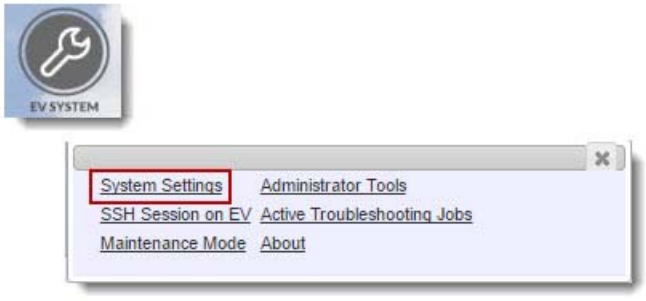
When a new EdgeMarc is auto-discovered, EdgeView adds it to the database according to the matching criteria defined on the EdgeView Settings page. If EdgeView auto-discovers an EdgeMarc that has been pre-configured with either the MAC address or hostname, but NOT the IP address or FQDN, then EdgeView will automatically update the EdgeMarc record in the EdgeView database to include the new IP address when the EdgeMarc sends its initial syslog message to EdgeView. It may also automatically push the initial configuration to the EdgeMarc if this has been set up previously. See Pre-Provisioning an EdgeMarc for more details.

Configuring Auto-Discovery in EdgeView

By default, auto-discovery is enabled in EdgeView. If auto-discovery is disabled, use this procedure to enable it and configure auto-discovery settings.

1. Open EdgeView and select **EV System** > **System Settings.**

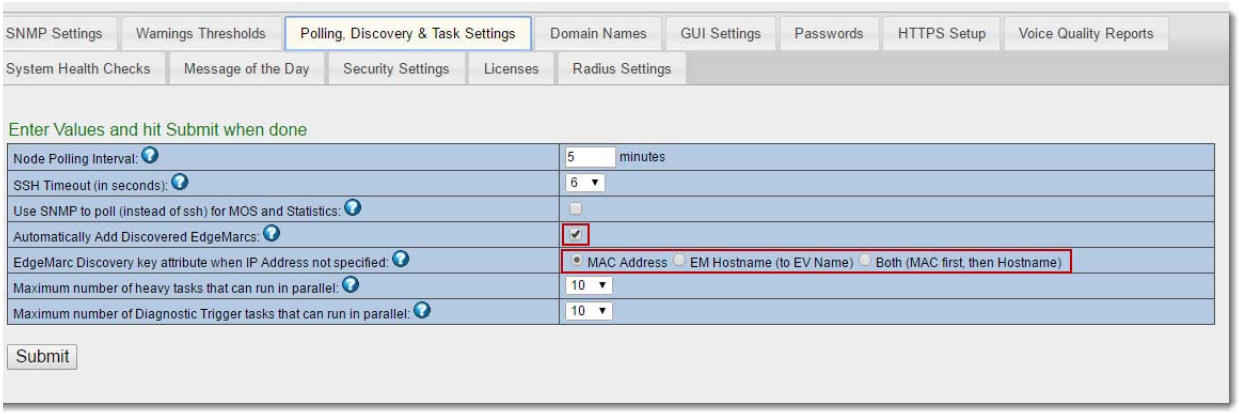
Figure 3-1 EV System Menu



2. In the EdgeView System Settings page, select the **Polling & Discovery Settings** tab. The screen shown in Figure 3-2 displays.

3. In the Polling & Discovery Settings page, verify that the **Automatically Add Discovered EdgeMarcs** checkbox is enabled. This box is enabled, by default.
4. In the **EdgeMarc Discovery Key attribute when IP Address not specified** field, select a matching option. See Setting the Matching Criteria for Auto-Discovery.
5. Click **Submit**.
6. Configure auto-discovery settings on the EdgeMarc. See Configuring Auto-Discovery Settings on the EdgeMarc.

Figure 3-2 Enabling/Disabling Auto-Discovery in EdgeView



Configuring Auto-Discovery Settings on the EdgeMarc

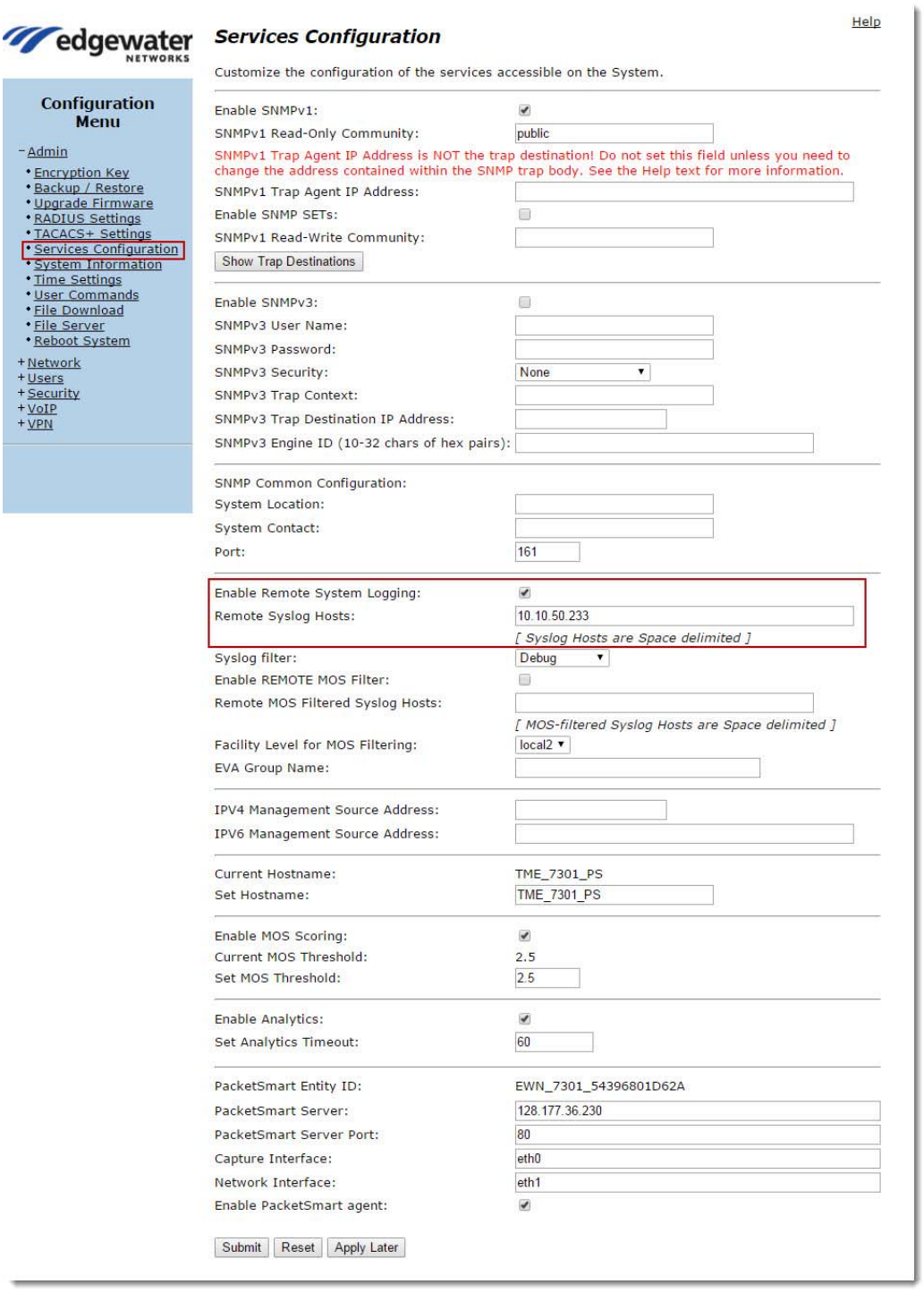
1. Open the EdgeMarc VOS user interface and point the EdgeMarc syslog field to EdgeView (Figure 3-3).
   a. On the EdgeMarc, select **Admin** > **Services Configuration** from the EdgeMarc Configuration menu.
   b. Enable the **Remote System Logging** checkbox.
   c. Enter the EdgeView IP address or FQDN in the **Remote Syslog Hosts** field. If you have several syslog repository servers, enter each IP address or FQDN separated by a space.
   d. Set the Syslog filter to **Debug**.
   e. Click **Submit**.



Tip

You can access the EdgeMarc GUI from within EdgeView by selecting the EdgeMarc from the device tree and choose **Operation** > **Launch EdgeMarc GUI**.

Figure 3-3 EdgeMarc Services Configuration Page



Manually Adding an EdgeMarc

If you are not using auto-discovery to add EdgeMarcs, you can add them manually as follows.

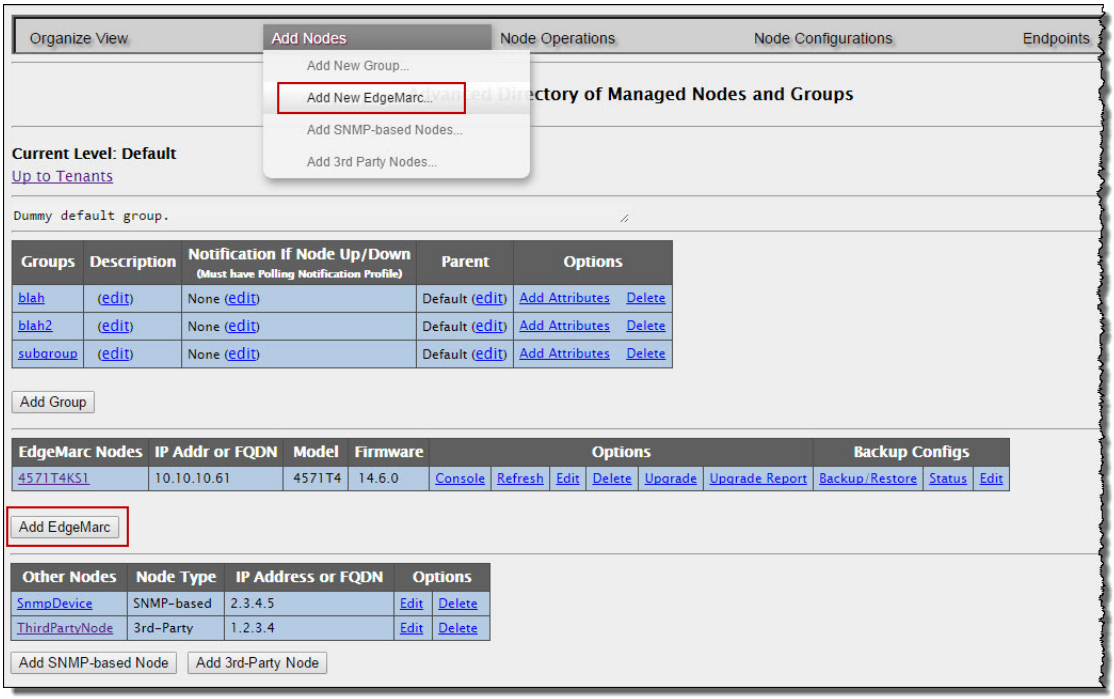
1. Open EdgeView and from the device tree, select the tenant or group to which you want to add the EdgeMarc. The EdgeMarcs that are currently in that level, if any, will display in the Advanced Directory of Managed Devices and Groups screen.

   If there are no tenants or groups, add the EdgeMarc to the Default Tenant.

   For details on how to create and manage Groups and nodes, refer to Chapter 4, *Basic Group, Node, and User Management*.

2. In the Advanced Directory of Managed Nodes and Groups screen, click **Add EdgeMarc** or select **Add Nodes** > **Add New EdgeMarc** from the menu bar (Figure 3-4).

Figure 3-4 Adding an EdgeMarc

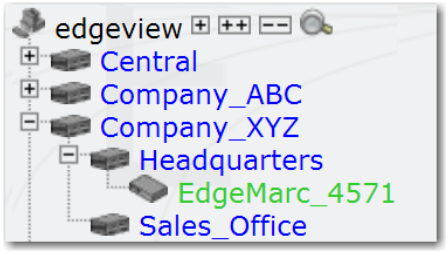


3. In the Add EdgeMarc Attributes and Addresses page (Figure 3-5):
   - Enter a Name
   - Enter the IP Address FQDN of the EdgeMarc. This address is not required if you are pre-provisioning the EdgeMarc. See Pre-Provisioning an EdgeMarc.
   - Verify that the correct group is selected.
   - Enter the SSH password for the EdgeMarc.
   - Click **Save**.

Note

The rest of the fields are optional. You can go back and set these fields later. See Editing EdgeMarc Attributes.

Once the EdgeMarc has been added, the message EdgeMarc was saved successfully! displays on the Add EdgeMarc Attributes and Addresses along with the configured values. The EdgeMarc will be added to the device tree and will appear in red until it has been discovered by EdgeView. Once the device has been discovered, it will appear in green in the device tree:



If configured, EdgeView can automatically push an EdgeMarc configuration template to the EdgeMarc during the next polling cycle. For more information see Chapter 7, *Using Templates*.

Figure 3-5 Add EdgeMarc Attributes and Addresses

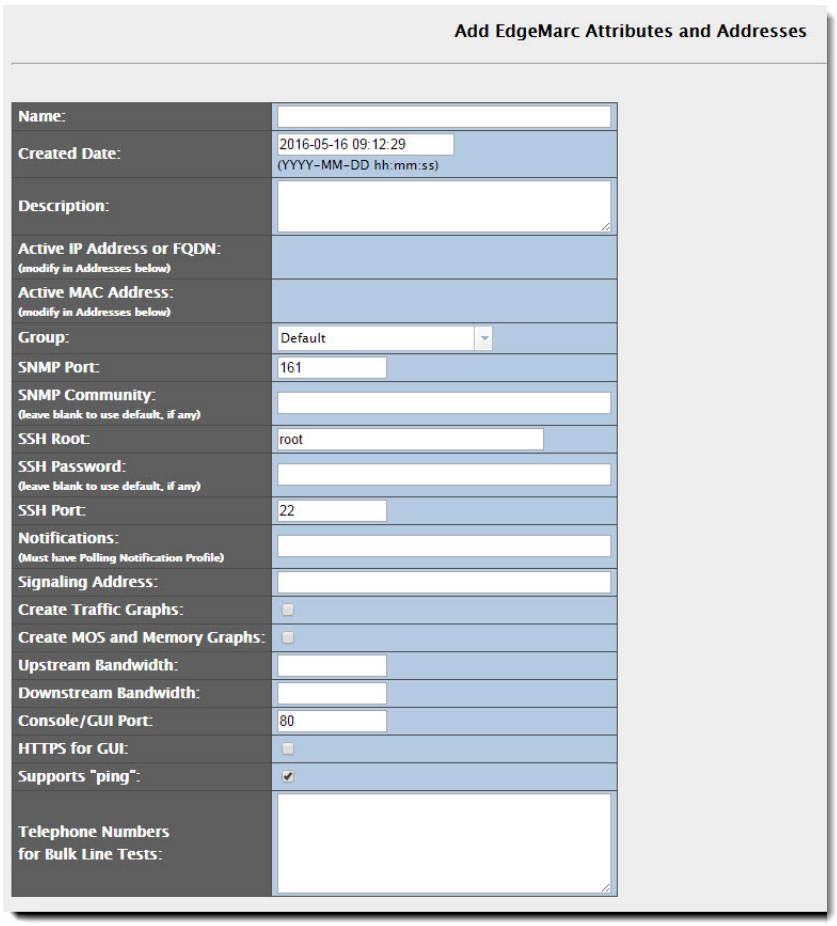


Table 3-1 defines the fields in the Add EdgeMarc Attributes and Addresses.

Table 3-1 Field Descriptions for the Add EdgeMarc Attributes and Addresses

Field	Description
Name	(Required) Assign a name to the EdgeMarc
Created Date	Displays the timestamp for when the EdgeMarc was added. This is assigned by EdgeView.
Description	(Optional) Type a description you want to assign to the EdgeMarc to make it easier to identify on the network.
Primary Address	(Required) Type the IP Address of the EdgeMarc.
MAC Address	(Optional) Type the MAC Address of the EdgeMarc. Generally, you do not need to enter this as EdgeView will enter it automatically when it polls the EdgeMarc. However, this field is necessary if you are pre-provisioning an EdgeMarc. See Pre-Provisioning an EdgeMarc. When pre-provisioning, enter the WAN MAC address here and then leave the Primary Address blank. This will initiate a workflow that will assign an IP Address to the EdgeMarc.

Group	Displays the currently selected group to which the EdgeMarc will be added. To change the group, select a different one from the drop-down box.
SNMP Port	The SNMP port for the EdgeMarc. This field is pre-populated with the value from the Tenants page. To change it, type a new value and click **Save**.
SNMP Community	The community string for the EdgeMarc. This field is pre-populated with the value from the Tenants page. To change it, type a new value and click **Save**.
SSH Root	The root password for the EdgeMarc. This field is pre-populated with the value from the Tenants page. To change it, type a new value and click **Save**.
SSH Password	(Required) Enter the SSH Password for the EdgeMarc. This value must match the login credentials configured on the EdgeMarc.
SSH Port	The SSH port used for the EdgeMarc. This field is pre-populated with the value from the Tenants page. To change it, type a new value and click **Save**.
Notifications	(Optional) Enter comma-separated email addresses to which you want to send EdgeMarc up/down notifications.
Signaling Address	Shows an IP-Address for the EdgeMarc that could be: • a virtual IP-address (if the EdgeMarc is configured as an HA pair) • a configured Signaling Alias on the EdgeMarc
Create Traffic Graphs	(Optional) Select the checkbox if you want EdgeView to gather link utilization statistics for this EdgeMarc and display them in a graph. The node must support SNMP in order for EdgeView to collect the appropriate statistics.
Create MOS Graphs	(Optional) Enable this checkbox if you want EdgeView to create MOS graphs for VoIP call quality monitoring.
Upstream Bandwidth Downstream Bandwidth	These fields assign bandwidth to the EdgeMarc. If the Traffic Shaper on the EdgeMarc is enabled, these fields will contain the Traffic Shaper values of the primary interface. If the Traffic Shaper on the EdgeMarc is disabled, the values can be set here in EdgeView. If the values are set in EdgeView, they will not be enforced on the EdgeMarc but will be used to display the set usage and the actual usage in a Report (WAN Traffic Report) from the EdgeView Report Server.
Console/GUI Port	(Optional) Enter the EdgeMarc port to use as a console port. By default, this is set to 80.
HTTPS for GUI	(Optional) Select the checkbox if you want to use HTTPS rather than HTTP to display the EdgeView GUI.

Supports Ping	(Optional) Select the checkbox if the EdgeMarc supports ping; DO NOT enable this checkbox if the EdgeMarc is not pingable. This checkbox is enabled by default. **Note:** In situations where this checkbox is enabled, the EdgeMarc goes down, and the provider blocks pings, the EdgeMarc will not come up again.
Telephone Numbers for Bulk Line Tests	(Optional) Enter the phone numbers to be used for Bulk Line Testing. The phone numbers must be on a separate line. Refer to Performing a Bulk Line Test.
Additional IP Addresses/MAC Addresses	If the EdgeMarc is configured with WAN Link Redundancy, enter an additional IP Address or FQDN here.

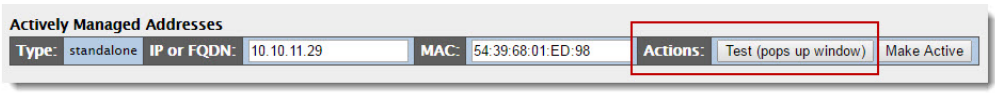
Testing EdgeMarc Connectivity

Click the **Test** button on the Add EdgeMarc Attributes and Addresses to test the SSH and SNMP connectivity for an EdgeMarc. It may take a couple of minutes to complete the SSH and SNMP tests. The **Test** button can be accessed at any time on the Edit Device Page which is accessible on the Advanced Directory of Managed Nodes and Groups page or the **Operations** > **Edit EdgeMarc Attributes** menu (Figure 3-6).

Tip

Performing this test when you add an EdgeMarc can save a lot of troubleshooting time later.

Figure 3-6 Testing the EdgeMarc Connectivity - Edit Device



Changing Polling and Discovery Settings

When EdgeView discovers an EdgeMarc, it automatically adds it to the database and sets up Plug & Dial. You can disable this setting and configure other auto-discovery settings on the Polling & Discovery page as described here.

To access the Polling & Discovery page:

1. Select **EV System** > **System Settings**.
2. Select the **Polling & Discovery Settings** tab. The Polling & Discovery Settings page displays (Figure 3-7).

3. Configure settings for auto-discovery. Refer to Table 3-2.
4. Click **Submit**.

Figure 3-7 Changing Auto-Discovery Settings

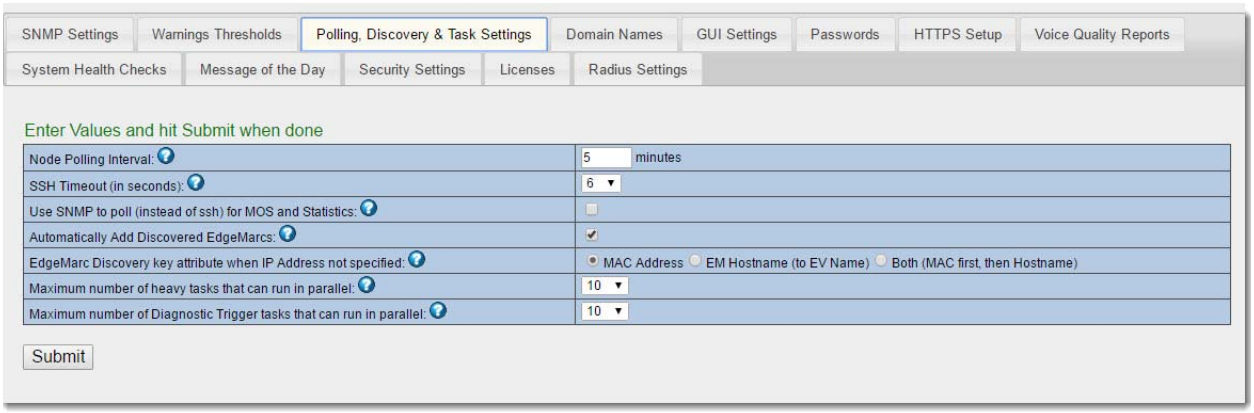


Table 3-2 Configuring Auto-Discovery Settings

If you want to...	Do this
Change the node polling interval	Enter a new value for the Node Polling Interval. The default is 5 minutes.
Change the SSH Timeout	Increase the SSH Timeout value above the minimum (6 seconds) only if nodes are showing down but are, in fact, accessible via SSH. The SSH Timeout is the number of seconds that EdgeView waits for a response from an SSH command into a node.
Enable/Disable auto-discovery	Check/uncheck the **Automatically Add Discovered EdgeMarcs** checkbox. Auto-discovery is enabled by default.
Set a matching criteria option for EdgeView to use if it discovers an EdgeMarc which does not have an IP address.	See Setting the Matching Criteria for Auto-Discovery for details on selecting a matching option.

Setting the Matching Criteria for Auto-Discovery

When EdgeView auto-discovers an EdgeMarc which does not have an IP address, you can set matching criteria so that EdgeView can identify the EdgeMarc, assign it an IP address, and automatically add it to the EdgeView database. You set this criteria on the Polling & Discovery page in the **EdgeMarc Discovery key attribute when IP Address not specified:** field.

Here's how the matching criteria works:

- If you set this option to **MAC Address** (the default setting), EdgeView will first check its database for the EdgeMarc MAC address. If it finds the MAC address in the database, EdgeView will assign the EdgeMarc

an IP address, add it to the database, and push out the configuration (if set) to the EdgeMarc.

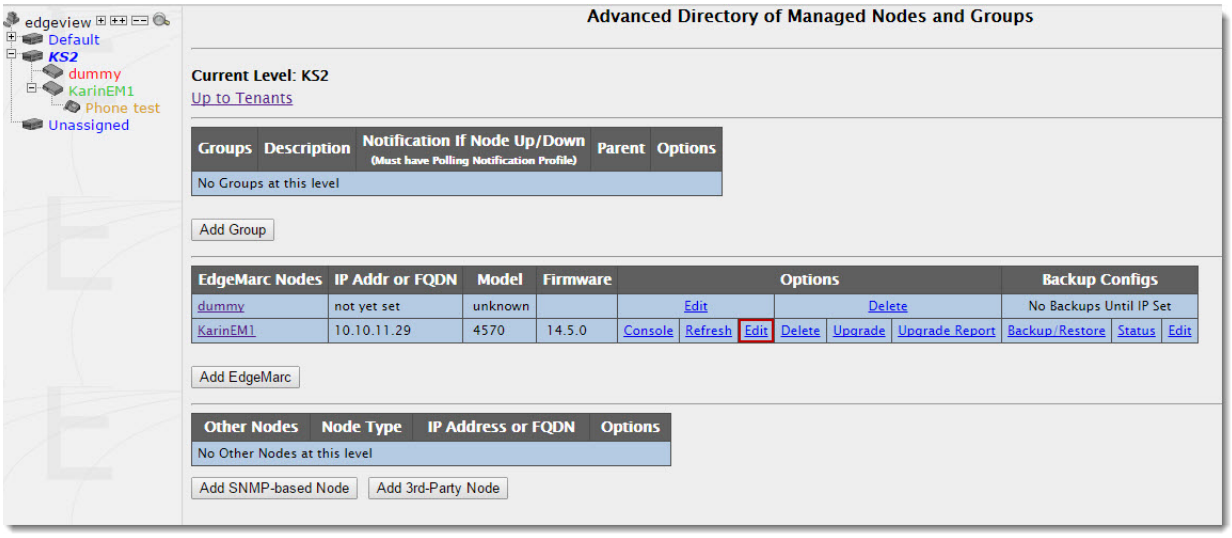
- If you set this option to **EM Hostname (to EV Name)**, EdgeView will first check to see if the hostname for the EdgeMarc matches the hostname in the EdgeView database. If there is a match, EdgeView will assign it an IP address, add it to the database, and push out the configuration (if set) to the EdgeMarc.
- If you set this field to **Both**, EdgeView will first try to match the EdgeMarc MAC address and then attempt to match the EdgeMarc hostname before assigning it an IP address and pushing out the configuration (if set) to the EdgeMarc.

Editing EdgeMarc Attributes

Once you have added an EdgeMarc, you can go back and edit the settings as follows:

1. Open the Edit Device Page for the EdgeMarc in either of the following ways:
   - From the device tree, select the group to which the EdgeMarc belongs. The Advanced Directory of Managed Nodes and Groups page displays. Click the **Edit** link for the EdgeMarc (Figure 3-8):

Figure 3-8 Accessing the Edit Device Page (from the Advanced Directory)



Or

- Select the EdgeMarc in the device tree and select **Operation** > **Edit EdgeMarc Attributes** from the menu bar(Figure 3-9).

Figure 3-9 Operation > Edit EdgeMarc Attributes

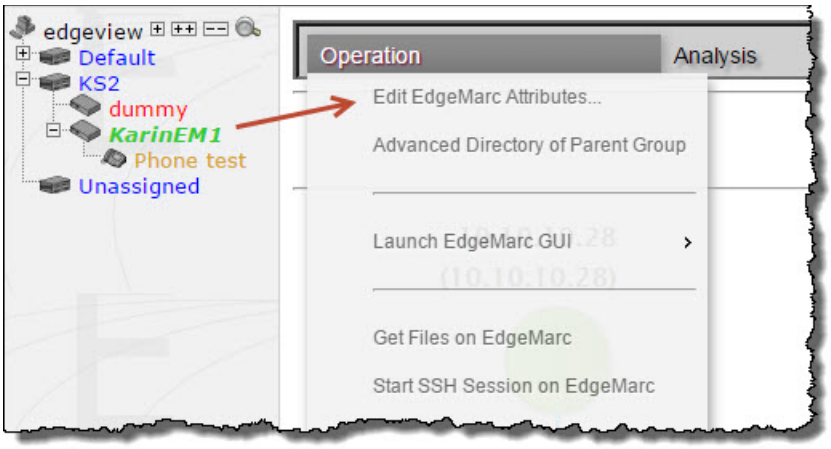
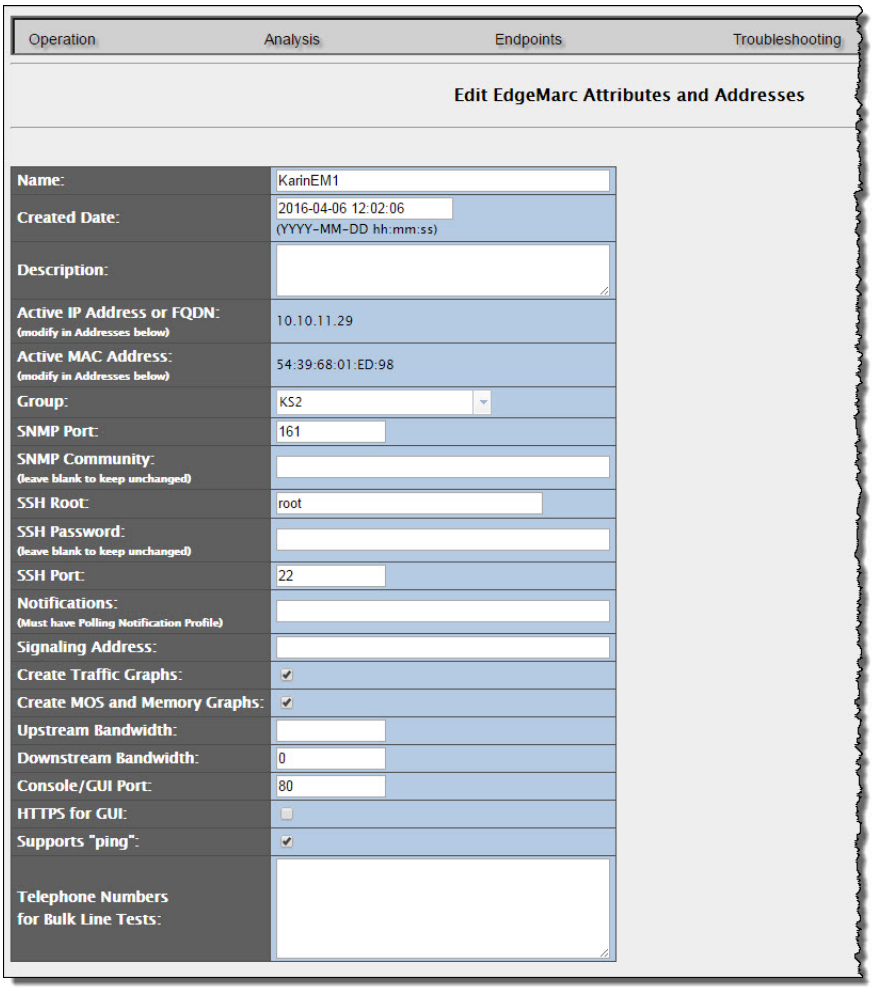


Figure 3-10 Edit Device Page



2. Edit the values on the page and click **Save**. Refer to Table 3-1 (earlier in this section) for descriptions of the fields on the Add/Edit Device page.

Adding an Additional IP Address

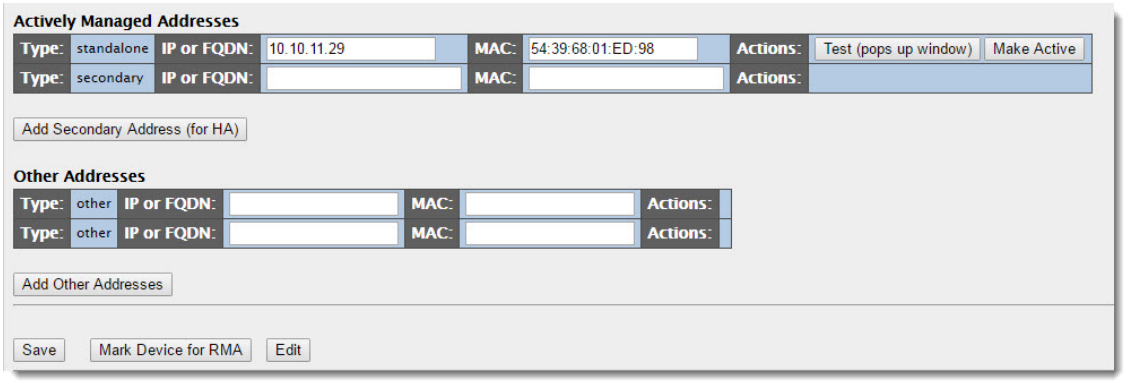
If the EdgeMarc is configured with WAN Link Redundancy or High Availability, enter an additional IP address or MAC address as follows:

1. On the Edit EdgeMarc Attributes and Addresses page (Figure 3-11), click the **Add Secondary Addresses (for HA)** button at the bottom of the page.

   Or

2. Click **Add Other Address**.
3. Enter an additional IP Address or FQDN.
4. Click **Save**.

Figure 3-11 Adding an Additional IP/MAC Address



Deleting an EdgeMarc from EdgeView

To delete an EdgeMarc from the device tree and EdgeView database:

1. Open the Advanced Directory of Nodes and Groups page for the EdgeMarc in either of the following ways:
   - From the device tree, select the group to which the EdgeMarc belongs.

     Or

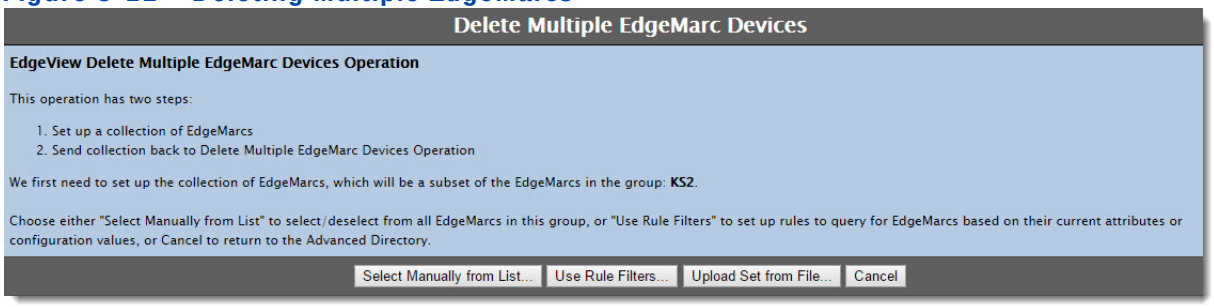
   - Select the EdgeMarc in the device tree and select **Operation** > **Advanced Directory of Parent Group** from the menu bar.
2. Click the **Delete** link for the EdgeMarc.
3. Confirm the deletion. The EdgeMarc will be removed from the device tree and from the EdgeMarc Nodes list on the Advanced Directory of

Nodes and Groups page. It will also be removed from the EdgeView database.

Deleting Multiple EdgeMarcs

1. From the device tree, select the parent group which contains the EdgeMarcs you want to delete. The Advanced Directory of Managed Nodes and Groups page displays.
2. Choose **Node Operations** > **Delete EdgeMarcs** from the menu bar (Figure 3-12).

Figure 3-12 Deleting Multiple EdgeMarcs



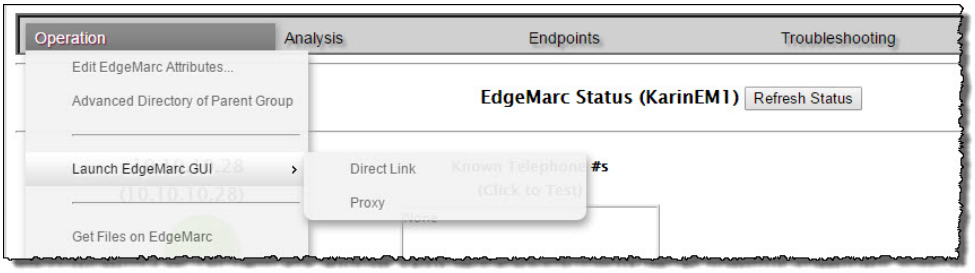
3. Follow the on-screen instructions to select a collection of EdgeMarcs.
4. Click **Delete EdgeMarc Devices**. The selected EdgeMarcs will be removed from the device tree and from the EdgeView database.

Launching the EdgeMarc GUI from EdgeView

You can launch the EdgeMarc GUI remotely from EdgeView as follows:

1. Select the EdgeMarc from the device tree.
2. Select **Operation** > **Launch EdgeMarc GUI** (Figure 3-13).

Figure 3-13 Launching the EdgeMarc GUI from EdgeView



3. Select an option for accessing the EdgeMarc GUI:
   - Select **Direct Link** to login directly to the EdgeMarc GUI.
   - Select **Proxy** to make an https connection to the EdgeMarc GUI.

When the login is successful, the EdgeMarc GUI will automatically be displayed on your screen.

Creating a Collection of EdgeMarcs

Most EdgeMarc node operations and node configuration can be performed on an EdgeMarc *collection*. By creating an EdgeMarc collection, a single task can be performed on multiple EdgeMarcs rather than individually.

You can create an EdgeMarc collection in EdgeView using any of these methods:

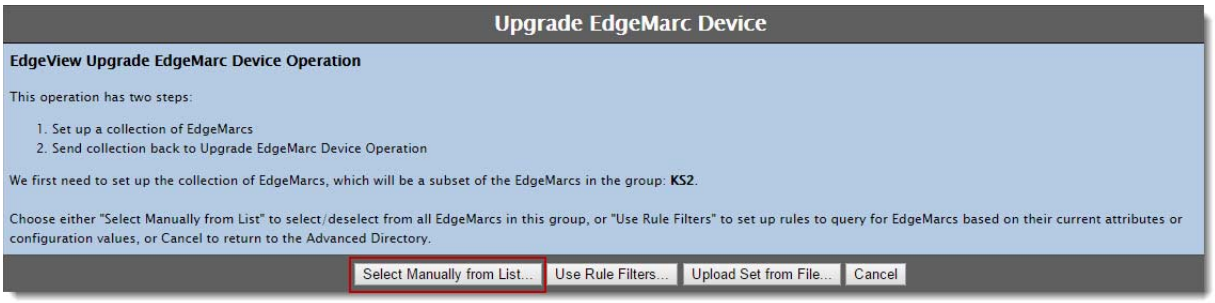
- Manually selecting EdgeMarcs to include in the collection.
- Creating Rule Filters so that EdgeView can automatically add EdgeMarcs to the collection according to matching criteria.
- Creating a collection of EdgeMarcs in an XML file and then uploading the file to EdgeView. See Creating an EdgeMarc Collection in an XML File for instructions.

Manually Selecting EdgeMarcs to Include in a Collection

To manually select EdgeMarcs to include in a collection:

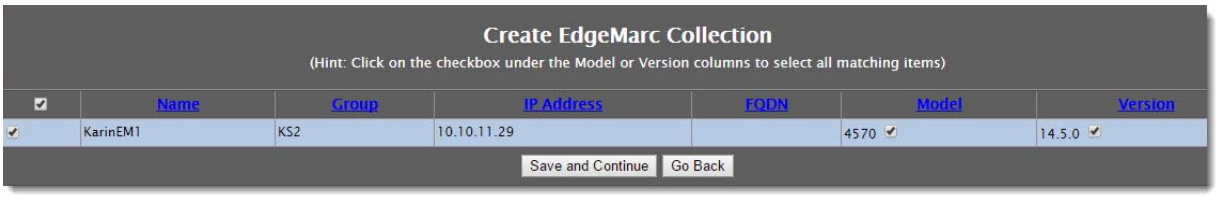
1. Start with any group-level operation by selecting a group (or tenant) in the device tree and selecting the task from the Node Operations or Node Configurations menu. For example, select **Node Operations** > **Upgrade EdgeMarcs**. The EdgeMarc device operation screen displays for the task (Figure 3-14).

Figure 3-14 Upgrade EdgeMarc Device Operation Screen



2. Click **Select Manually from List**. The Create EdgeMarc Collection screen displays (Figure 3-15). Initially, all EdgeMarcs in the group are selected.

Figure 3-15 Manually Creating an EdgeMarc Collection

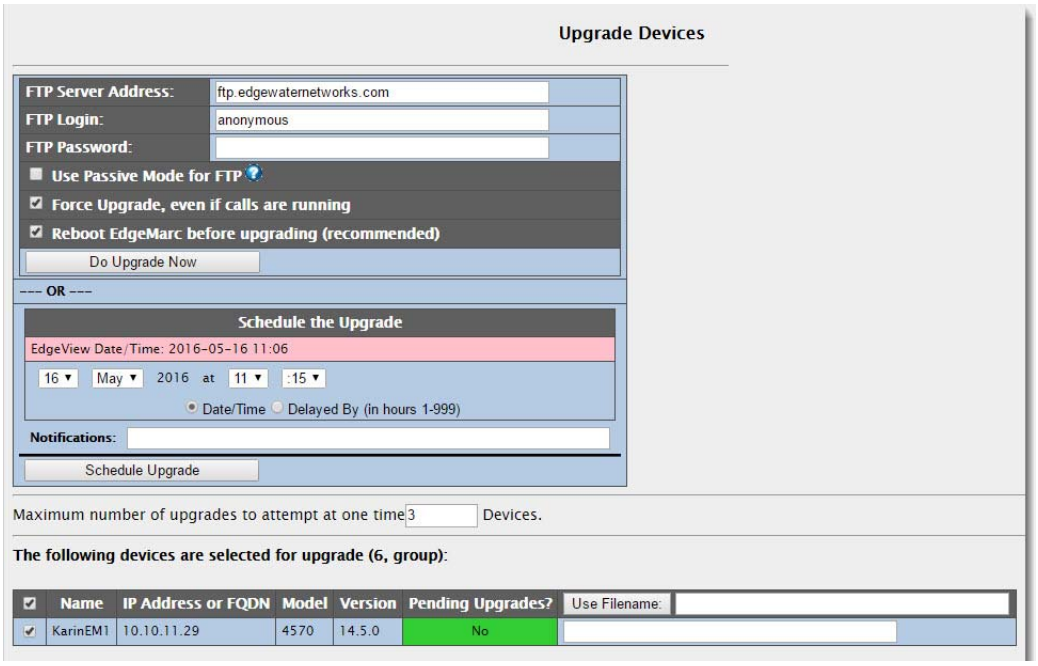


Tip

Click on the column titles to sort the list by that subject. For example, click Version to sort the list by version number.

3. Enable/disable the checkboxes to add or remove EdgeMarcs from the collection.
4. Click **Save and Continue**. The selected EdgeMarcs will be listed at the bottom of the screen (Figure 3-16).
5. Continue to perform the EdgeMarc operation.

Figure 3-16 List of Selected Devices for the Collection



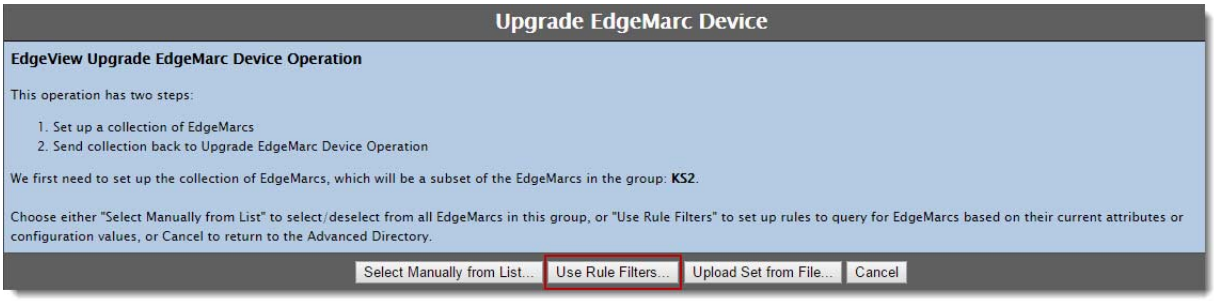
Using Rule Filters to Add EdgeMarcs to a Collection

You can set up a rule to query for EdgeMarcs based on their current attributes or configuration values. When you run the filter, EdgeMarcs which match the rule are automatically added to a collection. You can specify matching criteria for adding an EdgeMarc to a collection based upon the EdgeMarc Name, Group, Address, Model, Version, or a specific variable and value found in the config file.

To specify a Rule Filter:

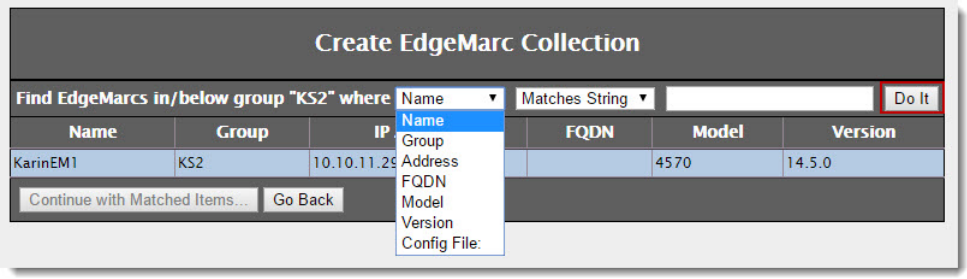
1. Start with any group-level operation by selecting a group (or tenant) in the device tree and selecting the task from the Node Operations or Node Configurations menu. For example, select **Node Operations** > **Upgrade EdgeMarcs**. The EdgeMarc device operation screen is displayed. Figure 3-17 shows an example of the EdgeMarc device operation screen for the Upgrade EdgeMarcs task.

Figure 3-17 Upgrade EdgeMarc Device Operation Screen - Use Rule Filters



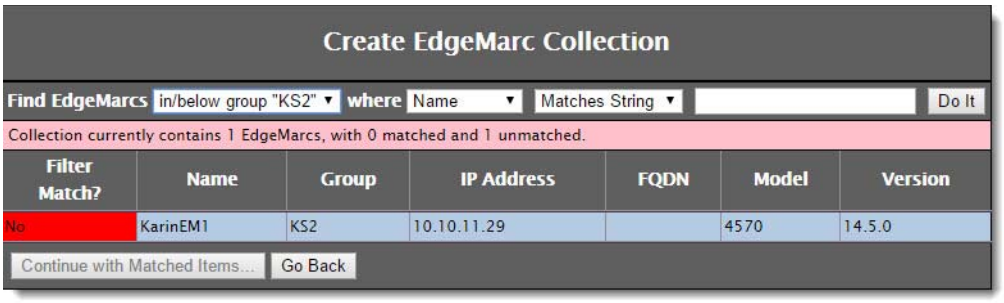
2. Click **Use Rule Filters**. The Create EdgeMarc Collection screen displays.
3. Select a filter from the drop-down menu and select a matching string (Figure 3-18).

Figure 3-18 Creating a Rule Filter



4. Click **Do it**. The EdgeMarcs that match the filter criteria will be flagged in green in the list of EdgeMarcs (Figure 3-19).

Figure 3-19 Creating a Rule Filter - Complete



5. Click **Continue with Matched Items**. The selected devices will be listed at the bottom of the screen. Refer to Figure 3-16. Click **Go Back** to discard your changes and return to the previous screen.
6. Continue to perform the EdgeMarc operation.

Creating an EdgeMarc Collection in an XML File

In addition to using the EdgeView GUI to create an EdgeMarc collection for group-level operations, you can also create an EdgeMarc collection separately in an XML file and then upload the file to EdgeView.

The format of the XML file must look like this:

```
<EDGEVIEW>
  <EDGEMARC>
    <ADDRESS> some IP address</ADDRESS>
</EDGEMARC>
  <EDGEMARC>
    <NAME>some EM name</NAME>
  </EDGEMARC>
  <EDGEMARC>
    <FQDN> some Fully Qualified Domain Name</FQDN>
  </EDGEMARC>
  <EDGEMARC>
    <MACADDR> some MAC address</MACADDR>
  </EDGEMARC>
</EDGEVIEW>
```

The following tags are supported to determine which EdgeMarc to match: <NAME>,<ADDRESS>,<MACADDR>, or <FQDN>

To create an EdgeMarc collection in an XML file:

1. Create an XML document that includes the required EDGEVIEW tags at the start and end of the document.
2. Inside the EDGEVIEW tags, add EDGEMARC tags for each EDGEMARC you wish to be part of the collection.
3. Inside each EDGEMARC tag, include one of the tags to select which EdgeMarc to match. This includes one of: <NAME>,<ADDRESS>,<MACADDR>, or <FQDN>

4. Enter the value to match against between the start and end tags for instruction #3.

Example:

Here's an example of how to add two EdgeMarcs to the file. One uses the IP address 192.168.2.1 and the other uses the <NAME>. The file would look like this:

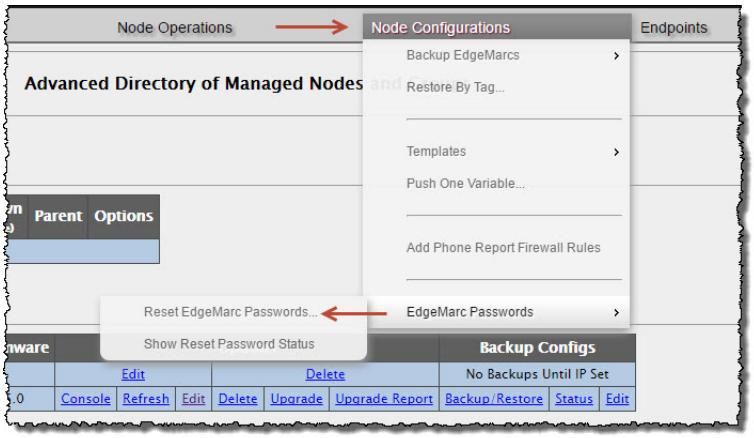
```
<EDGEVIEW>
  <EDGEMARC>
    <ADDRESS>192.168.2.1</ADDRESS>
</EDGEMARC>
  <EDGEMARC>
    <NAME>MyEM</NAME>
  </EDGEMARC>
</EDGEVIEW>
```

Uploading an EdgeMarc Collection XML File to EdgeView

Once you have created an XML collection file, you can upload the file to EdgeView as follows:

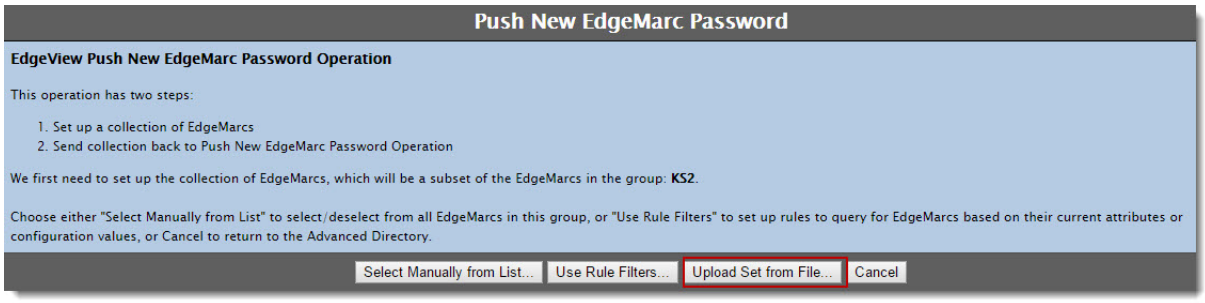
1. Start with any group-level operation by selecting a group (or tenant) in the device tree. For example, select **Node Configurations** > **Passwords** > **Reset EdgeMarc Passwords** (Figure 3-20).

Figure 3-20 Uploading an XML File for an EdgeMarc Collection



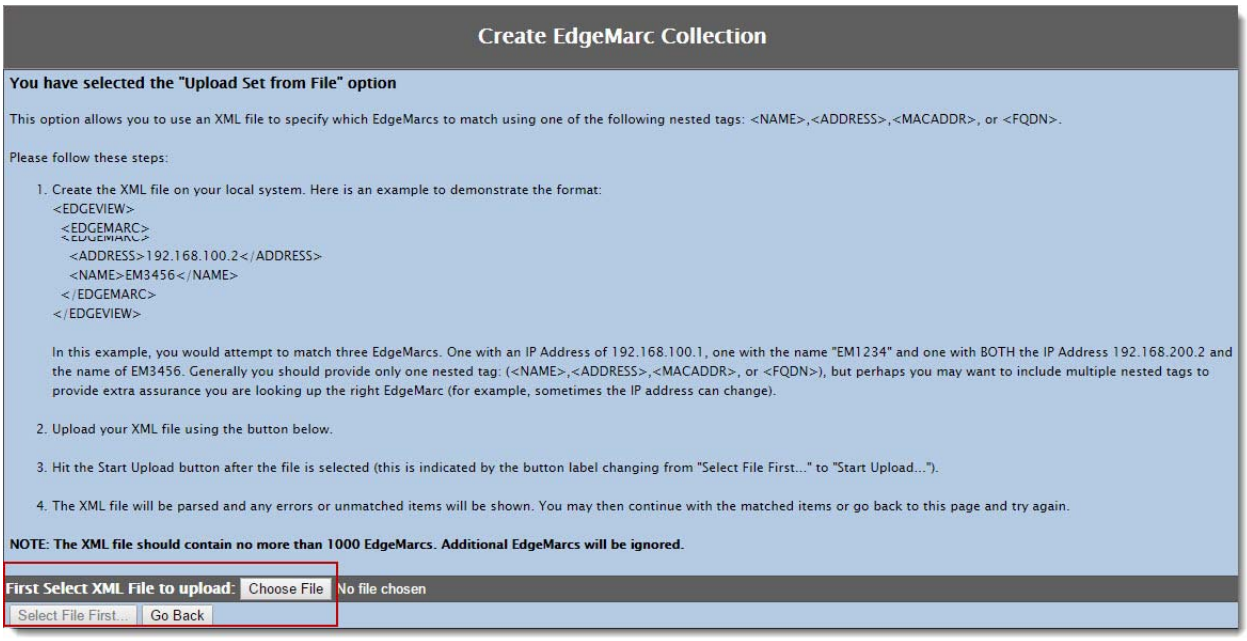
2. In the main EdgeMarc operation page, click **Upload Set from File** (Figure 3-21).

Figure 3-21 Uploading an XML Collection File



3. Click **Upload Set from File**. The Create EdgeMarc Collection page (Figure 3-22) displays.

Figure 3-22 Create EdgeMarc Collection Page



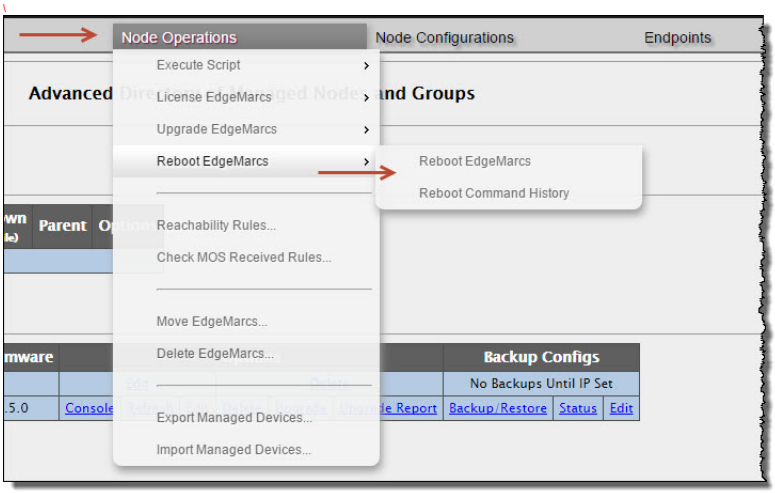
4. Click **Browse** and select the XML collection file to upload from your local drive.
5. Click **Start Upload**.
6. If there are errors, they will be shown. Correct the errors and upload the file again by clicking **Go Back and Retry Import Again**.
7. When upload is successful, click **Continue with Successfully Matched Items**.
8. Continue to perform the EdgeMarc operation.

Rebooting an EdgeMarc

EdgeView can remotely reboot an EdgeMarc or collection of EdgeMarcs. To view a table listing the history of the LAST reboot command status for each of the EdgeMarcs, select **Node Configuration** > **Reboot EdgeMarcs** > **Reboot Command History**.

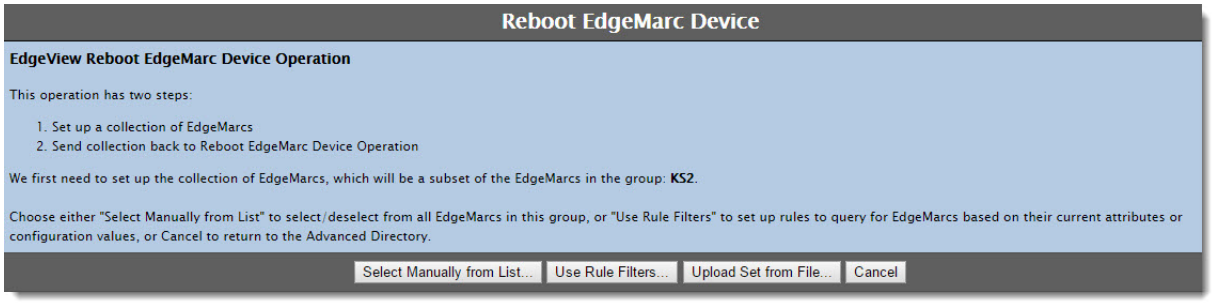
1. Select the group which contains the EdgeMarc or EdgeMarcs from the device tree.
2. Select **Node Operations** > **Reboot EdgeMarcs** > **Reboot EdgeMarcs** (Figure 3-23).

Figure 3-23 Rebooting EdgeMarcs



3. Set up a collection of EdgeMarcs using the information in Creating a Collection of EdgeMarcs as a guide.

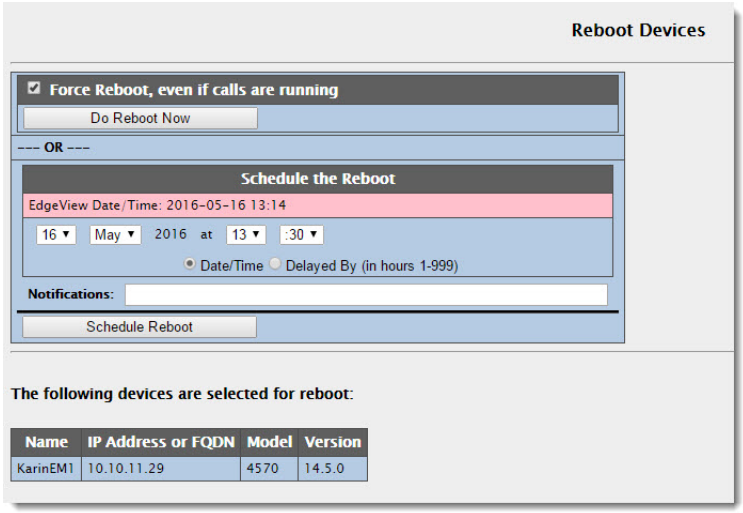
Figure 3-24 Reboot Devices - Create a Collection of EdgeMarcs



4. To reboot an EdgeMarc on the Reboot Devices screen, choose from the following options (Figure 3-25):
   - Select the **Force Reboot, even if calls are running** checkbox. Otherwise, EdgeView will wait until there are no calls currently running before doing the reboot.
   - Click **Reboot Now** to perform an immediate reboot.

- To schedule the reboot, enter a date and time for the reboot and click **Schedule Reboot**.
- In the **Notifications** box, enter email addresses which will be sent an email notification when the task has completed.

Figure 3-25 Reboot Devices Page

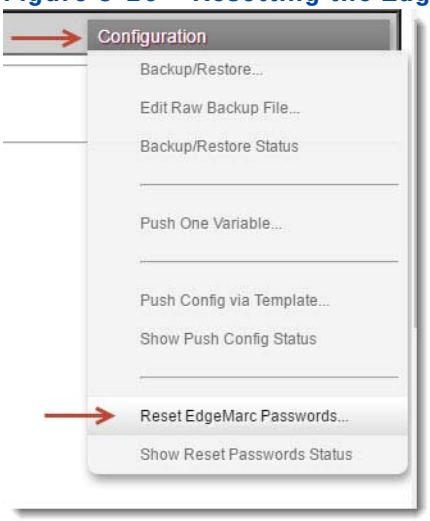


Changing the EdgeMarc Password

To change the password for the EdgeMarc GUI root user and read-only user in EdgeView:

1. Open EdgeView and select the EdgeMarc from the device tree. You can also change the password for a group of EdgeMarcs or all EdgeMarcs by selecting the group or tenant from the device tree.
2. On the EdgeMarc Status page, select **Configuration** > **Reset EdgeMarc Passwords** (Figure 3-26).

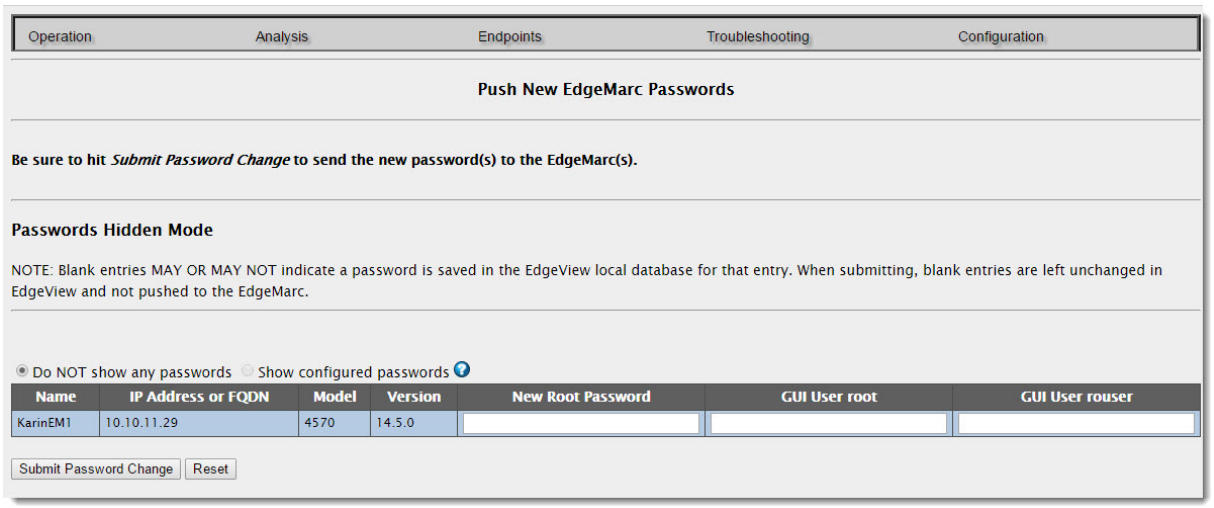
Figure 3-26 Resetting the EdgeMarc Password



3. In the Push New EdgeMarc Passwords page, enter new values for the **New Root Password**, **GUI User root** and **GUI User rouser** read-only user (Figure 3-27). Leave these fields blank if there is no change.
4. Click **Submit Password Change** to save the new password(s) or click **Reset** to discard your changes.
5. Choose **Configuration** > **Show Reset Passwords Status** to view the status of the password change operation.

If the password change is successful, the Push Password Status page will indicate in the **Comments** field that the password(s) were set.

Figure 3-27 Changing the Password for the Root User and Read-Only User

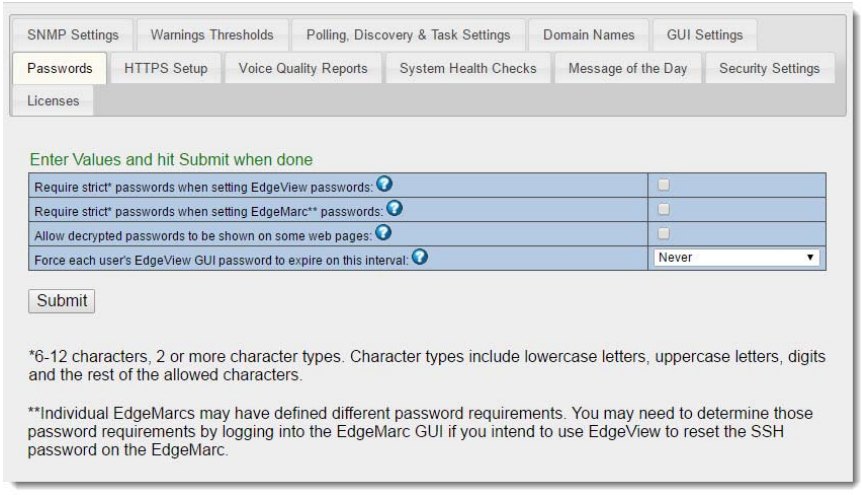


Displaying Decrypted Passwords in the EdgeView GUI

By default, passwords on the Push New EdgeMarc Passwords page and Add/Edit Devices page are encrypted. To see these passwords, you must allow them to be displayed as follows:

1. Choose **EV System** > **System Settings**.

Figure 3-28 EV-Systems Settings Passwords Tab



2. Select the **Passwords** tab.
3. Select the checkbox for **Allowed decrypted passwords to be shown on some web pages**.

4. Click **Submit**.

Marking a Device for RMA

If an EdgeMarc is defective and being replaced, click the **Mark Device for RMA** button on the Add/Edit Device page to stop the EdgeMarc from being actively polled. This state will allow the device to be replaced later with a new EdgeMarc.

Pre-Provisioning an EdgeMarc

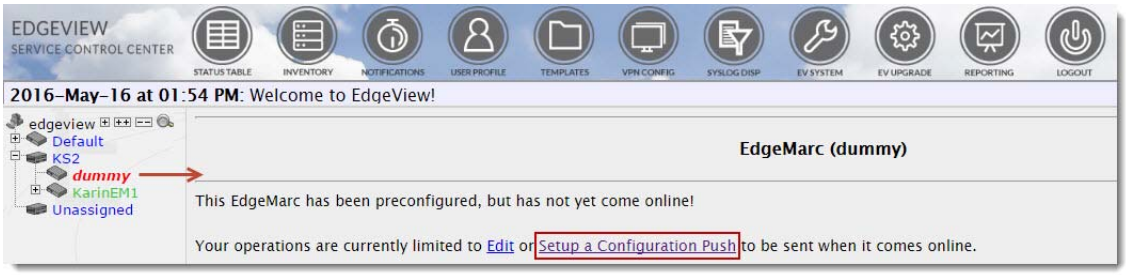
You can pre-provision an EdgeMarc in EdgeView so that upon discovery, EdgeView automatically pushes a configuration to the EdgeMarc and assigns it to the proper group. When you pre-provision an EdgeMarc, EdgeView puts the EdgeMarc in a holding state where it shows up in the device tree but is not active on the network. The EdgeMarc will be listed in red in the device tree until it is discovered, provisioned, and actively managed by EdgeView.

To push a configuration to the EdgeMarc during auto-discovery, you must first generate an EdgeMarc configuration template using the EdgeMarc Template Manager. See Chapter 7, *Using Templates*.

To pre-provision an EdgeMarc:

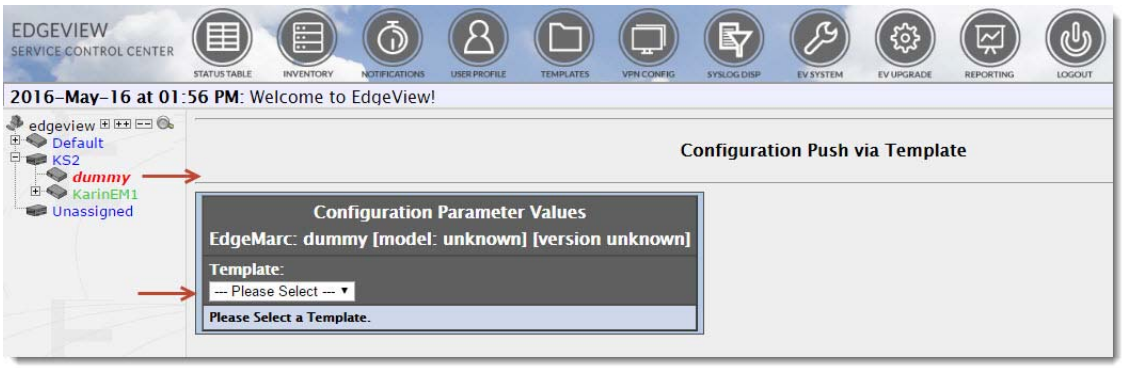
1. Add an EdgeMarc using the MAC address or hostname (if known). This allows the EdgeMarc to be auto-discovered when it is put on the network. Initially, the EdgeMarc will appear in red in the EdgeView device tree. See Adding an EdgeMarc.
2. Select the EdgeMarc from the device tree (Figure 3-29).

Figure 3-29 Pre-Provisioning an EdgeMarc



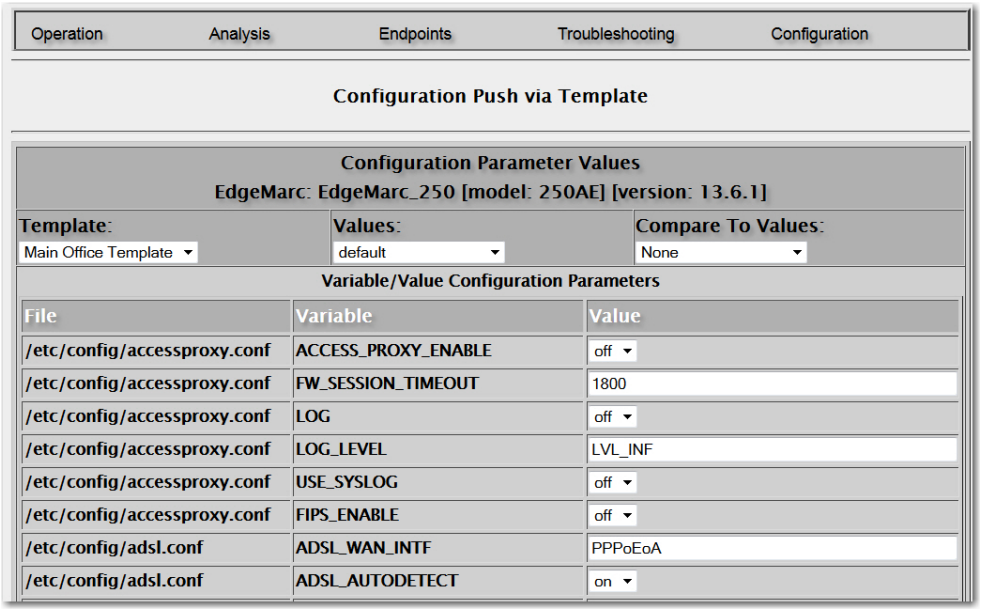
3. Click **Setup a Configuration Push**.
4. In the Configuration Push Via Template screen, select a template from the drop-down menu (Figure 3-30).

Figure 3-30 Selecting a Configuration Template to Push



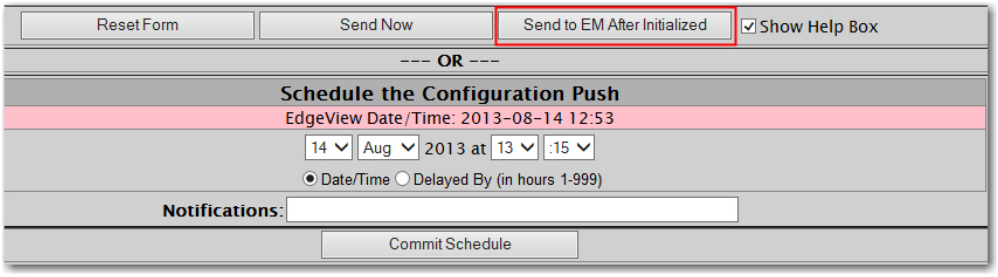
5. After a few moments, the parameters for the template display (Figure 3-31).

Figure 3-31 Configuration Push Via Template Page



6. Change the default values for variables as needed. See Editing Variables for an EdgeMarc Configuration Template.
7. Scroll to the bottom of the Configuration Push via Template page and click **Send to EM After Initialized** (Figure 3-32).

Figure 3-32 Send to EM After Initialized



When the EdgeMarc comes online, EdgeView will auto-discover it and display a message in the syslog that the EdgeMarc is alive. EdgeView will then push the configuration to the EdgeMarc. The EdgeMarc will be fully available on the network and manageable by EdgeView.

For more details about EdgeMarc configuration templates, see Chapter 7, *Using Templates*.

Backing Up and Restoring an EdgeMarc Configuration

You can store multiple configurations for the EdgeMarcs being managed by EdgeView in the EdgeView local database. This is useful in the unlikely event that the database is erased or to rollback changes for any given EdgeMarc to a known working configuration.

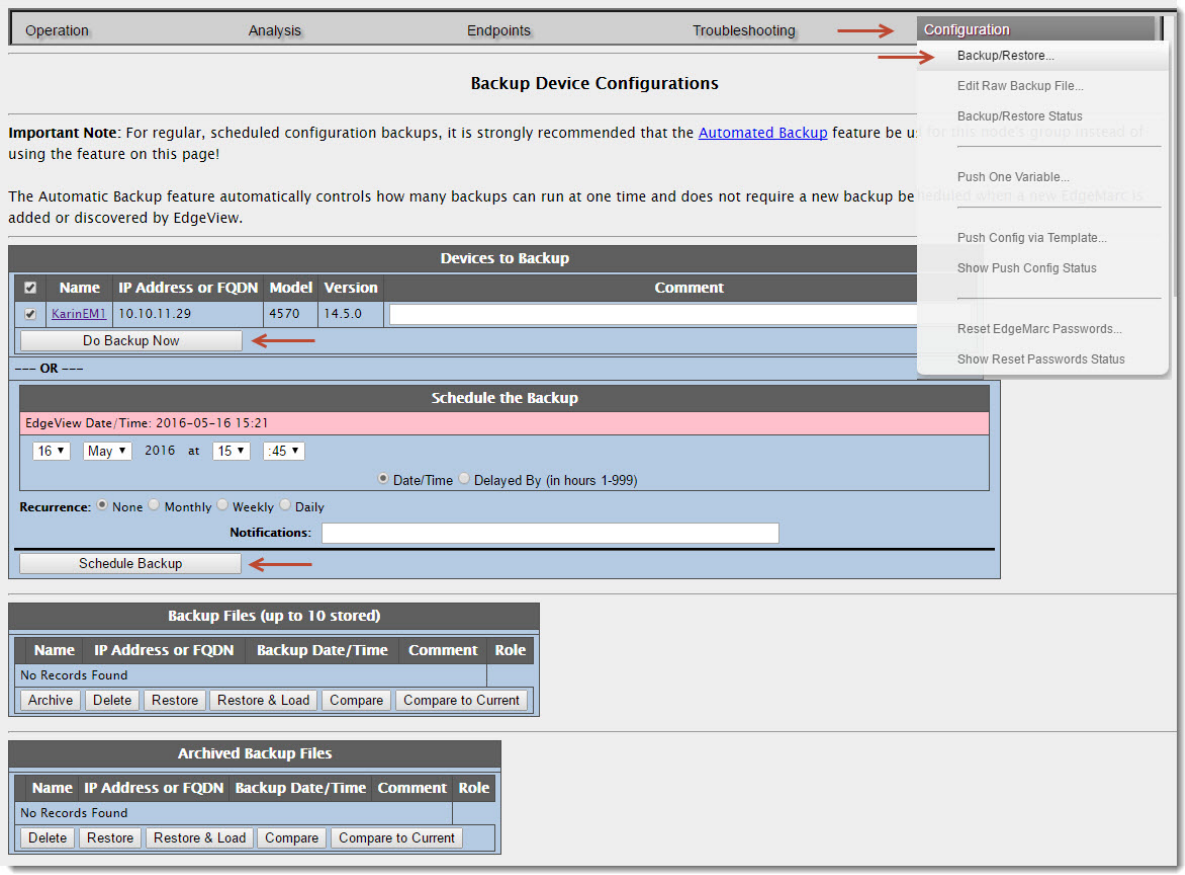
It is recommended that you create a backup file after you make any configuration changes to an EdgeMarc. You can backup the configuration for individual EdgeMarcs or EdgeMarcs which are nested in groups. The backup does not disrupt network operation.

Using EdgeView, you can backup an EdgeMarc configuration on-demand or according to a preset backup schedule. Additional backup management capabilities are also available including the ability to compare two saved configurations or compare a saved configuration with the current configuration of a selected EdgeMarc.

To access the backup and restore page:

1. Select an EdgeMarc from the device tree.
2. Choose **Configuration** > **Backup and Restore** (Figure 3-33).

Figure 3-33 Backing Up and Restoring an EdgeMarc



Up to 10 previous backups per EdgeMarc are stored and available to view. You can compare two saved configurations or compare a saved configuration with a stored configuration.

Backing Up an EdgeMarc (On-Demand)

To backup the EdgeMarc configuration on-demand:

1. Select the EdgeMarc from the device tree and select **Configuration** > **Backup and Restore** from the menu bar (Figure 3-33).
2. On the EdgeMarc Backup and Restore page, click **Do Backup Now** to start the backup. EdgeMarc provides the results of the backup request at the completion of the operation.
3. Once the backup is complete, click the **Click Here to Return to the main Backup/Restore** page. If this is the first time you have backed up this EdgeMarc, the backed up file will be listed in the Archived Backup Files section. If there is already a backup file for the EdgeMarc, subsequent backup files will be listed in the Backup Files (up to 10 stored) section on the page.

Backing Up an EdgeMarc Configuration (Scheduled)

To set a schedule for automatically backing up the EdgeMarc configuration:

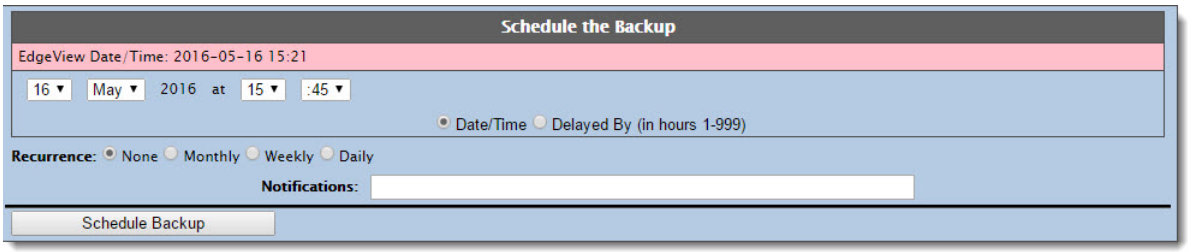
1. Select the EdgeMarc from the device tree and select **Configuration > Backup and Restore** from the menu bar (Figure 3-33).
2. In the EdgeMarc Backup and Restore page, go to the **Schedule the Backup** section and configure the settings for the backup. Refer to Table 3-3.

Table 3-3 Configuring Backup Settings

Setting	Description
Date and Time	Use the drop down boxes to select the date and time you want to start the backup.
Date/Time or Delayed By (in hours 1-999):	Choose **Date/Time** to do the backup on the set date and time or choose **Delayed By** to set the number of hours you want to delay the scheduled backup.
Recurrence	Select the frequency for doing the automatic backup.
Notifications	Enter comma-separated email addresses where you want to send automatic backup notifications.

3. Click **Schedule Backup.** You will be asked to confirm the schedule.
4. Click **OK**.

Figure 3-34 EdgeMarc Configuration Automatic Backup



Scheduling a Daily Backup of All EdgeMarcs (Tenant or Group Level)

You can create an automatic backup rule for performing daily backups at the tenant or group level. This is a much safer and more efficient backup method than doing individual backups for two reasons:

- The number of backup requests sent at one time is automatically controlled for all EdgeMarcs in the group.
- When new EdgeMarcs are auto-discovered or added to the group, they are automatically backed up on the next backup cycle.

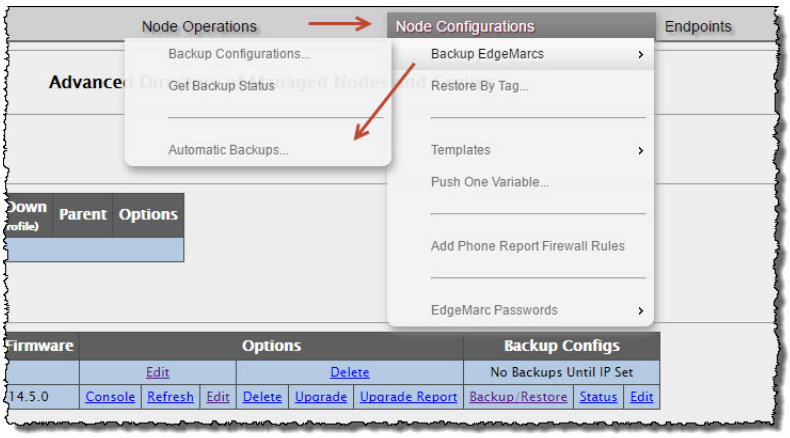
It is recommended that an automatic backup rule be created for each tenant (top level group) with “propagation to all subgroups” turned ON. For very large tenants, it may be more efficient to distribute the load by defining multiple automatic backup rules to run at different times of the day for sub-groups rather than a single rule that propagates to all sub-groups.

If you already have backups scheduled, consider canceling and creating an automatic backup rule instead.

To create an automatic backup rule:

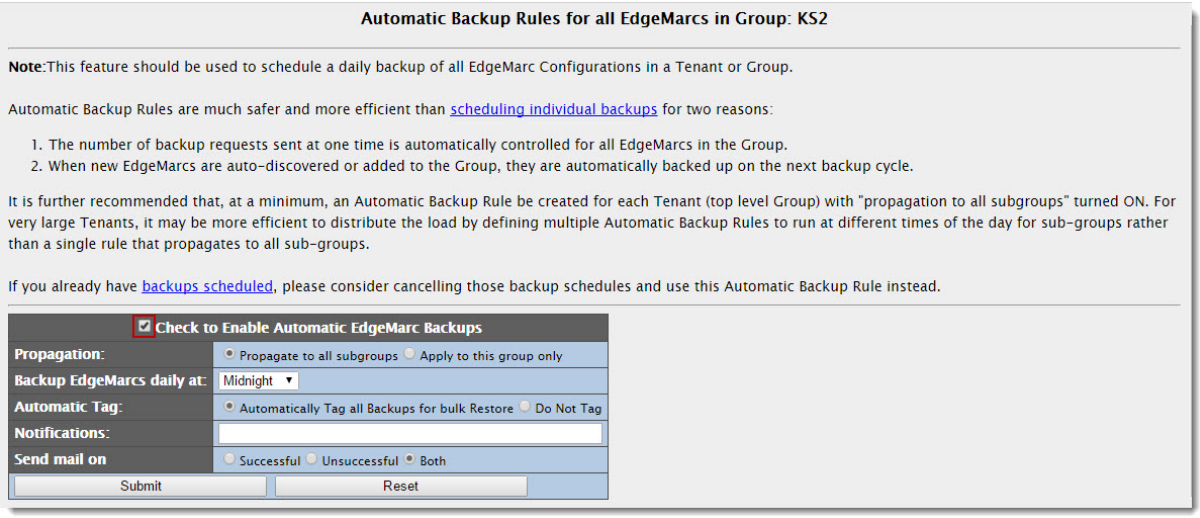
1. Select the EdgeMarc tenant or group from the device tree.
2. Choose **Node Configurations** > **Backup EdgeMarcs** > **Automatic Backups** (Figure 3-35).

Figure 3-35 Accessing the Automated Backup Page



3. In the Automatic Backup Rules page, select the checkbox for **Automatic EdgeMarc Backups** (Figure 3-36).

Figure 3-36 Automatic Backup Rules Page



4. Table 3-4 describes configuration fields.

Table 3-4 Automatic Backup Settings

Setting	Description
Propagation	Select whether to propagate the backup to all subgroups or only to the selected group.
Backup EdgeMarcs daily at	Choose the time of day to do the backup.
Automatic Tag	Choose whether to automatically tag all backups for build restore or choose **Do Not Tag**.
Notifications	Enter comma-separated email addresses where you want to send automatic backup notifications.
Send mail on	Click the radio button to select the email backup notices you want to receive: ■ Successful ■ Unsuccessful ■ Both

5. Click **Submit** to submit the rule or click **Reset** to reset the settings and start over. Once the new rule has been accepted, Automatic Backup Rules Saved Successfully will display.

Backing Up an EdgeMarc Configuration (Group Level)

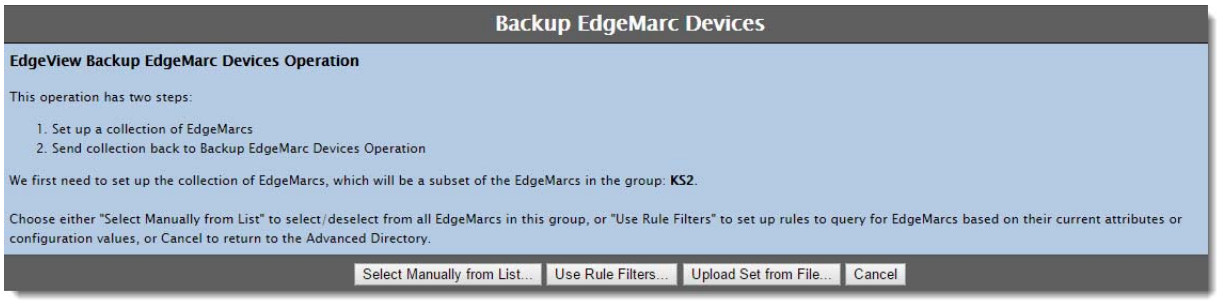
Caution

Do not use this method to backup EdgeMarcs on an ongoing basis. Instead, use the Automatic Backups feature. See Scheduling a Daily Backup of All EdgeMarcs (Tenant or Group Level).

To backup EdgeMarcs at the group level:

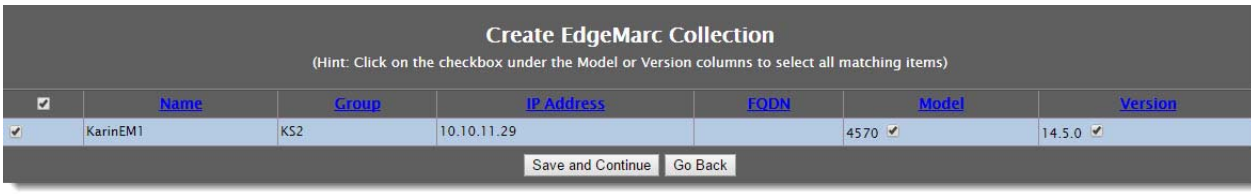
1. Select the group from the device tree.
2. Choose **Node Configurations** > **Backup EdgeMarcs**.
3. Click **Backup Configurations**.
4. In the Backup EdgeMarc Devices screen, click **Select Manually From List**.

Figure 3-37 Backup Configurations Screen



5. In the Create EdgeMarc Collection screen, select the group(s) to be backed up.

Figure 3-38 Create EdgeMarc Collection Screen

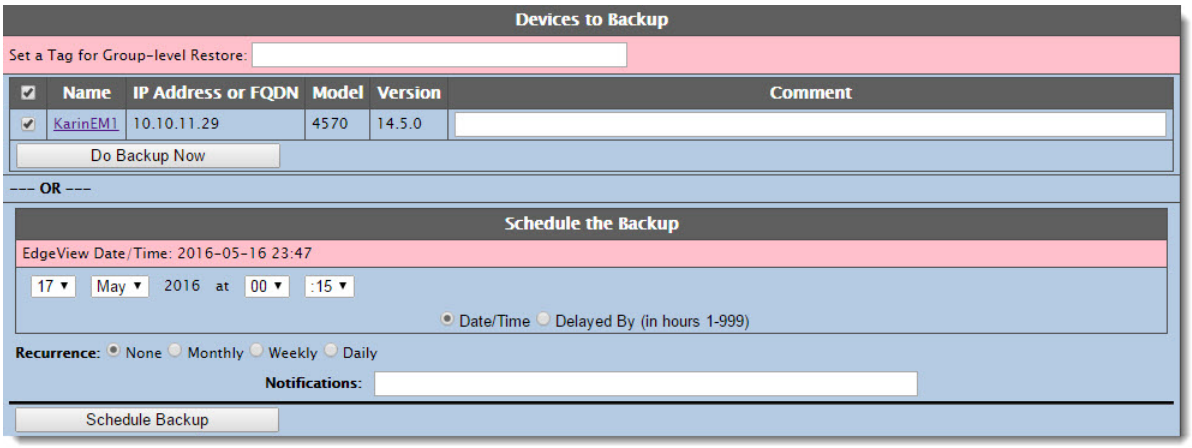


Tip

Click the column titles to sort the list of EdgeMarcs by Name, Group, IP Address, FQDN, Model or Version.

6. Click **Save and Continue**.
7. In the Devices to Backup screen, enter a tag to help identify this backup file.
8. Click **Do Backup Now** or **Schedule Backup** (Figure 3-39).

Figure 3-39 Tagging a Group Level Backup File



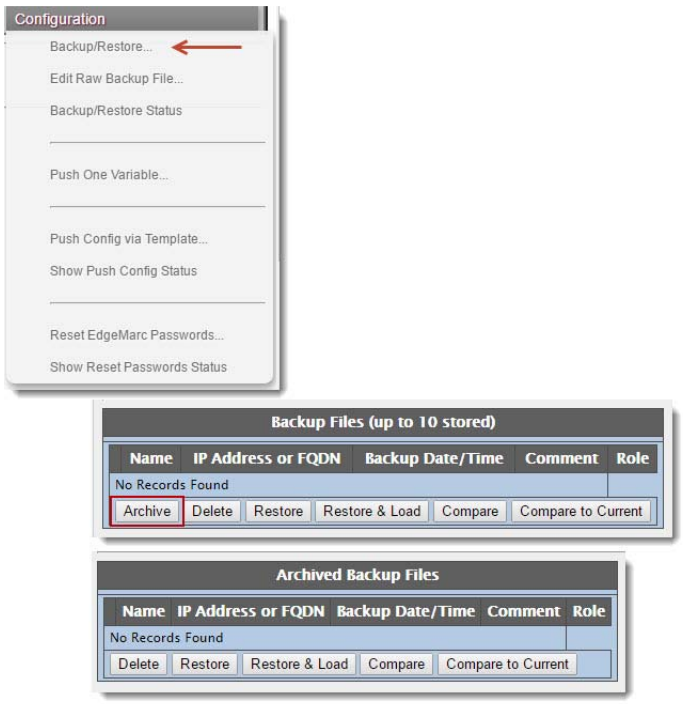
Managing EdgeMarc Backup Files

Archived backup files can only be deleted manually whereas backup files in the Backup File list have a rule that automatically deletes the oldest backup file once there are 10 backup files and a new one is added. If you do not want a backup file to be automatically deleted, move it to the Archived Backup Files list.

Moving a Backup File to the Archived Backup File List

1. Choose **Configuration** > **Backup/Restore**. In the Backup Files list on the Backup Device Configuration page, select the checkbox next to the backup file you want to move.

Figure 3-40 Backup and Archived Files



2. Click **Archive** at the bottom of the Backup File list. The file will now be listed in the Archived Backup Files list.

Deleting an Archived Backup File

1. In the Archive Backup Files list, select the checkbox next to the backup file you want to delete from the Archive Backup File list.
2. Click **Delete**.

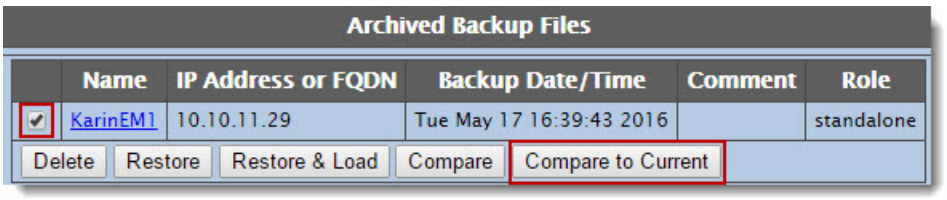
Comparing EdgeView Configuration Backup Files

To help you easily identify mis-configurations, EdgeView can compare the working EdgeMarc configuration file against a backup file or archived backup file. It can also compare backup files against archived backup files. EdgeView compares the values of variables in the files and lists the differences in a table.

