SIEMENS

RUGGEDCOM NMS v2.1

User Guide

For Linux

02/2017
RC1319-EN-01

Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd.

OpenNMS® is a registered trademark of The OpenNMS Group, Inc.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Open Source

RUGGEDCOM NMS is based on the OpenNMS® network management platform. OpenNMS and RUGGEDCOM RUGGEDCOM NMS are made available under the terms of the GNU General Public License Version 2.0 [http://www.gnu.org/licenses/gpl-2.0.html].

RUGGEDCOM NMS contains additional Open Source Software. For license conditions, refer to the associated *License Conditions* document.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity .

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com .

Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit www.siemens.com/ruggedcom or contact a Siemens customer service representative.

Contacting Siemens

Address
Siemens Canada Ltd
Industry Sector

Telephone
Toll-free: 1 888 264 0006
Tel: +1 905 856 5288

E-mail
ruggedcom.info.i-ia@siemens.com

300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Fax: +1 905 856 1995

Web

www.siemens.com/ruggedcom

Table of Contents

Preface

This guide describes RUGGEDCOM NMS v2.1, Siemens's network management system for RUGGEDCOM devices. It contains instructions and guidelines on how to use the software, as well as some general theory.

It is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for use by network and system planners, system programmers, and line technicians.

CONTENTS

Conventions

This User Guide uses the following conventions to present information clearly and effectively.

Alerts

The following types of alerts are used when necessary to highlight important information.

DANGER!
DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.

WARNING!
WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.

CAUTION!
CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.

IMPORTANT!
IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.

NOTE
NOTE alerts provide additional information, such as facts, tips and details.

CLI Command Syntax

The syntax of commands used in a Command Line Interface (CLI) is described according to the following conventions:

Example	Description
command	Commands are in bold.
command parameter	Parameters are in plain text.
command parameter1 parameter2	Parameters are listed in the order they must be entered.
command parameter1 *parameter2*	Parameters in italics must be replaced with a user-defined value.
command [parameter1 | parameter2]	Alternative parameters are separated by a vertical bar (|). Square brackets indicate a required choice between two or more parameters.
command { parameter3 | parameter4 }	Curly brackets indicate an optional parameter(s).
command parameter1 parameter2 { parameter3 | parameter4 }	All commands and parameters are presented in the order they must be entered.

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM ROS User Guides (Platform Specific)*
- *RUGGEDCOM ROX User Guides (Platform Specific)*
- *RUGGEDCOM ROX II User Guides (Platform Specific)*
- *RUGGEDCOM WIN Base Station User Guide*
- *RUGGEDCOM WIN CPE User Guide*

Accessing Documentation

The latest user documentation for RUGGEDCOM NMS v2.1 is available online at www.siemens.com/ruggedcom. To request or inquire about a user document, contact Siemens Customer Support.

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

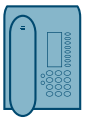
For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens Sales representative.

Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

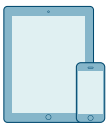
Online

Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.



Telephone

Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx .



Mobile App

Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

1 Introduction

Welcome to the RUGGEDCOM NMS (Network Management Software) v2.1 User Guide. This document details how to install and configure RUGGEDCOM NMS, as well as manage supported devices.

RUGGEDCOM NMS is a scalable, fully-feature, enterprise grade solution for monitoring, configuring and maintaining RUGGEDCOM mission-critical networks. It improves operational efficiency, speeds up system provisioning, and preserves data validity, while allowing focus on the key events in the network.

CONTENTS

Section 1.1

Features and Benefits

The following describes the many features and benefits offered by RUGGEDCOM NMS:

- **Primary Features**
  - Centralized Web-based management of RUGGEDCOM devices and IP-networks
  - Auto-discovery of device links and services and representation on a network map
  - Real-time monitoring and notification of events, alarms and thresholds
  - Continuous collection of traffic statistics for analysis and reporting
  - Deployment of firmware/software upgrades across RUGGEDCOM devices
  - Automatic backup of RUGGEDCOM device configuration data
  - Creation of templates and propagation of configuration changes across RUGGEDCOM ROS/ROX II devices
  - Monitoring RUGGEDCOM ROS, ROX II and WIN configurations and reports changes that exceed the authorized user defined boundaries
  - Bulk password changes of RUGGEDCOM ROS, ROX and WIN devices
- **Automated Network Discovery and Data Pooling**
  RUGGEDCOM NMS has a versatile pooling engine configurable to meet customer needs. Devices are discovered using ICMP pings and upon RUGGEDCOM NMS receiving traps or logs from a device. Services are detected for all

devices and a topology map is created. All discovered devices have their performance data regularly collected by the RUGGEDCOM NMS pooling system.

- **Alarms and Event Management**
  RUGGEDCOM NMS continuously monitors the network and reports any changes or errors it detects. Events can originate outside RUGGEDCOM NMS, such as SNMP traps or syslog messages generated by devices under management. RUGGEDCOM NMS can also generate events internally, such as upon the detection of a new device or when forcing a service scan of a device.

  Alarms are events that have been selected as being representative of the current health of the network. Many alarms can be cleared by the system without operator intervention. For example, when an alarm posted for a broken network link subsequently receives an event indicating the network link has been reestablished, the alarm condition is then removed from the alarm list. RUGGEDCOM NMS users can quickly and intuitively create and manipulate complex filtering criteria for the list of events and alarms to display.

  It is also possible for events and logs received by RUGGEDCOM NMS to be forwarded to one or multiple destinations.

- **Network Performance Monitoring and Reporting**
  RUGGEDCOM NMS continuously collects traffic statistics for analysis and reporting. Reports allow a network operator to assess the current and historical health of the network. These reports provide the tools needed to pro-actively detect issues and correct them before an outage or unacceptable network latency occurs.

  Through the Network Monitor feature, RUGGEDCOM NMS learns the traffic characteristics of all devices supporting RMON2 on your network.

  - Monitors network traffic for abnormal behavior such as a rapid rise or fall in throughput
  - Triggers RUGGEDCOM NMS events and notifications on discovery of abnormal traffic conditions
  - Automatically adjusts the monitoring baseline over time to account for natural increases in network traffic and allows users to define their own customized threshold rules

- **Network Mapping**
  RUGGEDCOM NMS provides powerful, flexible, browser-based mapping of network entities under RUGGEDCOM NMS management. It can automatically map and lay out a selected set of devices, save and restore custom map views, perform live map updates, display map updates in real-time, and more.

  - Icons specific to each device type
  - Hierarchical and organic views
  - Grouping of multiple objects under a single icon
  - Color coded representation of each node and link status
  - Graphical representation of the bandwidth used between ports
  - Network monitor usage gage (for overall usage of network bandwidth)
  - Geographical mapping for the RUGGEDCOM WIN base station
  - Drill down capability by clicking on desired devices icon and getting detailed information

- **Management of RUGGEDCOM Devices**
  RUGGEDCOM NMS is the perfect tool to perform the configuration management and maintenance of RUGGEDCOM devices running ROS, ROX, ROX II and WIN firmware. From a centralized platform, it is possible to perform a bulk update of a device firmware. Configuration data is automatically backed up on the RUGGEDCOM NMS server.

  RUGGEDCOM NMS can also automatically change the password used on RUGGEDCOM ROS, ROX and WIN devices on the network.

- **Dynamic Configuration**
  RUGGEDCOM NMS minimizes the time required when configuring ROS/ROX II based devices with the use of templates dynamically created from the data of an existing device. The Dynamic Configuration feature allows viewing, manipulating and comparing configuration data and distributing changes across multiple devices easily and efficiently.
- **Firewall Management**
  RUGGEDCOM NMS provides an interface for deploying, enabling and configuring firewall policies efficiently across multiple RUGGEDCOM ROX II devices.
- **Gold Configuration**
  RUGGEDCOM NMS helps prevent unwanted configuration changes on RUGGEDCOM ROS and ROX II devices. Being informed of any changes (including the ones being made from the character-based interface on the device itself) it identifies if the new values are inside the boundaries defined as valid and acceptable by the RUGGEDCOM NMS administrator. Notifications sent allow the RUGGEDCOM NMS user to compare the changed parameters to the original one, and if desired to restore the previous configuration.
- **APPS Management**
  RUGGEDCOM NMS supports the centralized deployments of RUGGEDCOM ELAN and CROSSBOW applications on RUGGEDCOM ROX II devices.
- **Licenses**
  RUGGEDCOM NMS can be obtained via a DVD or digital download. The license chosen will determine the maximum number of supported devices. Licenses exist for the management of up to 128, 256, 1024 or 1024+ devices.

Section 1.2

System Requirements

To guarantee reliability and responsiveness, RUGGEDCOM NMS is designed to run on dedicated hardware.

The following details the client and server requirements for RUGGEDCOM NMS:

IMPORTANT!
The operating system for the RUGGEDCOM NMS server must be installed with its default installation options. RUGGEDCOM NMS is designed to be the only application running on the system. Any applications or network services running at the same time beyond what is required for the installation and function of RUGGEDCOM NMS must not be installed.

NOTE
In some web browsers, multi-process architecture is enabled by default. When enabled, this functionality may prevent RUGGEDCOM NMS from dynamically configuring devices. If this occurs, refer to your browser help to disable multi-process architecture, or try using a different browser.

NOTE
To support more than 2000 devices, a more robust hardware profile scaled to the number of required devices is required. For more information, contact a Siemens Sales representative.

Client Side

- Internet Explorer 11
- Mozilla Firefox 50
- Adobe Flash Player 11.7.700.224

Server Side

- Debian 8.0 Jessie (64-bit), English
- Java SE Development Kit (JDK) 8u121 (64-Bit)

Hardware (up to 500 devices)

- Intel Core 2 Quad-Core CPU, 2.4 GHz or higher

Video Card (up to 500 devices)

- 1GB DDR3 Memory
- 625 MHz Engine Clock
- 667 MHz Memory Clock
- 10.7 GByte Memory Bandwidth

Video Card (More than 500 devices)

- Contact Siemens Customer Support.