To compare the working EdgeMarc configuration file with a backup file or archived backup file:

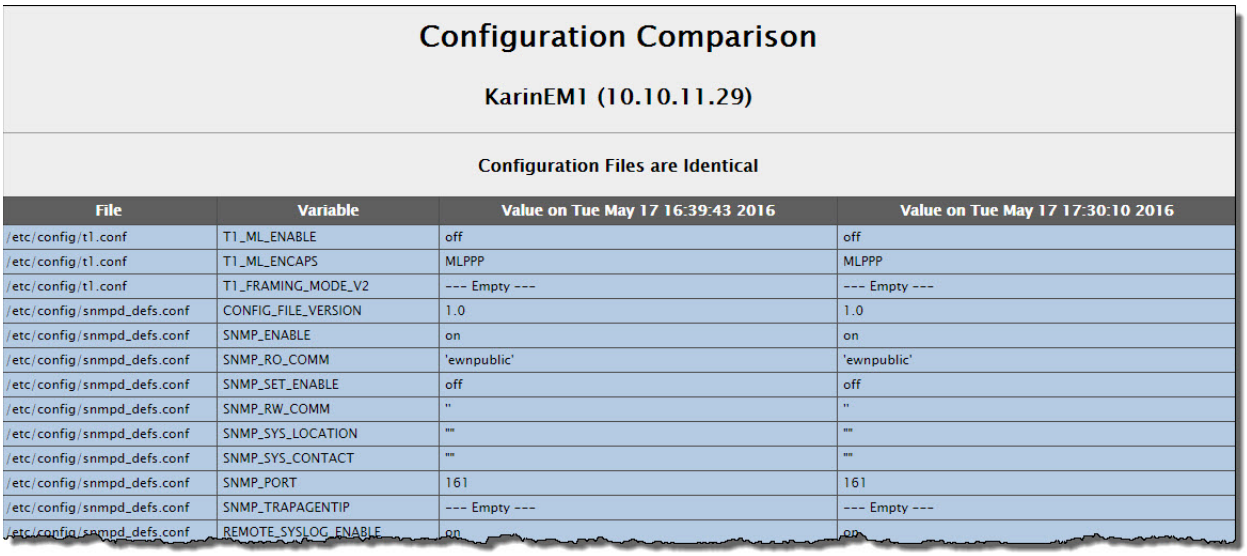
1. Select **Configuration** > **Backup and Restore**.
2. In the Backup Device Configurations page, select the file you want to compare from the Backup Files list or the Archived Backup Files list.

Figure 3-41 Comparing Backup Files



3. Click **Compare to Current.** Any differences will be listed in the Configuration File Differences table (Figure 3-42).

Figure 3-42 Configuration Comparison Results



Configuration Comparison

KarinEM1 (10.10.11.29)

Configuration Files are Identical

File	Variable	Value on Tue May 17 16:39:43 2016	Value on Tue May 17 17:30:10 2016
/etc/config/t1.conf	T1_ML_ENABLE	off	off
/etc/config/t1.conf	T1_ML_ENCAPS	MLPPP	MLPPP
/etc/config/t1.conf	T1_FRAMING_MODE_V2	--- Empty ---	--- Empty ---
/etc/config/snmpd_defs.conf	CONFIG_FILE_VERSION	1.0	1.0
/etc/config/snmpd_defs.conf	SNMP_ENABLE	on	on
/etc/config/snmpd_defs.conf	SNMP_RO_COMM	'ewnpublic'	'ewnpublic'
/etc/config/snmpd_defs.conf	SNMP_SET_ENABLE	off	off
/etc/config/snmpd_defs.conf	SNMP_RW_COMM	''	''
/etc/config/snmpd_defs.conf	SNMP_SYS_LOCATION	""	""
/etc/config/snmpd_defs.conf	SNMP_SYS_CONTACT	""	""
/etc/config/snmpd_defs.conf	SNMP_PORT	161	161
/etc/config/snmpd_defs.conf	SNMP_TRAPAGENTIP	--- Empty ---	--- Empty ---
/etc/config/snmpd_defs.conf	REMOTE_SYSLOG_ENABLE	on	on

Restoring the EdgeMarc Configuration



Note

You can only restore a configuration on an individual EdgeMarc basis. You cannot restore a configuration at the group or tenant level.

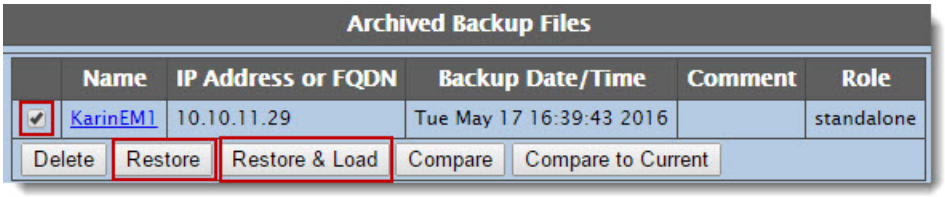
To restore the configuration for an individual EdgeMarc:

1. Select the EdgeMarc from the device tree and select **Configuration** > **Backup and Restore** from the menu bar. Refer to Figure 3-33. If you

are using sub-groups, your current position in the hierarchy can be found at the top of the screen next to the Current Level heading.

2. From the Backup Files list or Archived Backup Files list, select the file you want to restore.
3. Click **Restore** or **Restore & Load**, where **Restore & Load** restarts the network and **Restore** does not restart the network (Figure 3-43).

Figure 3-43 Restoring a Backup File



If you select **Restore & Load,** EdgeView will send a copy of the configuration to the EdgeMarc and then load that configuration.

Caution

Performing a configuration **Restore & Load** will interrupt voice, video, and data services since the EdgeMarc will automatically restart after downloading and installing the database configuration.

Upgrading the EdgeMarc VOS Firmware

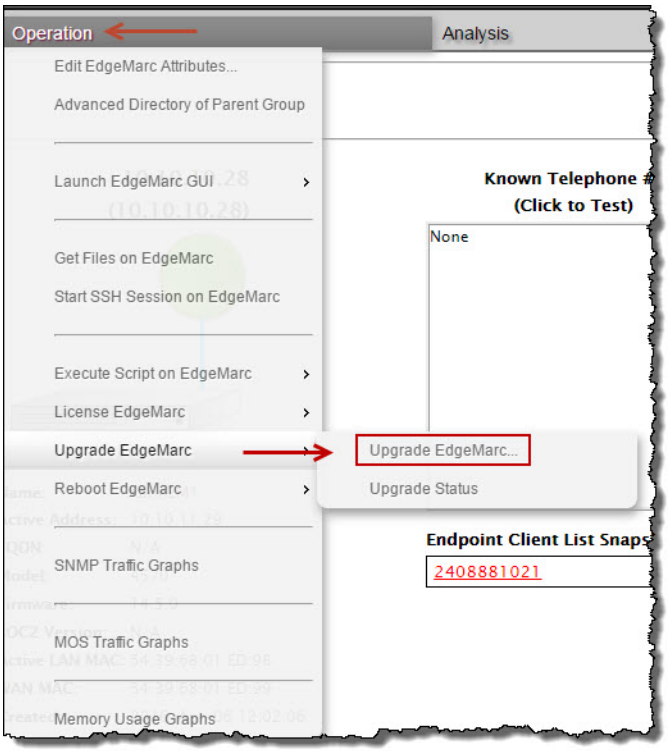
EdgeView can automatically load approved VOS firmware on an EdgeMarc or EdgeMarc group upon device boot-up. You can configure EdgeView to do a firmware upgrade on-demand or according to a set a schedule as described here. You can also configure rules for upgrading all EdgeMarcs in a group.

Upgrading the Firmware for an EdgeMarc

To upgrade an EdgeMarc to the latest VOS firmware version:

1. Select the EdgeMarc from the device tree.
2. In the EdgeMarc Status page, choose **Operation** > **Upgrade EdgeMarc** (Figure 3-44).

Figure 3-44 Upgrading an EdgeMarc



3. In the Upgrade Devices screen (Figure 3-45), specify settings for upgrading the firmware. Refer to Table 3-5.

Figure 3-45 Configuring Settings on the Upgrade Devices Screen

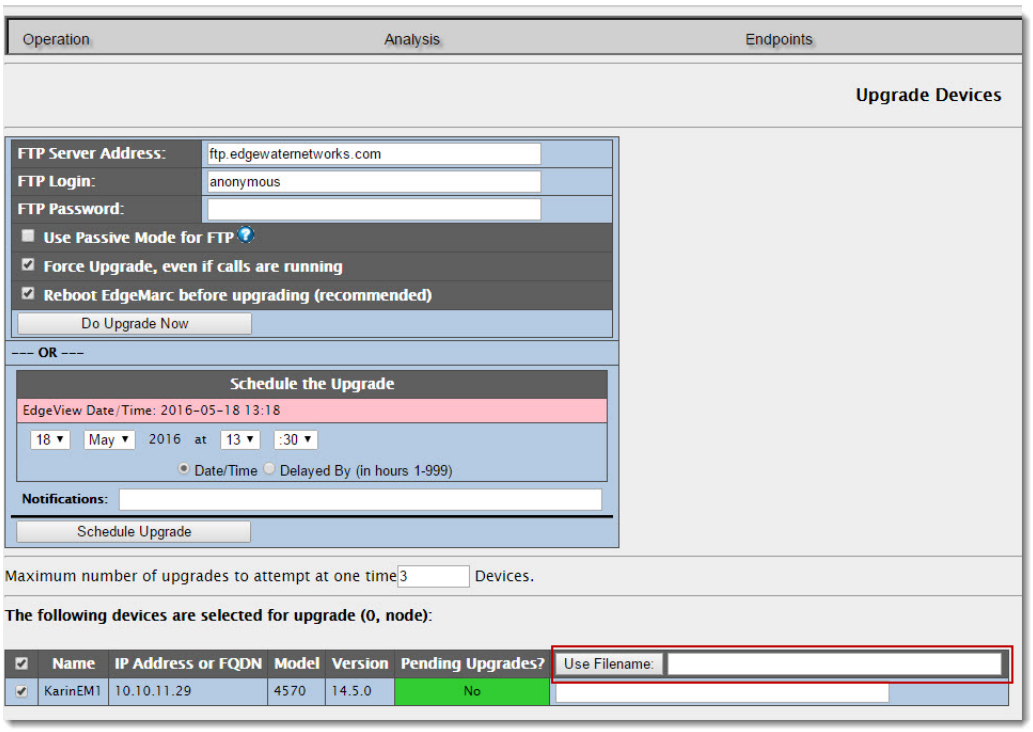


Table 3-5 Specifying Firmware Upgrade Settings

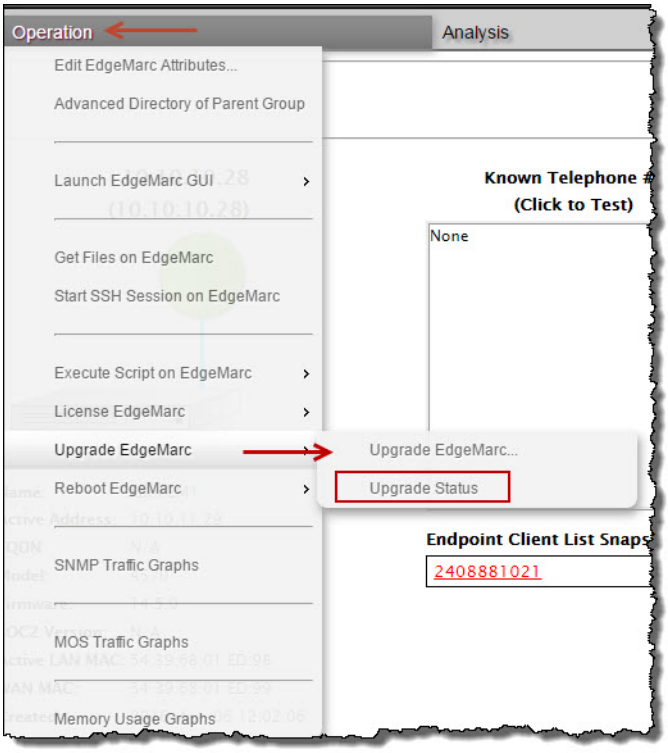
Field	Description
FTP Server Address	Enter the address for the FTP server which has the new VOS file distribution.
FTP Login	Enter the login name for the FTP server.
FTP Password	Enter the password for the FTP server.
Use Passive Mode for FTP	Enable if you want to force passive mode when the EdgeMarc uses FTP to get the new file distribution. This is disabled by default.
Force Upgrade, even if calls are running	By default, EdgeView will upgrade the EdgeMarc even if calls are running. If you prefer not to do this, disable the checkbox.

Reboot EdgeMarc before Upgrading (recommended)	By default, EdgeView will reboot the EdgeMarc before it begins the upgrade. If you prefer not to reboot the EdgeMarc before the upgrade (not recommended), disable the checkbox.
Use File Name	Enter the name of the upgrade file. The full filename of the image must be specified.

4. Click **Do Upgrade Now** to immediately start the upgrade, or schedule the upgrade for a later time and date and click **Schedule Upgrade**.

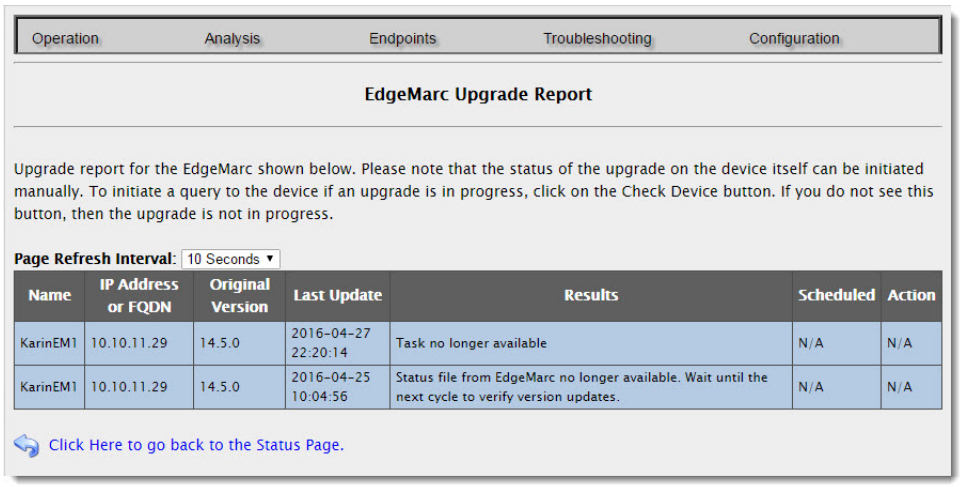
   Once the upgrade commences, the Upgrade Status Report screen will display information about the EdgeMarc upgrade process. You can view the upgrade report at anytime by selecting **Operation** > **Upgrade Status**.

Figure 3-46 EdgeMarc Upgrade Status



When the upgrade is complete, the Results column in the EdgeMarc Upgrade Report table will show “Completed Successfully.” If the upgrade is not successful, an error message will display in red in the Results column.(Figure 3-47).

Figure 3-47 Viewing the Upgrade Report and Status



See Debugging EdgeMarc Upgrade for details on how to debug an unsuccessful firmware upgrade.

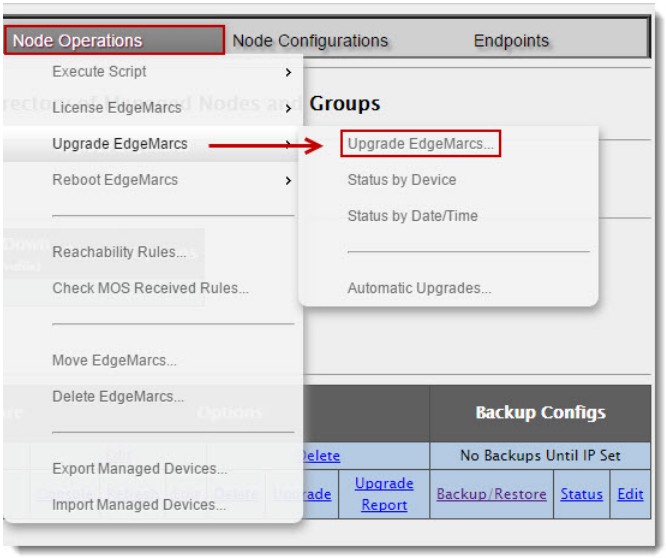
Upgrading the Firmware for an EdgeMarc Group

EdgeView can automatically load approved VOS firmware for an EdgeMarc group upon device boot-up. It displays a complete list of pending upgrades. You can cancel individual upgrades. Optionally, you can send an email notification upon upgrade.

To upgrade the VOS firmware for an EdgeMarc group:

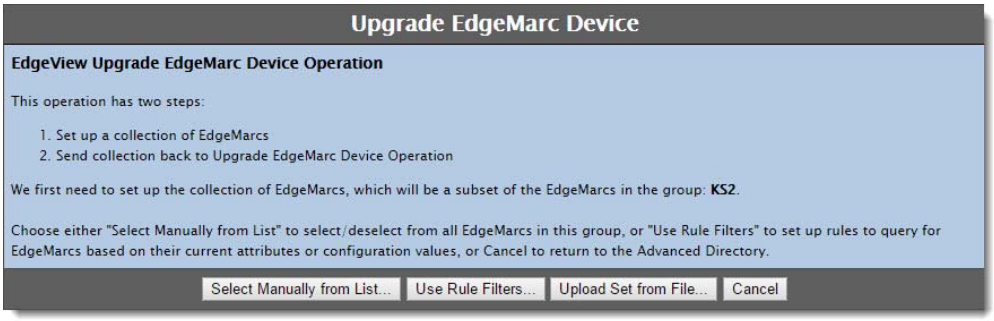
1. Select the group from the device tree.
2. Select **Node Operations** > **Upgrade EdgeMarcs** > **Upgrade EdgeMarcs** (Figure 3-48).

Figure 3-48 Upgrading Firmware for an EdgeMarc Group



3. Follow the directions in the Upgrade EdgeMarc Device screen (Figure 3-49). For more details on setting up a collection of EdgeMarcs, see Creating a Collection of EdgeMarcs.

Figure 3-49 Upgrade EdgeMarc Device Screen



4. Configure settings in the Upgrade Devices screen. Refer to Figure 3-45 for details.
5. Choose **Do Upgrade Now** or **Schedule Upgrade**.
6. Select **Node Operations** > **Upgrade EdgeMarcs** > **Status by Device** to view an upgrade report that shows the status of the upgrade on each EdgeMarc.
7. **Select Node Operations** > **Upgrade EdgeMarcs** > **Status By Date/Time** to view the upgrade status according to the date and time.

When the upgrade is complete, the Results column in the EdgeMarc Upgrade Report table will show “Completed Successfully.” If the upgrade is not successful, an error message will display in red in the Results column. Refer to Figure 3-47.

See Debugging EdgeMarc Upgrade for details on how to debug an unsuccessful firmware upgrade.

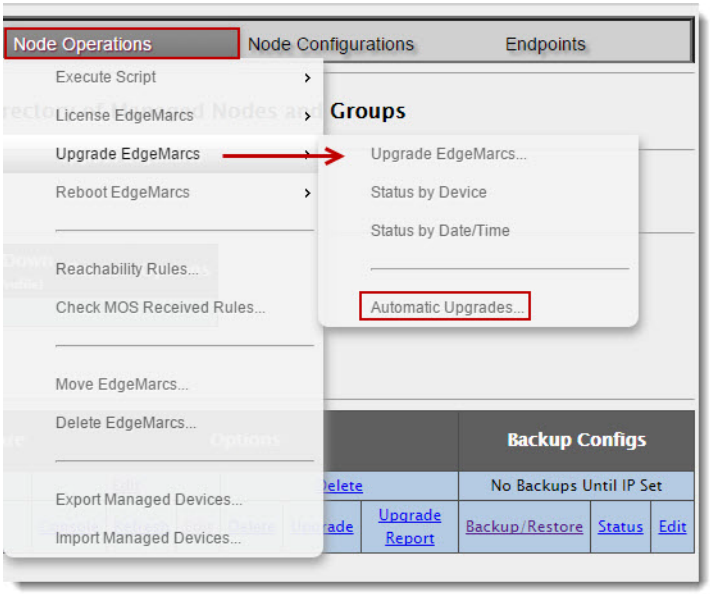
Automatically Upgrading the Firmware for an EdgeMarc Group

EdgeView can automatically upgrade the firmware for an EdgeMarc group upon device boot-up according to a set of defined rules.

To enable automatic upgrades and define rules for performing an automatic upgrade.

1. Select the group from the device tree.
2. Select **Node Operations > Upgrade EdgeMarcs > Automatic Upgrades** (Figure 3-50).

Figure 3-50 Configuring Settings for Automatically Upgrading an EdgeMarc Group



3. The Automatic Upgrade Rules for All EdgeMarcs in Group screen displays. Enable the **Check to Enable Automatic Upgrade** checkbox. Once enabled, the screen will be populated with default settings (Figure 3-51).
4. Create an automatic upgrade rule as described in Figure 3-6.

Figure 3-51 Enabling Automatic Firmware Upgrades

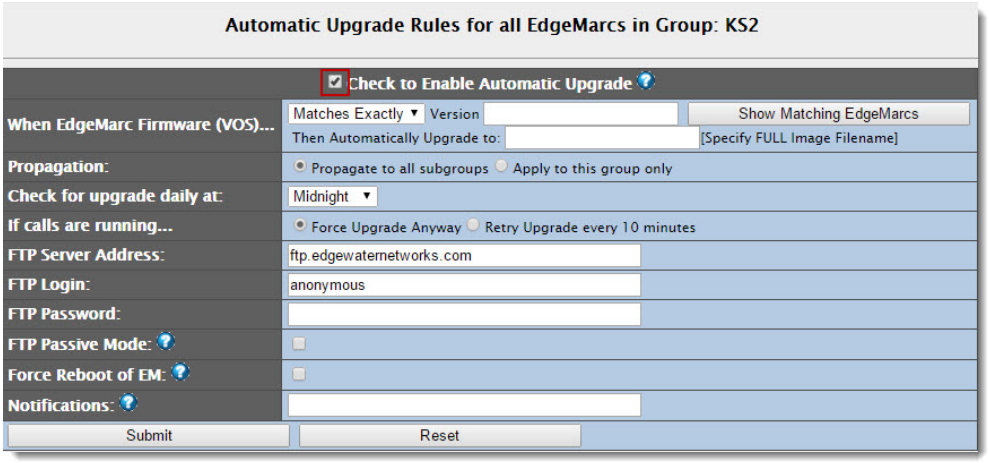


Table 3-6 Creating an Automatic Firmware Upgrade Rule

Setting	Description
Check to Enable Automatic Upgrade	When checked, EdgeMarcs matching the criteria set here will automatically upgrade themselves to the latest or specified VOS version.
When EdgeMarc Firmware (VOS)...	1. Select a matching criteria from the drop-down menu: **Matches Exactly**, **Matches Regex**, **Does Not Match**. 2. For **Version**, enter the firmware version number that corresponds to the matching criteria. The format is nn.nn.n. For example, if you choose “Matches Exactly” and enter 13.11.2 for the version, all EdgeMarcs running VOS firmware release 13.11.2 will be upgraded. 3. Click **Show Matching EdgeMarcs** to view a list of the EdgeMarcs which match the rule. A separate window will display. The actual set of EdgeMarcs (if any) may change before the upgrade rule is triggered if, for example, EdgeMarcs are added or deleted or the firmware version is updated. Click **Continue** to finish editing the rule. 4. For **Then Upgrade To...** enter the full filename of the VOS firmware image.
Propagation	Choose whether to propagate the upgrade to all subgroups or to apply the upgrade to only this group.
Check for upgrade daily at:	Select the time that you want EdgeView to check to see if the EdgeMarcs need to be upgraded.
If calls are running...	Select **Force Upgrade Anyway** if you want EdgeView to do the upgrade even if there are calls running. Select **Retry Upgrade every 10 minutes** if you want EdgeView to check the EdgeMarc every 10 minutes and wait until there are no calls running before doing the upgrade.
FTP Server Address	Enter the address or FQDN for the FTP server which has the EdgeMarc upgrade file distribution.

Table 3-6 Creating an Automatic Firmware Upgrade Rule (continued)

Setting	Description
FTP Login	Enter the login name for the FTP server.
FTP Password	Enter the password for the FTP server.
FTP Passive Mode	Enable this checkbox to force passive mode when the EdgeMarc uses FTP to get the new upgrade distribution.
Notifications	Enter email address(es) that will receive an email when this task is complete or has an error.
Submit	Click **Submit** to save and submit the automatic EdgeMarc firmware upgrade rule.
Reset	Click **Reset** to reset the page to the default settings.

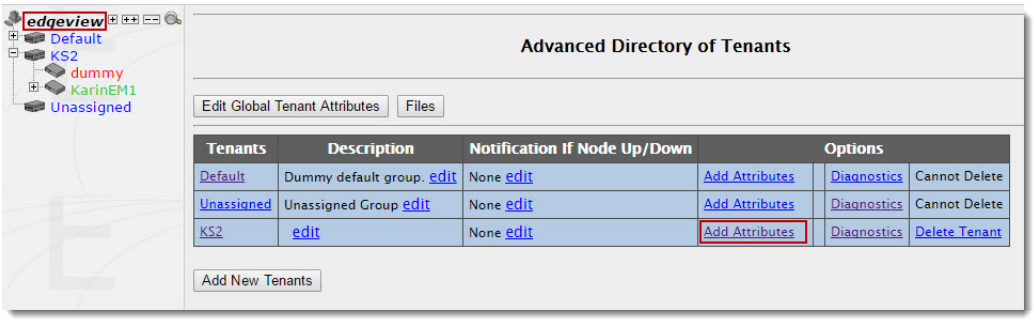
Limiting the Time of Day for EdgeMarc Upgrades

You can set an EdgeMarc Group/Tenant constraint that restricts the time of day when an EdgeMarc belonging to that group or tenant can be upgraded. The time restriction applies when the upgrade is scheduled and is not retroactive if changed. When the time restriction is enabled, any upgrades scheduled outside of the time range will be delayed until the next window is begins.

To set an upgrade time constraint for upgrading EdgeMarcs:

1. On the Advanced Directory of Tenants page, select a group or tenant and click **Add Attributes** from the Options column (Figure 3-52).

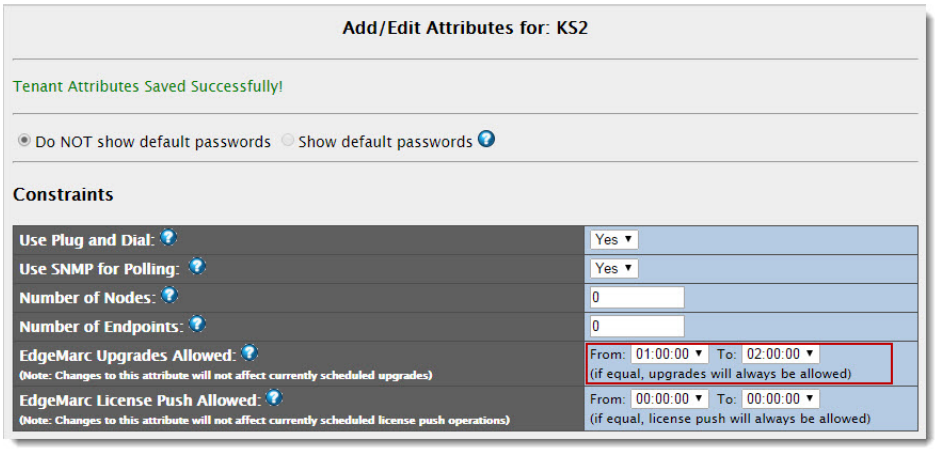
Figure 3-52 Advanced Directory of Tenants



The Add/Edit Attributes screen displays (Figure 3-53).

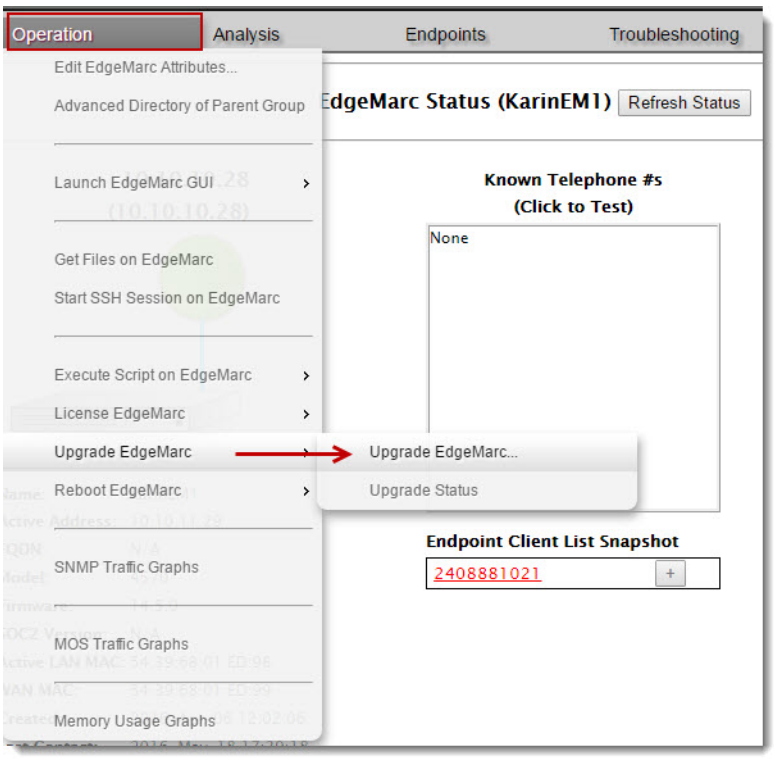
2. For the **EdgeMarc Upgrades Allowed** constraint, select From/To times from the drop-down menus to set the window of time that EdgeMarc upgrades will be allowed.
3. Click **Save Attributes** at the bottom of the screen. **Tenant Attributes Saved Successfully!** appears at the top of the screen.

Figure 3-53 Setting a Time Constraint for Updating an EdgeMarc Group/Tenant



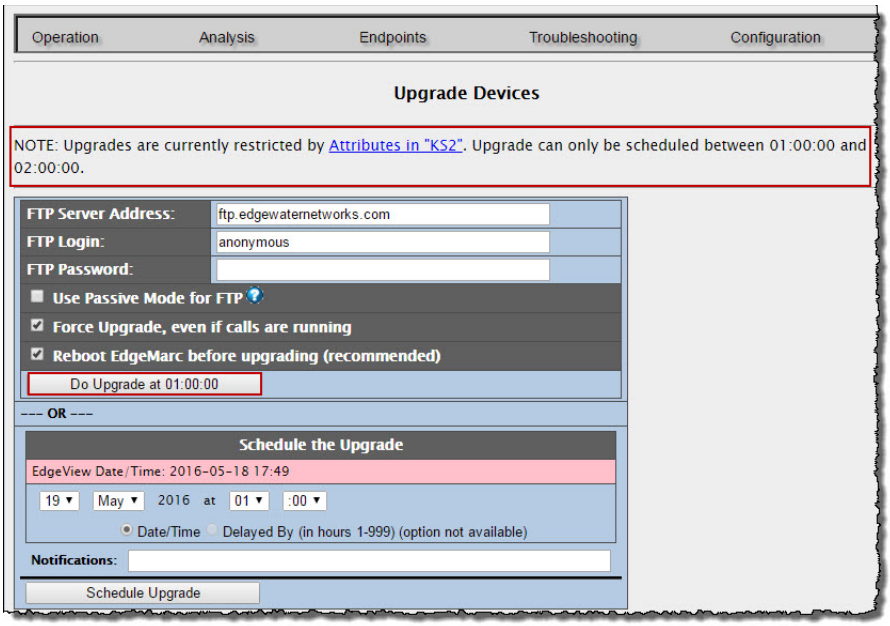
4. Choose the same group/tenant from the device tree and select an EdgeMarc.
5. Choose **Operation** > **Upgrade EdgeMarc** (Figure 3-54).

Figure 3-54 Operation Upgrade EdgeMarc



In the Upgrade Devices screen, a message displays at the top of the screen to alert you that the upgrade time constraint is set for the group/tenant. Also, the start time of the next upgrade window will be displayed in the **Do Upgrade** button (Figure 3-55).

Figure 3-55 EdgeMarc Upgrade Time Restriction



6. Click **Do Upgrade at** <*HH:MM:SS*> to schedule the upgrade for the beginning of the next window.

If you try to schedule an upgrade for outside the range, an error message will pop up.

Note

The **Delayed By** option is disabled when there is a time constriction on the schedule. This is by design.

Note

If there are multiple group attributes set up in the hierarchy, EdgeView uses the closest parent group to the EdgeMarc.

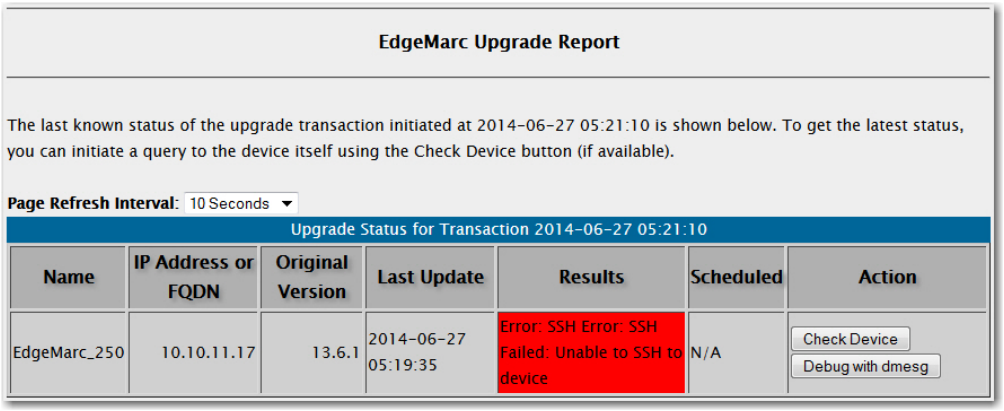
Note

If you schedule an upgrade then later change the From/To times so that the scheduled upgrade would fall outside this range, EdgeView does not go back and cancel the schedule. The time restrictions are only enforced during the scheduling process.

Debugging EdgeMarc Upgrade

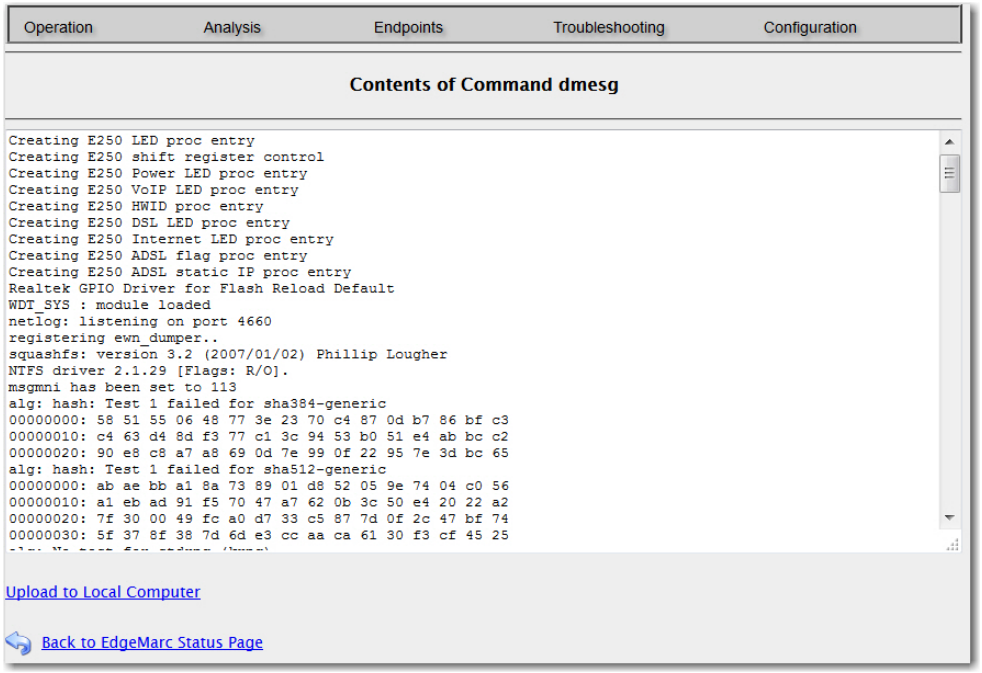
If the upgrade is unsuccessful, a **Debug with dmesg** button will show in the Action column of the EdgeMarc Upgrade Report screen for you to debug the issue (Figure 3-56).

Figure 3-56 Upgrade Unsuccessful



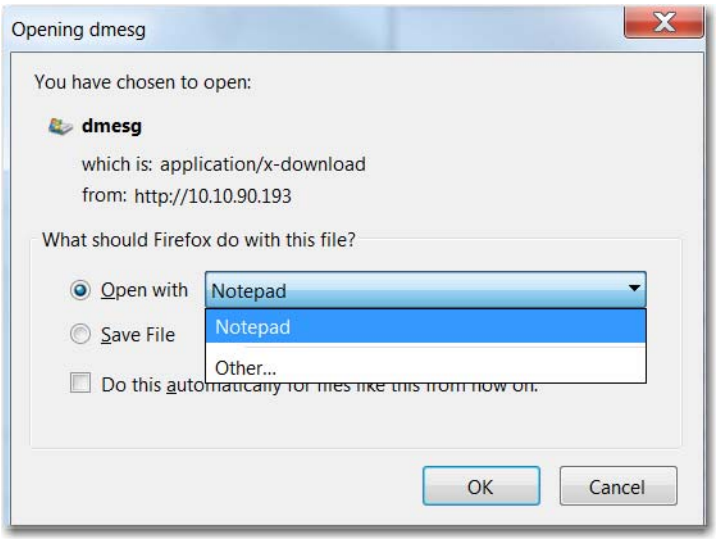
1. Click **Debug with dmesg**. EdgeView will run the dmesg command on the EdgeMarc and display the results (Figure 3-57).

Figure 3-57 Contents of the dmesg Command



2. If desired, choose **Upload to Local Computer** to upload and save the dmesg file to your computer or to view it in the application of your choice (Figure 3-58).

Figure 3-58 dmesg File Management



3. Choose the desired action and click **OK**.

Managing License Keys

To simplify provisioning and upgrade of EdgeMarc licenses, you can install EdgeMarc License Keys from EdgeView.

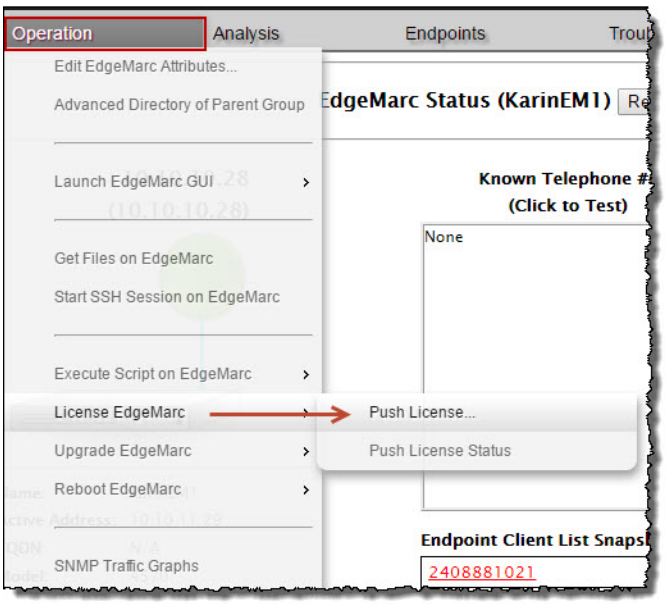
- Pushing a License Key to an EdgeMarc
- Pushing a License Key to a Group of EdgeMarcs

Pushing a License Key to an EdgeMarc

To push a license key to a single EdgeMarc:

1. Select the EdgeMarc in the device tree and then select **Operation** > **License EdgeMarc** > **Push License** (Figure 3-59).

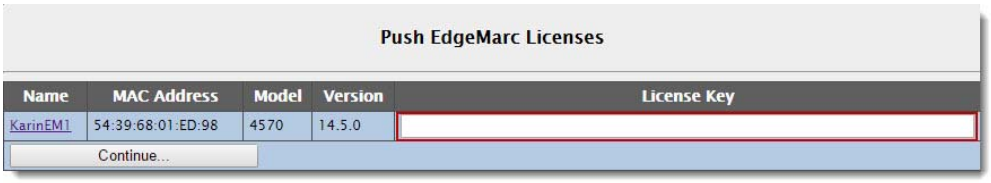
Figure 3-59 Operation - Push License



2. In the Push EdgeMarc Licenses screen, enter the license key for the EdgeMarc. The license key is in the format:

   aaaaa-bbbbb-ccccc-ddddd-eeee (original format) or fffff-ggggg-hhhhh-iiiii-jjjjj-kkkkk-lllll-mmmmm-nnnnn-ooooo (extended format). Each 5-letter or number set in the license key must be separated by dashes.

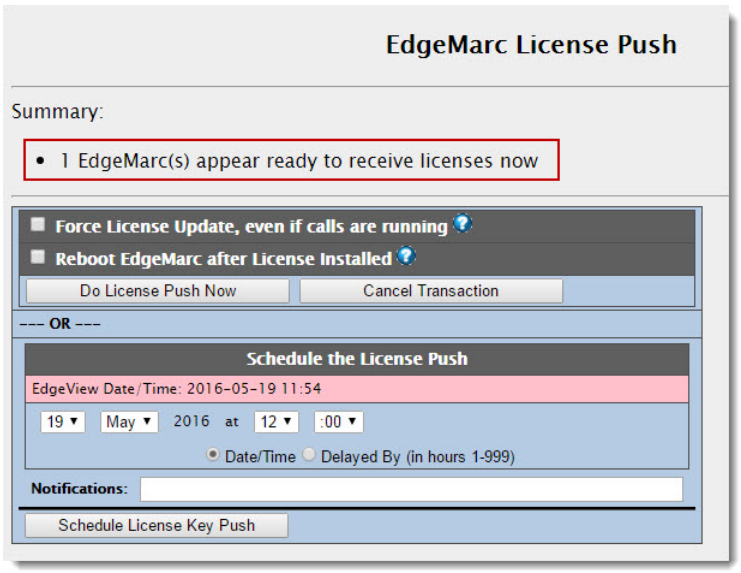
Figure 3-60 Entering the EdgeMarc License Key



3. Click **Continue**. The EdgeMarc License Push screen will display for you to set options for pushing the license key to the EdgeMarc (Figure 3-61). The number of EdgeMarcs ready to receive licenses will be displayed at the top of the page.

   If the license key cannot be validated, EdgeView will display an error message and the transaction will be canceled.

Figure 3-61 EdgeMarc License Push Screen



4. Configure options on the EdgeMarc License Push screen (Table 3-7).

Table 3-7 Configuring Options on the EdgeMarc License Push Screen

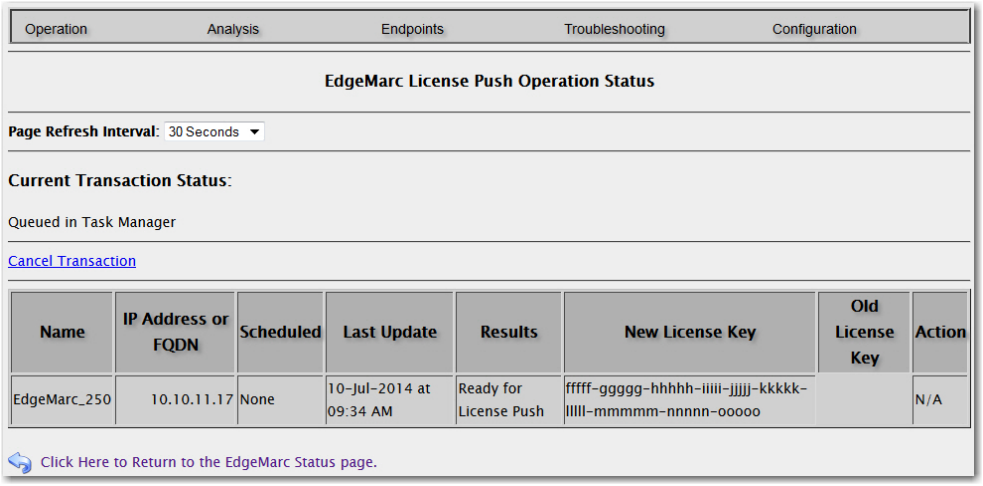
Option	Result
Force License Key Update Even When Calls are Running	Select this option if you do not want to immediately install the license key when calls are in progress. Instead, EdgeView will keep trying every 10 minutes until the EdgeMarc has no calls in progress.
Reboot EdgeMarc after License Installed	Select this option if you want to reboot the EdgeMarc after the license key is installed to make the license key to take effect.
Do License Push Now	Click this button to initiate a license key push according to the settings on this page.
Cancel Transaction	Click this button to cancel the license key push and return to the Push EdgeMarc Licenses screen.
Schedule the License Push Settings	Set the date and time that you want the license key to be pushed, or the number of hours you want the license key push to be delayed.
Notifications	Enter comma-separated email addresses that will receive a notification when the license key push occurs.
Schedule License Key Push	Click this button to schedule the license key push according to the settings on this page.

5. Click **Do License Push Now** or **Schedule License Key Push**. Once the license push commences, the results will be displayed in the EdgeMarc License Push Operation Status screen. If you specified notification email addresses, the results will be sent to them.

Note

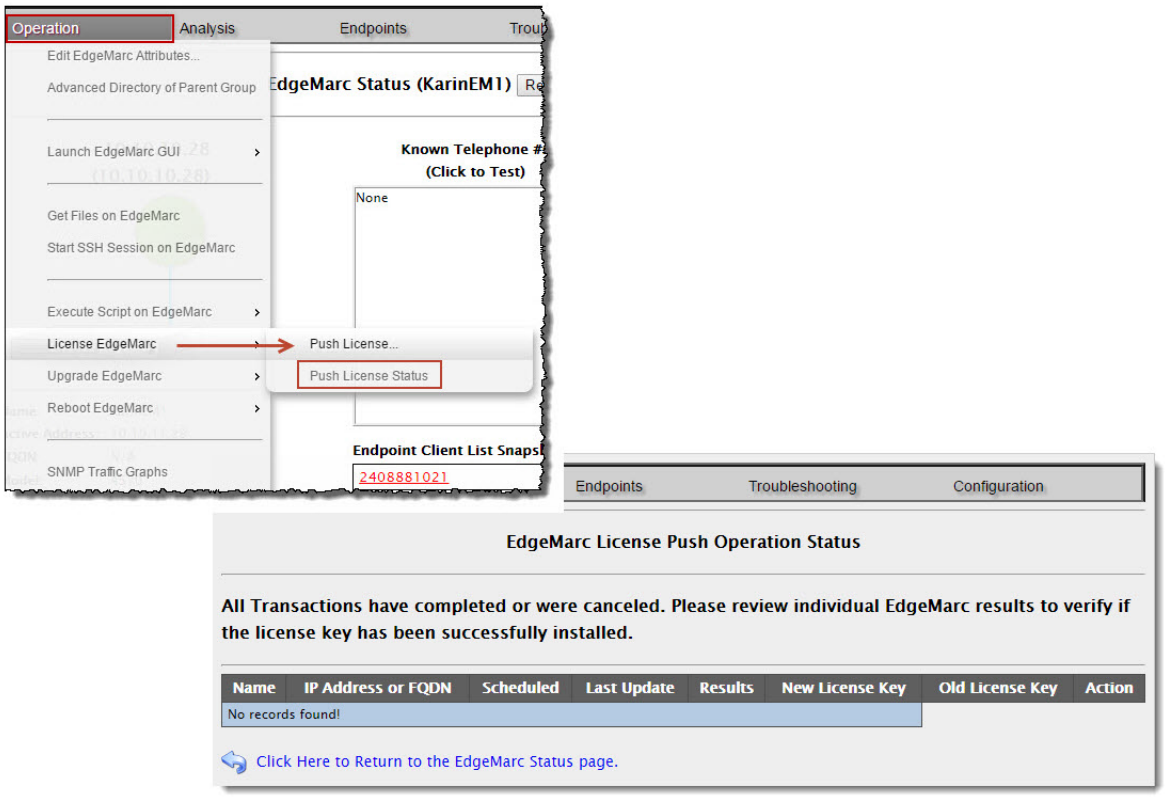
The license key push operation will be aborted if license key you are trying to push matches the currently installed license key.

Figure 3-62 License Key Push Status



To view the status of the license key push operation, choose **Operation** > **License Key Push** > **License Key Push Status** (Figure 3-63).

Figure 3-63 EdgeMarc License Push Operation Status Screen



Pushing a License Key to a Group of EdgeMarcs

To push a license key to a group of EdgeMarcs, you will first need to create/obtain a CSV file which maps the EdgeMarc MAC addresses to the license keys and then upload that file to EdgeView. Contact Edgewater Networks Technical Support to obtain the license key CSV file for your EdgeMarcs. Otherwise, you can create your own as described here.

Creating a CSV File for the License Key

License Keys can be entered into EdgeView through a comma-separated file (CSV) where each row looks like this:

<***mac address***>,<***license key***>

mac address is in the format XX:XX:XX:XX:XX

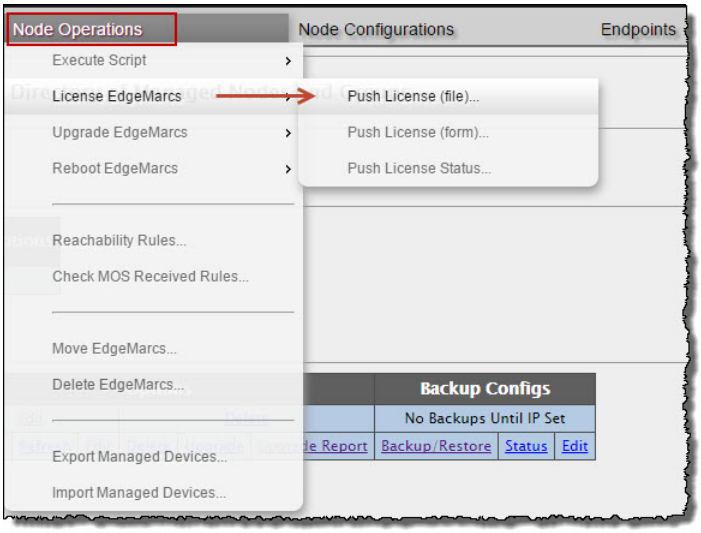
license key is in the format aaaaa-bbbbb-ccccc-ddddd-eeee (original format) or fffff-ggggg-hhhhh-iiiii-jjjjj-kkkkk-lllll-mmmmm-nnnnn-ooooo (extended format). Each 5-letter or number set in the license key must be separated by dashes.

Uploading and Pushing the License Key CSV File

To upload and push a license key CSV file to an EdgeMarc group in EdgeView:

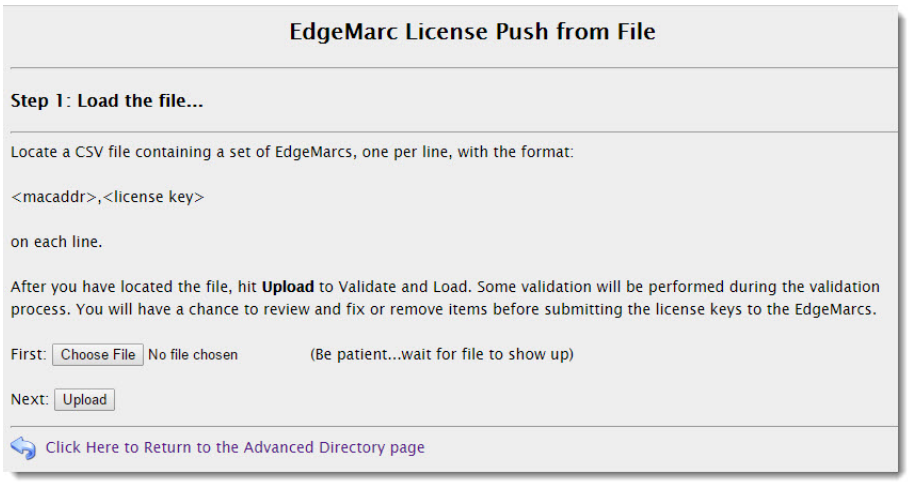
1. Select the group from the device tree. Each of the MAC address values in the CSV file must match an EdgeMarcs in the selected group (or sub group).
2. Choose **Node Operations** > **License EdgeMarcs** > **Push License (file)** (Figure 3-64).

Figure 3-64 Selecting Push License File



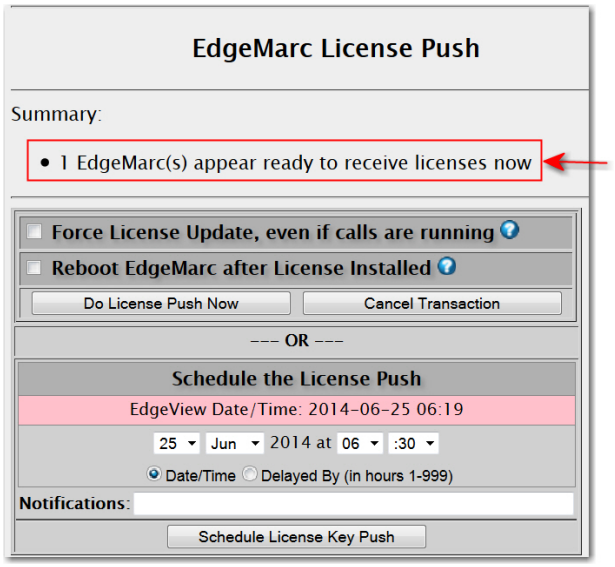
3. Follow the steps in the **EdgeMarc License Push from File** screen (Figure 3-65) to upload and process the file:
   a. Click **Browse** to locate and select the CSV file from your local drive.
   b. Click **Upload** to upload the CSV file to EdgeView. If a MAC address and/or license key in the file cannot be validated, EdgeView will display an error message and the transaction will be canceled. Note that it may take a few minutes for the file to upload.

Figure 3-65 EdgeMarc License Push from File



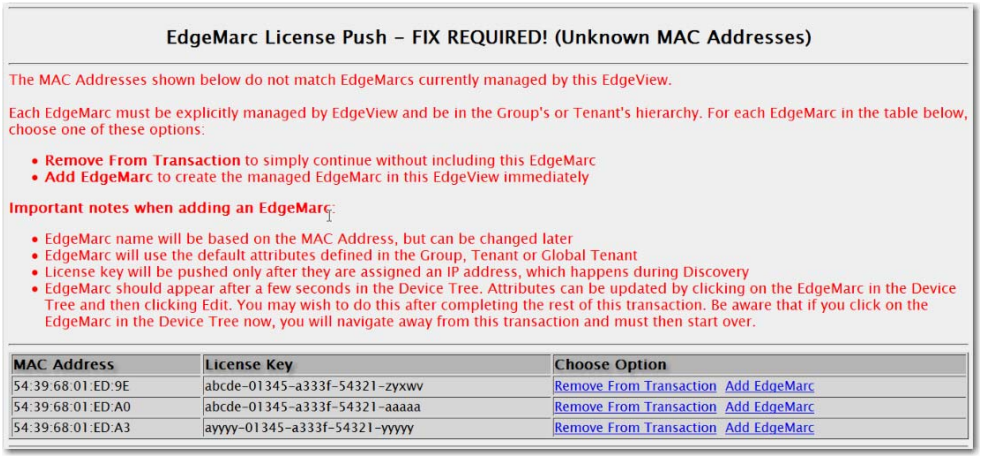
4. Once the file upload is successful, the EdgeMarc License Push screen displays. The number of EdgeMarcs which have been validated and are ready to receive the license is displayed at the top of the screen (Figure 3-66).

Figure 3-66 EdgeMarc License Push screen



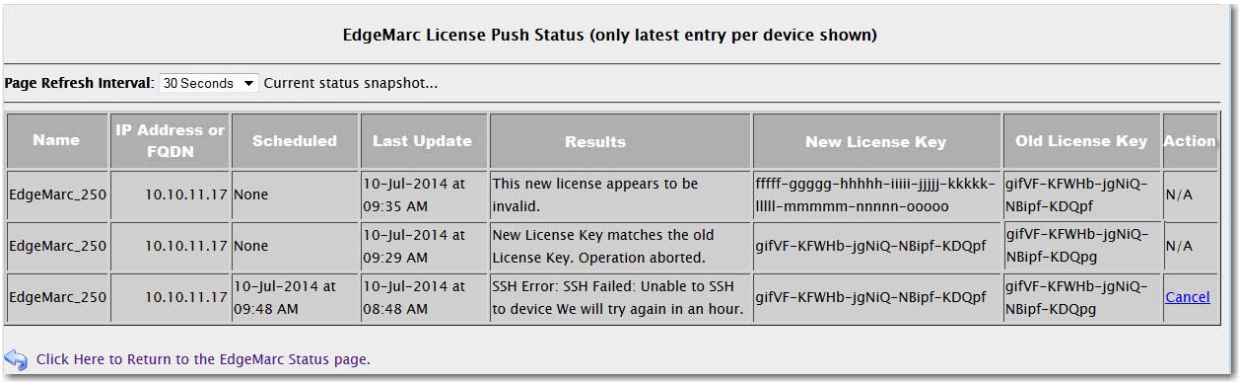
If there are MAC addresses which cannot be validated, EdgeView will list them in the following screen and provide instructions for how to resolve the issue (Figure 3-67).

Figure 3-67 Invalid License Key Push File



5. Follow the on-screen instructions to remove or add an EdgeMarc from/to the license key push transaction. If you do not choose one of these options, EdgeView will continue with the license key push transaction and only those EdgeMarcs which have a valid MAC address will be included.
6. Upon validation, the EdgeMarc License Key Push screen displays for you to select push options. Refer Managing License Keys.
7. Choose **Node Operation** > **License Key Push** > **License Key Push Status** to view results once the license key push is complete (Figure 3-68). If you specified notification email addresses in the EdgeMarc License Key push screen, the results will be sent to them.

Figure 3-68 License Key Push Status



4

Basic Group, Node, and User Management

This chapter covers the following topics:

- Understanding the EdgeView Hierarchy
- Managing Tenants
- Managing Node Settings
- Managing Users
- Managing Passwords

Understanding the EdgeView Hierarchy

To simplify device management in EdgeView, you can create a hierarchical view of your network by logically grouping the EdgeMarcs and managed nodes into smaller, isolated Tenants and groups. The EdgeView multi-tenant model allows settings to be applied globally with a single operation at any level in the hierarchy, automating many routine tasks. For example a group of EdgeMarcs can be backed up at one time rather than individually, and system attributes can be applied to a group of EdgeMarcs rather than to individual EdgeMarcs.

Once you create the hierarchy in EdgeView, you can add users and assign them Tenants. Each user is allowed to view and manage only their assigned Tenants. The same Tenant may be assigned to multiple users. When the user logs in to EdgeView, the device tree will show only the Tenants assigned to them.

You can add Tenants and groups in EdgeView at anytime and easily move groups and nodes to any level in the hierarchy. You can add as many Tenants, groups, and sub-groups as you want. However, groups and nodes may only be added to Tenants.

If you have a large number of EdgeMarcs and other nodes in your network, it's a good idea to create the EdgeView hierarchy first so that when devices are auto-discovered, EdgeView can automatically assign them to the correct group or Tenant. Auto-discovered devices will automatically assume the attributes assigned to their group or Tenant.

The device tree includes a 'Default' Tenant which you can use to add groups and nodes before you create your hierarchy in EdgeView. Groups and nodes added to the Default Tenant will use the Default Tenant attributes (or global attributes if no Default Tenant attributes are defined). The Default Tenant cannot be deleted.

Refer to the following sections for more information:

- Adding a Tenant
- Adding a Group
- Adding an EdgeMarc
- Adding a Third-Party Node
- Adding an SNMP-based Node

Tenant and Group Attributes

You can assign attributes to Tenants and groups which specify Plug & Dial, polling, SNMP and auto-discovery settings for devices assigned to that Tenant or group. Attributes may be set at the global level, Tenant level, and group level. By default, EdgeView assigns global attributes to the Default Tenant and to new Tenants and groups. You can override the global attributes by setting attributes at the Tenant level or group level. When an EdgeMarc is auto-discovered and added to a Tenant or group, EdgeView will assign it the attributes assigned to the Tenant or group. Tenant attributes override global attributes and group attributes override Tenant attributes (and global attributes).

Refer to the following sections for more information:

- Adding Tenant Attributes
- Editing Global Tenant Attributes
- Assigning Group Attributes

Limiting/Enabling User Access to EdgeView

Users may be given "specific rights" which limit and enable the EdgeView functions they are allowed to view and manage. For example, a user may be allowed specific rights to manage device configuration, system administration, and template settings. The other EdgeView functions will not be visible or accessible to the user when they log in.

For details on how to set specific rights for users, see Assigning Specific Rights to a User

Device Tree Hierarchy

The device tree shows the EdgeView hierarchy. The user is the root of the device tree and when a user logs in, their username is shown at the top (root) of the device tree. By default, the user is set to 'edgeview' and can

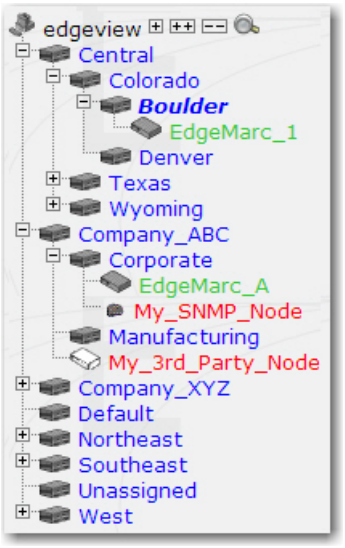
see all Tenants, groups, and nodes managed by EdgeView. When you make a selection in the device tree, it appears in italics for easy identification of your current location in the hierarchy. You can collapse the list of Tenants, groups, and nodes using the +/++, -- controls at the top of the device tree. You can also search for groups and nodes using the magnifying glass search function.



When EdgeView is managing a lot of groups, nodes, and endpoints, only part of the device tree shows up in the browser at one time. If you are currently working on a node in the device tree and another user adds a new node, EdgeView remembers your current location in the hierarchy so that when the device tree updates, you are returned to that location. This also happens if you do a full browser refresh.

Figure 4-1 shows an example of a device tree hierarchy.

Figure 4-1 Device Tree Hierarchy



In the example hierarchy shown in Figure 4-1, EdgeMarcs and other nodes are grouped by geographic location and by company. The Tenants are Central, Northeast, Southeast, and West, and Company_ABC and Company_XYZ. The corresponding states and cities are nested in groups and sub-groups under each geographic Tenant. Similarly, each company's functional areas (Corporate and Manufacturing) are nested in sub-groups under the company Tenant.

Using this example layout, you could assign a user to multiple locations that encompass a particular geographic area and company. For example, you could assign the Northeast Tenant and Company_ABC Tenant to one or multiple users. When a user logs in, their username will appear at the root of the device tree and they will see only the Northeast and Company_ABC

Tenants and groups. The user will be allowed to manage only those EdgeMarcs and nodes that are within the Northeast and Company_ABC Tenants.

Managing Tenants

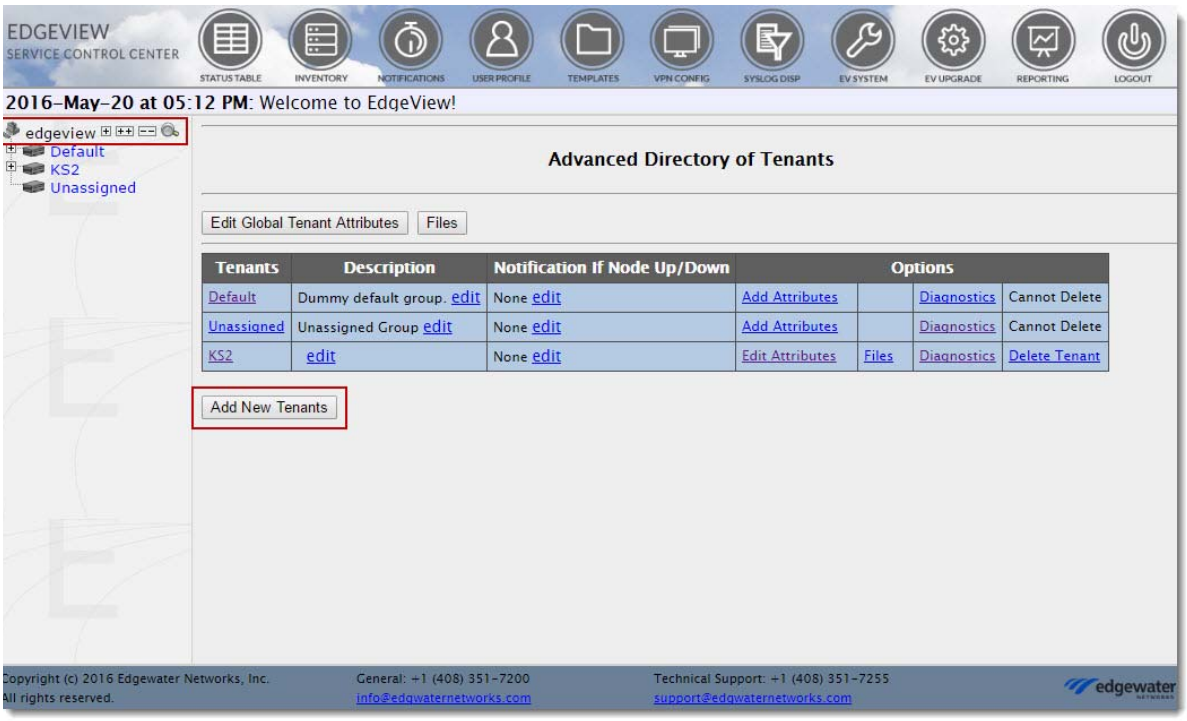
This section provides instructions for:

- Adding a Tenant
- Adding Tenant Attributes
- Editing Global Tenant Attributes
- Deleting a Tenant

Adding a Tenant

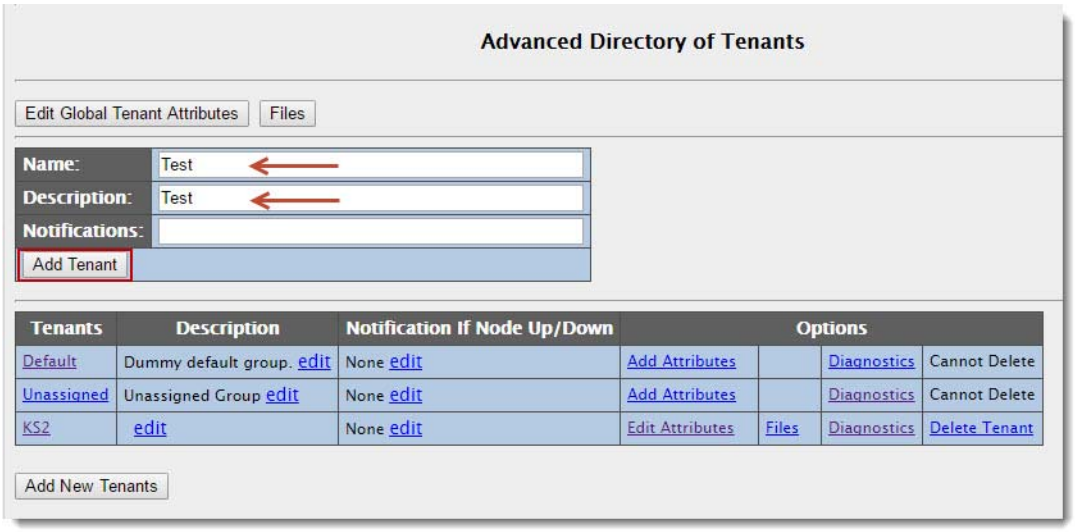
1. Click on the username icon at the root of the device tree (for example, 'edgeview') and select **Add New Tenants** from the Advanced Directory of Tenants page (Figure 4-2).

Figure 4-2 Advanced Directory of Tenants Page



2. Enter a name for the Tenant and optionally, a description and notification email addresses in the fields provided (Figure 4-3). You can go back and add the description and notification addresses later.

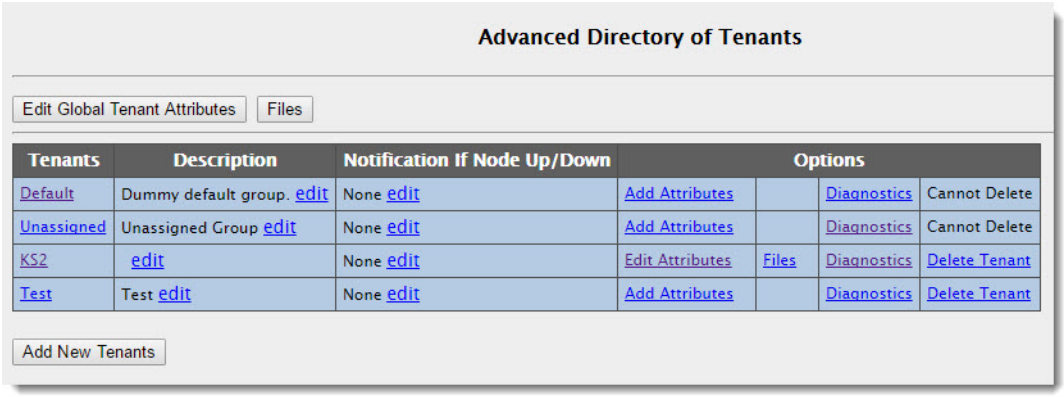
Figure 4-3 Add Tenant



3. Click **Add Tenant**.

   The new Tenant now displays in the Advanced Directory of Tenants (Figure 4-4).

Figure 4-4 Advanced Directory of Tenants



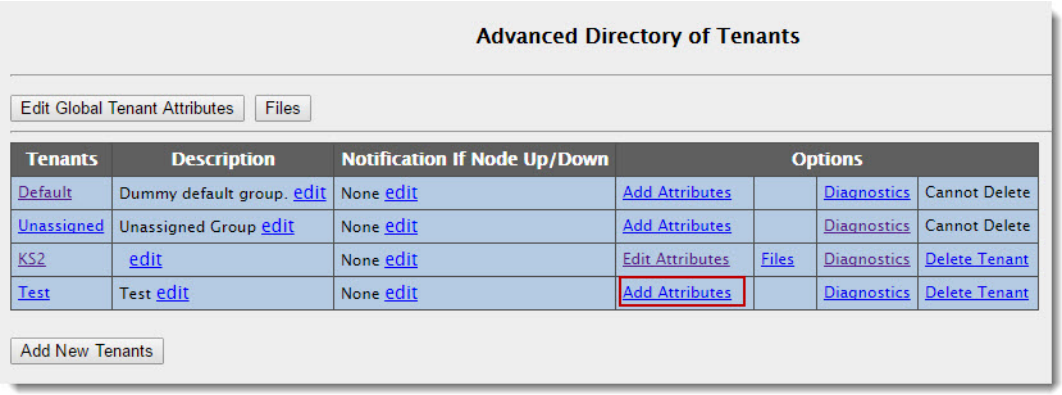
Adding Tenant Attributes

Tenant attributes specify system settings for the groups and nodes assigned to the Tenant. This information can also be specified at the global level and individual group level. Tenant attributes override attributes set at the global level. Group attributes override Tenant attributes (and global attributes).

To add Tenant attributes:

1. Select the username at the root of the device tree. For example, select ‘edgeview’.
2. In the Advanced Directory of Tenants page, select **Add Attributes** for the Tenant (Figure 4-5).

Figure 4-5 Adding Tenant Attributes



3. Configure settings in the Add/Edit Attributes page (Figure 4-6). For a description of each attribute setting, click the question mark balloons. These descriptions are listed in Table 4-1.
4. Click **Save Attributes**.

Figure 4-6 Add/Edit Tenant Attributes Page

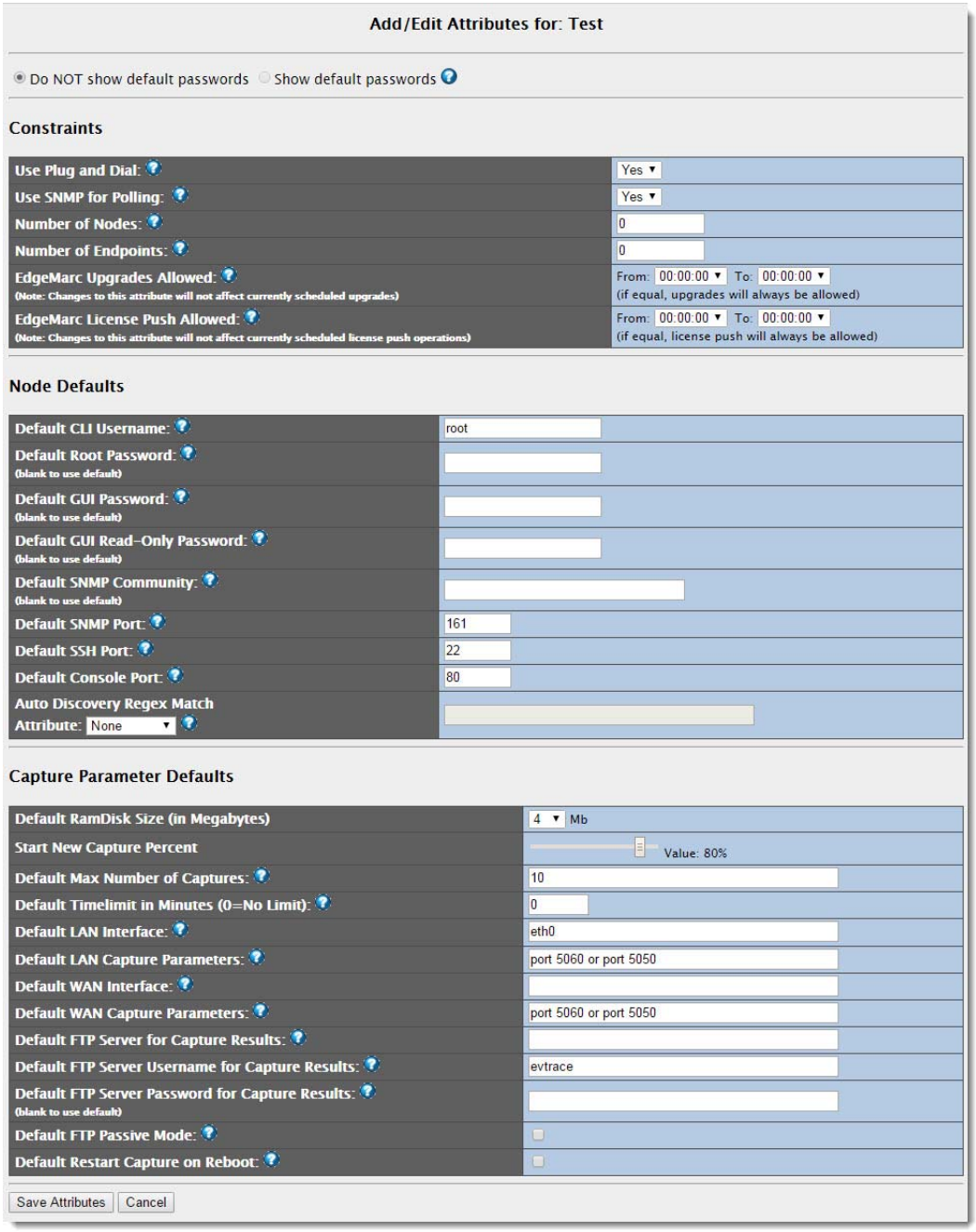


Table 4-1 Tenant Attributes

Field	Description
Name	Name of the Tenant. This field is not configurable.
Use Plug and Dial	When set to **Yes** (the default), the Tenant will be able to use Plug & Dial.
Use SNMP for Polling	When set to **Yes** (the default), devices belonging to the Tenant will try to gather statistics via SNMP during the polling cycle. This can be significantly faster than SSH but is less secure. If SNMP is not available for the device, it will poll using SSH.
Number of Nodes	For licensing purposes, this value will be used to limit the number of EdgeMarcs, third-party nodes, and SNMP-based nodes allocated to the Tenant.
Number of Endpoints	For licensing purposes, this value will be used to limit the number of endpoint devices, such as IP phones, allocated to the Tenant.
Default CLI Username	This username will be used as the default username. If you want the username to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default Root Password	This password will be used as the default CLI password. If you want the password to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default GUI Password	This password will be used as the default GUI password. If you want the password to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default GUI Read-Only Password	This password will be used as the default GUI password for read-only users. If you want the password to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default SNMP Community	This password will be used for the default SNMP community string. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default SNMP Port	This value will be used as the default SNMP port. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default SSH Port	This value will be used as the default SSH port. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default Console Port	This value will be used as the default GUI (console) port. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Auto Discovery Regex Match Attribute	When an unidentified device is auto-discovered, this regular expression is used to find matching devices so that they can automatically be moved to this Tenant. Select IP address or Host name for the drop-down box and specify a value.

* To show password information on the Add/Edit Tenant Attributes page, you must first allow decrypted passwords on the **EV System > System Settings > Passwords** tab. See Showing Decrypted Passwords.

Editing Global Tenant Attributes

If you do not assign Tenant attributes, EdgeView will assign all Tenants global attributes. Global attributes are edited in much the way that you edit Tenant attributes.

There are three types of global Tenant attributes you can set:

- **Constraints:** For the selected Tenant, constraints limit or allow Plug & Dial, SNMP polling, the number of nodes which can be added to the Tenant and the number of EdgeMarcs which can be added to the Tenant.
- **Node Defaults:** For the selected Tenant, this section sets global attributes for EdgeMarc settings which will automatically be populated on the Add/Edit Tenant Attributes Page.
- **Capture Parameter Defaults:** For the selected Tenant, this section sets global attributes for signaling capture settings which will automatically be populated on the Signaling Capture Page.

To edit global attributes:

1. Select the user at the root of the device tree. The default user is 'edgeview.'
2. In the Advanced Directory of Tenants page, click **Edit Global Tenant Attributes**. The Add/Edit Attributes for [Global] page displays.
3. Configure settings on the page. Click on the balloon icons for each field for descriptions of each setting.
4. Click **Submit**.

The following Figures and Tables define the global attribute settings you can set in EdgeView.

Figure 4-7 Configuring Constraints for Global Settings

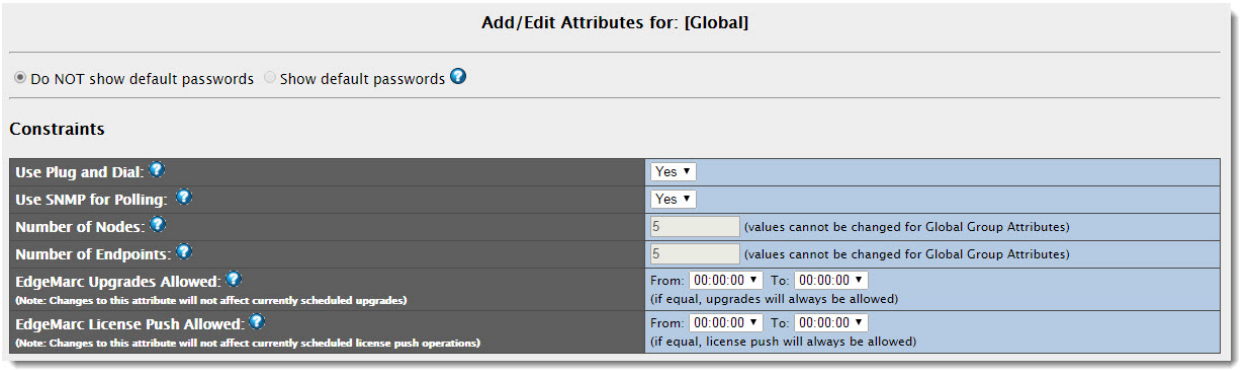


Table 4-2 Global Settings for Constraints

Use Plug and Dial	When set to Yes (the default), the group will be able to use Plug & Dial.
Use SNMP for Polling	When set to Yes, devices in this group will attempt to gather statistics via SNMP during the polling cycle. This can be significantly faster than SSH but is less secure. If SNMP is not available for the device, EdgeView will poll using SSH. The default is No.
Number of Nodes	For device licensing purposes, this value will be used to limit the number of EdgeMarcs, third party nodes, and other polled devices allocated to the group.
Number of Endpoints	For device licensing purposes, this value will be used to limit the number of endpoint devices, such as phones, allocated to the group.
EdgeMarc Upgrades Allowed	Allows an EdgeMarc upgrade only between the times of day shown. Constraint is shown only when upgrade is scheduled. **Note:** Changes to this attribute will not affect currently scheduled upgrades.
EdgeMarc License Push Allowed	Allows an EdgeMarc license push only between the times of day shown. Constraint is shown only when license push is scheduled. **Note:** Changes to this attribute will not affect currently scheduled license push operations

Figure 4-8 Global Settings for Node Defaults

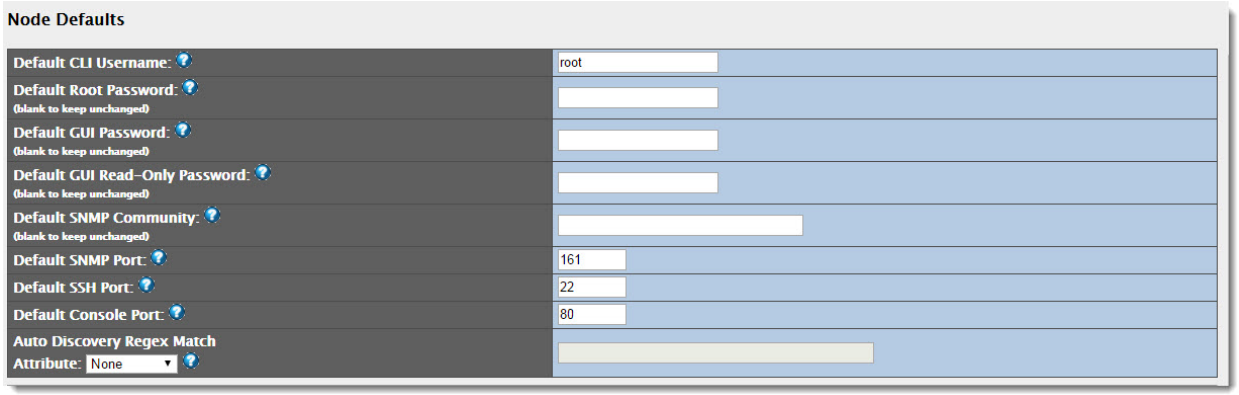


Table 4-3 Global Settings for Node Defaults

Default CLI Username	When a device is auto-discovered, this username will be used as the default username. The default is ‘root’.
Default Root Password	When a device is auto-discovered, this password will be used as the default CLI password. Leave this field blank to keep the password unchanged.
Default GUI Password	When a device is auto-discovered, this password will be used as the default GUI password. Leave this field blank to keep the password unchanged.
Default GUI Read-Only Password	When a device is auto-discovered, this password will be used as the default GUI password for read-only users. Leave this field blank to keep the password unchanged.

Table 4-3 Global Settings for Node Defaults

Default SNMP Community	When a device is auto-discovered, this value will be used for the default SNMP community. Leave this field blank to keep the SNMP community string unchanged.
Default SNMP Port	When a device is auto-discovered, this value will be used as the default SNMP port. The default is port 161.
Default SSH Port	When a device is auto-discovered, this value will be used as the default SSH port. The default is port 22.
Default Console Port	When a device is auto-discovered, this value will be used as the default GUI (console) port. The default is port 80.
Auto Discovery Regex Match Attribute	When an undefined device is auto-discovered, this regular expression is used to find matching devices so that they can automatically be moved into this group. Values are None, IP Address, or Hostname.

Figure 4-9 Capture Parameter Defaults

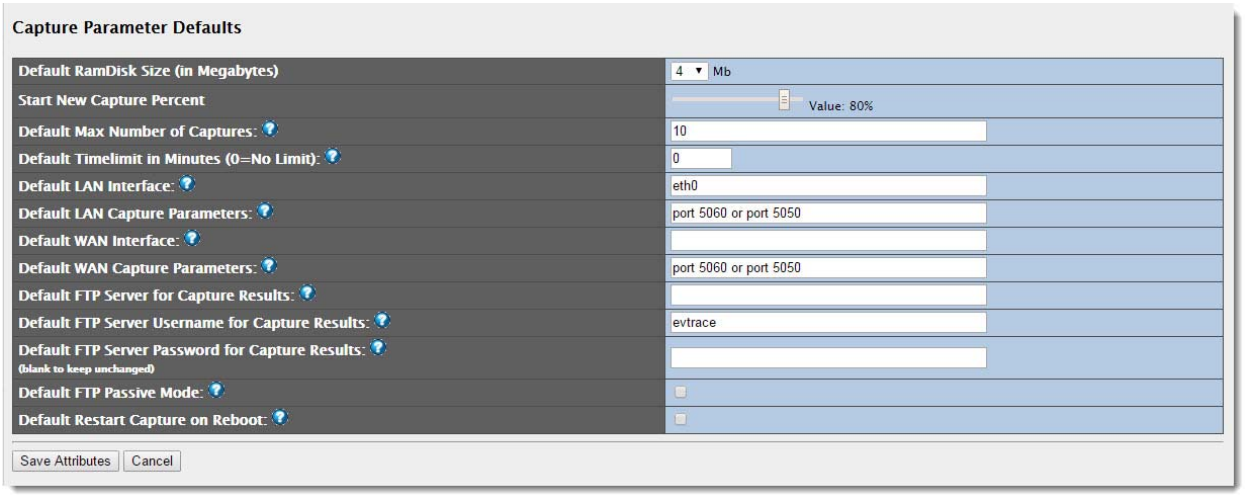


Table 4-4 Global Defaults for Capture Parameters

Default RAM Disk Size (in Megabytes)	Range is 4 MB to 16 MB. Default is 4 MB.
Start New Capture Percent	Default is 80%.
Default Max Number of Captures	The default maximum number of captures for an EdgeMarc. Default is 10.
Default Timelimit in Minutes (0=No limit)	The default time limit for capturing on EdgeMarcs. Default is 0 (no limit).
Default LAN Interface	The default LAN interface for EdgeMarc captures. Default is eth0.
Default LAN Capture Parameters	The default LAN capture port for EdgeMarcs. Default is port 5060 or port 5050.
Default WAN Interface	The default WAN interface to use for EdgeMarc captures.
Default WAN Capture Parameters	The default WAN capture parameters for EdgeMarcs

Table 4-4 Global Defaults for Capture Parameters

Default FTP Server for Capture Results	The IP address of the default FTP server which will receive the capture results. Leave blank to use the EdgeView IP address.
Default FTP Server Username for Capture Results	The default username for the FTP server which will receive the capture results.
Default FTP Server Password for Capture Results	The default password for the FTP server which will receive the capture results.
Default FTP Passive Mode	Default FTP passive mode. When enabled, EdgeView uses ftp -p on the EdgeMarc.
Default Restart Capture on Reboot	Default on/off as to whether to restart a capture after a reboot.

Deleting a Tenant

To delete a Tenant:

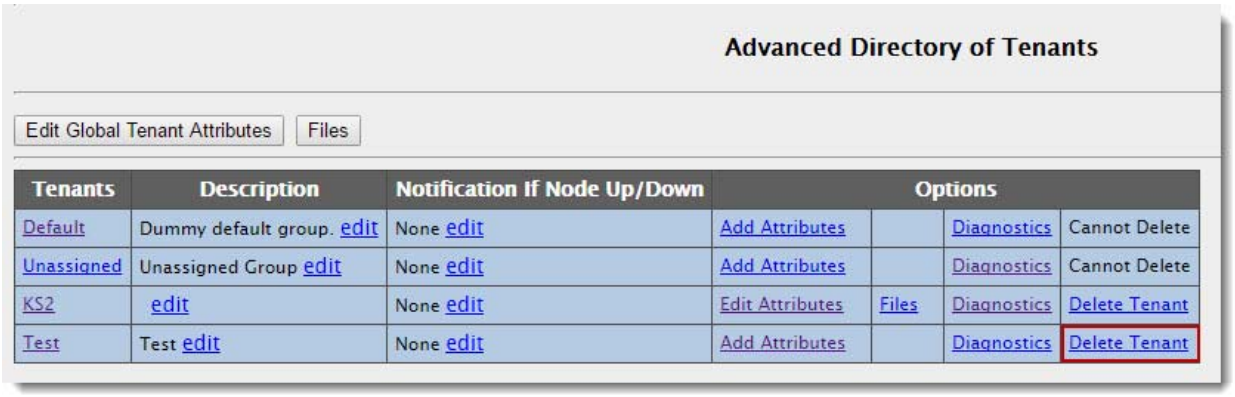
1. Click on the username in the device tree (for example 'edgeview').
2. In the Advanced Directory of Tenants, click **Delete Tenant** in the options column for the Tenant (Figure 4-10).
3. Click **OK** to confirm the deletion.



Caution

When you delete a Tenant, EdgeView will delete all sub-groups, nodes, and endpoints attached to the Tenant. Therefore, delete Tenants with caution.

Figure 4-10 Deleting a Tenant



Managing Groups

This section provides instructions for:

- Adding a Group
- Assigning Group Attributes
- Deleting a Group
- Assigning a Group to a Different Parent Group
- Moving an EdgeMarc from the Unassigned Group
- Moving Multiple EdgeMarcs to a Different Group

Adding a Group

Groups are added in the same way you add a Tenant except that you first select a Tenant or group from the device tree rather than selecting the username. You can add as many groups as you like to a Tenant or to a group.

To add a group:

1. Click on the Tenant or group in the device tree. The Advanced Directory of Managed Nodes and Groups page displays.
2. Click **Add Group** (Figure 4-11). Alternatively, select **Add Nodes** > **Add New Group** from the menu bar (Figure 4-12).