- 4 GB RAM
- 500 GB hard disk

Hardware (up to 2000 devices)

- Intel Core i7 CPU, 4.0 GHz or higher
- 8 GB RAM
- 1 TB hard disk

Section 1.3

Security Recommendations

The computer system running RUGGEDCOM NMS and the RUGGEDCOM NMS software should be appropriately secured:

Authentication

- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, etc.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Passwords should not be re-used across different user names and systems, or after they expire.
- Record passwords (including device passwords) in a safe, secure, off-line location for future retrieval should they be misplaced.
- File transfer protocols – FTP, HTTP, NFS and Windows File sharing – should not allow unauthenticated access to RUGGEDCOM NMS software, configuration or database directories.

Physical/Remote Access

- Use only SSL (Secure Sockets Layer) certificates. For more information about creating a self-signed SSL certificate, refer to Section 4.1, “Creating a Self-Signed Certificate” .
- Install the RUGGEDCOM NMS server in an access-controlled, physically secure location.
- Siemens recommends that only Administrator users access the server, to avoid unintentional or unauthorized modifications to files.
- Make sure RUGGEDCOM NMS is deployed behind a corporate firewall.
- Always log out of the RUGGEDCOM NMS Web user interface and lock access to the workstation when not physically present at the terminal.
- Where possible, configure the RUGGEDCOM NMS server to use the following modes for SSH (Secure Shell):
  - Use Counter (CTR) operation mode based ciphers. CTR mode is considered more secure than Cipher Block Chaining (CBC) operation mode.
  - Use SHA (256 bit) and SHA (512 bit) MAC algorithms. These are considered more secure than MD5 and 96 bit MAC algorithms.
- Be aware of any non-secure protocols enabled on the device. While some protocols, such as HTTPS, SSH and SNMPv3, are secure, others, such as Telnet, were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to RUGGEDCOM NMS/network.
- Regularly run anti-virus and anti-malware programs on the RUGGEDCOM NMS server to detect and quarantine potential security findings.

- Prevent access to external, untrusted Web pages while accessing the RUGGEDCOM NMS Web interface. This can assist in preventing potential security findings, such as loss of session confidentiality.

Hardware

- Make sure the latest software version is installed on the RUGGEDCOM NMS server. For the latest information on security issues for Siemens products, visit the Industrial Security website [http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm] . Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.

Policy

- Periodically audit the use, installation and configuration of RUGGEDCOM NMS to make sure it complies with these recommendations and/or any internal security policies.
- Review the user documentation for other Siemens products used in coordination with RUGGEDCOM NMS for further security recommendations.

Section 1.4

Open Source Software

RUGGEDCOM NMS is derived from and built upon the OpenNMS network management platform. OpenNMS is an enterprise-grade network management system maintained using an open source development model. OpenNMS and RUGGEDCOM NMS are made available under the terms of the GNU General Public License, available at www.siemens.com/ruggedcom.

RUGGEDCOM NMS extends the functionality of OpenNMS to provide enhanced support for RUGGEDCOM networking devices, including:

- ROS-based Ethernet switches and serial servers
- ROX-based network routers
- ROX II-based network routers
- WIN wireless network equipment

Siemens uses open source software components in many of its networking products, and is an active and contributing member of many open source projects. Siemens devotes considerable engineering resources to the evaluation, testing and maintenance of the components it uses, and works to make sure its enhancements are published back into the open source community.

Section 1.5

Product Licensing

RUGGEDCOM NMS uses a Product Activation Key (PAK) to enforce the limits of the license purchased by the user. The PAK contains a unique System Identifier, provided by the user, that ties the purchased software to the workstation/server on which it is intended to be run, as well as the date on which technical support from Siemens will end. For more information about determining the System Identifier, refer to Section 1.5.1, “Determining the System Identifier” .

After the support period ends, the existing software will continue to run, but software updates can no longer be applied and telephone support will end. **It is recommended that a new license be purchased before the existing license expires.**

When a new RUGGEDCOM NMS license is purchased, a unique PAK file is created by Siemens and renewed on an annual basis. Each PAK file is electronically secured and will become unusable if modified in the field. For more information about PAK files, contact Siemens Customer Support.

Demonstration versions of RUGGEDCOM NMS come with a pre-installed PAK file, which limits the number of devices that can be managed by RUGGEDCOM NMS to 20.

CONTENTS

Section 1.5.1

Determining the System Identifier

Prior to installing RUGGEDCOM NMS, users must provide the System ID (or System Identifier) of their host computer to Siemens , to allow the license file to be generated. Siemens will then provide the customized license file and all necessary installation files.

To determine the System ID, do the following:

NOTE
Siemens will provide a compressed ZIP file containing the files necessary to determine the system ID. For more information about obtaining the ZIP file, contact Siemens Customer Support.

1. Obtain the RUGGEDCOM NMS ZIP file (`ruggednms_systemID.zip`) from Siemens.
2. Open an X Window System (or X-Window) terminal session.

   IMPORTANT!
   Commands issued as the root user should be used with extreme caution. The root user has the highest privilege level in Linux. Some commands issued at this level (other than those described here) can render the system unrecoverable.

3. Open a shell window and elevate the root user by typing:

   ```
   su
   ```

4. Using the xvf option, untar the file `jdk-8u-121-linux-x64.tar.gz` to `/usr/lib/jvm`. The following directory will be created:

   `/usr/lib/jvm/jdk1.8.0_121`

5. Create a folder for the ZIP file by typing:

   ```
   mkdir /root/ruggednms_systemID
   ```

6. Extract the contents of the ZIP file to `/root/ruggednms_systemID`.
7. Change the directory by typing:

```
cd /root/ruggednms_systemID
```

8. Set the access permissions for the script `get_SystemID.sh` by typing:

```
chmod +x get_SystemID.sh
```

9. Run `get_SystemID.sh`. The System ID will be displayed on screen.

Section 1.5.2
Internal Messaging of Licensing Errors

When errors related to licensing arise, RUGGEDCOM NMS displays a message in the header and footer of the Web user interface. The color of the message indicates the severity of the issue/error, as follows:

- **Green** – An information message, typically to inform the user on the current status of the license
- **Yellow** – A warning message notifying the user of an issue that, if not addressed, will lead to a more sever problem
- **Red** – A serious problem requiring immediate attention

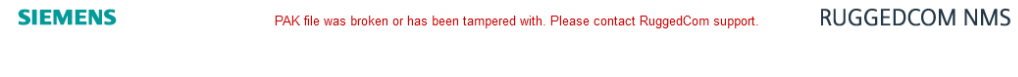


Figure 1: PAK File Error (Example)

IMPORTANT!
When licensing errors exist, RUGGEDCOM NMS prevents the addition of network resources to its database for monitoring. The error condition(s) must be corrected before RUGGEDCOM NMS can return to normal operation.

The following is a list of possible errors and their corresponding messages:

Error Condition	Error Message
PAK or Electronic Signature does not exist.	PAK file or e-signature does not exist or is corrupt. Please contact Siemens support.
PAK file is corrupt or has been tampered with.	PAK file was broken or has been tampered with. Please contact Siemens support.
The computer's unique System Identifier does not match the identifier in the PAK file.	System identifier is invalid. Please contact Siemens support.

Section 1.5.3
License Expiry

When the current license approaches or surpasses its expiration date, a message is displayed in the header of the RUGGEDCOM NMS Web user interface.

Figure 2: License Expiration Message

The message indicates how long before the license is set to expire and changes color based on the proximity of the expiry date.

- **Green** – 90 to 61 days remain before the license expires
- **Yellow** – 60 to 31 days remain before the license expires
- **Red** – 30 to 0 days remain before the license expires, or the license has already expired

NOTE
The license pertains only to technical support from Siemens, including access to Customer Support representatives, software updates, and more. The RUGGEDCOM NMS itself will remain functional even after the license has expired.

Section 1.5.4

License Restrictions for Managed Devices

The license restricts the number of devices that can be managed by RUGGEDCOM NMS. When that number reaches the limit of allowed devices, a message is displayed in the footer of the RUGGEDCOM NMS Web user interface.

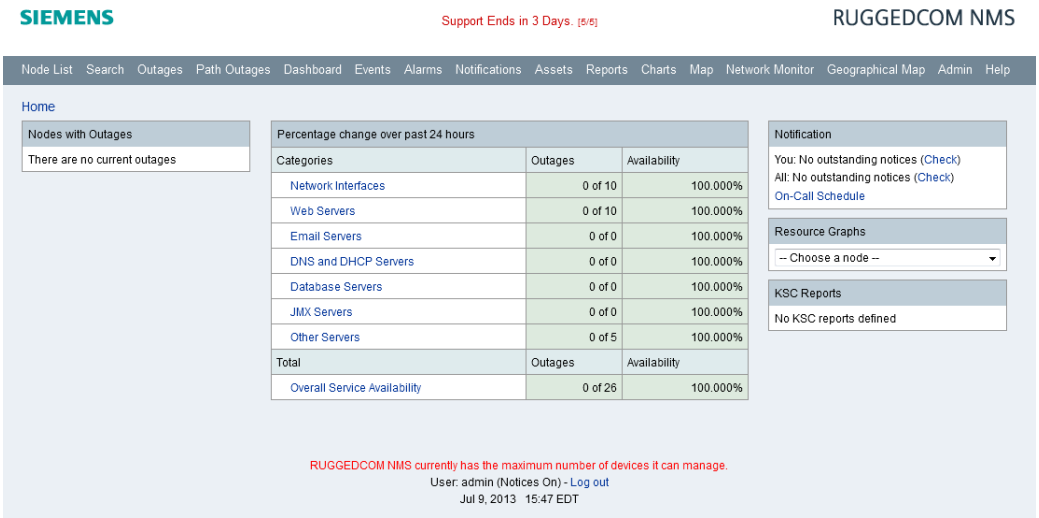


Figure 3: Maximum Number of Managed Devices Reached

The maximum number of managed devices allowed by the license is listed on the **Help** screen. For more information, refer to Section 3.6, "Viewing Product Information" .

To help users monitor the number of devices currently managed by RUGGEDCOM NMS, a default *Device Management Status* message appears in the header of the RUGGEDCOM NMS Web user interface. The message lists the number of managed devices and the maximum number allowed by the license.

Figure 4: Device Management Status Message

In this example, 11 devices are managed by RUGGEDCOM NMS out of a possible 20 devices.

The color of this *Device Management Status* message changes based on the ratio of managed devices to the maximum number of devices allowed.

- *Green* – 0 to 75% of the maximum allowed devices are managed
- *Yellow* – 76 to 99% of the maximum allowed devices are managed
- *Red* – 100% of the maximum allowed devices are managed

Section 1.6

Supported Devices

RUGGEDCOM NMS supports the following RUGGEDCOM devices:

ROS Devices

- i800, i801, i802, i803, RMC30, RP110, RS400, RS401, RS416, RS416P, RS900, RS900L, RS900W, RS910, RS910L, RS910W, RS920L, RS920W, RS930L, RS930W, RS900M, RS940G, RS950G, RS969, M969, RS1600, RS1600F, RS1600T, RS8000, RS8000A, RS8000H, RS8000T, RSG2100, RSG2100P, M2100, RSG2200, M2200, RSG2288, RSG2300, RSG2300P, RSG2488, RSG920P

ROX Devices

- RX1000, RX1000P, RX1100, RX1100P

ROX II Devices

- RX1400, RX1500, RX1501, RX1510, RX1511, RX1512, RX5000, MX5000, MX5000RE

WIN Devices

- WIN5114, WIN5214, WIN5118, WIN5218, WIN5123, WIN5223, WIN5125, WIN5225, WIN5135, WIN5235, WIN5137, WIN5237, WIN5149, WIN5249, WIN5151, WIN5251, WIN5158, WIN5258, WIN7014, WIN7015, WIN7018, WIN7023, WIN7025, WIN7035, WIN7225, WIN7233, WIN235, WIN7237, WIN7249, WIN7251, WIN7258

NOTE
RUGGEDCOM NMS will also detect and monitor other IP devices that use generic MIBs and support LLDP.

Section 1.7

Reserved Ports

The following lists the ports used by RUGGEDCOM NMS and the services associated with each. If devices managed by RUGGEDCOM NMS are behind a firewall, these ports must be allowed.

TCP Ports

Description	Port	Outbound?	Inbound?	Comments
XMPP	5222	Yes	No	Used for XMPP connection.
SSH	22	Yes	No	Used by SshMonitor for service monitoring and configuration management.
Telnet	23	Yes	No	Used for Telnet connection.
SMTP	25	Yes	No	Used by SmtpMonitor and MailTransportMonitor for service monitoring. Need only be allowed for SMTP servers. Used by Notifd for e-mail delivery of notifications, normally via a smart SMTP relay
HTTP	80	Yes	Sometimes	Used by HttpMonitor and PageSequenceMonitor for service monitoring. Sometimes used by Notifd for delivery of notifications via a web service or help-desk web form.
RMI	1099	Yes	Yes	Used by remote location pollers to register themselves with the RUGGEDCOM NMS server. Used by Java Management Extensions (JMX) to connect to monitored Java application servers for performance data collection.
RMI	1199	No	Yes	Used by the remote poller back-end for communication with running remote monitors, which may be located on the network.
HTTPS	443	Yes	Sometimes	Used by HttpsMonitor and PageSequenceMonitor for service monitoring. Sometimes used by Notifd for delivery of notifications via a web service or help desk Web form.
EventD	5817	Sometimes	Sometimes	Used for real time communication between the front-end and the back-end engine.
HTTP	8080	No	Yes	Used for HTTP access to the RUGGEDCOM NMS Web interface.
HTTP	8180	Yes	No	Used for HTTP service monitoring.
HTTPS	8081	No	Yes	Used for HTTPS access to the RUGGEDCOM NMS Web interface.
HTTPS	8181	Yes	No	Used for HTTPS service monitoring.
CAPSD and POLLER	5818	No	Yes	Used for DHCP service discovery.
SFTP	2222	No	Yes	Used for configuration management.
NETCONF	830	Yes	No	Used for NETCONF configuration management.

UDP Ports

Description	Port	Outbound?	Inbound?	Comments
XMPP	5222	Yes	No	Used for XMPP connection.
SNMP	161	Yes	No	Used for performance data collection. May also be used for some types of service polling. Normally should be allowed for all managed nodes.

Description	Port	Outbound?	Inbound?	Comments
SNMP Trap and Inform	162	No	Yes	Traps are unsolicited messages from an agent to a manager. Normally should be allowed from all managed nodes. Informs use the same port as traps, but are less ubiquitous. Informs require stateful rules since the manager must reply with an acknowledgment of receipt.
Syslog	514	No*	Yes	Inbound needed only if syslogd is enabled within RUGGEDCOM NMS for creating events from syslog messages. Outbound is only needed to select hosts if sending RUGGEDCOM NMS notifications via syslog.

2 Installing/Upgrading RUGGEDCOM NMS

This chapter describes how to install, update and restore components of RUGGEDCOM NMS.

CONTENTS

Section 2.1

Installing/Upgrading Debian

RUGGEDCOM NMS requires the system to have Debian Linux 8.0 (64-bit) installed. Other versions of Debian must be upgraded before RUGGEDCOM NMS v2.1 is installed.

When installing/updating Debian, note the following:

- Binaries and installation instructions are available from the Debian website (http://www.debian.org).
- Debian must be installed with only the components required to run the system, such as the desktop environment and standard system components. All other software required to run RUGGEDCOM NMS are automatically downloaded and installed during the installation of RUGGEDCOM NMS.

Section 2.2

Installing RUGGEDCOM NMS

To install RUGGEDCOM NMS for the first time, do the following:

NOTE

The installation package includes the following third-party applications required to support important features of RUGGEDCOM NMS:

- *Apache HTTP Web Server*
- *PostgreSQL Database*

All third-party applications are installed automatically when RUGGEDCOM NMS is installed for the fist time.

NOTE
Java SE Development Kit (JDK) 8u121 (64-Bit) is required to perform this procedure.

1. Obtain Java SE Development Kit (JDK) and install it to the default directory. For more information about installing Java, refer to Section 2.5, "Installing/Upgrading Java" .
2. Obtain the RUGGEDCOM NMS installer, available on a DVD or as a digital download. The installer file is digitally-signed by Siemens. For information about obtaining the latest installer, contact a Siemens Sales representative.
3. Make sure the workstation/server meets the minimum system requirements. For more information, refer to Section 1.2, "System Requirements" .
4. Make sure ports used by RUGGEDCOM NMS are not in use by the workstation/server or blocked by a firewall. For more information, refer to Section 1.7, "Reserved Ports" .
5. Open an X Window System (or X-Window) terminal session.

   IMPORTANT!
   Commands issued as the root user should be used with extreme caution. The root user has the highest privilege level in Linux. Some commands issued at this level (other than those described here) can render the system unrecoverable.

6. Open a shell window and elevate the root user by typing:

   ```
   su
   ```

7. Make sure the Apache Tomcat v5.5 servlet/JSP container is not installed on the workstation. The RUGGEDCOM NMS installation wizard is not compatible with this version of Tomcat.

   Remove Tomcat v5.5 by typing:

   ```
   apt-get remove tomcat5.5
   ```

8. Open sources.list by typing:

   ```
   gedit /etc/apt/sources.list
   ```

9. Add the following lines to sources.list:

   ```
   deb http://http.us.debian.org/debian/ jessie main contrib non-free
   deb-src http://http.us.debian.org/debian/ jessie main contrib non-free
   deb http://security.debian.org/ jessie/updates main contrib
   deb-src http://security.debian.org/ jessie/updates main contrib
   ```

10. If installing from a DVD, at the shell prompt, type:

    ```
    apt-cdrom add
    ```

    When the system requests a name for the DVD, type **RuggedNMS**.

11. Updated the list of source repositories by typing:

    ```
    apt-get update
    ```

    Make sure no errors are reported during the update process.

NOTE
The time required to install RUGGEDCOM NMS is dependent on Internet connection speeds.

12. Install RUGGEDCOM NMS and all dependent packages by typing:

```
apt-get install ruggednms
```

Once the installation is complete, proceed to the next steps.

IMPORTANT!
The system environment only needs to be set up once and is reserved for new installations of RUGGEDCOM NMS.

13. Setup the system environment by running the following script:

```
/root/ruggednms_scripts/update_env.sh
```

14. Exit all terminal sessions and open a new X Window System (or X-Window) terminal session.
15. By default, RUGGEDCOM NMS is installed as a service that runs in the background, but it can be installed as an application instead. To run RUGGEDCOM NMS as an application, run the following script:

```
/root/ruggednms_scripts/configure_ruggednms.sh
```

16. Create a self-signed Secure Socket Layer (SSL) certificate. For more information, refer to Section 4.1, “Creating a Self-Signed Certificate” .
17. If installing a licensed version of RUGGEDCOM NMS, obtain and install the Product Activation Key (PAK). For more information, refer to Section 2.4, “Licensing RUGGEDCOM NMS ” .
18. Install a Linux desktop environment. This is required to display dialog boxes that appear during startup and other processes.
19. Launch RUGGEDCOM NMS. For more information, refer to Section 3.2, “Launching RUGGEDCOM NMS ” .
20. Configure device discovery. For more information, refer to Section 6.4.10, “Managing Device Discovery” .
21. Configure device access. For more information, refer to Section 6.4.11, “Managing Device Access” .
22. Configure SNMP. For more information, refer to Section 6.5.1, “Configuring SNMP Globally” .
23. Enable logical maps. For more information, refer to Section 5.5.1, “Enabling Logical Maps” .
24. Configure users and passwords. For more information, refer to Section 4.8.1.1, “Adding a User” .
25. Configure the utilities and services required to manage RUGGEDCOM devices on the network.

Section 2.3

Upgrading RUGGEDCOM NMS

To upgrade an earlier version of RUGGEDCOM NMS to v2.1, do the following:

IMPORTANT!
During the upgrade process, configuration data from the previously installed release is automatically archived for future reference. However, if data encryption is enabled, the data will be inaccessible.

Consider disabling data encryption before upgrading RUGGEDCOM NMS.

1. [Optional] Disable data encryption. For more information, refer to Section 4.10.2, "Disabling Data Encryption" .
2. [Optional] Backup all RRD data for the previous release by copying the folder `/usr/share/opennms/share` to a temporary location. The existing folder will be overwritten during the installation/upgrade process.
3. [Optional] Retain information collected in the previous release by backing up the database. For more information, refer to Section 2.3.1, "Backing Up the Database" .
4. Install RUGGEDCOM NMS v2.1 as normal. For more information about installing RUGGEDCOM NMS, refer to Section 2.2, "Installing RUGGEDCOM NMS " .