Figure 4-11 Adding a Group

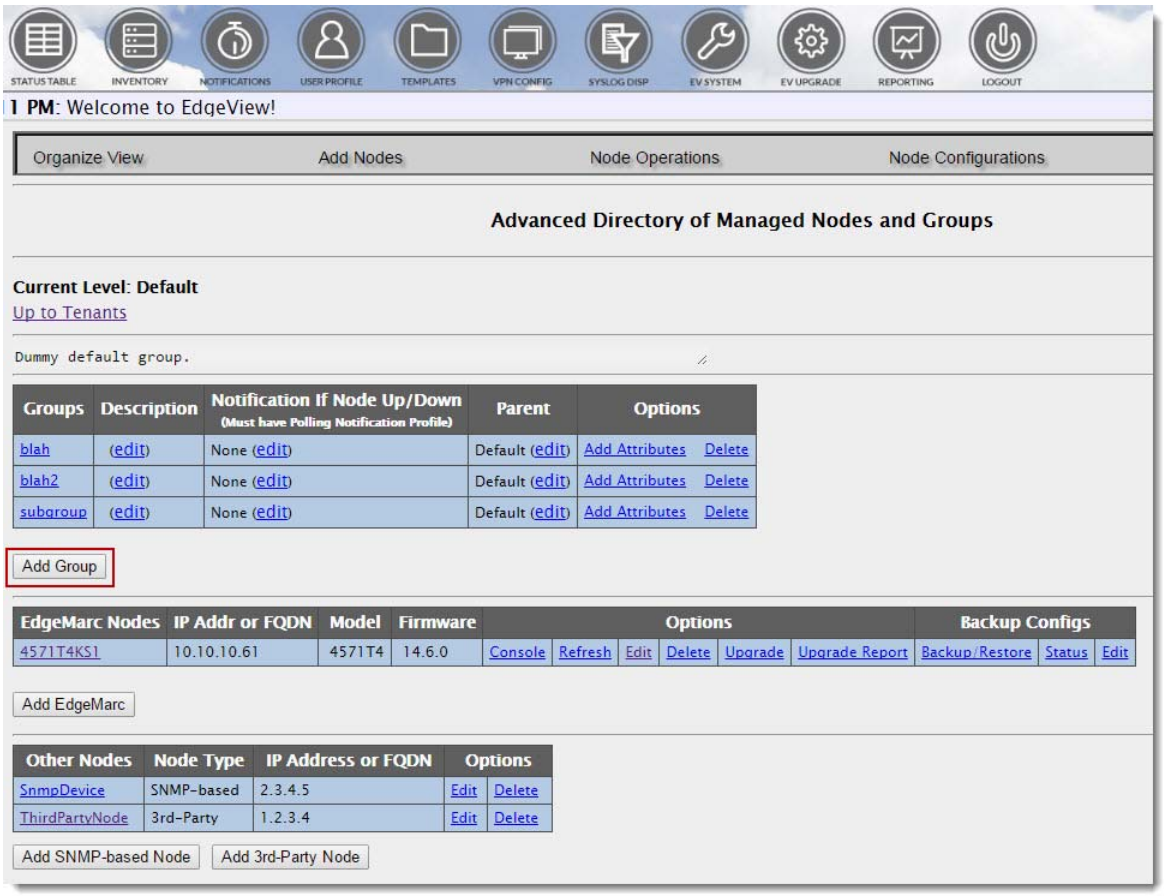
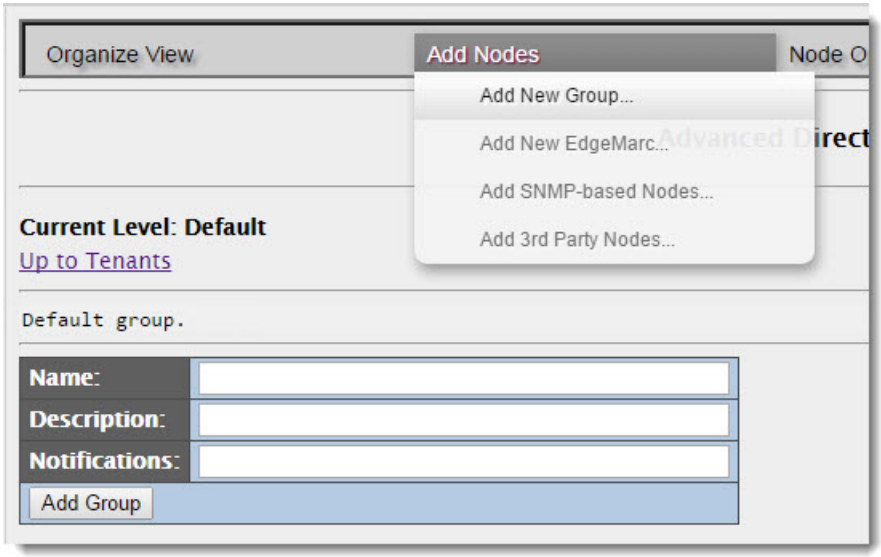
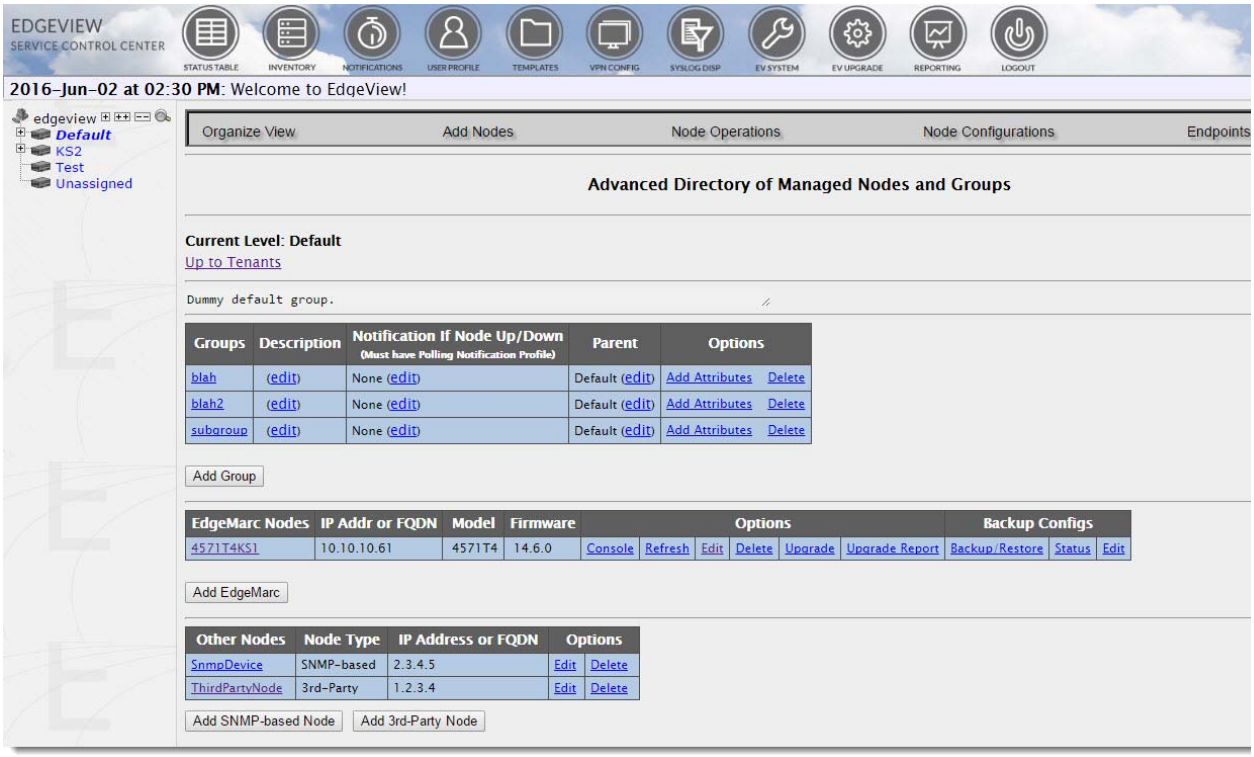


Figure 4-12 Adding a Group (from menu bar)



3. Enter a name for the group and (optionally) a description and notification up/down email addresses. You can go back and add the description and notification addresses later. Group names should be from 1 to 40 characters and should consist of letters, numbers, dashes, underscores, and periods.
4. Click **Add Group**. The group will now appear in the device tree under the Tenant or group and be listed in the Advanced Directory of Managed Nodes and Groups (Figure 4-13).

Figure 4-13 Adding a Group - Advanced Directory of Managed Nodes and Groups Page



Assigning Group Attributes

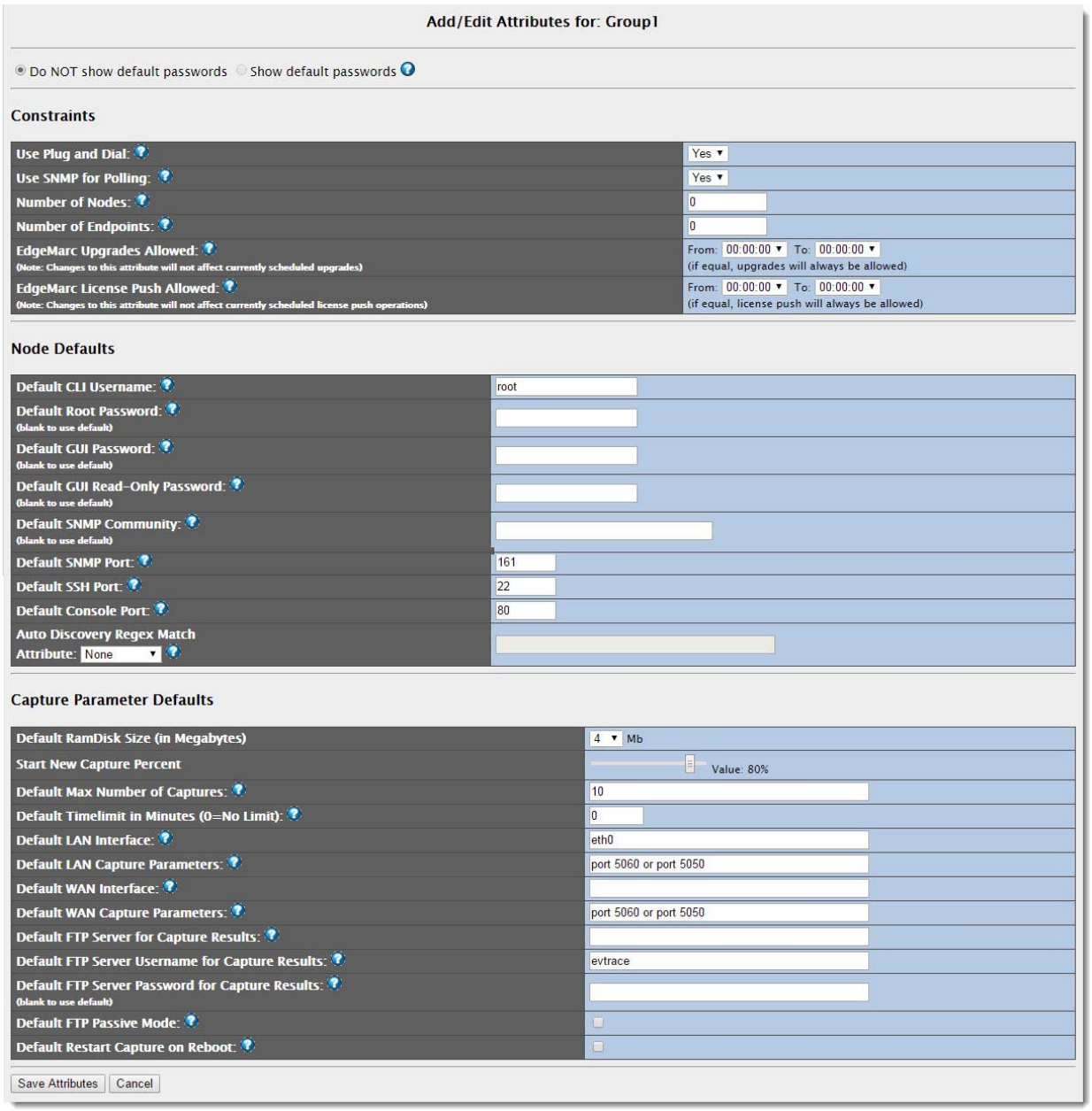
Group attributes specify system settings for the sub-groups and nodes in a group. Group attributes override Tenant attributes.

You set group attributes in the same way that you set Tenant attributes except you first select the Tenant or parent group from the device tree.

To add group attributes:

1. Select the Tenant or parent group from the device tree.
2. In the Advanced Directory of Managed Nodes and Groups page, click **Add Attributes** for the group. The Add/Edit Attributes for group page is displayed (Figure 4-14).

Figure 4-14 Adding Group Attributes



3. Configure settings in the Add/Edit Attributes page. For details about each attribute setting, click the question mark balloons. These descriptions are also provided in Table 4-5.
4. Click **Save Attributes**.

If attributes have already been set for a group, the Options column will show an **Edit Attributes** link for the group instead of an **Add Attributes** link.

Table 4-5 Group Attributes

Field	Description
Name	Name of the group. This field is not configurable.
Use Plug and Dial	When set to **Yes** (the default), the group will be able to use Plug & Dial.
Use SNMP for Polling	When set to **Yes** (the default), devices in this group will try to gather statistics via SNMP during the polling cycle. This can be significantly faster than SSH but is less secure. If SNMP is not available for the device, it will poll using SSH.
Number of Nodes	For licensing purposes, this value will be used to limit the number of EdgeMarcs, third-party nodes, and SNMP-based nodes allocated to the group.
Number of Endpoints	For licensing purposes, this value will be used to limit the number of endpoint devices, such as IP phones, allocated to the group.
Default CLI Username	This username will be used as the default username. If you want the username to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default Root Password	This password will be used as the default CLI password. If you want the password to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default GUI Password	This password will be used as the default GUI password. If you want the password to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default GUI Read-Only Password	This password will be used as the default GUI password for read-only users. If you want the password to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default SNMP Community	This password will be used for the default SNMP community string. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default SNMP Port	This value will be used as the default SNMP port. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default SSH Port	This value will be used as the default SSH port. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Default Console Port	This value will be used as the default GUI (console) port. If you want the value to be displayed on this page after you save the attributes, enable the **Show** checkbox.*
Auto Discovery Regex Match Attribute	When an unidentified device is auto-discovered, this regular expression is used to find matching devices so that they can automatically be moved to this group. Select IP address or Host name for the drop-down box and specify a value.

* To show password information on the Add/Edit Group Attributes page, you must first allow decrypted passwords on the **EV System > System Settings > Passwords** tab. See Showing Decrypted Passwords.

Deleting a Group

To delete a group:

1. Select the parent group or Tenant for the group from the device tree.
2. In the Advanced Directory of Managed Nodes and Groups page, click **Delete** in the Options column for the group. A confirmation box displays to advise you that EdgeView will attempt to promote nodes, endpoints, and configuration files to the parent group, if possible. Any group attributes, alerts, and MOS notifications for the group will be lost.
3. Click **OK** to confirm the deletion.



Note

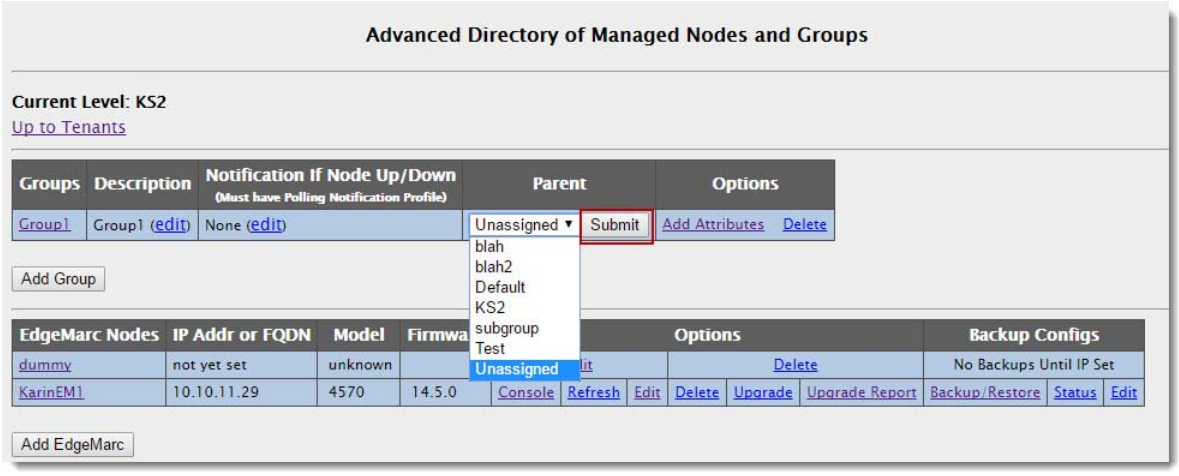
Deleting a group will not delete nodes contained within the group. Instead, these nodes will be automatically placed in the parent group or Tenant (if no parent group exists). You must delete nodes individually to remove them from the EdgeView database.

Assigning a Group to a Different Parent Group

You can move a group to a different group or Tenant by assigning it to a different "parent" as follows:

1. Open the Advanced Directory of Managed Nodes and Groups page and click **Edit** in the Parent column for the group.
2. Select the target group or Tenant from the drop-down menu (Figure 4-15) and click **Submit**. The device tree will be updated to reflect the group's new position in the tree.

Figure 4-15 Assigning a Group to a Different Parent



Moving an EdgeMarc from the Unassigned Group

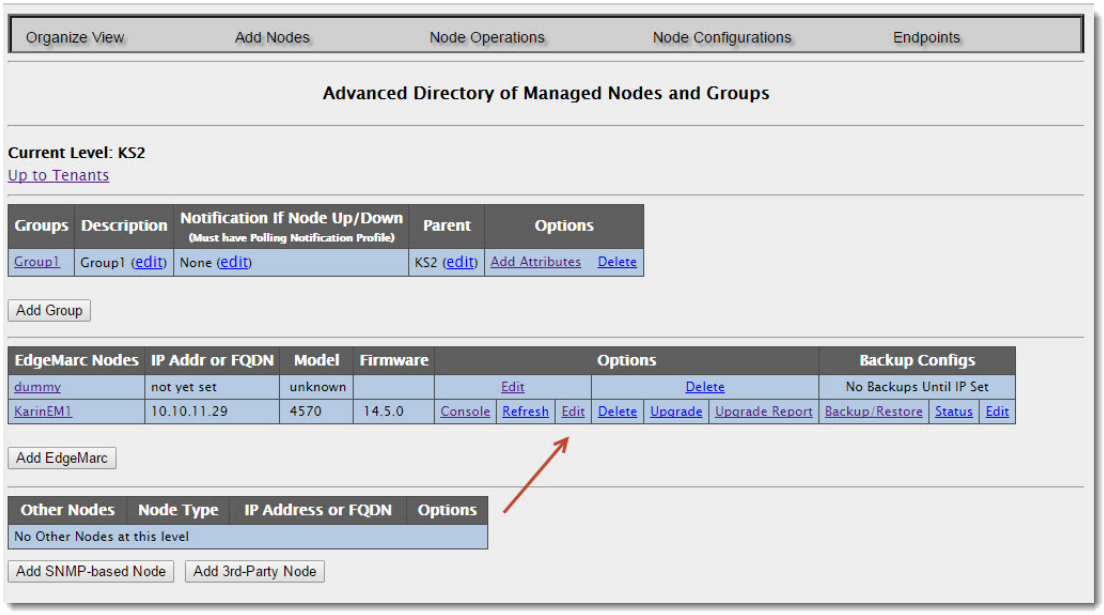
When an EdgeMarc comes online or is rebooted, EdgeView automatically adds it to the 'Unassigned' group in the device tree. If the Unassigned group does not exist, EdgeView will create it automatically. Once the EdgeMarc is in the Unassigned group, you can move it to any group as follows.

Note

The EdgeMarc must have a backup file before it can be moved to another group.

1. Select **Unassigned** from the device tree. The Advanced Directory of Managed Nodes and Groups page displays.
2. In the EdgeMarc Nodes column, find the EdgeMarc you want to move and click **Edit** in the Options column (Figure 4-16). Alternatively, you can click on the EdgeMarc in the device tree and then select the **Operations > Edit Attributes** menu option.

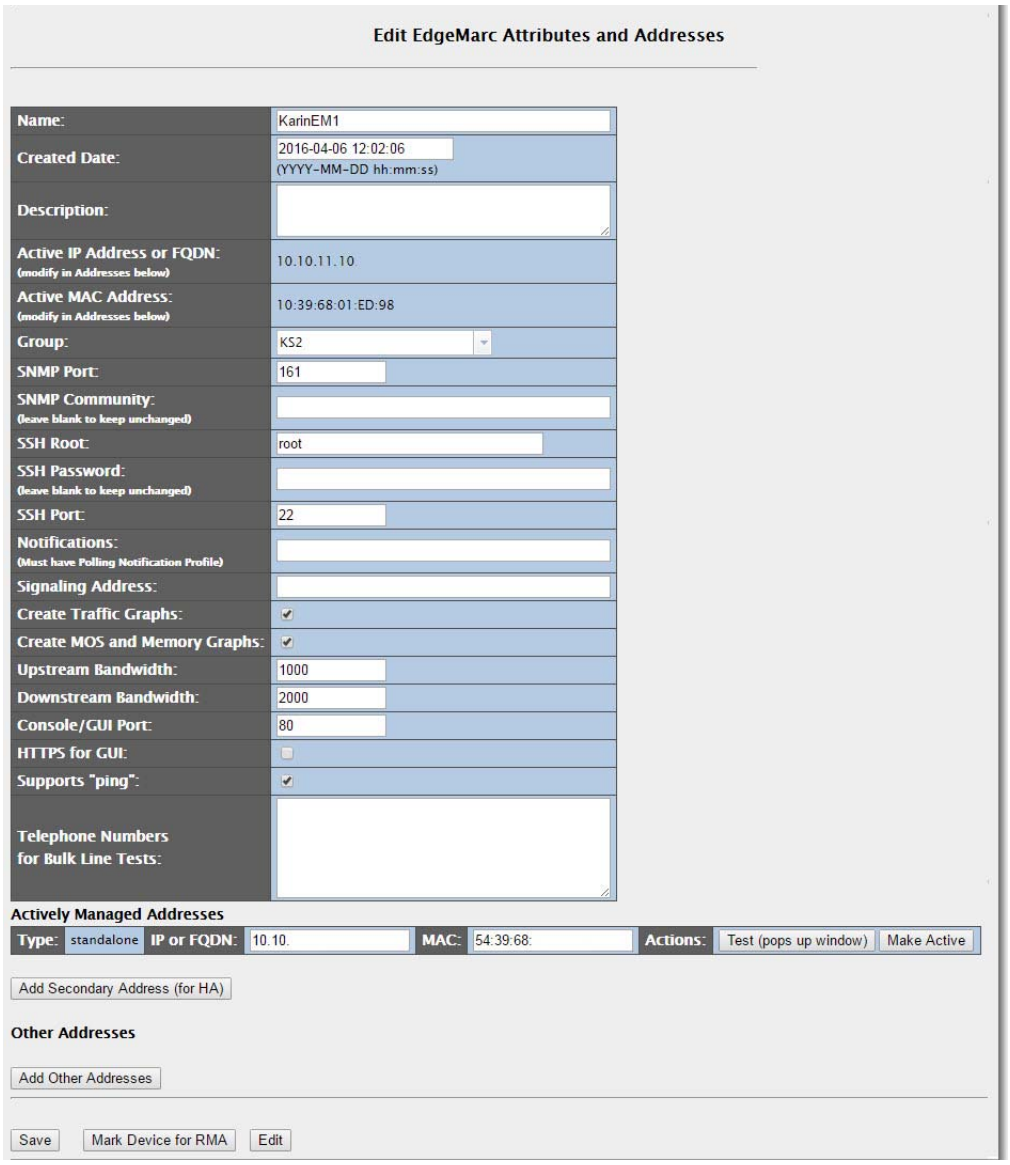
Figure 4-16 Moving an EdgeMarc from the Unassigned Group



3. In the Edit Device Page, select the group to which you want to move the EdgeMarc and click **Save**. After about one minute, the EdgeMarc will appear under the new group in the device tree.

In the example shown in Figure 4-17, EdgeMarc_A is moved from the Unassigned group to the Corporate group.

Figure 4-17 Moving an EdgeMarc from the Unassigned Group



Moving Multiple EdgeMarcs to a Different Group

You can move multiple EdgeMarcs to a different group with a single operation as follows:

1. From the device tree, select the parent group or Tenant which contains the EdgeMarcs you want to move. The Advanced Directory of Managed Nodes and Groups page displays.
2. Select **Node Operations > Move EdgeMarcs** from the menu bar. The screen shown in Figure 4-18 displays.

Figure 4-18 Moving Multiple EdgeMarcs to a New Group



3. Follow the instructions on the screen to create a collection of EdgeMarcs.
4. Select a target group for the selected EdgeMarcs.
5. Click **Move EdgeMarc Devices**. The selected EdgeMarcs will display under the target group in the device tree.

Managing Node Settings

EdgeView includes default settings that allow you to add nodes by entering a node name and the public IP address of the WAN interface. For each node type, you can specify settings for the management protocol(s) to be used by EdgeView to retrieve information from the node. By default, EdgeView polls each node at 5 minute intervals.

Nodes in EdgeView can be:

- Edgewater Networks Products (EdgeMarcs, EdgeProtects, and EdgeConnects)
- IP Phones
- Third-party devices (any device which can be reached via SSH protocol)
- SNMP-based devices

This section covers the following topics:

- Adding an EdgeMarc
- Adding a Third-Party Node
- Adding an SNMP-based Node
- Editing Node Settings
- Deleting a Node
- Moving a Node Between Groups

Adding an EdgeMarc

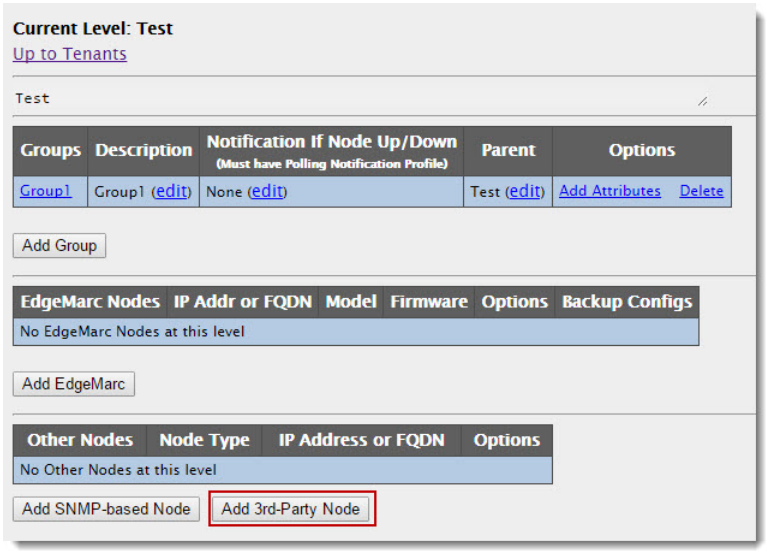
EdgeMarcs are typically added via auto-discovery but they can also be added manually from the Advanced Directory of Managed Nodes and Devices page. For details on adding EdgeMarcs, refer to Basic EdgeMarc Management.

Adding a Third-Party Node

To add a third-party device such as a router, switch, server, or firewall to EdgeView:

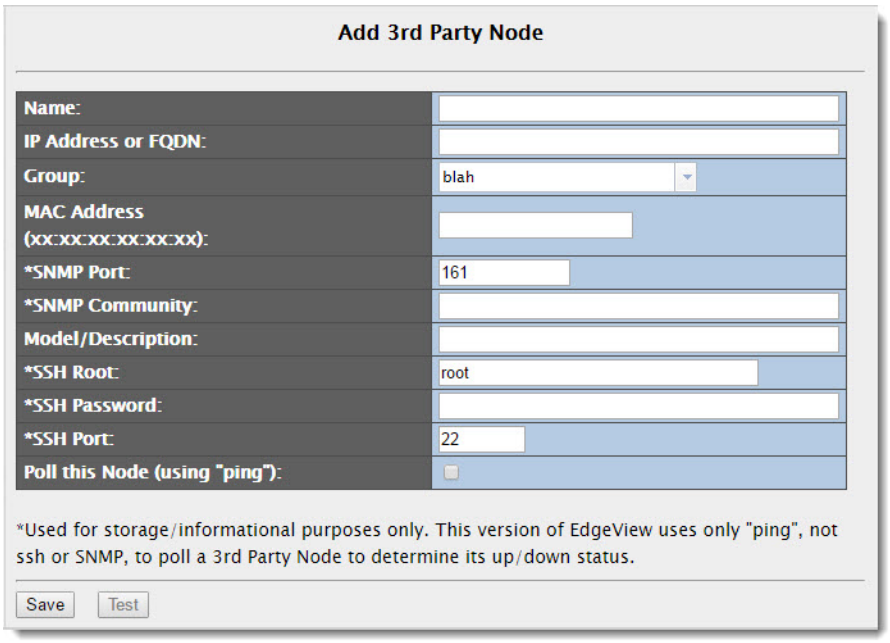
1. Select the level in the device tree where you want to create the third-party node. The Advanced Directory of Nodes and Groups page displays (Figure 4-19).

Figure 4-19 Add Third Party Node



2. Click the **Add 3rd Party Node** button. Alternatively, you can select **Add Nodes** > **Add Third Party Node** from the menu bar to access the Add 3rd Party Node page (Figure 4-20).

Figure 4-20 Add 3rd Party Node Page



3. Enter the node name and the IP address. The IP address is typically the public IP address of the WAN interface.
4. Specify the group membership for the node from the Group drop-down box.
5. Specify additional settings for the third-party node using the information in Table 4-6.
6. Click **Save**.

Table 4-6 Add 3rd Party Node Field Descriptions

Field	Description
Name	(Required) Type a name for the node.
IP Address or FQDN	(Required) Enter the IP Address or FQDN for the device.
Group	Group to which this node belongs.
MAC Address	MAC Address for the device.
*SNMP Port	The SNMP port to be assigned to the device.
*SNMP Community	The SNMP community string to be assigned to the device.
Model/Description	(Optional) Enter the model number of the device and/or any other descriptive information to help you locate the device on the network.
*SSH Root:	The default username for this device.
*SSH Password:	(Required) The default password for this device.

Table 4-6 Add 3rd Party Node Field Descriptions

Field	Description
*SSH Port:	The default SSH port for this device.
Supports “ping”	Indicate whether the device supports ping. This field is enabled by default.

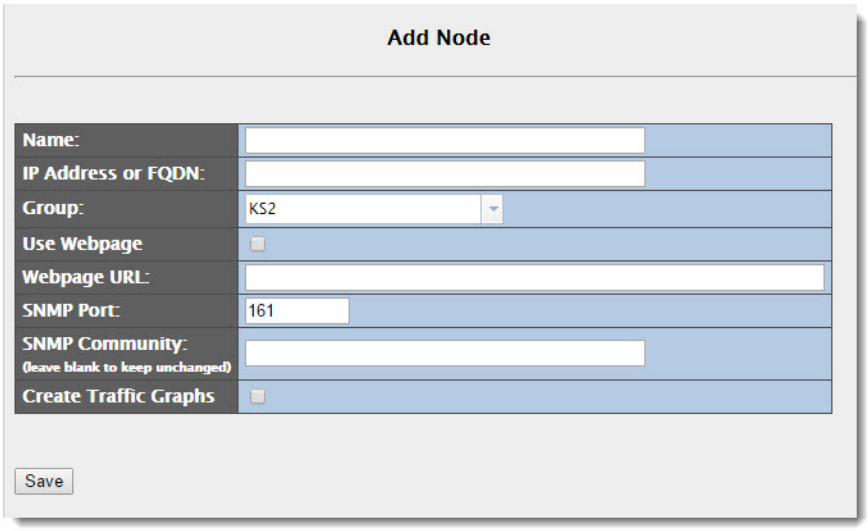
* Used for storage/informational purposes only. This version of EdgeView uses only “ping”, not SSH or SNMP to poll a 3rd Party Node to determine its up/down status.

Adding an SNMP-based Node

To add an SNMP-based device to EdgeView:

1. Select the level in the device tree where you want to add the SNMP-based node.
2. In the Advanced Directory of Nodes and Groups page, click **SNMP-based Node.** The Add Node page displays (Figure 4-21). Alternatively, you can select **Add Nodes > Add SNMP-based Node...** from the menu bar to access the Add Node page.

Figure 4-21 Add Node Page — SNMP-based Device



3. Minimally, enter the following information for the SNMP-based node. You can go back and add the other information later.
   - Name for node
   - IP Address or FQDN for the SNMP node
4. Click **Save**. The SNMP-based node will appear (in red) in the device tree until it is discovered by EdgeView.

Table 4-7 defines the fields on the Add Node page for an SNMP-based node.

Table 4-7 Adding an SNMP-based Node — Add Node Page

Field	Description
Name	(Required) Type a name for the node.
IP Address or FQDN	(Required) Enter the IP Address or FQDN for the device.
Group	Group to which this node belongs.
Use Webpage	(Optional) Enable this checkbox if the node will be managed using an HTTP session.
Webpage URL	If you are using HTTP, enter the URL of the web page that will be used to launch a web console session with the node.
SNMP Port	The default SNMP port for this device.
SNMP Community	The default community string for this device. Leave blank if unchanged.
Create Traffic Graphs	(Optional) Select the checkbox if you want EdgeView to gather traffic information for this EdgeMarc and display it in a graph. This option (also available at the Group level) provides the ability to add additional email addresses for the selected EdgeMarc or group. If the email address in the General Notifications is sufficient, there is no need to add one here.

Editing Node Settings

Once you have added a node, you can go back and edit the settings as follows:

1. From the device tree, select the parent group for the node.
2. In the Advanced Directory of Managed Nodes and Groups page, click the **Edit** link for the node you want to edit (Figure 4-22).
3. Edit the node settings (Figure 4-23).
4. Click **Save**.

Figure 4-22 Editing a Node

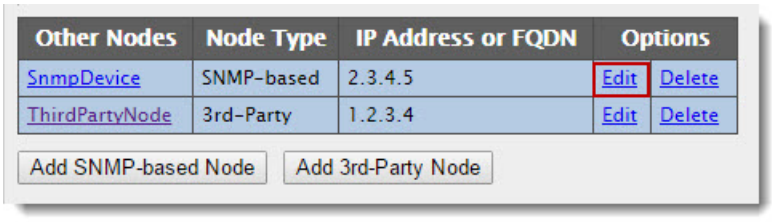
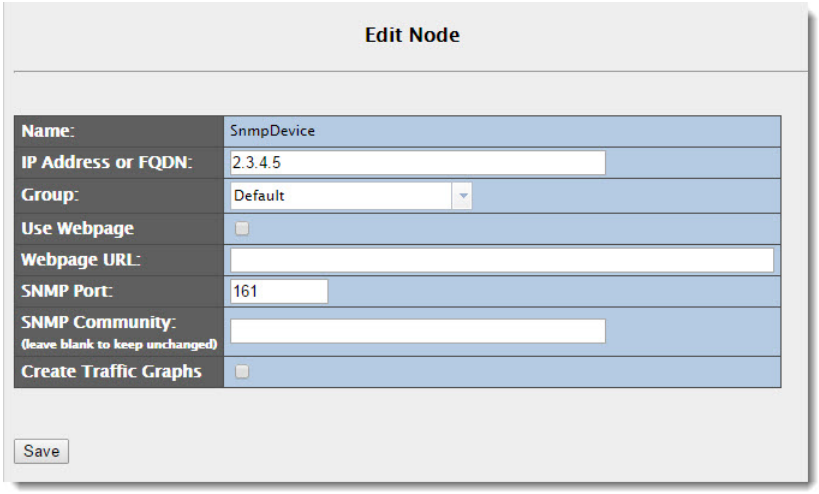


Figure 4-23 Editing a Node Page

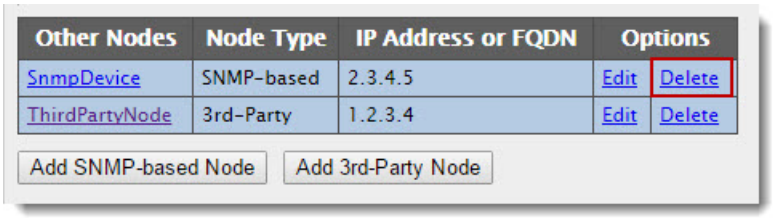


Deleting a Node

To delete a node:

1. From the device tree, select the parent group for the node.
2. In the Advanced Directory of Managed Nodes and Groups page, click the **Delete** link in the Options column for the node you want to delete (Figure 4-24). A confirmation box displays for you to confirm the deletion.
3. Click **OK** to confirm the deletion.

Figure 4-24 Deleting a Node

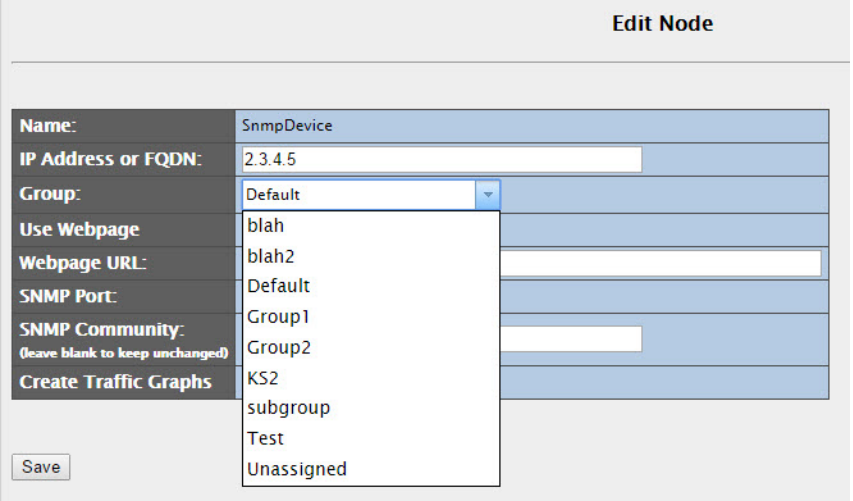


Moving a Node Between Groups

1. From the device tree, select the parent group for the node you want to move.
2. In the Advanced Directory of Managed Nodes and Groups page, click **Edit** in the Options column for the node you want to move. The Edit Node page displays.
3. From the **Group** drop-down menu, specify the group membership for the node.

4. Click **Save**.

Figure 4-25 Moving a Node



Managing Users



In EdgeView, you can add users and assign them the Tenants which they are allowed to manage. Users are allowed to manage only their assigned Tenants. The same Tenant may be assigned to multiple users. When the user logs in to EdgeView, the device tree will show only the Tenants assigned to them.

You can assign “specific rights” to users which allow them access to all or specific EdgeView files and features. For example, you can assign rights to individual users which allow them to view the Syslog, configure devices, and manage system administration settings. When the user logs in to EdgeView, the interface will show only the icons and menus for the features they are allowed to access.

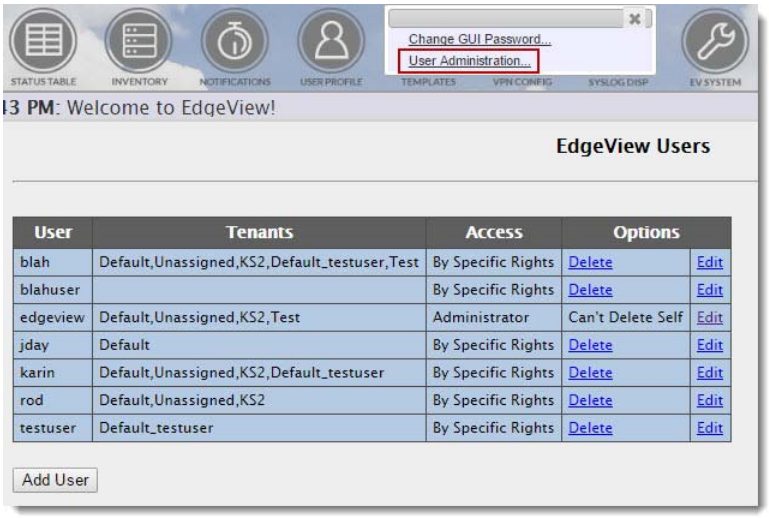
This section covers the following topics:

- Adding a User
- Deleting a User
- Editing a User
- Assigning Specific Rights to a User
- Verifying User Access to EdgeView

Adding a User

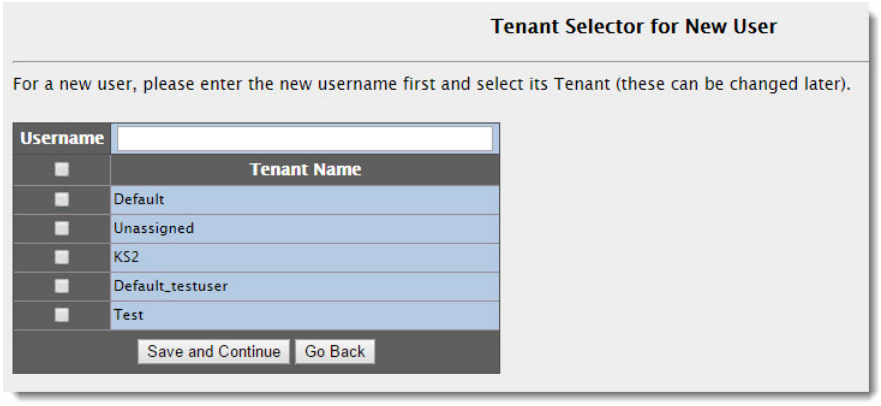
1. Click the **User Profile** icon in the EdgeView icon bar. The EdgeView Users page displays (Figure 4-26).

Figure 4-26 Adding a User



2. Click **Add User**. The Tenant Selector for New User page displays (Figure 4-28).

Figure 4-27 Add User Page



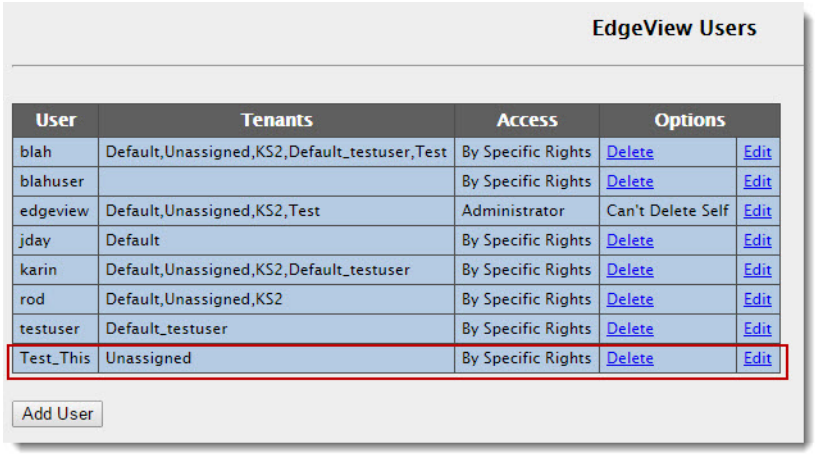
3. Enter a name for the user. This is the name the user will use to log in to EdgeView. This name will appear at the root of the device tree when the user logs in.
4. Select the checkboxes for the Tenants you want to assign to this user.
5. Click **Save and Continue**.
6. In the Add/Edit User page (Figure 4-28), enter the user's email address and contact information.

Figure 4-28 Tenant Selector for New User Page



7. (Optional) Enter additional information for this user in the Info box.
8. Type and confirm a password.
9. Click the checkboxes to assign specific rights for this user. See Assigning Specific Rights to a User for more details.
10. Click **Save**. The new user will be listed in the EdgeView Users page along with the assigned Tenants (Figure 4-29).
11. Verify the user's settings in Verifying User Access to EdgeView.

Figure 4-29 EdgeView User - Add User Confirmed



Deleting a User

To delete a user:

1. Click the **User** icon.
2. In the EdgeView Users page, click **Delete** in the Options column for the user you want to delete. A pop-up box will display for you to confirm the deletion.
3. Click **OK** to confirm the deletion. The user will be removed from the EdgeView Users list.

Note

You cannot delete the default user ‘edgeview’.

Editing a User

To edit the settings for a user:

1. Click the **User** icon.
2. In the EdgeView Users page, click **Edit** in the Options column for the user.
3. In the Add/Edit User page, make your desired changes.
4. Click **Save**.

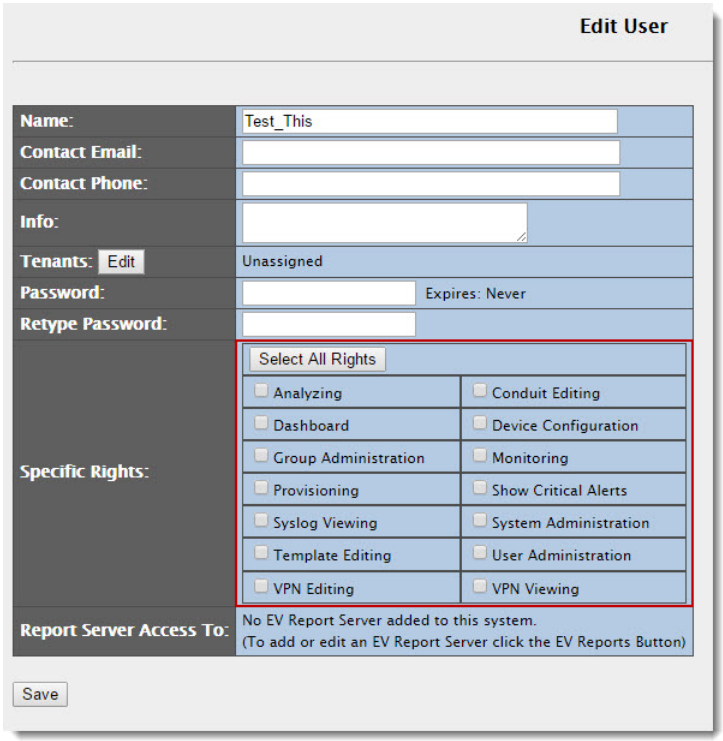
Assigning Specific Rights to a User



When you assign specific rights to a user, the user will see only the icons and menus they need for managing the settings they have been allowed in EdgeView. You can assign specific rights to a user at any time as follows:

1. Click the **User Profile** icon. The EdgeView Users page displays with a list of the users and their assigned Tenants.
2. Click **Edit** in the options column for the user to open the user profile (Figure 4-30).

Figure 4-30 Editing a User



3. In the Add/Edit User page, click the checkboxes next to the rights you want to assign. To allow this user access to all EdgeView features, click **Select All Rights**.



Note

At least one of these rights must enabled: Monitoring, System Administration and/or User Administration Rights.

4. Click **Save**.
5. Verify the user's settings in Verifying User Access to EdgeView.

Table 4-8 lists the EdgeView icons and menus associated with the Specific Rights selections on the Add/Edit Users page.

Table 4-8 EdgeView Menus Associated with Specific Right Selections

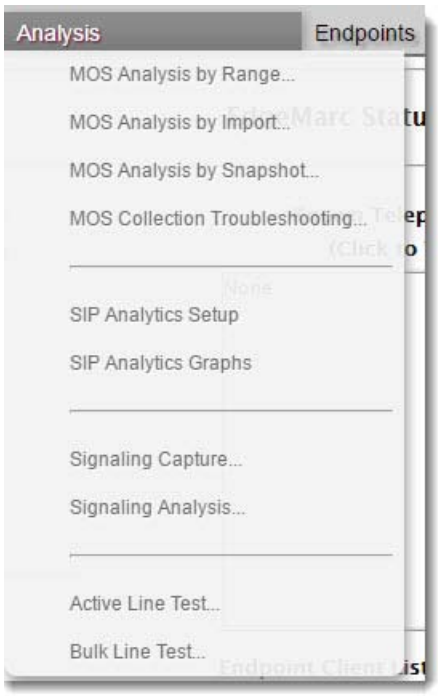
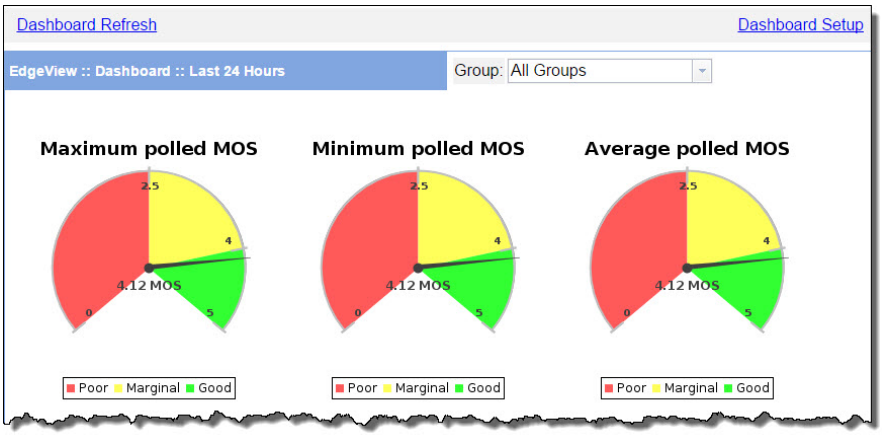
Specific Right	EdgeView Menu
Analyzing	Allows the user access to the **Analysis** menu in the EdgeMarc Status page to perform MOS analysis and signaling captures in EdgeView. 
Dashboard 	Allows the user access to the **Reporting** icon and Reporting Dashboard . 

Table 4-8 EdgeView Menus Associated with Specific Right Selections

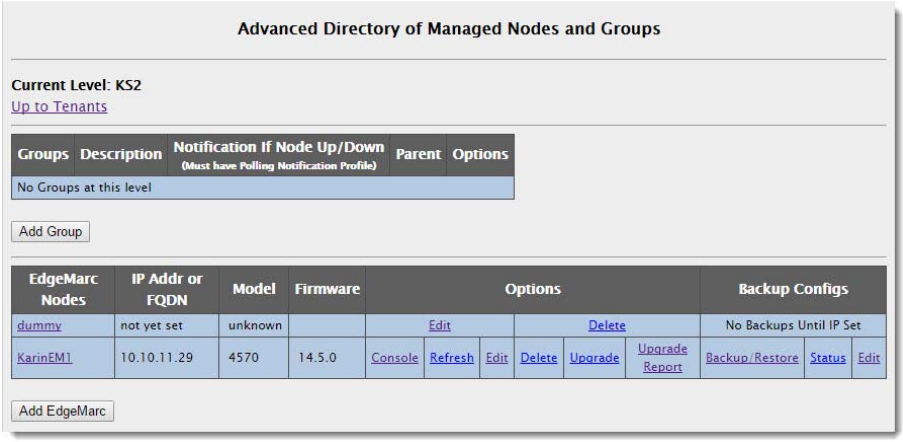
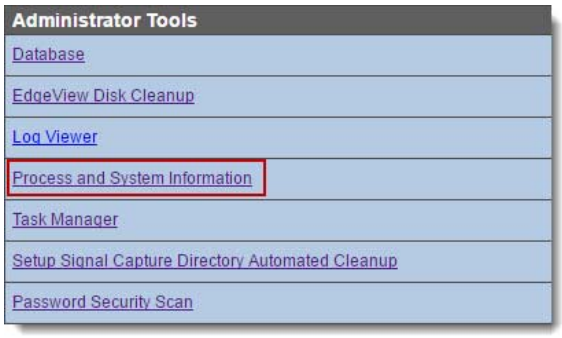
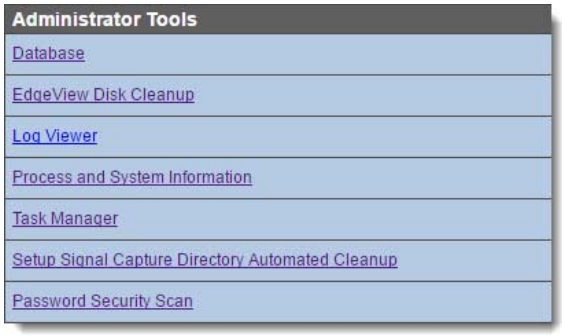
Specific Right	EdgeView Menu
Group Administration	Allows the user access to the Advanced Directory of Managed Nodes and Groups page for adding/editing/deleting nodes and groups and assigning attributes. 
Provisioning	Allows the user access to the **Process and System Information** page in the EdgeView Administrator Tools menu. 
System Administration 	Displays the **EV System** icon for accessing EdgeView Administrator Tools. 

Table 4-8 EdgeView Menus Associated with Specific Right Selections

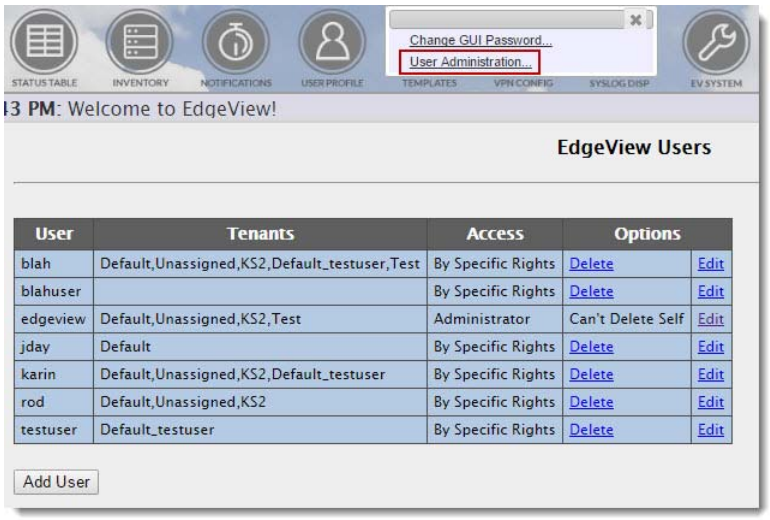
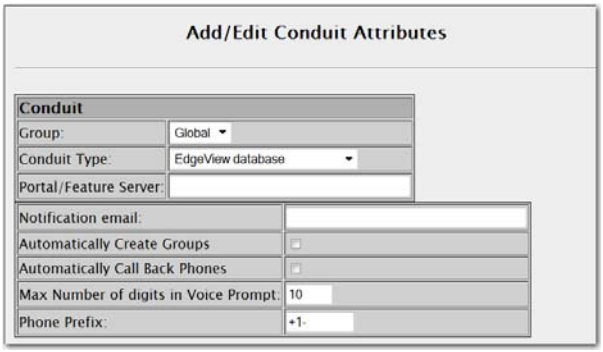
Specific Right	EdgeView Menu
User Administration 	Displays the **User Profile** icon for access to the EdgeView Users page. 
VPN Editing/Viewing 	Displays the **VPN Config** icon for access to the VPN editing and viewing features. 
Conduit Editing 	Displays the **Conduits** icon for access to the Add/Edit Conduit Attributes page. This is available only for licensed Plug & Dial systems. 

Table 4-8 EdgeView Menus Associated with Specific Right Selections

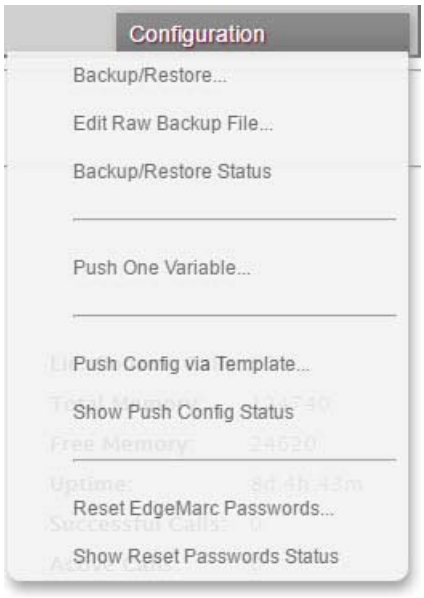
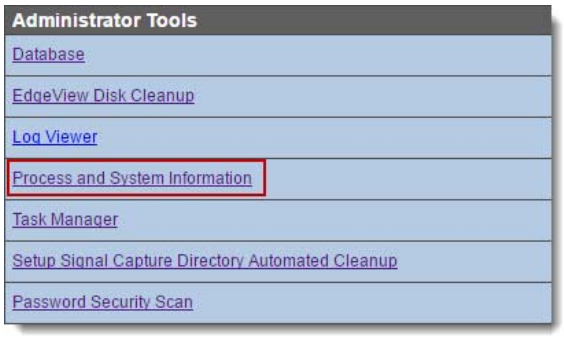
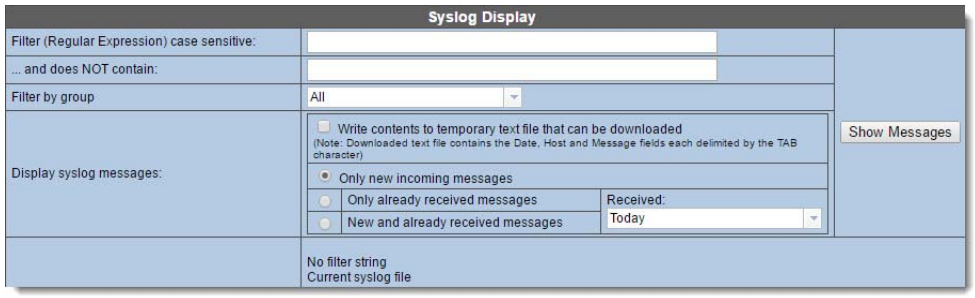
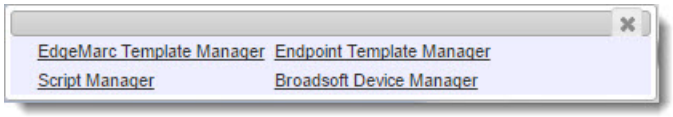
Specific Right	EdgeView Menu
Device Configuration	Allows the user access to the **Configuration** menu in the EdgeMarc Status page. 
Monitoring   	Allows the user access to the **Process and System Information** page in the EdgeView Administrator Tools menu. Minimally, a user should be allowed Monitoring rights so they can view their managed devices in EdgeView. 

Table 4-8 EdgeView Menus Associated with Specific Right Selections

Specific Right	EdgeView Menu
Syslog Viewing 	Displays the **Syslog Disp** icon to view syslog messages. 
Template Editing 	Displays the **Templates** icon for access to the Templates menu which includes options for managing EdgeMarc Template and Phone Template settings. 

Verifying User Access to EdgeView

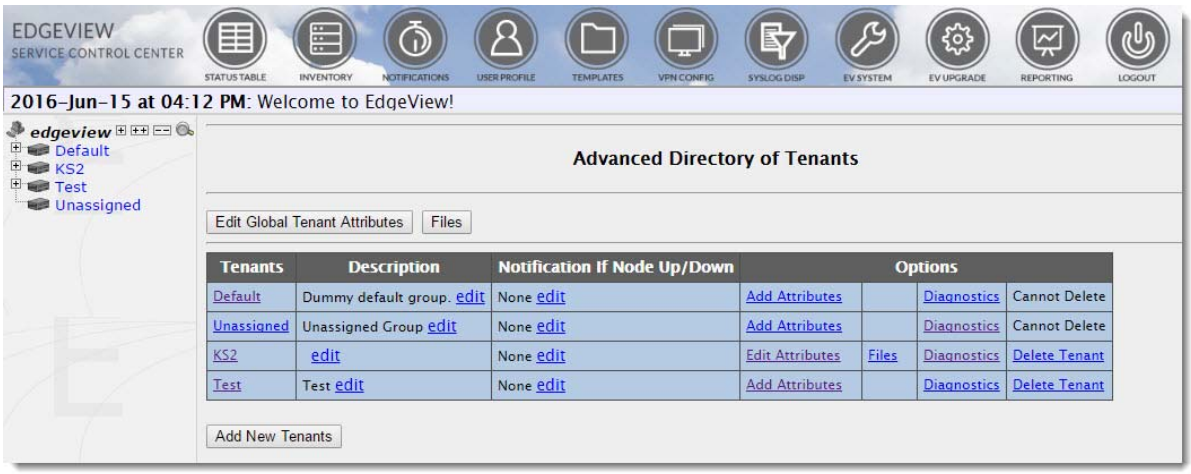
Once you have added a user and assigned specific rights, verify that the user has access to EdgeView and to the assigned features as follows:

1. Log out of EdgeView and close all browser windows.
2. Open a new browser window and log in using the username and password you set when you added the user.

When EdgeView comes up, it should show the username at the root level of the device tree, the Tenants the user is allowed to manage, and the icons for the specific rights set for this user.

Figure 4-31 shows users listed at the root level of the device tree along with the company and tenants the user is allowed to manage. The icon bar shows only the icons that were configured in EdgeView for each user.

Figure 4-31 Verifying a New User



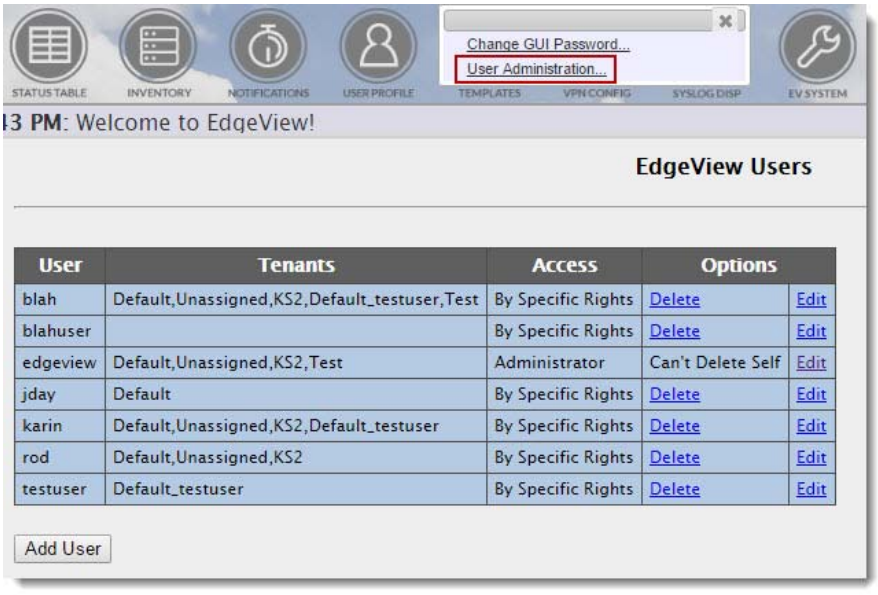
Managing Passwords



To change the password that administrators and end users use to access EdgeView:

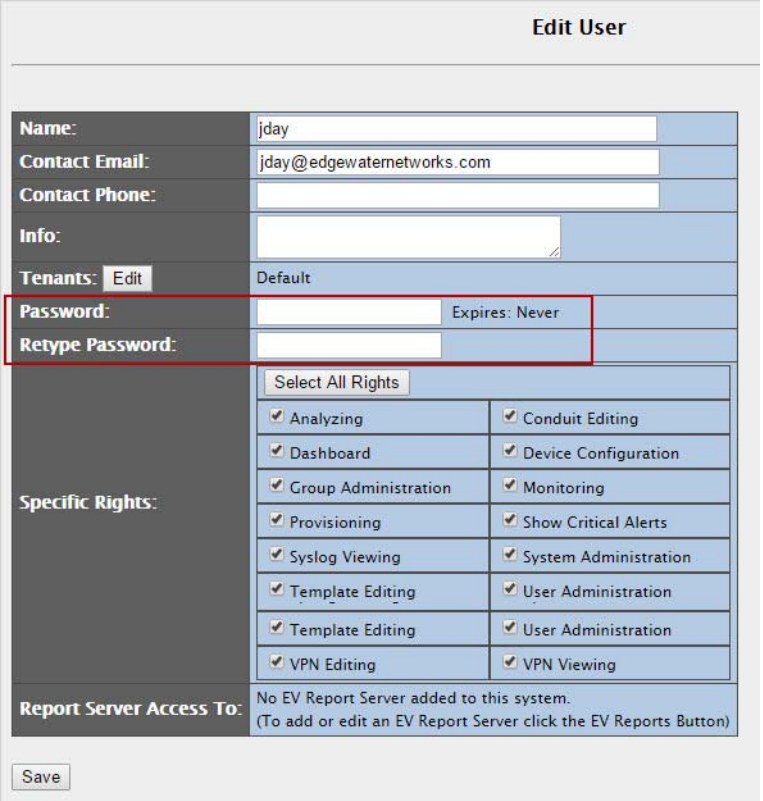
1. Log in to EdgeView and click **User Profile** > **User Administration**. The EdgeView Users page displays (Figure 4-32).

Figure 4-32 EdgeView Users Page



2. Click **Edit** in the Options column. The Edit User page displays (Figure 4-33).

Figure 4-33 Changing the EdgeView Password



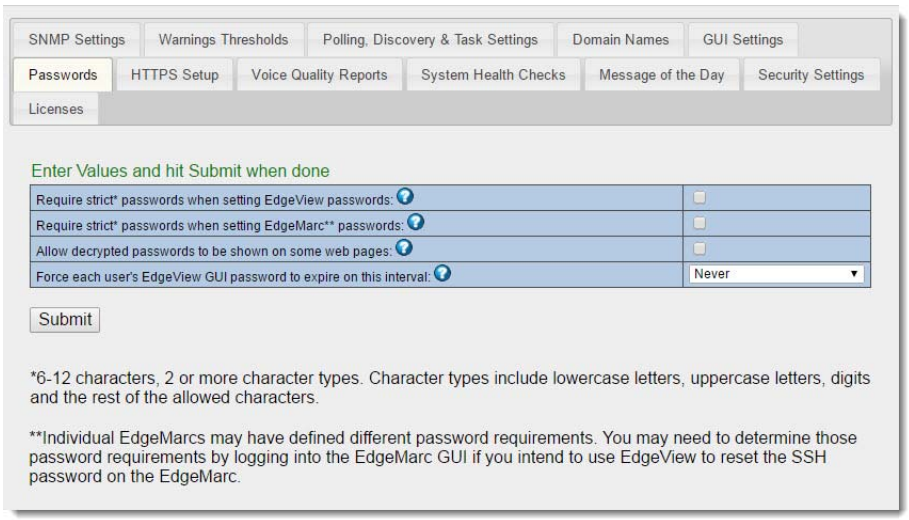
3. Type a new password in the **Password** and **Retype Password** fields. The password can be up to 100 characters.
4. Click **Save**. The EdgeView log in dialog box will display.
5. Log in with the new password.

Enforcing Strict Passwords

You can enforce a strict password when the user sets a password for EdgeView or an EdgeMarc. Strict passwords require 6-8 characters, two or more character types, and no dictionary words. Character types include lowercase letters, uppercase letters, digits and the rest of the allowed characters. The password restrictions are enforced when the user changes their password the first time they log in to EdgeView and when an EdgeMarc is added or changed in EdgeView. Strict passwords are disabled by default.

To set strict password settings, choose **EV System** > **System Settings** > **Passwords**. For more details, refer to Configuring Password Settings.

Figure 4-34 EdgeView Passwords Page



5

Managing EdgeView System Settings

This chapter describes how to use the EdgeView system tools to configure settings for EdgeView.

- Configuring EdgeView System Settings
- Starting an SSH Session in EdgeView via CLI
- Using Maintenance Mode
- Using EdgeView Administrator Tools
- Viewing Active Troubleshooting Jobs
- Viewing the Current Software Version and Patches Installed on EdgeView

Configuring EdgeView System Settings



The System Settings menu is the central point for EdgeView system-wide global configurations. The settings you configure here apply to all nodes managed by EdgeView.

To access the EdgeView Settings:

1. Choose **EV System** > **System Settings** (Figure).

Figure 5-1 System Settings

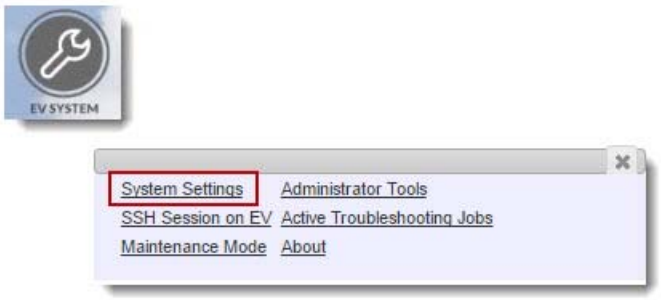


Figure 5-2 EdgeView System Menu > System Settings

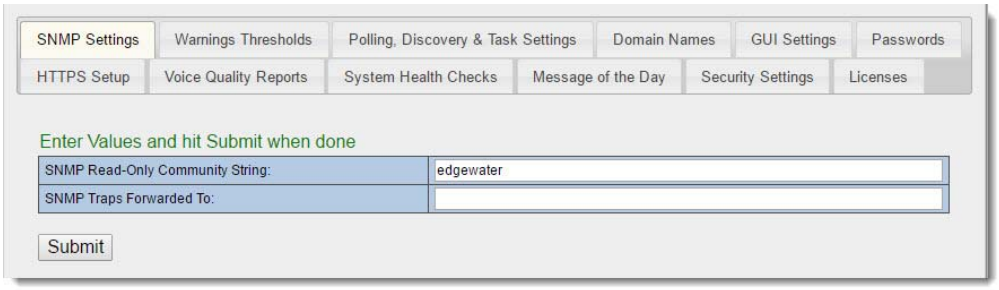


Table 5-1 defines the tabs on the System Settings page.

Table 5-1 System Settings Tabs

Tab	Use this tab to...
SNMP Settings	Configure an SNMP Read-Only Community String and where to forward SNMP Traps. See "Configuring SNMP Network Management Settings."
Warnings Thresholds	Configure warning thresholds for transmit and receive errors and MOS scoring. See "Setting Warning Thresholds."
Polling, Discovery and Task Settings	Enable SNMP polling and set the polling interval. You also use this tab to enable/disable auto-discovery and change auto-discovery settings. See "Configuring Polling and Discovery Settings."
Domain Names	Enable Reverse DNS Lookup in EdgeView so that EdgeView sends SNMP traps to a FQDN rather than to an IP address. See "Enabling Reverse DNS Lookup Settings."
GUI Settings	Set the GUI timeout value and customize the device tree display. See "Setting the EdgeView GUI Timeout Value" and "Setting the EdgeView GUI Timeout Value."
Passwords	Enforce a strict password when the user sets a password for EdgeView or an EdgeMarc. See "Configuring Password Settings."
HTTPS Setup	Configure EdgeView for HTTPS. See "Setting Up HTTPS for EdgeView."

Table 5-1 System Settings Tabs

Tab	Use this tab to...
Voice Quality Reports	Configure EdgeView to capture the MOS score generated directly by the IP phone (through the SIP Publish method) for voice quality reporting. See "Capturing Phone MOS Scores."
System Health Checks	Set up and schedule daily system checks. See "Setting Up and Scheduling Daily System Health Checks."
Message of the Day	Set the message of the day that displays in the status bar. See "Setting a Message of the Day."
Security Settings	Configure EdgeView enhanced security settings which allow you to restrict and/or allow access to EdgeView, enable Anonymous FTP, and open FTP ports to all sites. See "Configuring EdgeView System Security Settings."
Licenses	Install the EdgeView Product and Support License keys for the first time, update your product license key when you add nodes to EdgeView, and activate your support license after renewal. See "EdgeView Licenses."

Configuring SNMP Network Management Settings

1. Choose **EV System** > **System Settings** (Figure).

When you first open the EV System settings page, the **SNMP Settings** tab displays (Figure 5-2). Use the information in Table 5-2 to configure the following SNMP settings for EdgeView.

Figure 5-3 Configuring SNMP Settings

Table 5-2 SNMP Settings

Field	Description
SNMP Read-Only Community String	The SNMP "password" which allows outside network management systems access to EdgeView. Default = public 127.0.0.1
SNMP Traps Forwarded To:	The IP address of the network management system to which EdgeView will forwards traps.

Default SNMP Settings in EdgeView

By default, the SNMP Read-Only Community String is set to public 127.0.0.1. The default setting ensures that only EdgeView can access the EdgeView SNMP MIBs. If you are *accessing* the EdgeView itself via SNMP (NOT the same as *using* SNMP to access EdgeMarcs), you need to do two things to make SNMP work on EdgeView:

2. Remove the public 127.0.0.1 IP address so that other computers can access EdgeView, and
3. Open the Firewall UDP port 161.

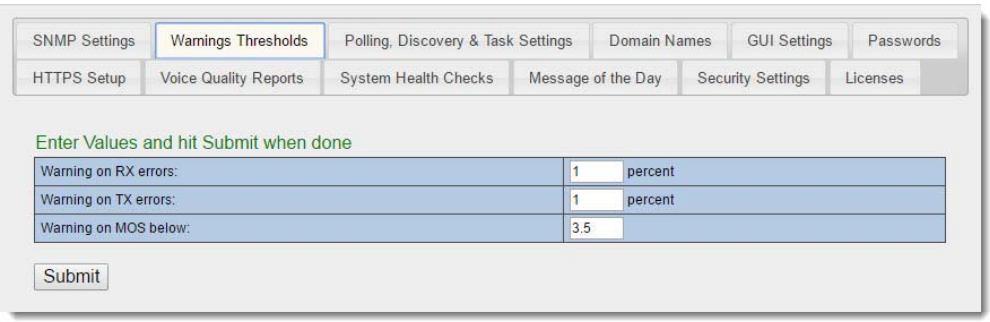
Once you have changed these settings, you should be able to access the EdgeView MIBs via SNMP. Note that once you remove the 127.0.0.1

address, you cannot add it back; you must use the firewall to block other computers from accessing the EdgeView MIBs.

Setting Warning Thresholds

1. Choose **EV System** > **System Settings** (Figure).
2. Select the **Warnings Thresholds** tab from the System Settings page (Figure).

Figure 5-4 Configuring Warning Thresholds



3. Configure the following warning thresholds:

Warning on RX Errors

At the specified device polling interval, EdgeView retrieves interface statistics from all live interfaces on the EdgeMarc, including error statistics. You can specify a percentage here that tells EdgeView to display a warning when the percentage of receive errors on a given interface exceeds the threshold. When an EdgeMarc or other interface exceeds the error threshold, it will be listed in yellow in the device tree and on the EdgeMarc Status page. The default warning error threshold is 10 percent.

Warning on TX Errors

You can specify a percentage here that tells EdgeView to display a warning when the percentage of transmit errors on a given interface exceeds the threshold. Default = 10 percent. See description above.

Warning on MOS Below

At the specified device polling interval, EdgeView calculates an average MOS score for the last 25 calls. If the average MOS score falls below the number specified here, the EdgeMarc will be shown as yellow in the device tree and in the EdgeMarc Status page. The default MOS score threshold is 2.5.

Configuring Polling and Discovery Settings

1. Choose **EV System** > **System Settings** (Figure).
2. Select the **Polling & Discovery Settings** tab on the System Settings page to set the node polling interval, SSH timeout, enable SNMP polling, and configure auto discovery settings using the information in Table 5-3.

Caution

Do not change the Node Polling Interval and SSH Timeout unless there are performance problems usually due to a slow network or a heavily loaded system. These settings should only be changed when recommended by your Support Representative.

Figure 5-5 Polling and Discovery Tab

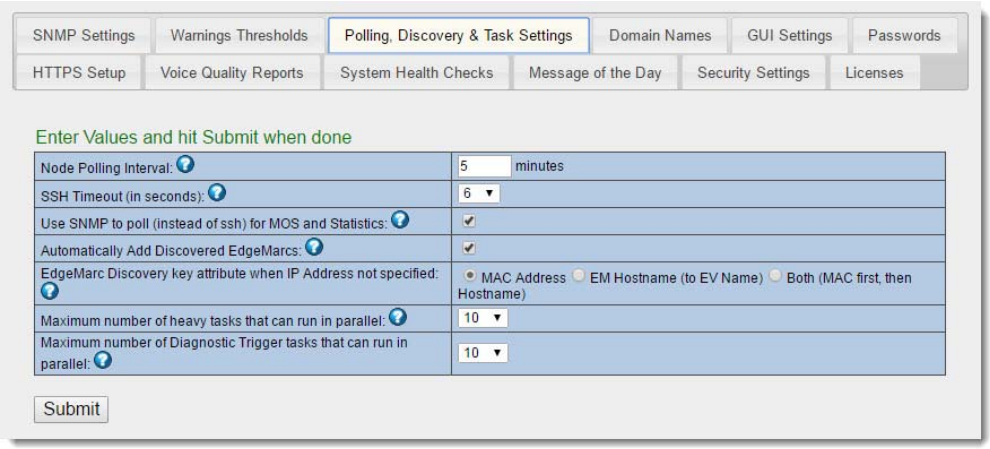


Table 5-3 Polling Settings

Field	Description
Node Polling Interval	The polling frequency. The default is every 5 minutes.
SSH Timeout (in seconds)	Timeout in seconds that EdgeView waits for a response from an SSH command into a node. The minimum default value is 6 seconds. Increase above the minimum only if nodes are showing status DOWN but are accessible via SSH.
Use SNMP to poll (instead of ssh) for MOS and Statistics	Enables SNMP polling for EdgeView.
Automatically Add Discovered EdgeMarcs	Enables/disables auto-discovery of EdgeMarcs. Auto-discovery is enabled by default.

Table 5-3 Polling Settings

Field	Description
EdgeMarc Discovery key attribute when IP Address not specified	Sets the matching criteria for auto discovering EdgeMarcs. See Specifying Matching Criteria for Auto-Discovery on page 130 for more details.

SSH Polling with EdgeView

By default, EdgeView polls EdgeMarcs through SSH to determine whether the EdgeMarc is up or down and to gather certain types of data such as:

- Number of active calls
- Successful calls
- Average MOS
- Licensed number of concurrent calls
- Total memory and free memory
- Uptime

SNMP Polling with EdgeView

EdgeView optionally supports SNMPv1 polling which has much less overhead than SSH and thus can poll more EdgeMarcs within a given time period. SNMP polling is recommended method to poll EdgeMarcs.

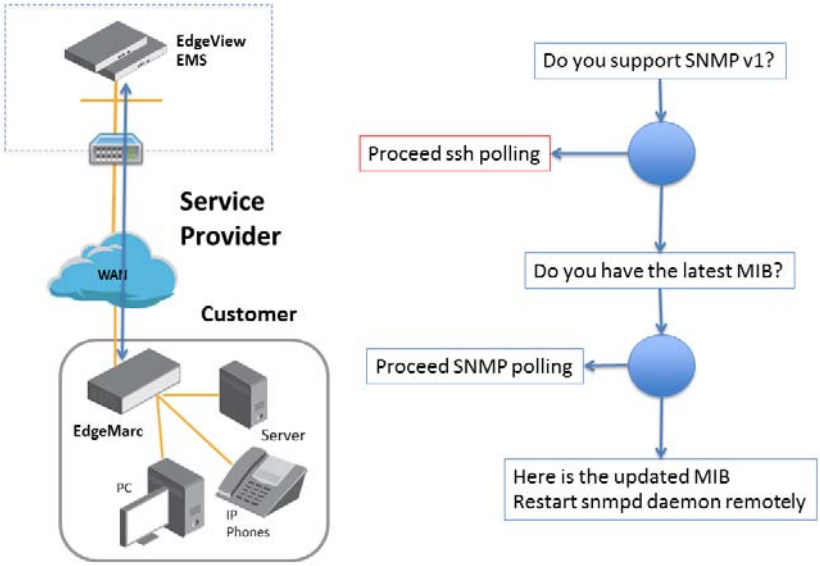
Due to the high overhead of SSH, the number of EdgeMarcs that can complete in a given poll cycle is limited to 1,000 in a default 5 minute Node Polling Interval (actual number depends on several factors). If your deployment has more than a thousand EdgeMarcs, use SNMP polling to ensure the polling cycle completes. The SNMP polling method has much less overhead and is therefore much more efficient. Depending on the platform and other factors, the SNMP method can typically support 10 to 50 times the number of EdgeMarcs.

Understanding Polling on EdgeView

During the polling cycle, EdgeView checks if SNMPv1 is supported on the EdgeMarc (through SSH polling). If it is supported, EdgeView checks the MIB on each EdgeMarc to ensure it is up-to-date. For a given EdgeMarc, if it is NOT up-to-date, EdgeView will push an update to the EdgeMarc and restart the snmpd daemon. Once this process is complete, the EdgeMarc will be polled through SNMP. This does not interrupt any calls.

If an EdgeMarc does not support SNMP, EdgeView will continue to poll that EdgeMarc through SSH until the EdgeMarc configuration is changed. Figure 5-6 illustrates the polling process flow.

Figure 5-6 EdgeView Polling Process Flow

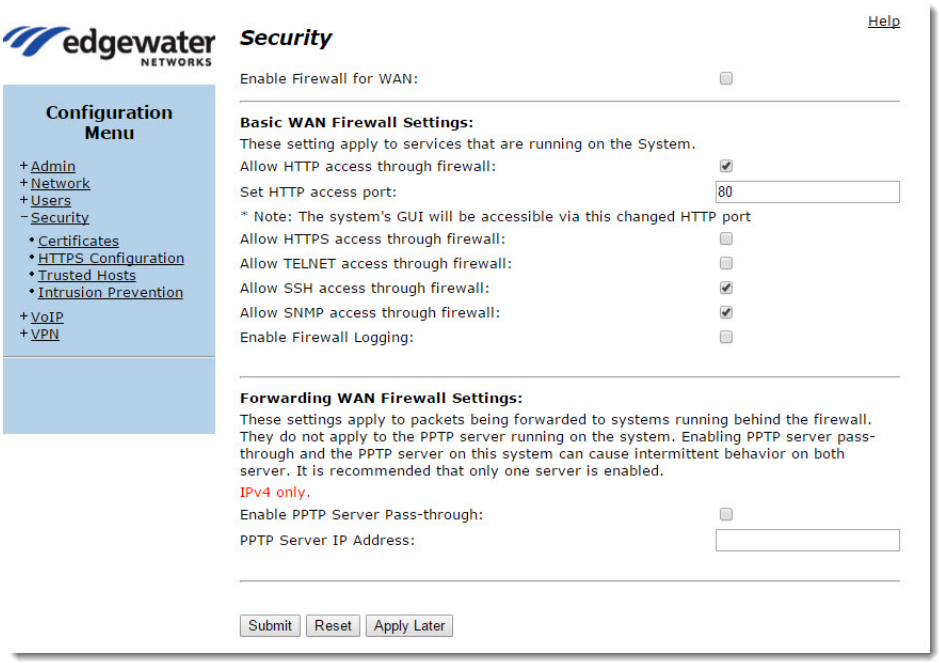


Configuring the EdgeMarc for SNMP Polling

The steps below assume you are starting from the factory default settings. Refer to the *EdgeMarc VOS User Guide* for more detailed information on the different EdgeMarc configuration steps.

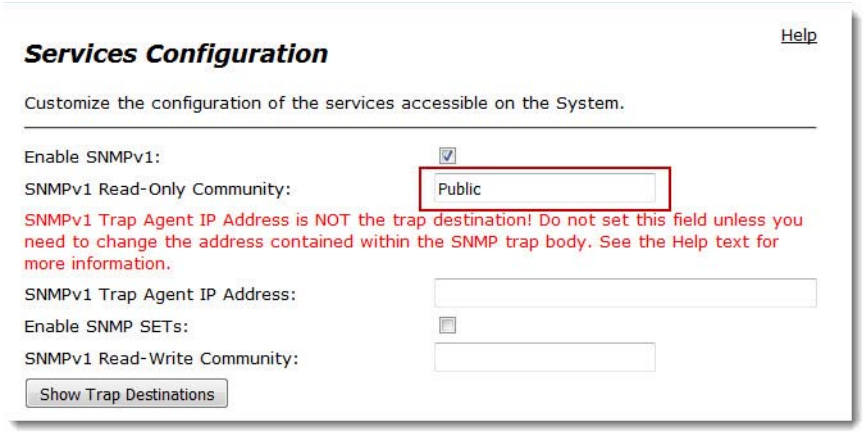
1. Open a web browser and enter the IP address of the EdgeMarc in the **URL** line: http://192.168.1.1
2. From the EdgeMarc Configuration Menu, choose **Security** (Figure 5-7).

Figure 5-7 Configuring the EdgeMarc for SNMP Polling



3. On the EdgeMarc Security page, enable the following fields:
   - Allow HTTP access through firewall
   - Allow SSH access through firewall
   - Allow SNMP access through firewall
4. Click **Submit** or **Apply Later** to validate.
5. From the EdgeMarc Configuration menu, choose **Admin** > **Services Configuration**. The EdgeMarc Services Configuration page displays (Figure 5-8).

Figure 5-8 EdgeMarc Services Configuration Page



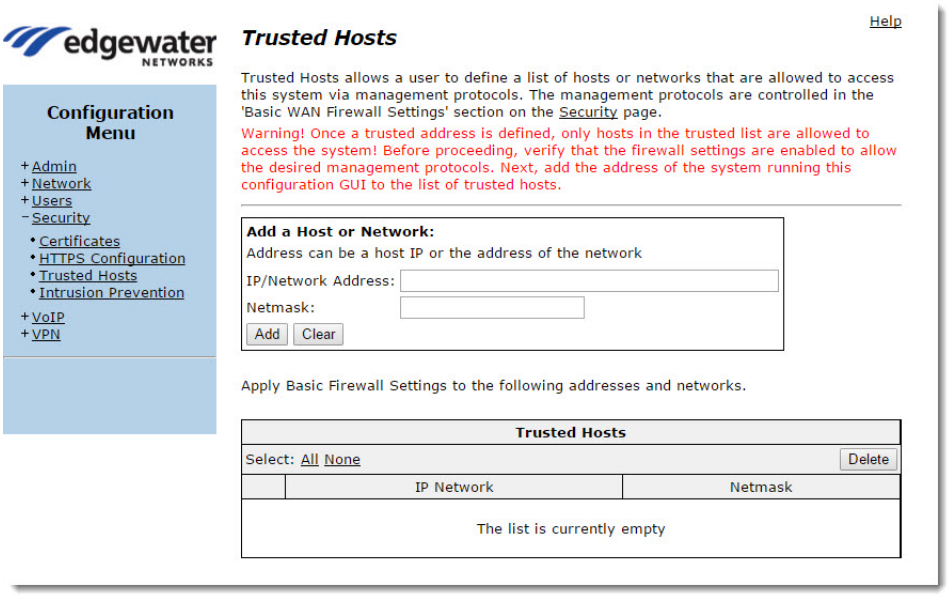
6. Set the following fields to allow the EdgeMarc to expose its SNMP MIBs to the EdgeView (or to a third party).
   - Select the **Enable SNMP v1** checkbox.
   - Enter **Public** in the **SNMP v1 Read-Only Community** field.
   - Click **Submit** or **Apply Later** to validate.

Note

The SNMP v1 Read-Only Community field must be specified in order to enable SNMP v1.

7. If using trusted management, add EdgeView as a trusted host:
   a. From the EdgeMarc Configuration menu, select **Security** > **Trusted Hosts**.
   b. Enter the EdgeView IP address and Netmask and click **Add** (Figure 5-9).

Figure 5-9 Adding EdgeView as a Trusted Host



Changing the Node Polling Interval

EdgeView polls each node according to the frequency defined on the EdgeView Polling & Discovery Settings page. The default is every 5 minutes. You typically only need to increase this number if you have too many EdgeMarcs for your particular system and EdgeView cannot complete the 5 minute polling cycle.

To change the node polling interval, enter a new value for the **Node Polling Interval** on the Polling & Discovery tab and click **Submit**.

Enabling/Disabling Auto-Discovery

By default, EdgeView automatically discovers EdgeMarcs when they come online. To disable this setting, disable the **Automatically Add Discovered EdgeMarcs** checkbox on the **Polling & Discovery Settings** tab and click **Submit**.

See Adding an EdgeMarc via Auto-Discovery on page 26 for more details.

Specifying Matching Criteria for Auto-Discovery

When EdgeView auto-discovers an EdgeMarc that does not have an IP address, you can set matching criteria so that EdgeView can identify the EdgeMarc, assign it an IP address, and automatically add it to the EdgeView database. You set this criteria on the Polling & Discovery page in

the **EdgeMarc Discovery key attribute when IP Address not specified:** field.

Here's how the matching criteria works:

- If you set this option to **MAC Address** (the default setting), EdgeView will first check its database for the EdgeMarc MAC address. If it finds the MAC address in the database, EdgeView will assign the EdgeMarc an IP address, add it to the database, and push out the configuration (if set) to the EdgeMarc.
- If you set this option to **EM Hostname (to EV Name)**, EdgeView will first check to see if the hostname for the EdgeMarc matches the hostname in the EdgeView database. If there is a match, EdgeView will assign it an IP address, add it to the database, and push out the configuration (if set) to the EdgeMarc.
- If you set this field to **Both**, EdgeView will first try to match the EdgeMarc MAC address and then attempt to match the EdgeMarc hostname before assigning it an IP address and pushing out the configuration (if set) to the EdgeMarc.

You can set matching criteria so that EdgeView can identify an EdgeMarc during auto-discovery, assign it an IP address, and automatically add it to the EdgeView database.

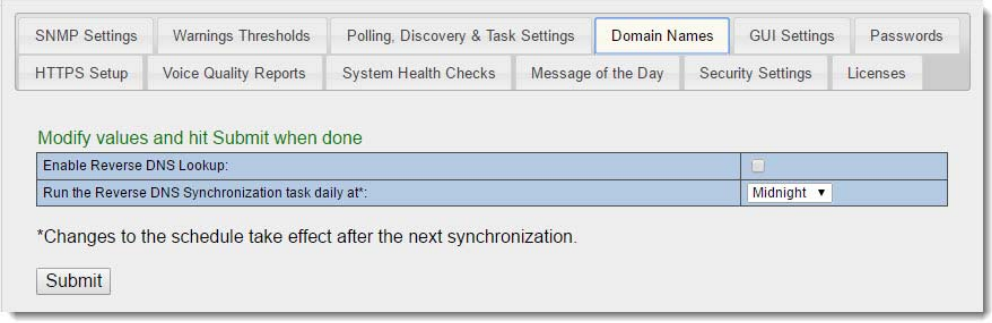
Enabling Reverse DNS Lookup Settings

By default, SNMP traps initiated by EdgeView to an EdgeMarc are sent to the EdgeMarc IP address. However, some network management systems (NMS) track edge devices by Fully Qualified Domain Name (FQSN) rather than by IP address. In these cases, you need to enable Reverse DNS Lookup in EdgeView so that EdgeView sends SNMP traps to a FQDN rather than to an IP address. This allows the NMS to properly associate the SNMP trap with the correct EdgeMarc. You should also enable reverse DNS lookup if the EdgeMarc is configured to send SNMP traps to a FQDN.

To enable reverse DNS lookup:

1. Choose **EV System** > **System Settings.**
2. Click the **Domain Names** tab. (Figure 5-10).
3. Enable the **Enable DNS Lookup** checkbox.
4. Click **Submit**.

Figure 5-10 Enabling Reverse DNS Lookup



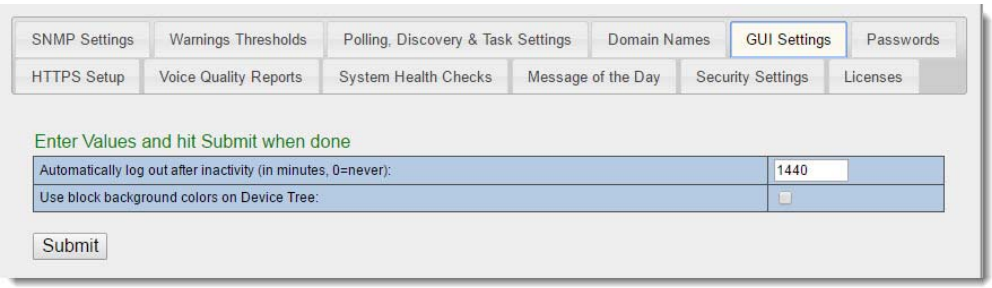
Setting the EdgeView GUI Timeout Value

If there is inactivity on the EdgeView GUI for a configured number of minutes, EdgeView will automatically log out the user. The default is 1440 minutes.

To set the number of minutes of inactivity before the user is logged out:

1. Choose **EV System** > **System Settings**.
2. Click the **GUI Settings** tab (Figure 5-11).
3. In the **Automatically Log Out After inactivity (in minutes 0=never)** enter the number of minutes.
4. Click **Submit**.

Figure 5-11 Setting the EdgeView GUI Timeout Value



Customizing the Device Tree Display

The device tree uses different font colors to list nodes and to indicate node status. Alternatively, the device tree can display nodes with a colored block background instead of using colored fonts. Nodes in the Up status are shown with a green background and nodes in the Down status are shown

with a red background. This can make it easier to see at-a-glance which nodes are in the down status.

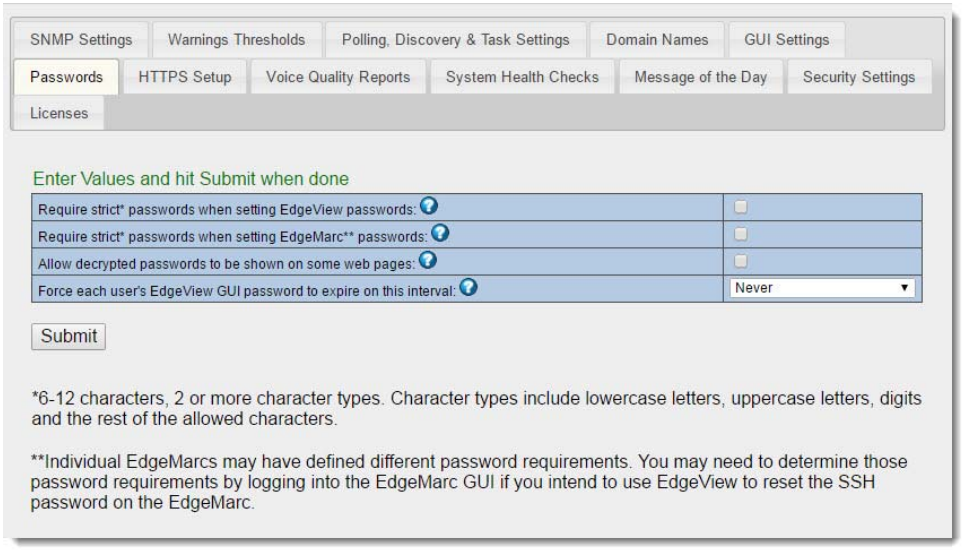
To change the device tree node display to use block background colors:

1. Choose **EV System** > **System Settings**.
2. Select the **GUI Settings** tab.
3. Select the **Use block background colors on Device Tree** checkbox (Figure).
4. Click **Submit**. The new setting will take effect after the next polling cycle.

Configuring Password Settings

Use the **Passwords** tab (Figure 5-12) to configure settings for enforcing strict passwords for EdgeView and EdgeMarc, showing decrypted passwords in some EdgeView web pages, and setting an interval to force users to change their GUI password.

Figure 5-12 Passwords Tab



Enforcing Strict Passwords

You can enforce a strict password when the user sets a password for EdgeView or an EdgeMarc. Strict passwords require 6-8 characters, two or more character types, and no dictionary words. Character types include lowercase letters, uppercase letters, digits and the rest of the allowed characters. The password restrictions are enforced when an EdgeMarc is added or changed in EdgeView. The restrictions are also imposed when you reset EdgeMarc passwords at the top level (**Node Configurations** > **EdgeMarc Passwords** > **Reset EdgeMarc Passwords)**. Strict passwords are disabled by default.