   CAUTION!
   Configuration hazard – risk of data corruption and/or loss. The data structure and content of configuration files may not be compatible between software releases. Do not copy archived configuration files directly into `/usr/share/opennms/etc/` *without first making sure they are compatible with the new version of RUGGEDCOM NMS installed.*

   To protect against potential compatibility issues, it is recommended instead to only use the configuration data archived under `/usr/share/opennms/etc-backup/` *for reference.*
5. [Optional] Restore the RRD data from the previous release by copying the temporary `share` folder to `/usr/share/opennms/share` .
6. [Optional] Restore the database for the previous release. For more information, refer to Section 2.3.2, "Restoring the Database" .
7. Configure RUGGEDCOM NMS v2.1. If necessary, use the configuration data that was automatically archived during the upgrade process to `/usr/share/opennms/etc-backup/` as reference. For more information about configuring RUGGEDCOM NMS, refer to Chapter 6, *Managing/Configuring Devices* .

   Alternatively, if the configuration data is compatible with the currently installed release, copy the configuration data from `/usr/share/opennms/etc-backup/` to `/usr/share/opennms/etc/` .
8. [Optional] Enable data encryption. For more information, refer to Section 4.10.1, "Enabling Data Encryption" .

CONTENTS

Section 2.3.1
Backing Up the Database

To back up the database, do the following :

1. Open an X Window System (or X-Window) terminal session.
2. Open a shell window.
3. Create a temporary database dump by typing:

   ```
   pg_dump -U postgres -Fc opennms >  /tmp/rnms-db.dump
   ```

   Where:

   - `/tmp/rnms-db.dump` is the path and name of the database dump file

Section 2.3.2
Restoring the Database

To restore the database, do the following:

1. Open an X Window System (or X-Window) terminal session.
2. Open a shell window.
3. Quit the pgAdmin tool.
4. Restore the database by typing:

   ```
   pg_restore -U postgres -d opennms  /tmp/rnms-db.dump
   ```

   Where:

   - */tmp/rnms-db.dump* is the path and name of the database dump file
5. [Optional] Delete the temporary dump file by typing:

   ```
   rm  /tmp/rnms-db.dump
   ```

   Where:

   - */tmp/rnms-db.dump* is the path and name of the database dump file

Section 2.4
Licensing RUGGEDCOM NMS

A Product Activation Key (PAK) is required for enabling licensed versions of NMS. If upgrading an existing installation of RUGGEDCOM NMS, the previous PAK file is retained. A new PAK file is only required for new installations.

To obtain and install a PAK file, do the following:

1. Obtain the system identifier. For more information about determining the system ID, refer to Section 1.5.1, "Determining the System Identifier".
2. Copy the system identifier and send it to Siemens Customer Support in text format. A Product Activation Key (PAK) file will be sent via e-mail.
3. Save the PAK file under `/usr/share/opennms/etc`.
4. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS".

Section 2.5
Installing/Upgrading Java

RUGGEDCOM NMS must have the Java Runtime Environment (JRE) for Java Development Kit (JDK) v1.8 installed on the server to access important features. Earlier versions of the Java runtime environment currently installed must be upgraded before RUGGEDCOM NMS v2.1 is launched.

To install or upgrade the Java runtime version currently installed and link it to RUGGEDCOM NMS, do the following:

1. Obtain the Linux JDK self-extracting binary `(jdk-8u121-linux-x64.tar.gz)`.
2. Open an X Window System (or X-Window) terminal session.

3. Untar the tarball to the `/usr/lib/jvm` folder by typing:

```
tar -xvf jdk-8u121-linux-x64.tar.gz
```

4. [Optional] When upgrading Java, and RUGGEDCOM NMS is already installed, do the following:

   Link the new version of the Java run time environment by typing:

```
/root/ruggednms_scripts/create_java_link.sh
```

Section 2.6

Uninstalling RUGGEDCOM NMS

To uninstall RUGGEDCOM NMS v2.1, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server.
2. Stop RUGGEDCOM NMS by running the following script:

```
/root/ruggednms_scripts/stop_ruggednms.sh
```

3. Stop PostgreSQL by typing:

```
/etc/init.d/postgresql stop
```

4. Stop Apache by typing:

```
/etc/init.d/apache2 stop
```

5. Back up the RUGGEDCOM NMS database. For more information, refer to Section 2.3.1, "Backing Up the Database" .
6. Uninstall RUGGEDCOM NMS by typing:

```
apt-get purge --auto-remove ruggednms\*
```

7. Uninstall PostgreSQL by typing:

```
apt-get purge --auto-remove postgresql\*
```

8. Uninstall Apache by typing:

```
apt-get purge --auto-remove apache2\*
```

9. Delete the opennms directory by typing:

```
rm -r /usr/share/opennms
```

10. Delete the ruggednms_script directory by typing:

```
rm -r /root/ruggednms_script
```

11. Restart the computer.

3 Using RUGGEDCOM NMS

This chapter describes how to use the RUGGEDCOM NMS interface. It describes the following tasks.

CONTENTS

Section 3.1

Using the Web User Interface

The Web user interface is the client-side configuration tool for RUGGEDCOM NMS. It provides operators and administrators access to a variety of features related to the configuration of not only RUGGEDCOM NMS, but also the devices under its management.

The Web user interface consists of four major sections:

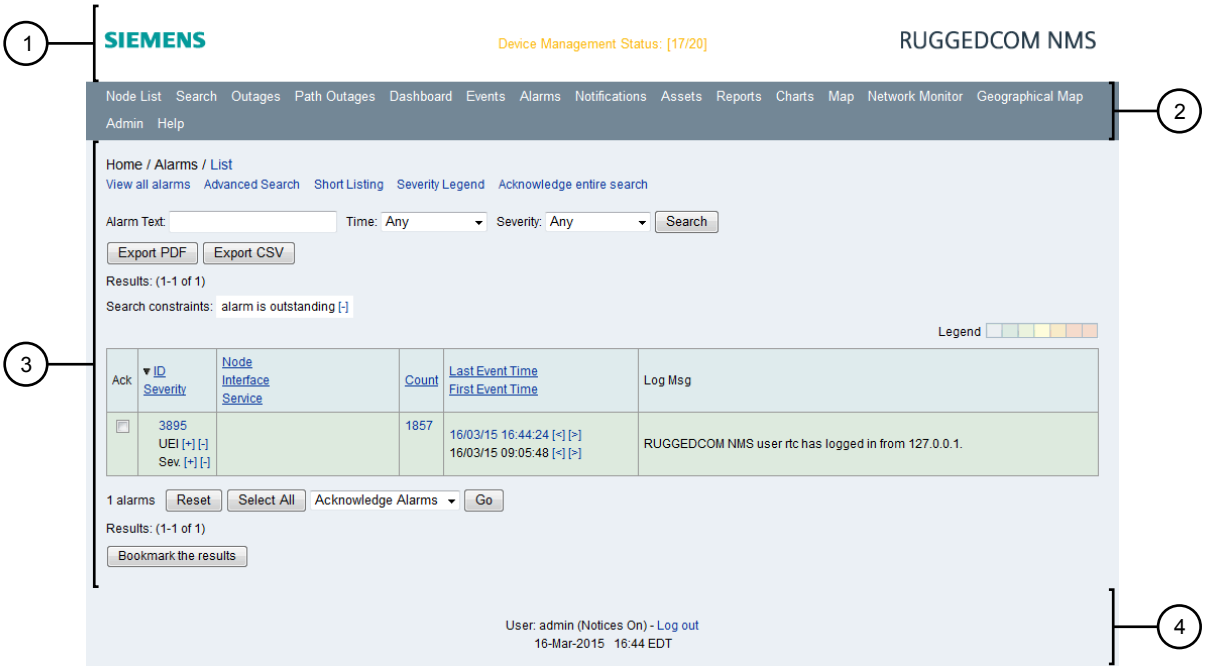


Figure 5: The Web User Interface

1. Header Area **2.** Menu Bar **3.** Main Area **4.** Footer Area

- **Header and Footer**
  The header and footer areas display important messages to the user related to licensing, firmware upgrades, configuration uploads, and more.
- **Menu Bar**
  The menu bar provides links to a series of menus and screens. For more information about each menu item, refer to Section 3.1.2, “Menus” .
- **Main Area**
  The main area is where menu options, parameters, reports, lists of events, and more appear.

CONTENTS

Section 3.1.1

The Home Screen

With the exception of Dashboard users, the **Home** screen is the starting point for users when they start a new Web session. It displays information about network outages, device availability and outstanding notifications. It also provides quick access to standard resource performance reports and KSC reports.

NOTE
*Users designated as Dashboard users are taken directly to the **Dashboard** screen when they start a new Web session. For more information, refer to* Section 3.7, "Using the Dashboard" .

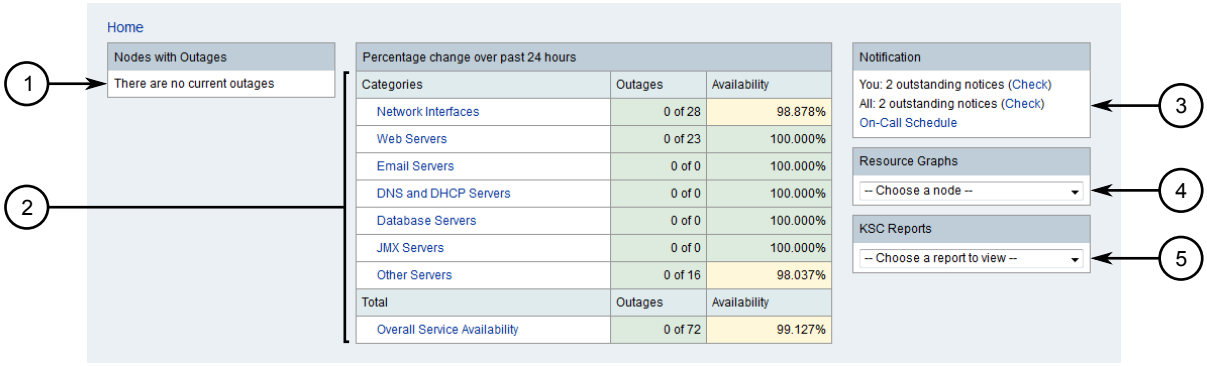


Figure 6: The Home Screen

1. Outages Information **2.** Device Availability Information **3.** Outstanding Notifications **4.** Resource Graphs **5.** KSC Reports

It includes the following areas:

- **Outages**
  The **Nodes with Outages** area lists devices that have experienced outages. Click on the device's IP address or label to view the full device details. For more information, refer to Section 6.4.2, "Viewing Device Details" .
- **Percentage change over past 24 hours**
  The **Percentage change over past 24 hours** table details the overall availability of devices managed by RUGGEDCOM NMS within the past 24 hours, including the number of outages that have been experienced. For more information, refer to Section 5.1, "Monitoring Device Availability" .
- **Notification**
  The **Notification** indicates how many notifications have not been acknowledged. Notifications directed toward the current user and total number of outstanding notifications are counted separately.

  To view the outstanding notifications, click **Check**. For more information about notifications, refer to Section 5.2.4, "Managing Notifications" .
- **Resource Graphs**
  The **Resource Graphs** area provides quick access to standard resource performance reports. To access a report, select a node from the list and then select one or more resources to query. For information about generating standard resource performance report, refer to Step 2 in Section 5.4.2.1, "Generating Standard Reports" .
- **KSC Reports**
  The **KSC Reports** area provides quick access KSC (Key SNMP Customized) reports. To access a report, select an available report from the list. For information about KSC reports, including how to create them, refer to Section 5.4.3, "Managing KSC Reports" .

To return to the home screen at any time, simply click the Siemens logo at the top of the screen.

Section 3.1.2
Menus

The menu bar across the top of the Web user interface provides access to information and tools needed to manage a full network using RUGGEDCOM NMS.

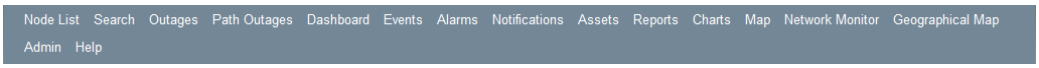


Figure 7: Menu Bar

Available links include:

- **Node List** – Displays a list of all devices managed by RUGGEDCOM NMS and provides access to further details and management options. For more information, refer to Section 6.4.2, "Viewing Device Details" .
- **Search** – Provides access to tools for searching for information about devices managed by RUGGEDCOM NMS. For more information, refer to Section 6.4.1, "Searching for Devices within RUGGEDCOM NMS " .
- **Outages** – Provides access to tools for viewing details about current and past network outages. For more information, refer to Section 5.2.5.1, "Viewing a List of Outage Notifications" .
- **Path Outages** – Displays a list of configured path outages. For more information, refer to Section 5.2.7, "Managing Path Outages" .
- **Dashboard** – Displays the dashboard, a useful tool for analyzing the health of the network. For more information, refer to Section 3.7, "Using the Dashboard" .
- **Events** – Provides access to tools for viewing, searching for, and acknowledging events. For more information, refer to Section 5.2.2, "Managing Events" .
- **Alarms** – Provides access to tools for viewing, searching for, and acknowledging alarms. For more information, refer to Section 5.2.3, "Managing Alarms" .
- **Notifications** – Provides access to tools for viewing, searching for, and acknowledging notifications. For more information, refer to Section 5.2.4, "Managing Notifications" .
- **Assets** – Displays the asset information configured for each device managed by RUGGEDCOM NMS. For more information, refer to Section 6.4.9, "Managing Asset Information" .
- **Reports** – Provides access to tools for viewing and generating performance reports. For more information, refer to Section 5.4, "Managing Performance Reports" .
- **Charts** – Displays important charts that detail the average severity of alarms, the number of outages per protocol, and the number of nodes compared to available interfaces and services.
- **Map** – Opens the logical mapping tool. For more information, refer to Section 5.5, "Managing Logical Maps"
- **Network Monitor** – Provides access to the network monitoring tool for RUGGEDCOM ROS devices. For more information, refer to Section 6.9.3, "Managing Network Monitoring" .
- **Geographical Map** – Opens the geographical mapping tool. For more information, refer to Section 5.6, "Managing Geographical Maps" .
- **Admin** – Provides access to a series of tools for configuring RUGGEDCOM NMS and the devices under its management. For more information, refer to Chapter 6, *Managing/Configuring Devices* .
- **Help** – Displays important information about the version of RUGGEDCOM NMS running on the server. For more information, refer to Section 3.6, "Viewing Product Information" .

Section 3.2
Launching RUGGEDCOM NMS

To launch RUGGEDCOM NMS on the server, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server.
2. At the shell prompt, type:

```
cd /usr/share/opennms/scripts/
/root/ruggednms_scripts/start_ruggednms.sh
```

If encryption is enabled and the passphrase is not saved locally, the **Configuration File Encryption** dialog box appears.

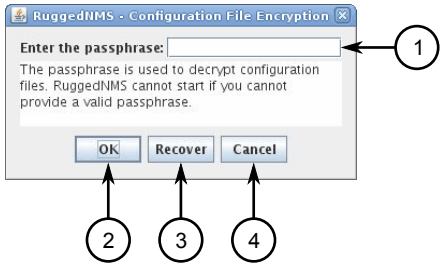


Figure 8: Configuration File Encryption Dialog Box

1. Enter the Passphrase Box **2.** OK Button **3.** Recover Button **4.** Cancel

NOTE
*If the password is forgotten, use the **Recover** to reset the encryption settings. For more information, refer to* *Section 4.10.4, "Resetting the Encryption Passphrase"* .

3. Under **Enter the passphrase**, type the passphrase and then click **OK**.
4. Log in to RUGGEDCOM NMS. For more information, refer to Section 3.5, "Logging In/Out" .

Section 3.3
Restarting RUGGEDCOM NMS

To restart RUGGEDCOM NMS on the server side, do the following:

- Open a terminal application on the RUGGEDCOM NMS server and run the following script:

  `/user/share/opennms/scripts/restart_ruggednms.sh`

Section 3.4
Default Usernames and Passwords

The following default passwords are pre-configured for RUGGEDCOM NMS:

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to RUGGEDCOM NMS, change the default passwords before commissioning the RUGGEDCOM NMS server. For more information, refer to *Section 4.8.1.4, "Resetting a User Password"* .

Mode	Username	Password
Administrator	admin	Admin123456_
Operator	operator	Operator123456_
Guest	guest	Guest123456_

Section 3.5

Logging In/Out

To log in or out of RUGGEDCOM NMS Web interface, do the following:

Logging In

1. Launch a Web browser and navigate to `{protocol}://{domain-name}:{port}/ruggednms`, where:
   - *{protocol}* is either `https` for secure connections or `http` for non-secure connections. For more information about enabling one or both protocols, refer to Section 4.2, "Enabling/Disabling HTTP and/or HTTPS Access" .
   - *{domain-name}* is the domain name for the RUGGEDCOM NMS server.
   - *{port}* is the port used by the RUGGEDCOM NMS server. For more information about controlling the designated port, refer to Section 4.2, "Enabling/Disabling HTTP and/or HTTPS Access" .

   For example:

   ```
   https://rnms.ruggedcomnms.com:8081/ruggednms
   ```

   The **Login** screen appears.

Figure 9: RUGGEDCOM NMS Login Screen

1. Username Box **2.** Password Box **3.** Log In Button

NOTE
RUGGEDCOM NMS features three default user accounts: admin, operator and guest. Additional user accounts can be added. For information about adding user accounts, refer to *Section 4.8.1.1, "Adding a User"* .

2. In the **Username** box, type the user name.

NOTE
If a unique password/passphrase has not been configured, use the factory default password. For more information, refer to *Section 3.4, "Default Usernames and Passwords"* .

IMPORTANT!
RUGGEDCOM NMS features a Brute Force Attack (BFA) protection mechanism to reduce the likelihood of a successful unauthorized login via the Web interface. This mechanism monitors the number of consecutive failed login attempts made by individual users within one minute of their first attempt. By default, after four failed login attempts, the user's account is blocked for 300000 milliseconds or five minutes.

The BFA protection mechanism is completely configurable by administrators. For more information about configuring BFA protection, refer to *Section 4.4, "Configuring Brute Force Attack Protection"* .

3. In the **Password** box, type the password associated with the user name.
4. Click **Log In**. The RUGGEDCOM NMS dashboard appears.

Logging Out

To log out, click the **Log Out** link at the bottom of any screen.

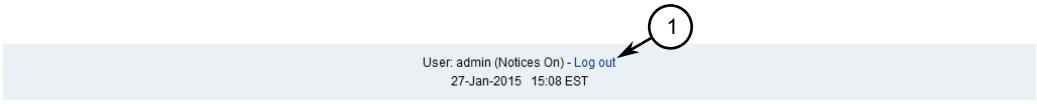


Figure 10: Logout

1. Log Out Link

Section 3.6

Viewing Product Information

To view product information about RUGGEDCOM NMS, including version information, license information, the system identifier, and more, do the following:

1. Log in to RUGGEDCOM NMS. For more information, refer to Section 3.5, “Logging In/Out” .
2. On the menu bar, click **Help**. The **Help** screen appears.

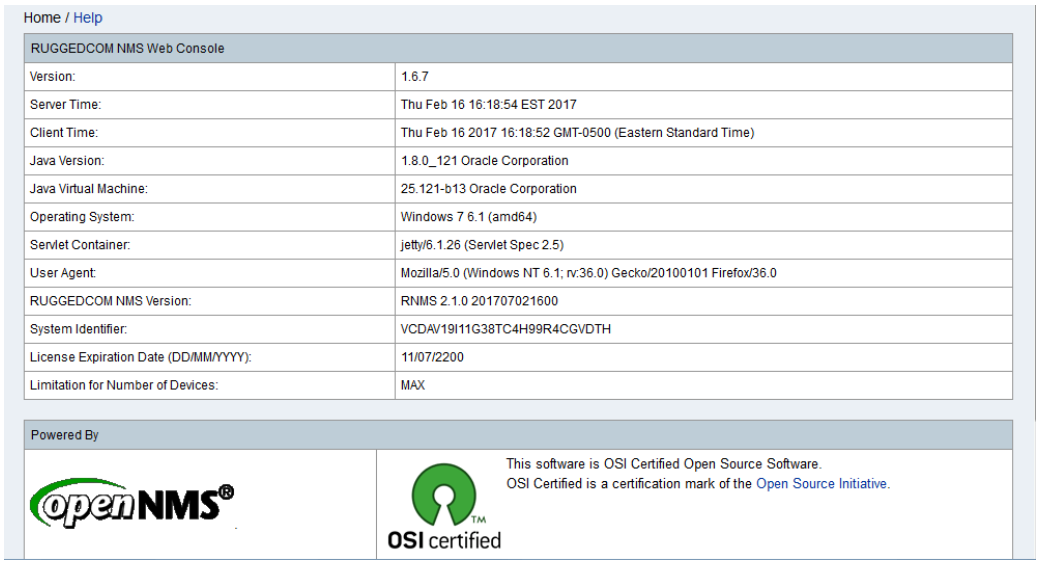


Figure 11: Help Screen (Demonstration Version Shown)

During troubleshooting or when ordering an updated license, authorized Siemens personnel may request specific information about the current installation, such as the operating system, user agent, or which versions of specific third-party applications are installed.