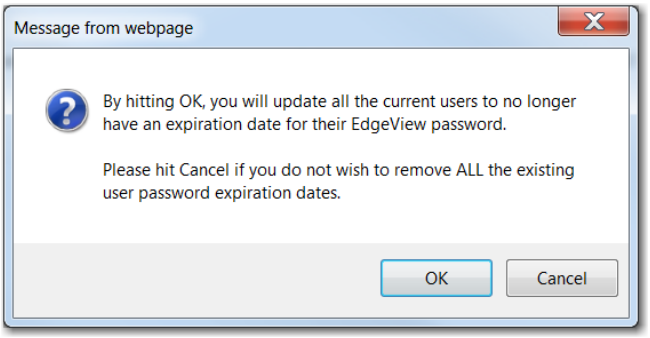
To enable a strict password:

1. Choose **EV System** > **System Settings**.
2. Select the **Passwords** tab.
3. Enable the **Require strict passwords when setting EdgeView Passwords** and/or **Require strict passwords when setting EdgeMarc Passwords** checkbox.
4. Click **Submit**.

Showing Decrypted Passwords

By default, decrypted passwords are not shown on the Add/Edit Attributes page. If you prefer to make those passwords visible to the user, change the setting as follows:

1. Choose **EV System** > **System Settings**.
2. Select the **Passwords** tab.
3. Enable the **Allow decrypted passwords to be shown on some web pages** checkbox.
4. Click **Submit**. The following popup will display to warn you that enabling this setting will cancel the forced password expiration date for all existing EdgeView user password expiration dates.



Caution

Due to security implications, use caution when allowing decrypted passwords to be displayed in EdgeView.

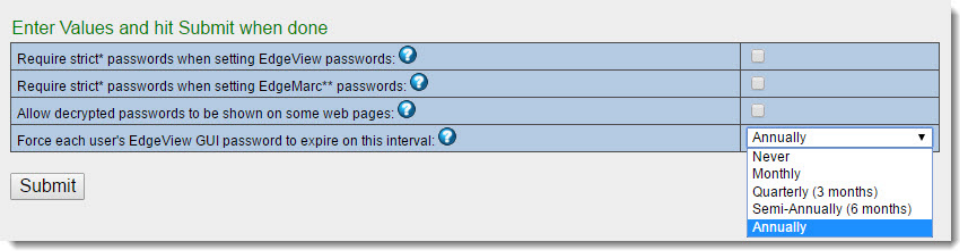
Forcing Users to Change Their Password

You can configure settings that force users to change their EdgeView GUI password on a routine basis.

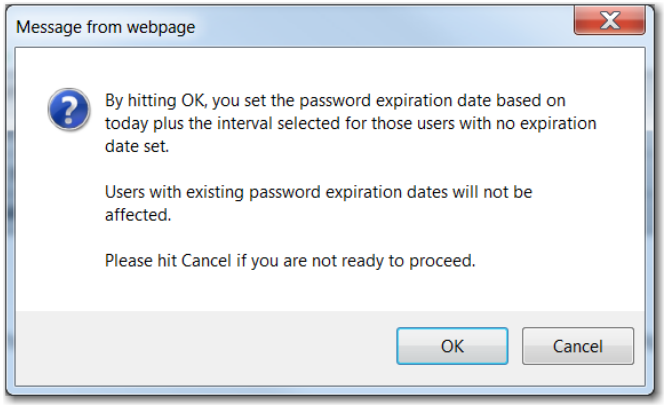
To force a password reset:

1. Choose **EV System** > **System Settings** > **Passwords** (Figure 5-13).

Figure 5-13 Forcing a Password Change



2. From the drop-down menu for **Force each user's EdgeView GUI password to expire on this interval**, select the interval after which the password will expire.
3. Click **Submit**. The following popup will display to notify you that the password expiration date will be applied only to users with no expiration date set.



4. Click **OK**.

When the expiration date is reached and the user tries to authenticate through the GUI, they will be forced to enter a new password before any EdgeView operations can be performed. The selected interval will be used to set a new expiration date when the password is changed.

Setting Up HTTPS for EdgeView

To configure EdgeView for HTTPS, follow these steps:



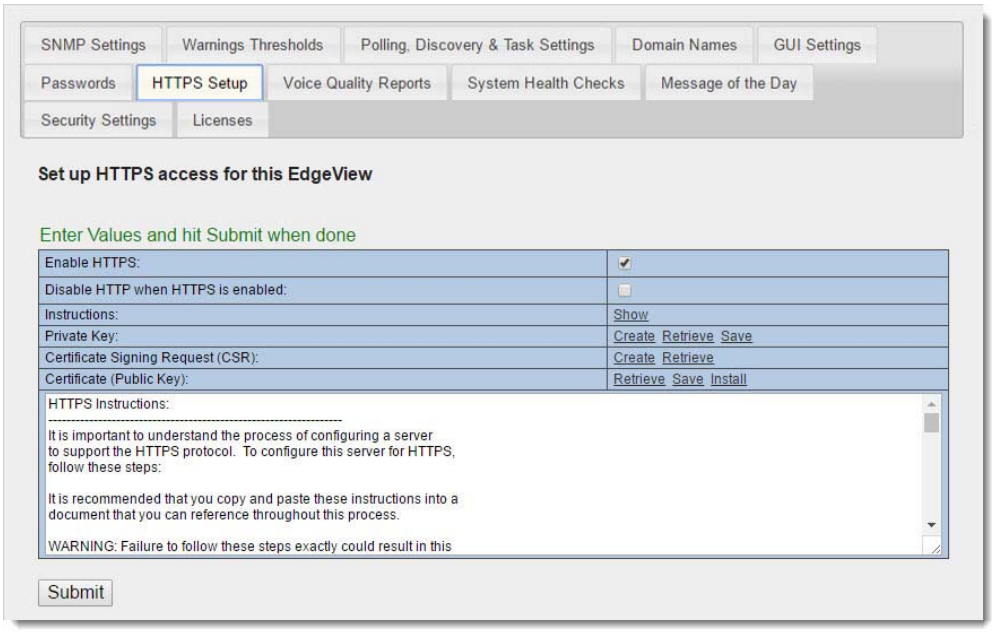
Caution

Failure to follow these steps exactly could result in this EdgeView becoming unreachable via the web GUI. Recovery of the web GUI is can be accomplished by accessing this EdgeView via SSH and issuing the following command /ewn/ssl/ssl_enable.pl

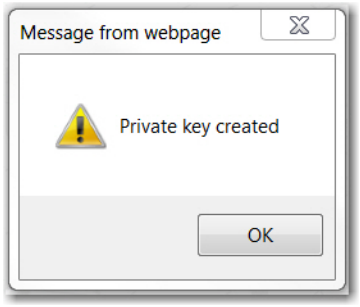
1. Choose **EV System** > **System Settings**.

2. Select the **HTTPS Setup** tab (Figure 5-14).

Figure 5-14 Setting Up HTTPS for EdgeView



3. Enable the **Enable HTTPS** checkbox.
4. Click the **Show** link to view instructions about setting up HTTPS. These instructions are repeated here for your reference.
5. Create a private key (if you don't already have one):
   a. Click the **Create** link to the right of the Private Key label. Once the key has been created, the following message box displays:



   b. To view the private key, click the **Retrieve** link. The key will display in the text box.
   c. Click **Save** to save the private key.
   d. Optionally, copy the private key to a file on your EdgeView local drive (for backup purposes).
6. To upload an existing private key, copy and paste it into the text box and click the **Save** link to the right of the **Private Key** label.

7. Create a Certificate Signing Request (CSR) which can be used when purchasing an SSL certificate from a certificate authority such as Verisign:
   a. Click the **Create** link to the right of the CSR label.
   b. Enter the CSR details in the CSR form and click **Create CSR**. The CSR will be created and displayed in the text box.
8. Copy the CSR from the text box and save it in a file on your EdgeView local drive.
9. Purchase an SSL Certificate from a certificate authority.
10. Save the SSL certificate to your EdgeView local drive.
11. Copy the certificate and paste it into the text box on the HTTPS Setup screen.
12. Click the **Save** link to the right of the **Certificate (Public Key)** label.
13. Click the **Install** link to the right of the Certificate (Public Key) label to install the SSL certificate and private key.
14. Check the **Enable HTTPS** checkbox.
15. Click **Submit**.

Capturing Phone MOS Scores

To configure EdgeView to capture the MOS score generated directly by the IP phone (through the SIP Publish method) for voice quality reporting.

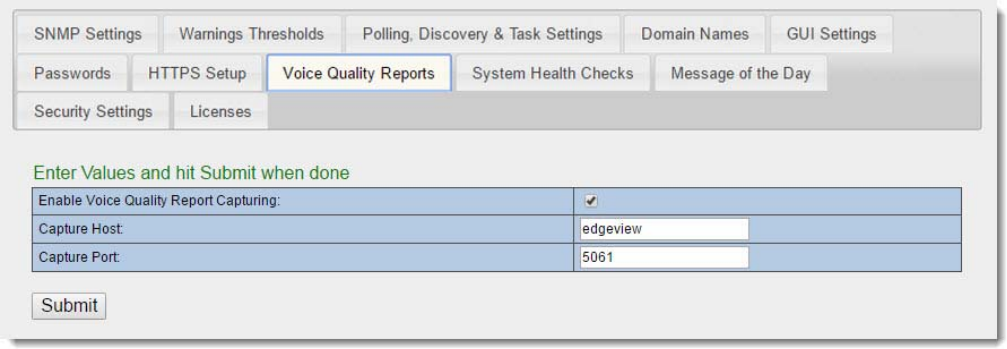


Note

The phones must be behind an EdgeMarc monitored by EdgeView.

1. Choose **EV System** > **System Settings**.
2. Select the **Voice Quality Reports** tab.
3. Configure the following settings:
   a. Enable the **Voice Quality Capturing** checkbox.
   b. Enter a value for the **Capture Interface**. The default is eth0.
   c. Enter a **Capture Host Name**. The default is edgeview.
   d. Specify a **Capture Port**. The default is 5061.
4. Click **Submit**.

Figure 5-15 Configuring Phone MOS Scores



Setting Up and Scheduling Daily System Health Checks

EdgeView can perform daily system checks and send the resulting error reports in email to your support organization or support representative. It is highly recommended that you set up and schedule daily system checks.

To setup and schedule daily system checks:

1. Choose **EV System** > **System Settings**.
2. Select the **System Health Checks** tab (Figure 5-16).
3. Mouse over the question mark icons to display details about how to configure each setting.
4. Click **Submit**.

Figure 5-16 Configuring Daily System Checks

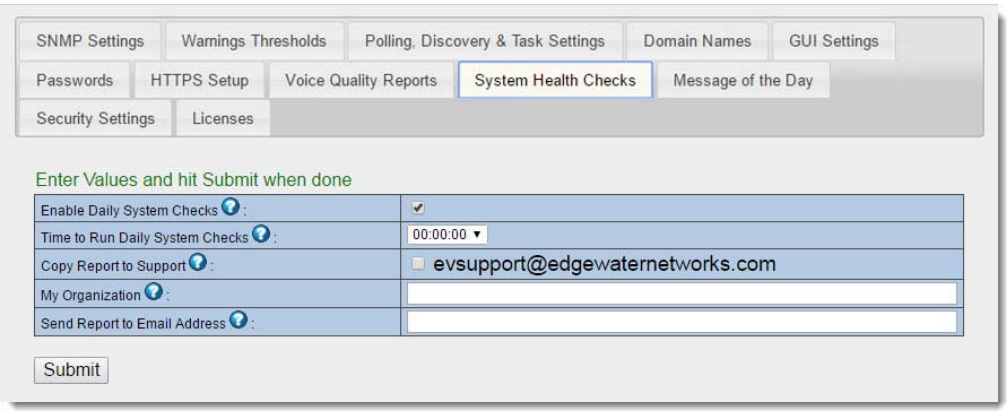


Table 5-4 System Health Check Settings

Field	Description
Enable Daily System Checks	Check this box to send a daily sanity report to the email address and optionally a support representative to validate that your system is running optimally.
Time to Run Daily System Checks	Enter the time of day you want EdgeView to run the report. The report can be database intensive so try to specify the time of day when the system is used least.
Copy Report to Support	Check this box if you want the sanity report to also be sent to your Edgewater Networks support representative at support@edgewaternetworks.com.
My Organization	Enter a name for your company/organization so that the Edgewater Networks support representative can associate the report with your organization.
Send Report to Email Address	Enter a comma-separated list of email addresses which will receive the sanity report from EdgeView.

Setting a Message of the Day

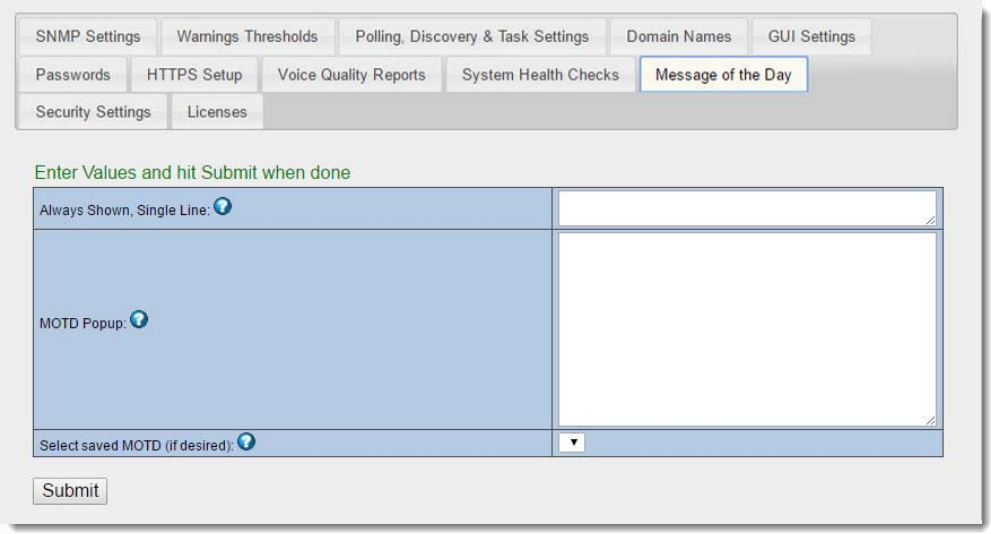
You can set a “Message of the Day” (MOTD) to be displayed in a single line at all times above the device tree (up to 100 characters). Additionally, you can set a multi-line alert message which displays in a popup when a user logs in to EdgeView. Once a MOTD has been submitted, it will be added to the MOTD drop-down menu for you to select and reuse, if desired.

If you change the MOTD, the new message will be displayed in EdgeView when the user refreshes their browser. In addition, the message will continue to display after a full day even if the user does not close the browser but refreshes it.

To set the message of the day:

1. Choose **EV System** > **System Settings**.
2. Select the **Message of the Day** tab (Figure 5-17).

Figure 5-17 Setting a Message of the Day



3. Configure MOTD settings as follows:
   - In the **Always Shown, Single line** box, type a message of the day you want to display in a single line above the device tree. The message can be up to 100 characters.
   - In the **MOTD Popup** box, type a multi-line message to be shown to the user in a popup when they log in to EdgeView. For example, you could enter a disclaimer. After you enter the text, a test pop up will be displayed so you can see what the message looks like before saving it.
   - If you want to use a MOTD which has been used previously, select it from the **Saved MOTD** drop down box.
4. Click **Submit**.

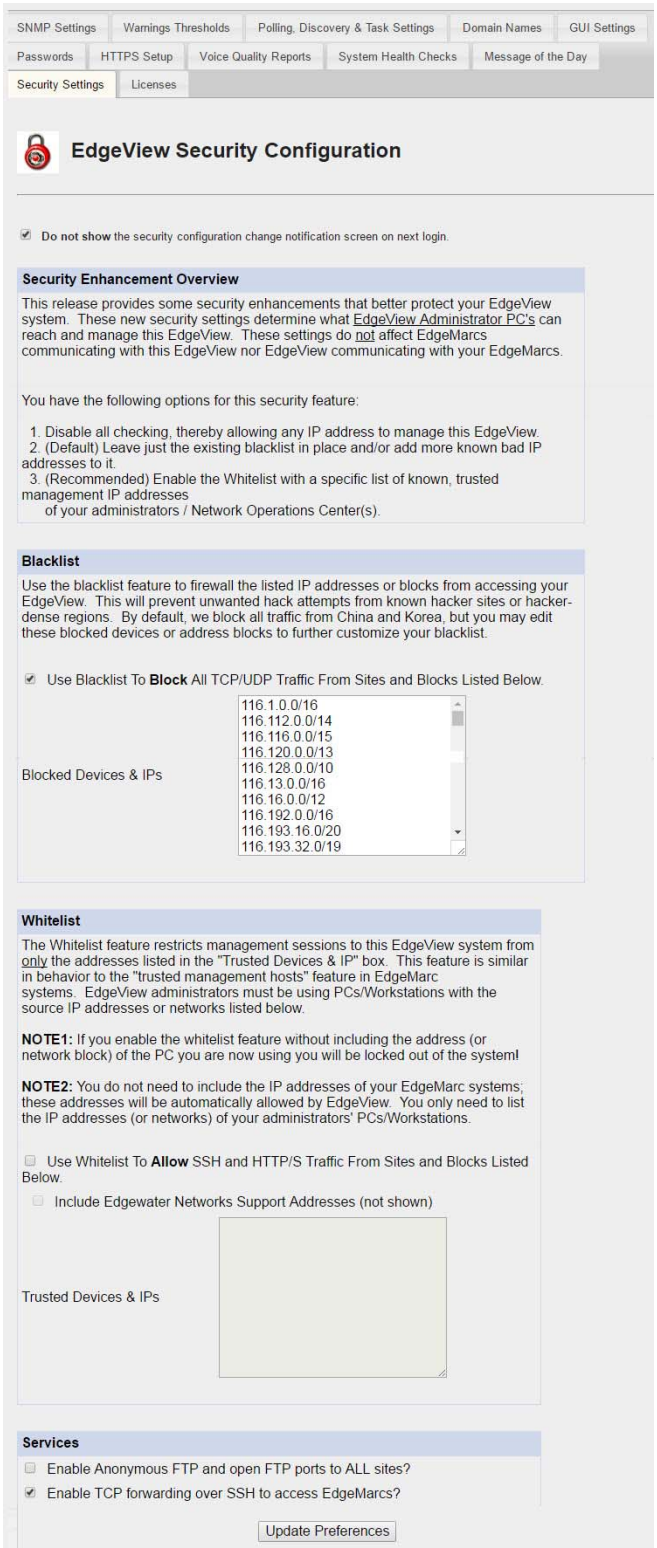
Configuring EdgeView System Security Settings

The **Security Settings** tab displays the EdgeView Security Configuration page which provides an overview of the enhanced EdgeView security features as well as descriptions and instructions for using the Blacklist and Whitelist features to restrict and enable access through the firewall. You can also enable Anonymous FTP and open FTP ports to all sites from this page. Review the System Security page thoroughly to ensure EdgeView follows the security policy for your organization.

Note

Edgewater strongly recommends that you specify a Whitelist to ensure EdgeView is not accessible to unauthorized users. By default, all EdgeMarcs and EdgeConnects in the device tree are in the Whitelist.

Figure 5-18 EdgeView System Security Page



Tip

This page is also accessible from the EdgeView Security Change Notification page (which displays at log in). If you prefer not to view this page each time you log in to EdgeView, enable the **Do not show security configuration change notification screen on next login** checkbox.

Note

Edgewater Networks strongly recommends that you specify a Whitelist to ensure EdgeView is not accessible to unauthorized users.

Note

When EdgeView applies a Blacklist and Whitelist, it applies the Blacklist first and then it applies the Whitelist.

Configuring a Blacklist

Blacklists allow you to block persistent hacking attempts by specifying a list of IP addresses that will be completely blocked from accessing EdgeView. Any input to EdgeView from these IP addresses is dropped.

If you have an EdgeView outside the firewall, the IP address of the EdgeView specified here must be managed inside the firewall.

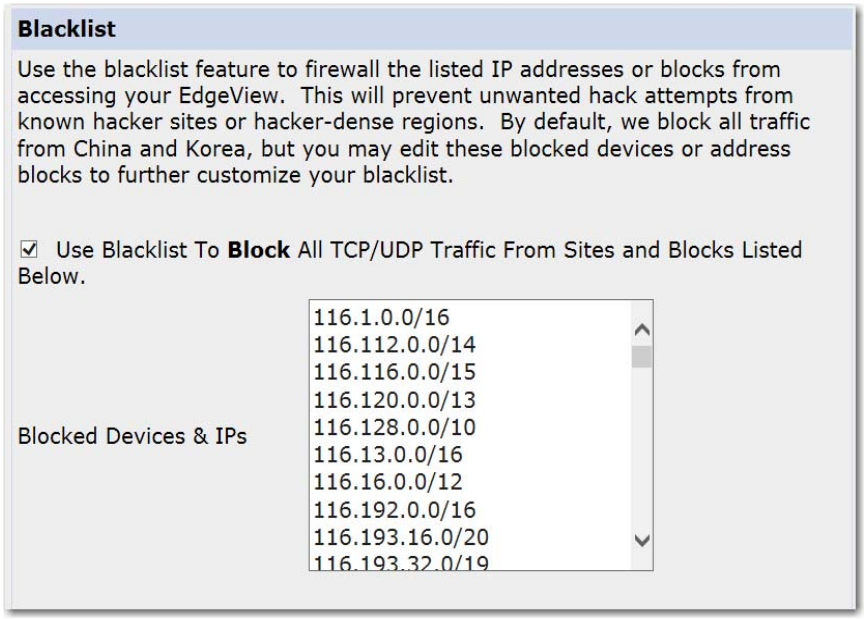
Caution

When configuring a range of IP addresses in your Blacklist, do not specify an IP address range that includes EdgeMarcs.

To configure a Blacklist:

1. Choose **EV System > System Settings**.
2. Select the **System Security** tab. The EdgeView Security Configuration page displays.
3. Scroll to the Blacklist section and select the checkbox for **Use Blacklist to Block All TCP/UDP Traffic From Sites and Blocks Listed Below** (Figure 5-19).
4. Click in the **Blocked Devices & IPs** box and type the IP addresses that you want to include in the Blacklist.
5. Click **Update Preferences**.

Figure 5-19 Configuring a Blacklist



Configuring a Whitelist

For EdgeViews that are not behind a firewall (for example, an EdgeView on the edge of the Internet), the Whitelist feature specifies a list of IP addresses that are allowed to conduct a management session with EdgeView. IP addresses that are not in the Whitelist are blocked from accessing EdgeView. By default, all EdgeMarcs in the device tree are in the Whitelist.

The Whitelist feature is similar in behavior to the “trusted management hosts” feature on the EdgeMarc. EdgeView administrators must use PCs/Workstations with the source IP addresses or networks listed in the Whitelist.

Caution

If you enable the Whitelist feature without including the IP addresses (or networks) of your administrators' PCs/Workstations in the “Trusted Devices and IP” list, you will be locked out of the system! Should this occur, contact Edgewater Networks technical support.

Note

You do not need to include the IP addresses of your EdgeMarc systems in the Whitelist; these addresses will be automatically allowed by EdgeView.

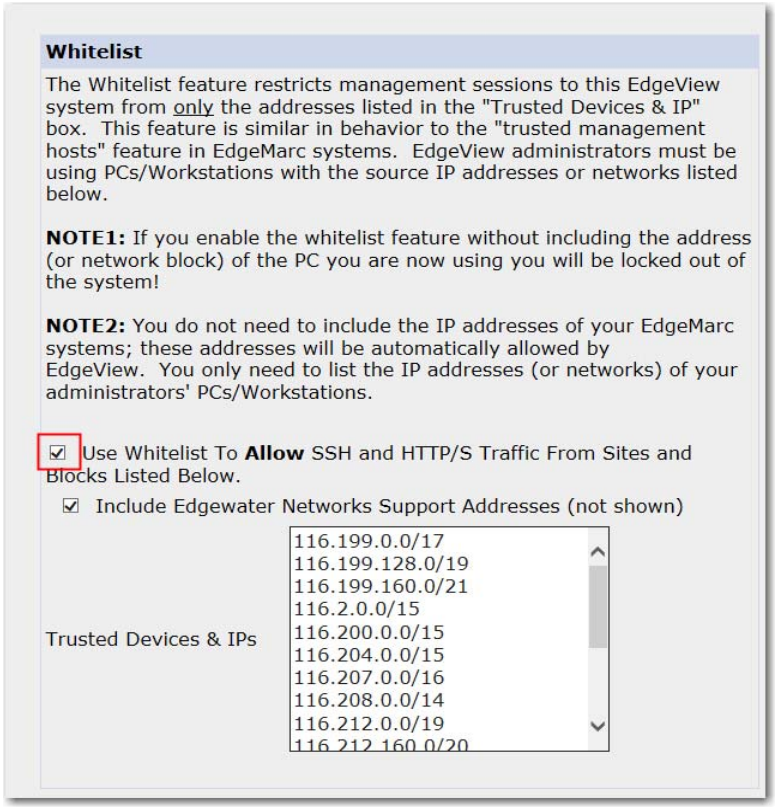
Note

The Whitelist is only for EdgeView management ports (80, 443, and 22 SSH ports).

To configure a Whitelist:

1. Choose **EV System > System Settings.**
2. Select the **System Security** tab. The EdgeView Security Configuration page displays.
3. Scroll to the Whitelist section on the page and select the checkbox for **Use Whitelist to Allow SSH and HTTP/S Traffic From Sites and Blocks Listed Below** (Figure 5-20).
4. Click in the **Trusted Devices & IPs** box and type the IP addresses that you want to include in the Whitelist.
5. Enable the **Include Edgewater Networks Support Addresses (not shown)** checkbox if you want to allow Edgewater Networks technical support to access to your box.
6. Click **Update Preferences**.

Figure 5-20 Configuring a Whitelist



Enabling Anonymous FTP

To configure EdgeView to accept FTP traffic from any node EXCEPT from those IP addresses which are blocked in the Blacklist or IP addresses which are specifically exempted from the firewall:

1. Choose **EV System > System Settings.**
2. Select the **System Security** tab. The EdgeView Security Configuration page displays.
3. Scroll to the Services section on the page (Figure 5-21) and select the checkbox for **Anonymous FTP and open FTP ports for all sites?**
4. Click **Update Preferences**.

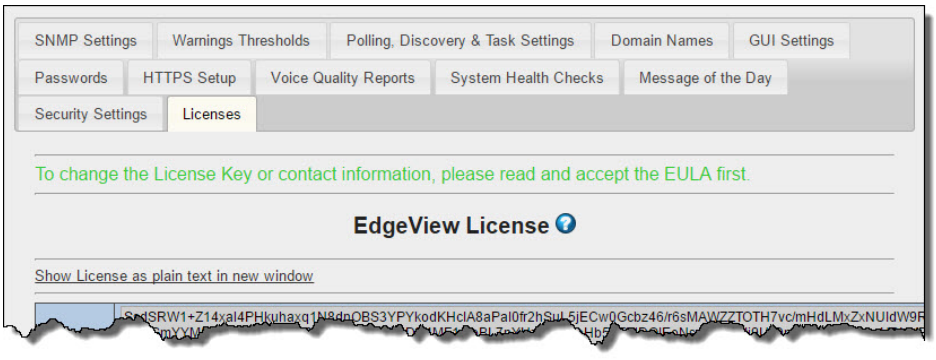
Figure 5-21 Enabling Anonymous FTP



EdgeView Licenses

Choose the **EV System > System Settings > Licenses** tab (Figure 5-22) to install and update your Product and Support license keys. Refer to Chapter 10, *Licensing* for instructions on installing the EdgeView Product and Support License keys for the first time, and how to update your product license key should you need to add nodes to EdgeView. It also includes instructions for activating your support license after renewal.

Figure 5-22 Licenses Tab



EdgeView requires a Product License key to enable features of the product, and a Support License key to allow the product to receive TAC support service. These license keys may also be required to install patches and perform upgrades.

When you purchase an EdgeView and a Support License, Edgewater Networks will email you a Product License key and Support License key. The email will include the MAC address, license key, and URL to the location of the .ova file.

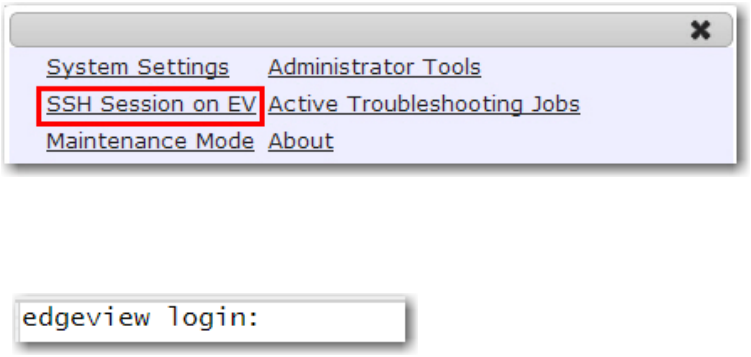
Starting an SSH Session in EdgeView via CLI

Note

This feature is available only to administrators; users are not allowed to access this feature.

Click the **EV System** icon and select **SSH Session on EV** from the EV System menu to start an SSH session (Figure 5-23).

Figure 5-23 EV System Menu > SSH Session on EV



Using Maintenance Mode

When performing system maintenance functions for EdgeView such as a system upgrade, it is recommended that you put EdgeView in "Maintenance Mode" to stop normal operations, such as device polling and collections, and to warn users that EdgeView maintenance is in progress.

Maintenance Mode temporarily disables many of the EdgeView services, such as gathering MOS statistics and polling devices. While in Maintenance

Mode, EdgeView will display a critical alert to all users until Maintenance Mode ends.

Caution

Maintenance Mode should not be used for normal operations. In Maintenance Mode, any scheduled and non-scheduled tasks that are waiting to run will be canceled.

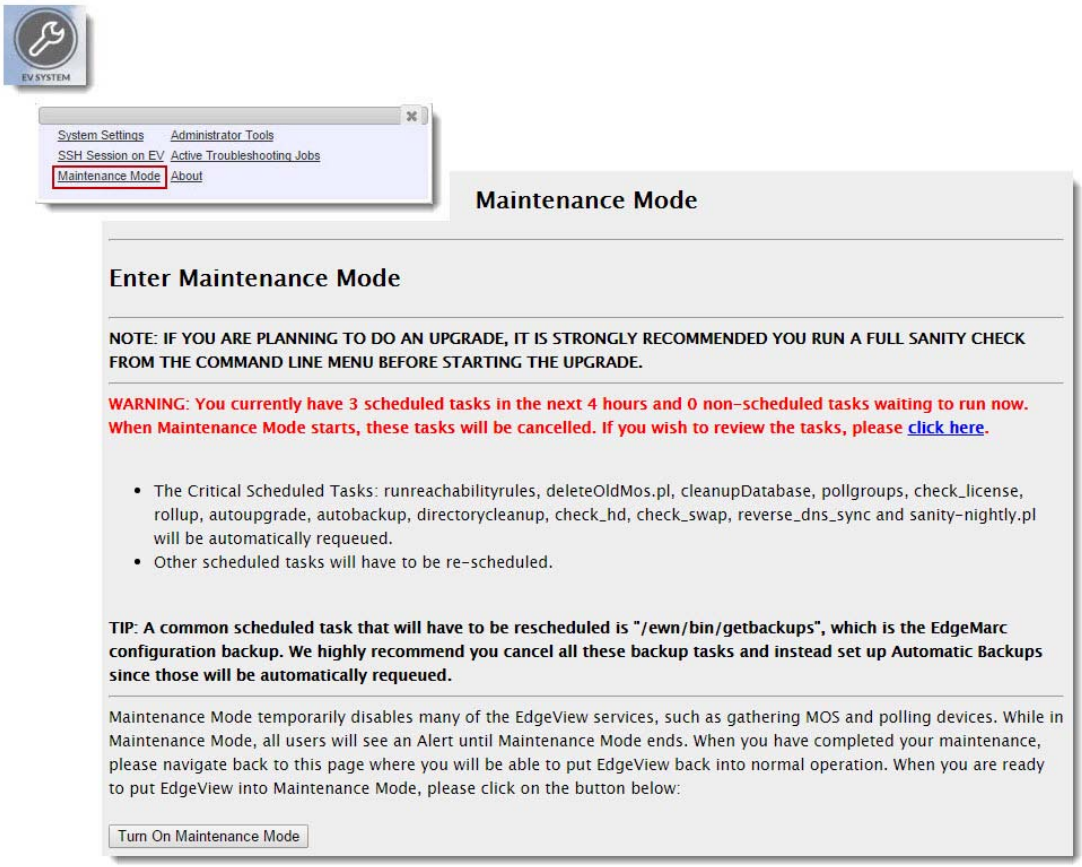
To turn on Maintenance Mode:

1. Choose **EV System > Maintenance Mode** (Figure 5-24).
2. Click **Turn On Maintenance Mode**.

When you have completed your maintenance, navigate back to this page and click **Turn Off Maintenance Mode** to put EdgeView back into normal operation. The poller and collection processes will restart and the critical alert will be cleared.

Refer to the on-screen help on the Maintenance Mode page for more details on using the Maintenance Mode feature.

Figure 5-24 Turning On Maintenance Mode



Using EdgeView Administrator Tools



EdgeView includes system-level tools that help system administrators to:

- Verify the database has or does not have corrupted tables
- Perform backup and restore operations
- Remove old or outdated log files
- View a log file without going into a command prompt
- Check the Operating System version
- Verify all the EdgeView processes are running as expected or restart them if not
- View/cancel scheduled tasks
- Setup signal capture and directory automated cleanup
- Scan the EdgeView database or EdgeMarc nodes for matching passwords and return a report of the results.

To access the Administrator Tools:

1. Click the **EV System** icon and select **Administrator Tools** from the EV System menu. The Administrator Tools menu displays (Figure 5-25).

Figure 5-25 Administrator Tools Menu

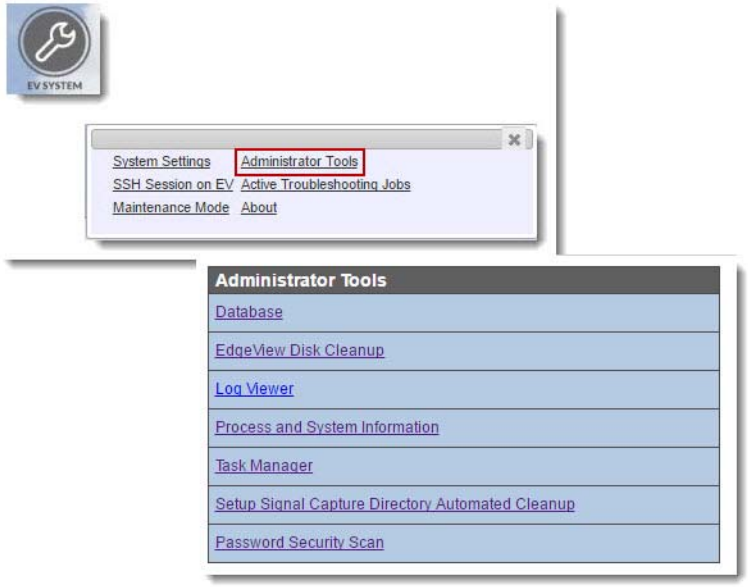


Table 5-5 defines the Administrator Tools that are available:

Table 5-5 Administrator Tools

Tool	Description
Database	Use these tools to check, backup, and restore the EdgeView database.

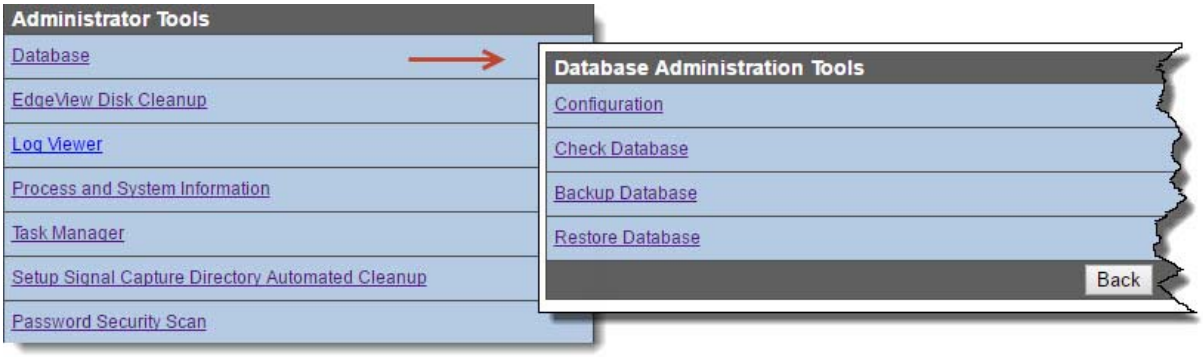
Table 5-5 Administrator Tools (continued)

Tool	Description
EdgeView Disk Cleanup	Use this tool to view and remove unneeded files and directories from the EdgeView database to save disk space.
Log Viewer	Use this tool to view the log files in the EdgeView database that typically need to be reviewed when there is a problem.
Operating System Version	Use this tool to view information about the current operating system on EdgeView.
Process Information	Use this tool to view a list of the critical EdgeView processes and their current state (running/not running). You can restart and start processes from this page. You can also view general information about the EdgeView system such as the Uptime and disk space.
Task Manager	Allows you to view and cancel tasks. In most cases, transitory (non-scheduled) tasks can be safely canceled.
Setup Signal Capture Directory Automated Cleanup	Allows you to setup a signal capture file cleanup rule to automatically clean up files older than a specified number of days and (optionally) send a notification.
Password Security Scan	Scans either the EdgeView database or EdgeMarc notes for matching passwords and then returns a report of the results.
HA Pair Information	Displays the HA pair status, including the Active Node, heartbeat status, and whether there has been a manual failover. This tool is available only if you are using an HA setup. Contact Edgewater support for information about High Availability.

EdgeView Database Administration Tools

Use the Database Administration Tools to test, check and save database configuration settings, perform a database check, perform/schedule a database backup, and restore the database to a selected backup file. To access the Database Administration Tools, open the Administrator Tools menu and select **Database**.

Figure 5-26 EdgeView Database Tools Menu



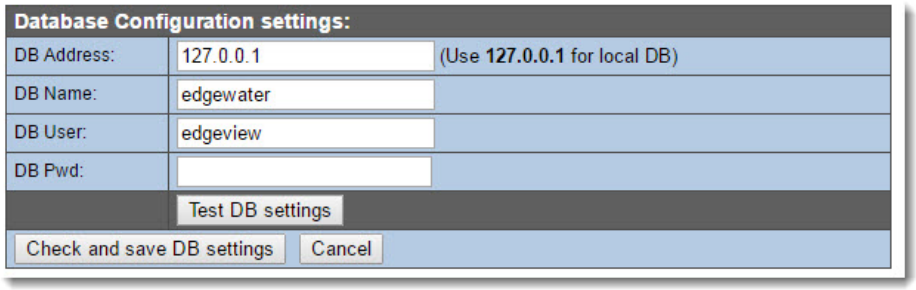
Testing and Saving Database Configuration Settings

Select the **Configuration** option on the Database Administration Tools page to configure, test, and save database settings to a file (Figure 5-27).

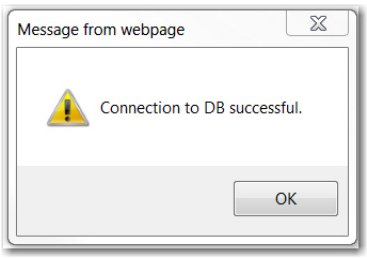
Note

Change the database configuration setting only if you work with an external database that has a changed IP address. There is no need to use this option when working with a local database (default) or a newly setup external database as all settings will be done automatically with the external database setup scripts.

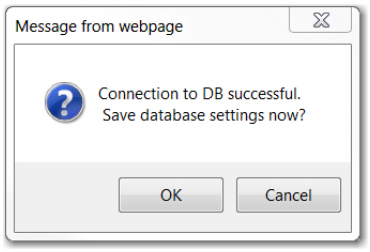
Figure 5-27 Database Configuration Settings



Click **Test DB settings** to verify there is connectivity to the EdgeView database. The following pop-up will display to confirm the connection:



Click **Check and Save DB settings** to verify there is connectivity to the EdgeView database and save the current settings. The following pop-up displays:



Checking the Status of EdgeView Database Tables

System Administrators should periodically check the EdgeView database to verify that all the tables are working properly. This is particularly important if the system seems to be having problems or if there was a hard reboot or unexpected shutdown.

To check the database, open the Administrator Tools menu and select **Check Database** (Figure 5-28). A list of the MySQL tables in the EdgeView database displays, along with their status. The Status column displays a status of **OK** or **Needs Repair** for each table in the EdgeView database.

Note

Allow additional processing time to receive status for tables that contain more data.

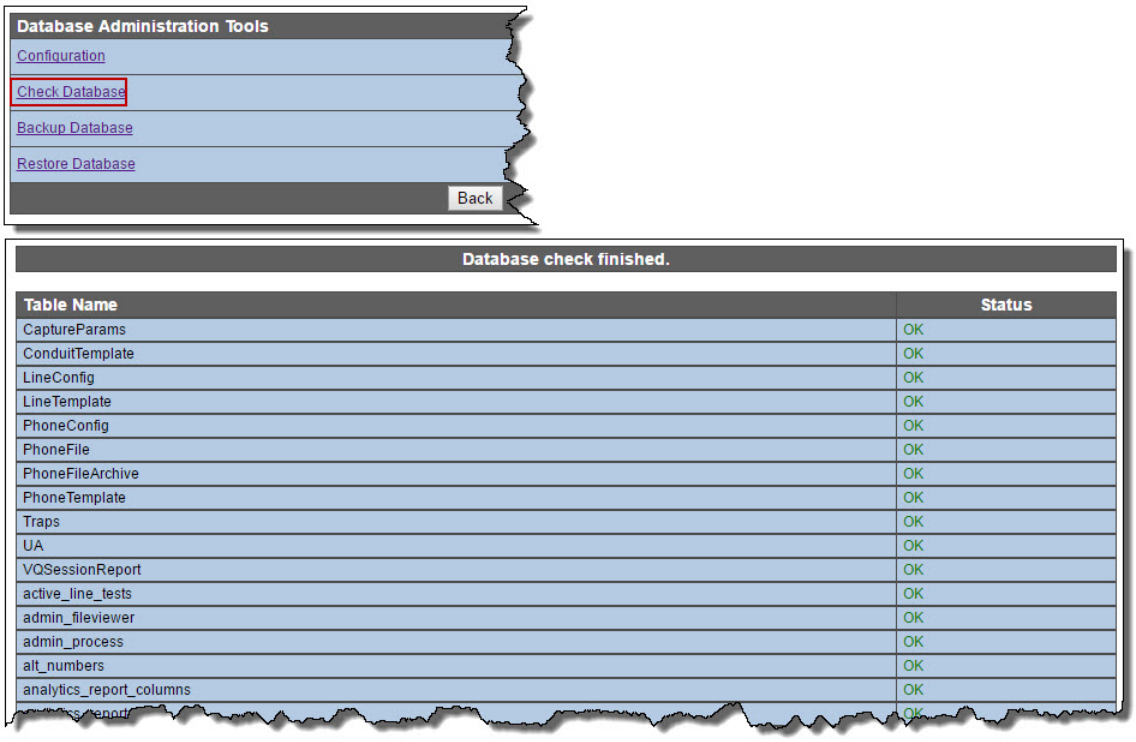
Managing EdgeView Historical Data with mysql Partitioning

Database Administration Tools in that allows admins to schedule Partitioning. The page informs the admin if partitioning has already been done, and will allow the admin to delete a scheduled partitioning if they need to change the schedule. Choose **EV System** > **Administrative Tools** > **Database** to access the new page.

By dynamically creating partitions for large data tables, data can be managed more efficiently by dropping the partitioned data as needed

rather than deleting record ranges. Additionally, replication for the partition drop commands can be turned off allowing the system to keep more historical data on the Report Server.

Figure 5-28 Checking the Database



Backing Up the EdgeView Database

EdgeView should be backed up locally or to an external FTP server on a regular basis, especially before an upgrade. You can backup EdgeView on-demand or according to a schedule.

When you do a backup, the entire EdgeView database will be copied to the local drive or external FTP server. This may use a lot of disk space. EdgeView will check to see if there is enough disk space on the destination before it begins copying files. If there is not enough disk space to do the backup, EdgeView will not attempt to copy the database. This applies to both scheduled and non-scheduled backups.

When needed, you can use the **Restore Database** link on the Administrator Tools menu to select the backup file and restore the EdgeView database.

Note

It is recommended that you perform a database check before you backup the database.

Note

The Database Backup feature is not available if the database is external.

To backup the EdgeView database:

1. Choose **EV System** > **Administrator Tools** > **Database**.
2. Select **Backup Database** and configure settings in the Database Backup screen (Figure 5-29).

Figure 5-29 Database Backup Screen

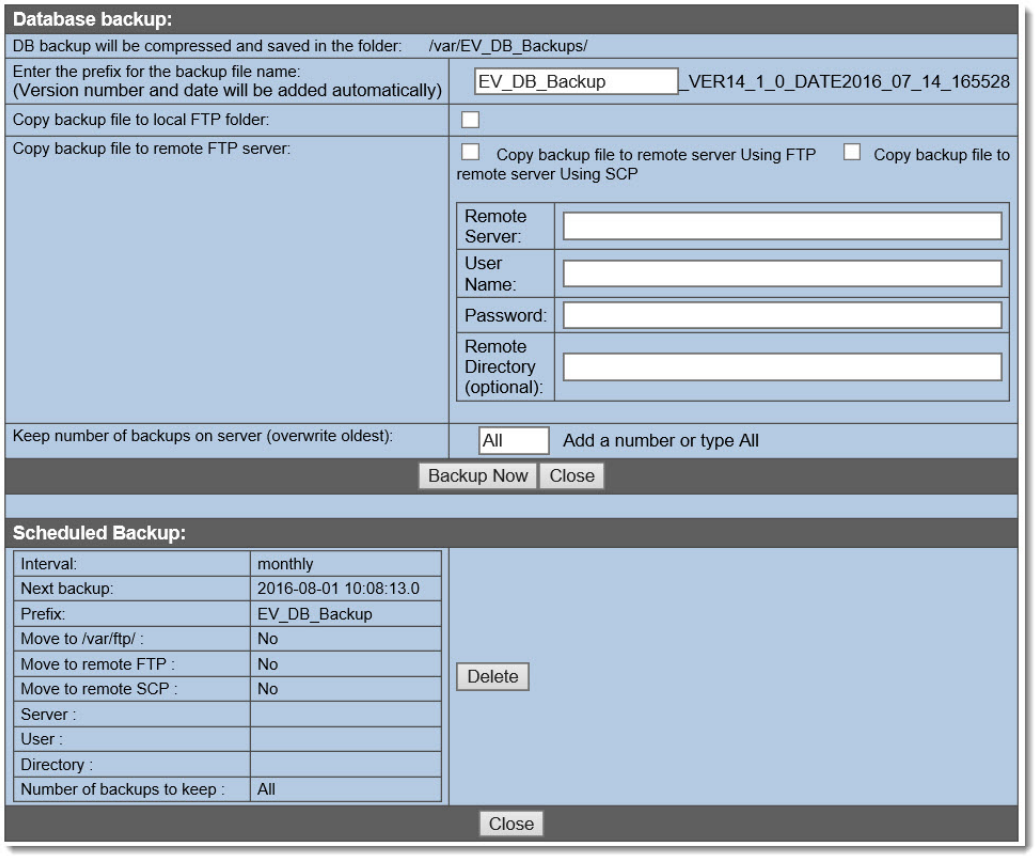
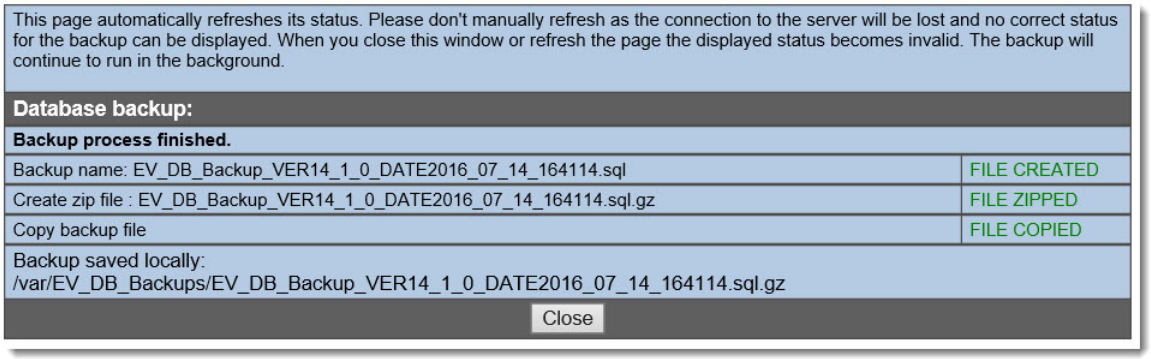


Table 5-6 Configuring Database Backup Settings

Setting	Description
DB backup will be compressed and saved in the folder	Lists the location of where the backup file will be saved in the EdgeView database.
Enter the prefix for the backup file name	Enter a prefix which will precede the backup file name. The version number and date will already be displayed and appended to the prefix.
Copy backup file to local FTP folder	Select the checkbox if you want EdgeView to copy the backup file to a folder on the local FTP server.
Copy backup file to remote FTP server	Select the checkbox if you want to copy the backup file to a remote FTP server. Enter values for the FTP Server name, user, password, and FTP remote directory (optional).
Keep number of backups on server (overwrite oldest)	Set the maximum number of database backups to be saved on the server. When this limit is reached, the next backup process will automatically delete the oldest backup.
Backup Now	Click this button to do an immediate backup using the current settings.
Close	Click this button to close the window without doing a backup.
Schedule the database backup with the above settings	To schedule a backup, select a frequency (daily, weekly, monthly), start date, and time, and click **Schedule**.
Schedule	Click this button to schedule a backup using the current settings on the page.

Once the backup is successful, a Backup Process Finished notice is displayed (Figure 5-30).

Figure 5-30 Backup Complete Screen



Caution

DO NOT RENAME THE DATABASE BACKUP FILE.

Note

Important! Copy this backup file to a temporary server. The backup file is located on the EdgeView in the folder /var/EV_DB_Backups/

Note

Important Note for HA Systems: You only need a database backup of the currently active EdgeView.

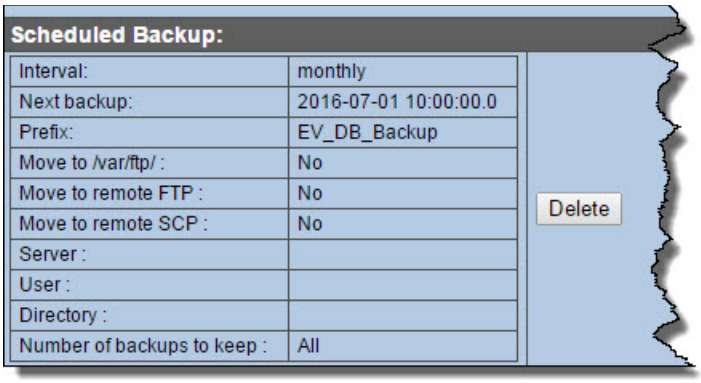
Deleting a Scheduled Backup

Deleting a scheduled backup will delete all recurring backups in the future. You must first delete the currently scheduled backup settings.

To delete scheduled backups:

1. On the Database Backup Screen, click **Schedule** (Figure 5-31).
2. Click **Delete** next to the scheduled backup.

Figure 5-31 Deleting a Scheduled Backup



Restoring the Database

To restore the EdgeView database to a previous state, complete the following steps.

Caution

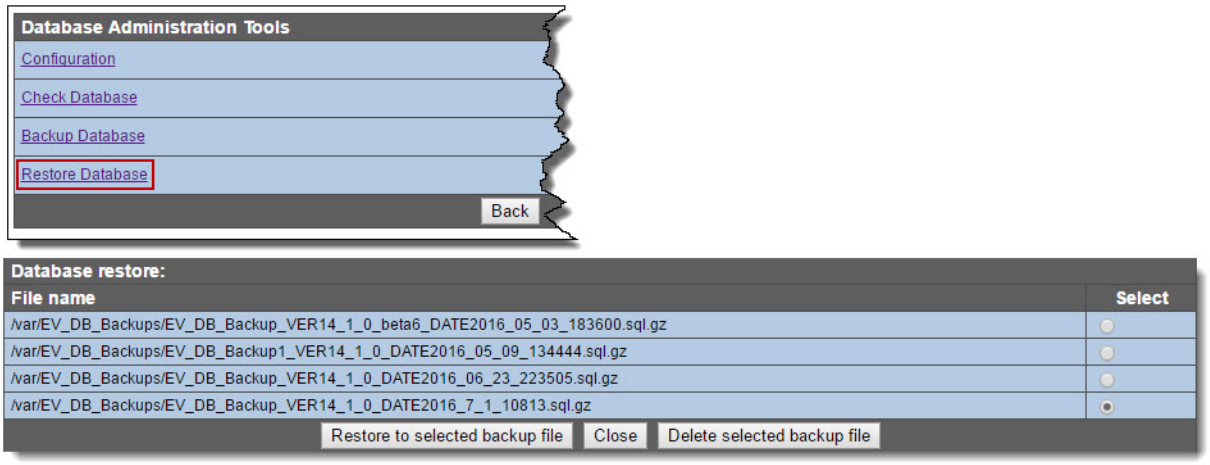
Edgewater Networks recommends that you make a backup of the current database before overwriting it.

Note

You can only restore an EdgeView database of the same EdgeView software version. When you restore the database, all data collected from the time the backup starts to the moment you start the restoration is lost.

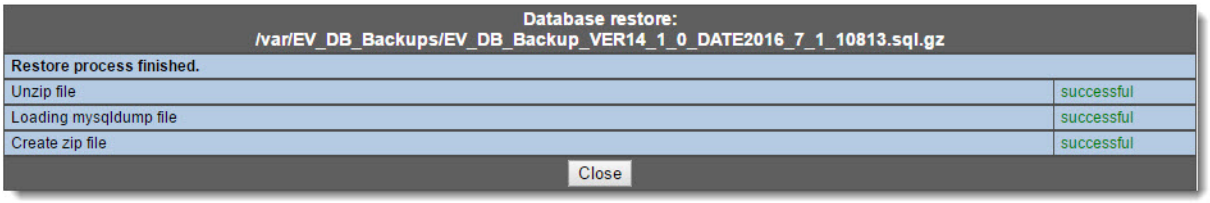
1. Select **Restore Database** from the Database Administration Tools (Figure 5-32). A list of the database backup files stored on the FTP server displays.
2. From the Database Restore page, choose the database backup file you want to restore.
3. Click **Restore to selected backup file**.

Figure 5-32 Database Restore Screen



When the restore process in finished, a database restore notification displays (Figure 5-33.)

Figure 5-33 Database Restore Notification



4. Restart EdgeView. The current EdgeView database will be overwritten with the selected backup file.

Deleting a Database Backup File from the EdgeView Database

To remove a Database backup file from the EdgeView database:

1. Select **Restore Database** from the Database Administration page. A list of the database backup files in the EdgeView database displays.
2. Select the backup file that you want to remove and click **Delete selected backup file**.
3. Confirm you selection in the confirmation dialog box.

The selected backup file will be removed from the EdgeView database.

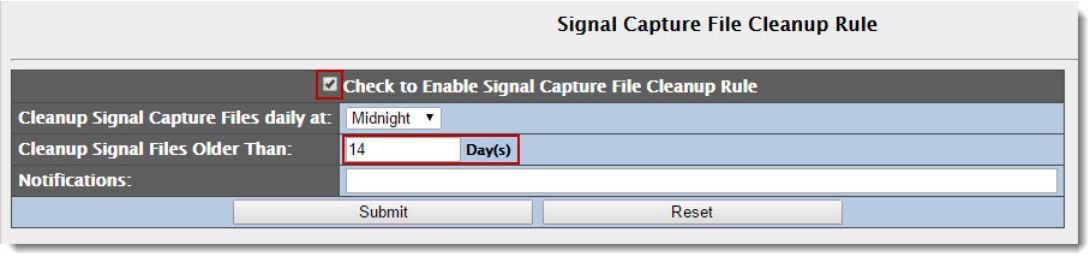
EdgeView Signal Capture File Cleanup Configurable Storage

EdgeView signal file captures can now be kept on the system for a configurable number of days. The **Cleanup Signal Files Older Than**

drop-down menu with limited options is replaced by a configurable field that allows you to enter any value, “14” for instance (Figure 5-34).

1. Choose **EV System** > **Administrator Tools**.
2. Click **Setup Signal Capture Directory Automated Cleanup**.
3. Select the **Check to Enable Signal Capture File Cleanup Rule** checkbox. Configuration fields become active.
4. Enter a value in the C**leanup Signal Files Older Than** field.

Figure 5-34 Signal Capture File Cleanup Rules

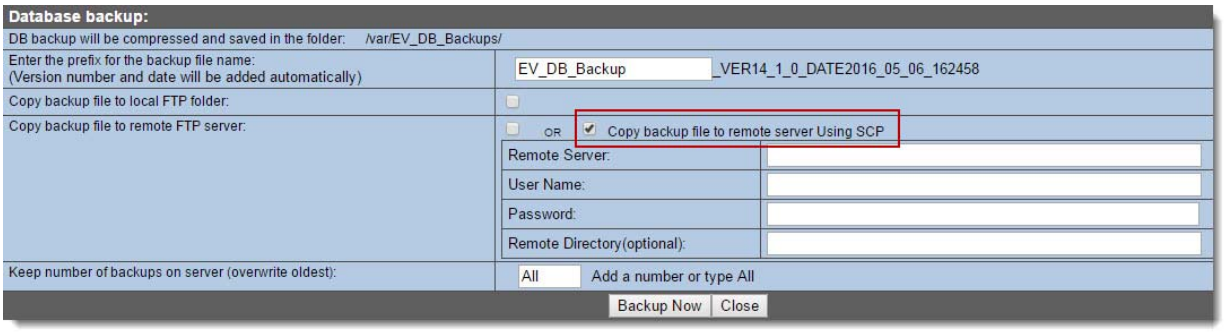


SCP Support for EdgeView Database Backup and Restore

SCP is added as an option for secure automatic system backup. The GUI now has an SCP checkbox in addition to FTP. You can enable either FTP or SCP. To enable backup using SCP:

1. Choose **EV System** > **Administrator Tools**.
2. Click **Database** in the Administrator Tools window.
3. Click **Backup Database** in the Database Administration Tools window.
4. Select the **Copy backup file to remote server using SCP** checkbox (Figure 5-35).
5. Enter SCP information in the fields provided.

Figure 5-35 SCP Database Backup

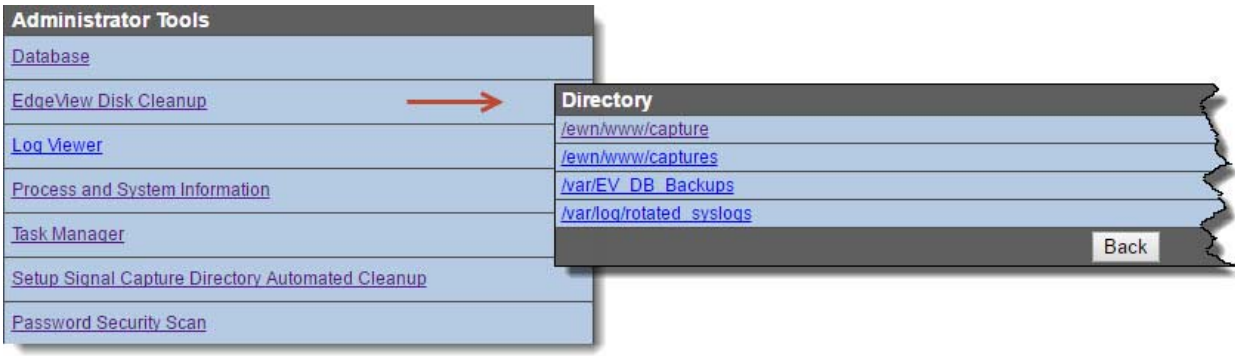


EdgeView Disk Cleanup Tool

Certain files can be safely removed from the EdgeView database to save disk space. For example, you can periodically remove the /var/log files and /var/tmp files.

1. Select **EdgeView Disk Cleanup** from the Administrator Tools menu. A list of the EdgeView /log, /tmp, /capture, and /captures directories displays (Figure 5-36).
2. Select the file you want to remove or the directory that contains the files you want to remove. A list of the files in the selected directory displays.

Figure 5-36 EdgeView Database Directory Files



3. Click the **Select** checkbox for each file you want to delete.
4. Click **Deleted Selected files in Directory** to remove the selected files from the EdgeView database.
5. Click **Back to Directory List** to return to the list of directories.

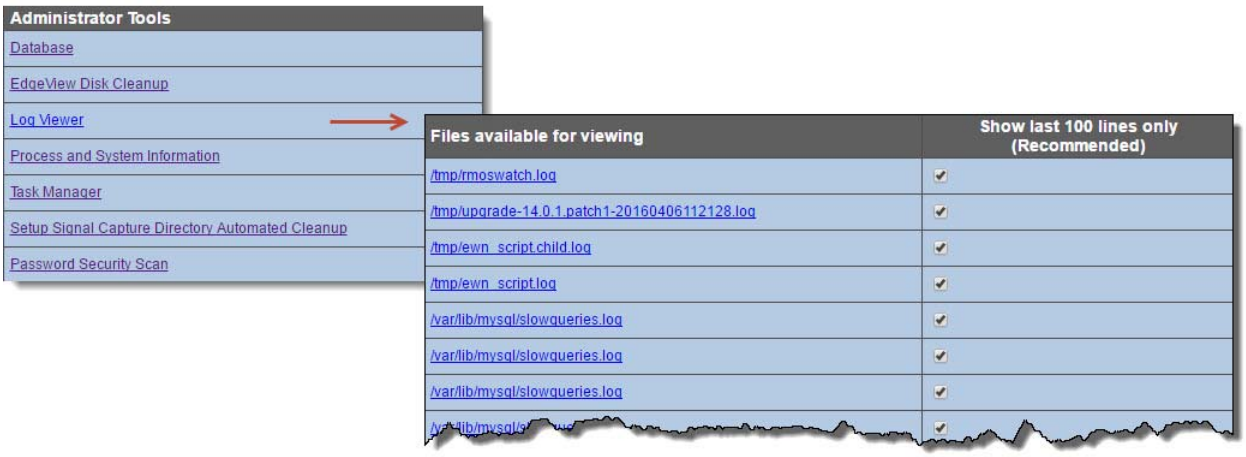
Caution

DO NOT DELETE THE DIRECTORIES! Only delete the files within the directories.

Viewing EdgeView Log Files

1. Select **Log Viewer** from the Database Administration Tools menu to view a list of the log files generated in EdgeView. The Log Viewer screen displays (Figure 5-37).

Figure 5-37 Viewing Log Files



2. Click on a log file in the list to view its contents. Because log files can be quite large, it is recommended that you show only the last 100 lines in the log file. If you want to show more lines, disable the **Show last 100 lines only** checkbox for the file.

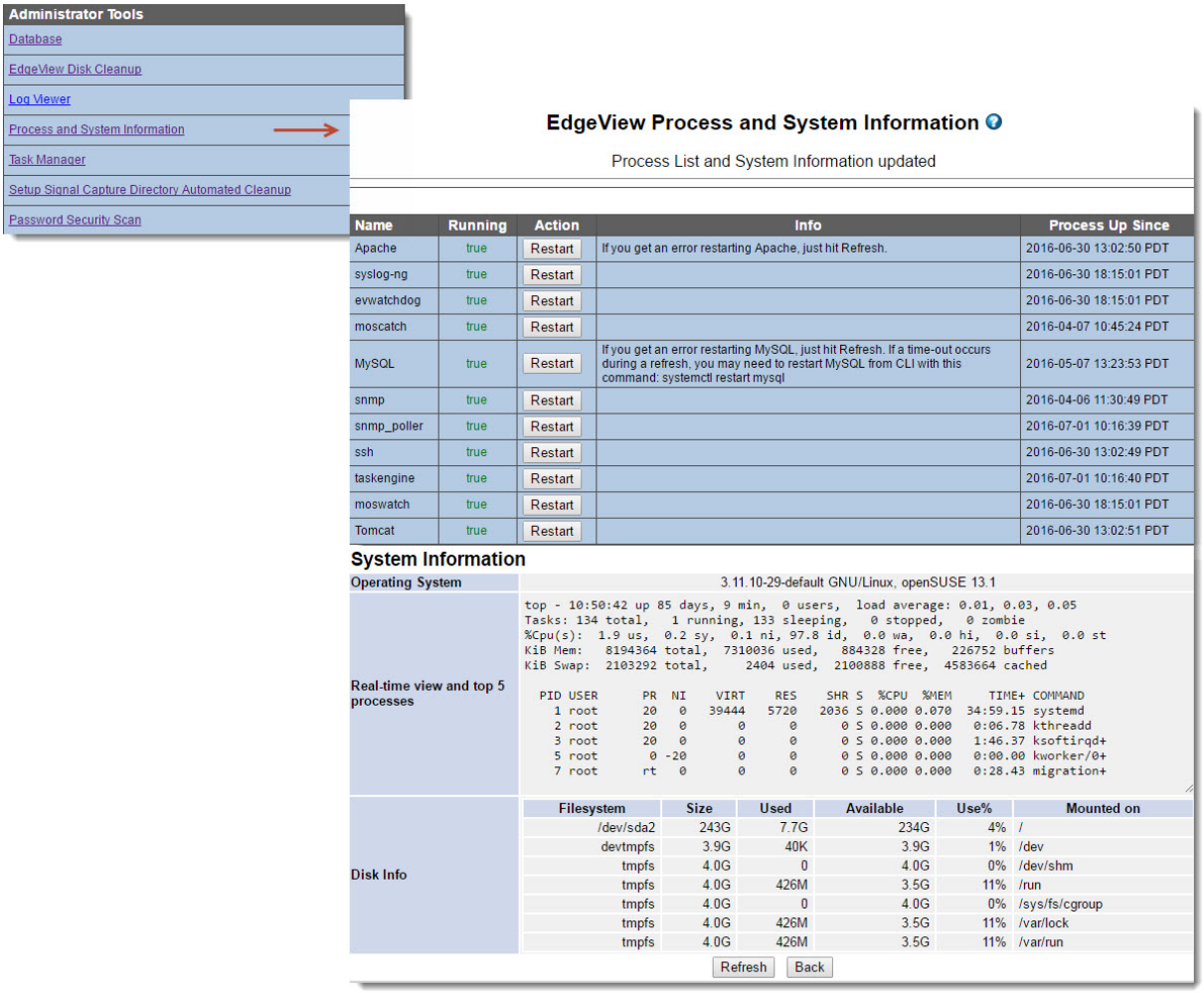
Viewing EdgeView Process and System Information

When troubleshooting issues for EdgeView managed nodes, one of the first things to check is the process list to see which processes are currently running on EdgeView. To access the process list, select **Process Information** on the Administrator Tools menu (Figure 5-38).

Some processes shown in the process list screen may not be applicable if you are not using certain EdgeView features such as Plug & Dial. Key processes to look for are Apache and MySQL. If these processes are not running, EdgeView will not run properly. Should this occur, click **Restart** in the Action column to restart these processes. The Disk Info section at the bottom of the process list shows general information about the EdgeView system such as the uptime and disk space.

If EdgeView is part of a HA Pair, the process list will include high availability status information for both EdgeViews in the pair.

Figure 5-38 Viewing the Process List

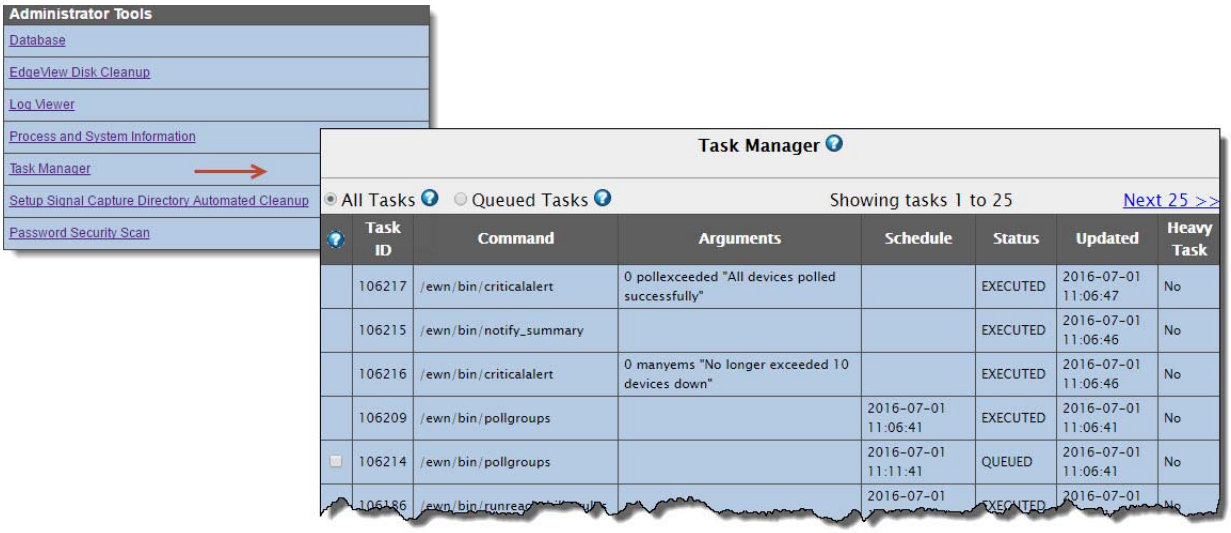


Viewing EdgeView Tasks

Select **Task Manager** from the Administrator Tools menu to display a list of the tasks which have been executed on EdgeView or are in the Queue and waiting to be executed (Figure 5-39). Tasks are listed in the order of when the task status was last updated; the latest update is shown first. Mouse over the question mark icons to view more details about how to use the Task Manager.

To list only the Queued tasks, enable by the **Queued Tasks** option. If there are many Queued tasks waiting, click **Cancel All Queued But Non-scheduled Tasks** to allow the task engine to catch up.

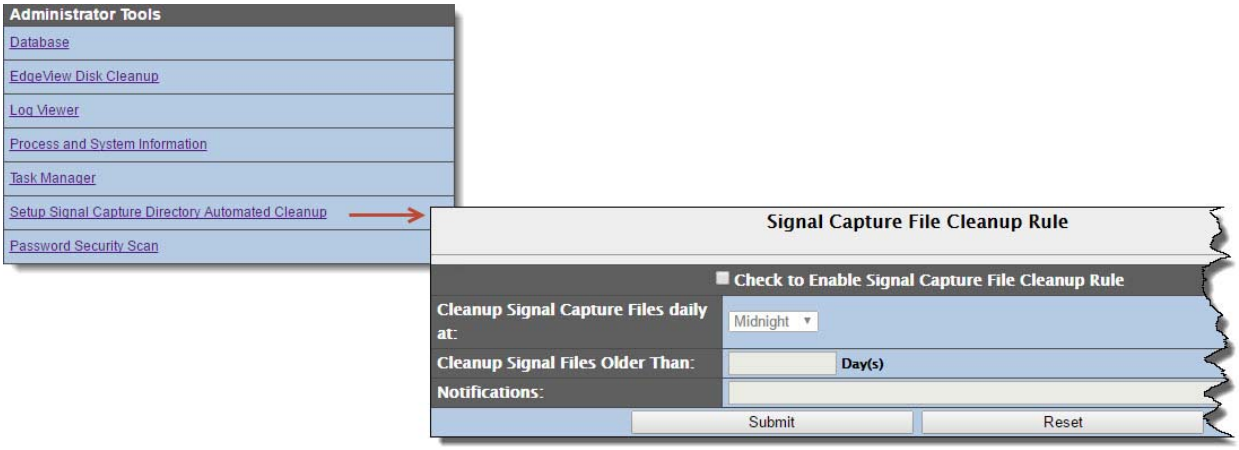
Figure 5-39 Task Manager



Setting Up EdgeView Hard Disk Automated Cleanup

Select **Setup Signal Capture Directory Automated Cleanup** from the Administrator Tools menu to configure a rule that tells EdgeView to automatically clean up signal capture files older than a specified number of days and (optionally) send email notifications.

Figure 5-40 Automated Cleanup of Signal Capture Files



To configure a signal capture file cleanup rule:

1. Select the checkbox next to Check to Enable Signal Capture File Cleanup Rule.
2. From the **Cleanup Signal Capture Files daily at** drop-down box, select the time that you want to do the file cleanup.

3. From the **Cleanup Signal Files Older than** drop down menu, select the number of days of files that you want to remove.
4. In the **Notifications** field, enter comma-separated email addresses of the recipients you want to send notifications to when the file cleanup completes.
5. Click **Submit**.

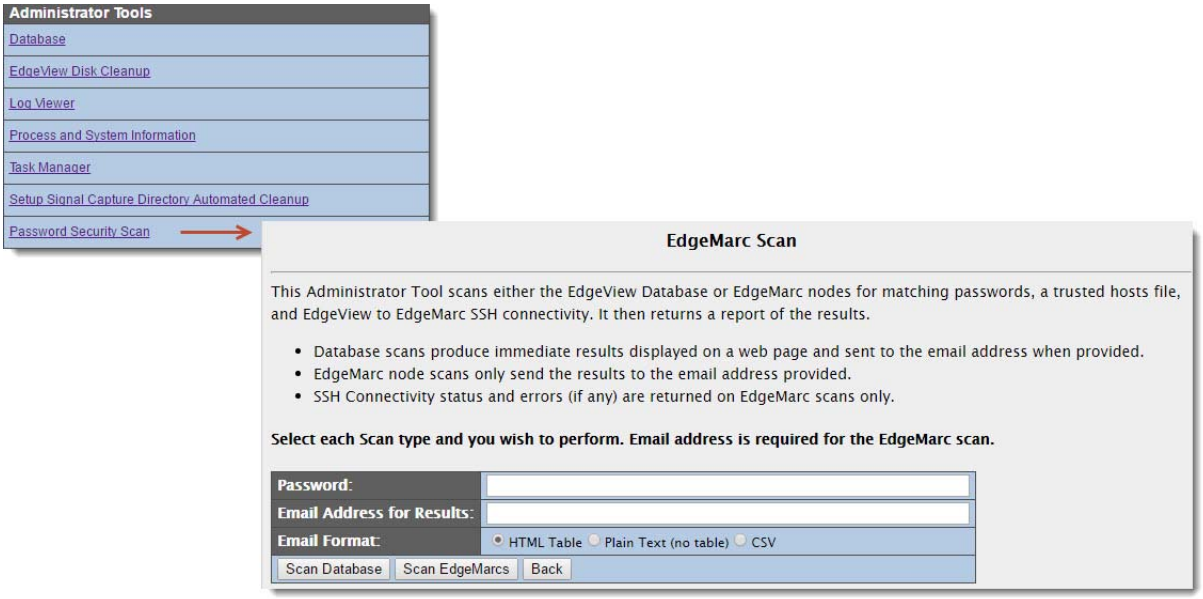
Performing a Password Security Scan

EdgeView features a Password Security Scan Administrator Tool to scan for matching passwords in either the EdgeView database or the EdgeMarc itself. This is generally used to find EdgeMarcs that still have their factory settings or for EdgeMarcs that may have old passwords set. There may be other uses as well.

To use the tool:

1. Choose **EV System** > **Administrator Tools >Password Security Scan**. The Password Security Scan page displays (Figure 5-41).

Figure 5-41 Password Security Scan



2. Enter a password to search for.
3. If you would like to receive a report of the results, enter an email address. Note that this is the ONLY way to see the results when the EdgeMarc itself is checked (as opposed to using the value in the EdgeView database).
4. Select the format of the email report if used. Generally HTML provides the more readable report. Select CSV if you plan to put the data into a spreadsheet.

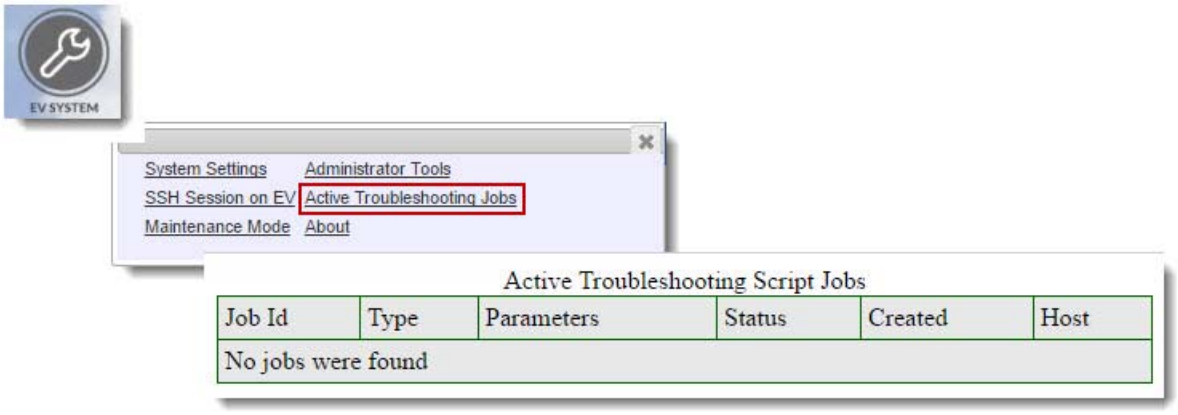
5. Click **Scan Database** (for local EV database) or **Scan EdgeMarcs** (to look on each EdgeMarc itself).
6. Confirm the operation, if necessary.
7. View the results. If an email is specified, you should receive an email report once the scan completes.

The report shows the matching EdgeMarcs, the un-matching EdgeMarcs and if the EdgeMarc scan option was chosen, any reason why the EdgeMarc could not be scanned. For example, if the EdgeMarc has been down for over 30 minutes, then no scan attempt was made.

Viewing Active Troubleshooting Jobs

Select **Active Troubleshooting Jobs** from the EV System menu to display a list of the debug scripts that are currently running for all nodes (Figure 5-42). For details on the available debug scripts, see the EdgeView Troubleshooting Tools section in Chapter 8, *MOS Analysis and Troubleshooting*.

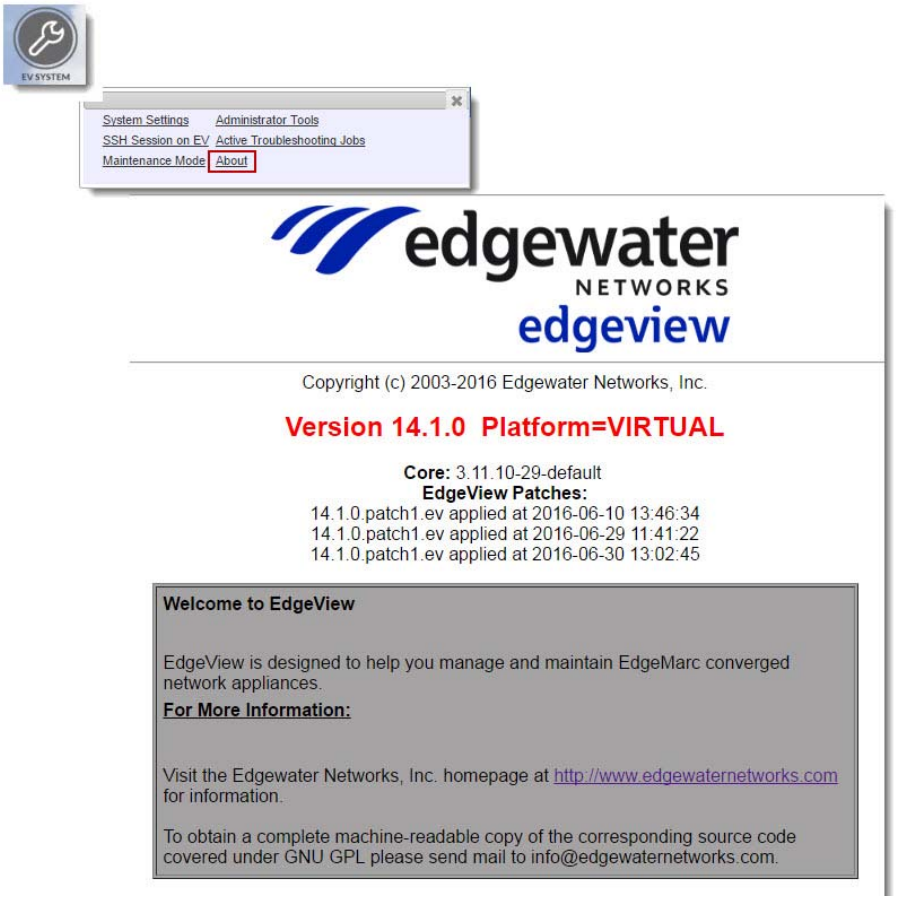
Figure 5-42 Accessing the Active Troubleshooting Jobs Screen



Viewing the Current Software Version and Patches Installed on EdgeView

Select **About** from the EV System menu to view information about the software version and patches installed on EdgeView (Figure 5-43).

Figure 5-43 Viewing System Information for EdgeView



6

Status and Notifications

To help you monitor the devices on your network, EdgeView offers many options for viewing status, managing alerts and MOS notifications, and sending email notifications for the status of managed nodes and devices. This section provides guidelines for viewing node and group status and configuring email notification settings in EdgeView.

Viewing Status in EdgeView

EdgeView can show you at-a-glance a detailed status of the managed EdgeMarcs, phones, third-party devices, and SNMP-based devices on your network. Table 6-1 describes the types of status that can be displayed.

Table 6-1 EdgeView Status Definitions

Status	Description
General EdgeMarc Status	Shows an at-a-glance view of the EdgeMarc status, SIP server status, and data gathered by EdgeView during the most recent polling cycle. See Viewing General EdgeMarc Status.
Global EdgeMarc Status	Displays color-coded status of all the EdgeMarcs that EdgeView is managing as well as the group to which each EdgeMarc belongs. See Viewing Global EdgeMarc Status.
Group Status	Shows group level status for each group managed by EdgeView. See Viewing Group Status.
Other Nodes	Shows the status for third-party nodes and SNMP-based nodes that are being managed by EdgeView. See Viewing the Status of Other Nodes.
IP Phone Status	Shows the status for the IP phones that are being managed by EdgeView. See Viewing IP Phone Status.
EdgeConnect Status	Shows the status for the EdgeConnects that are being managed by EdgeView. See Viewing EdgeConnect Status.

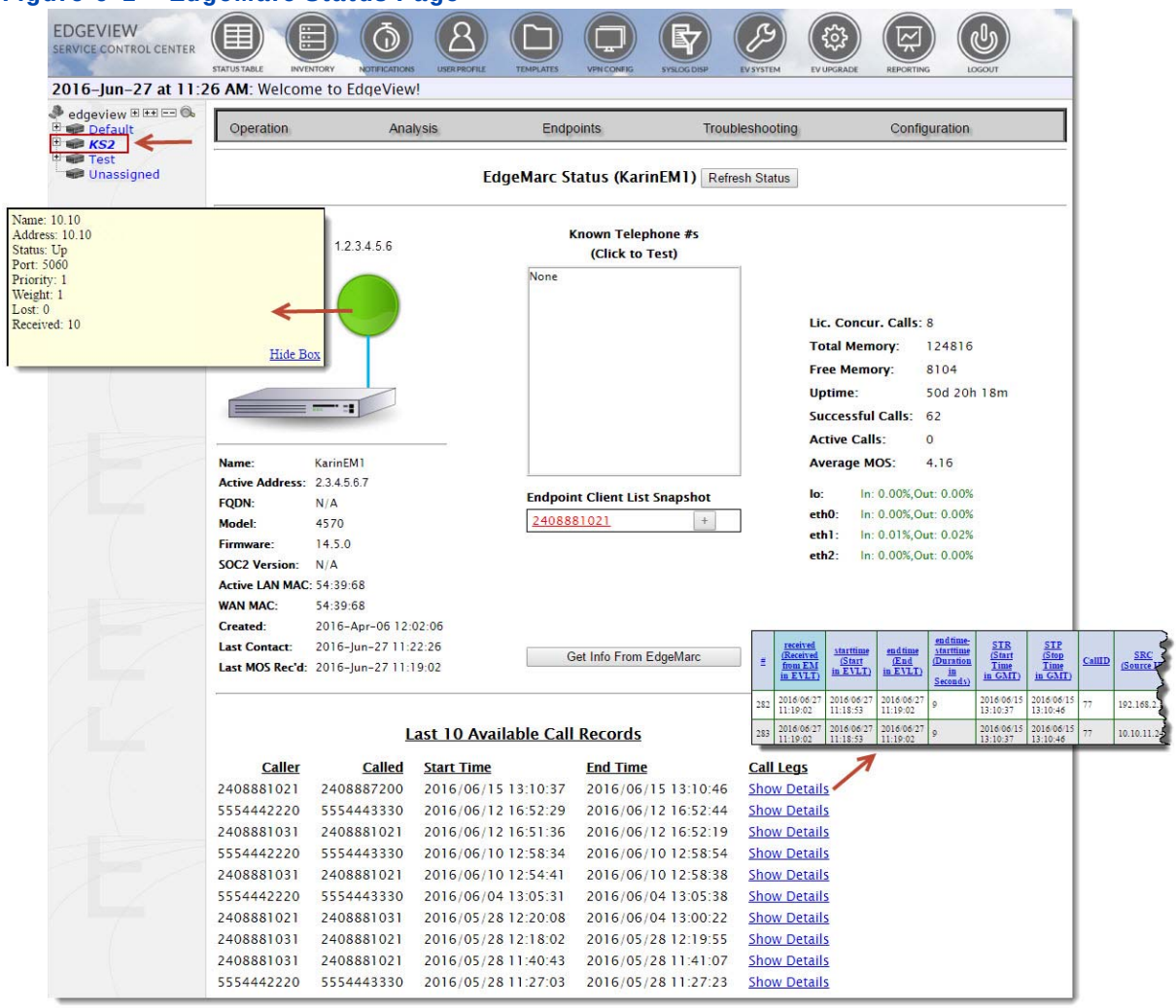
Viewing General EdgeMarc Status

The EdgeMarc Status page shows an at-a-glance view of the EdgeMarc status, SIP server status, and data gathered by EdgeView during the most recent polling cycle. The information displayed in the EdgeMarc Status page includes the EdgeMarc network configuration, a list of the phones connected to the EdgeMarc, and calling statistics.

To view EdgeMarc status:

1. Click on an EdgeMarc in the device tree (Figure 6-1).

Figure 6-1 EdgeMarc Status Page



EdgeView SSHs into each EdgeMarc on a (default) 5-minute interval and gather information such as the EdgeMarc model number, the VOS (firmware) version, RAM statistics, call statistics, and average MOS. If there is a problem with SSH polling, a warning will be shown for the Last SSH Poll.

2. Click on the balloon for more information about the SIP server. The color of the balloon in the middle of the page indicates the general status of the SIP servers connected to the EdgeMarc:

   Green = Up

   Red = Down

   Yellow = Idle

   If there is more than one SIP server, there will be two balloons, one green for the active SIP server and one yellow/amber for the SIP server that is not active. If there are more than two SIP servers, the status will show in tabular format below the EdgeMarc device graphic on the page.

3. At the bottom of the EdgeMarc Status page, click **Show Details** to display call statistics information for the last 10 available call records.

Other features such as monitoring, analysis, Plug & Dial, troubleshooting and configuration are launched from the menu bar at the top of the EdgeMarc Status page.

Storing and Graphing Memory Usage on the EdgeMarc

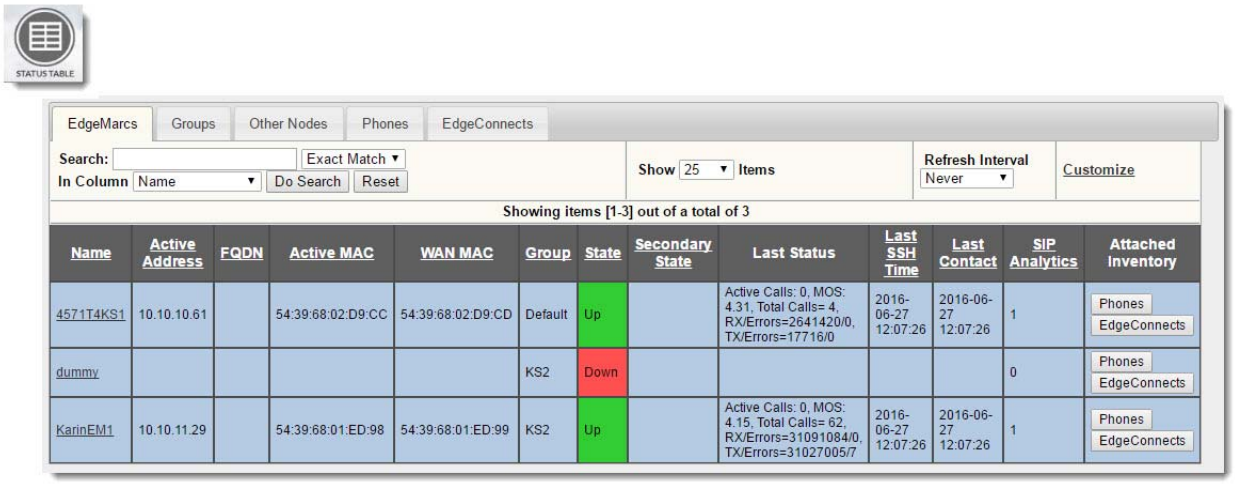
EdgeView currently reports memory statistics on every polling cycle. However, this data is only shown on the EdgeMarc Status page and in the rollover on the Device Tree, and no statistics history is kept on the system.

In release 14.0.1, the EdgeView poller now collects and stores statistics history and displays the data in graphs on the Memory Use Statistics page to better pinpoint memory usage, spikes, and leaks. The automatic rollup routine (/ewn/bin/rollup) processes the information and captures the values similarly to the way interface and MOS data is collected in the MOS Traffic Graphs on the EM Status page/Operation menu.

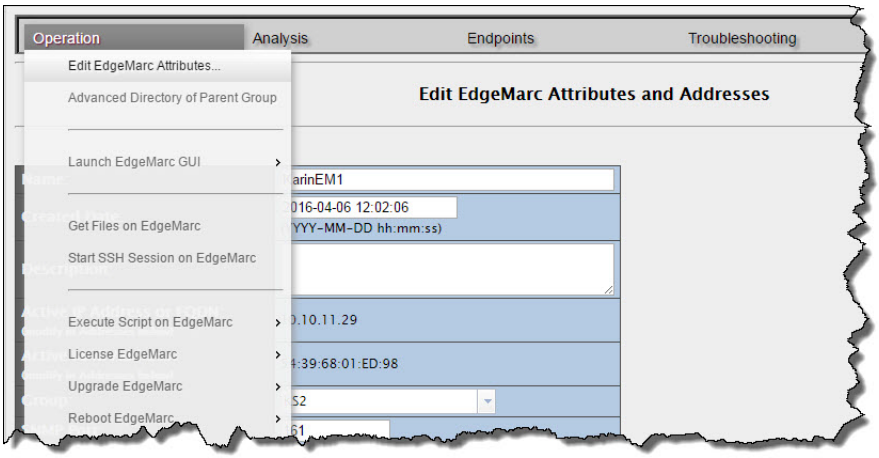
To access the Memory Use Statistics page:

1. Click **Status Table**.

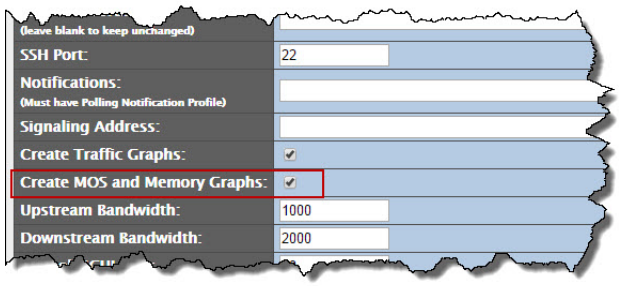
Figure 6-2 Status Table Page



2. Select an EdgeMarc from the **Name** column.
3. Click **Operation** and select **Edit EdgeMarc Attributes** from the drop-down menu.