Section 3.7

Using the Dashboard

Similar to the **Home** screen, the **Dashboard** provides a detailed single-screen summary of the entire network managed by RUGGEDCOM NMS. It details outages and availability, outstanding alarms and notifications, and provides access to standard resource performance reports. The advantage of the Dashboard, however, is that it

can be customized for individual users, allowing them to display categories of information that are meaningful to their individual role, location, department, company, etc.

Once a user is assigned a Dashboard view, they are automatically taken to their Dashboard – bypassing the **Home** screen – whenever they start a new Web session for RUGGEDCOM NMS. Non-Dashboard users can also access the default Dashboard by clicking **Dashboard** on the menu bar.

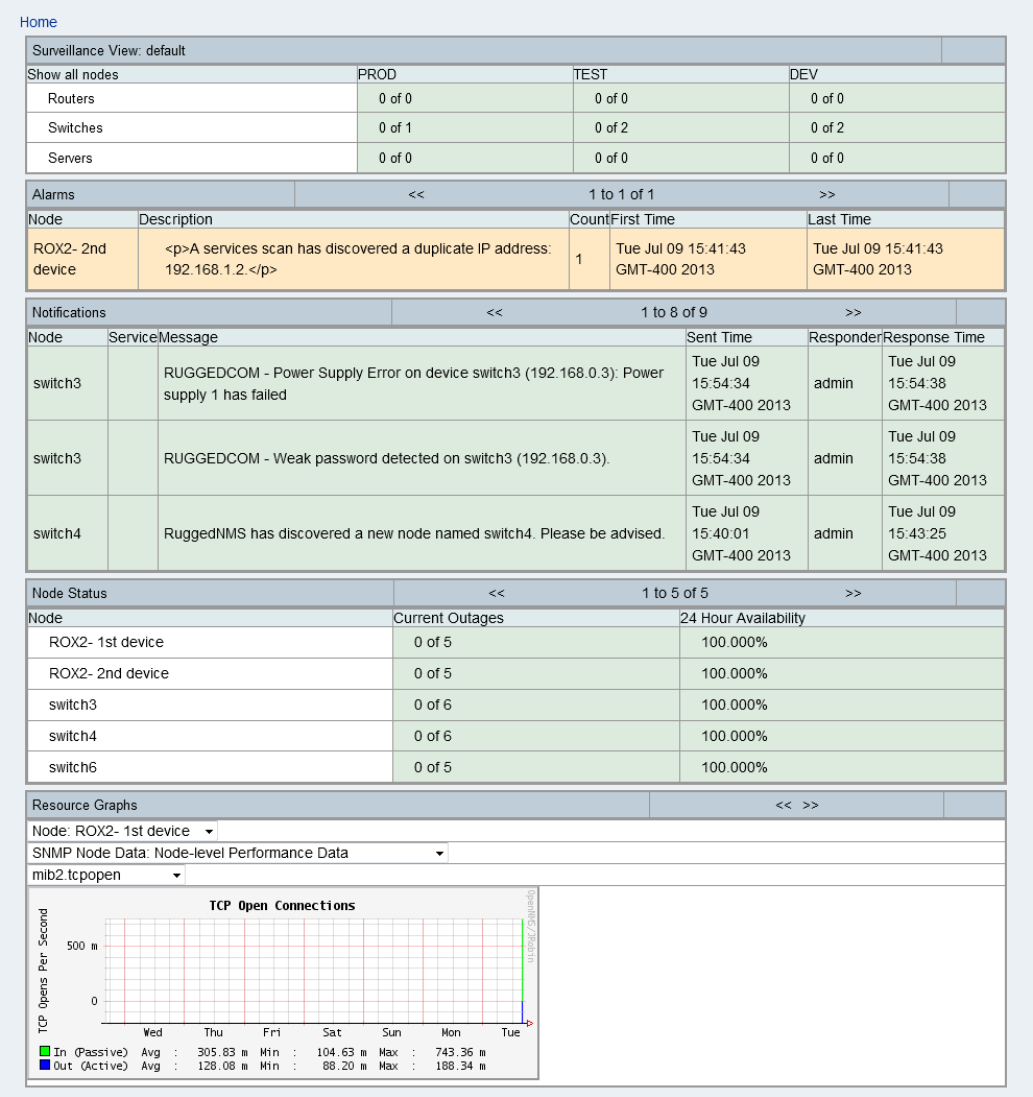


Figure 12: Default Dashboard Screen

CONTENTS

- Section 3.7.2, “Customizing the Dashboard”

Section 3.7.1
Dashlets

Each Dashboard includes the following five *dashlets*:

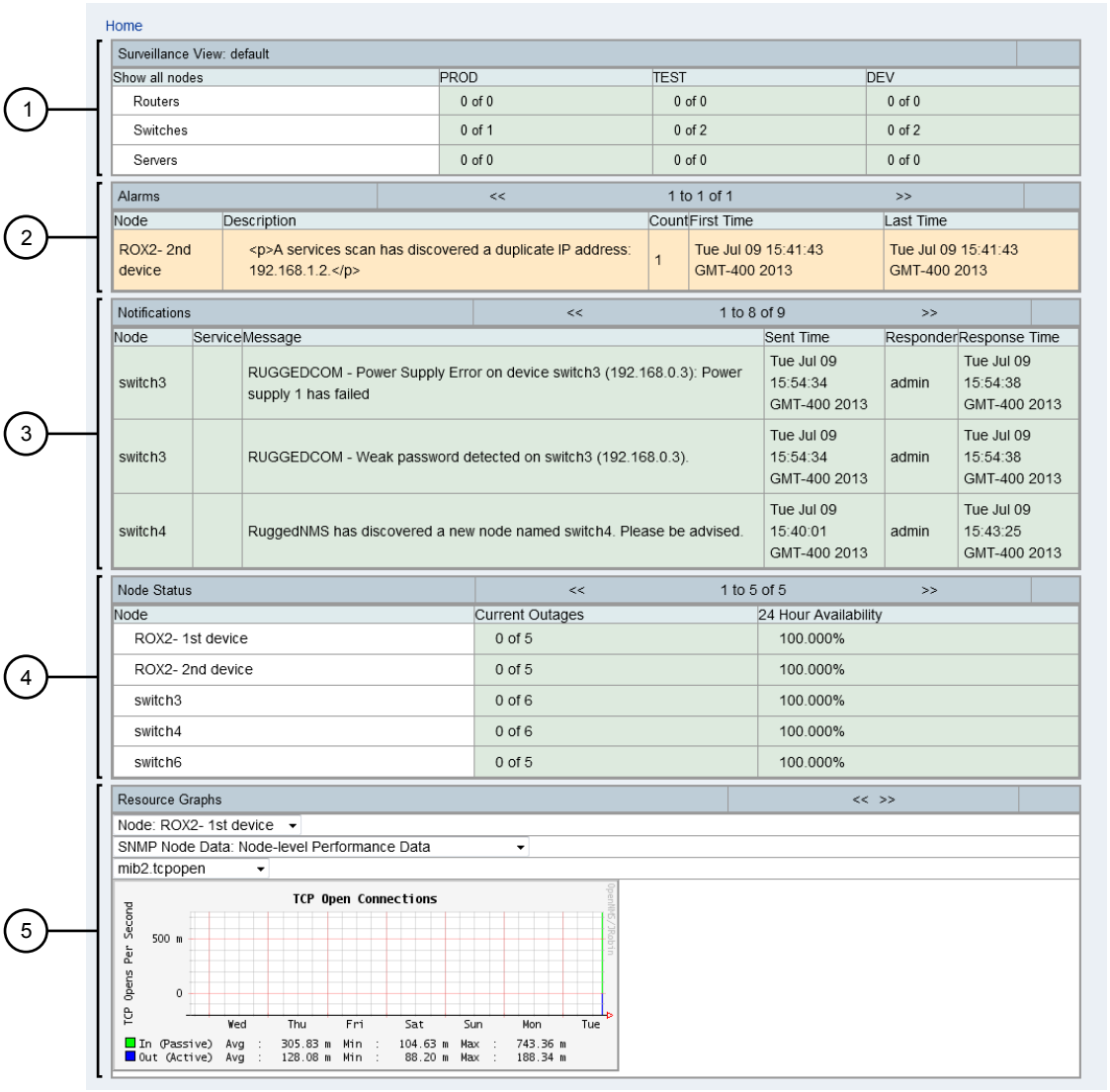


Figure 13: Dashboard Dashlets

1. Surveillance View Dashlet **2.** Alarms Dashlet **3.** Notifications Dashlet **4.** Node Status Dashlet **5.** Resource Graphs Dashlet

- **Surveillance View**
  The **Surveillance View** dashlet lists the surveillance categories assigned to the Dashboard view. The default Dashboard available for all users displays the default surveillance categories, while a customized Dashboard cany list categories chosen by the user.

Information presented in the other dashlets is based on the devices belonging to these categories. If a row or column is selected in the dashlet, the data presented in all other dashlets aligns with the selected surveillance category.

- **Alarms**
  The **Alarms** dashlet lists all outstanding alarms associated with the devices represented by the surveillance categories.
- **Notifications**
  The **Notifications** dashlet lists all outstanding notifications associated with the devices represented by the surveillance categories.
- **Node Status**
  The **Node Status** dashlet details outages and overall availability of devices represented by the surveillance categories over the last 24 hours.
- **Resource Graphs**
  The **Resource Graphs** dashlet provides quick access to standard resource performance reports related to the devices represented by the surveillance categories.