4. Select the **Create MOS and Memory Graphs** checkbox.



5. Click **Operation** and select **Memory Usage Graph**. The Memory Usage Statistics page displays (Figure 6-3 and Figure 6-4).

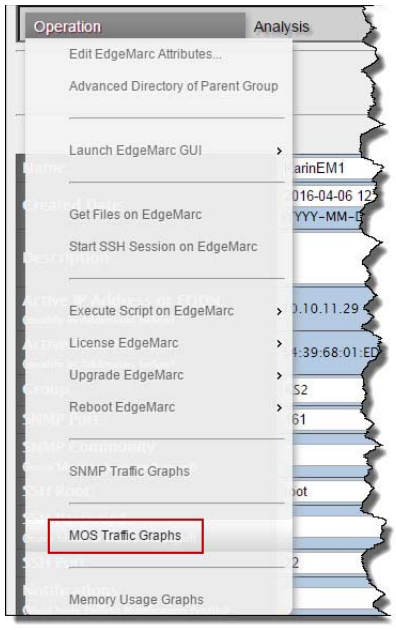
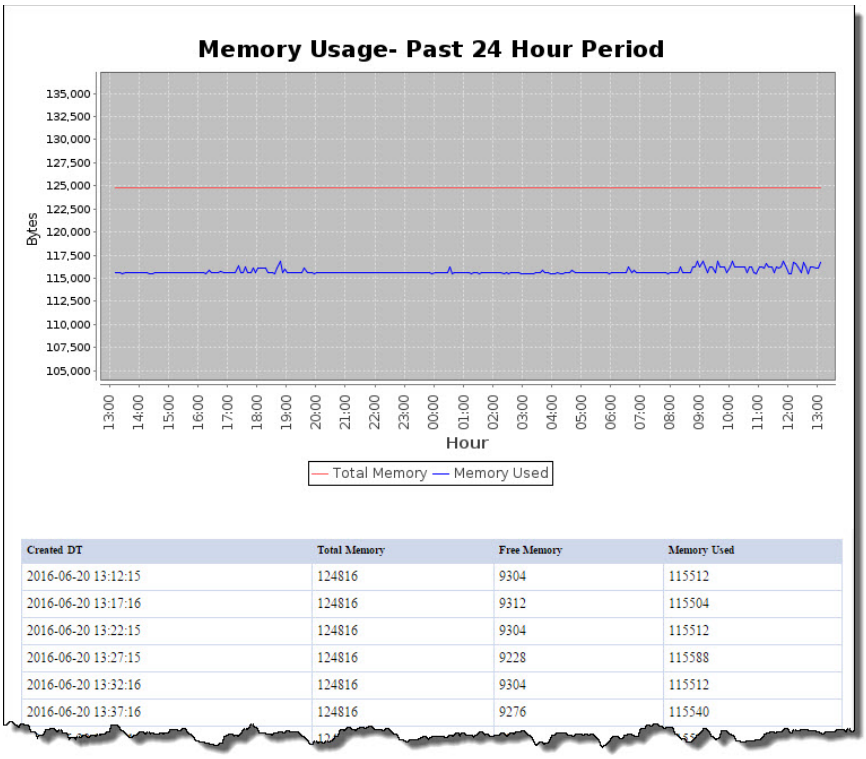
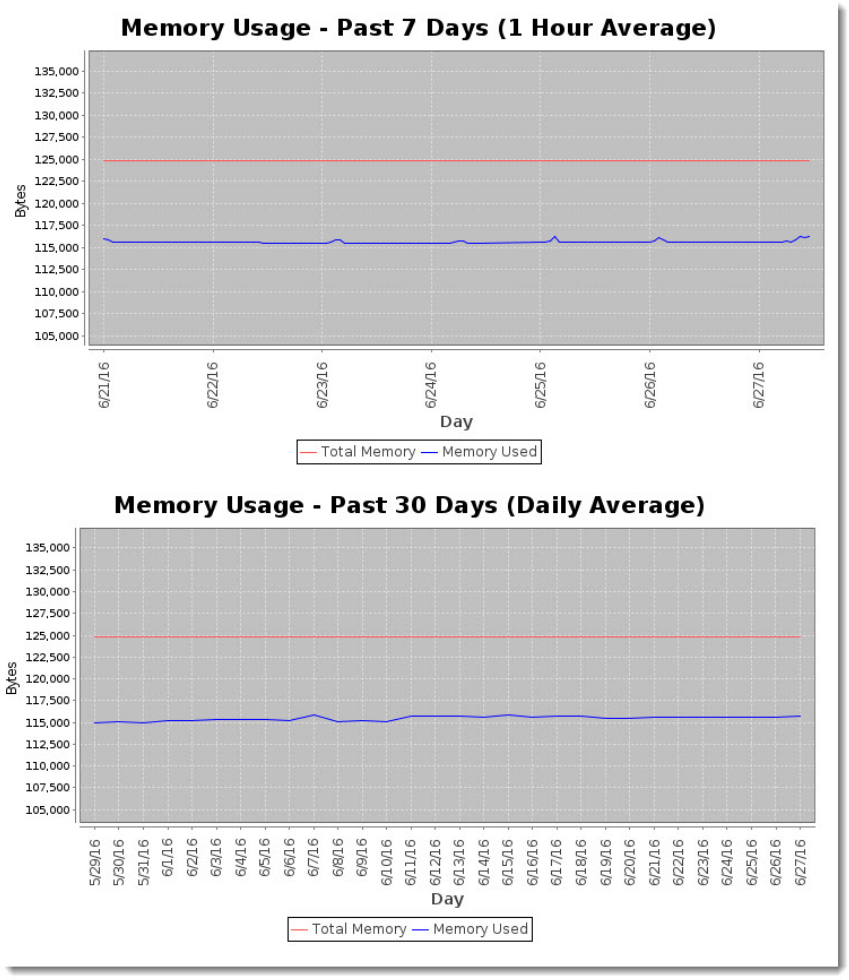


Figure 6-3 Memory Usage Statistics



Created DT	Total Memory	Free Memory	Memory Used
2016-06-20 13:12:15	124816	9304	115512
2016-06-20 13:17:16	124816	9312	115504
2016-06-20 13:22:15	124816	9304	115512
2016-06-20 13:27:15	124816	9228	115588
2016-06-20 13:32:16	124816	9304	115512
2016-06-20 13:37:16	124816	9276	115540

Figure 6-4 Memory Usage Statistics Continued



Viewing the Phone Numbers Managed by EdgeView

The Known Telephone Numbers box in the middle of the page lists the phone numbers that are being explicitly managed by EdgeView. Click on a phone number in the list to perform an active line test to check the connectivity between the EdgeMarc and the phone. See Performing an Active Line Test to Verify EdgeMarc Connectivity in Chapter 8, *MOS Analysis and Troubleshooting*.

Viewing the Endpoint Client List Snapshot

The Endpoint Client List Snapshot box lists the identifiers of all endpoints attached to the EdgeMarc. These endpoints may or may not be explicitly managed by EdgeView. To explicitly manage an endpoint, click on the button with the plus (+) sign. The phone number will be added to the List of Known Telephone Numbers.

Manually Initiating a Call

Click the **Get Info From EdgeMarc** button to manually initiate a call to gather information from the endpoints attached to the EdgeMarc.

Viewing Node Status with EdgeView

Click the **Status Table** icon in the EdgeView icon bar to display the Main Status page which shows all nodes and endpoints being monitored by EdgeView. The Main Status page features tabs that display status specific to the EdgeMarcs, groups, third-party and SNMP nodes, IP phones, and EdgeConnects being managed by EdgeView (Figure 6-5).

Figure 6-5 Main Status Page



EdgeMarcs | Groups | Other Nodes | Phones | EdgeConnects

Search: Exact Match | In Column Name | Do Search | Reset | Show 25 Items | Refresh Interval Never | Customize

Showing items [1-3] out of a total of 3

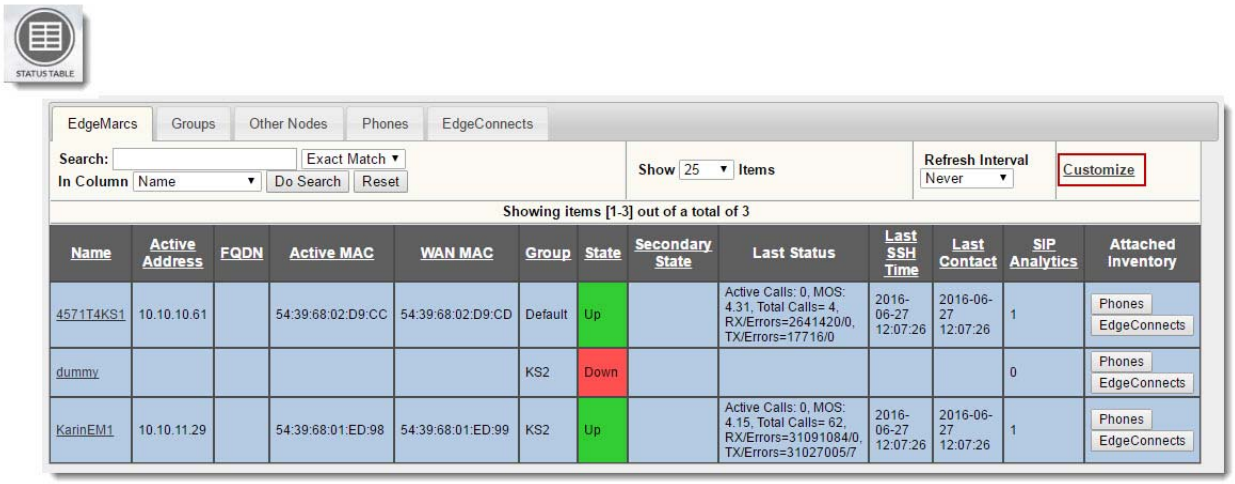
Name	Active Address	FQDN	Active MAC	WAN MAC	Group	State	Secondary State	Last Status	Last SSH Time	Last Contact	SIP Analytics	Attached Inventory
4571T4KS1	10.10.10.61		54:39:68:02:D9:CC	54:39:68:02:D9:CD	Default	Up		Active Calls: 0, MOS: 4.31, Total Calls= 4, RX/Errors=2641420/0, TX/Errors=17716/0	2016-06-27 12:07:26	2016-06-27 12:07:26	1	Phones EdgeConnects
dummy					KS2	Down					0	Phones EdgeConnects
KarinEM1	10.10.11.29		54:39:68:01:ED:98	54:39:68:01:ED:99	KS2	Up		Active Calls: 0, MOS: 4.15, Total Calls= 62, RX/Errors=31091084/0, TX/Errors=31027005/7	2016-06-27 12:07:26	2016-06-27 12:07:26	1	Phones EdgeConnects

Customizing the Status Table

You can customize which columns you want to display in the Main Status page and the order in which you want them to appear. To customize the Main Status table:

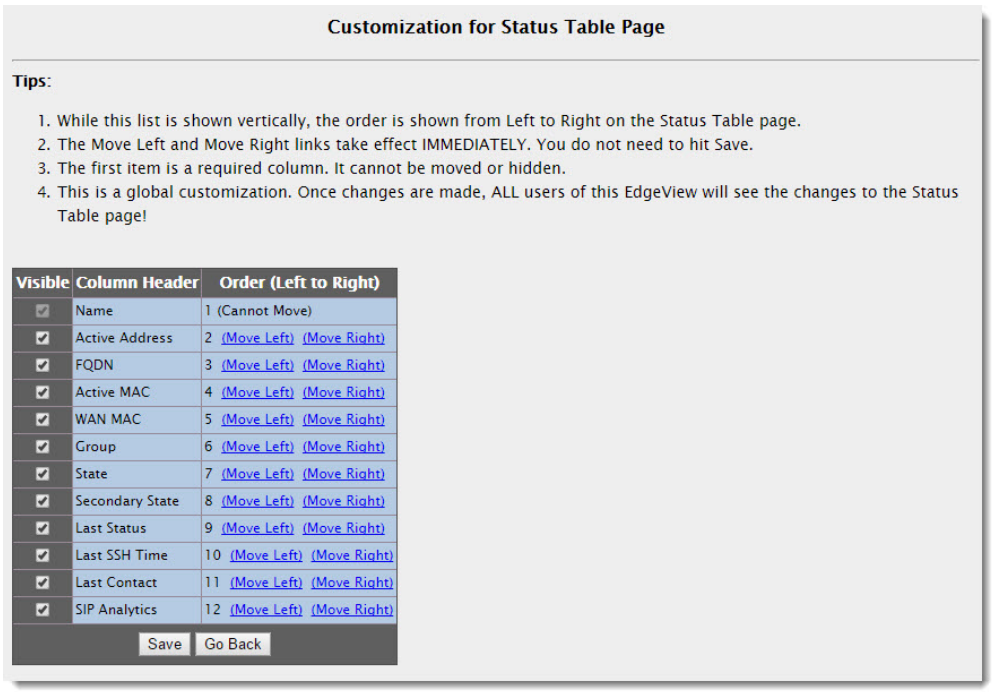
1. Click **Customize** in the status screen (Figure 6-6).

Figure 6-6 Customizing the Status Table



2. In the Customization for Status Table Page (Figure 6-7), enable/disable the checkboxes to select which columns you want to display in the table.
3. Click **Move Left** or **Move Right** to change the order of the columns in the table.
4. Read the on-screen tips for more information about how these settings take effect.
5. Click **Save**.

Figure 6-7 Customization for Status Table Page



Viewing Global EdgeMarc Status

Click the **EdgeMarcs** tab in the Main Status page to display color-coded status of all the EdgeMarcs that EdgeView is managing as well as the group to which each EdgeMarc belongs. Refer to Figure 6-5. Click the column headings in the table to filter the status details by EdgeMarc Name, IP address, Group Name, Up/Down State, Secondary State and Last SSH time.

Secondary State Warnings

The Secondary State column shows the EdgeMarcs which are reachable but cannot be accessed by EdgeView via SSH. For these EdgeMarcs, a warning will be displayed. You can filter on that column to view all the EdgeMarcs that have warnings.

Using the Search Function

The Search fields at the top of the page allow you to search for a specific EdgeMarc, IP address, Group, State, Secondary State, Last SSH Time, and

Last Contact. EdgeView will display only the status that matches the search criteria. To do a search:

1. Type an entry in the **Search** field.
2. Select the search criteria (Exact Match, Starts With, Ends With or Contains).
3. Select the column on which you want to search.
4. Click **Do Search**.
5. Click **Reset** to clear the search results.

Viewing EdgeMarc Node Status

Click the **Phones** and **EdgeConnects** buttons in the Attached Inventory column to view the status of the phones and EdgeConnects (if any) that are connected to the EdgeMarc.

Changing the Number of EdgeMarcs Displayed

Click the **Show Items** drop-down box on the Main Status page to select the number of EdgeMarcs that you want to display in the status window. By default, status is displayed for 25 EdgeMarcs.

Specifying a Refresh Interval

From the **Refresh Interval** drop-down box, select how often you want EdgeView to update the status. EdgeView will refresh the status on the page according to the interval you set here.

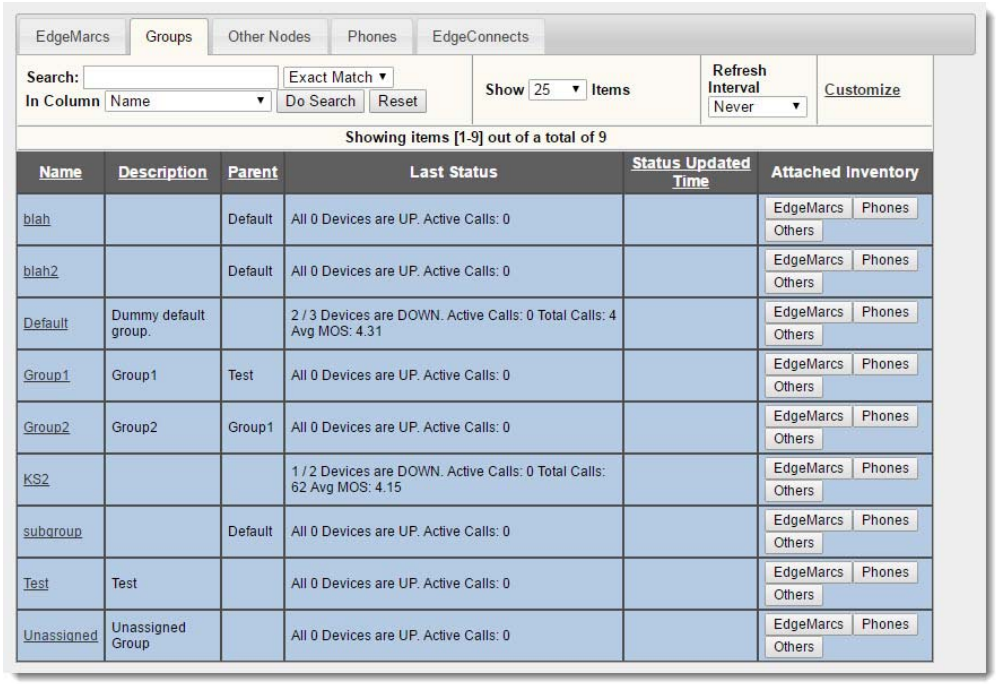
Viewing Group Status

Click the **Groups** tab in the Main Status page to display group level status for each group managed by EdgeView. Refer to Figure 6-8. The status includes the group name, description, the parent to which the group belongs, the time stamp and results of the most recent poll. The buttons in the Attached Inventory column display the EdgeMarcs, phones and other nodes associated with the selected group.

Click the **Show Items** and **Refresh Interval** drop-down boxes to select the number of groups you want to display in the table and how often you want EdgeView to update the group status. By default, the Group Status Table displays status for 25 groups. EdgeView updates the status every minute.

Use the Search function to search for groups by Name, Description, Parent or Status Updated Time. The Group Status table will display status for the group(s) that match the search criteria. Refer to Using the Search Function for more details.

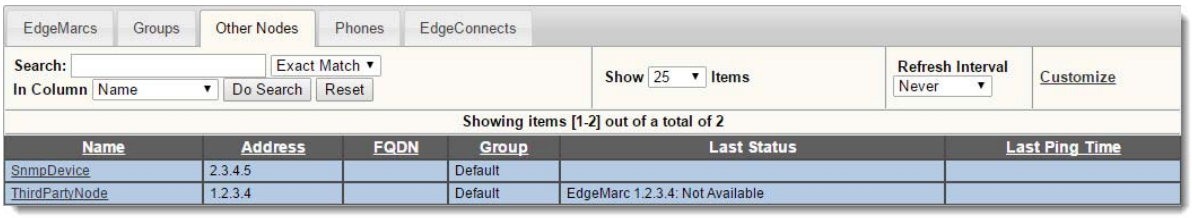
Figure 6-8 Groups Status Table



Viewing the Status of Other Nodes

1. Click the **Other Nodes** tab in the Main Status page to display the status for third-party nodes and SNMP-based nodes that are being managed by EdgeView (Figure 6-9).

Figure 6-9 Other Nodes Table



The status displayed in the Other Nodes Status table includes the node name, IP address, the parent to which the node belongs, the time stamp and results of the most recent ping, and the current device up/down state.

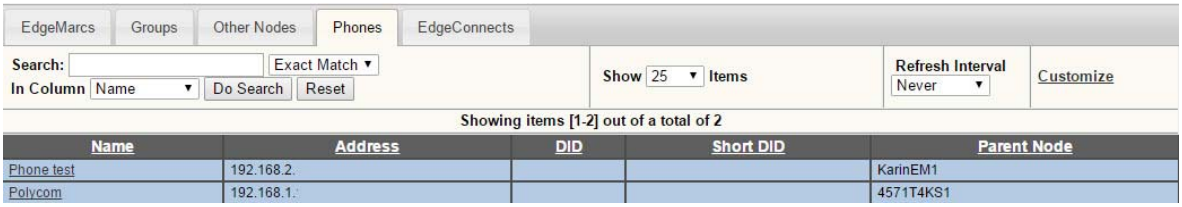
2. Click the **Show Items** and **Refresh Interval** drop-down boxes to select the number of nodes you want to display in the table and how often you want EdgeView to update the status in the table. By default, the Other Devices Table displays status for 25 items and EdgeView updates the status every minute.

3. Use the **Search** field to search for devices by Name, IP address, Parent, Last Ping time or state. The table will display status that matches the search criteria. Refer to Using the Search Function.

Viewing IP Phone Status

1. Click the **Phone Status** tab in the Main Status page to display the status for the IP phones that are being managed by EdgeView. The phone Name, IP address, DID, Short DID, Parent Group to which the phone belongs, and the provisioning status all display in the Phone Status Table (Figure 6-10). Click on any column title in the table to sort the information by that topic.

Figure 6-10 Phones Status Tab



2. Use the **Show Items** and **Refresh Interval** drop-down boxes to select the number of IP phones you want to display in the table and how often you want EdgeView to update the phone status in the table. By default, the Phone Status Table displays status for 25 phones and EdgeView updates the status every minute.
3. Use the **Search** field to search for nodes by Name, IP address, Parent, Last Ping time or state. The table will display status that matches the search criteria. Refer to Using the Search Function.

Viewing EdgeConnect Status

1. Click the **EdgeConnects** tab in the Main Status page to display the status for the EdgeConnects that are being managed by EdgeView (Figure 6-9). The EdgeConnect Name, IP address, New Address, Parent Group to which the EdgeConnect belongs, and the current Up/Down status all display in the EdgeConnect Status Table. Click on any column title in the table to sort the information by that topic.

Figure 6-11 EdgeConnect Status Table



2. Use the **Show Items** and **Refresh Interval** drop-down boxes to select the number of EdgeConnects you want to display in the table and how often you want EdgeView to update the EdgeConnect status. By

default, the EdgeConnect Status Table displays status for 25 EdgeConnects and EdgeView updates the status every minute.

3. Use the **Search** field to search for nodes by Name, IP address, Parent, Last Ping time or state. The table will display status that matches the search criteria. Refer to Using the Search Function.

Sending UP/DOWN Status Notifications at the Tenant, Group and Node Level

EdgeView can send an email notification to alert you each time the UP/DOWN status changes for nodes at the group level and node level. Additionally, you can configure a “Polling Notification Profile” which specifies preferences for sending up/down status notifications.

When node UP/DOWN status notifications are set at the group (or Tenant) level, EdgeView will send an email notification when the UP/DOWN status changes for ANY EdgeMarc in the group or sub-groups in the hierarchy. When node UP/DOWN status notifications are set at the node level, EdgeView will send an email notification when the UP/DOWN status changes for the associated EdgeMarc node.

At least one Polling Notification Profile must be set and be active for EdgeView to send a group level or node level email notification(s). Although there may be email addresses configured for the group level or node level notifications, EdgeView will only send a notification if there is an active Polling Notification Profile for the current time (or if **Always On** is selected in the profile).



Note

If you assign the same notification email addresses at multiple levels in the hierarchy, duplicate notification messages will be sent. Since there may be many nodes associated with a group, use the email notification feature with caution to avoid bombarding the specified email addresses with messages.

Setting Node UP/DOWN Status Notifications at the Tenant Level

To set an UP/DOWN Status notifications at the Tenant level:

1. Select the Tenant from the device tree. To see all Tenants, select the user at the top of the tree (for example 'edgeview'). The Advanced Directory of Tenants page displays (Figure 6-12).

Figure 6-12 Setting a Node UP/DOWN Status Notification (Tenant)



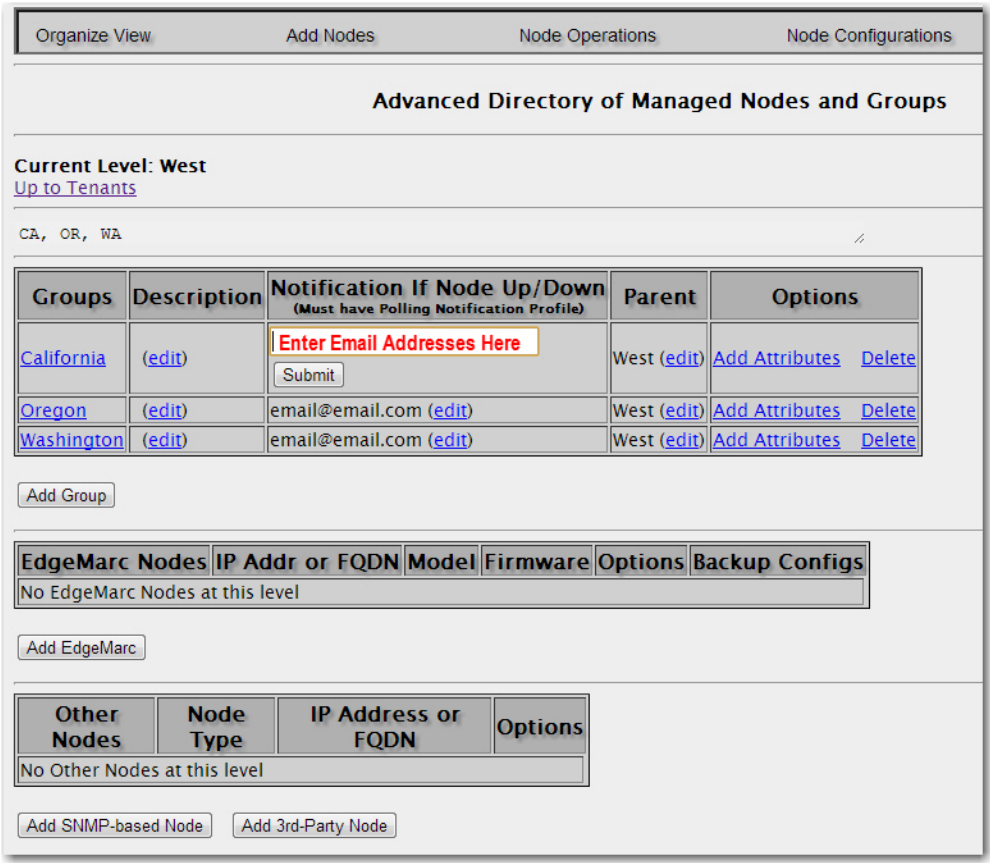
2. Click **Edit** in the 'Notification If Node Up/Down' column for the Tenant.
3. Enter an email address(es) in the address field. Separate multiple email addresses with a comma.
4. Click **Submit**.

Setting Node UP/DOWN Status Notifications at the Group Level

To set a node UP/DOWN status notification at the group level:

1. Select the group from the device tree. The Advanced Directory of Managed Nodes and Devices page displays (Figure 6-13).
2. Click **Edit** in the 'Notification if Device Up/Down' column for the group.
3. Enter the email address(es) to which you want to send node up/down notifications. Separate multiple email addresses with a comma.
4. Click **Submit**.

Figure 6-13 Setting a Node UP/DOWN Status Notification (Group Level)

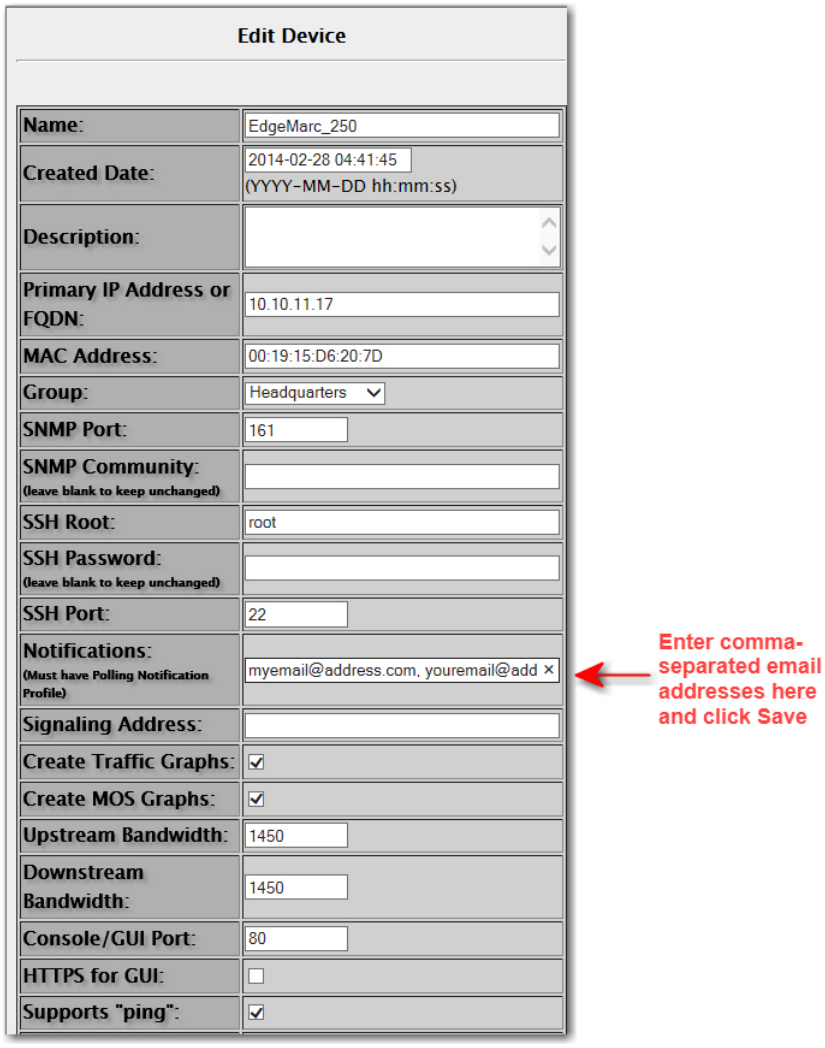


Setting Node UP/DOWN Status Notifications for an EdgeMarc Node

To set a node UP/DOWN notification for an EdgeMarc node:

1. Access the Edit Device page for the EdgeMarc node in one of the following ways:
   - From the device tree, select the parent group for the EdgeMarc node. The Advanced Directory of Managed Nodes and Devices page displays (Figure 6-13). In the EdgeMarc Node table, click **Edit** in the 'Notification if Device Up/Down' column for the EdgeMarc Node.
   - Select the EdgeMarc node from the device tree and then select the **Operation > Edit Device** menu option.
2. In the Notifications field on the **Edit Device** page (Figure 6-14) enter the email address(es) to which you want to send node up/down notifications. Separate multiple email addresses with a comma.
3. Click **Save**.

Figure 6-14 Setting an UP/DOWN Notification for an EdgeMarc Node



Viewing Inventory

Click the **Inventory** icon in the EdgeView icon bar to display inventory pages for the EdgeMarc, Groups, Other Nodes, Phones, and EdgeConnects.



The Inventory page features tabs that display status specific to the EdgeMarcs, groups, third-party and SNMP nodes, IP phones, and EdgeConnects being managed by EdgeView. Refer to the examples in Figure 6-16 and Figure 6-17.

Viewing CSV Inventory Output

Select the **CSV Output** checkbox to see device information in comma-separated value (CSV) format. When generating a CSV Inventory Report, the entire Group tree is now listed under the Group category.

1. Select the **Inventory** tab from EdgeView GUI.
2. Select the **EdgeMarcs** tab from Inventory page.
3. Select **CSV Output** checkbox.

Figure 6-15 CSV Inventory Output

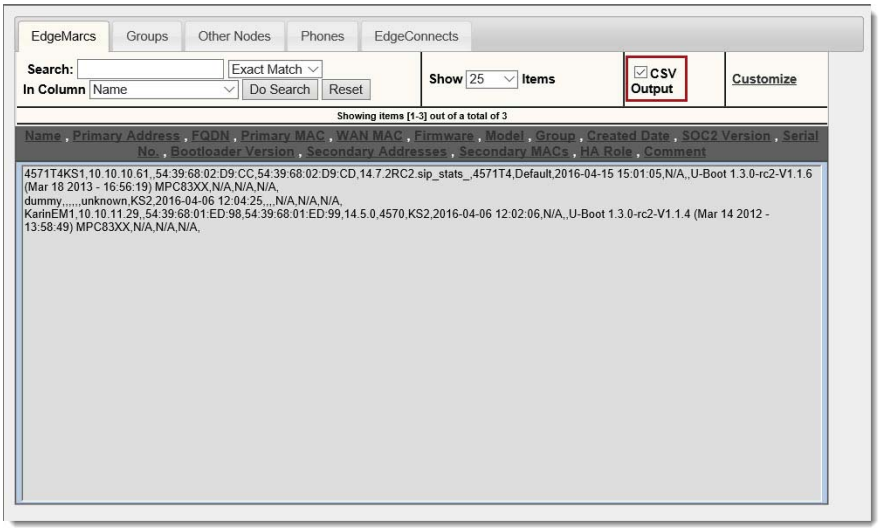


Figure 6-16 EdgeMarc Inventory Page

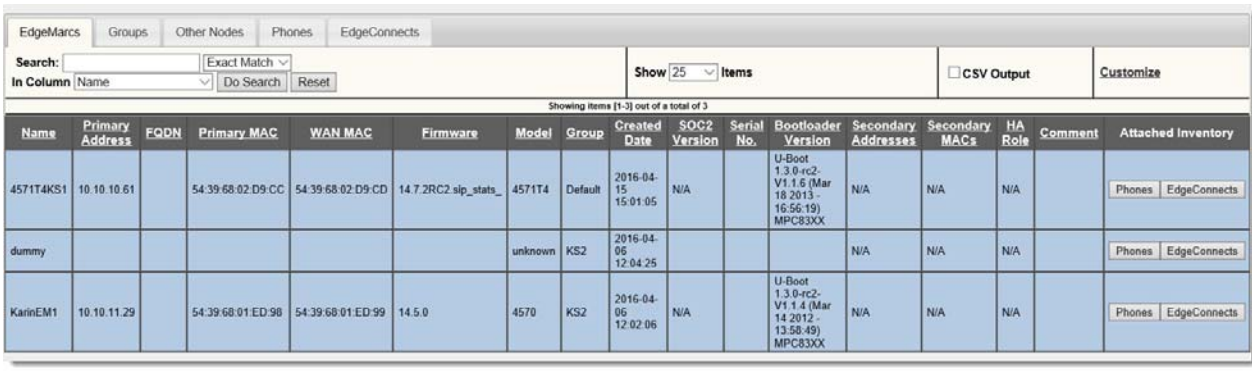
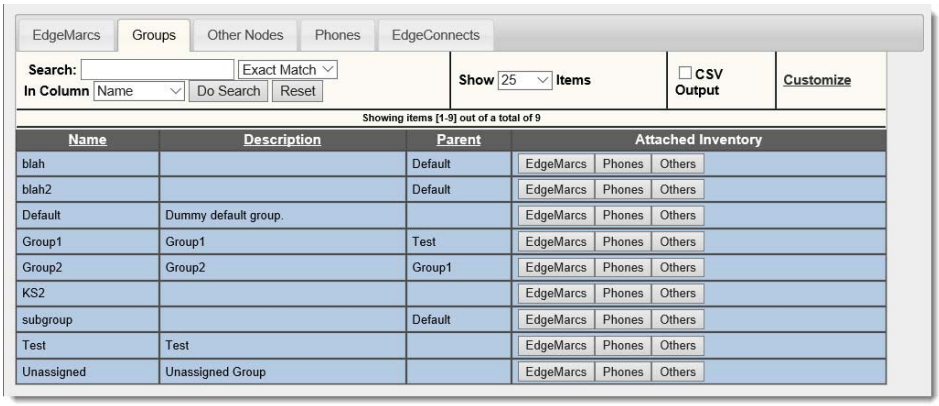


Figure 6-17 Group Inventory Page



Configuring Email Status Notifications

EdgeView can automatically send email notifications to alert you of device status and certain events that occur on the EdgeView system and managed groups and nodes. To set configure notification settings, click the **Notifications** icon and choose from the following menus:

Figure 6-18 Configuring Email Notifications

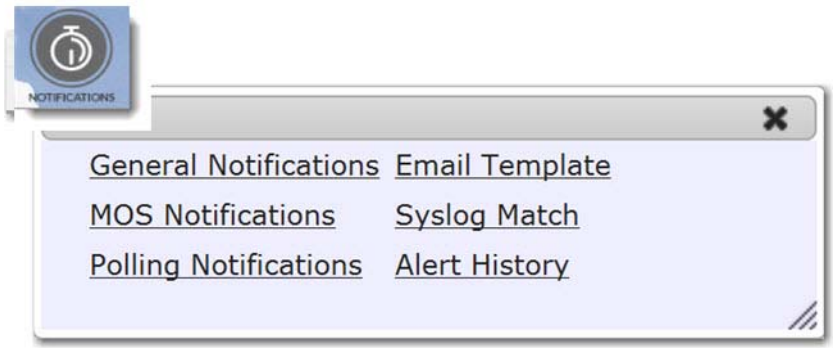


Table 6-2 Configuring E-Mail Status Notifications

Notification	Description
General Notifications	Displays the General System Notifications page for configuring alerts for the following system-level events: • Hard drive disk space is reaching the available threshold • Swap space is reaching the available threshold • IP address changes in the syslog • EdgeMarc crashes • EdgeMarc hostname synchronization issues • Number of free node licenses is below 10% See Configuring General System Notifications.
MOS Notifications	Displays the EdgeView MOS Notifications page for specifying rules for: • Sending MOS Alerts on CAC Exceeded Events • Sending MOS Alerts on Survivability Changes • Sending SNMP Traps for MOS Alerts • Enabling Live MOS Capture • Testing MOS Notification Alert Settings See Sending Notifications When the SIP Server Status Changes.
Polling Notifications	Displays the Polling Notification Profiles page for setting up notifications for events triggered during or upon completion of the polling cycle. See Creating a Polling Notification Profile.
Email Template	Displays the Notification Email Template page for customizing the email Subject for different email notification types and to customize the footer for support-oriented emails (alerts) and sales-oriented emails (license issues). See Configuring the Email Notification Template.
Syslog Match	Displays the Syslog Match page for configuring EdgeView to run a script when a specified message appears in the syslog. The script can be run in EdgeView or on the EdgeMarc node. Once the script has executed, EdgeView will send an email to a specified email address. See Executing a Script and Sending Notifications on a Syslog Match.
Alert History	Shows all outgoing email notifications sent by EdgeView sorted by the most recent date/time first. The subject is included and the body of the message can be read from the **Show Details** link. See Viewing Notification Alert History.

Configuring General System Notifications

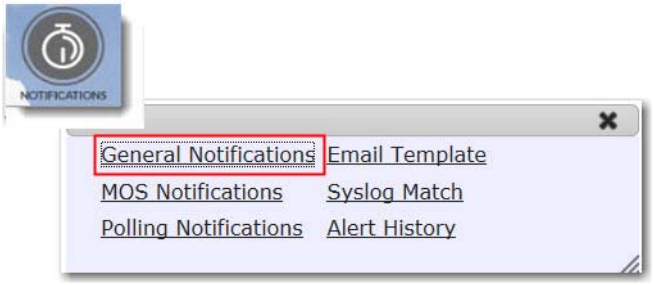


EdgeView can send email notifications for the following system events:

- Hard drive disk space is reaching the available threshold
- Swap space is reaching the available threshold
- IP address changes in the syslog
- EdgeMarc crashes
- EdgeMarc hostname synchronization issues
- Number of free node licenses is below 10%

You can specify the email address(es) where you want the notifications sent. Email recipients are notified at the end of the polling cycle.

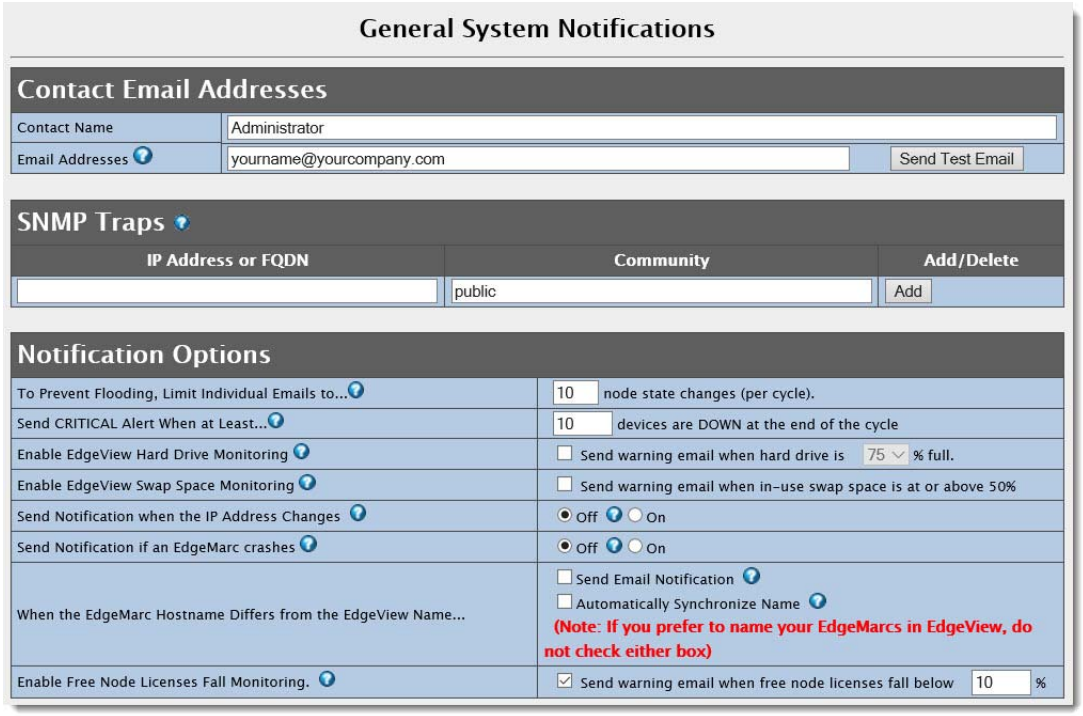
Figure 6-19 General Notifications Menu



To configure a general system notification:

1. Select **Notifications > General Notifications**. The General System Notifications page displays (Figure 6-20).

Figure 6-20 General System Notifications Page



- Hover your mouse over the help icon next to each field for help on configuring general system notification options. The help descriptions are included in Table 6-3.

Table 6-3 General System Notifications Field Descriptions

Field	Description
Contact Name	Assign any name that you want to appear in the notification emails.
Email Addresses	Enter comma-separated email address(es) that will receive system level notifications and (potentially) all up/down notifications.
To Prevent Flooding, Limit Individual Emails to...	When the end of the polling cycle method is used, the number set here limits the number of notifications sent to email addresses at the group level or node level. The default is 10. The limit counts the number of nodes that send out notifications and when the set number is reached, subsequent emails are not sent during this polling cycle. This can help limit a flood of emails if there is a system-wide outage. Note that the summary email will still include all the nodes.
Send CRITICAL Alert When at Least...	When the number of devices set here are DOWN at the end of the polling cycle, a critical alert will be sent unless the device has been down for more than a day. The default is 10 devices. **Note:** The alert will not be cleared until the next polling cycle and only if the number of devices is less than this threshold.

Table 6-3 General System Notifications Field Descriptions

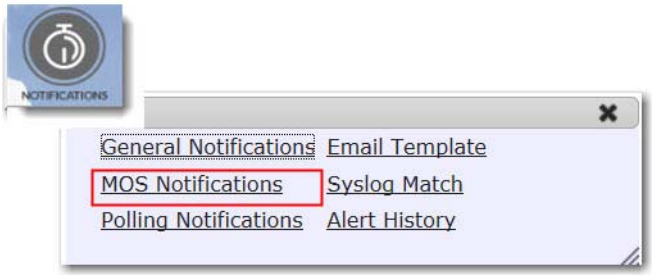
Field	Description
Enable EdgeView Hard Drive Monitoring	When enabled, an email will be went to the (list of) addresses in the **Email Addresses** field when the EdgeView hard drive reaches the specified threshold.
Enable EdgeView Swap Space Monitoring	When enabled, an email will be went to the (list of) addresses in the **Email Addresses** field when the EdgeView in-use swap space reaches the specified threshold.
Send Notification when the IP Address Changes	When enabled, EdgeView will examine the IP address of incoming messages to the syslog and send a notification if the IP address has changed for a KNOWN device.
Send Notification if an EdgeMarc crashes	When enabled, EdgeView will watch the syslog for a message indicating that an EdgeMarc ALG module has crashed. EdgeView will then get the tinfo file and email it to the list of addresses in the Email Address field.
When the EdgeView Hostname Differs from the EdgeView Name...	When the **Send Email Notification** setting is enabled, EdgeView will send a notification to the addresses in the **Email Addresses** field when the EdgeMarc hostname and the EdgeMarc name in the EdgeView database are out of sync. When the **Automatically Synchronize Name** setting is enabled, EdgeView will automatically change the EdgeView name to match the EdgeMarc Hostname. If you prefer to name your EdgeMarcs in EdgeView, do not check this box.
Send Email Notification when free node licenses fall below 10%	When **On**, each time a new EdgeMarc or other node is added, EdgeView will check to see if the number of licensed free nodes falls below 10%. If so, it sends an email message to the addresses in the **Email Addresses** field. This field is set to **On** by default.

Sending MOS Alert Notifications



EdgeView can send MOS alert notifications to provide proactive notification of poor VoIP call performance in the network. You can configure EdgeView to send email notifications when it receives a MOS threshold exceeded alarm from any node being monitored. This feature requires all nodes to report syslog events to EdgeView.

Figure 6-21 MOS Notifications Menu

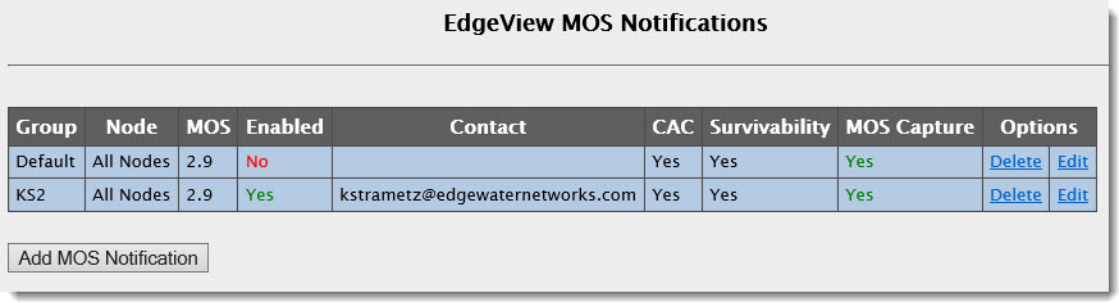


Adding/Editing a MOS Alert

To add MOS alert notifications at the group or node level:

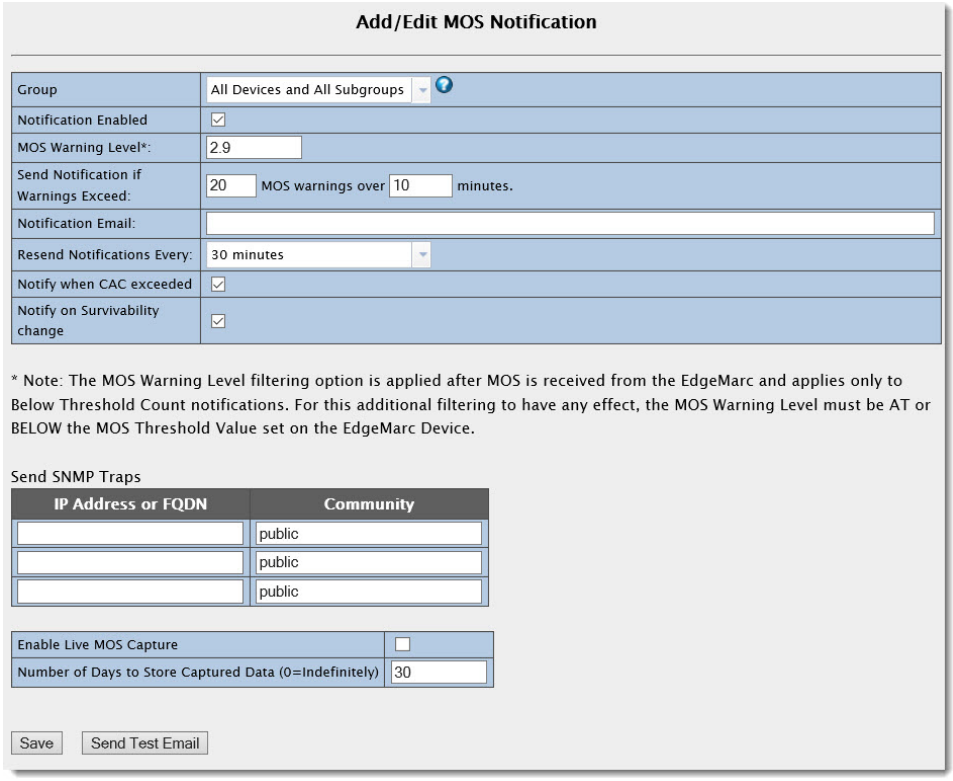
1. Select **Notifications > MOS Notifications** (Figure 6-22).

Figure 6-22 Adding a MOS Notification



2. Click **Add MOS Notification** to add a new MOS notification or click **Edit** to edit an existing MOS notification. The Add/Edit MOS Notification screen displays (Figure 6-23).

Figure 6-23 Add/Edit MOS Notification



3. From the Group drop-down menu, select a Tenant, group, or node for which you want to apply the notification as follows:
   - To apply the notification to all nodes or groups visible to this user, select **All Devices and All sub-groups**.
   - To apply the notification to a Tenant or group, select it. If their are nodes in a group, they will be selectable from the Node drop-down box.
   - To apply the notification to an individual node, select the group to which the node belongs and then select the node under that group from the **Node** drop-down menu. Only nodes directly under that group can be selected. To select nodes under sub-groups, first select the sub group from the **Group** drop-down menu and then select the node from the **Node** drop-down menu.

   Note that the page is refreshed when the group is changed, so any changes will be lost.
4. Check the **Notification Enabled** checkbox.
5. Enter a **MOS Warning Level**. This is the MOS value used to trigger an alert notification. When the MOS from the EdgeMarc reaches this threshold or below, it will send an alarm. The default is 2.9. Whether an alarm is sent depends on the Send Notifications rule and whether this notification is set up for this specific node or is in the group. The

warning level must be at or below the warning value set on the EdgeMarc.

6. Enter values for **Send Notification if Warnings Exceed** (for example, how many warnings are received before an email notification is sent).
7. In the **Notification Email** field, enter the email address(es) that will receive the MOS notifications.
8. In the **Resend Notifications Every** drop-down box, select a value for how often you want EdgeView to resend the MOS notifications. The default is 30 minutes.
9. Configure additional MOS alert settings. See the following topics:
   - Sending MOS Alerts on CAC Exceeded Events
   - Sending MOS Alerts on Survivability Changes
   - Sending SNMP Traps for MOS Alerts
   - Enabling Live MOS Capture
   - Testing MOS Notification Alert Settings
10. Click **Save**. The MOS Alert will be listed in the EdgeView MOS Notifications table (Figure 6-22).

Deleting a MOS Alert

To delete a MOS alert:

1. Select **Notifications > MOS Notifications**.
2. In the EdgeView MOS Notifications table, click **Delete** for the MOS alert you want to delete. A confirmation dialog box displays.
3. Confirm the deletion. Upon confirmation, the MOS alert will be deleted from the EdgeView MOS Notifications table.

Sending MOS Alerts on CAC Exceeded Events

Enable the **Notify when CAC exceeded** checkbox in the Add/Edit MOS Notification page to send a notification when an EdgeMarc generates a Call Admission Control (CAC) message. EdgeMarcs generate CAC messages to indicate that there is insufficient WAN bandwidth available to support new VoIP call requests.

Sending MOS Alerts on Survivability Changes

Enable the **Notify on Survivability change** checkbox in the Add/Edit MOS Notification page to send an alert whenever an EdgeMarc node transitions into or out of local survivability mode.

Sending SNMP Traps for MOS Alerts

EdgeView can send SNMP traps for notification alerts. Under **SNMP Traps** in the Add/Edit MOS Notification page, enter the IP address and community

string for the destination SNMP manager(s). EdgeView will send a trap to third-party network management systems for the following events:

Event	Description
Device Down	EdgeView detects that a device is down.
MOS Threshold	An EdgeMarc MOS is below threshold.
CAC Limit	An EdgeMarc CAC limit threshold.
Survivability Change	An EdgeMarc changes survivability state.

Enabling Live MOS Capture

To enable or disable continuous MOS capture, click the **Live MOS Capture** checkbox. If enabled, specify the number of days that captured data will be stored in the MOS database (0=indefinitely). The default is set to store 30 days of data. If disabled, MOS statistics sent from EdgeMarc nodes will not be saved in the EdgeView database.

Tip

If you are using EdgeView Reports, you may want to increase the number of days that data is stored in the database.

Testing MOS Notification Alert Settings

After you set MOS notification settings on the Add/Edit MOS Notification page, click **Send Test Email** to send a test email to the notification addresses. The following popup will display to confirm the email was sent. The recipient will receive a test email notification.

Note

If the pop up window does not display, check the pop-up blocker settings in your web browser.

Figure 6-24 Sending a Test Email for a MOS Notification

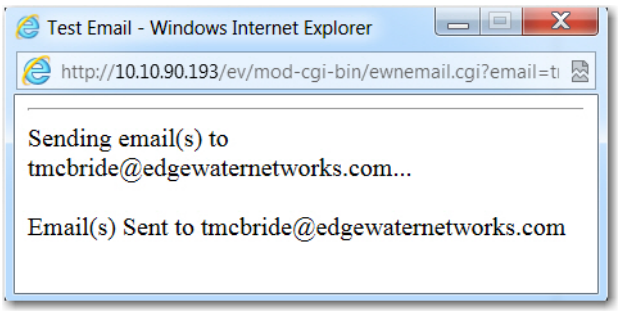
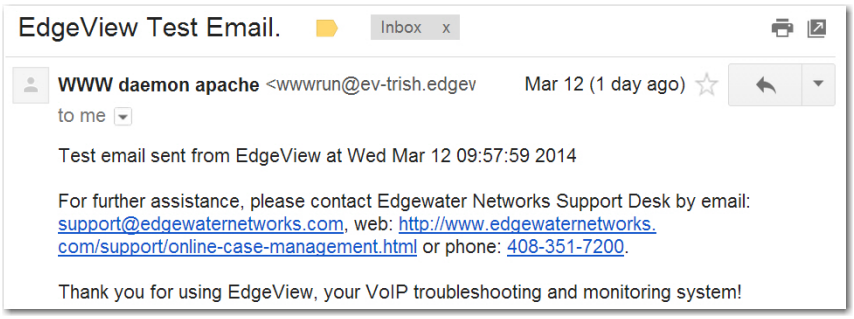


Figure 6-25 shows an example of the test email that is sent.

Figure 6-25 Notification Test Email



If the test email notification is successful, click **Save** to save your changes. The new or changed email notification will now appear in the list of MOS Notifications.

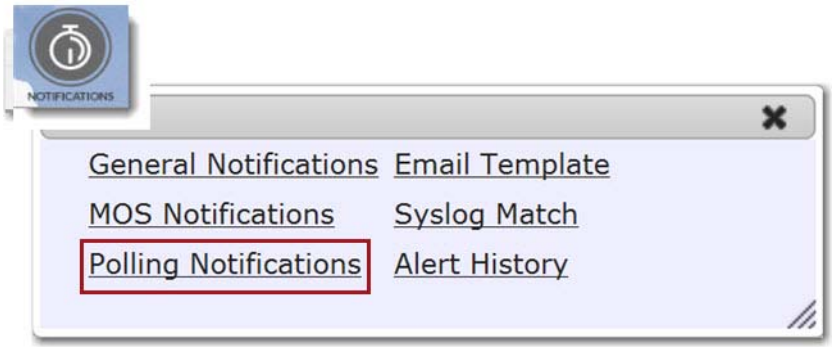
Creating a Polling Notification Profile

You can set preferences for sending UP/DOWN status notifications in a *Polling Notification Profile*. A Polling Notification Profile specifies the email recipients, time period, frequency, and email format for UP/DOWN status notifications. EdgeView uses these settings to send a summary email which includes a table showing the state changes for the groups and nodes.

Note

At least one Polling Notification Profile must be set and be active for EdgeView to send a group level or node level email notification(s). Although there may be email addresses configured for the group level or node level notifications, EdgeView will only send a notification if there is an active Polling Notification Profile for the current time (or if Always On is selected in the profile).

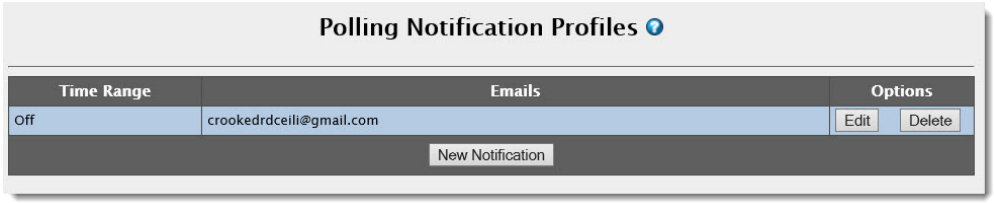
You can create Polling Notification Profiles to send SNMP traps for node UP/DOWN status notifications and also to send a separate email notification when the SIP server registration state changes. See Sending SNMP Trap Notifications and Sending Notifications When the SIP Server Status Changes for details.



To create a Polling Notification Profile:

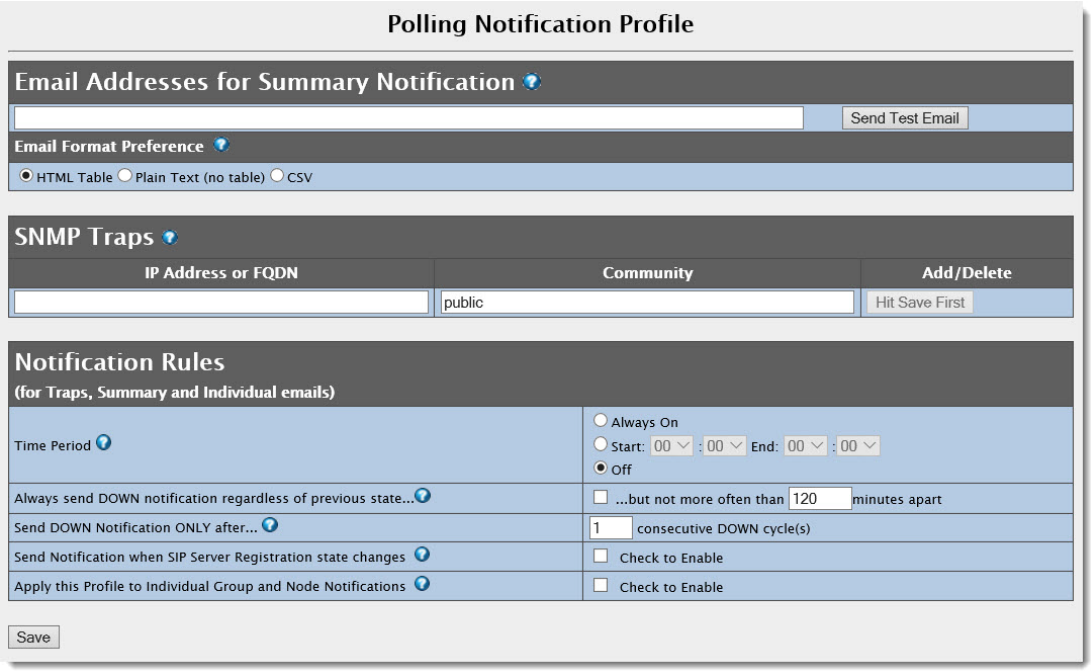
1. Select **Notifications > Polling Notifications**. The Polling Notification Profiles page displays (Figure 6-26). This page lists all profiles by Time Range and email recipients, with options to edit and delete.

Figure 6-26 Polling Notification Profiles



1. Click **New Notification**. The Polling Notification Profile page displays (Figure 6-27). Hover your mouse over the help icon next to each field for details about how to configure the field.

Figure 6-27 Polling Notification Profile Page



2. Enter the email addresses used for polling notifications. Separate multiple email addresses with a comma.
3. Choose the format for the email notification: HTML Table for a nicely formatted table, Plain Text if your emailer does not accept HTML, or CSV for exporting to a spreadsheet.
4. To send SNMP traps in addition to emails, enter the IP Address or FQDN and the Community String for where to send the SNMP Trap and click Add. See Sending SNMP Trap Notifications.
5. Set Notification Rules (Table 6-4).
6. When you are done configuring settings, click **Save**. The new profile will be listed in the Polling Notification Profiles table (Figure 6-27) and will take effect at the end of the next polling cycle.
7. Click **Send Test Email** to verify that the notification is properly configured.

Table 6-4 Setting Notification Rules

Field	Description
Time Period	Specify a time period for when the notifications should be sent. For example, if you set a time period of 9 a.m. to 5 p.m., EdgeView will only send the email notifications during that time period. Notifications or SNMP traps will not be sent for polling cycles that occur outside this window. Select **Always On** if you want to use this time period for all notifications. Set this to **Always Off** if you do not want EdgeView to send this notification until the user selects **Always On**. This is useful, for example, if you need to temporarily stop the notification from being sent during a maintenance window. This saves you from having to re-enter all the information for the rule.
Always Send DOWN notification regardless of previous state...	Enable this checkbox and specify the frequency, in minutes, that EdgeView should use when sending email/SNMP trap notifications if the EdgeMarc is down. EdgeView will send a notification regardless of whether the previous state of the EdgeMarc was UP or DOWN but not more often than the specified number of minutes. The default is 120 minutes apart.
Send DOWN Notification ONLY after...	Specify the number of consecutive down cycles the EdgeMarc must be down before EdgeView sends an email and/or SNMP trap notification. The default is 1 consecutive down cycle. See "Sending Notifications When the SIP Server Status Changes."
Send Notification when SIP Server registration status changes	Enable this checkbox if you want EdgeView to send a notification when the SIP server state changes for SIP servers attached to the polled EdgeMarc. See "Sending Notifications When the SIP Server Status Changes."
Apply this Profile to Individual Group and Node Notifications	Enable this check box if you want to use the rules of the profile to determine if emails are sent to the notifications defined for group or node attributes.

Editing a Polling Notification Profile

1. Select **Notifications > Polling Notifications**.
2. In the Polling Notification Profiles page, click **Edit** in the Options column for the polling notification profile you want to edit.
3. Change settings as described in Figure 6-4.
4. Click **Save**. Your changes will take effect at the end of the next polling cycle.

Deleting a Polling Notification

1. Select **Notifications > Polling Notifications**.
2. In the Polling Notification Profiles page, click **Delete** in the Options column for the polling notification profile you want to delete.

3. Click **OK** in the delete confirmation dialog box to delete the notification profile.

Sending SNMP Trap Notifications

In addition to sending email notifications, you can send SNMP traps to the email address(es) set on the Polling Notification Profile page.

To configure a SNMP trap notification:

1. Select **Notifications > Polling Notifications**.
2. In the Polling Notification Profiles page, Click **New Notification**.
3. Enter a valid IP Address or FQDN and a community string to which the SNMP traps should be forwarded.
4. Click **Add**.
5. Click **Save.** The trap will take effect at the end of the next polling cycle.

Deleting an SNMP Trap Notification

To delete an SNMP trap notification:

1. Select **Notifications > Polling Notifications**.
2. In the Polling Notification Profiles page, click **Edit** for the polling notification.
3. Click **Delete**.
4. Click OK in the delete confirmation dialog box. The change will take effect at the end of the next polling cycle and the trap will be removed from the list of SNMP traps.

Sending Notifications When the SIP Server Status Changes

EdgeView can send a separate email notification when the SIP server state changes (e.g. from UP to DOWN or from DOWN to IDLE) for any SIP server attached to the polled EdgeMarc. The notification is sent at the end of the polling cycle.

To set this option, enable the **Send Notification when SIP Server registration status changes** checkbox for a Polling Notification Profile.

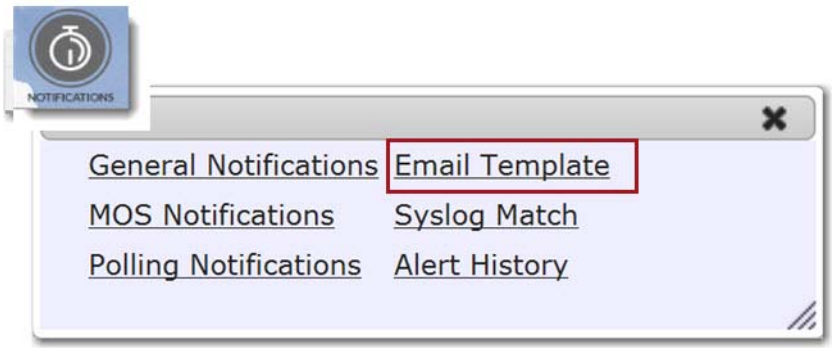
The SIP server registration status notification works as follows:

1. EdgeView polls the EdgeMarc.
2. If the EdgeMarc SIP Server status changes, EdgeView will send a notification to the email address(es) configured in the Polling Notification Profile.
3. EdgeView will also send an email notification to the addresses set in the **Notification if Node UP/DOWN** field at the group- and/or node level.
4. If the EdgeMarc UP/Down status changes during the same polling cycle, a separate email notification will be sent to the addresses configured for the EdgeMarc group and/or node.

Configuring the Email Notification Template

Select the **Notifications > Email Template** menu to customize the Subject text for the email that gets sent out for general notifications and also add your own text for the customer support and sales information that displays in the footer of the email notification.

Figure 6-28 Email Template Menu



To customize the email notification template:

1. Select **Notifications > Email Template**. The Notification Email Template page displays (Figure 6-29).

Figure 6-29 Editing the Email Notification Template



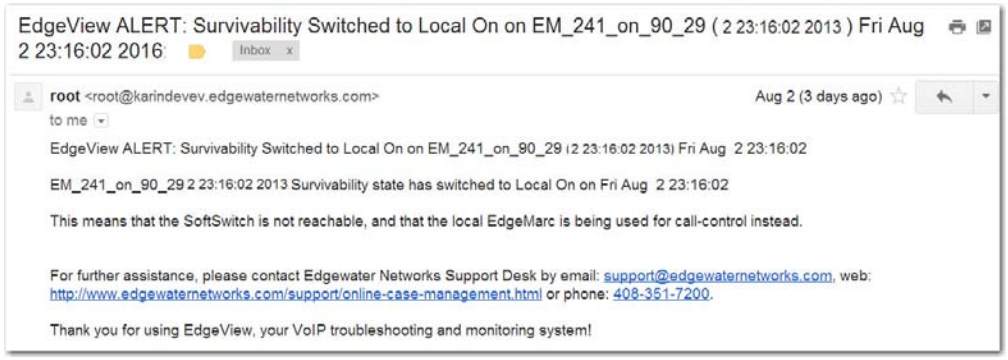
2. Hover your mouse over the help icon next to each type of alert for a description of the acceptable variables for that entry. To change a setting, type your own values between the percent (%) signs in the text string.
3. Under the **Email Footer for Support Oriented Emails** heading, type the text that you want to display at the end of email notifications to assist users with contact and support information.
4. Under the **Email Footer for Sales Oriented Emails** heading, type the text that you want to display at the end of sales-oriented notifications (for example, notifications sent for licensing issues) to assist users with contact and other information.
5. Click **Save**.

Sample MOS Notification Email

Depending upon the settings on the Notification Email Template page, the notification email will include the following information:

- Name of the group or node that measured the MOS event
- Node IP address
- Reported time
- Number of MOS values below the configured threshold
- Monitored time period
- Lowest MOS score measured and the average below threshold value

Figure 6-30 Sample MOS Notification Email — Survivability Event



Executing a Script and Sending Notifications on a Syslog Match



You can configure EdgeView to run a script when a specified message appears in the syslog. The script can be run in EdgeView or on the EdgeMarc node. Once the script has executed, EdgeView will send an email to a specified email address.

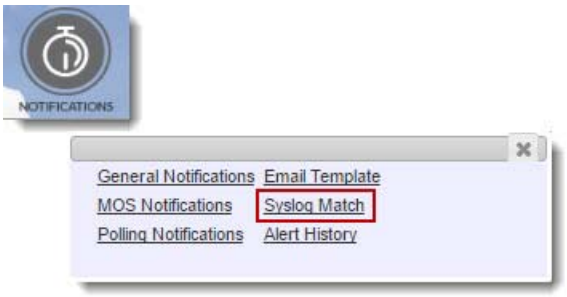
You can set up a regular expression to match any text which is logged by MOSwatch (the Syslog Parser). When a syslog entry matches the “value to match,” a script will be executed and an email notification will be sent to the specified email address(es).



Caution

This is a very powerful feature and takes up a lot of resources to run. It is recommended that you only use this feature for debugging purposes.

Figure 6-31 Syslog Match Notification Menu



To configure EdgeView to run a script and send a notification on a syslog match:

1. Select **Notifications** > **Syslog Match**. The Syslog Match Notifications page displays (Figure 6-32).

Figure 6-32 Syslog Match Notification

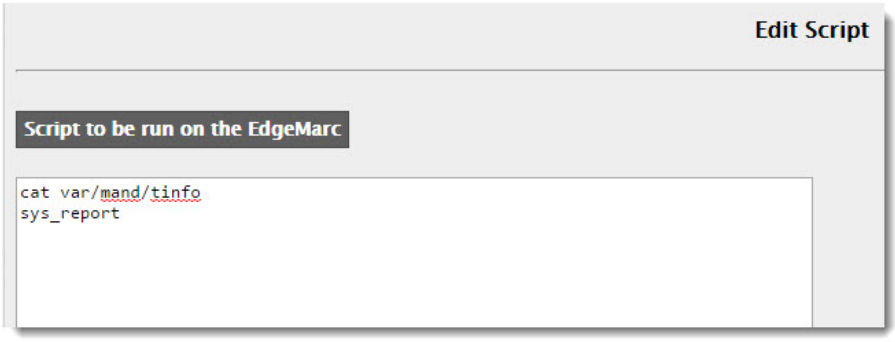
Send Email Notification on Syslog Match

(Note: Using this feature can affect system performance)

Value to Match	Send To	Add/Delete	Script	Edit Script
Bob	employee@mycompany.com	Delete	None	Edit Script
Julie	tech@mycompany.com	Delete	None	Edit Script
13\.6\..*	user@mycompany.com	Delete	None	Edit Script
14\.0\..*	user@mycompany.com	Delete	None	Edit Script
		Add		

2. In the Value to Match column, enter the regular expressions to match. For example, to see if a particular EdgeMarc running 14.0.x does a network restart, enter **14\.0\..***
3. In the Send to column, enter email notification address(es).
4. Click **Add**.
5. Click **Edit Script**. The Edit Script page displays (Figure 6-33).

Figure 6-33 Editing a Script



6. Type the script to be run when a syslog entry matches the Value to Match and click **Save**.

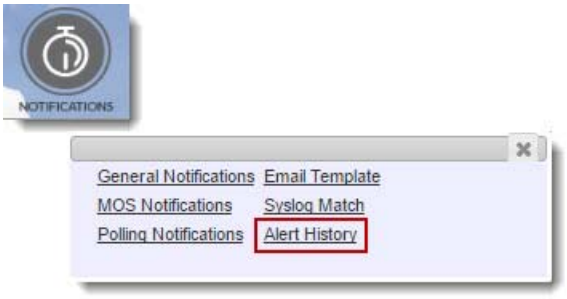
Tip

If you are not getting the results you expect, verify that you have properly checked or unchecked the **Run Script on the EdgeView (unchecked = Run Script on EdgeMarc)** checkbox.

Viewing Notification Alert History

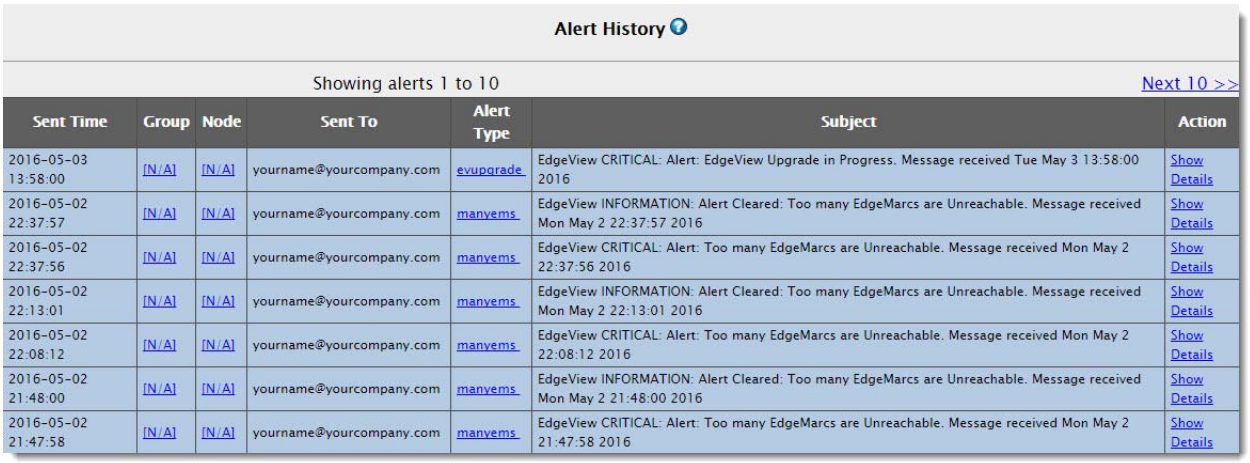
Select **Notifications** > **Alert History** to view a summary of all email notifications records which have been sent to the General Email Notifications list (Figure 6-34).

Figure 6-34 Alert History Notification Menu



From this page, you can click **Show Details** to view more details about each alert. Refer to Figure 6-36.

Figure 6-35 Viewing Alert History



Alert History

Showing alerts 1 to 10 Next 10 >>

Sent Time	Group	Node	Sent To	Alert Type	Subject	Action
2016-05-03 13:58:00	[N/A]	[N/A]	yourname@yourcompany.com	evupgrade	EdgeView CRITICAL: Alert: EdgeView Upgrade in Progress. Message received Tue May 3 13:58:00 2016	Show Details
2016-05-02 22:37:57	[N/A]	[N/A]	yourname@yourcompany.com	manyems	EdgeView INFORMATION: Alert Cleared: Too many EdgeMarcs are Unreachable. Message received Mon May 2 22:37:57 2016	Show Details
2016-05-02 22:37:56	[N/A]	[N/A]	yourname@yourcompany.com	manyems	EdgeView CRITICAL: Alert: Too many EdgeMarcs are Unreachable. Message received Mon May 2 22:37:56 2016	Show Details
2016-05-02 22:13:01	[N/A]	[N/A]	yourname@yourcompany.com	manyems	EdgeView INFORMATION: Alert Cleared: Too many EdgeMarcs are Unreachable. Message received Mon May 2 22:13:01 2016	Show Details
2016-05-02 22:08:12	[N/A]	[N/A]	yourname@yourcompany.com	manyems	EdgeView CRITICAL: Alert: Too many EdgeMarcs are Unreachable. Message received Mon May 2 22:08:12 2016	Show Details
2016-05-02 21:48:00	[N/A]	[N/A]	yourname@yourcompany.com	manyems	EdgeView INFORMATION: Alert Cleared: Too many EdgeMarcs are Unreachable. Message received Mon May 2 21:48:00 2016	Show Details
2016-05-02 21:47:58	[N/A]	[N/A]	yourname@yourcompany.com	manyems	EdgeView CRITICAL: Alert: Too many EdgeMarcs are Unreachable. Message received Mon May 2 21:47:58 2016	Show Details

Table 6-5 defines the information shown in the Alert History page.

Table 6-5 Alert History Definitions

Column	Description
Group Name	Group name for the alert.
Node Name	Node name for the alert.
Sent Time	Time the email notification was sent.
Alert Type	Type of event that caused the alert. Click on the entry in the Alert Type column to show only those type of alerts.
Email To	Email address(es) where the alert was sent.
Subject	Description of the event that caused the alert.
Body	Click **Show Details** to view the details about the alert and the email notification message. Refer to Figure 6-36.

Figure 6-36 Viewing Alert Details



7

Using Templates

EdgeMarc Configuration Templates

You can create and generate EdgeMarc Configuration Templates in EdgeView which can be re-used by EdgeMarcs globally at the Tenant or Group level and locally at the EdgeMarc Node level. An EdgeMarc Configuration Template is an XML file that describes all the configuration files for a given EdgeMarc or group of EdgeMarcs. An EdgeMarc Configuration template specifies the file names, variable names, types, constraints, and descriptions that can (but not necessarily must) be set for an EdgeMarc. The information and settings will vary depending on the EdgeMarc implementation.

You can access, manage, and modify the XML template file directly by editing the XML content, or by using the EdgeMarc Configuration Template Editor. Once you generate a template, you can use the Template Editor to modify values for variables via the GUI rather than typing them manually in the XML file via the console interface. You can also use the Template Editor to perform error-checking of all values that are entered, and to provide the user with a brief description of each value that can be edited as they hover over each variable to be edited. The Template Editor allows the administrator user to establish restrictions on what values may be modified, thus furthering the reliability and security of configuration file deployment.



Caution

Reuse of an existing template across EdgeMarcs or groups of EdgeMarcs that consist of different versions and models may render one or more of the EdgeMarcs inoperable. Confirm that each of the variables, values, raw files, and IP addresses used in a configuration template are appropriate for each affected EdgeMarc.

For additional details on managing EdgeMarc Templates, see the *Using EdgeView to Generate and Push EdgeMarc Templates* document in the Edgewater Network Knowledgebase: www.edgewaternetworks.com/kb

Generating a Template

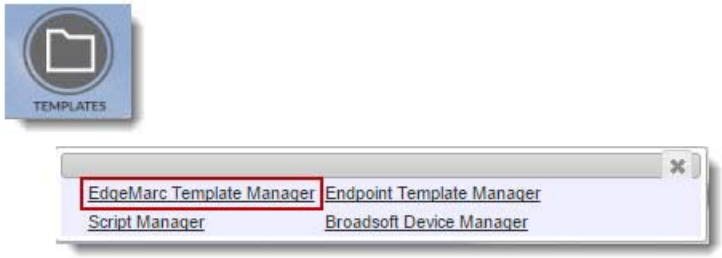


The first step in creating or modifying a template file is to generate a template from an existing EdgeMarc template and give it a name. When EdgeView initially generates a template, it remotely copies the master configuration file from the selected EdgeMarc and generates an XML-based template from that master configuration file. The Generator attempts to "guess" at the configuration file type. If the file type is a variable/value type, the Generator will also guess at the variable types when it generates the XML template. The variable types can be one of five types currently supported: string, integer, float, enumerated and regular expression.

To generate a configuration template:

1. Click the **Templates** icon in the icon bar and select **EdgeMarc Template Manager** from the menu (Figure 7-1).

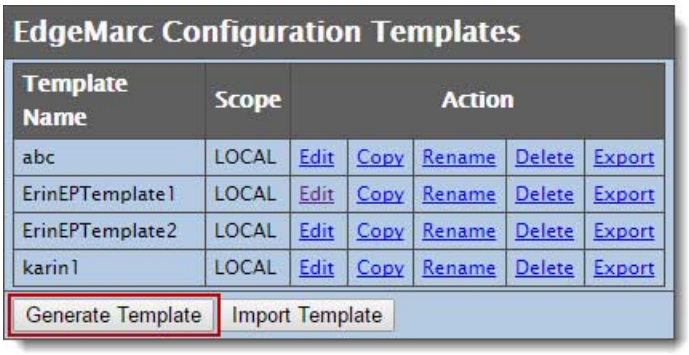
Figure 7-1 EdgeMarc Template Manager



The EdgeMarc Configuration Templates page displays.

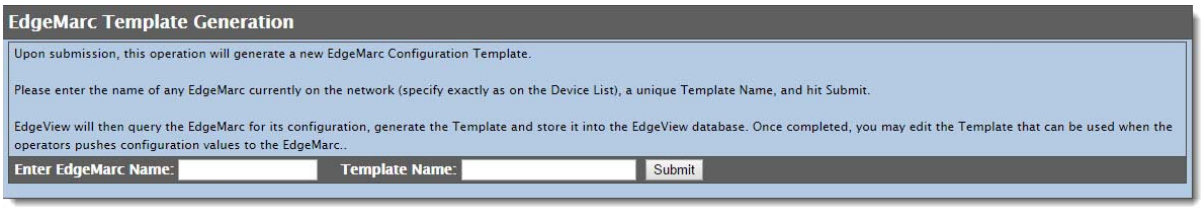
2. Click **Generate Template** (Figure 7-2).

Figure 7-2 EdgeMarc Configuration Templates - Generate



The EdgeMarc Template Generation page displays (Figure 7-3).

Figure 7-3 EdgeMarc Template Generation Page

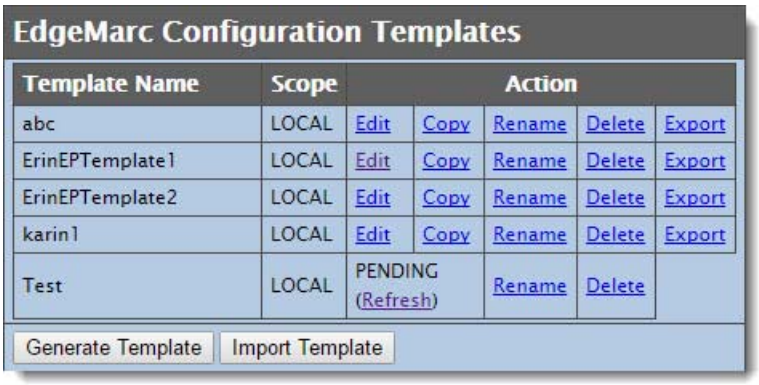


3. Follow the on-screen help to generate a new EdgeMarc configuration template:
   a. Enter the name of any EdgeMarc currently on the network (specify exactly as the device appears in the device tree).
   b. Enter a unique Template Name. The Template name must start with a non-space and then contain only letters, numbers, underscores or spaces.
   c. Click **Generate Template**.

   EdgeView will query the EdgeMarc for its configuration, generate the Template and store it in the EdgeView database. Once completed, you may edit the Template to be used by the network operator to push configuration values to the EdgeMarc.

   The EdgeMarc Configuration Templates page will show “PENDING” until the Template is generated (Figure 7-4).

Figure 7-4 New Template Pending



Once the template is successfully generated, it will be listed in the EdgeMarc Configuration Templates table.

If EdgeView is unable to generate the template, an error will display in the table. Verify that you typed the EdgeMarc name *exactly* as shown in the device tree and try again.

Editing Variables for an EdgeMarc Configuration Template

You can use the EdgeMarc Configuration Template Editor to edit an existing template or redeploy it across an individual EdgeMarc, group of EdgeMarcs, or globally to all EdgeMarcs managed by EdgeView.

To access the Template Editor:

1. Click the **Edit** link for the template in the EdgeMarc Configuration Templates table (Figure 7-5).

Figure 7-5 EdgeMarc Configuration Templates - Edit

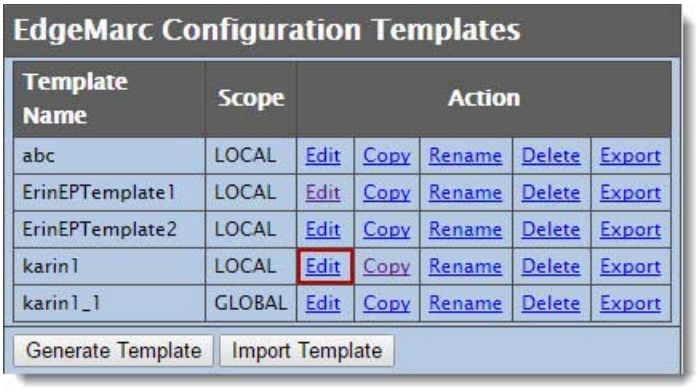
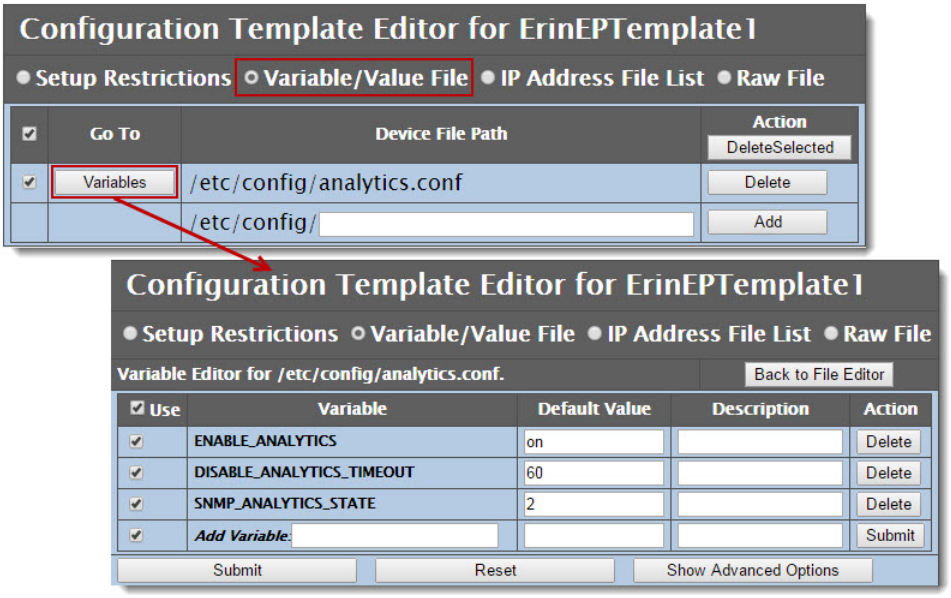


Figure 7-6 shows the Configuration Template Editor main screen.

2. To edit a variable, click the **Variables** button for a configuration file, change the value and/or description, and click **Submit**. When you click the **Variables** button, the current settings for each variable in the file are displayed, along with a brief description of the variable (if set). To see the available values for a variable, double-click in the **Default Value** box. You can also add a new variable if you know the proper syntax and the variable is supported by the EdgeMarc.

For more details on editing EdgeMarc Configuration Templates and variables, refer to the *Using EdgeView to Generate and Push EdgeMarc Templates* document in the Edgewater Network Knowledgebase: www.edgewaternetworks.com/kb

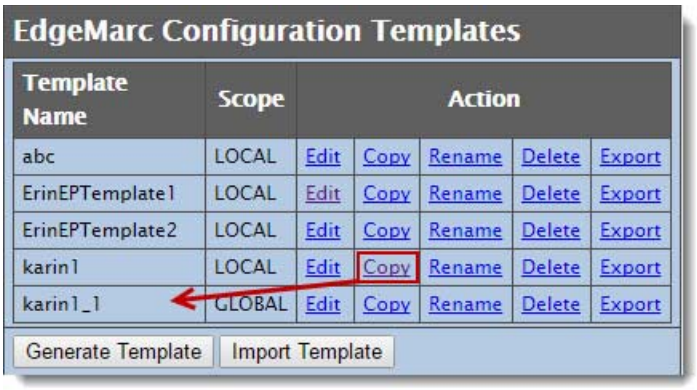
Figure 7-6 Editing EdgeMarc Configuration Template Variables



Making Copies of a Template

You can make duplicate copies of a generated template in the EdgeMarc Configuration Templates table by clicking the **Copy** link for the template (Figure 7-7). A new entry will appear in the table with a _<*n*> appended to the Template name. You can make multiple copies of the same template. The number appended to the Template Name increments for each copy of the Template (for example, _2, _3, _4 and so on).

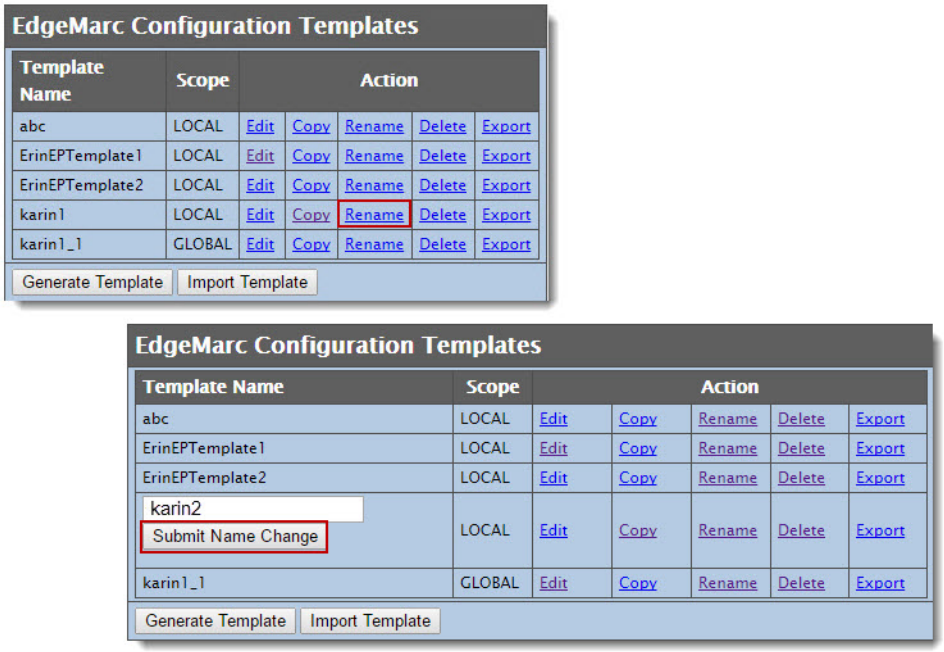
Figure 7-7 EdgeMarc Configuration Templates - Copy



Renaming a Template

1. Click the **Rename** link for an EdgeMarc Template in the EdgeMarc Template table.

Figure 7-8 EdgeMarc Configuration Templates - Rename



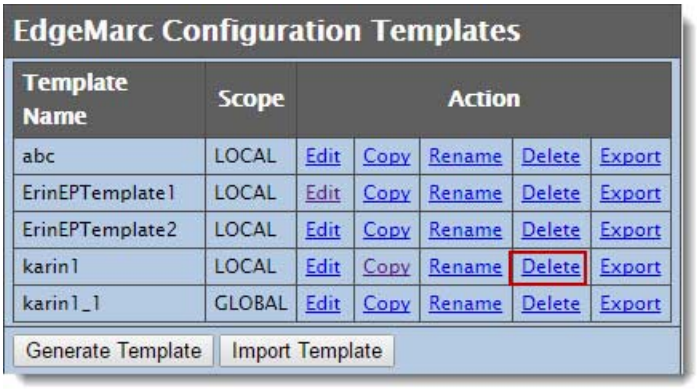
2. Type a new Template Name.
3. Click **Submit Name Change**.

The template will be renamed in the Template table.

Deleting a Template

1. Click the **Delete** link for an EdgeMarc Template in the EdgeMarc Template table.

Figure 7-9 EdgeMarc Configuration Templates - Delete



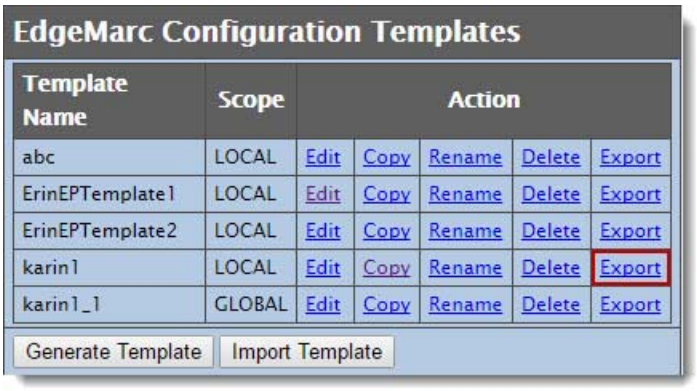
2. A dialog box asks if you are sure you want to delete the file. Click **OK** to confirm deletion.

The template will be removed from the Template table.

Exporting a Template to an XML-based File

1. Click the **Export** link for an EdgeMarc Template in the EdgeMarc Template table.

Figure 7-10 EdgeMarc Configuration Templates - Export



2. Select a location to download the XML-based file to your local drive.
3. Save the file.

Once you have saved the file to your local drive, you can open it in a text editor, edit the file, and save your changes. The file can then be imported back into the EdgeView Configuration Template Manager.

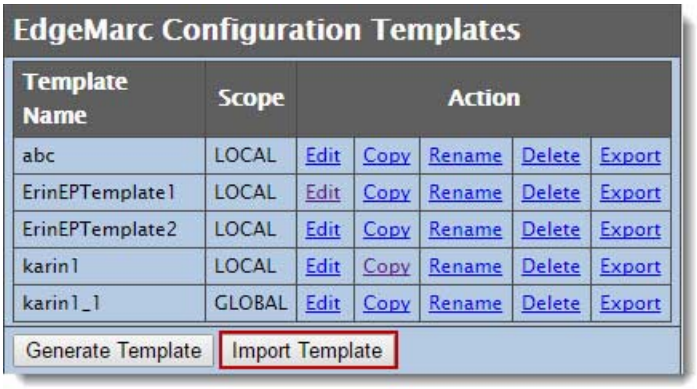
Importing an XML-based Template File

If you have saved an EdgeMarc XML-based template file on your local computer, you can upload a copy to the EdgeView database for modification. The template will show up in the template list and can then be edited in EdgeView. The XML file can be a file that was generated from another EdgeMarc via the Export function described previously.

To import a Template file:

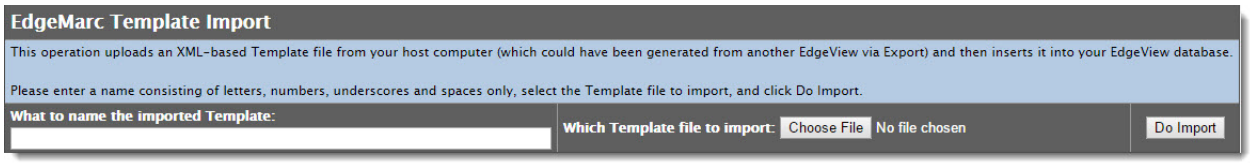
1. In the EdgeMarc Configuration Templates page, click **Import Template** (Figure 7-11).

Figure 7-11 EdgeMarc Configuration Templates



The EdgeMarc Import Template page screen displays (Figure 7-12).

Figure 7-12 EdgeMarc Template Import



2. Follow the on-screen instructions to import the file:
   a. Assign a unique name to the Template. The name must consist only of letters, numbers, underscores, and spaces.
   b. Browse to the template file you want to import from your local drive.
   c. Click **Do Import**.

Once the import function completes, the template is added to the EdgeMarc Configuration Templates page.

Updating the EdgeMarc Configuration on a Global, Group, or Individual Node Level

You can do a “configuration push” to update an EdgeMarc configuration. A configuration push may be used to update a single value/variable pair, or deploy a configuration template containing many value/variable pairs.

For details on how to perform an EdgeMarc configuration push, refer to the *Using EdgeView to Generate and Push EdgeMarc Templates* document in the Edgewater Networks Knowledgebase:
www.edgewaternetworks.com/kb

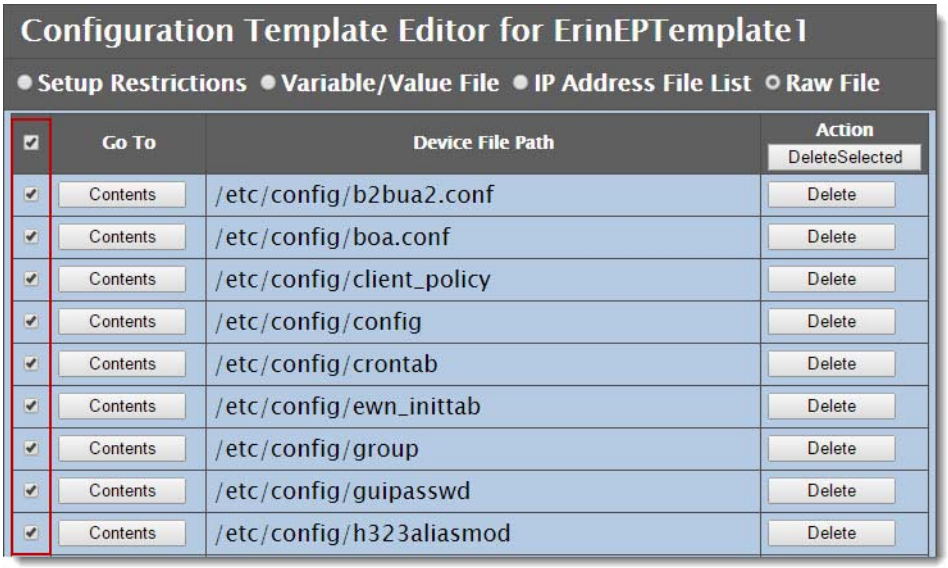
This document also describes how to use the configuration push feature to schedule an update to an EdgeMarc configuration file or set of EdgeMarc configuration files. The update can take effect at an individual node, group or global level.

Configuration Template Editor

It is now easier to modify templates and template values when editing EdgeMarc templates in **Templates** > **EdgeMarc Template Manager**. Now it is easier to delete configuration files out of your template that you don’t need to change. Checkboxes allow you to select and mass-delete configuration files in a template using the Delete Selected button. This feature is available on the following pages:

- Variable/Value File
- IP Address File List
- Raw File (Figure 7-13)

Figure 7-13 EdgeMarc Template Manager - Raw File Page

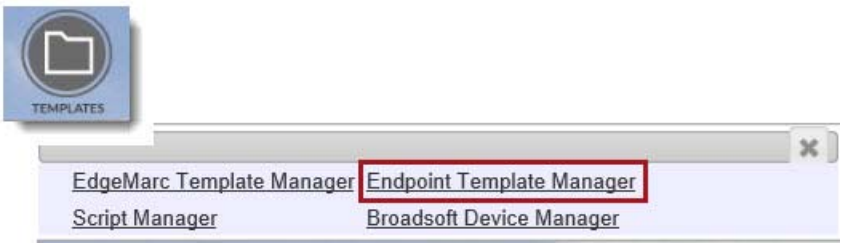


Managing Endpoint Templates

To manage an endpoint template:

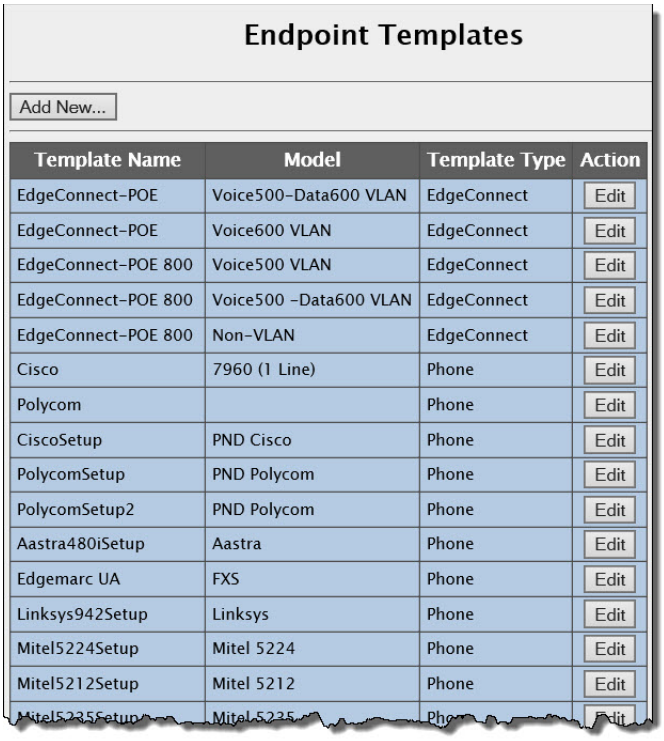
1. Click the **Templates** icon in the icon bar and select **Endpoint Template Manager** from the menu (Figure 7-14).

Figure 7-14 EdgeMarc Template Manager



The Endpoint Template page is displayed (Figure 7-15).

Figure 7-15 Endpoint Template Configuration Page



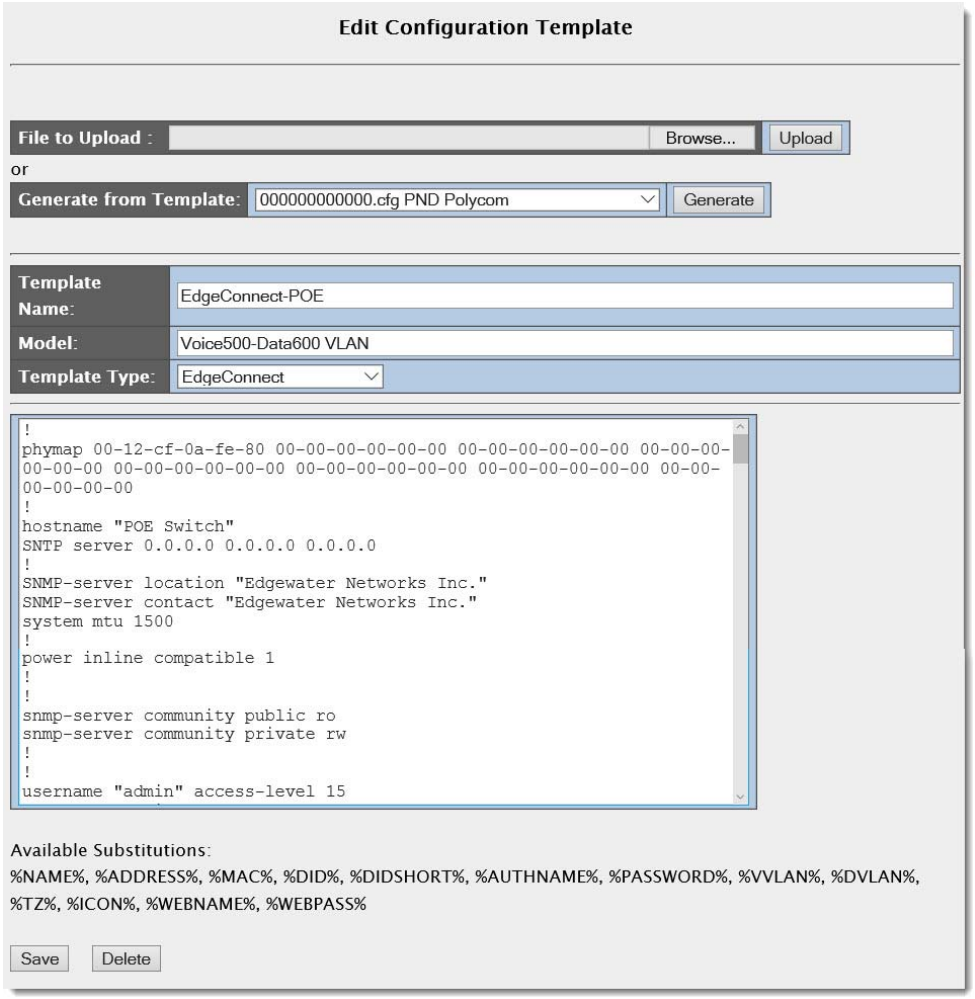
Endpoint Templates

Add New...

Template Name	Model	Template Type	Action
EdgeConnect-POE	Voice500-Data600 VLAN	EdgeConnect	Edit
EdgeConnect-POE	Voice600 VLAN	EdgeConnect	Edit
EdgeConnect-POE 800	Voice500 VLAN	EdgeConnect	Edit
EdgeConnect-POE 800	Voice500 -Data600 VLAN	EdgeConnect	Edit
EdgeConnect-POE 800	Non-VLAN	EdgeConnect	Edit
Cisco	7960 (1 Line)	Phone	Edit
Polycom		Phone	Edit
CiscoSetup	PND Cisco	Phone	Edit
PolycomSetup	PND Polycom	Phone	Edit
PolycomSetup2	PND Polycom	Phone	Edit
Aastra480iSetup	Aastra	Phone	Edit
Edgemarc UA	FXS	Phone	Edit
Linksys942Setup	Linksys	Phone	Edit
Mitel5224Setup	Mitel 5224	Phone	Edit
Mitel5212Setup	Mitel 5212	Phone	Edit

2. Add or edit a template by clicking **Add New** at the top of the page or by clicking **Edit** next to an existing template. The Add or Edit Configuration Template page is displayed (Figure 7-16)

Figure 7-16 Editing a Configuration Template Page



3. Edit the current template by changing the information in the Template Name and Model fields. Change the type of template by choosing a template from the **Template Type** drop-down menu.
4. Upload or generate a new template:
   - Click **Browse** to find a template file on your system and click **Upload**.

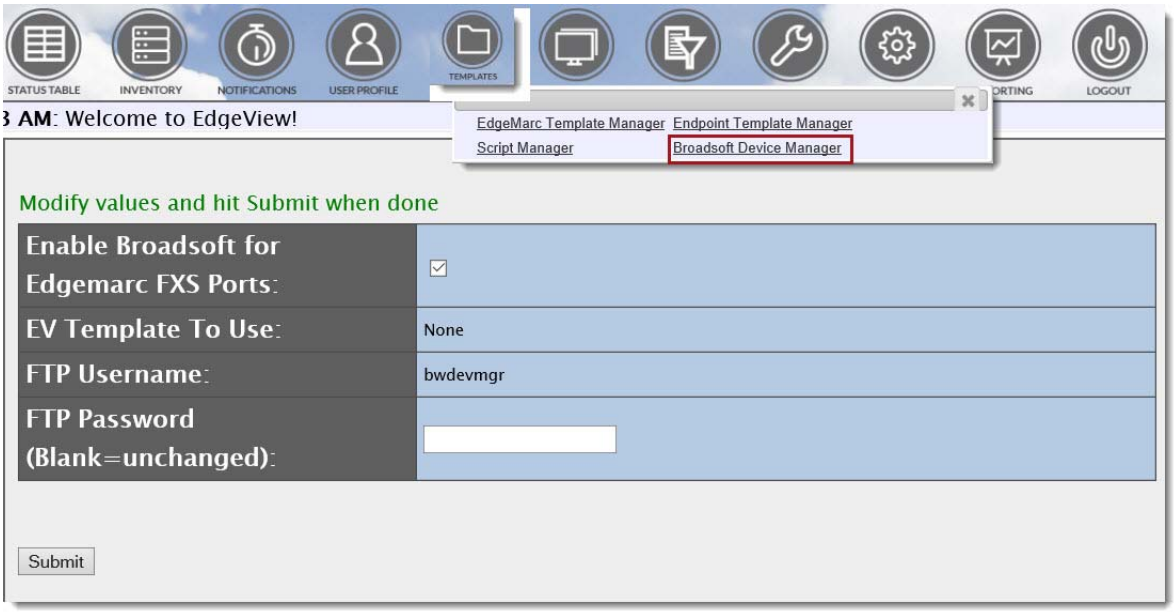
     Or
   - Choose a template file from the **Generate from Template** drop-down menu and click **Generate**.

   The updated information will be displayed in the white box.
5. Click **Save**.

Configuring Broadsoft Device Manager

1. Choose **Templates** > **Broadsoft Device Manager** (Figure 7-17).

Figure 7-17 Broadsoft Device Manager Page



2. Select the Enable Broadsoft for EdgeMarc FXS Ports checkbox.
3. (Optional) Enter an FTP password in the field provided. If the field is left blank, your default password is used.
4. Click **Submit**. The system alerts you if the changes were saved successfully.

Configuring Script Manager

Refer to Running an EdgeMarc Device Script in Chapter 8, *MOS Analysis and Troubleshooting*.

8

MOS Analysis and Troubleshooting

EdgeView retrieves and stores a tremendous amount of call quality information that is calculated locally in each EdgeMarc node. EdgeView polls each node at 5-minute intervals and retrieves call quality statistics for the last 50 calls processed by a specific node. The call quality information is collected, aggregated, and presented in several different ways.

Collecting and Analyzing MOS Statistics

To help you analyze and diagnose VoIP problems on the network, EdgeView provides mean opinion score (MOS) statistics for EdgeMarcs, groups, and nodes. EdgeView can also analyze the VoIP signaling processes running on an EdgeMarc and display flow results in an on-demand signaling ladder. You can enter a date and time range for MOS analysis and signaling captures to help you narrow the results to the estimated time when an issue occurred for root cause analysis and correlation. Other customizations are also available as described in this chapter.

Troubleshooting and Diagnostics

To quickly display diagnostics for an EdgeMarc, select the EdgeMarc from the device tree and then select the **Analysis > MOS Collection Troubleshooting** option in the menu bar. EdgeView will check connections, syslog data and MOSwatch processes on the EdgeMarc, check the EdgeMarc configuration against the records in the EdgeView database, and display a report with tips to help you diagnose problems. Additionally, EdgeView can perform active line tests and bulk line tests which enable automated connectivity and call quality testing from an EdgeMarc to any number of destination telephone numbers.

For further troubleshooting and debugging, EdgeView provides an easy way to run EdgeMarc device scripts. You can specify various logging levels for each script.

This chapter covers the following main topics:

- Viewing the Syslog
- Call Quality Measurement Using EdgeView MOS Analysis
- Signaling Capture and Analysis
- EdgeView Troubleshooting Tools
- Running a Shell Script on an EdgeMarc

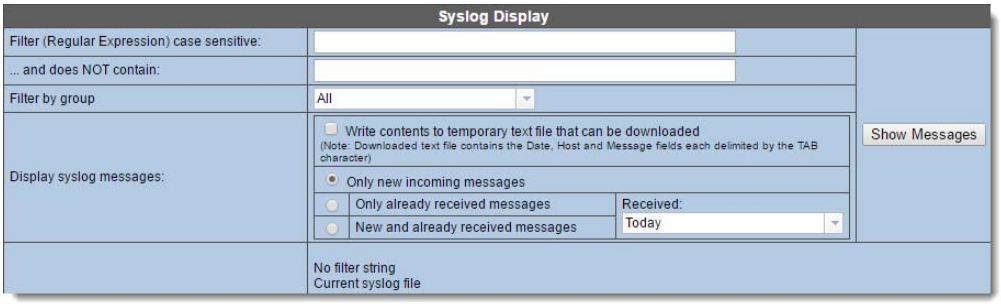
Viewing the Syslog

The EdgeView Syslog contains useful information for system management, analysis, and security auditing and is a good place to start when troubleshooting network issues. To access the EdgeView Syslog, click the **System Disp** icon in the EdgeView icon bar.



You can filter messages in the Syslog by EdgeMarc, group, date, and by the message receipt status (incoming, new, received). You can also save the Syslog to a temporary file which can be downloaded to your local drive.

Figure 8-1 EdgeView Syslog



Viewing Syslog Messages

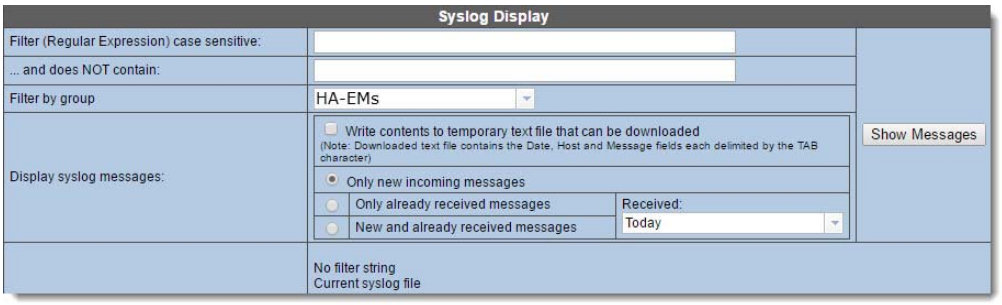
To view syslog messages on the Syslog Display screen, click **Show Messages**. The messages will begin displaying in the Syslog message box.

Syslog Display for High Availability

The EdgeMarc Syslog Display page device table now shows events from both EdgeMarc devices in an HA pair. Configuration management is carried out via the primary EdgeMarc with the sync feature configured.

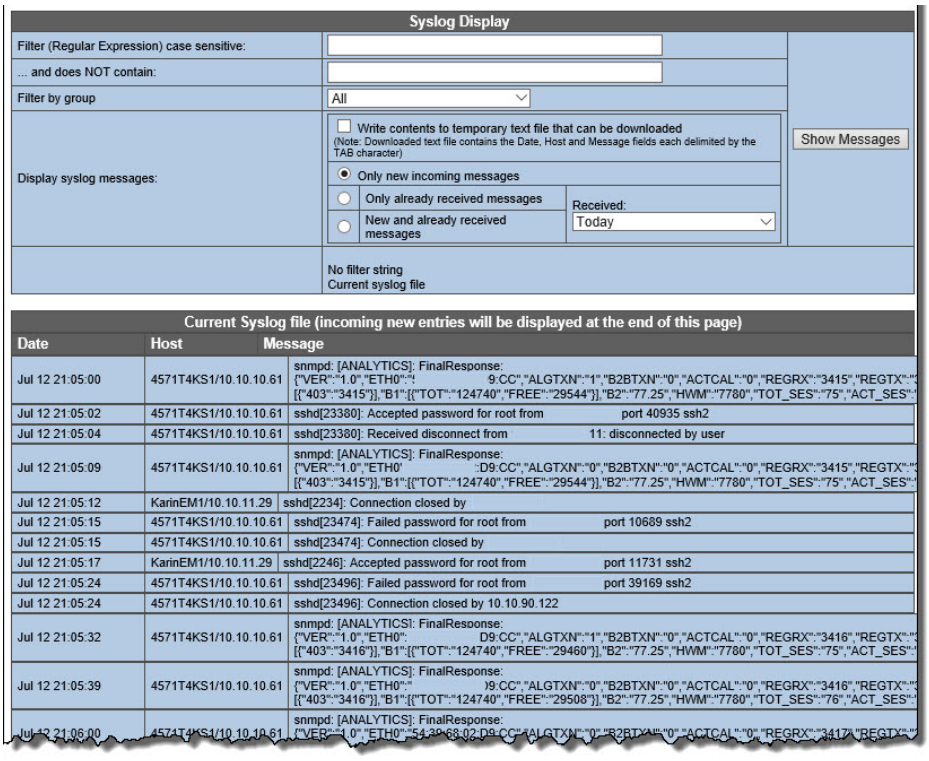
1. Click **Syslog Disp**.
2. Select the **Default** group from the **Filter by group** drop-down menu.
3. Select the primary node in the HA pair from the **Filter by EdgeMarc** drop-down menu (Figure 9).

Figure 9 Syslog Display for High Availability



4. Click **Show Messages**. Any syslog messages from the secondary node are now displayed (Figure 8-1).

Figure 8-1 Secondary Node Syslog Messages



Configuring Syslog Settings

You can filter messages in the Syslog according to a defined character string, by a group or by an EdgeMarc. You can also choose to display Syslog messages by the receipt status (incoming, new, received) or to display previously logged messages for a selected number of days. The following table provides instructions for configuring settings for how you want to display messages in the Syslog.

Table 8-1 Configuring Syslog Settings

If you want to...	Then do this...
Filter on a sequence of characters	Enter a regular expression (case sensitive) for the filter. To further refine the filter, enter characters that you do not want the filter to pick up.
Write contents of the Syslog to a temporary file that can be downloaded.	Select the checkbox. The downloaded text file contains the date, host, and message fields delimited by the TAB character.
Display only new incoming Syslog messages	Select the checkbox.
Display only already received messages	Select the checkbox and then choose the number of days for which you want to display data from the **Received** drop-down menu.
Display new and already received messages	Select the checkbox and then choose the number of days for which you want to display data from the **Received** drop-down menu.
Show messages logged in the Syslog	Click the **Show Messages** button.
Stop Syslog updates and download the messages to a file	Click the link and refer to Downloading the Syslog to a Local File.

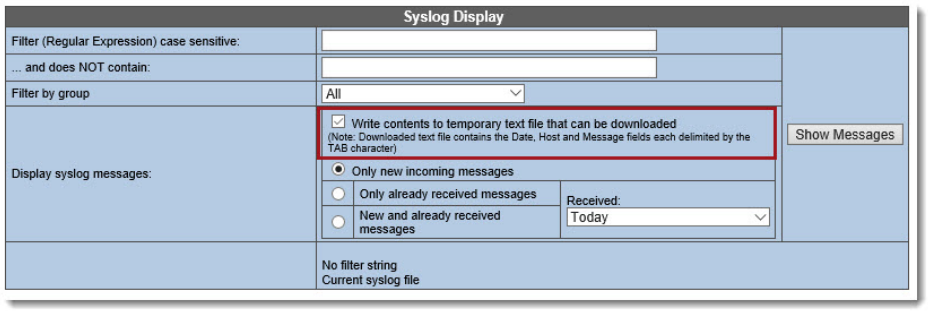
Downloading the Syslog to a Local File

EdgeView can simultaneously write out the contents captured from the Syslog to both the EdgeView GUI (Syslog Display page) and a temporary file saved in EdgeView (with up to a 2 second delay for content captured continuously). When this feature is enabled, a link will appear above the messages displayed on the Syslog Display page, allowing you to view or save the temporary log file. The temporary file contains the date, the EdgeMarc host information, and the message. Each of these fields are TAB-delimited and each entry has a new line at the end.

To create and download a temporary Syslog file in EdgeView:

1. Click the **Syslog Disp**. icon.
2. In the Syslog Display screen, check the box that says **Write contents to temporary file that can be downloaded** (Figure 8-2).

Figure 8-2 Creating a Temporary Syslog File



3. Select an option from the Display syslog messages. If you choose to view received messages, choose the number of days to go back from the **Received** drop-down menu.
4. Click **Show Messages**. The Syslog messages will display in the Syslog message box.
5. When you are ready to download the file, click **Download File** or **Stop Updates and Download to File**. Do one of the following:
   - Click **Open** to view the Syslog in a text file.
   - Click **Save** to download the file to your local drive as a .log file.
   - Click **Cancel** to return to the Syslog Display page.

Viewing Average Mean Opinion Score (MOS) Data

The audio quality of calls is represented by a “MOS” (Mean Opinion Score) value between 1.0 (worst) and 5.0 (best). MOS scores are calculated by measuring several call quality statistics for the duration of the call and then comparing them against a calibration file. Depending on the codec, a MOS value of 4.0 is generally considered good and is the expected value for a “toll quality” PSTN call. Any value over 3.0 is generally considered average or OK.

Within the EdgeMarc node, a MOS value is assigned to every call and for each direction of the call (WAN to LAN and LAN to WAN). This is useful to quickly identify networking problems that affect call quality as either “LAN” or “WAN” side issues for further troubleshooting. The MOS value is calculated continuously in the EdgeMarc nodes. The average MOS score of the last 50 calls measured in both directions for any node can be seen by selecting the EdgeMarc from the device tree and viewing the EdgeMarc Main Status page.

Viewing MOS Data for the Last 10 Calls

To view MOS data for the last 10 calls:

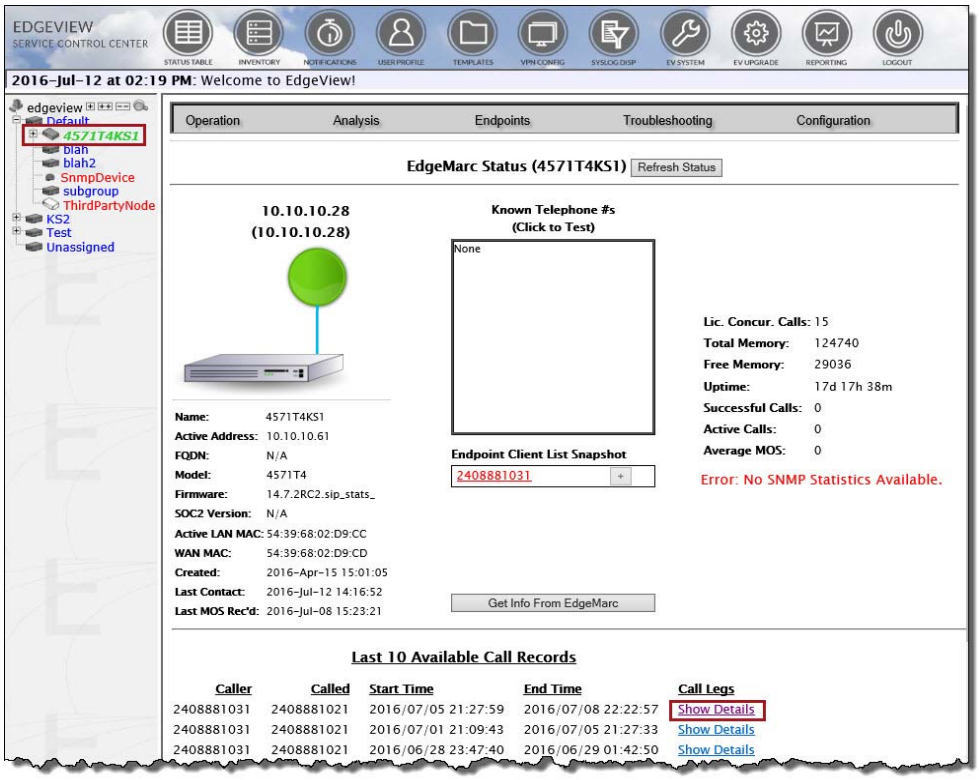
1. Select the EdgeMarc from the device tree
2. Click the **Show Details** link from the Last 10 Available Call Records table at the bottom of the EdgeMarc Status page (Figure 8-3). Refer to Viewing MOS Statistics for Call Legs.



Note

The ALG must be running on the EdgeMarc in order for EdgeView to perform a MOS calculation.

Figure 8-3 Viewing MOS Data for the Last 10 Calls



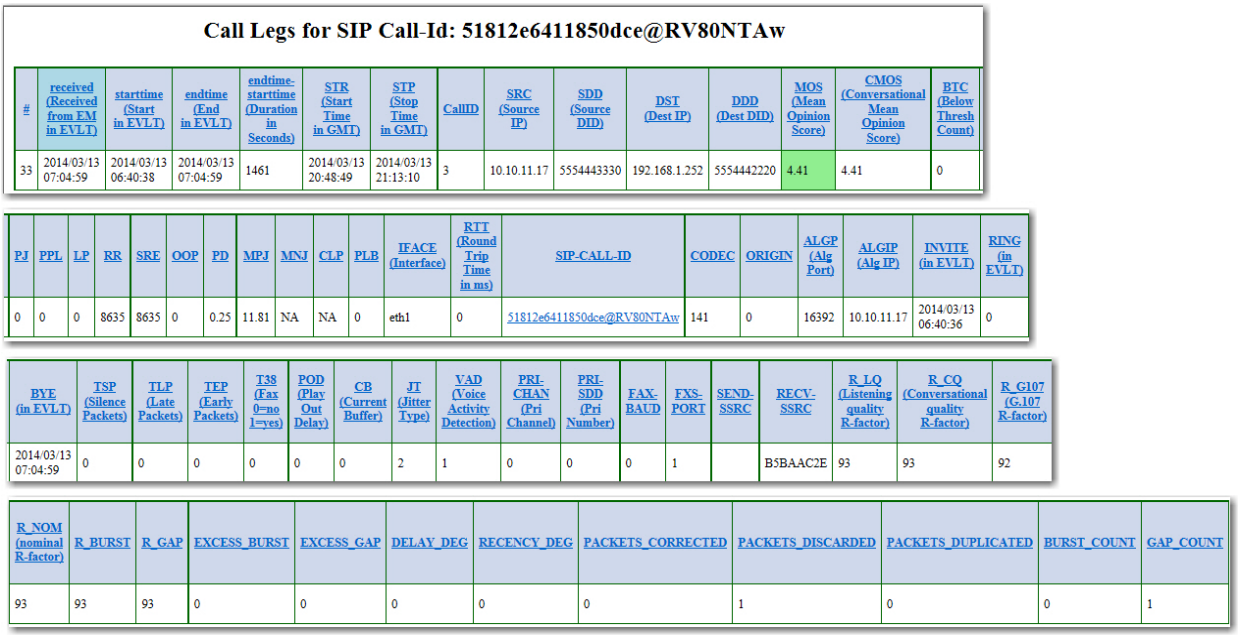
Viewing MOS Statistics for Call Legs

1. Select the EdgeMarc from the device tree
2. Click the **Show Details** link from the Last 10 Available Call Records table at the bottom of the EdgeMarc Status page (Figure 8-3). Refer to Viewing MOS Statistics for Call Legs.

   The results are displayed in a table with many columns and statistics. To see them all, scroll the window to the right. The table has sortable

columns and fields. Some columns have links which point you to the Edgewater Knowledgebase for more information. Figure 8-4 shows call leg statistics. Table 8-2 defines the data shown in the Detailed Call Statistics report.

Figure 8-4 Call Legs



Call Legs for SIP Call-Id: 51812e6411850dce@RV80NTAw

#	received (Received from EM in EVLT)	starttime (Start in EVLT)	endtime (End in EVLT)	endtime-starttime (Duration in Seconds)	STR (Start Time in GMT)	STP (Stop Time in GMT)	CallID	SRC (Source IP)	SDD (Source DID)	DST (Dest IP)	DDD (Dest DID)	MOS (Mean Opinion Score)	CMOS (Conversational Mean Opinion Score)	BTC (Below Thresh Count)
33	2014/03/13 07:04:59	2014/03/13 06:40:38	2014/03/13 07:04:59	1461	2014/03/13 20:48:49	2014/03/13 21:13:10	3	10.10.11.17	5554443330	192.168.1.252	5554442220	4.41	4.41	0

PJ	PPL	LP	RR	SRE	OOP	PD	MPJ	MNJ	CLP	PLB	IFACE (Interface)	RTT (Round Trip Time in ms)	SIP-CALL-ID	CODEC	ORIGIN	ALGP (Alg Port)	ALGIP (Alg IP)	INVITE (in EVLT)	RING (in EVLT)
0	0	0	8635	8635	0	0.25	11.81	NA	NA	0	eth1	0	51812e6411850dce@RV80NTAw	141	0	16392	10.10.11.17	2014/03/13 06:40:36	0

BYE (in EVLT)	TSP (Silence Packets)	TLP (Late Packets)	TEP (Early Packets)	T38 (Fax 0=no 1=yes)	POD (Play Out Delay)	CB (Current Buffer)	JT (Jitter Type)	VAD (Voice Activity Detection)	PRI-CHAN (Pri Channel)	PRI-SDD (Pri Number)	FAX-BAUD	FXS-PORT	SEND-SSRC	RECV-SSRC	R_LQ (Listening quality R-factor)	R_CQ (Conversational quality R-factor)	R_G107 (G.107 R-factor)
2014/03/13 07:04:59	0	0	0	0	0	0	2	1	0	0	0	1		B5BAAC2E	93	93	92

R_NOM (nominal R-factor)	R_BURST	R_GAP	EXCESS_BURST	EXCESS_GAP	DELAY_DEG	RECENCY_DEG	PACKETS_CORRECTED	PACKETS_DISCARDED	PACKETS_DUPLICATED	BURST_COUNT	GAP_COUNT
93	93	93	0	0	0	0	0	1	0	0	1

Table 8-2 Call Analysis Definitions

Heading	Description
Received	Date and time the call was received by EdgeView (in EdgeView local time). This is the time when the call ended and the EdgeMarc sends out the MOS scores.
Start time	Date and time the call started in EdgeView local time
End time	Data and time the call ended in EdgeView local time.
End time-start time	Duration of the call (in seconds)
STR	Start time of the call in GMT (on the EdgeMarc)
STP	Stop time of the call in GMT (on the EdgeMarc)
Call ID	Caller ID
SRC	Source IP address
SDD	Source DID phone number
DST	Destination IP address
DDD	Destination DID phone number
MOS	Average Mean Opinion Score over the duration of the call (1 to 5)
CMOS	Conversational Mean Opinion Score

Table 8-2 Call Analysis Definitions (continued)

Heading	Description
BTC	Count of below threshold messages issued for the call
PJ	Proportion of degradation due to jitter (%)
PPL	Proportion of degradation due to MOS based packet loss (%)
LP	Number of lost packets detected for the call
RR	Total number of RTP packets received
SRE	Sum of received and expected packets: total expected packets
OOP	Number of out-of-sequence packets
PD	Mean absolute 1-t packet delay variation milliseconds)
MPJ	Maximum positive jitter (milliseconds)
MNJ	Minimum negative jitter (milliseconds)
CLP	Maximum number of consecutive lost packets
PLB	Average packet loss burst length
IFACE	Port interface
RTT	Round trip time (in milliseconds)
SIP-CALL-ID	The unique ID generated by the originating IP Device to globally identify the call flow. This ID will be used to search for corresponding logs in other device on the network that might have played a role in this call.
CODEC	Indicates the Codec used during the call. Commonly used codecs include: 0 = G711 - Mulaw 8 = G711 - Alaw 9 = G722 18 = G729
ORIGIN	Indicates if this is an incoming or outgoing call. A “1” indicates that the RTP stream is flowing in the same direction as the invite, and a 0 if it is not.
ALGP	ALG Port
ALGIP	IP address for the ALG
INVITE	The time of the INVITE request (in EdgeView Local Time)
RING	The time of the RING request (in EdgeView Local Time)
BYE	The time of the BYE request (in EdgeView Local Time)
TSP	Silence Packets
TLP	Late Packets
TEP	Early Packets
T38	0 = no; 1 = yes

Table 8-2 Call Analysis Definitions (continued)

Heading	Description
POD	Play out delay
CB	Current Buffer
JT	Jitter Type
VAD	Voice Activity Detection
PRI CHAN	PRI Channel
PRI SDD	PRI Number
FAX-BAUD	
FXS-PORT	
SEND-SSRC	Send Synchronization Source ID
RECV-SSRC	Receive Synchronization Source ID
R_LQ	Listening quality R-Factor
R_CQ	Conversational quality estimate R-Factor
R_G107	G.107 R-factor
R_NOM	Nominal R-factor
R_BURST	R-Factor for burst
R_GAP	R-Factor for gap
EXCESS BURST	Determines how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the Excess Burst size exceeds the rate limit with a probability that increases as the burst size increases.
EXCESS GAP	Determines how large traffic gaps can be before all traffic exceeds the rate limit. Traffic that falls between the normal gap size and the Excess Gap size exceeds the rate limit with a probability that increases as the gap size increases.
DELAY DEG	Delay degradation.
RECENCY DEG	Recency degradation. Using an example of a ten-minute VoIP call, there are two possible scenarios. 1. There can be significant distortion at the beginning of the call, but the rest of the call is fine. 2. There can be nine minutes of perfect quality, and, in the last minute, there can be exactly the same distortion as in the first scenario. Experiments have shown that the perceived quality score will be significantly less in the second scenario than in the first scenario. The RECENCY DEG count captures these kinds of effects.
PACKETS CORRECTED	Number of packets corrected.

Table 8-2 Call Analysis Definitions (continued)

Heading	Description
PACKETS DUPLICATED	Number of packets duplicated.
BURST COUNT	Number of transport packet loss/discard burst occurrences over the interval.
GAP COUNT	Number of transport packet loss/discard gap occurrences over the interval.

Understanding MOS Scores

For each call in the Detailed Call Statistics report, there will be:

- No MOS score if the call is between 2 stations behind the EdgeMarc LAN (if the Media is not anchored by the Central SBC).
- One MOS score if it is an outgoing call from an FXS or FXO port to the PSTN.
- Two MOS scores—one from the WAN and one from the LAN.
- Three MOS scores (if the IP phones support SIP publishing and Voice Quality Report Capturing is enabled with EdgeView as the collector). You can enable Voice Quality Report Capturing on the **EV System > Voice Quality Reports** tab. Refer to Capturing Phone MOS Scores in *Managing EdgeView System Settings*.

You can have more MOS scores if the calls involve two EdgeMarcs. In the Last 10 Calls list on the EdgeMarc Status page, the MOS record for both EdgeMarcs involved in the call will be brought in, even if only one EdgeMarc is selected. Therefore, in this case, you can have up to six MOS scores.

Overview of Important MOS Statistics

MOS Statistic	Description
Packet Loss (LP)	EdgeMarc quality analysis uses the RTP sequence numbers to determine the expected and actual received packets. For example, if an EdgeMarc receives the following sequence 1-2-3-4-7-8-9-10, the expected number of packets is 10 and the actual packets received is 8 with 2 lost packets (20%).
Maximum number of consecutive lost packets (CLP)	This is the worst-case consecutive packet loss experienced during the call.
Average packet loss burst length (PLB)	Tis the mean length of all the packet-loss bursts during the call.
Number of out of sequence packets (OOP)	This is a count of the packets received that are out of sequence.
Jitter	Jitter is determined from the time stamp in the RTP stream and the codec in use. If the codec uses 20ms intervals, the EdgeView statistics monitoring will expect a packet every 20ms.
Negative Jitter (MPJ)	This indicates that a packet arrived earlier than expected. The timing is always derived from the last RTP packet received.
Positive Jitter (PPJ)	This indicates a packet arrived later than expected. The timing is always derived from the last RTP packet received.
Proportion of degradation to MOS based on packet loss (PPL)	This percentage indicates which element has had the most impact on the MOS degradation.
Proportion of degradation to MOS based on Jitter (PJ)	This percentage indicates which element has had the most impact on the MOS degradation.
Degradation due to network conditions	This is an estimate of what network conditions are occurring based on the packet loss and jitter profiles. For example, a large burst of packet loss could be associated with a router's buffer overflowing due to link congestion or failure. Jitter could be related to a LAN switch becoming congested.

Additional information regarding call quality statistics can be found online using Edgewater Networks Knowledgebase:
www.edgewaternetworks.com/kb

Call Quality Measurement Using EdgeView MOS Analysis

EdgeView includes many options for analyzing call statistics. The statistics for call analysis can come from a snapshot of the current measurements in the EdgeMarc in-memory log or from a log file that has been saved on an external system. Snapshots are useful for real-time troubleshooting and provide a historical record of call quality performance over time for further analysis.

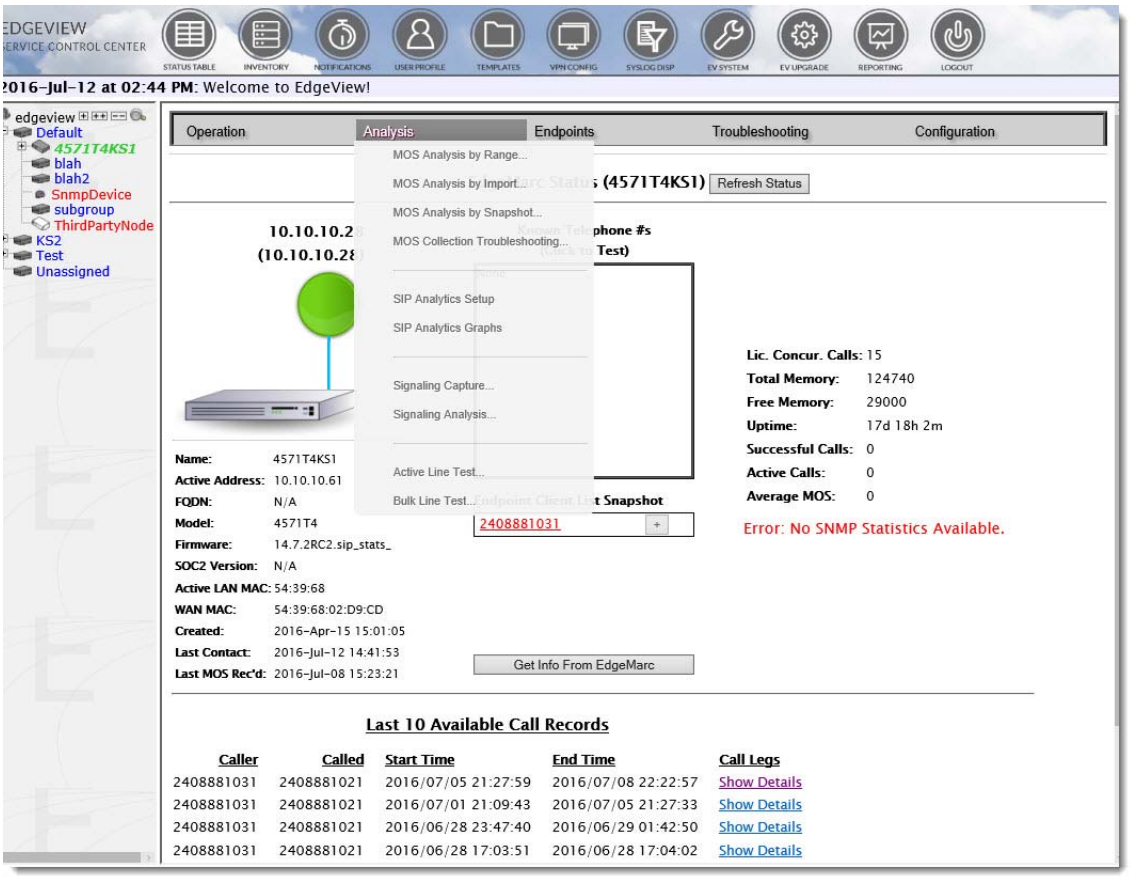
EdgeView call analysis allows you to:

- Analyze call statistics by a date/time range
- Import a MOS analysis file or syslog file to EdgeView for analysis
- Analyze the latest MOS data from the EdgeMarc rather than from the saved data
- Troubleshoot why MOS data has not been received by EdgeView
- Perform and analyze signal captures
- Perform Active Line Tests to verify that a call completes
- Perform Bulk Line Tests to analyze call quality

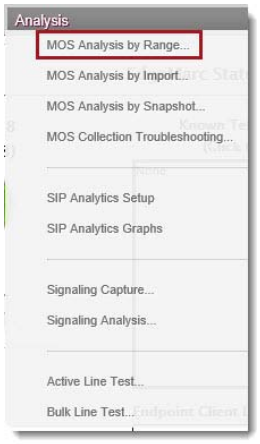
Accessing Call Analysis Options

To access call analysis options in EdgeView, select an EdgeMarc from the device tree and select **Analysis** from the menu bar (Figure 8-5).

Figure 8-5 Accessing Call Analysis Options

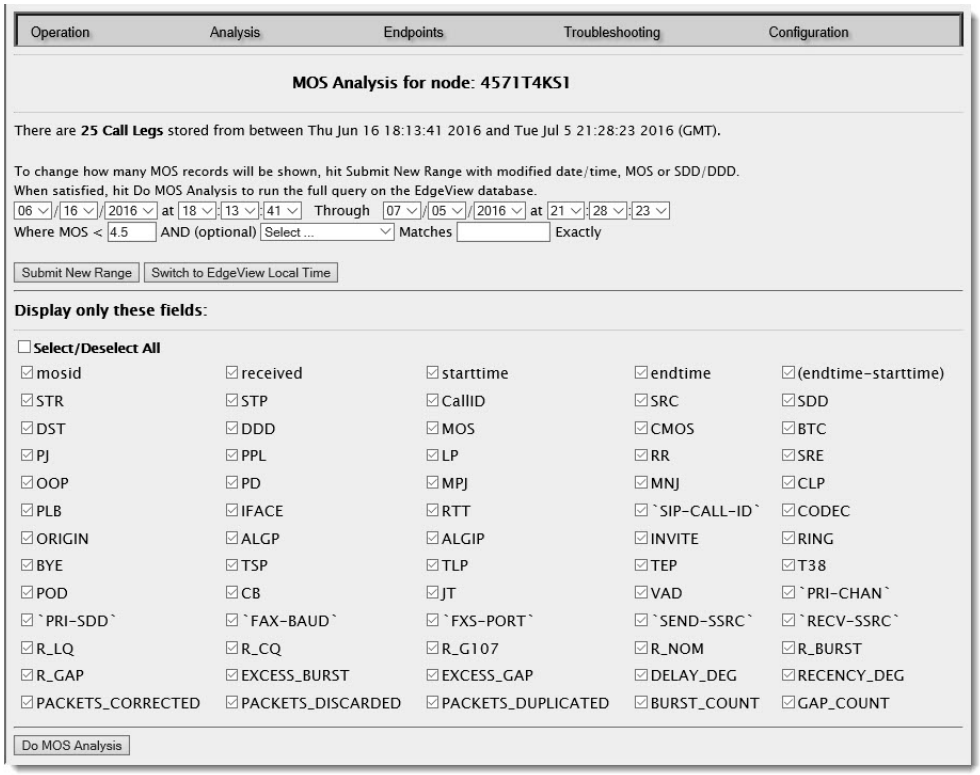


Each MOS analysis option generates a table with sortable columns and fields. Some columns have links which point you to the Edgewater Networks Knowledgebase for more information. Performing a MOS Analysis By Date/Time Range.



Select the **Analysis > MOS Analysis by Range** option to run a MOS analysis on data previously stored in EdgeView with filters for date/time, source, or destination DIDs. The MOS Analysis for Node page displays (Figure 8-6). Since there may be hundreds to thousands of call legs to analyze, this option allows you to specify a date and time range to filter the records that are displayed in the results. If the range you specify will return thousands of entries, EdgeView will display a pop-up warning.

Figure 8-6 MOS Analysis By Range

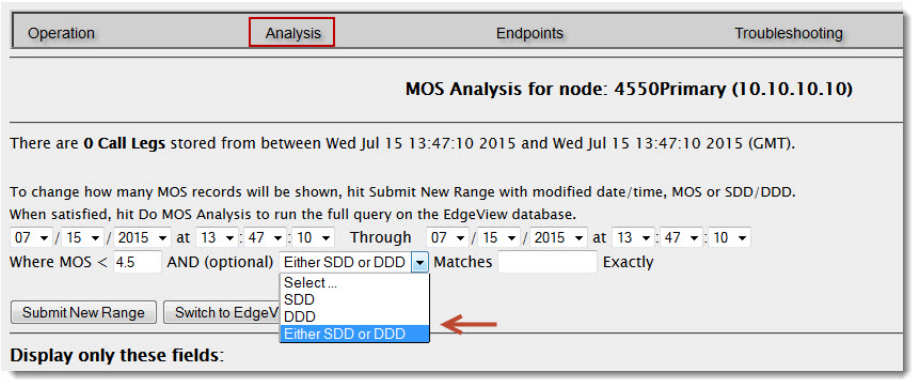


To generate a report for a specified date and time range:

3. Modify the date and time range for which you want EdgeView to do the MOS analysis.
4. Select a MOS score threshold (default = 4.5).

5. Optionally, select SDD, DDD or SDD and DDD from the drop-down menu. If you select SDD or DDD, enter a match criteria in the Matches field.

Figure 8-7 MOS Analysis for Node Page



6. Enable/disable the checkbox for the type of call records to be displayed in the MOS analysis results. By default, all are selected.

Tip

To reduce the number of columns displayed in the MOS report, deselect the fields that are not of interest. Also, click the **Switch to EdgeView Local Time** button to display the results of the MOS analysis in EdgeView Local Time rather than GMT (the default).

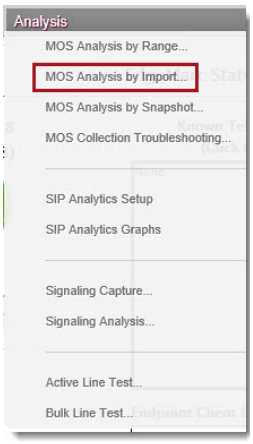
7. Click **Submit New Range**. The MOS Analysis settings will be updated.
8. Click **Do MOS Analysis** to perform a MOS Analysis using these settings. EdgeView will perform the analysis and display the results in a table. Refer to Figure 8-6.

   As shown, you can click on any underlined value to display an Edgewater Networks Knowledgebase article with corrective steps for resolving the problem.

Note

If the list of call legs is too high, EdgeView may propose that you reduce the range since it might take too long to get the results.

Importing a File for MOS Analysis



Select the **Analysis > MOS Analysis by Import** option to run a MOS analysis on a previously saved file or syslog data. The **EdgeView MOS File Import** screen shown in Figure 8-8 displays. To import a file:

1. Select the file type for the MOS analysis file or syslog data you want to import. Refer to Table 8-3 for a description of the supported file types.
2. If you are importing an EdgeView syslog file, click **Import File**. Otherwise, click **Browse** and select the MOS analysis file or syslog data you want to analyze and then click **Import File**.

Figure 8-8 MOS Analysis By Import

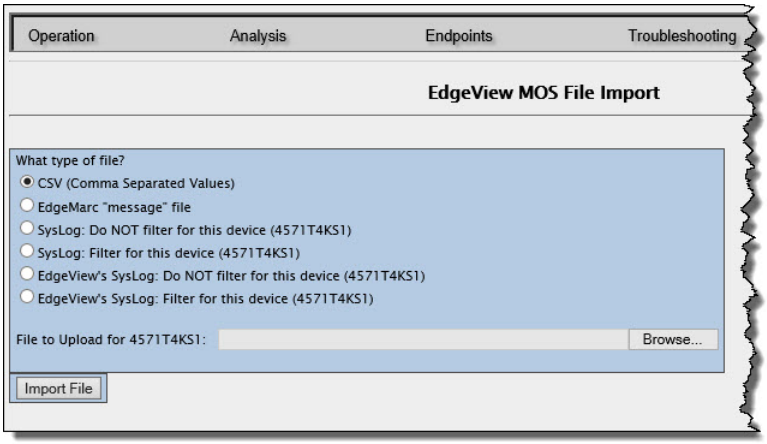


Table 8-3 Supported File Types for MOS Analysis

File Type	Description
CSV	Comma Separate Values. The file must be stored locally on your computer prior to importing.
EdgeMarc "message" file	The etc/log/message file retrieved from an EdgeMarc. The file must be stored locally on your computer prior to importing.
SysLog: DO NOT filter for this device	A syslog formatted file. The file must be stored locally on your computer.
SysLog: Filter for this device	A syslog formatted file. The file must be stored locally on your computer.

Table 8-3 Supported File Types for MOS Analysis (continued)

File Type	Description
EdgeView SysLog: DO NOT filter for this device	EdgeView local syslog server. This file is imported from EdgeView and does NOT need to reside on your computer.
EdgeView SysLog: Filter for this device	EdgeView local syslog server. This file is imported from EdgeView and does NOT need to reside on your computer.

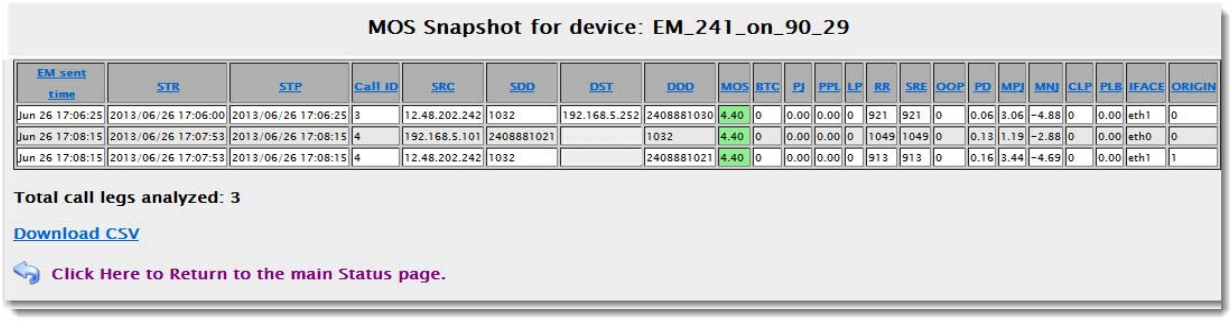
Performing a MOS Analysis by Snapshot



Select the **Analysis > MOS Analysis by Snapshot** option to perform a MOS analysis on the latest MOS data from the selected EdgeMarc. EdgeView will access the EdgeMarc and pull the MOS data out of the syslog file for analysis. The resulting report shows the number of call legs analyzed (Figure 8-9). This process can take a several minutes or longer.

Click **Download .CSV** to save the snapshot file to your local computer.

Figure 8-9 MOS Analysis by Snapshot



EM sent time	STR	STP	Call ID	SRC	SDD	DST	DDD	MOS	BTC	PJ	PPL	LP	RR	SRE	OOP	PD	MPJ	MNJ	CLP	PLB	IFACE	ORIGIN
Jun 26 17:06:25	2013/06/26 17:06:00	2013/06/26 17:06:25	3	12.48.202.242	1032	192.168.5.252	2408881030	4.40	0	0.00	0.00	0	921	921	0	0.06	3.06	-4.88	0	0.00	eth1	0
Jun 26 17:08:15	2013/06/26 17:07:53	2013/06/26 17:08:15	4	192.168.5.101	2408881021		1032	4.40	0	0.00	0.00	0	1049	1049	0	0.13	1.19	-2.88	0	0.00	eth0	0
Jun 26 17:08:15	2013/06/26 17:07:53	2013/06/26 17:08:15	4	12.48.202.242	1032		2408881021	4.40	0	0.00	0.00	0	913	913	0	0.16	3.44	-4.69	0	0.00	eth1	1

Working with Snapshot Files

Snapshot files can be used to pinpoint network gateways that consistently produce poor MOS scores, calls that experience excessive jitter, latency, packet loss, and much more. This same information is available if you are continuously capturing call quality statistics. See Enabling Live MOS Capture for more details.

The snapshot file can be sorted by selecting any of the columns on the top of the table (for example, EM Sent Time, SRC, MOS, etc.). Statistics are provided on a per call basis in both the LAN to WAN and WAN to LAN directions. This is useful for determining whether a particular call quality problem is being caused by networking issues on the LAN side of the EdgeMarc or in the WAN. To view the LAN and WAN side measurements on a per call basis, sort by the Call ID field.

Another common practice is to sort the file by MOS score to quickly identify calls and endpoints that have experienced poor call quality. EdgeView highlights these entries in red (highly impaired), yellow (moderately impaired), and green (not impaired). You will also notice other statistics that use the same color scheme to highlight values considered out of the ordinary. Most of these statistics contain a hyperlink to Edgewater Networks Knowledgebase. Click the hyperlink to display additional information, common problems for poor performance, and troubleshooting tips.

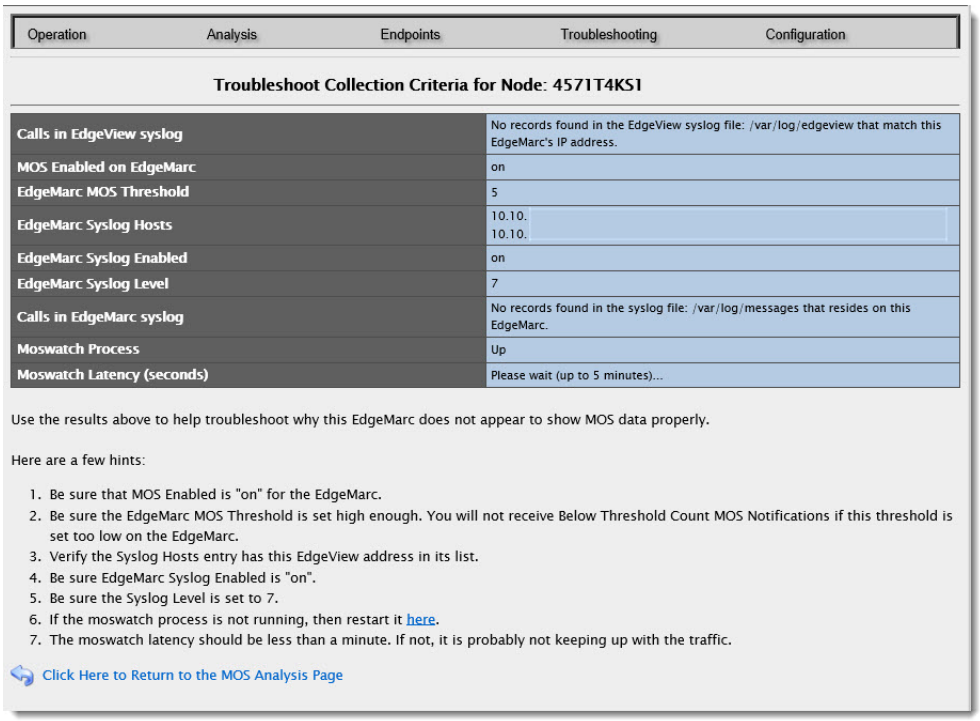
Troubleshooting MOS Collection Data



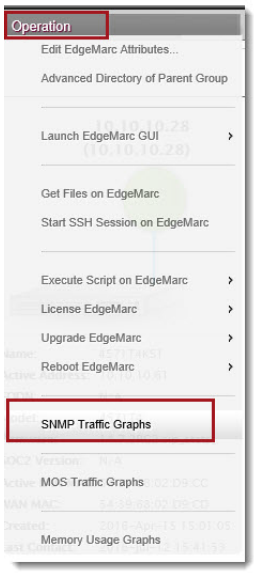
Select the **Analysis > MOS Collection Troubleshooting** option to troubleshoot why MOS data has not been received by EdgeView. EdgeView will access the EdgeMarc, check connections, data, and the node, and display a report. EdgeView compares the EdgeMarc configuration against the records in the EdgeView database and displays a report with tips to help you diagnose problems. If EdgeView has no records for a given process, it displays a message in the report.

Figure 8-10 illustrates the type of MOS diagnostics data that EdgeView displays.

Figure 8-10 Viewing MOS Diagnostics for a Device



Viewing SNMP Traffic Graphs



EdgeView provides a graphical view of traffic statistics collected via SNMP for a managed node. The SNMP traffic graphs are useful in analyzing the WAN/LAN bandwidth utilization over time on a managed EdgeMarc.

To create and view SNMP Traffic graphs:

1. Enable the **Create Traffic Graphs** setting in the EdgeMarc Add/Edit Device page. See Editing EdgeMarc Attributes.
2. Select an EdgeMarc from the device tree and then select **Operation > SNMP Traffic Graphs**.
3. Select a discovered MIB-2 interface from the table by clicking on the radio button next to the description. A daily traffic graph will display to show the traffic statistics collected for the selected MIB-2 interface. You can also choose to run monthly and yearly summary graphs (if available).

Figure 8-11 shows an example of a Daily Traffic Graph for the eth0 - ethernetCsmacd(6) interface. SNMP traffic statistics for the interface are displayed in a table below the SNMP traffic graph (Figure 8-12).

Figure 8-11 Daily SNMP Traffic Graph (5-minute average)

Interface	Speed	Last Polled	Admin Status	Oper Status	Util % In	Util % Out
lo - softwareLoopback(24)	10000000	2014-06-26 08:57:16	up	up	0.00	0.00
eth0 - ethernetCsmacd(6)	100000000	2014-06-26 08:57:16	up	up	0.00	0.00
eth2 - ethernetCsmacd(6)	100000000	2014-06-26 08:57:16	up	up	0.00	0.00

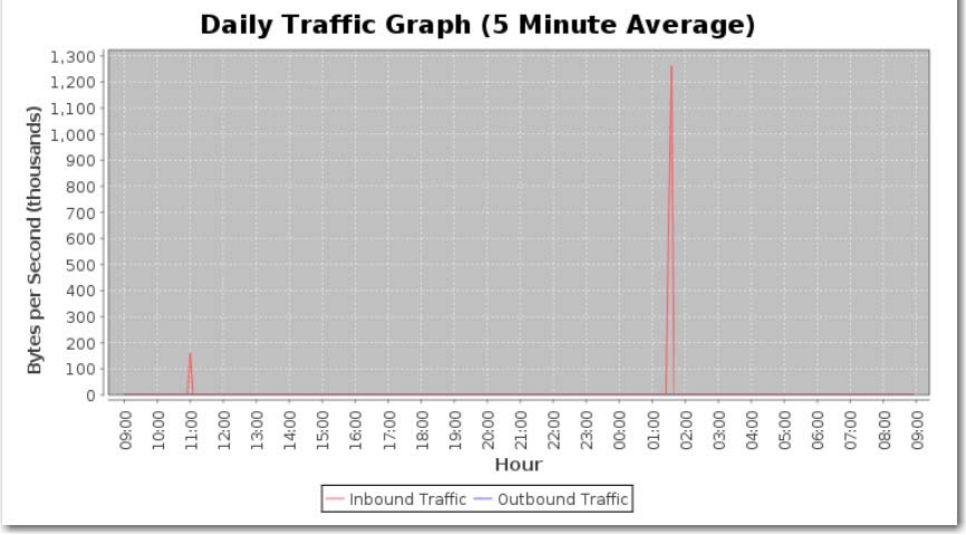
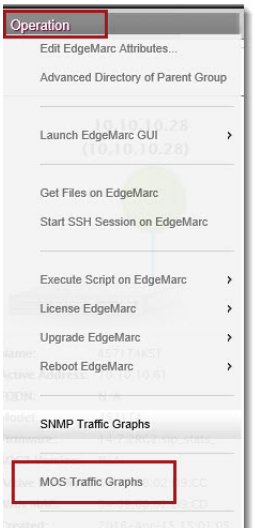


Figure 8-12 SNMP Traffic Statistics

Poll DT	In Octets	In Discard	In Err	Out Octets	Out Discard	Out Err	BPS In	BPS Out	% Util In	% Util Out
2014-06-25 09:00:00	2041261023	0	0	939767723	0	0	4432.35	300.45	0.00	0.00
2014-06-25 09:05:00	2041417263	0	0	939778567	0	0	4166.40	289.17	0.00	0.00
2014-06-25 09:10:00	2041576799	0	0	939790386	0	0	4240.16	314.13	0.00	0.00
2014-06-25 09:15:00	2041738384	0	0	939801752	0	0	4308.93	303.09	0.00	0.00
2014-06-25 09:20:00	2041897583	0	0	939814072	0	0	4245.31	328.53	0.00	0.00
2014-06-25 09:25:00	2042053906	0	0	939825323	0	0	4154.76	299.03	0.00	0.00
2014-06-25 09:30:00	2042217965	0	0	939836709	0	0	4374.91	303.63	0.00	0.00

Viewing Traffic Graphs for MOS Statistics



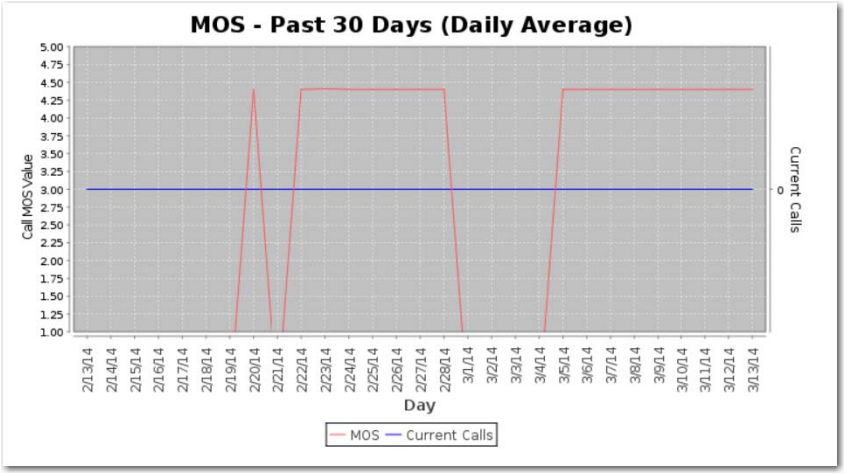
EdgeView provides daily, weekly, and monthly graphs of MOS statistics that have been collected for each managed node. These graphs are useful in determining the call quality performance of any given node over time.

To access these graphs:

1. Enable the **Create MOS Graphs** setting in the EdgeMarc Add/Edit Device page. See Editing EdgeMarc Attributes.
2. Select an EdgeMarc from the device tree and then select **Operation > MOS Traffic Graphs**. Three MOS Traffic Graphs will be displayed showing daily, weekly, and monthly MOS statistics.

Figure 8-10 shows an example of a MOS Traffic Graph for the MOS statistics over the past 30 days.

Figure 8-13 MOS Traffic Graph: Past 30 Days (Daily Average)



Sending MOS Alert Notifications

EdgeView can send MOS alert notifications to provide proactive notification of poor VoIP call performance in the network. You can configure EdgeView to send email notifications when it receives a MOS threshold exceeded alarm from any node being monitored.

For details about configuring MOS alerts and other notifications, see Chapter 6, *Status and Notifications*.

SIP Analytics

Realtime voice and data analytics enable EdgeView to determine the status of system performance and assist in collecting troubleshooting diagnostics. The EdgeMarc requires VOS version 14.3 to send system data to EdgeView running version 14.0; EdgeView then collects and displays the data. Perpetual and subscription licensing provides flexible management options.

The analytics process includes:

- Data Gathering—The EdgeMarc collects all the SIP signaling data and sends it to EdgeView for processing, archive, and reporting.
- Data Reporting—EdgeView receives the SIP signaling data from the EdgeMarc, processes and archives it, and generates graphical and tabular reports.

The type of analytics collected include:

- Network Analytics—Based on the start and end date and time for the network, EdgeView Tree branch, or specific EdgeMarc.
- Voice Analytics—Voice SIP-related statistics as configured (duration in seconds, minutes, and hours).

VoIP Protocol and System Analytics for EdgeMarc management is supported on the following EdgeMarc platforms:

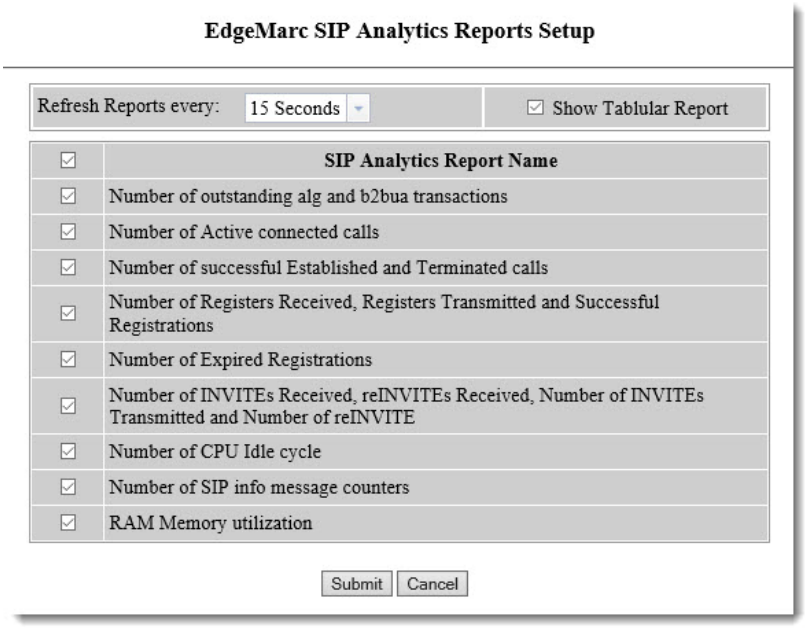
- EdgeMarc 4700, 4750
- EdgeMarc 7300, 7301, 7400
- Virtual EdgeMarc 4550, 4552

Configuring VoIP Protocol and System Analytics

To set up analytics on the EdgeView:

1. Select a supported device from the Device Tree.
2. Click **Analysis** and choose **SIP Analytics Graphs** from the drop-down menu.
3. Click **Report Setup** on the EdgeMarc SIP Analytics Graphs page. Configuration fields are displayed (Figure 8-14).

Figure 8-14 EdgeMarc SIP Analytics Reports Setup



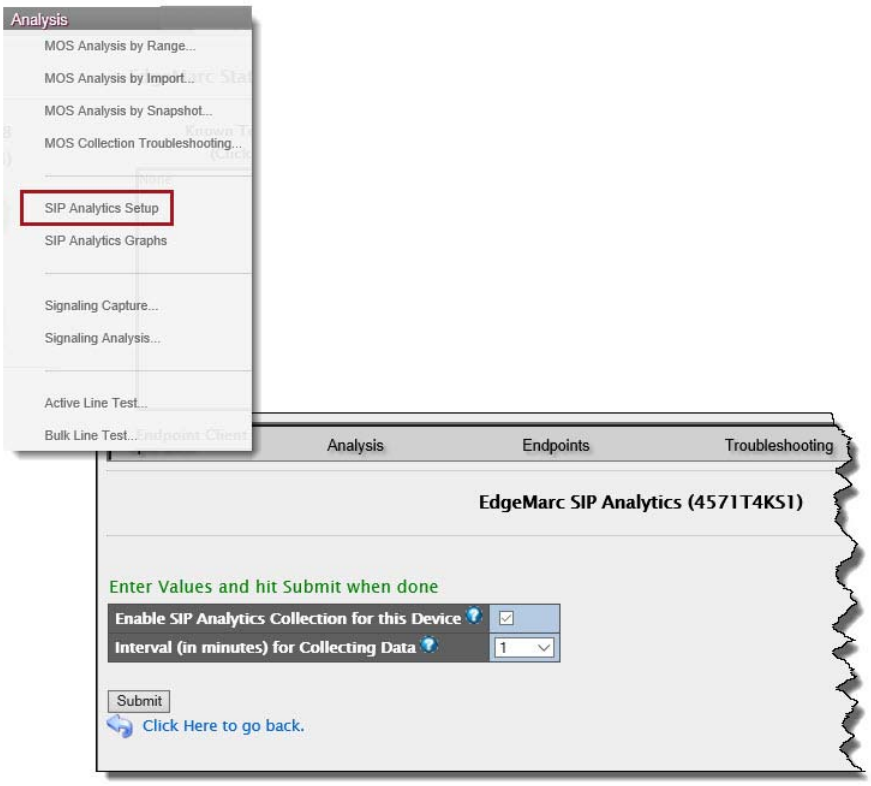
4. Select the **SIP Analytics Report Name** checkbox to select all checkboxes on the page.
5. Click **Submit** to save your changes.

Managing VoIP Protocol and System Analytics

To manage analytics on EdgeView:

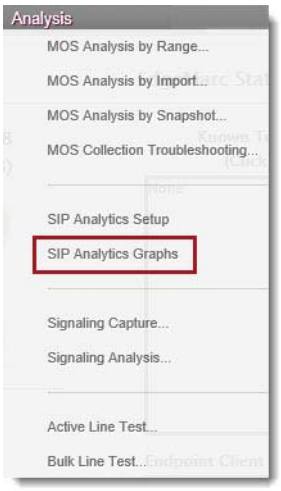
1. Set up Analytics on the EdgeView as shown in Figure 8-14.
2. Select a supported device from the Device Tree.
3. Click **Analysis**.
4. Choose **SIP Analytics Setup** from the drop-down menu. The EdgeMarc SIP Analytics page is displayed.

Figure 8-15 SIP Analytics Setup Page



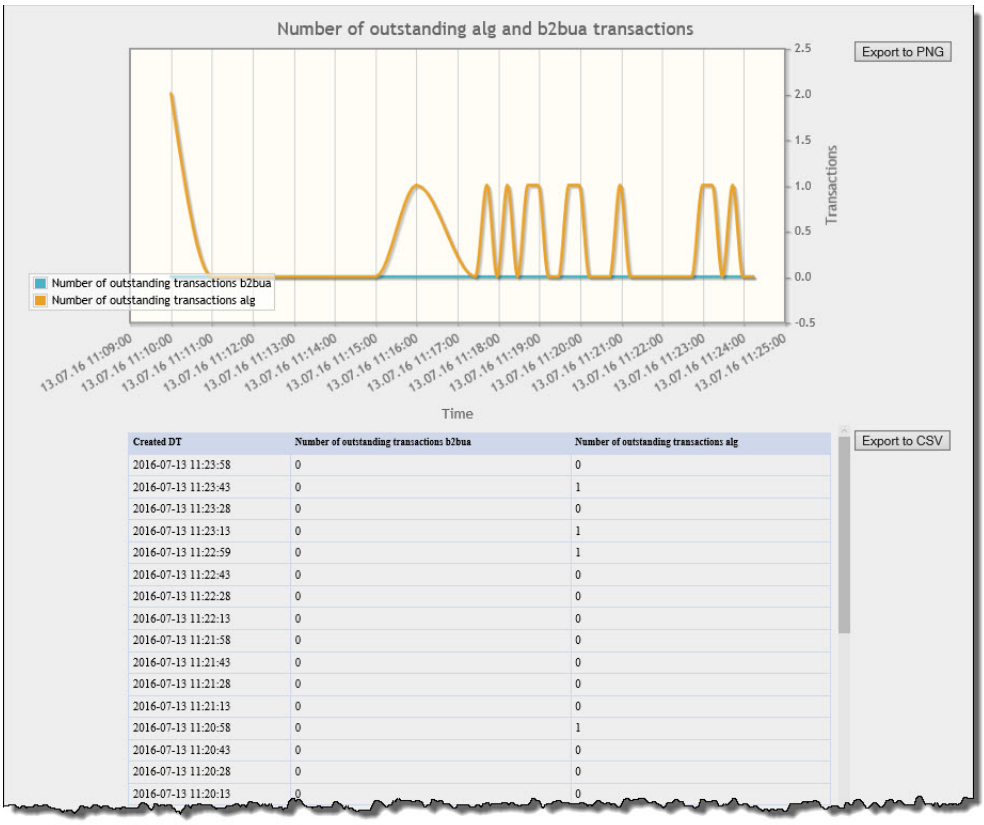
5. Select the **Enable SIP Analytics Collection for this Device** checkbox.
6. Choose a value from the **Interval (in minutes) for Collecting Data** drop-down menu. Values are 1 to 1440, default is 5.
7. Click **Submit**.
8. To view analytics graphs, click **Analysis**.

Figure 8-16 Analysis Menu



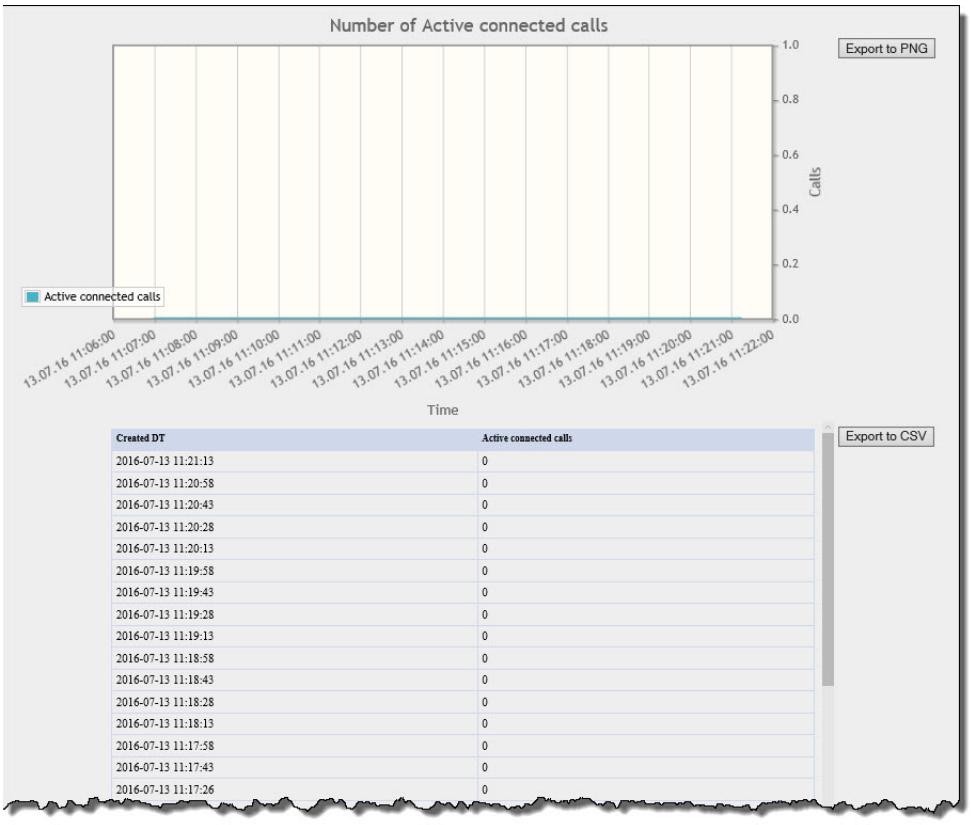
9. Choose **SIP Analytics Graphs** from the drop-down menu. The EdgeMarc SIP Analytics Graphs page is displayed.
10. Observe the following graphs on the page:
    - Number of Outstanding ALG and B2BUA Transactions
    - Number of Registers Received, Registers Transmitted, and Successful Registrations
    - Number of Successful Established and Terminated Calls
    - Number of Registers Received, Registers Transmitted, and Successful Registrations
    - Number of Expired Registrations
    - Number of INVITES and reINVITES Received and Transmitted
    - Number of CPU Idle Cycle
    - Number of SIP Info Message Counters
    - RAM Memory Utilization

Figure 8-17 Number of Outstanding ALG and B2BUA Transactions



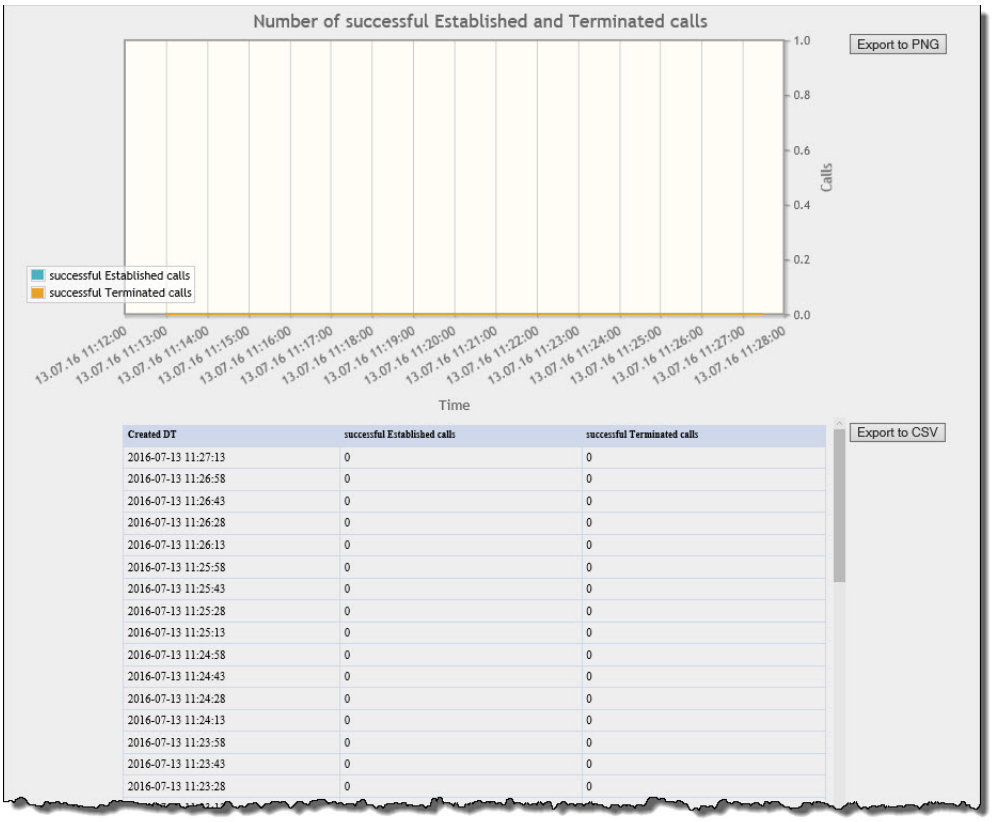
Created DT	Number of outstanding transactions b2bua	Number of outstanding transactions alg
2016-07-13 11:23:58	0	0
2016-07-13 11:23:43	0	1
2016-07-13 11:23:28	0	0
2016-07-13 11:23:13	0	1
2016-07-13 11:22:59	0	1
2016-07-13 11:22:43	0	0
2016-07-13 11:22:28	0	0
2016-07-13 11:22:13	0	0
2016-07-13 11:21:58	0	0
2016-07-13 11:21:43	0	0
2016-07-13 11:21:28	0	0
2016-07-13 11:21:13	0	0
2016-07-13 11:20:58	0	1
2016-07-13 11:20:43	0	0
2016-07-13 11:20:28	0	0
2016-07-13 11:20:13	0	0

Figure 8-18 Number of Active Connected Calls



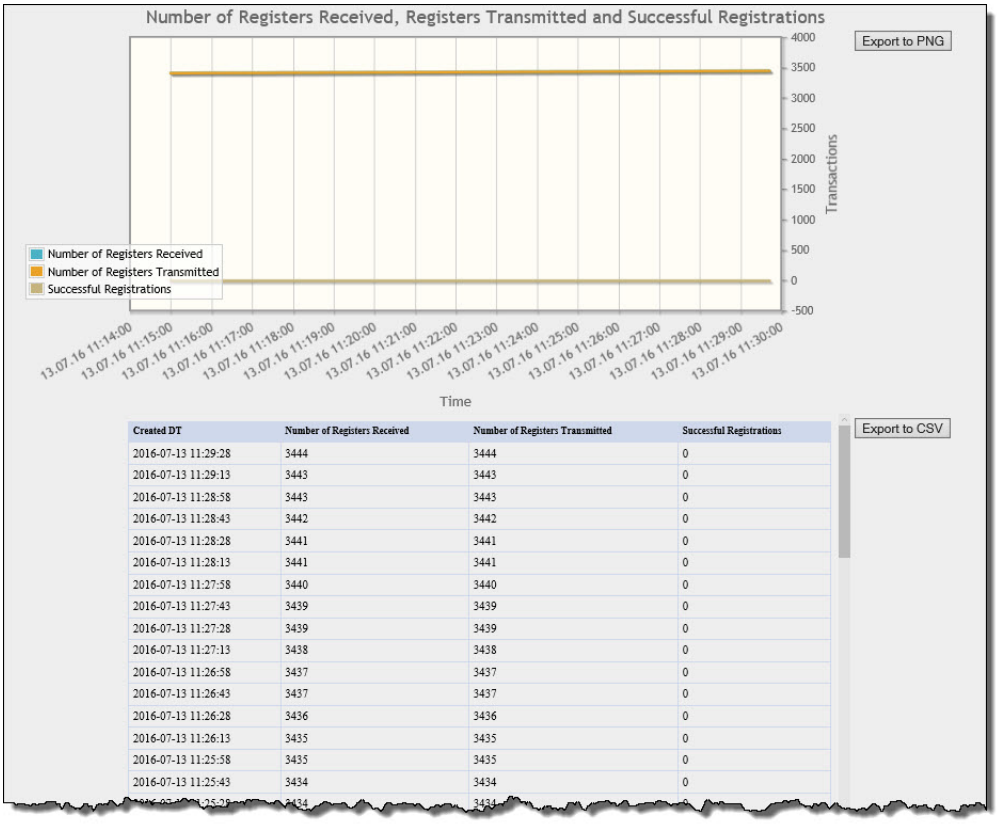
Created DT	Active connected calls
2016-07-13 11:21:13	0
2016-07-13 11:20:58	0
2016-07-13 11:20:43	0
2016-07-13 11:20:28	0
2016-07-13 11:20:13	0
2016-07-13 11:19:58	0
2016-07-13 11:19:43	0
2016-07-13 11:19:28	0
2016-07-13 11:19:13	0
2016-07-13 11:18:58	0
2016-07-13 11:18:43	0
2016-07-13 11:18:28	0
2016-07-13 11:18:13	0
2016-07-13 11:17:58	0
2016-07-13 11:17:43	0
2016-07-13 11:17:26	0

Figure 8-19 Number of Successful Established and Terminated Calls



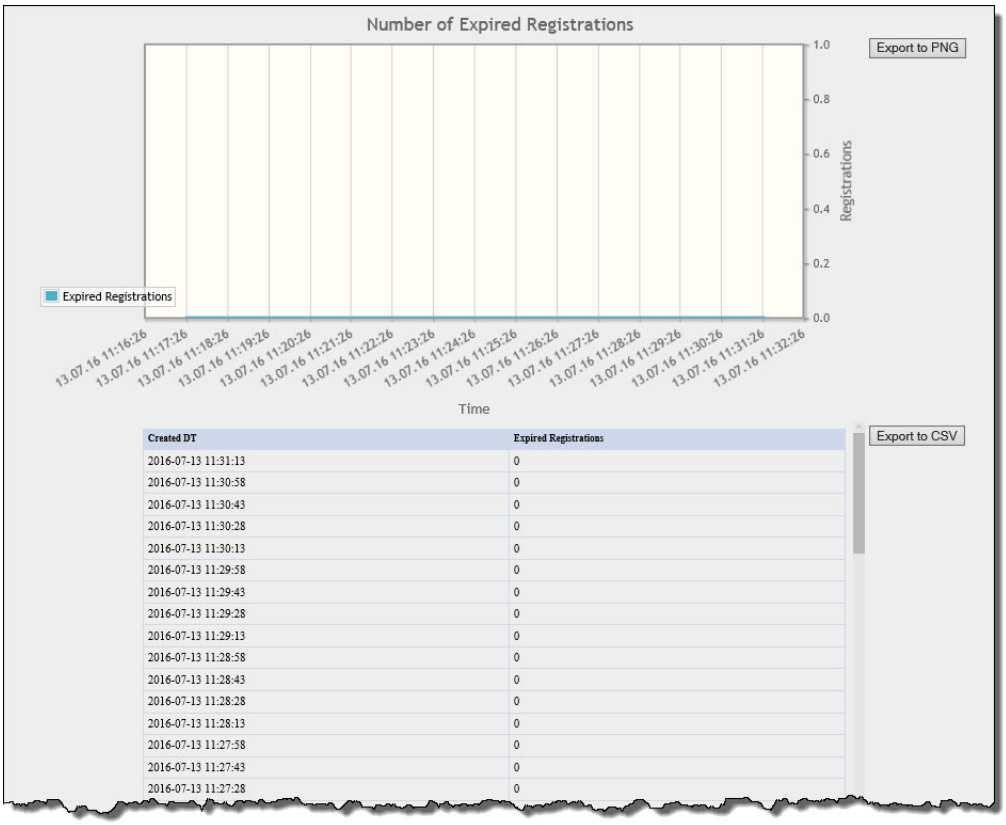
Created DT	successful Established calls	successful Terminated calls
2016-07-13 11:27:13	0	0
2016-07-13 11:26:58	0	0
2016-07-13 11:26:43	0	0
2016-07-13 11:26:28	0	0
2016-07-13 11:26:13	0	0
2016-07-13 11:25:58	0	0
2016-07-13 11:25:43	0	0
2016-07-13 11:25:28	0	0
2016-07-13 11:25:13	0	0
2016-07-13 11:24:58	0	0
2016-07-13 11:24:43	0	0
2016-07-13 11:24:28	0	0
2016-07-13 11:24:13	0	0
2016-07-13 11:23:58	0	0
2016-07-13 11:23:43	0	0
2016-07-13 11:23:28	0	0

Figure 8-20 Number of Registers Received, Registers Transmitted, and Successful Registrations



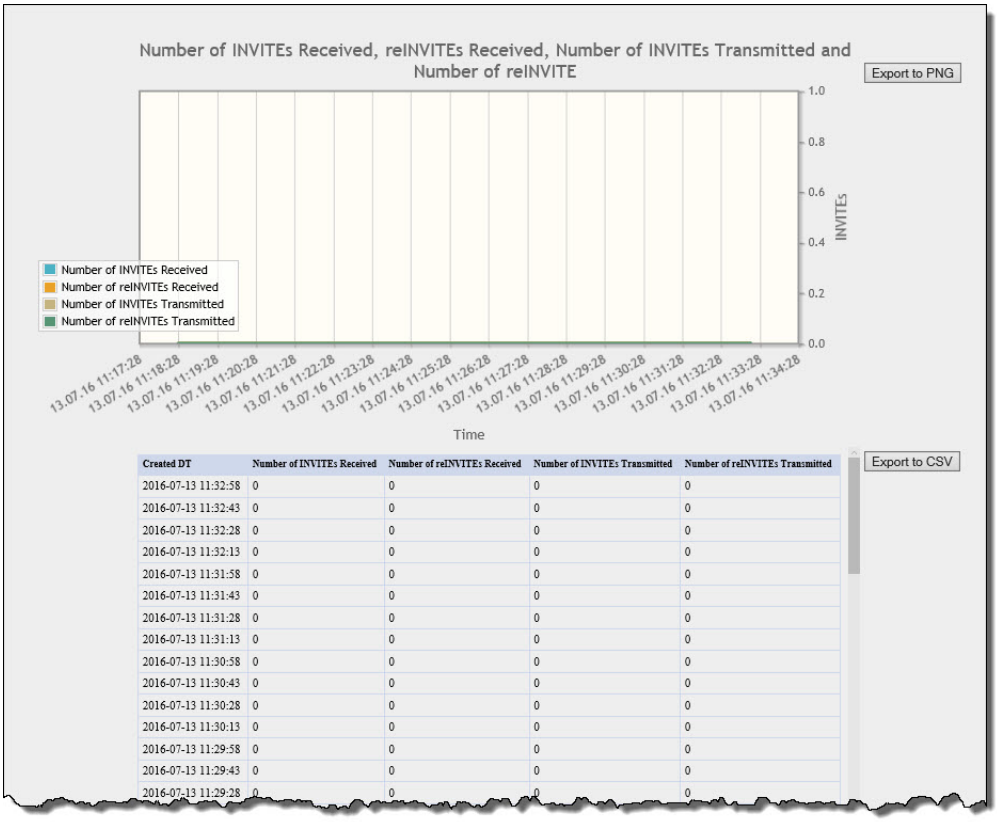
Created DT	Number of Registers Received	Number of Registers Transmitted	Successful Registrations
2016-07-13 11:29:28	3444	3444	0
2016-07-13 11:29:13	3443	3443	0
2016-07-13 11:28:58	3443	3443	0
2016-07-13 11:28:43	3442	3442	0
2016-07-13 11:28:28	3441	3441	0
2016-07-13 11:28:13	3441	3441	0
2016-07-13 11:27:58	3440	3440	0
2016-07-13 11:27:43	3439	3439	0
2016-07-13 11:27:28	3439	3439	0
2016-07-13 11:27:13	3438	3438	0
2016-07-13 11:26:58	3437	3437	0
2016-07-13 11:26:43	3437	3437	0
2016-07-13 11:26:28	3436	3436	0
2016-07-13 11:26:13	3435	3435	0
2016-07-13 11:25:58	3435	3435	0
2016-07-13 11:25:43	3434	3434	0

Figure 8-21 Number of Expired Registrations



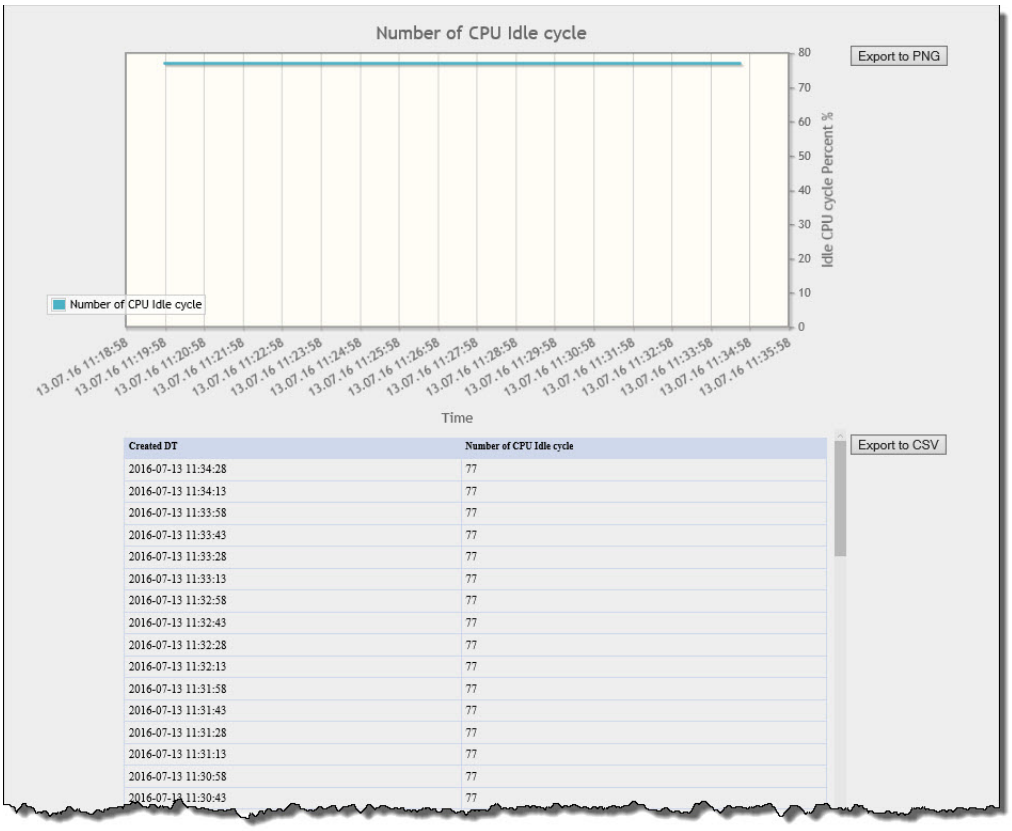
Created DT	Expired Registrations
2016-07-13 11:31:13	0
2016-07-13 11:30:58	0
2016-07-13 11:30:43	0
2016-07-13 11:30:28	0
2016-07-13 11:30:13	0
2016-07-13 11:29:58	0
2016-07-13 11:29:43	0
2016-07-13 11:29:28	0
2016-07-13 11:29:13	0
2016-07-13 11:28:58	0
2016-07-13 11:28:43	0
2016-07-13 11:28:28	0
2016-07-13 11:28:13	0
2016-07-13 11:27:58	0
2016-07-13 11:27:43	0
2016-07-13 11:27:28	0

Figure 8-22 Number of INVITES and reINVITES Received and Transmitted



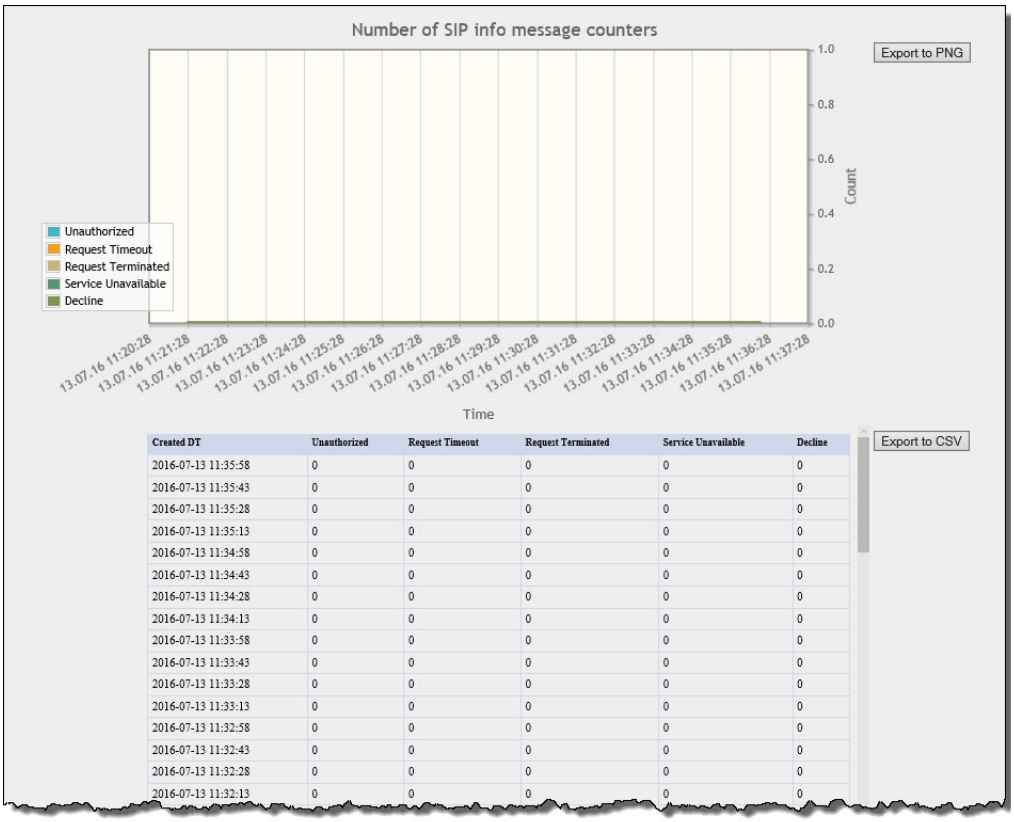
Created DT	Number of INVITEs Received	Number of reINVITEs Received	Number of INVITEs Transmitted	Number of reINVITEs Transmitted
2016-07-13 11:32:58	0	0	0	0
2016-07-13 11:32:43	0	0	0	0
2016-07-13 11:32:28	0	0	0	0
2016-07-13 11:32:13	0	0	0	0
2016-07-13 11:31:58	0	0	0	0
2016-07-13 11:31:43	0	0	0	0
2016-07-13 11:31:28	0	0	0	0
2016-07-13 11:31:13	0	0	0	0
2016-07-13 11:30:58	0	0	0	0
2016-07-13 11:30:43	0	0	0	0
2016-07-13 11:30:28	0	0	0	0
2016-07-13 11:30:13	0	0	0	0
2016-07-13 11:29:58	0	0	0	0
2016-07-13 11:29:43	0	0	0	0
2016-07-13 11:29:28	0	0	0	0

Figure 8-23 Number of CPU Idle Cycle



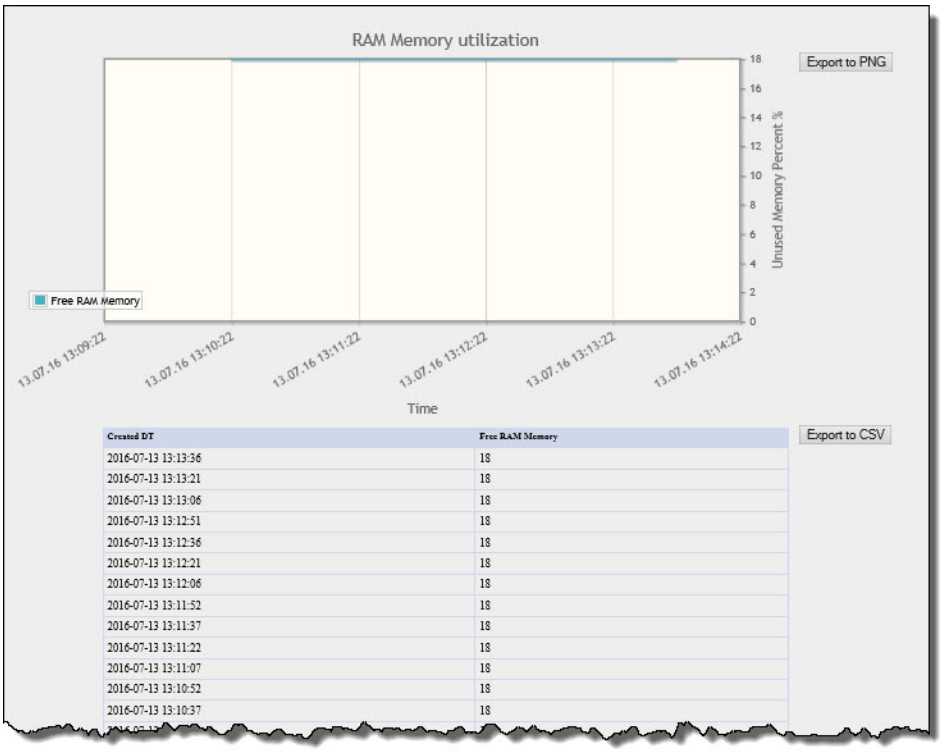
Created DT	Number of CPU Idle cycle
2016-07-13 11:34:28	77
2016-07-13 11:34:13	77
2016-07-13 11:33:58	77
2016-07-13 11:33:43	77
2016-07-13 11:33:28	77
2016-07-13 11:33:13	77
2016-07-13 11:32:58	77
2016-07-13 11:32:43	77
2016-07-13 11:32:28	77
2016-07-13 11:32:13	77
2016-07-13 11:31:58	77
2016-07-13 11:31:43	77
2016-07-13 11:31:28	77
2016-07-13 11:31:13	77
2016-07-13 11:30:58	77
2016-07-13 11:30:43	77

Figure 8-24 Number of SIP Info Message Counters



Created DT	Unauthorized	Request Timeout	Request Terminated	Service Unavailable	Decline
2016-07-13 11:35:58	0	0	0	0	0
2016-07-13 11:35:43	0	0	0	0	0
2016-07-13 11:35:28	0	0	0	0	0
2016-07-13 11:35:13	0	0	0	0	0
2016-07-13 11:34:58	0	0	0	0	0
2016-07-13 11:34:43	0	0	0	0	0
2016-07-13 11:34:28	0	0	0	0	0
2016-07-13 11:34:13	0	0	0	0	0
2016-07-13 11:33:58	0	0	0	0	0
2016-07-13 11:33:43	0	0	0	0	0
2016-07-13 11:33:28	0	0	0	0	0
2016-07-13 11:33:13	0	0	0	0	0
2016-07-13 11:32:58	0	0	0	0	0
2016-07-13 11:32:43	0	0	0	0	0
2016-07-13 11:32:28	0	0	0	0	0
2016-07-13 11:32:13	0	0	0	0	0

Figure 8-25 RAM Memory Utilization



Created DT	Free RAM Memory
2016-07-13 13:13:36	18
2016-07-13 13:13:21	18
2016-07-13 13:13:06	18
2016-07-13 13:12:51	18
2016-07-13 13:12:36	18
2016-07-13 13:12:21	18
2016-07-13 13:12:06	18
2016-07-13 13:11:52	18
2016-07-13 13:11:37	18
2016-07-13 13:11:22	18
2016-07-13 13:11:07	18
2016-07-13 13:10:52	18
2016-07-13 13:10:37	18

Signaling Capture and Analysis

EdgeView can be used to provide detailed EdgeMarc LAN and WAN signaling traces for VoIP calls that includes call ladder diagrams and SIP header information. This information is collected by the EdgeMarc nodes and sent to EdgeView at the completion of the capture.

Configuring Signaling Capture Settings



Select the **Analysis > Signaling Capture** option to perform a signaling capture. Use the buttons at the bottom of the Signaling Capture page (Figure 8-26) to start, stop, and view a signaling capture.

Refer to the descriptions in Table 8-4 to configure Signal Capture settings.

The signaling captures are stored in a RAM disk in the EdgeMarc. This RAM disk must be periodically cleared and the information sent to EdgeView for permanent storage. The EdgeMarc node will send the signaling capture to EdgeView when the configured percentage of RAM in the EdgeMarc has been used to store the signaling captures. Once this percentage has been reached, the capture files will be sent to EdgeView and deleted locally in the EdgeMarc. For best results, use the default values.

Figure 8-26 Signaling Capture Page

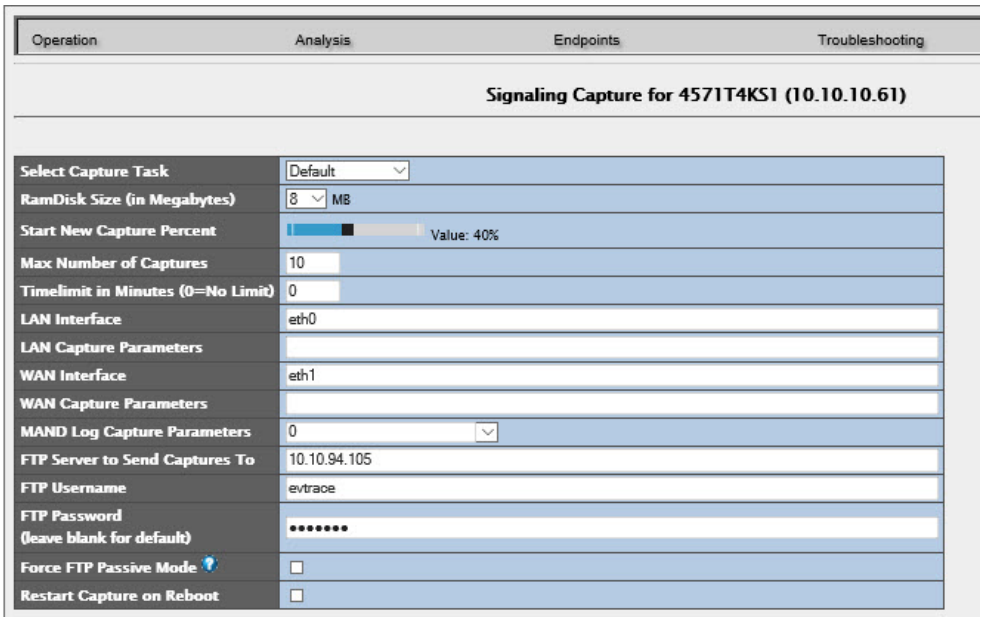


Table 8-4 Signal Capture Settings

Field	Description
RamDisk Size (in Megabytes)	The maximum disk space EdgeView can use on the EdgeMarc for signaling capture processes. Default is 8MB.

Start New Capture Percent	When the percentage of available RAM disk space on the EdgeMarc exceeds the percentage set here, EdgeView will FTP the results. Slide the blue bar left or right to select a percentage. Default is 80%.
Max Number of Captures	If the captures exceed this number, EdgeView will stop doing captures. Default is 10.
Time Limit in minutes (0=No limit)	The number of minutes you want EdgeView to do signaling captures. When this time limit is reached, signaling capture by the EdgeMarc node will be turned off. Enter 0 (the default) if there is no time limit. Default is 0.
LAN Interface	The LAN interface that you want to sniff (for example eth0.20 for interface eth0 for VLAN 20). Include the VoIP VLAN number if you are using VLANs (for example, eth0.500). Default is eth0.
LAN Capture Parameters	The signaling port used for LAN-side captures. Use port 5060 or port 5050.
WAN Interface	The WAN interface that you want to sniff (for example pvc0). Default is eth1.
WAN Capture Parameters	The signaling port used for WAN-side captures. Use port 5060 or port 5050.
FTP Server to Send Captures To	The IP address of the FTP server. This is typically the IP address for EdgeView.
FTP User Name	The user name that is used to log in to the FTP server.
FTP Password	The password that is used to log in to the FTP server.
Force FTP Passive Mode	Forces passive FTP by using the **ftp -p** command on the EdgeMarc.
Restart Capture on Reboot	Enable if you want to restart signaling capture when an EdgeMarc is rebooted.

Tips for Configuring Signal Capture Settings

- EdgeView stores signaling capture data in a packet capture file (PCAP file). When you do a signal capture, a PCAP file is created for the LAN or WAN interface that you want to sniff. If you enter a value for both the LAN and WAN interface, two PCAP files are generated—one for each interface.
- If you want to capture the signalization, specify port 5060 in the **Capture Parameters** field. If you want to capture both voice and signalization, set the filter in the **Capture Parameters** field to UDP (assuming the signalization is configured to be on the UDP protocol).

  For more information about setting the capture filter parameters, refer to the *Unix tcpdump Manual*: www.tcpdump.org/tcpdump_man.html

- The signal capture settings will be used for subsequent signal captures unless you change them.
- If you are using a third-party FTP server, make sure that the EdgeMarc can FTP the file at the Firewall level. Otherwise, you will not be able to do a signal capture.

Performing a Signal Capture

To perform a signal capture:

1. In the Signaling Captures page, click **Start Capture** to start the capture. It can take 10 seconds or more for the system to begin capture. The system issues the following message:

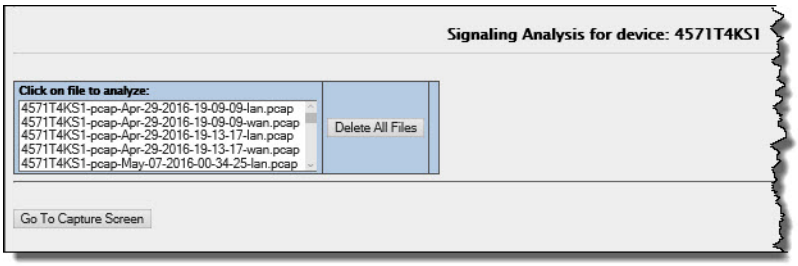
   "Capture script started successfully and is now in progress on this EdgeMarc."

2. Click **Stop Capture** to stop the capture. Once the signaling capture stops, the EdgeMarc will send the files to EdgeView. The system issues the following message:

   "Capture script notification to stop has been sent to the EdgeMarc. It takes some time to complete the stop process. Please wait 30 seconds before starting another capture on this EdgeMarc."

3. Click **View Captures** to view the files that were analyzed (Figure 8-27). If the capture was successful, a message will display when you view the files.

Figure 8-27 Signaling Capture



Analyzing the Signaling Capture



Select the **Analysis > Signaling Analysis** option to analyze a signaling capture file and display the results in a PCAP file. The Signaling Analysis for Device screen shown in Figure 8-28 displays. You can enter a date/time range for stored signaling captures which will help you narrow the results to the estimated time when the issue occurred. You can then download the PCAP file and open it with a PCAP editor for further analysis.

To analyze a signaling capture file:

1. Select the file from the list of capture files in the Signaling Analysis for device screen. Options for the signaling analysis will display on the screen (Figure 8-28).
2. To narrow the results, select a time window and SIP options to exclude from the call ladder (SIP OPTIONS messages, SIP REGISTER messages and SIP SUBSCRIBE messages).
3. Select the **Endpoints to Capture** to display both or only one of the VoIP endpoints.
4. Click **Do Analysis**. A new browser window will open that shows the results of the analysis in a call ladder (Figure 8-29). The messages are color-coded. Click on any leg in the call ladder to view the SIP activity between two endpoints. The activity is shown in the SIP message box at the bottom of the page.

   The SIP call ladder contains three frames:

   - The source and destination IP addresses used for the call.
   - The call ladder showing the call flow.
   - The SIP header detail for the call leg that is selected in the second frame.

Figure 8-28 Analyzing a Signaling Capture File

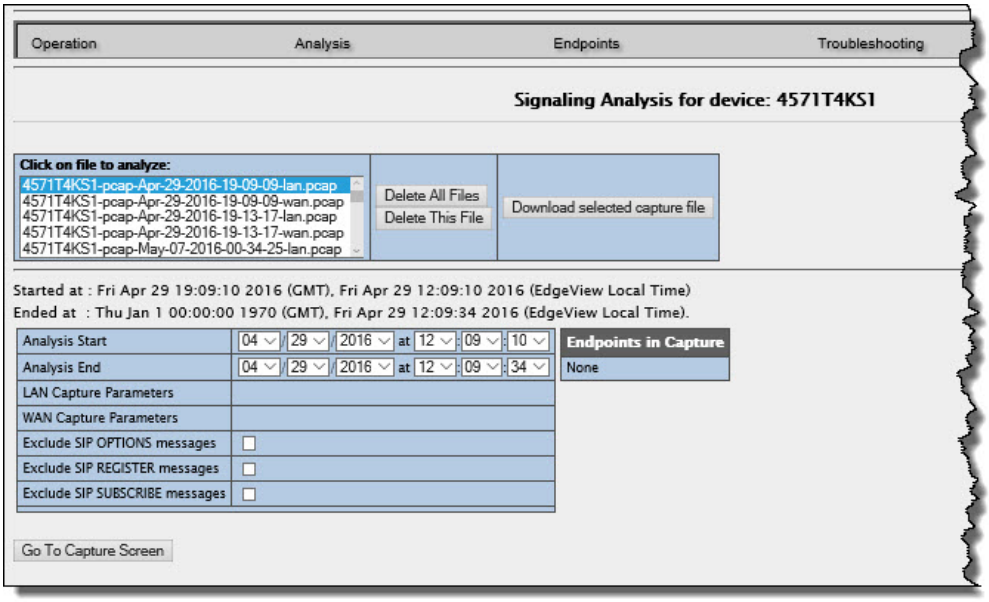
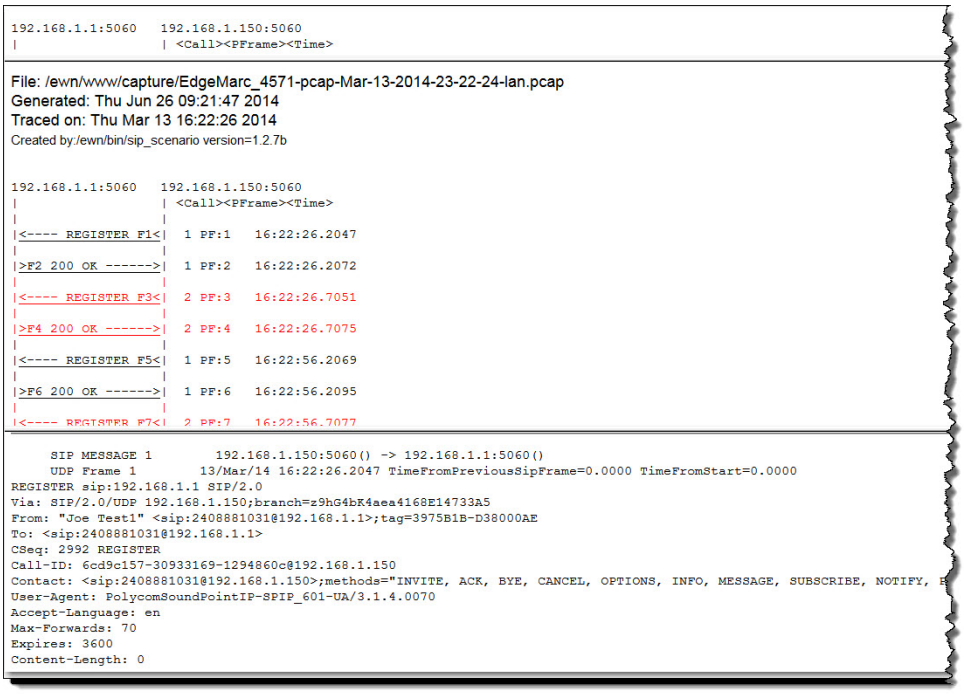


Figure 8-29 On Demand Signaling Ladder



Downloading a Signaling Capture PCAP File

To download a PCAP file to your local computer:

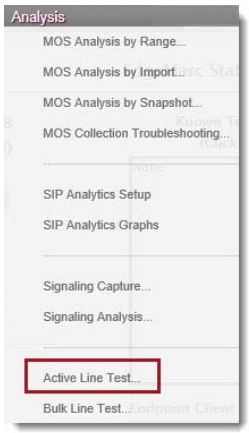
1. Select the file in the Signaling Analysis for device screen.
2. Click **Download selected pcap file**.
3. Select a location on your local drive to download the file.

Deleting Signaling Capture Files

To delete a signaling capture file:

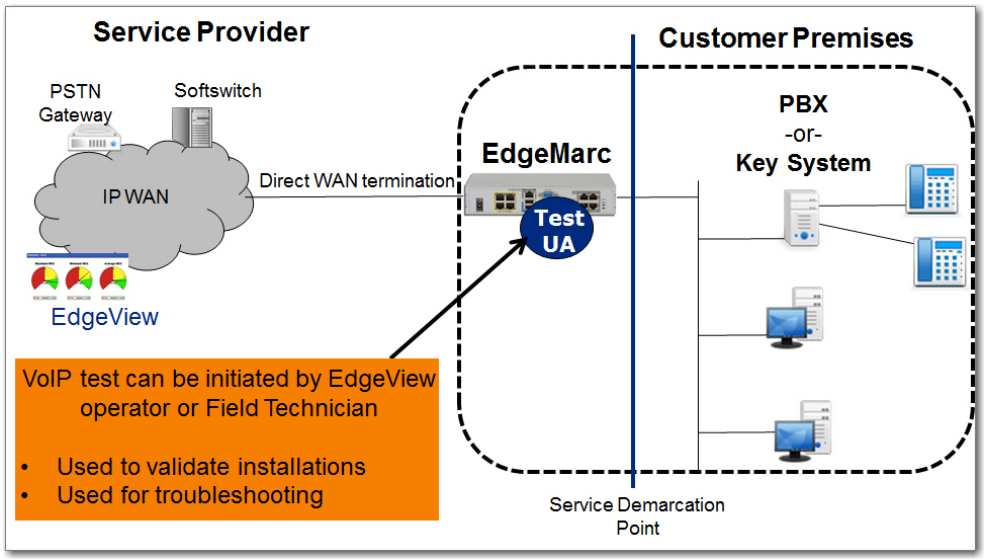
1. Select the file in the Signaling Analysis for device screen.
2. Click **Delete This File**.
3. Confirm the deletion. The file will be removed from the signaling capture file list.
4. To delete all signaling capture files, click **Delete All Files**.

Performing an Active Line Test to Verify EdgeMarc Connectivity



You can verify the connectivity of any EdgeMarc and obtain a MOS report without remote assistance using the Active Line test feature. An active line test generates a call from an EdgeMarc to an IP phone on the LAN or to a phone on the PSTN. It can also generate a call from an EdgeMarc to an EdgeMarc. Figure 8-30 illustrates how to test the EdgeMarc remotely using the EdgeMarc integrated VoIP Test Agent.

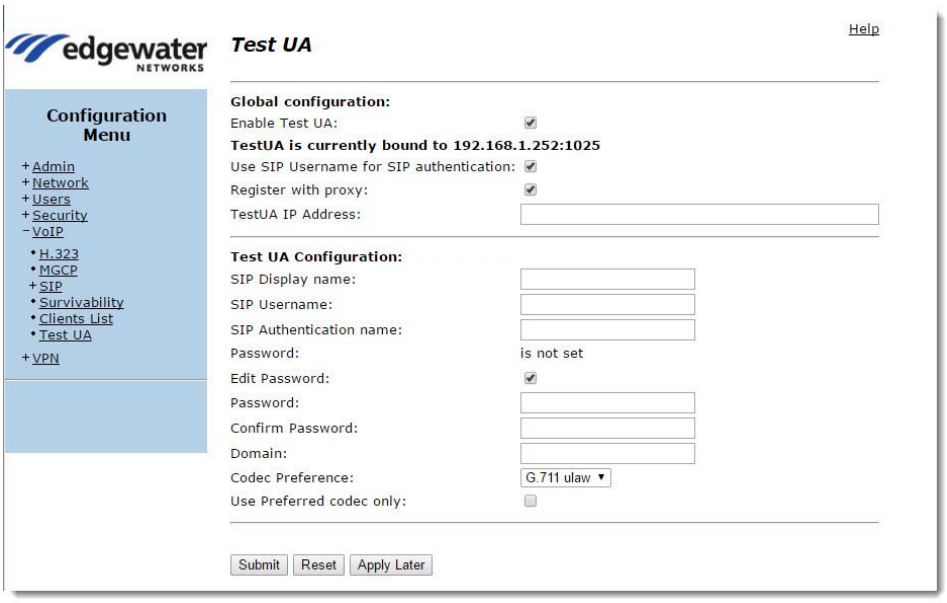
Figure 8-30 Active Line Test



To perform an active line test:

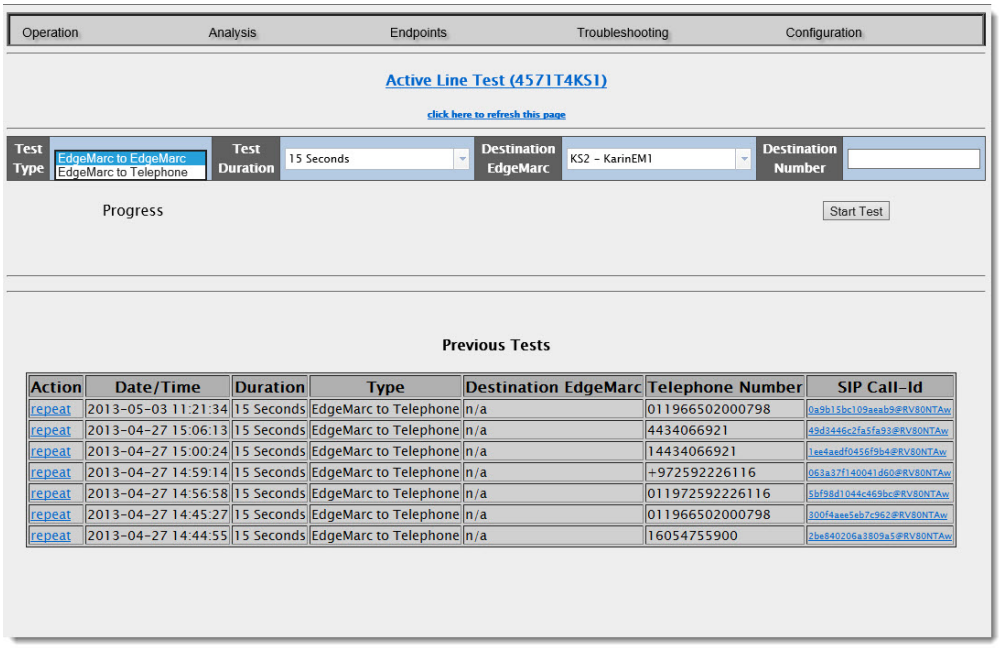
1. On the EdgeMarc, open the EdgeMarc user interface and select **VoIP > Test UA** from the Configuration Menu. Configure settings for a VoIP Test (Figure 8-31). For more details, refer to the *EdgeMarc VoIP Operating System User Guide.*

Figure 8-31 Configuring the EdgeMarc for a VoIP Test



2. From the EdgeView user interface, select the EdgeMarc from the device tree and select **Analysis > Active Line Test**. The Active Line Test screen displays.

Figure 8-32 Active Line Test Screen



3. Select a Test Type from the drop-down box: EdgeMarc to EdgeMarc or EdgeMarc to Telephone (Figure 8-32).

Tip

The most common type of test is to test the signalization from an EdgeMarc to a telephone.

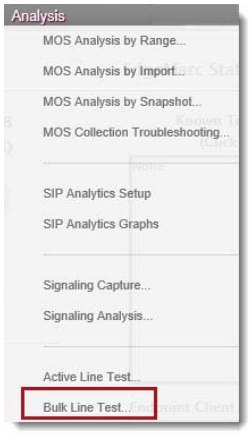
4. Specify a **Test Duration**. The default duration for the test is 30 seconds. You may specify up to a 20 minute duration.
5. Select a **Destination EdgeMarc** from the drop-down box.

Note

If the selected Test Type is EdgeMarc to EdgeMarc, the Destination EdgeMarc must be registered as a node in EdgeView.

6. Enter a **Destination Number**. The destination number must be registered with the SIP server on the corresponding EdgeMarc.
7. and the name or phone number of the destination EdgeMarc or endpoint.
8. Click **Start Test**. A status window reports the progress of the test.

Performing a Bulk Line Test



You can enable automated connectivity and call quality testing from an EdgeMarc to any number of destination phone numbers using the Bulk Line Test feature. When you start a bulk line test, EdgeView will issue commands to the EdgeMarc such that the Test UA in the EdgeMarc will automatically place a 5-second test call to each of the numbers designated for bulk line testing. The call is analyzed as any normal call in EdgeView through MOS records sent from the EdgeMarc to EdgeView. For a bulk line test, EdgeView displays results only for reachability and call quality. If a call cannot connect, the reason for the error is displayed.

You can view more detailed statistics about bulk line test calls by selecting the call(s) from the Last 10 Available Call Records section on the EdgeMarc Status page.

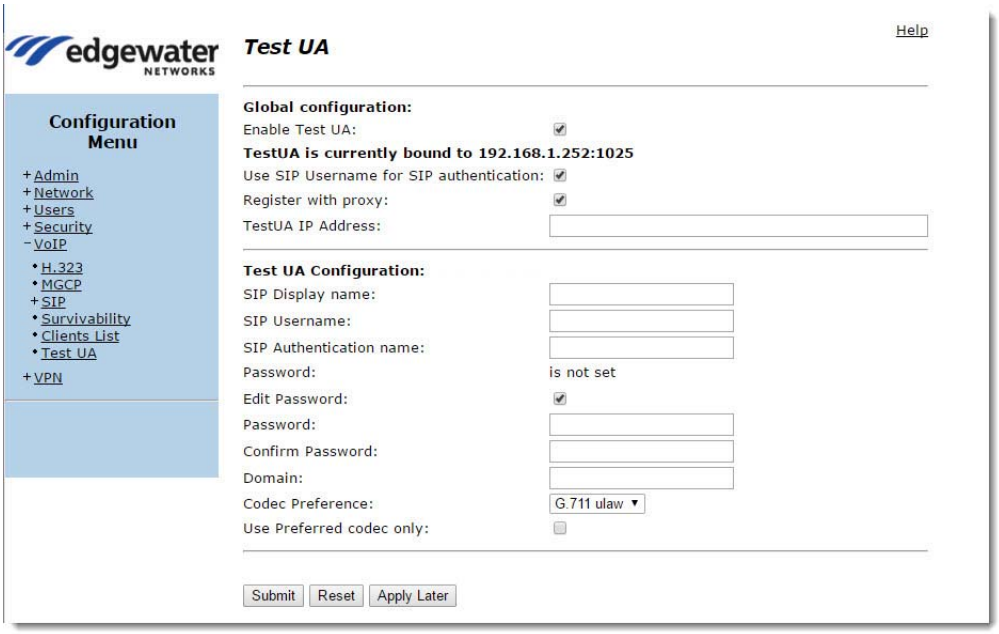
A bulk line test can be initiated through EdgeView or by sending HTTP commands. To perform the test from EdgeView, you need to enable TestUA settings on the EdgeMarc and also configure settings on the EdgeView Bulk Line Test page as described here.

Setting Up a Bulk Line Test

To setup a bulk line test:

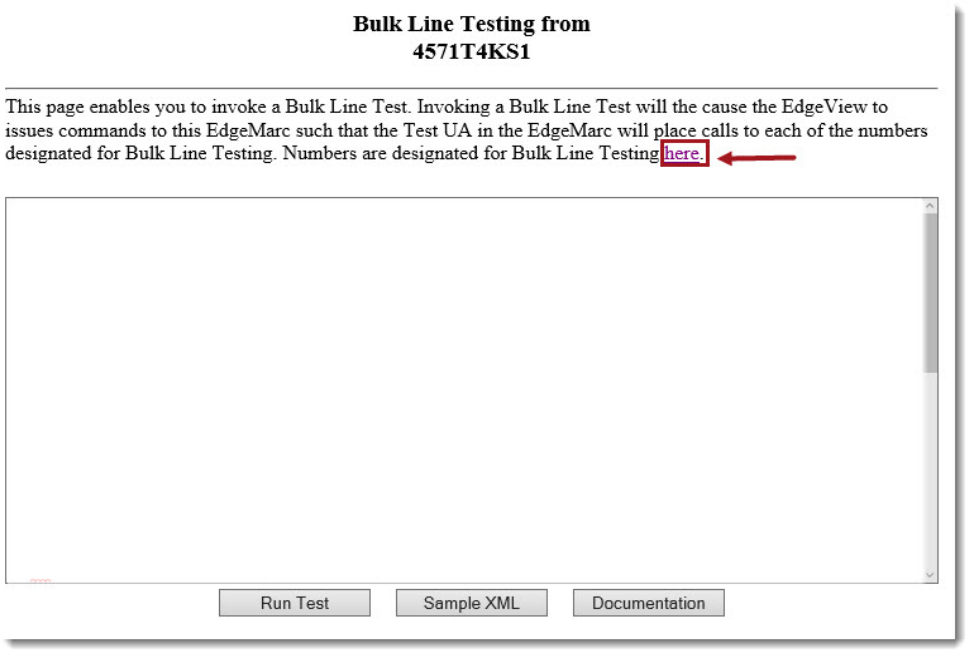
1. Open the EdgeMarc user interface and configure it for a VoIP Test (Figure 8-33). For more details, refer to the *EdgeMarc VoIP Operating System User Guide.*

Figure 8-33 Configuring the EdgeMarc for a VoIP Test



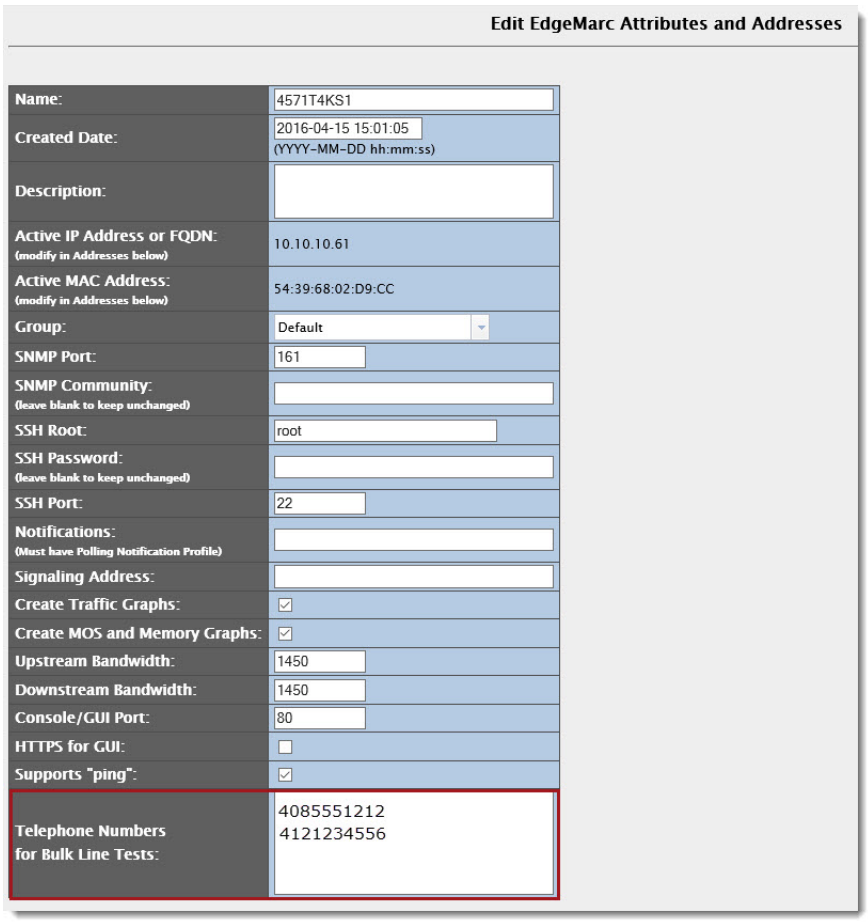
2. Open EdgeView and select the EdgeMarc from the device tree.
3. Select **Analysis > Bulk Line Test**. The Bulk Line Testing page displays (Figure 8-34).

Figure 8-34 Bulk Line Testing Screen



4. Click the **here** link to add phone numbers for the bulk line test. The EdgeView Edit Device page opens (Figure 8-35).

Figure 8-35 Edit EdgeMarc Attributes and Addresses Page



5. Enter phone numbers for the bulk line test and click **Save**. Each phone number must be on a separate line. Therefore, you need to press **Return** after each entry.

Initiating a Bulk Line Test

Once you have enabled TestUA on the EdgeMarc and configured bulk line test settings in EdgeView, click **Run Test** on the Bulk Line Testing page. Depending on how many phone numbers you are testing, it may take several seconds for the test results to display.

Bulk Line Test Output

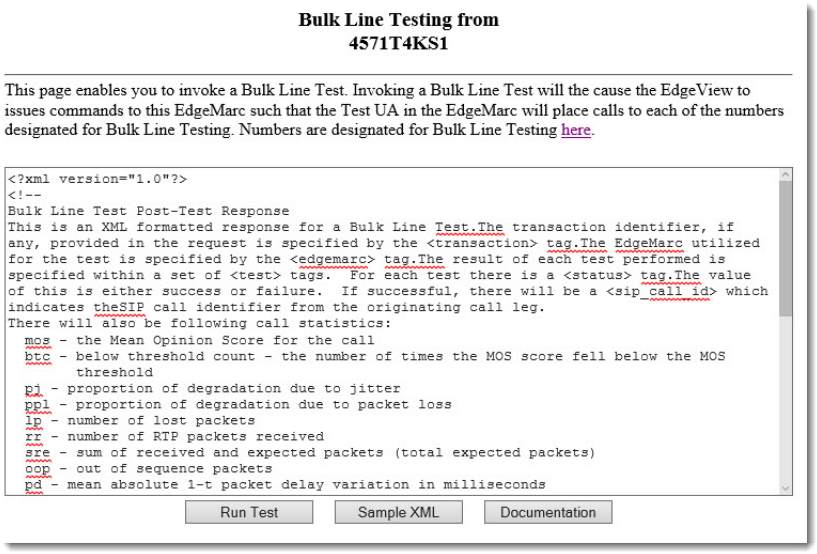
In the bulk line test results, the EdgeMarc utilized for the test is specified by the <edgemarc> tag. The result of each test performed is specified within a set of <test> tags. For each test there is a <status> tag with the value of either success or failure. If successful, there will be a <sip_call_id> which indicates the SIP call identifier from the originating call leg.

The example shown in Figure 8-36 shows the bulk line test results for three phone numbers:

- 5558881031
- 5558881032
- 5556661009

The bulk line test calls to 5558881031 and 5556661009 were successful and call quality statistics are displayed. However, the bulk line test call to 5558881032 failed. Therefore, the <error code> tag containing the SIP error code and an <error_description> tag containing the SIP error message “Command timed out” were displayed.

Figure 8-36 Sample Bulk Line Test Output



The bulk line test tag definitions in Table 8-5 are listed at the top of the Bulk Line Test page. Click the **Documentation** button on the Bulk Line Test page to see additional tag descriptions.

Table 8-5 Bulk Line Test Tag Definitions

Tag	Description
mos	Mean Opinion Score for the call
btc	Below Threshold Count. The number of times the MOS score fell below the MOS threshold.
pj	Proportion of degradation due to jitter
ppl	Proportion of degradation due to packet loss
lp	Number of lost packets
rr	Number of RTP packets received
sre	Sum of received and expected packets (total expected packets)
oop	Out of sequence packets
pd	Mean absolute 1-t packet delay variation in milliseconds
mpj	Maximum positive jitter in milliseconds
mnj	Maximum negative jitter in milliseconds
clp	Maximum number of consecutive lost packets
plb	Average packet loss burst length
rtt	Round-trip delay

Initiating a Bulk Line Test via HTTPS Commands

A bulk line test can be initiated from EdgeView or by sending HTTP commands or HTTPS commands (if you have setup your EdgeView to work as a secure HTTPS server). The HTTP request method has the following format:

```
http://<your EdgeView IP>/ev/cgi-bin/runalt.cgi?<query parameter>
```

For example:

```
http://10.10.10.207/ev/cgi-bin/runalt.cgi?em=EM_222_207&dn=5558881032
```

This would make a call from EM_222_207 to phone number 5559991032.

The following table defines the HTTP query parameters. These are also listed on the EdgeView Bulk Line Test page.

Parameter	Definition
tid	Optional; transaction ID
em	Text string that identifies the EdgeMarc (see note below)
dn	Optional; destination number. If a destination number is not provided, EdgeView will utilize the list of numbers defined for Bulk Line Testing for the specified EdgeMarc.

Parameter	Definition
td	Optional; test duration in seconds
cbip	Optional; default is requesting IP
cbport	Optional; call back port default is 443
cburl	Optional; call back URL. If not specified, test results are returned across the requesting connection.
cbuser	Username for callback authentication
cbpswd	Password for callback authentication

The XML response document will contain the test tags defined previously in Table 8-5. These are also listed on the EdgeView Bulk Line Test page.

EdgeView Troubleshooting Tools

The Troubleshooting function in EdgeView provides an easy way to run EdgeMarc device scripts from within EdgeView to troubleshoot and debug problems. You can run the following EdgeMarc device scripts within EdgeView:

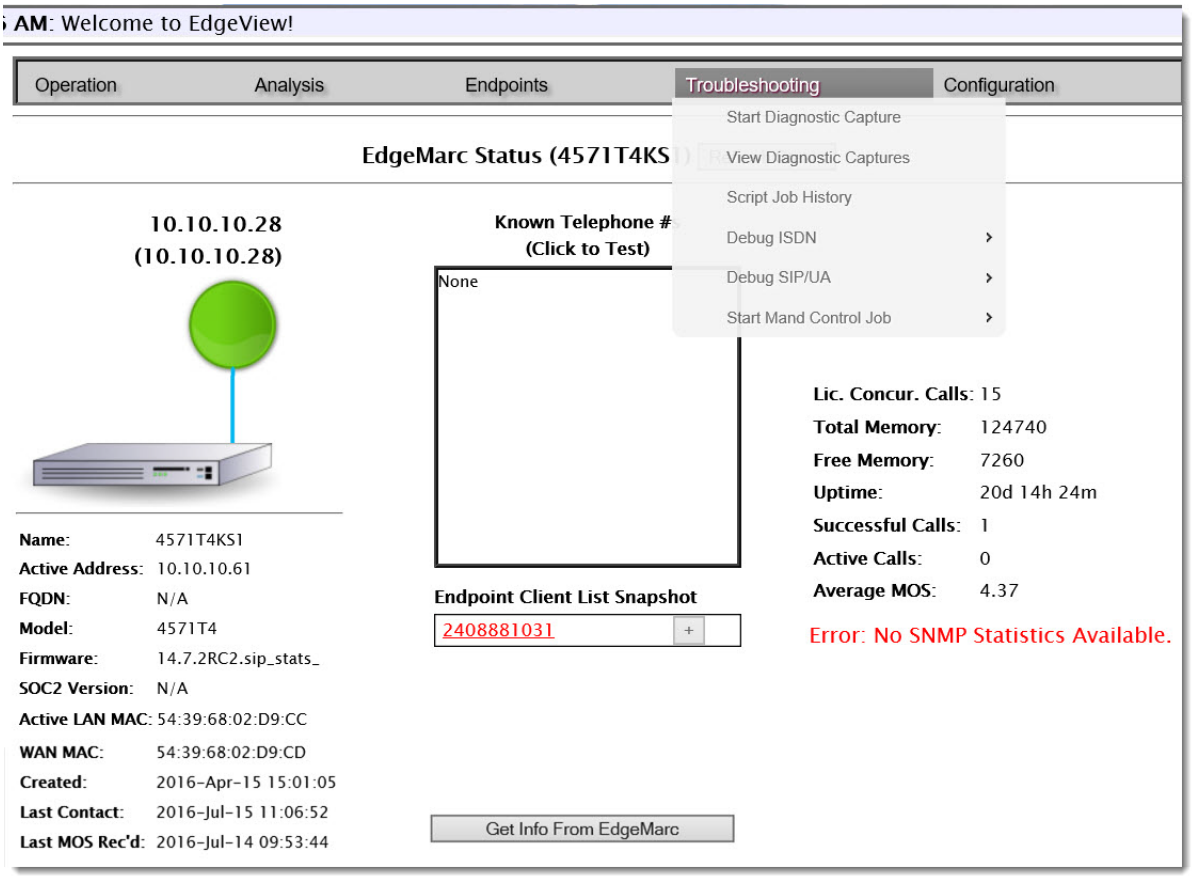
- Debug ISDN
- Debug SIP/UA
- MAND Control Job

Running an EdgeMarc Device Script

To run a device script:

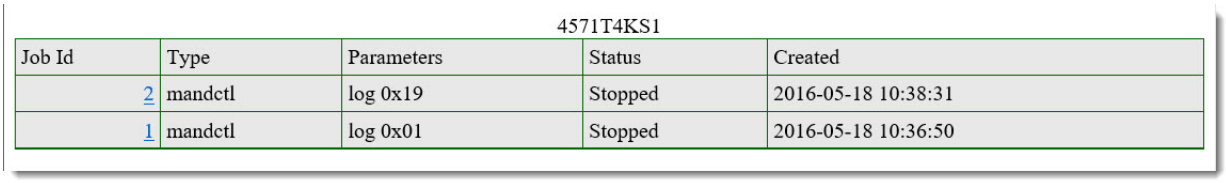
1. Select the EdgeMarc from the device tree and click **Troubleshooting** in the EdgeMarc Status page menu bar (Figure 8-37).

Figure 8-37 Running EdgeMarc Device Scripts in EdgeView



2. Select a device script and then select the desired debug level from the sub-menu. You can run multiple device scripts simultaneously. EdgeView will SSH into the EdgeMarc and issue the debug command associated with the selected device script. The debug output will display in the page as if the page was a terminal that is running the debug command. Table 8-6 lists the available device scripts and associated debug levels.
3. Select **Script Job History** for a list of the device scripts that have been previously run (Figure 8-38).

Figure 8-38 Device Script History



4571T4KS1

Job Id	Type	Parameters	Status	Created
2	mandctl	log 0x19	Stopped	2016-05-18 10:38:31
1	mandctl	log 0x01	Stopped	2016-05-18 10:36:50

Device Script Termination Methods

- Click the **Stop** button to disable the debugging operation while staying on the page.
- All debugging operations terminate after one hour.

Table 8-6 Device Scripts and Debug Levels

Device Script	Debug Level(s)	Description
Debug ISDN	Q921 Layer 1 Q921 Layer 2 Q931	Enables logging for Q921/Q931 debugging. Debug logs are sent to syslog. **Note:** Messages received by the EdgeMarc are marked as MSG received. Messages sent by the EdgeMarc are prefixed with REQ_. For example a SETUP message sent from the EdgeMarc on PRI will be logged as REQ_SETUP.
Debug SIP/UA	ERROR DEBUG SIMPLIFIED DEBUG STACK	The DEBUG option enables debugging for UA without restarting the UA process. This is useful when debugging the current UA state. The SIMPLIFIED DEBUG option reduces the preamble of each log message so that debugs are easy to read for technical support. The STACK option disables logging completely. **Note:** By default, enabling a logging level does not restart UA.
Start Mand Control Job	INFO SIP, INFO RTPSC, SIP, INFO	The INFO option displays only responses to Query commands. If you are not issuing Query commands you will not see any INFO output. The SIP and INFO option displays all debug logs related to SIP processing, in addition to the INFO logging messages. The RTPSC option displays messages for RTP media streams where the signaling is not being processed, in addition to the SIP and INFO logging messages. This is an internal debug command.

Viewing Active Device Script Jobs

Click the **EV System** icon and select **Device Script Jobs** from the EV System menu to display a list of the debug scripts that are currently running for all EdgeMarc nodes (Figure 8-39).

Figure 8-39 Accessing the Device Script Jobs Screen



Remote Phone GUI Access Support

This troubleshooting feature finds and connects to any VoIP phone web GUI that is connected to an EdgeMarc managed by EdgeView using the **Access Web GUI** button. You can also use this feature to access other third-party devices that have HTTP access such as switches.

Note

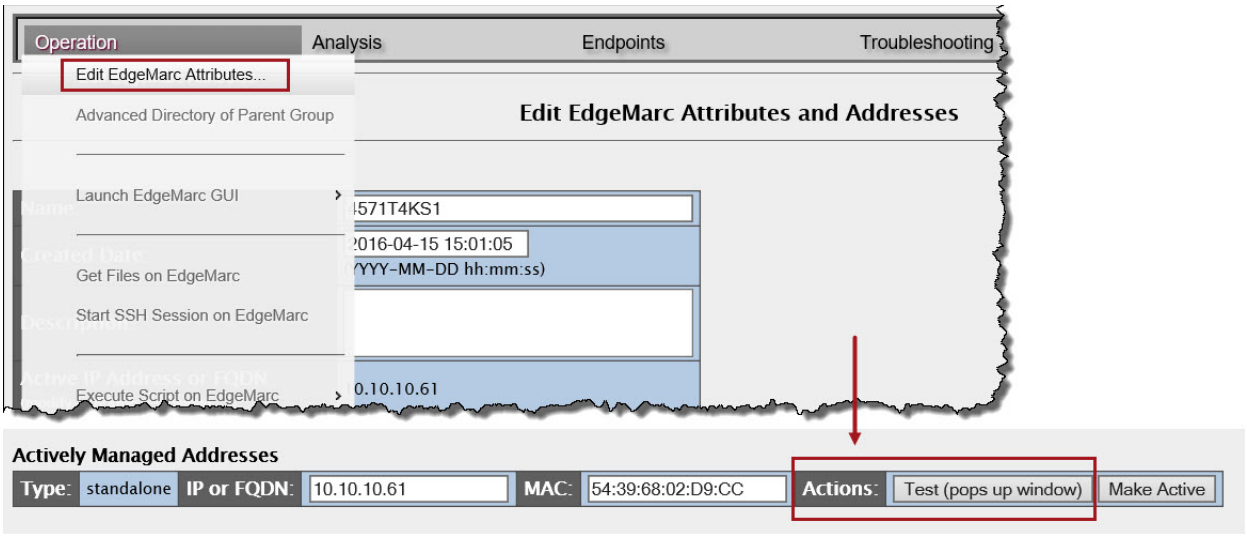
This feature must be licensed before it can be used. Contact Edgewater Networks support.

Testing for SSH

EdgeView must have SSH access to the EdgeMarc. Check the specific EdgeMarc:

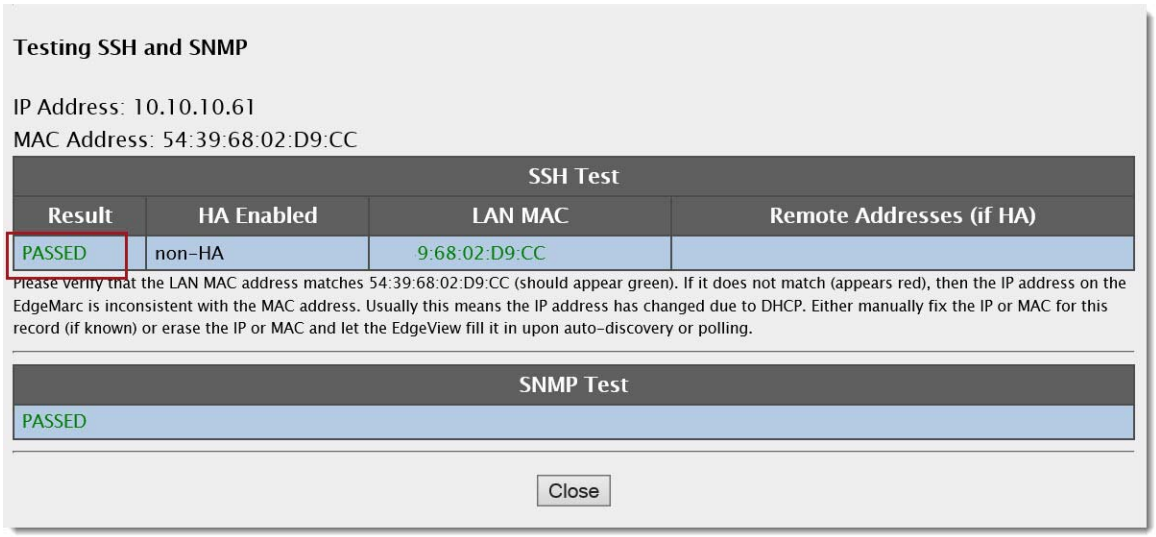
1. Select an EdgeMarc from the Device Tree.
2. Click Operation and select Edit EdgeMarc Attributes from the drop-down menu.
3. Scroll to Actively Managed Addresses and click **Actions** > **Test**.

Figure 8-40 Checking the EdgeMarc SSH Connection



SSH confirmation appears in the SSH Test Result column (Figure 8-41).

Figure 8-41 Testing SSH and SNMP



Configuring a Phone on an EdgeMarc:

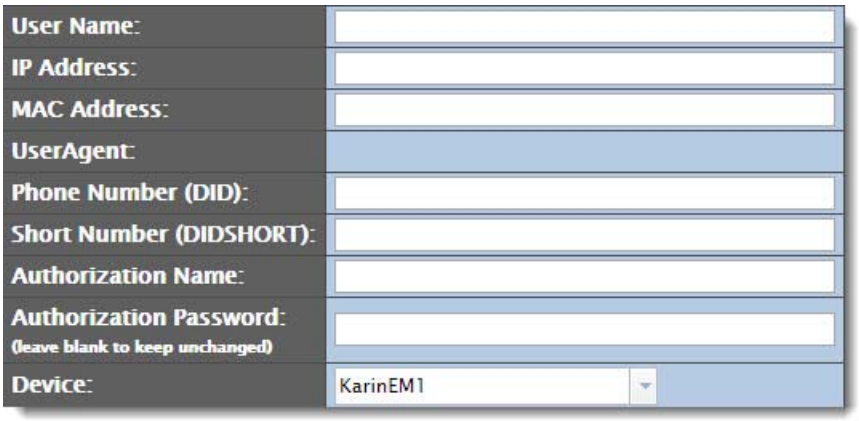
1. From the Device Tree left panel navigation, select an EdgeMarc and go to **Endpoints** > **Add a WAN Phone** (Figure 8-42).

Figure 8-42 Endpoints - Adding a Phone



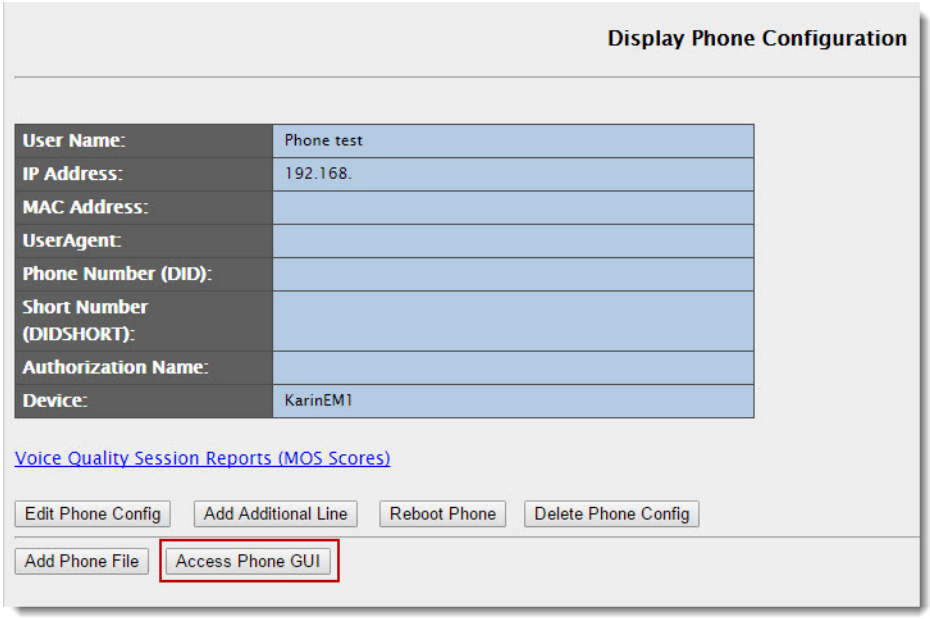
2. The Add Phone Configuration page is displayed. Enter a name for the phone and the phone IP address in the fields provided (Figure 8-43).

Figure 8-43 Add a Phone



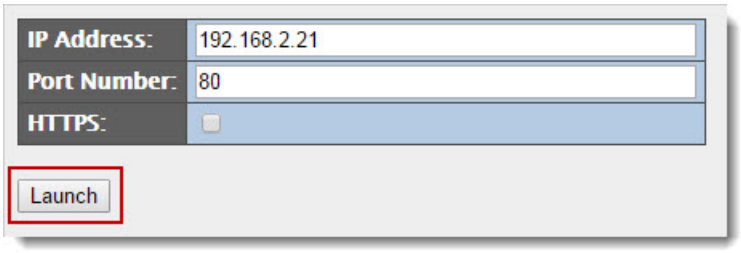
3. Click **Save**. The phone is added to the Device Tree for the selected EdgeMarc.
4. Click the new phone entry in the Device Tree. The Display Phone Configuration page is displayed (Figure 8-44).

Figure 8-44 Display Phone Configuration Page



5. Click **Access Phone GUI**.

Figure 8-45 New Phone Entry



6. Click **Launch**.
7. Enter the phone GUI username and password in the Authentication Required popup window and click **Login**. You are now logged in to the phone's GUI page.

Running a Shell Script on an EdgeMarc

Using EdgeView, you can run a shell script on an EdgeMarc or set of EdgeMarcs in a Group, capture the results or error output, and optionally email the results.

To use this feature, you must first create the script in EdgeView. The script can then be used on any EdgeMarc.

Caution

Running a script on the EdgeMarc can potentially impair EdgeMarc performance or potentially disable the EdgeMarc entirely.

Caution

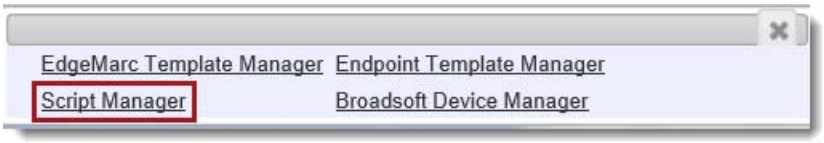
ONLY USERS WITH ADVANCED KNOWLEDGE OR IN A LAB ENVIRONMENT SHOULD USE THIS FEATURE AND ONLY THOROUGHLY TESTED SCRIPTS SHOULD EVER BE DEPLOYED TO A PRODUCTION EDGEMARC!

Creating a Script

To create a script:

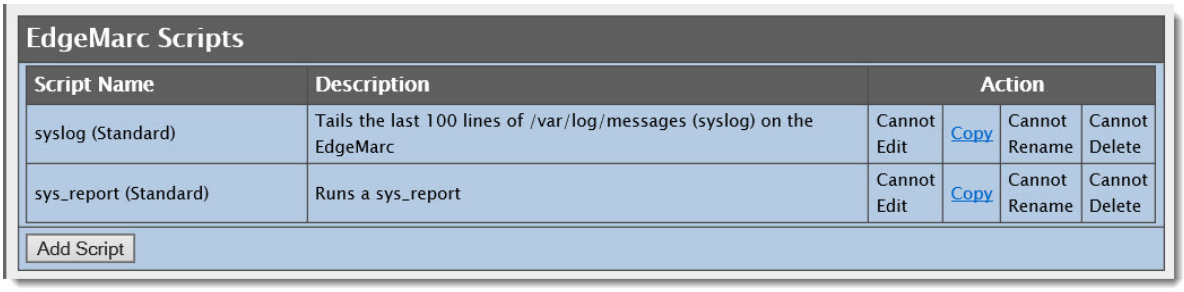
1. Choose an EdgeView from the Device Tree and select **Templates > Script Manager**.

Figure 8-46 Templates Menu



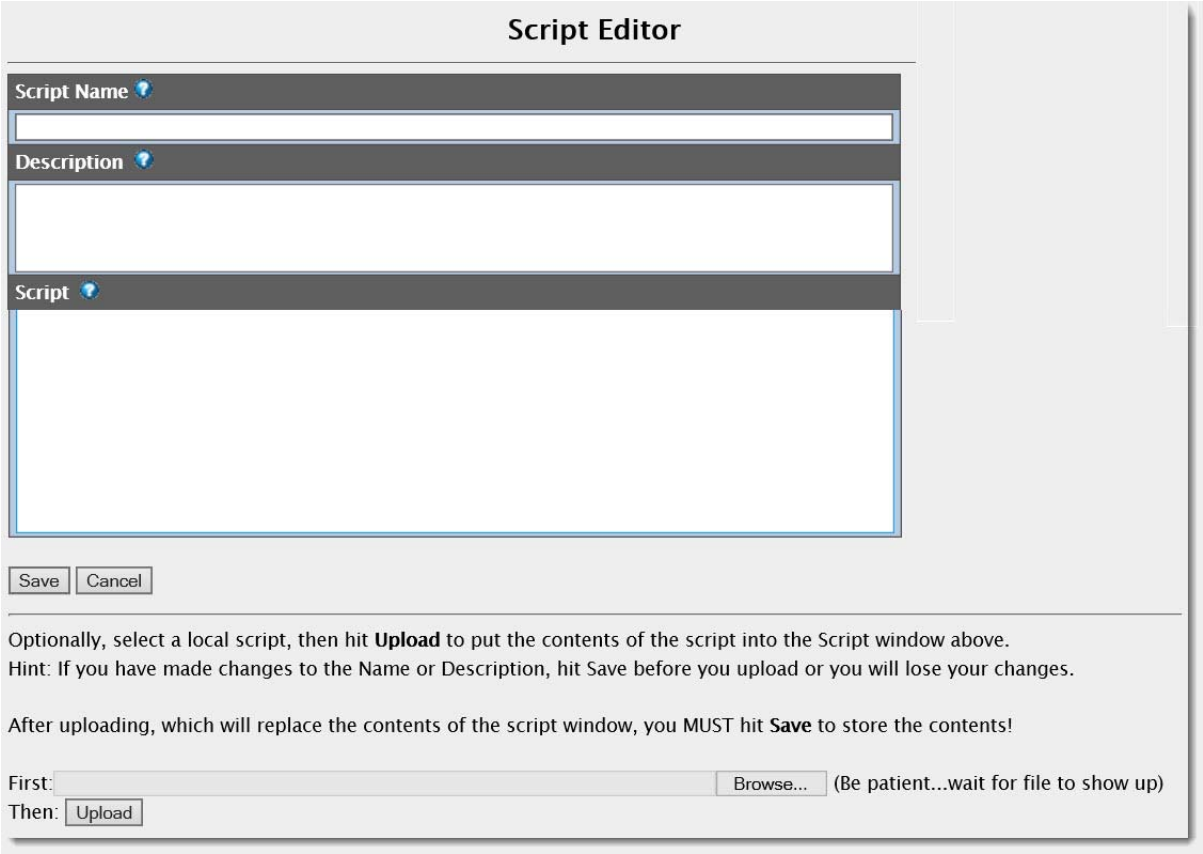
2. Click **Script Manager** to display the EdgeMarc Scripts screen. By default, two scripts are included (syslog (Standard) and sys_report (Standard):

Figure 8-47 EdgeMarc Scripts Screen



3. Click **Add Script**. The Script Editor screen displays (Figure 8-48).

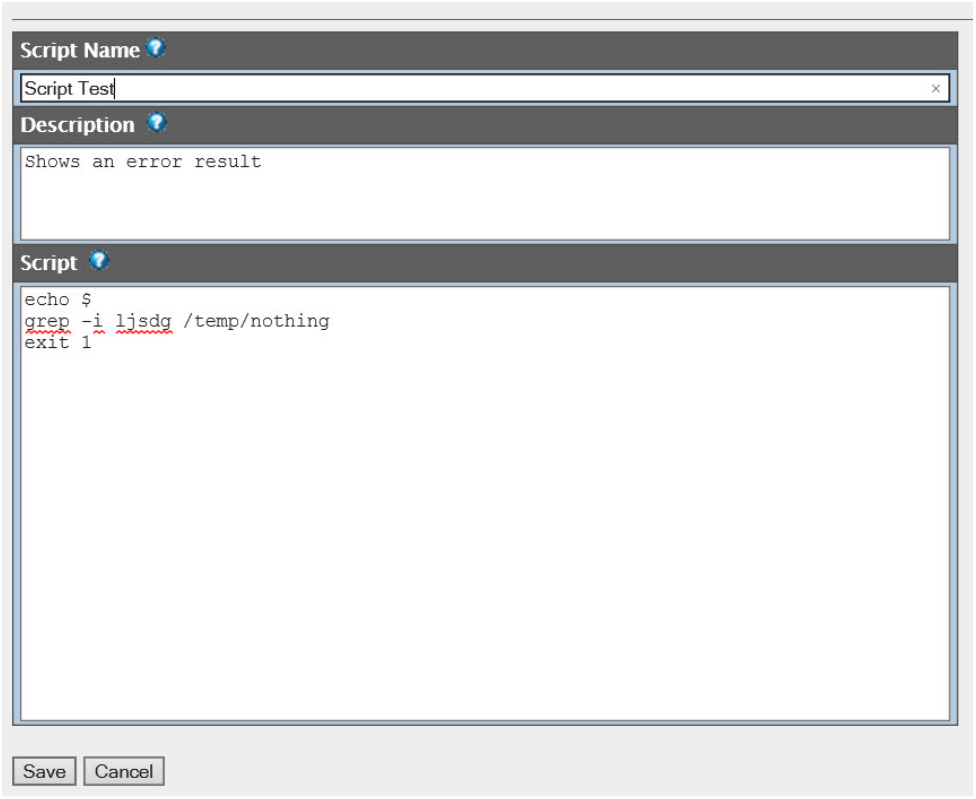
Figure 8-48 Script Editor Screen



4. Under **Script Name**, enter a name you would like to call your script. The script name you enter here will be displayed in the script results. The name must be unique per EdgeView. For example, “show error.”
5. Under **Description**, enter a description of the script. For example, “Shows an error result.”
6. Under **Script**, enter the script commands directly or click **Browse...** to upload an existing shell script from your computer. Click the question mark help icon for instructions on how to upload the script.

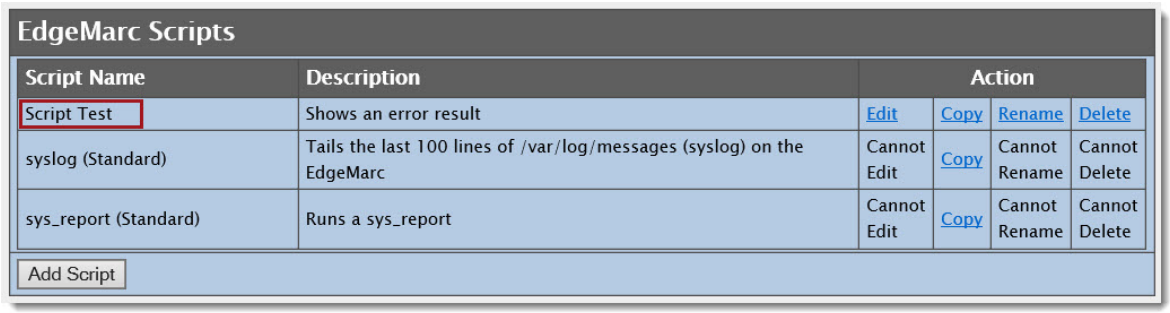
   Figure 8-49 shows an example of the script commands for the “show error” script.

Figure 8-49 Adding a Script



7. When you are satisfied with the script, click **Save** to save the script in EdgeView. A message indicates that the script was saved successfully.
8. Select **Click Here to Return to the Main Script Page.** The "show error" script will now be displayed in the list of scripts (Figure 8-50).

Figure 8-50 Adding the Show Error Script



Editing, Copying, Renaming, and Deleting a Script

Once you have added a script, you can edit, copy, rename and delete it at any time as follows.

To edit a script:

1. Click **Edit**.
2. Type new values for the **Name**, **Description**, and/or **Script.**
3. Click **Save**.

To copy a script:

1. Click **Copy**. The script name will appear in the script list with a number appended to the name. For example, “show error_1.”
2. Click **Save**.

To rename a script:

1. Click **Rename**.
2. Type a new name for the script.
3. Click **Submit Name Change**.
4. Click **Save**.

To delete a script:

1. Click **Delete**.
2. Confirm the deletion.
3. Click **Save**.

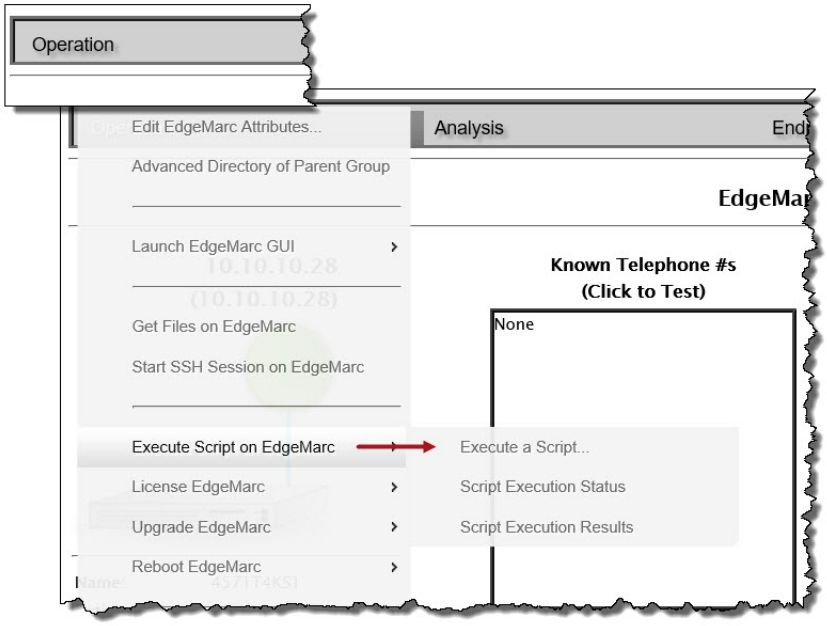
Executing a Script on an EdgeMarc

Once you have created a script, you can execute the script, with optional arguments, on any EdgeMarc currently managed by EdgeView.

To execute the script:

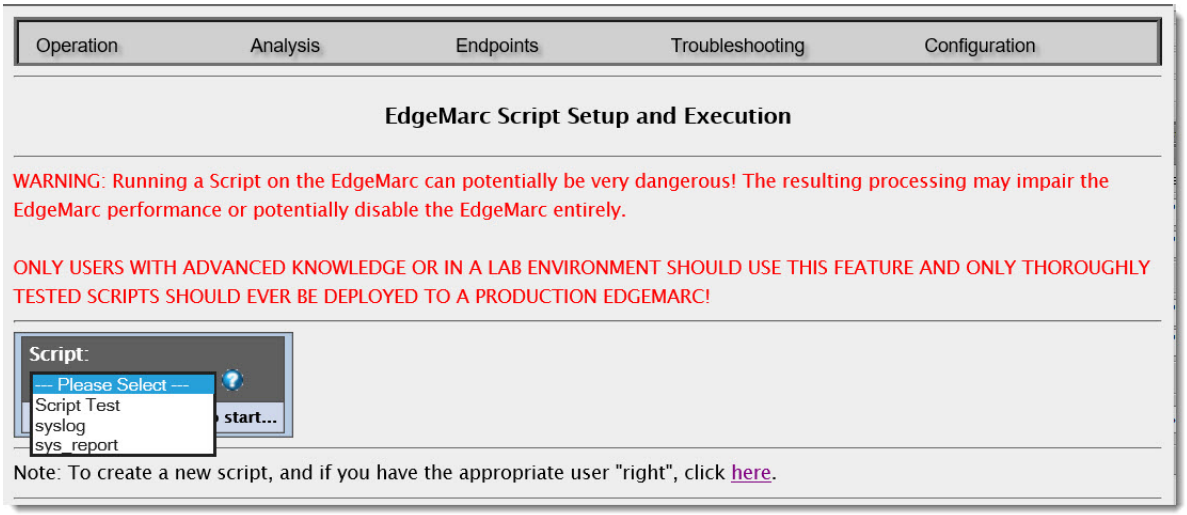
1. In EdgeView, select an EdgeMarc or Group from the device tree.
2. Select the **Operation** menu (if you selected an EdgeMarc) or the **Node Operations** menu (if you selected a group of EdgeMarcs).
3. Select **Execute Script on EdgeMarc** or **Execute Script** (Figure 8-51).

Figure 8-51 Executing a Script



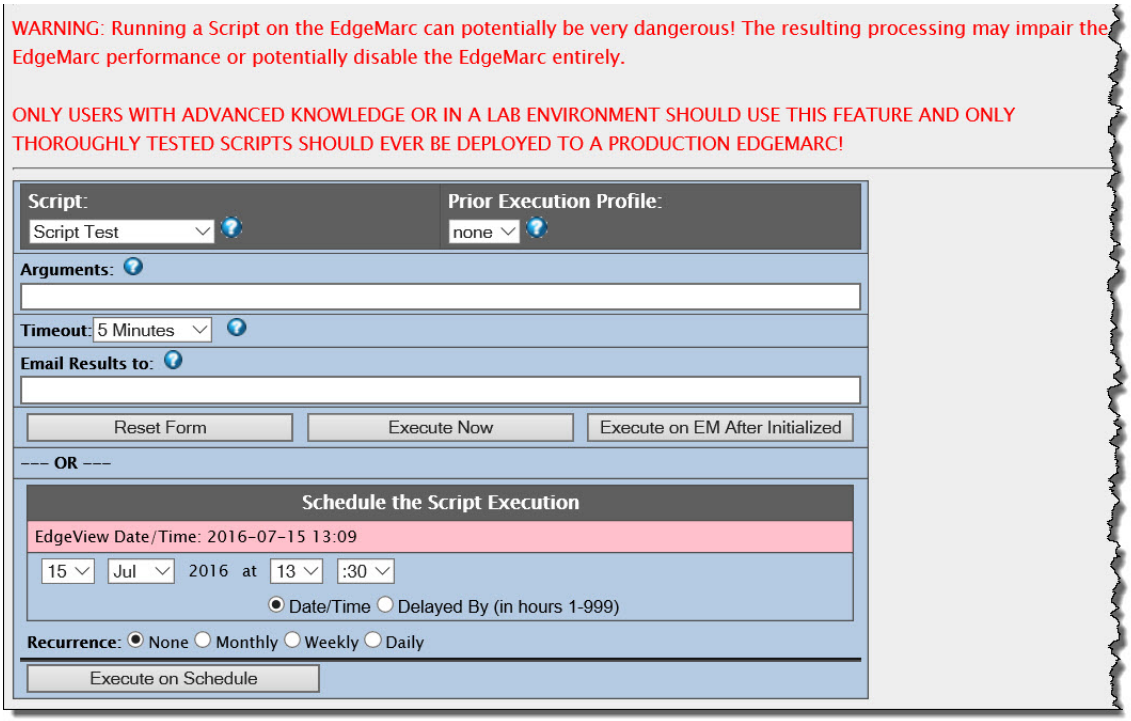
4. In the EdgeMarc Script Setup and Execution page, select the script from the drop-down menu (Figure 8-52).

Figure 8-52 Selecting a Script



Once you select the script, the rest of the web page displays (Figure 8-53).

Figure 8-53 EdgeMarc Script Setup and Execution Web Page



5. Set options for running the script in the EdgeMarc Script Setup and Execution page as follows:

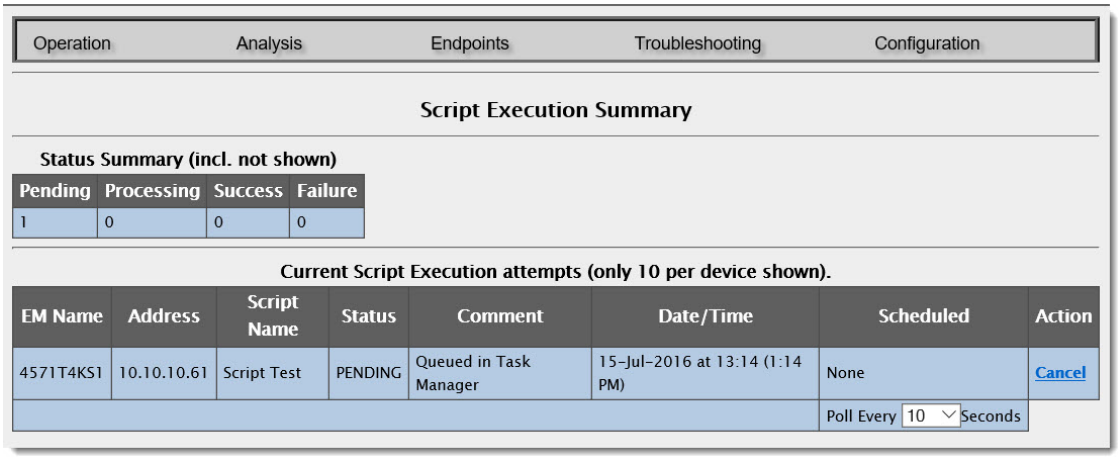
Option	Description
Script	Name of script you selected from the Script drop-down menu.
Prior Execution Profile	Select this option to run a script on the same EdgeMarc or Group using the same arguments, timeout and email addresses used previously.
Arguments	Enter any arguments you would pass into the script. The script must be written in a way to accept these values. Note that arguments with spaces need to be delimited by quotes.
Timeout	Enter the maximum time the script should be allowed to run and complete. The default is five (5) minutes. Increase or decrease the timeout value depending on how long you think the script will take to run.
Email Results to	Enter any email addresses to which you want to send the results. Note that you can always access the report later through the EdgeView web interface (up to 1 year).
Reset Form	Clears the current settings on the page.
Execute Now	Click to execute the script immediately.

Execute on EM after Initialized	Click to set options for executing a script on a pre-provisioned EdgeMarc. See Executing a Script on a Pre-Provisioned EdgeMarc.
Schedule the Script Execution	Set the date and time that you want the script to be executed. You can also set a delay period (in hours) for executing the script.
Recurrence	Select a frequency for running the script: **None**, **monthly**, **weekly**, **daily**. If you want to run the script just this one time, select **None** (the default).
Execute on Schedule	Click to execute the script according to the script execution schedule.

6. When you click **Execute Now**, a warning dialog box will display to warn you of the possible consequences of running the script. Read the warning and click **OK**. The Script Execution Summary page displays (Figure 8-54).

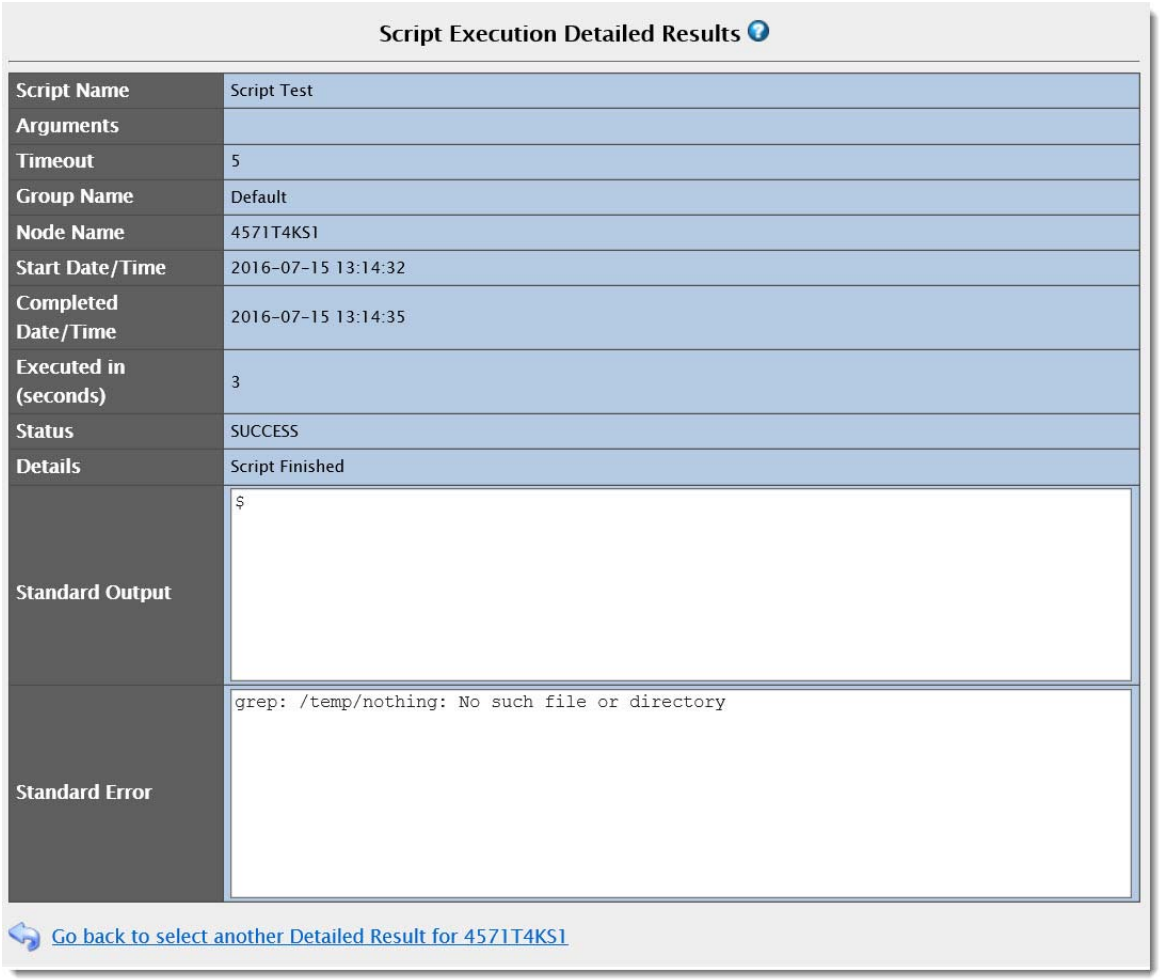
   As the script is running, the status is displayed in the Script Execution Summary screen. The status is polled every 10 seconds by default.

Figure 8-54 Script Execution Summary Screen



7. Once the script completes, you can click on the **Results** link in the Actions column to see the report (Figure 8-55).

Figure 8-55 Script Execution Detailed Results

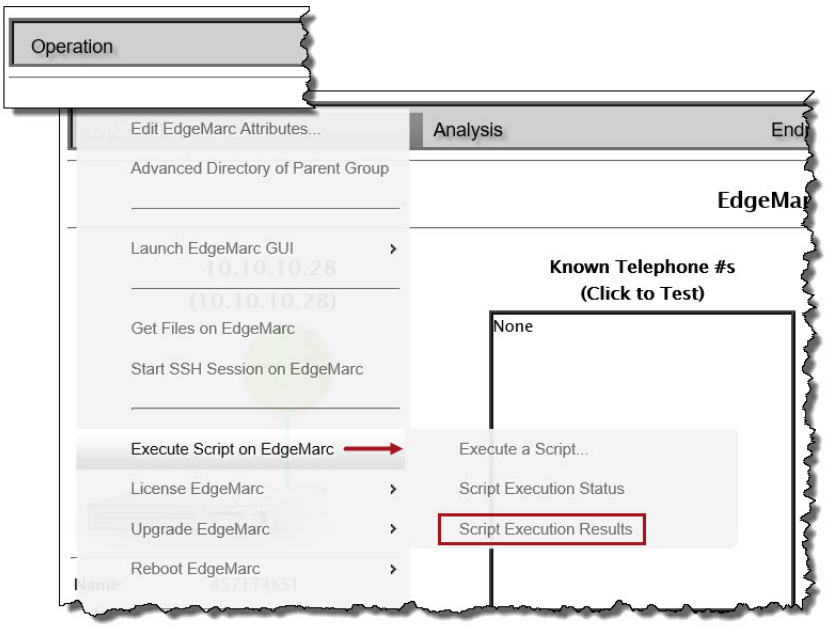


Viewing the Script Results

To view the current and previous results from running a script:

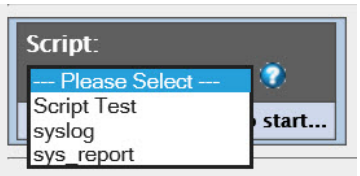
1. Select the EdgeMarc or Group in the Device Tree.
2. Select **Operations** (or **Node Operations**) > **Script Execution Results** (Figure 8-56).

Figure 8-56 Script Execution Results (EdgeMarc)



3. In the Script Execution Details Results screen, select the script from the drop down box (Figure 8-57).

Figure 8-57 Selecting an Executed Script



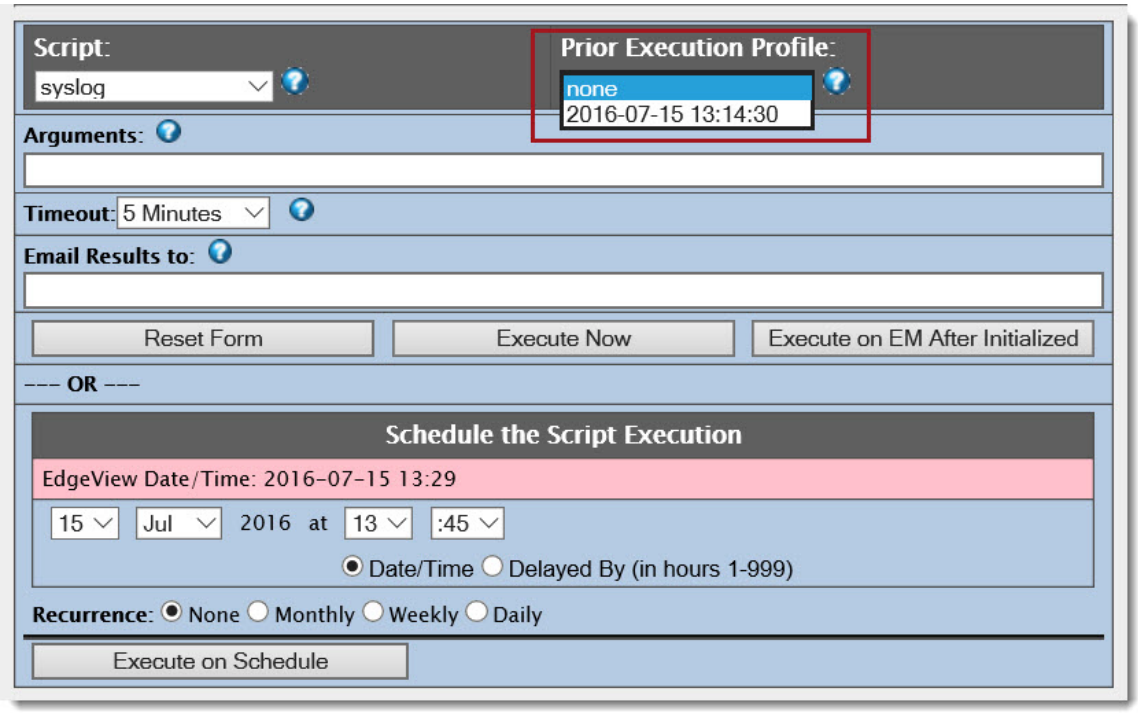
Running a Script Using Previous Settings

You can run the script on the same EdgeMarc or Group using the “Prior Execution Profile” option on the EdgeMarc Script Setup and Execution screen. EdgeView remembers the arguments, timeout, and email addresses that were used the last time you ran the script.

To execute the script:

1. In EdgeView, select the EdgeMarc or Group from the device tree.
2. Select the **Operation** menu (if you selected an EdgeMarc) or the **Node Operations** menu (if you selected a group of EdgeMarcs).
3. Select **Execute Script on EdgeMarc** or **Execute Script**.
4. Select the script from the Prior Execution Profile drop down box (Figure 8-58).

Figure 8-58 Selecting a Prior Execution Profile



5. The options that were used the last time the script ran will already be set on the screen. You can change them if desired.
6. When the script completes, the details will be displayed in the Script Execution Summary screen.

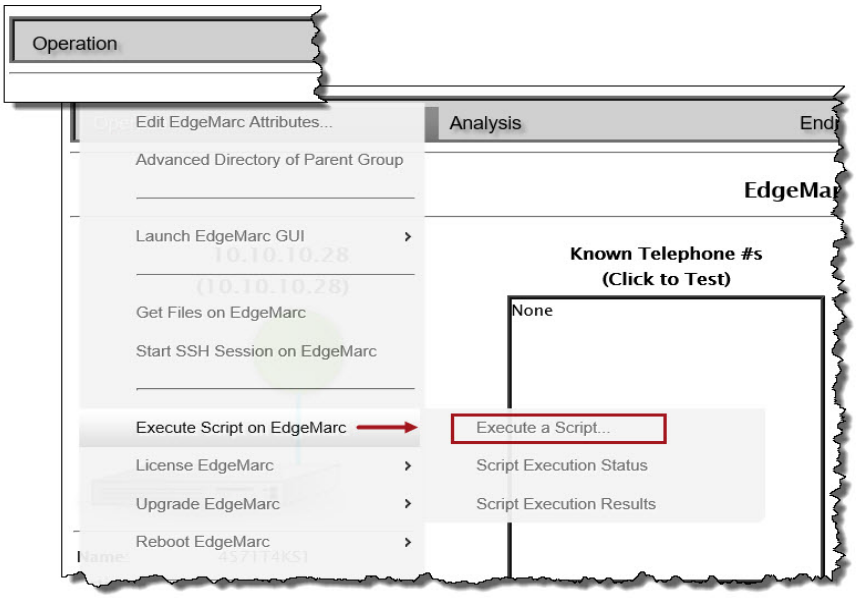
Executing a Script on a Pre-Provisioned EdgeMarc

Similar to configuration push feature, if you have an EdgeMarc that is pre-provisioned (no IP address) you can configure EdgeView to execute a script on an EdgeMarc as soon as it comes online. Once the EdgeMarc is in the Syslog, EdgeView looks for any scripts that match the EdgeMarc MAC address and executes any scripts that are pending for that EdgeMarc.

To execute a script on an EdgeMarc after initialization:

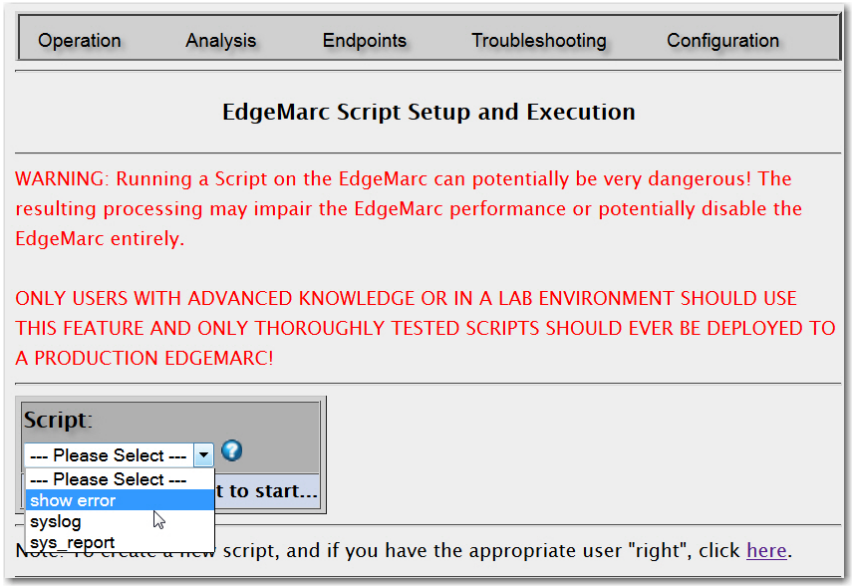
1. Select an EdgeMarc from the device tree and select **Operation > Execute a Script on EdgeMarc > Execute a Script** (Figure 8-59).

Figure 8-59 Executing a Script on the EdgeMarc



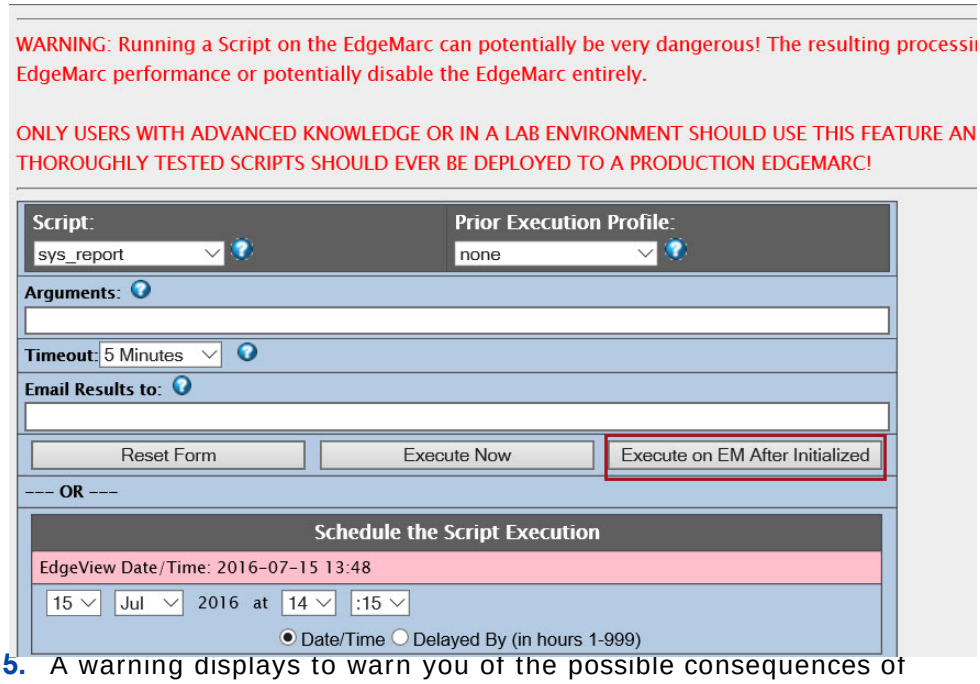
2. Select a script in the EdgeMarc Script Setup and Execution screen (Figure 8-60).

Figure 8-60 Selecting a Script



3. If necessary, enter any arguments, a new Timeout, and email addresses where you want to email the report results.
4. Select **Execute on EM After Initialized** (Figure 8-61).

Figure 8-61 Selecting Execute on EM After Initialized



5. A warning displays to warn you of the possible consequences of executing the script. Read the warning and click **OK**.
6. Once the EdgeMarc comes online and the script completes, you can click on the **Results** link in the Actions column to see the report.

Web Services to Support Running a Shell Script on the EdgeMarc

The following Web Services are available to run a shell script on the EdgeMarc:

- ExecuteScript
- ExecuteScriptStatus
- ExecuteScriptStatusGetIDs
- ExecuteScriptOutput
- ExecuteScriptOutputGetIDs

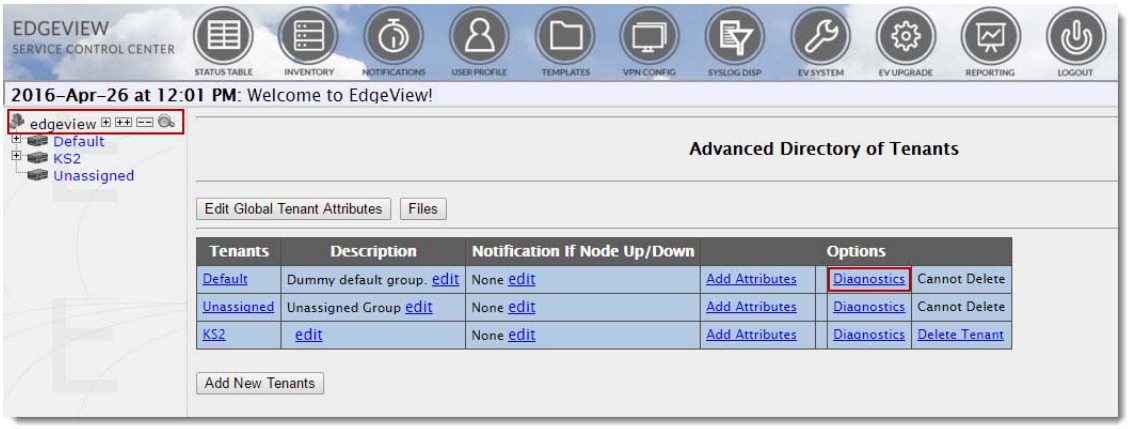
See the WSDL and Example scripts in the *EdgeView Web User Guide Services Guide* for details or contact your support representative for assistance.

Automatic Trigger Diagnostics Support

EdgeView automatic trigger setup can be easily accessed from the main Tenants screen:

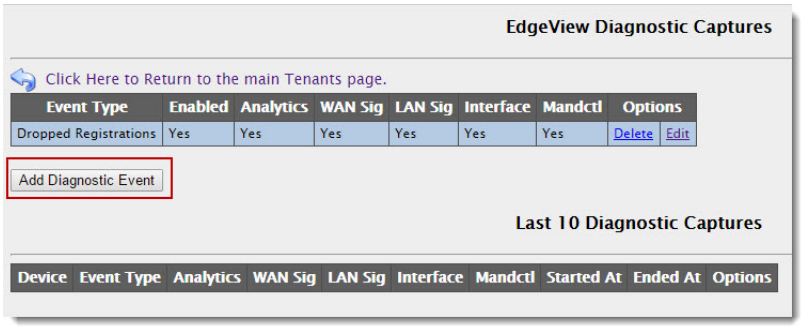
1. Click the EdgeView top level tree option on the left side navigation. The Advanced Directory of Tenants page is displayed (Figure 8-62).

Figure 8-62 Advanced Directory of Tenants



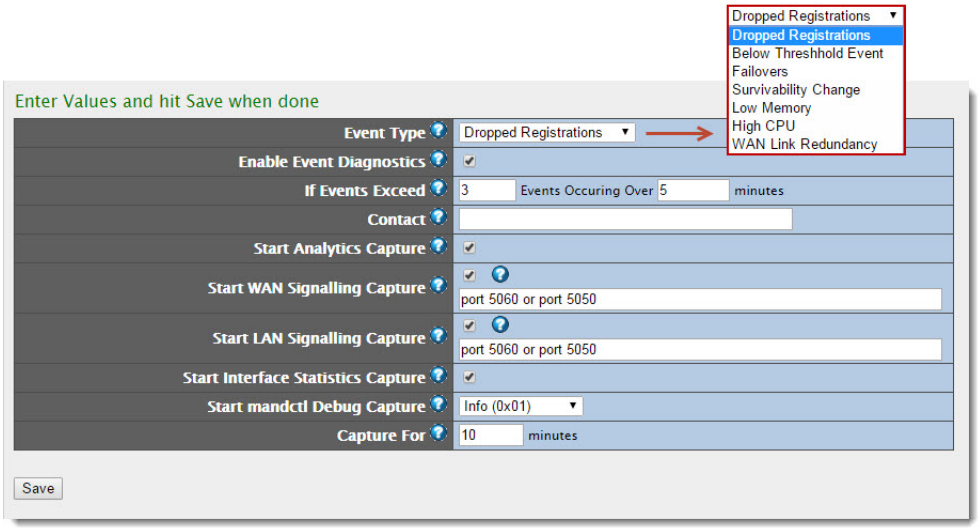
2. In the Options menu click **Diagnostics**. The EdgeView Diagnostic Captures page is displayed (Figure 8-63).

Figure 8-63 EdgeView Diagnostic Captures



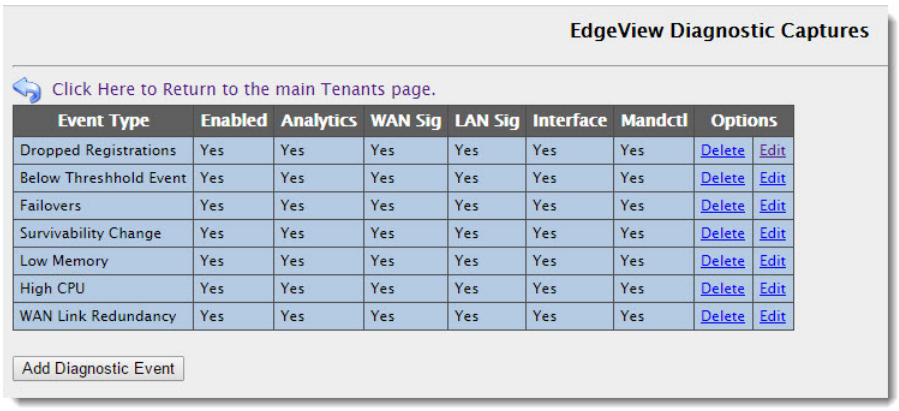
3. Click **Add Diagnostics** to add a diagnostic event (Figure 8-64).

Figure 8-64 Add a Diagnostic Event



4. Choose a diagnostic event from the **Event Type** drop-down menu:
   - Dropped Registrations
   - Below Threshold Count
   - Failovers
   - Survivability Change
   - Low Memory
   - High CPU
   - WAN Link Redundancy
5. Enter information as needed in the fields provided and click **Save**. Configured events appear in the Event table (Figure 8-65).

Figure 8-65 Tenant Diagnostics Event Table



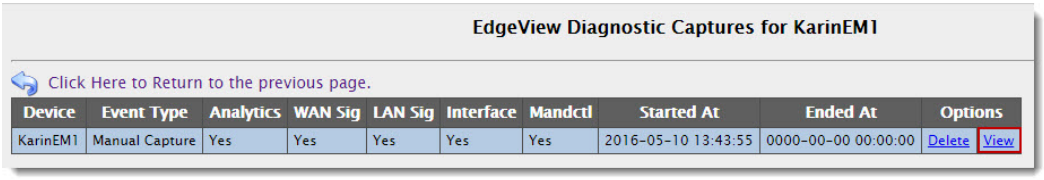
Event Type	Enabled	Analytics	WAN Sig	LAN Sig	Interface	Mandctl	Options	
Dropped Registrations	Yes	Yes	Yes	Yes	Yes	Yes	Delete	Edit
Below Threshhold Event	Yes	Yes	Yes	Yes	Yes	Yes	Delete	Edit
Failovers	Yes	Yes	Yes	Yes	Yes	Yes	Delete	Edit
Survivability Change	Yes	Yes	Yes	Yes	Yes	Yes	Delete	Edit
Low Memory	Yes	Yes	Yes	Yes	Yes	Yes	Delete	Edit
High CPU	Yes	Yes	Yes	Yes	Yes	Yes	Delete	Edit
WAN Link Redundancy	Yes	Yes	Yes	Yes	Yes	Yes	Delete	Edit

Once an event is triggered, an email is (optionally) sent to the person indicated in that screen. The email also has a direct link to the associated Dashboard page.

To start or view diagnostic captures:

1. Click the **Status Table** button.
2. Select the EdgeMarc for which you want to see diagnostics.
3. Click **Troubleshooting** > **Start Diagnostics Capture**.
4. Click **Troubleshooting** > **View Diagnostic Capture** (Figure 8-66).

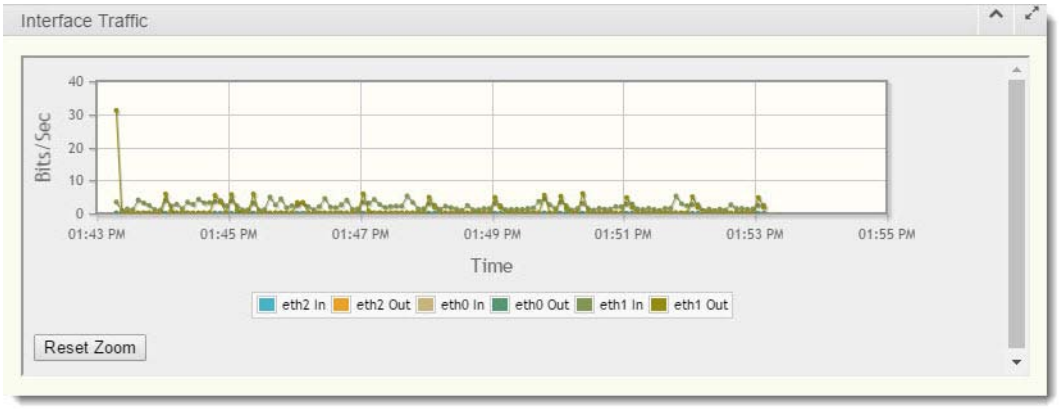
Figure 8-66 View Diagnostic Capture



Device	Event Type	Analytics	WAN Sig	LAN Sig	Interface	Mandctl	Started At	Ended At	Options	
KarinEM1	Manual Capture	Yes	Yes	Yes	Yes	Yes	2016-05-10 13:43:55	0000-00-00 00:00:00	Delete	View

5. In the Options column, click **View**. The EdgeView Diagnostics page is displayed with graphs and other report information for the following:
   - Interface Traffic
   - Memory, CPU Usage and Calls
   - SIP Info Messages
   - System Report
   - WAN and LAN Signaling Ladder
   - MOS Analysis
   - mandctl Logs

Figure 8-67 EdgeView Diagnostics Information - Interface Traffic



Signaling Capture Support

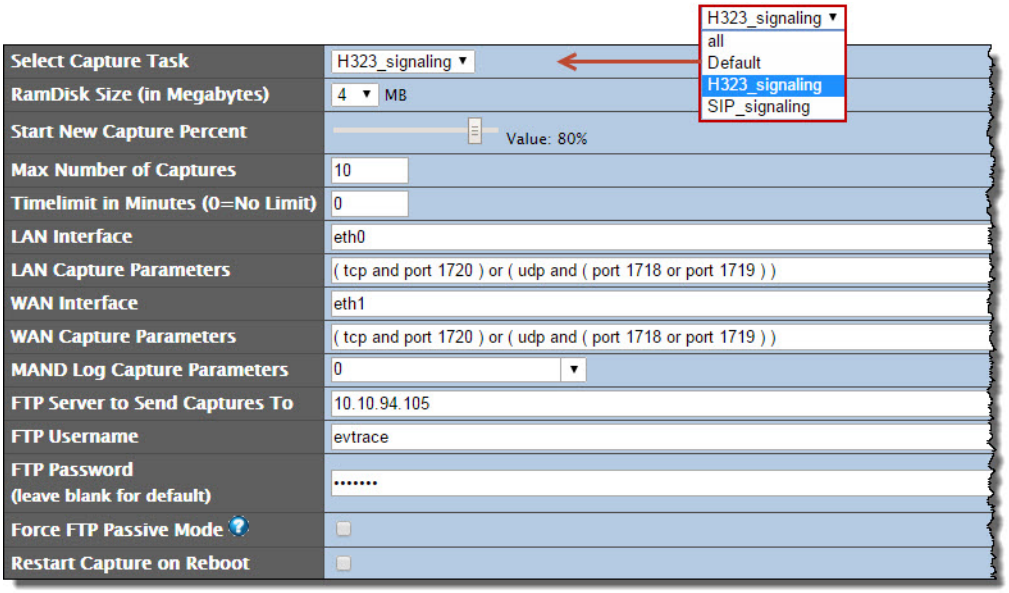
- Auto Populate for Signal Captures
- Generating mandctl Logs

Auto Populate for Signal Captures

Signaling Capture now has several options that autopopulate the search fields on the page. Choose **Analysis** > **SIP Signaling Capture** and select one of the following options from the **Select Capture Task** drop-down menu:

- All
- Default
- H323_signaling (Figure 8-68)
- SIP_signaling

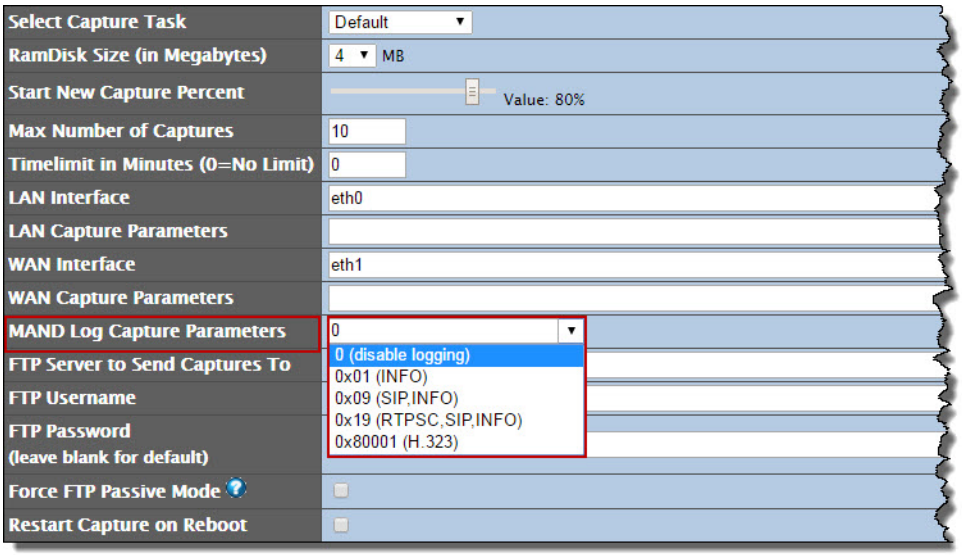
Figure 8-68 Select Capture Task—H323 Signaling



Generating mandctl Logs

Signaling Capture now has an option for generating mandctl logs. When taking captures, these logs are reported in the **Analysis** > **SIP Signaling Capture** MAND Log Capture Parameters field (Figure 8-69). You can type any value into the **MAND Log Capture Parameters** field, you are not limited to the drop-down menu defaults. For example, you can include both SIP and H.323 by entering “0x80019.”

Figure 8-69 Mand Log Capture Parameters



9

EdgeView Upgrade

This section provides instructions for:

- Performing a Minor or Patch Upgrade
- Performing a Full Upgrade

Contact Edgewater support for information about High Availability.



Caution

Use the **EV Upgrade** > **Migrate** feature with Edgewater support.

Performing a Minor or Patch Upgrade



Caution

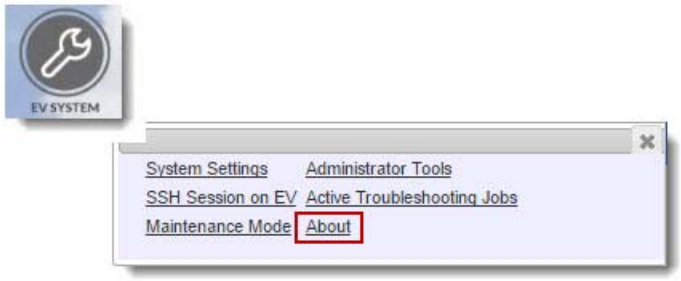
Patches cannot be rolled back.

Performing a minor or patch upgrade on EdgeView replaces only those files that are necessary to satisfy a bug fix or enhancement. This differs significantly from a full upgrade of EdgeView where the entire distribution is downloaded and replaced. Be sure to read the description for each patch to assess the potential service impact. For example, some patches may strongly advise that you install them during a maintenance window. As always, a full backup of the system should be performed before any patch or upgrade.



Verifying the Current EdgeView Software Version and Patches

1. Log in to EdgeView.
2. Click the **EV System** icon and select **About** to verify which version of software is installed on EdgeView.



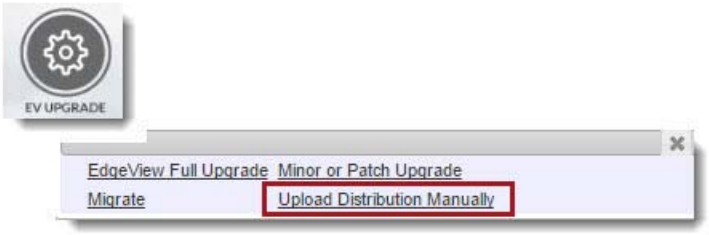


3. Verify which patches have been installed on EdgeView since the last upgrade:
   a. Click the **EV Upgrade** icon and select **Minor or Patch Upgrade**.
   b. Click **Check for Patches on Server**. A list of the patches which have been installed since the last upgrade will appear at the bottom of the screen.

Starting a Minor or Patch Upgrade

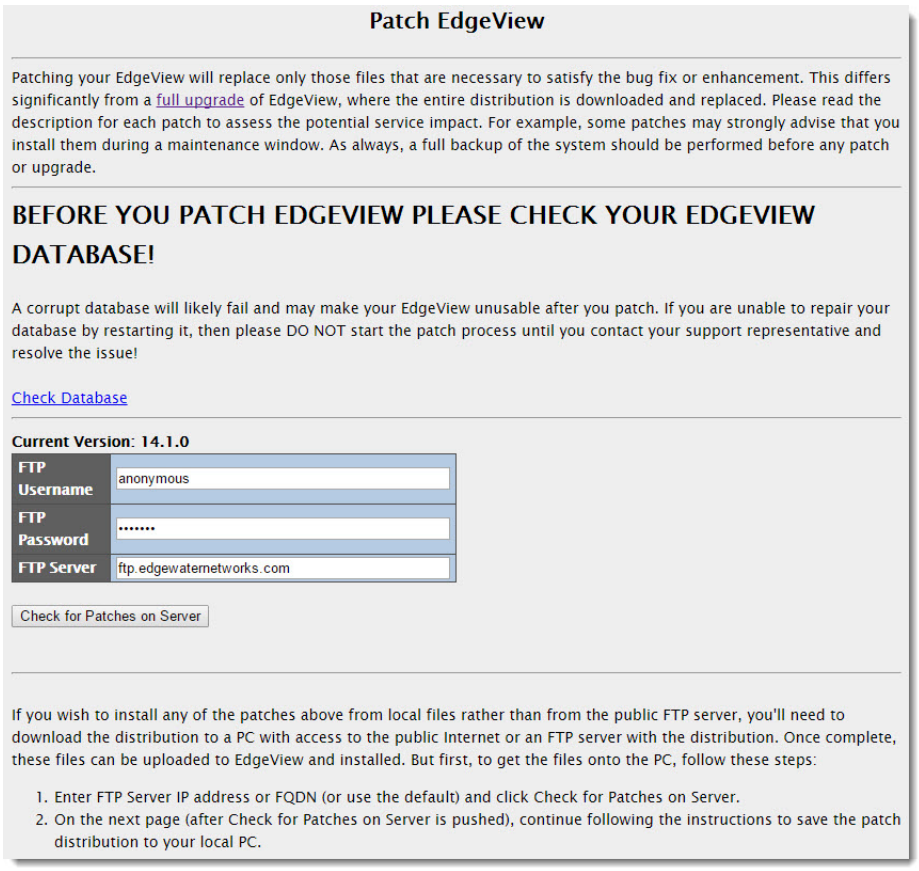
Before you begin the patch upgrade, refer to the release notes that accompany each EdgeView release for the patch upgrade file names and special instructions. It is also recommended that you put EdgeView in maintenance mode. See Using Maintenance Mode.

1. Click the **EV Upgrade** icon:



2. In the **EV Upgrade** sub-menu, select **Minor or Patch Upgrade**. This opens the Patch EdgeView screen shown in Figure 9-1.

Figure 9-1 Patch EdgeView Screen



3. HIGHLY RECOMMENDED: On the Patch EdgeView page, click **Check Database** to verify all the database tables are clean and not corrupt.



Caution

With a corrupt database, the upgrade/patch will likely fail and may make your EdgeView unusable. DO NOT start the patch process until you contact your Edgewater Networks support representative and resolve the issue.



Note

On HA systems be sure to check both sides of the HA pair.

1. In the Patch EdgeView screen, use the default settings. If the distribution is on an FTP server other than the default ftp.edgewaternetworks.com, enter the FTP server IP Address or Fully Qualified Domain Name (FQDN) in the FTP Server box.

   You can also install the patch from local files. Refer to Downloading the Patch Files to a Local Computer.

2. Click **Check for Patches on Server**.

3. Click **Apply Patch** in the Action column for the patch. The patch will automatically begin installing. A status box will display on the screen to show the installation progress. When the installation is complete, the status box will indicate “Patch Finished” in the **Details** field.

Downloading the Patch Files to a Local Computer

To install a patch from local files rather than from the public FTP server, you will need to download the distribution to a computer with access to the public Internet or an FTP server with the distribution. There are three files in the distribution:

<xx.x.x.patch< >.ev

<xx.x.x.patch< >.sh

<xx.x.x.patch< >.tgz

where **xx.x.x.patch< >** is the patch release number

Once complete, these files can be uploaded to EdgeView and installed.



Note

If you are downloading the distribution from the ftp.edgewaternetworks.com server, you need to specify the binary mode.

1. On the Patch EdgeView screen, enter the FTP Server IP address or the FQDN (or use the default) and click **Check for Patches on Server**.
2. On the next page (after you click **Check for Patches on Server**), follow the instructions to save the patch distribution to your computer.

Manually Uploading a Software Patch

If your EdgeView is behind a Firewall, you can manually upload a software patch in one of two ways:

- Upload the files directly to the /tmp directory in EdgeView using scp or ftp (if enabled for EdgeView). This is known as the *Direct Upload method*.

  Or

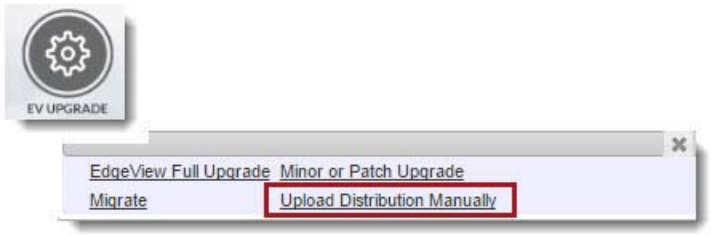
- Use the browser to upload the files. This is known as the *Browser method*.

Which method should you use?

If you have a simple patch to install, use the Browser method. For larger uploads, such as a full upgrade, use the Direct Upload method as the browser may time out.

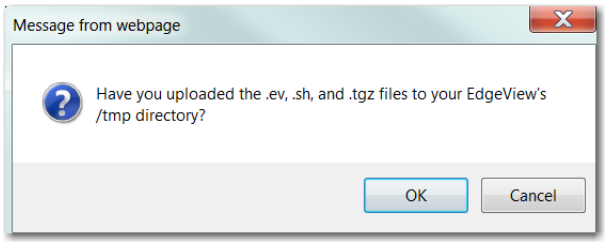
Manually Installing a Minor Upgrade or Patch via Direct Upload

1. Download all three files in the patch distribution to your local drive. Refer to Downloading the Patch Files to a Local Computer.
2. Use any standard scp or ftp application to upload the files to the EdgeView /tmp directory.
3. Once the files are uploaded, click the **EV Upgrade** icon and select **Upload Distribution Manually** from the sub-menu:



The Upload to EdgeView screen displays.

4. Click on the **Install From Direct Upload button**. The following dialog box will display to remind you to upload the upgrade files:



Note

You must use scp or ftp to upload the files before installing the distribution onto your EdgeView. If you are unsure how to do that, contact your support representative.

The files will be installed on EdgeView as if you had done it directly through the network.

5. To verify that the patch is installed on EdgeView, click the **EV System** icon and select **About**.

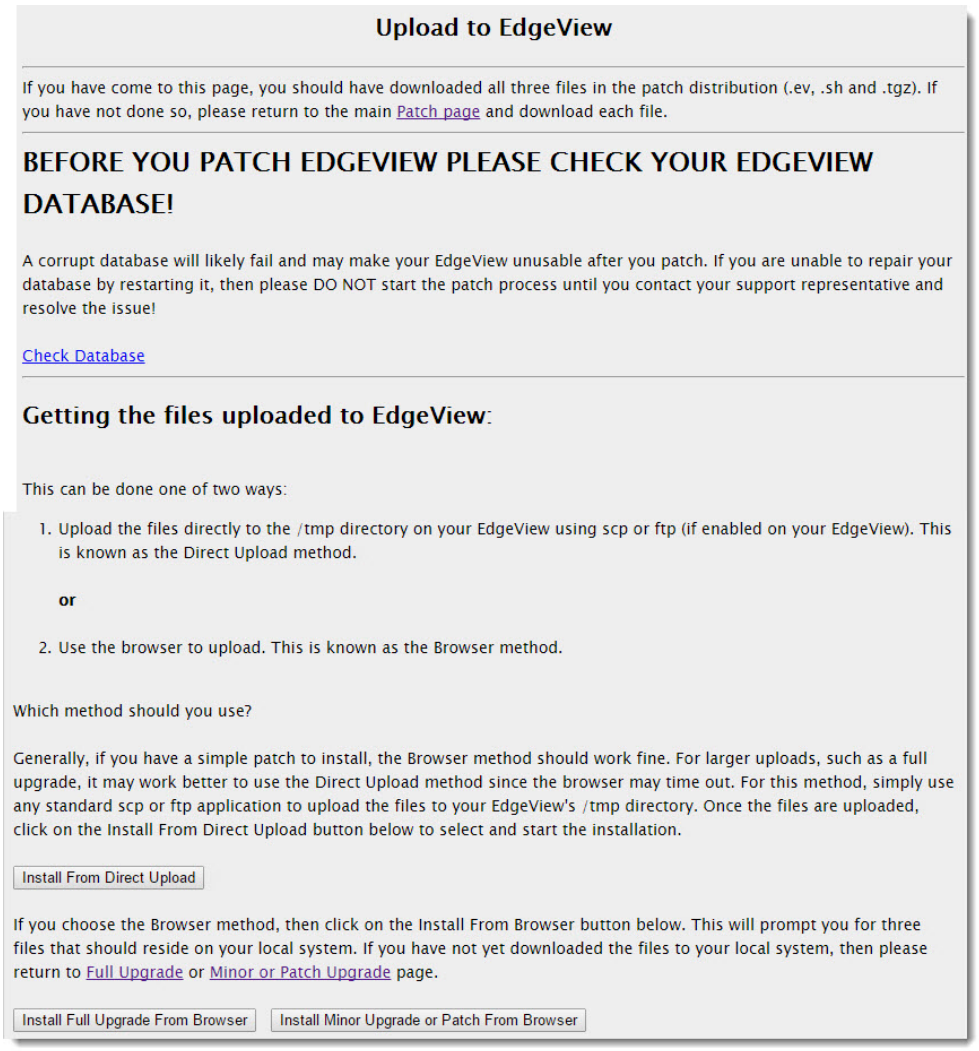
Manually Installing a Minor Upgrade or Patch Using a Browser

1. Download all three files in the patch distribution to your local drive. Refer to Downloading the Patch Files to a Local Computer.
2. Click the **EV Upgrade** icon and select **Upload Distribution Manually** from the sub-menu:



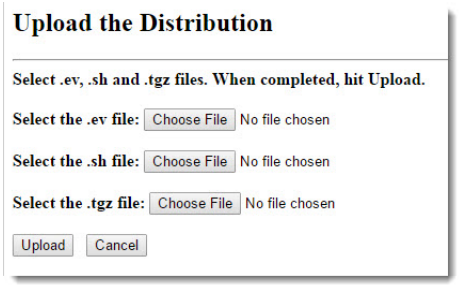
The Upload to EdgeView screen displays (Figure 9-2).

Figure 9-2 Upload to EdgeView



3. Click the **Install Minor Upgrade or Patch From Browser** button at the bottom of the screen. You will be prompted to upload the three files you downloaded in step 1 (Figure 9-3).

Figure 9-3 Uploading the Patch Release Files



4. For each file, click the **Choose File** button and select the file from your local drive.
5. When all three files have been selected, click **Upload** to start the installation. The files will be installed on EdgeView as if you had done it directly through the network.
6. To verify that the patch is installed on EdgeView, click the **EV System** icon and select **About**.

Performing a Full Upgrade

Note

This option is not available if your support license has expired.

When you upgrade EdgeView from one major release to another (for example, from EdgeView 14.0 to 14.1), you need to do a full upgrade. The difference between a full upgrade and a patch upgrade is that the full upgrade replaces all of the EdgeView source files while a patch upgrade replaces only those files which have changed. A patch release may take several minutes to install while a full upgrade could take several hours.

A full upgrade replaces the entire EdgeView distribution, and as such should be scheduled during a maintenance window. As always, a full backup of the system should be performed before any patch or upgrade, but especially for a full upgrade. You can download the upgrade files at anytime and perform the upgrade later.

Note

Before you begin the upgrade procedure, it is highly recommended that you put EdgeView in maintenance mode. Refer to Using Maintenance Mode for instructions.

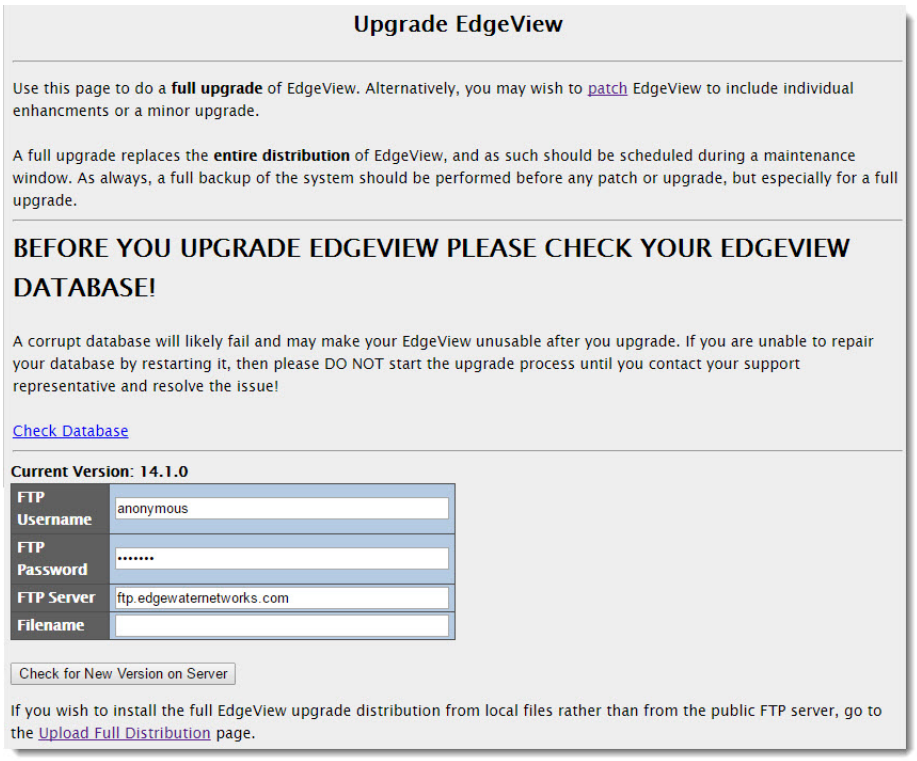
To do a full upgrade of EdgeView:

1. Click the **EV Upgrade** icon and choose **EdgeView Full Upgrade** from the sub-menu:



The Upgrade EdgeView screen displays (Figure 9-4).

Figure 9-4 Performing a Full Upgrade of EdgeView



2. HIGHLY RECOMMENDED: On the Upgrade EdgeView page, click **Check Database** to verify all the database tables are clean and not corrupt.

Caution

A corrupt database will likely fail and may make your EdgeView unusable after you install the patch. If you are unable to repair your database by restarting it, DO NOT start the patch process until you contact your Edgewater Networks support representative and resolve the issue.

Note

On HA systems be sure to check both sides of the HA pair.

3. Follow the wizard instructions on the screen to manually run the upgrade process through the EdgeView GUI.

10

Licensing

- Overview
- Installing the EdgeView Product License Key
- Installing or Updating the Support License Key

Overview

EdgeView requires Product and Support License keys to enable features of the product and to allow the product to receive TAC support service, respectively. These license keys are also required to install patches and perform upgrades.



Note

You need two license keys: an EdgeView Product License key and a Support License key.

When you purchase an EdgeView and a Support License, Edgewater Networks will email you a Product License key and Support License key. The email will include the MAC address, license key, and URL to the location of the OVA file.

If you later add more nodes to your EdgeView Product License, Edgewater Networks will send you a new license key. You will need to enter the key in EdgeView to activate the new Product License. Also, if your Support License expires, you will need to enter a new Support License key.

Installing EdgeView License Keys the First Time

The first time you log in to EdgeView, you will immediately be prompted to change the global login credentials. Once you have changed the login credentials, the EdgeView License Key screen displays for you to install the EdgeView Product License key and Support License key.

To install the EdgeView Product and Support License Keys for the first time, refer to Installing the EdgeView Product License and Support License Keys.

Installing the EdgeView Product License Key

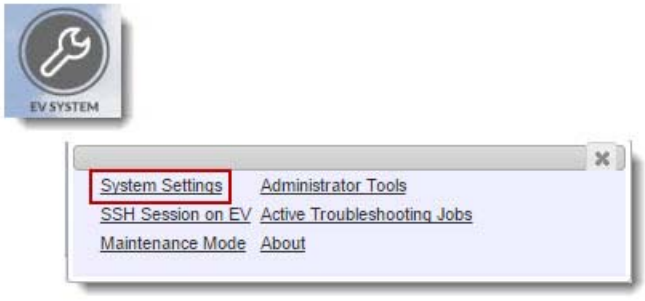
The EdgeView Product License specifies the number of EdgeMarcs (and similar nodes), endpoints, and conduits that can be managed by EdgeView. You purchase an EdgeView product license based upon the number of nodes you need. You can add additional nodes and will need to update the product license key in EdgeView.

Before installing the EdgeView Product License key, consider the following:

- The Product License may have an expiration date that will disable the license after the expiration date.
- The Product License key is very large (requiring a copy/paste due to its size).
- The Product License key has a token to track whether this EdgeView can use the Web Service API (Enabled=on) or not (Enabled=off).
- You must read and accept the End-User License Agreement for any new or updated license.
- A link to **Show License as plain text in new window** will display the decoded license key contents in a text window that can be copied/pasted easily for support calls, for example.
- High Availability (HA) has three possible values: off, primary and secondary. The *primary* indicator should be used only on the HA primary system. Similarly, the *secondary* indicator should be used only on the secondary system. When HA is set to primary or secondary, a new field known as the High Availability Partner Node is required. This is the MAC address of the other HA system, namely the secondary system's MAC if on the primary and vice versa. If HA is off, this field displays N/A.

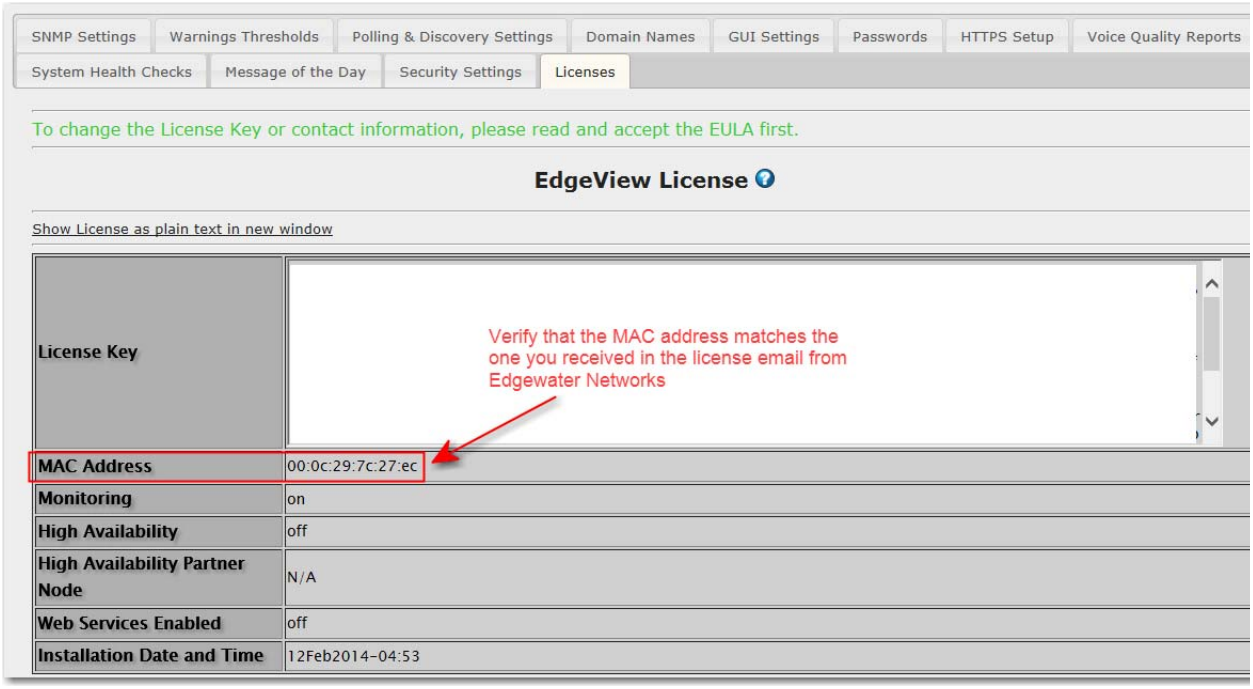
To install the Product License key:

1. Select **EV System** > **System Settings**.



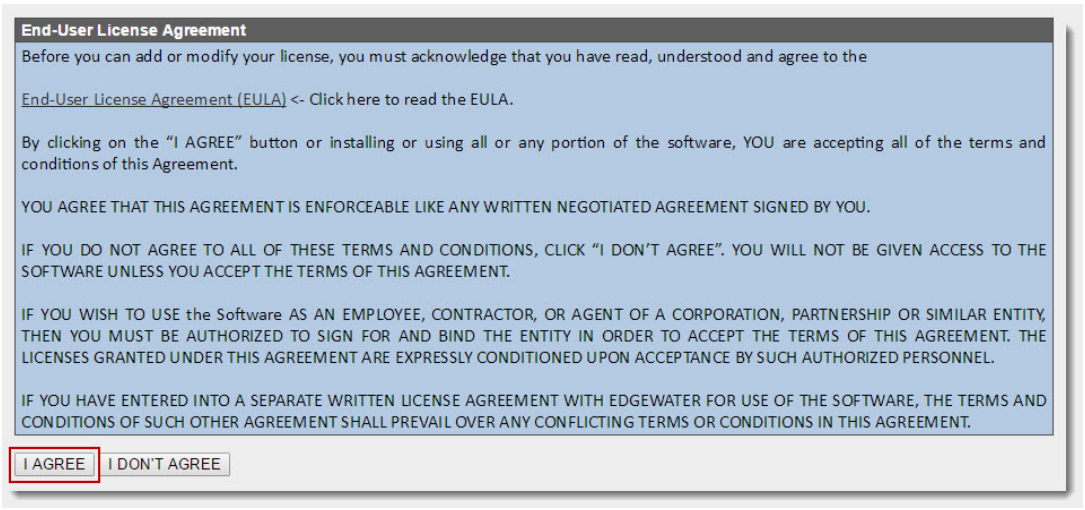
2. Select the **Licenses** tab. The EdgeView License Key screen displays (Figure 10-1). The MAC Address field will be pre-populated with the EdgeView MAC address. Verify that the MAC address matches the one you received in the License email from Edgewater Networks.

Figure 10-1 Installing the EdgeView Product License



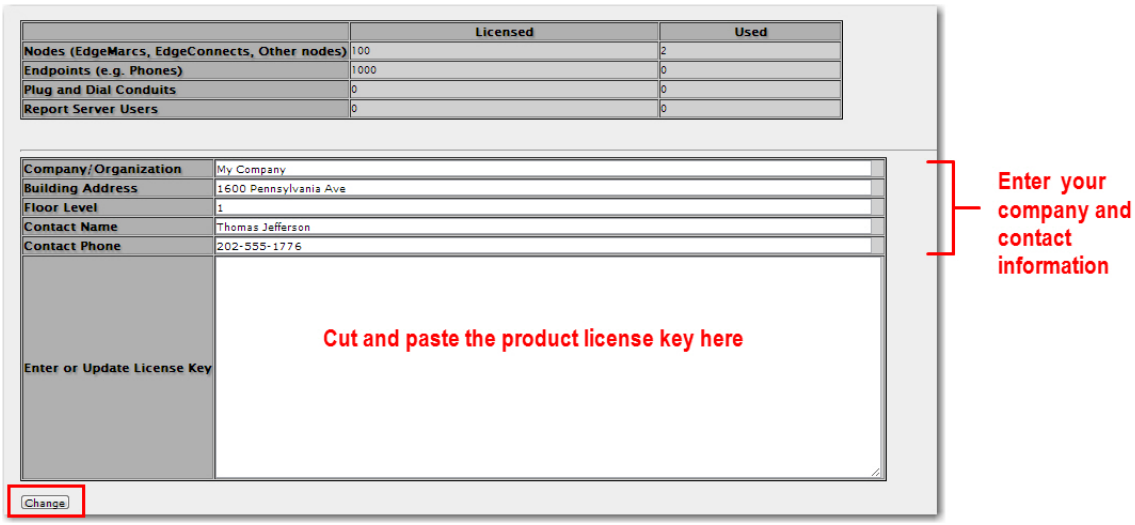
3. Click **I Agree** to accept the End User License Agreement (Figure 10-2).

Figure 10-2 EdgeView License Agreement



4. You may now update your Contact information and/or the EdgeView or Support License Key. Copy and paste the product license key that you receive in email into the Enter or Update License Key box Figure 10-3).

Figure 10-3 Entering the Product License Key



5. Enter your company and contact information.
6. Click **Change**. The license key will appear as encrypted text in the license key text box. Once the system accepts the product license key, the following text will appear in green at the top of the screen.

EdgeView Product License Key and contact information updated.

Tip

To view the license information as plain text, click **Show License as Plain Text in New Window**.

Viewing the Number of Licensed Nodes

Your EdgeView Product License specifies the maximum number of nodes that can be managed by EdgeView. The total number of nodes governed by users cannot exceed the number of nodes specified in your license agreement. Nodes include EdgeMarcs, EdgeConnects, SNMP nodes, and Third-party nodes.

The number of licensed nodes along with the License Agreement will be shown at the bottom of the screen (Figure 10-4). If you have exceeded the node limit and you attempt to add a node, you will receive a warning message.

Figure 10-4 Number of Licensed Nodes

	Licensed	Used
Nodes (EdgeMarcs, EdgeConnects, Other nodes)	5	3
Endpoints (e.g. Phones)	5	0
Plug and Dial Conduits	5	0
Report Server Users	5	0*
Edgemarc SIP analytics (EdgeMarcs)	5	2

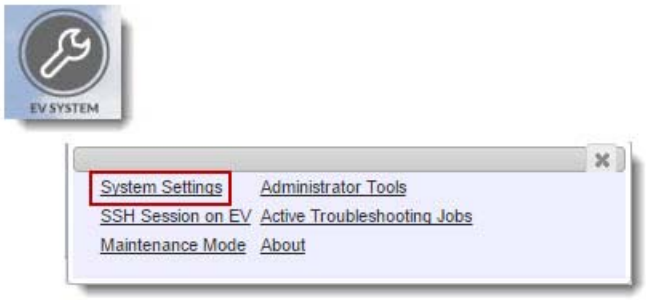
*Note: Actual usage may be higher if users were created directly on the Report Server

Installing or Updating the Support License Key

The EdgeView Support License allows for upgrades and patches until the expiration date. It does not affect other product functions before or after the expiration date. When the support license expires, contact your Edgewater Networks support representative for a new one.

To install the Support License key:

1. Select **EV System** > **System Settings**.



2. Select the **Licenses** tab. The EdgeView License Key screen displays (Figure 10-1).
3. Read and accept the EULA (Figure 10-2).
4. At the bottom of the **EV System** > **System Settings** > **Licenses** page (Figure 10-5), enter the EdgeView Support License key. This is the support license key sent to you in email from Edgewater Networks.

Figure 10-5 Installing the Support License Key



5. Click **Change**. Once the system accepts the support license key, the following text appears in green at the top of the screen:

   EdgeView Support License Key changed (see below for any errors)

   The support expiration date will be shown in the **Support Expiration** field and the end user license agreement will be displayed on the screen.

6. Click **I Agree** to Install the Support License Key.
7. Click **Change**. The EdgeView login screen will re-display for you to log in with your new credentials.

11

EdgeView Reports

EdgeView offers comprehensive reporting features via the Reporting Dashboard and the add-on EdgeView Reports (EdgeView Reports) module.

This chapter provides instructions for how to access and customize the EdgeView Reporting Dashboard. It also provides an overview of EdgeView Reports and instructions for registering an EdgeView Reports Server with EdgeView.

- Overview
- EdgeView Reporting Dashboard
- What Can You Do With EdgeView Reports?
- Registering the EdgeView Reports Server With EdgeView

Overview

Reporting Dashboard

The EdgeView Reporting Dashboard provides a graphical snapshot of the current system status using graphs and charts which show a summary of the statistics gathered by EdgeView over the past 24 hours. The pie charts, bar charts, and graphs on the Dashboard display real-time call quality performance metrics including minimum, maximum, and average Mean Opinion Scores (MOS), MOS polling and reporting statistics, below threshold count (BTC) alerts and more. You can view more detailed data for a particular device by clicking an area in the pie chart or graph.

EdgeView Reports

EdgeView integrates with EdgeView Reports, an add-on module which provides enhanced reporting functionality for trend analysis. EdgeView Reports includes a comprehensive library of reports which can be adapted to fit your needs and then printed or saved in a range of useful formats. With EdgeView Reports, you can run reports to assess the entire network or to focus on specific regions, groups or customers. In addition to on-demand reporting, you can configure EdgeView Reports to automatically run and deliver selected reports at regularly scheduled

intervals. The reports can be generated and delivered in HTML, Excel, CSV, RTF, text, and PDF file formats.

To obtain the EdgeView Reports add-on module, contact your Edgewater Networks sales and support representative. For more details about how to use EdgeView Reports, refer to the following documents available in the Edgewater Networks Knowledgebase: www.edgewaternetworks.com/kb

- *EdgeView Reports for EdgeView User Guide*
- *EdgeView Reports for EdgeView Administrator Guide*
- *Setting Up EdgeView Reports on EdgeView*
- *EdgeView Installation Guide*
- *Migrating from an EdgeView Reports Server to EdgeView*
- *EdgeView Reports Release Notes*

EdgeView Reporting Dashboard

Note

To view the Dashboard, the user must be assigned a specific right to access the Dashboard. For instructions on granting specific rights, refer to Assigning Specific Rights to a User.

To access the Reporting Dashboard:

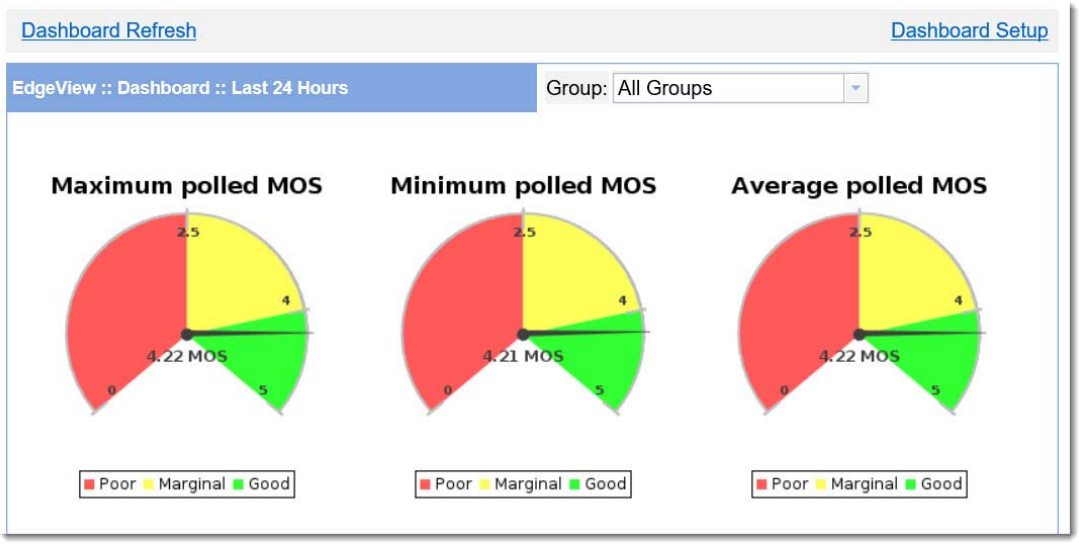
1. Select the **Reporting** icon in the EdgeView icon bar. The EdgeView Reporting menu displays (Figure 11-1).

Figure 11-1 Accessing EdgeView Reporting Menu



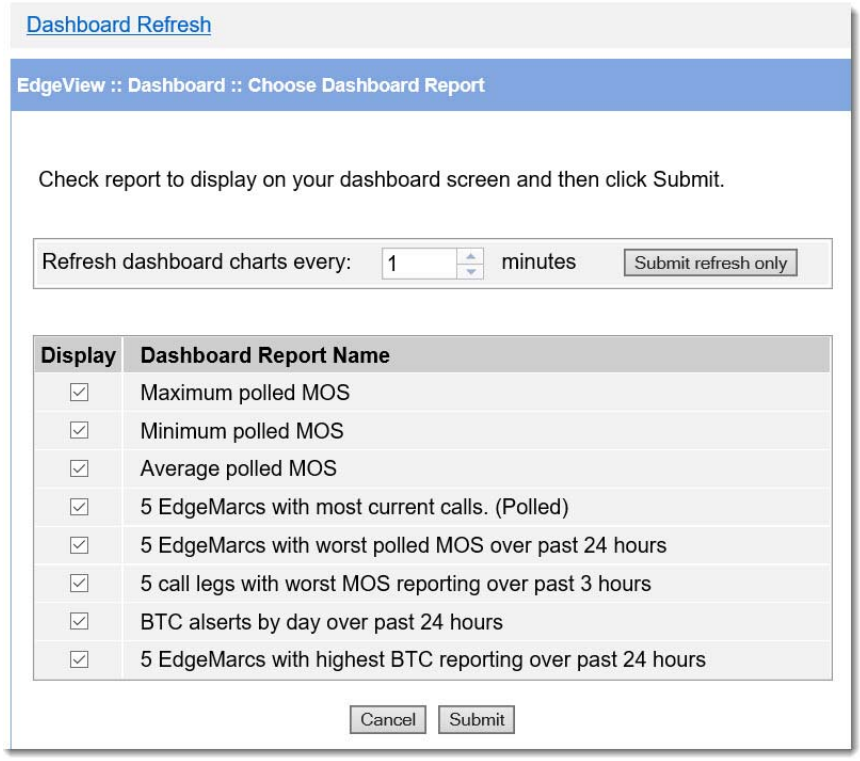
2. Select **Dashboard**. The main Dashboard page displays (Figure 11-2).

Figure 11-2 Main Dashboard Page



3. Click the **Dashboard Setup** link in the top right corner of the screen. The Dashboard Setup page displays (Figure 11-3).

Figure 11-3 Dashboard Setup Page



4. Select the checkbox next to the reports you want to monitor from the Dashboard.

Note

All authorized users (with or without administrator privileges) can customize which reports are displayed on the Dashboard.

Tip

You can change which reports you are monitoring on the Dashboard at any time.

5. Click **Submit** to submit your changes or click **Cancel** to discard your changes. EdgeView will re-display the Dashboard with your new settings.

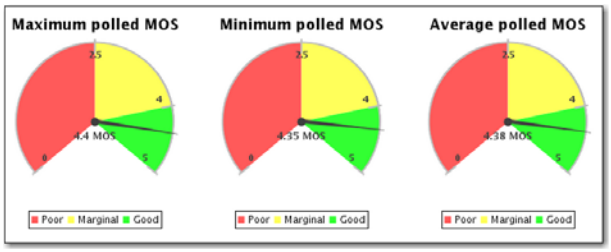
Figure 11-4 shows the Dashboard reports you can monitor. Table 11-1 provides a description of each report.

Figure 11-4 Dashboard Reports

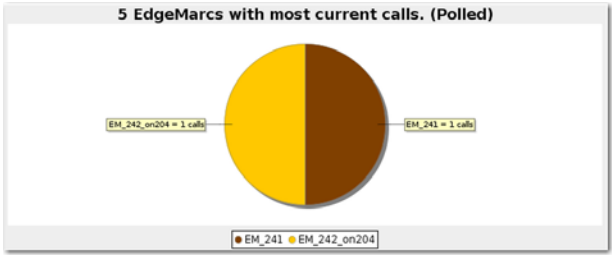


Table 11-1 Report Descriptions

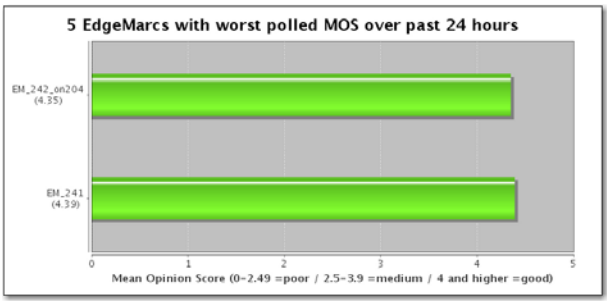
The monitoring gauges in the Dashboard provide a high-level view of the maximum, minimum, and average polled mean opinion score (MOS). These scores indicate the overall system status. The gauges initially show the status of all groups but you can customize the Dashboard to show the status for selected groups. You can also specify which gauges you want the Dashboard to display.



This pie chart shows the 5 EdgeMarcs with the most current calls in the most recent poll. Each color in the chart represents a different EdgeMarc. Click a color in the pie chart to view detailed host information for the associated EdgeMarc.



This bar chart shows the 5 EdgeMarcs with the worst Mean Opinion Score (MOS) over the past 24 hours. Click on a bar in the chart to view detailed information such as the EdgeMarc hostname, caller ID, source and destination IP addresses, and the number of alerts that occurred on the EdgeMarc over the past 24 hours. The scoring criteria is listed at the bottom of the graph.



This bar chart shows the 5 call legs with the worst MOS report status over the past 24 hours. Click on a bar in the chart to view more details about the call leg. The scoring criteria is listed at the bottom of the graph.

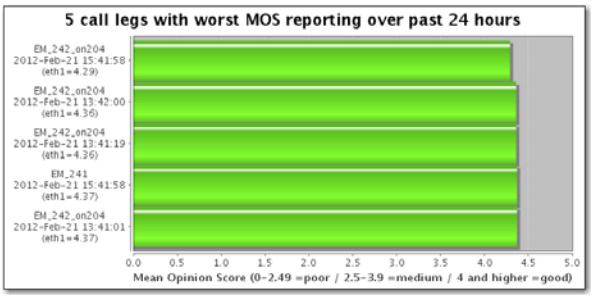
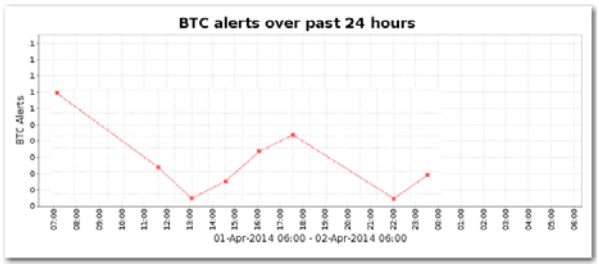
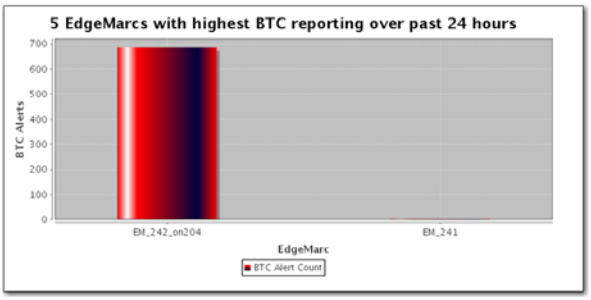


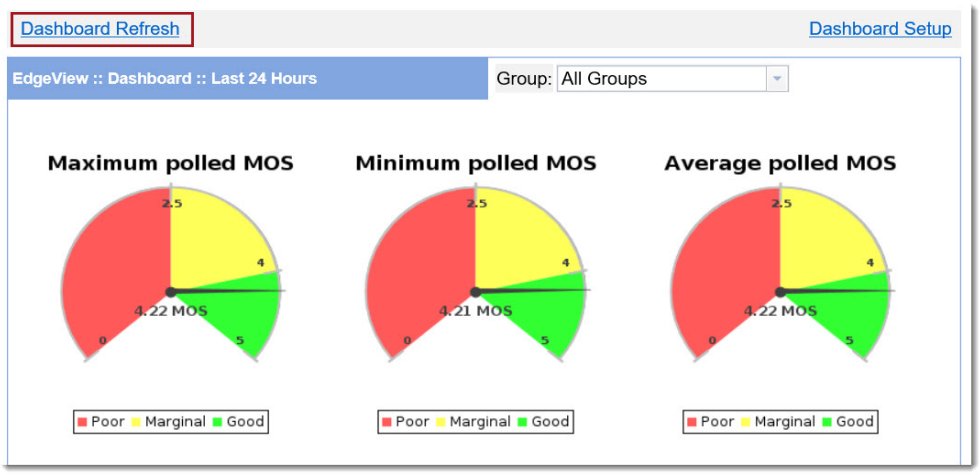
Table 11-1 Report Descriptions

This graph shows the Below Threshold Count (BTC) alerts over the past 24 hours. Click on a point in the graph to view more details about the alert such as the EdgeMarc hostname, caller ID, source and destination IP addresses, and the number of alerts that occurred on the EdgeMarc over the past 24 hours.	
This bar graph shows the 5 EdgeMarcs with the highest BTC reporting over the past 24 hours. Click on a bar to view more details such as the EdgeMarc caller ID, source and destination IP addresses and the number of BTC alerts on the EdgeMarc over the past 24 hours.	
The date, time, and interval for the last refresh is displayed at the bottom of the Dashboard.	

Refreshing the Dashboard

The graphs on the Dashboard refresh every minute or according to the interval set in the Dashboard Reports Setup screen. You can do an immediate refresh by clicking the **Dashboard Refresh** link at the top of the Dashboard screen (Figure 11-5).

Figure 11-5 Refreshing the Dashboard

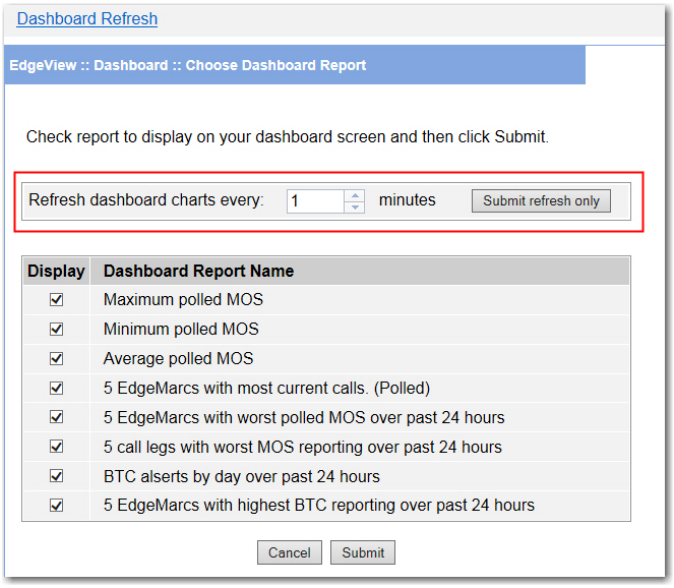


Changing the Refresh Interval

To change the refresh interval for the EdgeView Reports Dashboard:

1. Open the EdgeView Dashboard and select the **Dashboard Setup** link at the top of the screen (Figure 11-2).
2. In the **Dashboard Setup** screen, select a refresh interval for how often you want EdgeView to refresh the Dashboard (Figure 11-6).

Figure 11-6 Selecting a Dashboard Refresh Interval



3. Click **Submit refresh only** to save your change and return to the Dashboard. Your changes to the refresh interval will also be made when you click **Submit** after choosing which reports to display.

What Can You Do With EdgeView Reports?

To see a preview of EdgeView Reports capabilities:

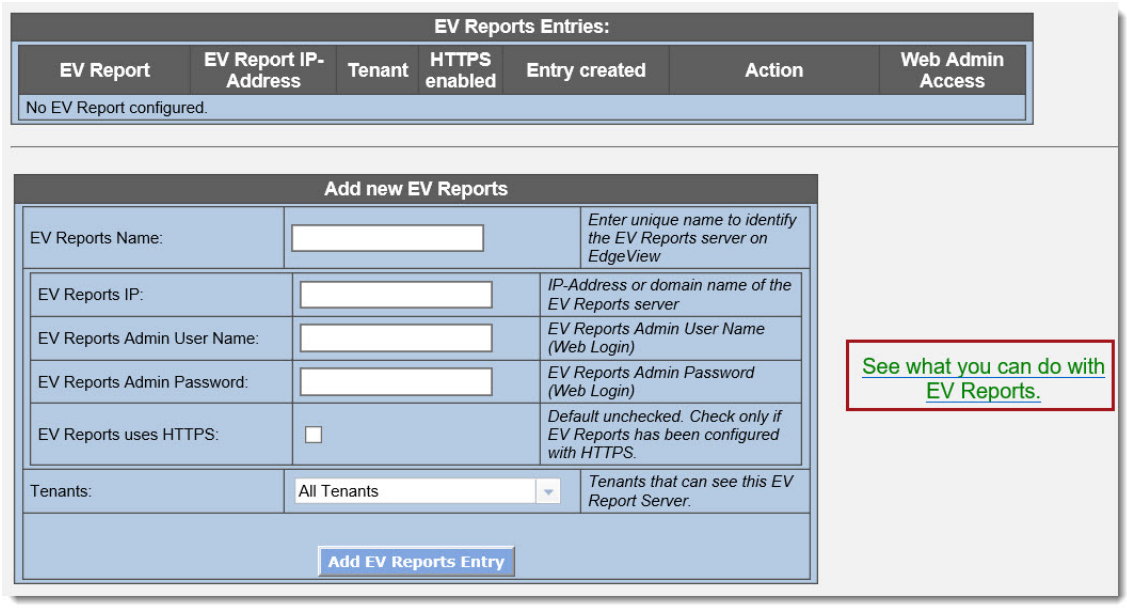
1. Select **Reporting > EdgeView Reports** on the Reports menu (Figure 11-7).

Figure 11-7 EdgeView Reporting Menu



The EdgeView Reports Entries screen displays (Figure 11-8).

Figure 11-8 EdgeView Reports Entries screen



2. Click the **See what you can do with EdgeView Reports** link the EdgeView Reports Info Page. This page provides examples of reports and an overview of how to perform the following tasks in EdgeView Reports:
   - Monitor your EdgeMarcs with Dashboard Charts
   - Create ad hoc reports or schedule auto-run reports

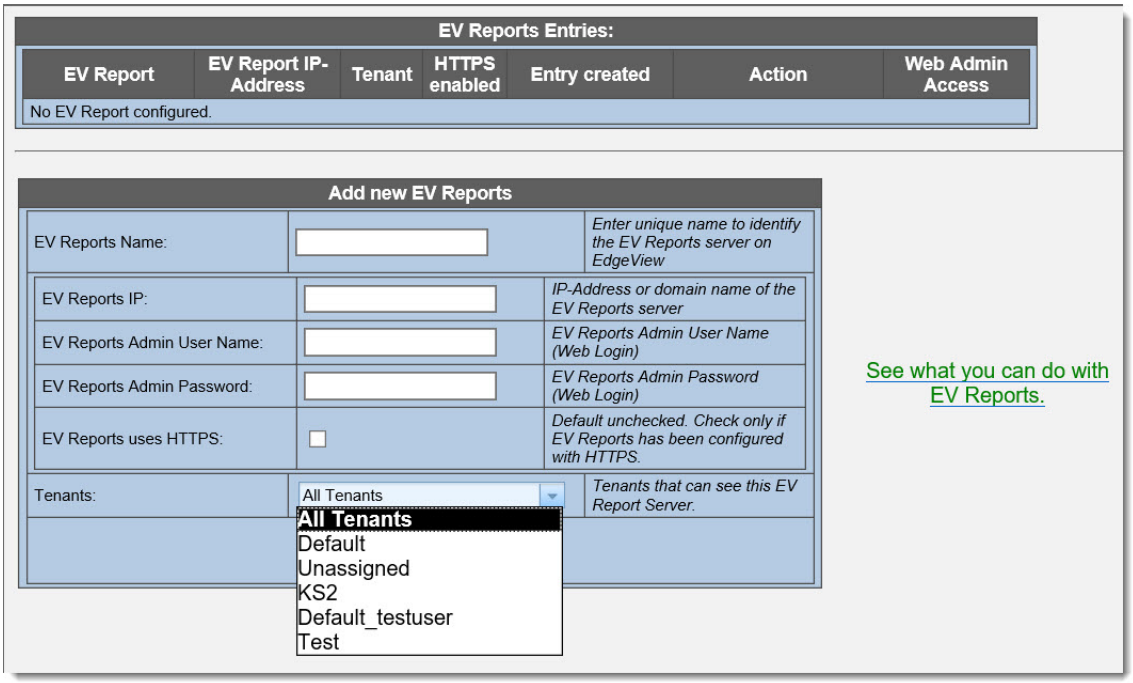
Registering the EdgeView Reports Server With EdgeView

If you have purchased an EdgeView Reports license, you will need to register the EdgeView Reports Server with EdgeView before you can use EdgeView Reports.

To register the EdgeView Reports Server with EdgeView:

1. Select **Reporting** > **EdgeView Reports**. The EdgeView Reports screen displays (Figure 11-9).

Figure 11-9 Registering the EdgeView Reports Server



2. Follow the on-screen help to specify information for the EdgeView Reports Server:
   a. In the **EdgeView Reports Name** box, enter a unique name to identify the EdgeView Reports Server on EdgeView.
   b. In the **EdgeView Reports IP** box, enter the IP address or domain name of the EdgeView Reports Server.
   c. Enter the **EdgeView Reports Admin User Name** and **EdgeView Reports Admin Password** for the EdgeView Reports Server.

Note

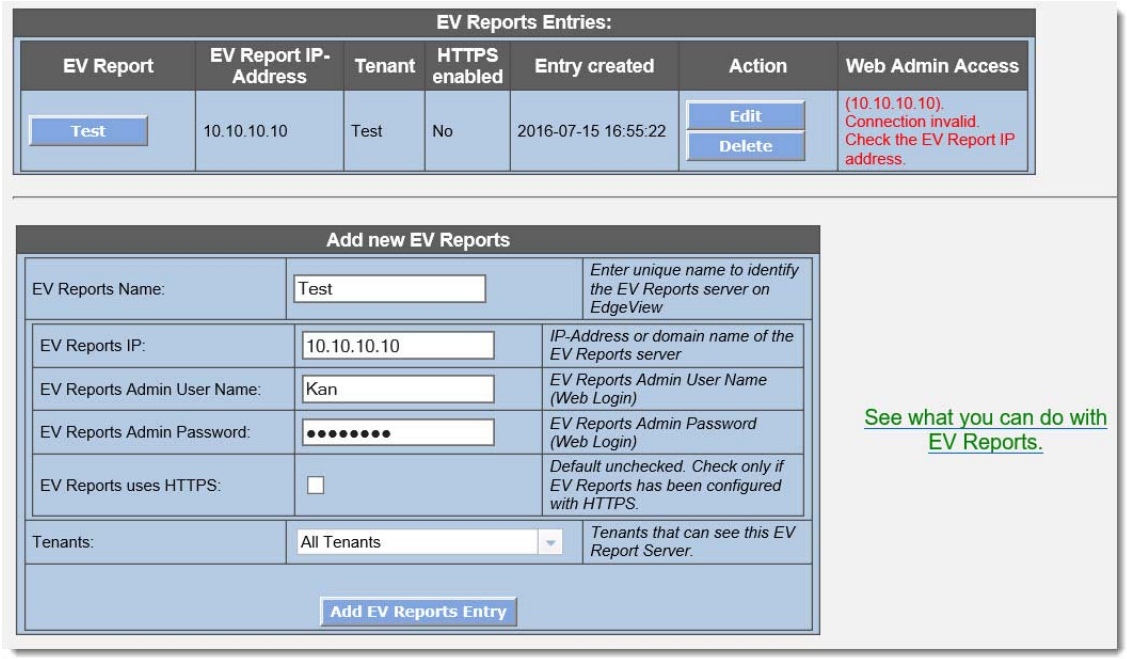
Admin users only have access to the EdgeView Reports **Administrator** tab for administrative tasks and therefore, cannot create reports. Admin users do not count towards the EdgeView License Key user limit.

d. (Optional) Enable the **EdgeView Reports uses HTTPS** checkbox *only* if HTTPS is enabled on EdgeView Reports.

e. From the **Tenants** drop down menu, select the Tenant which is allowed to access the EdgeView Reports Server.

3. Click **Add EdgeView Reports Entry**. The new entry will appear in the list of EdgeView Reports entries (Figure 11-10).

Figure 11-10 Adding an EdgeView Reports Entry

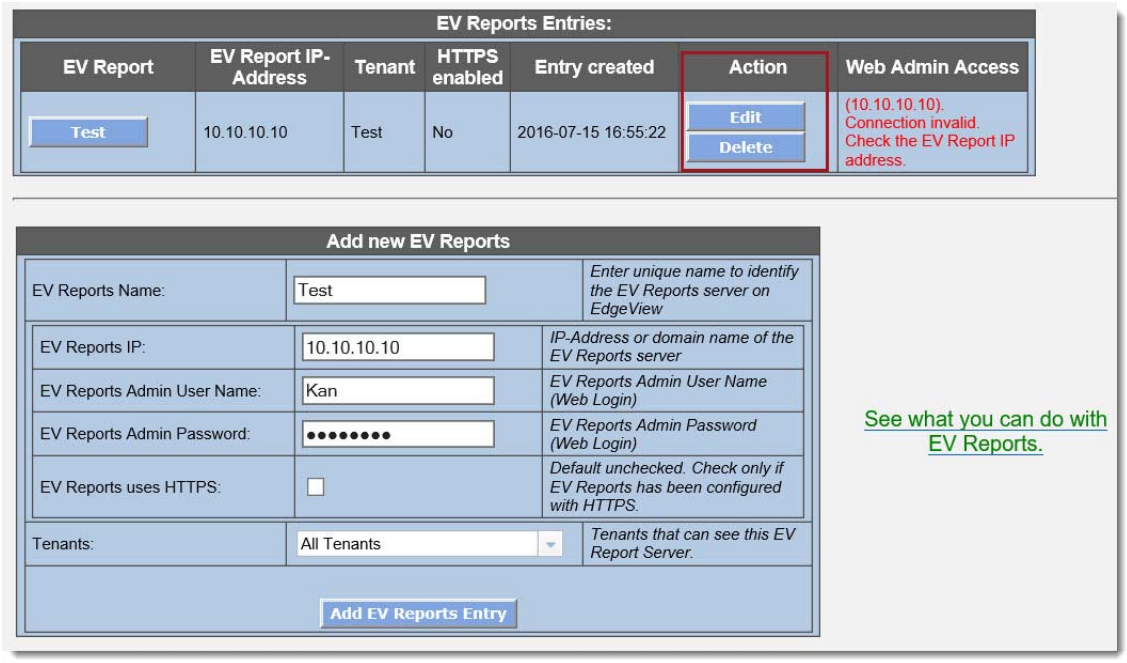


Editing an EdgeView Reports Server Entry

To edit an EdgeView Reports server entry:

1. Click the **Edit** button for the EdgeView Reports entry in the EdgeView Reports Entries screen list (Figure 11-11). The Edit EdgeView Reports screen displays.
2. Make your changes and click **Update EdgeView Reports Entry**.

Figure 11-11 Editing an EdgeView Reports Server Entry



Deleting an EdgeView Reports Server Entry

To delete an EdgeView Reports server entry:

1. Click the **Delete** button for the EdgeView Reports entry in the EdgeView Reports Entries list (Figure 11-11).
2. Click **OK** in the pop-up to confirm the deletion. The entry will be removed from the EdgeView Reports Entries list.

12

EdgeView Recommended Ports

Application	Protocol	Port	Description
SSH	TCP	22	CLI access (optional for management)
HTTP	TCP	80	GUI access (optional for management, configurable)
HTTPS	TCP	443	GUI access (optional for management, configurable)
FTP	TCP	21	File download (optional)
SYSLOG	UDP	514	Syslog messages (configurable)
SMTP	TCP	25	System notification messages
SNMP	UDP	161, 162	System monitoring (optional for management)
SNTP	TCP	123	Unit clock (configurable)
DNS	UDP	53	DNS resolution
Plug and Dial	UDP	5060	Optional: Only when feature is enabled
Voice Quality Reporting	UDP	5061	Optional: Only when feature is enabled
High Availability	UDP	694	Optional: For heartbeat between HA pairs
RADIUS	UDP	1812, 1813	Optional: Only when feature is enabled

Glossary

B

Blacklist

A Blacklist specifies a block of IP addresses that will be denied access to EdgeView. Blacklists allow you to block persistent hacking attempts by specifying a list of IP addresses that will be completely blocked from accessing EdgeView. Any input to EdgeView from these IP addresses is dropped.

If you have an EdgeView outside the firewall, the IP address of the EdgeView specified here must be managed inside the firewall.

C

CAC

Call Admission Control. Prevents oversubscription of VoIP networks. It is used in the call set-up phase and applies to real-time media traffic as opposed to data traffic. CAC mechanisms complement and are distinct from the capabilities of Quality of Service tools to protect voice traffic from the negative effects of other voice traffic and to keep excess voice traffic off the network.

Conduit

EdgeView uses conduits to communicate with the upstream softswitch for Plug and Dial. Using the conduit, EdgeView will inform the softswitch of a new phone and associate that phone with the requested user's profile. The EdgeView database includes an internal conduit. Additionally, EdgeView supports selected Broadsoft and Metaswitch conduits.

CSV

Comma Separated Values. CSV is an exportable file that can be opened with XLS in a table format.

D

default gateway

A router on a computer network that serves as an access point to another network.

Device

EdgeMarcs, IP phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug and Dial phones and Plug and Dial conduits.

Device Tree	Shows hierarchical, collapsible lists of the EdgeMarcs, Tenants, groups, EdgeConnects, phones, configuration Files and other nodes/devices managed by EdgeView. The entries in the device tree are associated with icons and are color-coded for quick identification of node/device type and service-affecting problems. You can use the controls at the top level of the device tree to expand and collapse the folders in the hierarchy, and also to search for groups and nodes/devices managed by EdgeView.
Device Tree Node Level	The “node level” in the device tree refers to the individual nodes/devices being managed by EdgeView. Nodes/devices include EdgeMarcs, phones, third-party nodes, SNMP-based nodes and EdgeConnects. If licensed, a node/device may also be Plug & Dial conduits.
Device Tree Group Level	The “group level” in the device tree refers to all the nodes/devices in a group. There may also be sub groups shown at the group level.
Device Tree Top Level	The “Top Level” in the device tree refers to the Tenants being managed by EdgeView.
DHCP	Dynamic Host Configuration Protocol is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual intervention.
DID and Short DID	Direct Inward Dial number usually called the “phone number”. Short DID is usually 3-5 digits for PBX-style dialing.
DN	Directory number.
DNS	Domain Name System. System used on the Internet for translating names of network nodes into addresses.

E

EdgeMarc Configuration Template	An XML file that describes all the configuration files for a given EdgeMarc or group of EdgeMarcs. An EdgeMarc template specifies the file names, variable names, types, constraints, and descriptions that can (but not necessarily must) be set for an EdgeMarc. The information and settings will vary depending on the EdgeMarc implementation.
EdgeMarc Configuration Template Manager	An application in EdgeView which provides a simple way to create, modify, and manage EdgeMarc templates. Using the Template Manager, you can generate, edit, copy, rename, delete, import and export template files. Once you've made your modifications, the template can be saved and used by the end user to push configuration values to the EdgeMarc.

EV EdgeView

EdgeView Configuration Template Editor Once you have generated an EdgeMarc configuration template, use the Editor to modify configuration settings in the template. Accessible from the EdgeMarc Configuration Template Manager.

EdgeView Group A collection of EdgeMarcs, IP phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug & Dial phones and Conduits that have been grouped together in EdgeView to make them easier to manage. By grouping nodes/devices, you can apply a single action to all nodes/devices in the group at once which saves you from having to configure each node/device individually. Groups can also contain other groups, often referred to as “sub-groups.”

EdgeView Product License The EdgeView product license specifies the number of nodes which can be managed by your EdgeView. The EdgeView product license does not expire. You purchase an EdgeView product license based upon the number of nodes you need. You can add additional nodes; however if you do so, you will need to update the product license key in EdgeView.

EdgeView Support License The EdgeView support license is set by the Edgewater Networks sales or support team at the time your product is shipped. It has a fixed expiration date. The support license key allows for upgrades and patches until the expiration date. When your EdgeView support license expires, EdgeView is still operational but you can no longer do patch upgrades or install new software on the EdgeView. A red alert displays at the top of the EdgeView License page in the EdgeView GUI when the support license is about to expire.

Endpoint An endpoint typically refers to a phone but it can be any device managed by EdgeView.

F

Feature Server The upstream switch at the customer premises to which EdgeView communicates to get information about the phones. Also referred to as a “softswitch.”

G

Generic Phone Configuration File All phone manufacturers have a common or *generic* phone configuration file for each phone model. EdgeView Plug and Dial includes these files for each supported phone model. In a typical IP phone deployment (without Plug and Dial) system administrators must modify the generic phone configuration files with customer-specific network and phone settings. EdgeView Plug and Dial simplifies this process by automatically creating phone-specific configuration files based on input retrieved by the IVR when the user self-provisions their phone.

Generic Phone Template A template file which is created from the phone manufacturer's generic phone configuration file. Generic phone templates are referred to as "Plug & Dial Templates" in EdgeView.

Group A collection of EdgeMarcs, IP phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug & Dial phones and Conduits which are grouped in EdgeView to make them easier to manage. By grouping nodes/devices, you can apply a single action to all nodes/devices in the group at once which saves you from having to configure each node/device individually. Groups can also contain other groups, often referred to as "sub-groups."

GUI Graphical User Interface

H

HA High Availability. High Availability (HA) is designed to eliminate a single point of failure in a network configuration. High Availability uses the concept of a Primary and Secondary system with a heartbeat to define which system is active and which one is Idle and an automated data replication. If the active system is failing, then the idle system becomes active automatically.

I

IP Address A device identifier on a TCP/IP network.

IP Address File List One of the three types of EdgeMarc configuration files. Contains only a list of IP addresses separated by new lines. Other EdgeMarc configuration file types are a Raw File and Variable/Value file.

IVR Interactive voice response (IVR) is a technology that allows users to interact with a company's host system via a telephone keypad or by speech recognition, after which they can service their own inquiries by following the IVR dialogue. IVR systems can respond with prerecorded or dynamically generated audio to further direct users on how to proceed. IVR applications can be used to control almost any function where the interface can be broken down into a series of simple interactions. IVR systems deployed in the network are sized to handle large call volumes.

J

Jitter The variation in packet transit delay caused by queuing, contention, and serialization effects on the path through the network. In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

M

MAC address Media Access Control address. A hardware address that uniquely identifies each node of a network.

Menu Bar The EdgeMarc Status page menu bar which contains sub-menus for monitoring, provisioning, configuring and performing operations on EdgeMarcs and other nodes/devices managed by EdgeView. The menu bar options change depending on which level you are at in the device tree.

MOS Mean Opinion Score. MOS is a test used in telephony networks to obtain the user's view of the quality of the network.

N

Node / Device EdgeMarcs, phones, third-party nodes, SNMP-based nodes, EdgeConnects and (if licensed) Plug & Dial phones Conduits.

O

Other Devices Third-party nodes and SNMP nodes.

P

Parent Group When there are sub-groups under group, the top level group is considered the Parent group. A Tenant is the parent group for a group which nested directly underneath the Tenant.

Phone Template A configuration file used to provision a phone.

Phone-specific Configuration File A phone-specific configuration file which contains MAC address-specific configuration information such as the phone number (DID), phone extension, phone display name, and the AuthName/Pwd. The content of the phone-specific file overrides what is in the generic phone configuration file. Phone-specific files typically have the phone's MAC address embedded in the filename.

Phone-specific Template A template file which is created from a phone-specific configuration file. These files can also be used without Plug and Dial; you can manually set up a phone using these files without using the IVR. Phone-specific templates are referred to as "Phone Templates" in EdgeView.

Plug & Dial Refers to the workflow for automatically managing endpoints when a conduit is used. Sometimes referred to as "PnD", Plug-n-Dial, PND, and P&D.

PoE Power over Ethernet.

R

Raw File One of the three types of EdgeMarc configuration files. A Raw File may be any text file, especially those that do not meet the formats of the other two file types: Variable/Value File or IP Address File List.

RegEx Regular Expression.

Rights Provides the system administrator with the ability to restrict users from using certain parts of EdgeView. Examples include Analyzing, Monitoring, Template Editing, Conduit Editing, Provisioning, VPN Editing, VPN Viewing, Device Configuration and System Administration. Also referred to as "specific rights."

S

SIP Session Initiation Protocol. Protocol designed to signal the setup of voice and multimedia calls over IP networks.

SIP Server The upstream SIP proxy server.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks as a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP Read-Only Community String The SNMP password EdgeView uses so that outside Network Management Systems can access it.

Softswitch The upstream switch at the customer premises that EdgeView communicates with to retrieve information about the clients. Also referred to as the “feature server.”

Specific Rights Provides the system administrator with the ability to restrict users from using certain parts of EdgeView. Examples include Analyzing, Monitoring, Template Editing, Conduit Editing, Provisioning, VPN Editing, VPN Viewing, Device Configuration and System Administration.

SSH Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network.

State The UP/DOWN status of a node.

Strict Password Strict passwords require 6-8 characters, 2 or more character types and no dictionary words.

Substitution Variables Special variables that will, at deployment time, be replaced with actual useful values.

Survivability The Survivability feature enables an EdgeMarc to provide local calls (station to Station or station to PSTN if there is local PSTN connectivity) when the WAN link is failing.

Syslog System Logs (syslog). Debugging logs that are collected by EdgeView and used to diagnose and resolve issues. These messages are not ordinarily seen by the user.

T

Tenant A Tenant is at the top level of the EdgeView hierarchy. Groups are assigned to a Tenant. A Tenant is always tied to at least one group but the group may have sub-groups.

Trap A Simple Network Management Protocol “trap” is a message which is initiated by a network element and sent to the network management system.

U

Unassigned Group The “Unassigned” group in EdgeView is the default group which EdgeView uses when it auto-discovers an unknown device or a device which has not been assigned to a group. If the Unassigned group does not exist, EdgeView will automatically create it when an unknown device is auto-discovered.

V

Variable/Value File One of the three types of EdgeMarc configuration files. Contains variable/value pairs only of the format: variable=value. Other types of EdgeMarc configuration files are an IP Address File List and a Raw File List.

VPN A Virtual Private Network extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network

VPN Group A logical grouping of EdgeMarcs for VPN configurations.

VPN Policy Defines the values of VPN properties.

W

WAN Wide Area Network.

Whitelist A Whitelist specifies a block of IP addresses that are allowed to conduct management sessions with EdgeView. For EdgeViews that are not behind a firewall (an EdgeView on the edge of the Internet), the Whitelist feature specifies a list of IP addresses that are allowed to conduct a management session with EdgeView. IP addresses that are not in the Whitelist are blocked from accessing EdgeView.

The Whitelist feature is similar in behavior to the “trusted management hosts” feature on the EdgeMarc. EdgeView administrators must use PCs/Workstations with the source IP addresses or networks listed in the Whitelist.