Other than the **Surveillance View** dashlet, all other dashlets include controls for scrolling through the available data.

- To view the next item in a dashlet, click **>>**
- To view the previous item in a dashlet, click **<<**

Section 3.7.2

Customizing the Dashboard

Customization of the Dashboard involves the following steps:

1. **Define Surveillance Categories**

   Add surveillance categories that are meaningful to the company and/or individual users, and remove categories that are not required. For more information, refer to Section 4.11.1, “Adding a Surveillance Category” .

2. **Assign Devices**

   Assign devices to one or more surveillance categories as needed. For more information, refer to Section 6.4.2.5, “Surveillance Category Membership” .

3. **Define Dashboard Users**

   Assign users to be Dashboard users. For more information, refer to Section 3.7.2.1, “Assigning Dashboard Users” .

4. **Define Custom Surveillance Views**

   Create a custom surveillance view for each Dashboard user. For more information, refer to Section 3.7.2.2, “Creating Custom Surveillance Views” .

CONTENTS

- Section 3.7.2.2, “Creating Custom Surveillance Views”

Section 3.7.2.1
Assigning Dashboard Users

To designate users as Dashboard users, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/magic-users.properties.xml`

2. Locate the following line and add the required user names:

   ```
   role.dashboard.users=
   ```

   For example:

   ```
   role.dashboard.users=jsmith,jdoe
   ```

3. Save and close the file.

When the assigned Dashboard users log in to RUGGEDCOM NMS, they are taken directly to the **Dashboard**, bypassing the standard **Home** screen.

Section 3.7.2.2
Creating Custom Surveillance Views

Custom surveillance views define the surveillance categories displayed in the Surveillance View dashlet on the dashboard.

To create a custom surveillance view for a user, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/surveillance-view.xml`

   The following is an example of the default `surveillance-view.xml` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<surveillance-view-configuration
 xmlns:this="http://www.opennms.org/xsd/config/surveillance-views"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.opennms.org/xsd/config/surveillance-views http://www.opennms.org/
xsd/config/surveillance-views.xsd"
 default-view="default" >
 <views>
                                      1

  <!-- default view here -->
  <view name="default" refresh-seconds="300" >
                                      2

   <rows>
                                      3

    <row-def label="Routers" >
                                      4

     <category name="Routers"/>
    </row-def>
    <row-def label="Switches" >
```

```
     <category name="Switches" />
    </row-def>
    <row-def label="Servers" >
     <category name="Servers" />
    </row-def>
   </rows>
   <columns>
                                        5

    <column-def label="PROD" >
                                        6

     <category name="Production" />
                                        7

    </column-def>
    <column-def label="TEST" >
     <category name="Test" />
    </column-def>
    <column-def label="DEV" >
     <category name="Development" />
    </column-def>
   </columns>
  </view>
 </views>
</surveillance-view-configuration>
```

1. The `<views>` element defines the various views available.
2. The `<view>` element defines the rows and columns in the Surveillance View dashlet.
3. The `<row>` element defines the rows.
4. The `<row-def>` element defines a row.
5. The `<column>` element defines the columns.
6. The `<column-def>` element defines a column.
7. The `<column>` element defines the surveillance category for the given row or column.

2. Create a new view by either duplicating an existing `<view>` – including its child elements – or adding a new `<view>` element.
3. Set the `name` attribute for the view element to the name of the user. For example:

```
<view name="jsmith" refresh-seconds="300" >
```

4. [Optional] Change the refresh interval in the `refresh-seconds` attribute to control how often RUGGEDCOM NMS refreshes the data in the Surveillance View dashlet.
5. Under the `<rows>` and `<columns>` elements, add `<row-def>` and `<column-def>` elements respectively for each surveillance category.

   For example:

```
<rows>
 <row-def label="Servers" >
  <category name="Servers" />
 </row-def>
</rows>
<columns>
 <column-def label="PROD" >
  <category name="Production" />
 </column-def>
 <column-def label="TEST" >
  <category name="Test" />
 </column-def>
 <column-def label="DEV" >
  <category name="Development" />
```

```
 </column-def>
</columns>
```

In this example, the Servers surveillance category will intersect with the Production, Test and Development surveillance categories in the Surveillance View dashlet.

6. Save and close the file.
7. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 3.8

Available Shell Scripts

Several Linux shell scripts are available to support the installation and operation of RUGGEDCOM NMS. All scripts are located in `/usr/share/opennms/scripts/`.

Script	Command	Description
`add-admin-user.sh`	**`./add-admin-user.sh`**	Opens the `magic-users.properties` configuration file for editing.
`add-cert.sh`	**`./add-cert.sh`**	Creates a self-signed certificate. This script should ONLY be run once when RUGGEDCOM NMS is first installed.
`clean_logs.sh`	**`./clean_logs.sh`**	Clears out-dated information from the log files.
`clear_database.sh`	**`./clear_database.sh`**	Clears all existing data from the database. This script should only be used when absolutely necessary as all historical data in the database will be lost.
`config_ldap_login.sh`	**`./config_ldap_login.sh`**	Opens the LDAP configuration file for editing.
`configure_ruggednms.sh`	**`./configure_ruggednms.sh`**	Configures the system. This script should ONLY be run once when RUGGEDCOM NMS is first installed.
`create_java_link.sh`	**`./create_java_link.sh`**	Creates a symbolic link to the latest JAVA JDK that is installed in the system.
`edit_configmgnt.sh`	**`./edit_configmgnt.sh`**	Edits the configuration file for the Configuration Management Daemon.
`edit_file.sh`	**`./edit_file.sh`** *`filename`*	Opens the selected configuration file for editing.
`edit_javamail.sh`	**`./edit_javamail.sh`**	Opens the Java mail configuration file for editing.
`get_logs.sh`	**`./get_logs.sh`**	Archives the current RUGGEDCOM NMS server system log files to `/usr/share/opennms/scripts/log_files.tar.gz`. This would typically be used in response to a request from Siemens Customer Support to capture the log files for submission to Siemens for debugging purposes.
`get_rosdebugkit.sh`	**`./get_rosdebugkit.sh`**	Archives all available ROS debug kit data acquired by RUGGEDCOM NMS to `/usr/share/opennms/scripts/ros_debugkit.tar.gz`.
`get_systemID.sh`	**`./get_systemID.sh`**	Retrieves the unique System identifier for the Product Activation Key (PAK).
`install_PAK.sh`	**`./install_PAK.sh`**	Installs the Product Activation Key (PAK). The PAK file created by Siemens must be in the `/usr/share/opennms/scripts` directory for installation.

Script	Command	Description
`install_rox_firmware.sh` <ROX zip filename>	**`./install_rox_firmware.sh`** *`zip-filename`*	Installs a ROX firmware release on the ROX software repository server under RUGGEDCOM NMS (`/usr/share/opennms/ruggednms/debian386`). Example: `./install_rox_firmware.sh ROX.zip`
`read_daemon_log.sh`	**`./read_daemon_log.sh`** *`log-filename`*	Opens the daemon log. Example: `./read_daemon_log.sh capsd.log`
`read_webapp_log.sh`	**`./read_webapp_log.sh`** *`log-filename`*	
`restart_postgresql.sh`	**`./restart_postgresql.sh`**	Restarts the Postgre SQL database daemon.
`start_ruggednms.sh`	**`./start_ruggednms.sh`**	Starts the RUGGEDCOM NMS application.
`status.sh`	**`./status.sh`**	Displays the status of RUGGEDCOM NMS processes.
`stop_ruggednms.sh`	**`./stop_ruggednms.sht`**	Stops the RUGGEDCOM NMS application.
`update_env.sh`	**`./update_env.sh`**	This script should ONLY be run once, when RUGGEDCOM NMS is first installed.

Section 3.9

Editing RUGGEDCOM NMS Configuration Files

RUGGEDCOM NMS makes extensive use of XML (eXtensible Meta Language) files to configure RUGGEDCOM NMS and the devices it manages. Care and attention to detail is required when editing XML files, as small errors can affect the performance of RUGGEDCOM NMS.

When editing XML configuration files, note the following:

- Avoid potential problems by only making the recommended modifications to the RUGGEDCOM NMS configuration files outlined in this User Guide.
- Backup files before editing them in case the previous version needs to be restored.
- XML code wrapped between comment tags (e.g. <-- and -->) is ignored by RUGGEDCOM NMS. Comment tags are used to provide information to the user or to disable features/settings. For example:

```
<--<element attribute="value"/>-->
```

- Always make sure XML tags are properly closed. For example:

```
<element attribute="value"> <-- Wrong
<element attribute="value"/> <-- Correct
```

- Always make sure attribute values are enclosed in double-quotes, not single quotes. For example:

```
<element attribute='value'/> <-- Wrong
<element attribute="value"/> <-- Correct
```

- Each XML file adheres to a specific hierarchical structure of parent and children elements. Make sure elements are properly contained within their parent structure.
- Make sure each file is saved with UTF-8 encoding.

4 Configuring RUGGEDCOM NMS

This chapter describes how to configure RUGGEDCOM NMS.

CONTENTS

Section 4.1

Creating a Self-Signed Certificate

RUGGEDCOM NMS initially includes an SSL certificate common to all installations when accessing the user interface via HTTPS. However, this default certificate should be replaced before RUGGEDCOM NMS is deployed.

NOTE
A self-signed certificate is a certificate signed by the person creating it, not a trusted Certificate Authority (CA). A self-signed certificate allows a user to create a unique certificate for their installation of RUGGEDCOM NMS.

NOTE
Self-signed certificates are flagged by browsers as insecure.

To create a self-signed certificate, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and run the following script:

   `/root/ruggednms_scripts/add_cert.sh`

   A command prompt window appears.

NOTE
Passwords must be at least six characters long.

2. If a certificate already exists, a confirmation message appears asking whether or not to remove the certificate. Press **Y** and then press **Enter** to remove the current certificate.
3. When prompted, type a Keystore password. The certificate is generated and installed.

Section 4.2
Enabling/Disabling HTTP and/or HTTPS Access

To enable/disable HTTP, HTTPS, or both, do the following:

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. HTTP is not a secure protocol. Communications over HTTP can be intercepted and critical information, such as authentication passwords and session cookies can be viewed by others.

HTTPS is enabled by default in RUGGEDCOM NMS and should not be disabled unless necessary.

NOTE
*Parameters are disabled, or **commented out**, by adding a # symbol before the parameter name. Uncommenting a parameter (removing the # symbol) enables the parameter.*

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/opennms.properties`

2. The following parameters control HTTP and HTTPS access:

   HTTP Access

   ```
   org.opennms.netmgt.jetty.port = 8080
   opennms.rtc-client.http-post.base-url = http://localhost:8080/ruggednms/rtc/post
   opennms.datafeeder.message-broker.http.url = http://localhost:8080/netmap/messagebroker/
   streamingamf
   ```

   HTTPS Access

   ```
   org.opennms.netmgt.jetty.https-port = 8081
   opennms.rtc-client.https-post.base-url = https://localhost:8081/ruggednms/rtc/post
   opennms.datafeeder.messagebroker.https.url = https://localhost:8081/netmap/messagebroker/
   securestreamingamf
   ```

   For strictly HTTP access, comment out the HTTPS-related parameters, or vice versa for HTTPS access. Alternatively, enable both HTTP and HTTPS access by uncommenting each set of parameters.

3. Save and close the file.
4. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, “Restarting RUGGEDCOM NMS ” .

Section 4.3
Enabling SSH Access

Before using RUGGEDCOM NMS to access devices via the SSH hyperlink, the SSH client must be installed and the registry updated on the client machine.

To enable the SSH hyperlink, do the following:

1. Obtain the PuTTY SSH Windows Installer (**.msi**).
2. Copy the directory `/usr/share/opennms/ssh_client` to the C:\ drive of the client machine.
3. Install the PuTTY SSH client on the client machine using the installation wizard.
4. Restart Windows.
5. Log in to the client machine.
6. In Windows Explorer, navigate to ***C:\ssh_client***.
7. Double click **ssh.reg** to update the registry. A prompt appears to confirm if you are sure you want to add information to the registry.
8. Click **Yes** to confirm. A message appears confirming successful addition to the registry.
9. [Optional] Click the **SSH** hyperlink on the RUGGEDCOM NMS node page to open an SSH session to the device.

Section 4.4
Configuring Brute Force Attack Protection

RUGGEDCOM NMS features a Brute Force Attack (BFA) protection mechanism to reduce the likelihood of an attack via the Web interface. This mechanism monitors the number of consecutive failed login attempts made by individual users within one minute of their first attempt. By default, after three failed login attempts, the user's account is blocked for 300000 milliseconds or five minutes.

IMPORTANT!
The BFA protection system is not applicable to SNMP. Follow proper security practices for configuring SNMP. For example:

- *Do not use SNMP over the Internet*
- *Use a firewall to limit access to SNMP*
- *Do not use SNMPv1*

The following error message appears on the login screen when a user is blocked:

```
Your log-in attempt failed, please try again
Reason: User account is locked
```

The attack is also logged in the `spring` under /usr/share/opennms/logs/daemon. For example:

```
2015-01-16 14:32:10,958 WARN  [1547012359@qtp-1597817717-21] LoggerListener:
 Authentication event AuthenticationFailureBadCredentialsEvent: admin; details:
 org.springframework.security.web.authentication.WebAuthenticationDetails@fffbcba8: RemoteIpAddress:
 10.200.19.184; SessionId: y4bzup8orfcebui6tq3voooh; exception: Bad credentials
2015-01-16 14:32:12,970 WARN  [1547012359@qtp-1597817717-21] LoggerListener:
 Authentication event AuthenticationFailureBadCredentialsEvent: admin; details:
 org.springframework.security.web.authentication.WebAuthenticationDetails@fffbcba8: RemoteIpAddress:
 10.200.19.184; SessionId: y4bzup8orfcebui6tq3voooh; exception: Bad credentials
```

```
2015-01-16 14:32:14,530 WARN  [1547012359@qtp-1597817717-21] LoggerListener:
 Authentication event AuthenticationFailureBadCredentialsEvent: admin; details:
 org.springframework.security.web.authentication.WebAuthenticationDetails@fffbcba8: RemoteIpAddress:
 10.200.19.184; SessionId: y4bzup8orfcebui6tq3voooh; exception: Bad credentials
2015-01-16 14:32:17,791 WARN  [1547012359@qtp-1597817717-21] Spring: Brute force attack detected.
 Locked User account [admin].
```

The BFA protection mechanism is completely configurable by administrators.

To configure the BFA protection mechanism, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/configmgtd-configuration.xml`

2. Locate and modify the values for the following parameters:

   ```
   brute-force-login-threshold="3"
   brute-force-burst-time-slice="60000"
   brute-force-block-timeout="300000"
   ```

Parameter	Description
brute-force-login-threshold	**Default:** 3 The maximum number of failed login attempts allowed within the specified time period.
brute-force-burst-time-slice	**Default:** 60000 The time in milliseconds (ms) in which the maximum number of failed login attempts must be exceeded before a user is blocked.
brute-force-block-timeout	**Default:** 300000 The time in milliseconds (ms) a user is blocked from accessing RUGGEDCOM NMS.

3. Save and close the file.
4. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, “Restarting RUGGEDCOM NMS ” .

Section 4.5

Configuring/Disabling a Remote Syslog Server

RUGGEDCOM NMS can be set to automatically forward all RUGGEDCOM NMS server system log files to a remote Syslog server, or event message collector.

To configure or disable a previous configured remote Syslog server for RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **Northbound Interface** and then click **Log Export**. The **Log Export** screen appears.

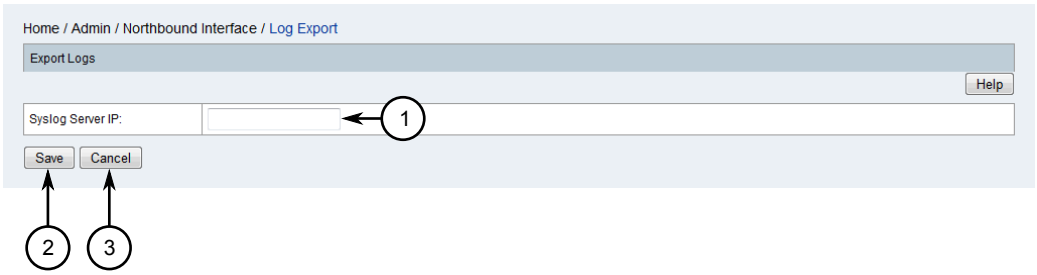


Figure 14: Log Export Screen

1. Syslog Server IP Address Box **2.** Save Button **3.** Cancel Button

2. Under **Syslog Server IP Address**, either:
   - Type the IP address of the remote Syslog server to enable remote Syslog collection
   - Delete the current IP address to disable remote syslog collection
3. Click **Save**.

Section 4.6

Configuring the Management Daemon

RUGGEDCOM NMS uses a configuration management daemon to download configuration and firmware files from RUGGEDCOM devices to the RUGGEDCOM NMS server for backup and maintenance. The behavior of the daemon is controlled by an XML configuration file that consists of a single `<configmgtd-configuration/>` that includes a series of attributes. For example:

```
<configmgtd-configuration
   threads = "1"
   bulk-upload-retry = "6"
   poll-config-ver-retry = "3"
   .
   .
   .
</configmgtd-configuration>
```

Configuring the Daemon

To configure the attributes for the configuration management daemon, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and run the following script:

   `/root/ruggednms_scripts/edit_configmgmt.sh`

   This script opens the following configuration file in gedit :

   `/usr/share/opennms/etc/configmgtd-configuration.xml`

   The configuration file consists of a single `<configmgtd-configuration/>` element with multiple attributes that define the behavior of the daemon.
2. Configure the following attributes for the `<configmgtd-configuration/>` element as required:

Attribute	Description
archive-location	The directory on the RUGGEDCOM NMS server where old data for RUGGEDCOM devices managed by RUGGEDCOM NMS is stored.
basestation-accumulated-upgrade-failure-percentage	The maximum percentage of failed upgrades to RUGGEDCOM WIN base station devices allowed. If the overall upgrade failure percentage exceeds the threshold, all pending upgrades are canceled. For example, a value of *50* allows the bulk upgrade process to fail for half of the selected WIN base station devices. If RUGGEDCOM NMS is unable to upgrade one of the remaining devices, the bulk upgrade process is aborted.
basestation-file-operation-after-wait	The time in milliseconds (ms) to wait between RUGGEDCOM WIN base station file operations.
basestation-file-operation-init-wait	The time in milliseconds (ms) to wait before starting a RUGGEDCOM WIN base station file operation.
basestation-file-operation-wait-interval	The time in milliseconds (ms) to wait between base station file operations.
basestation-file-transfer-after-wait	The time in milliseconds (ms) to wait after a file is transferred to a RUGGEDCOM WIN base station device.
basestation-file-transfer-retry-time	The maximum number times to retry transferring a file to a RUGGEDCOM WIN base station device.
basestation-password	The password for the RUGGEDCOM WIN base station file transfer.
basestation-password-max-length	The maximum length of the file transfer password that can be used for a RUGGEDCOM WIN base station device.
basestation-poller-interval	The SNMP poll interval for RUGGEDCOM WIN base station device.
basestation-reboot-init-wait	The time in milliseconds (ms) to wait initially for a RUGGEDCOM WIN base station to reboot.
basestation-reboot-wait-interval	The time in milliseconds to wait between RUGGEDCOM WIN base station reboots.
basestation-run-secondary-wait-interval	The time in milliseconds (ms) to wait between base station run secondary retries.
basestation-sftp-session-timeout	The maximum time in milliseconds (ms) before SFTP file transfer to RUGGEDCOM WIN base stations timeout.
basestation-snmp-operation-interval	The time in milliseconds (ms) to wait after a successful firmware upgrade for a RUGGEDCOM WIN base station's secondary partition.
basestation-ssh-port-number	The SSH port number used for accessing RUGGEDCOM WIN base stations.
basestation-timeout-operation	The maximum time in milliseconds (ms) before a file operations on RUGGEDCOM WIN base stations timeout.
basestation-timeout-reboot	The maximum time in milliseconds (ms) to wait for a RUGGEDCOM WIN base station to reboot.
basestation-upgrade-secondary-timeout	The time in milliseconds (ms) to wait for a firmware upgrade to a RUGGEDCOM WIN base station's secondary partition to complete.
basestation-upgrade-thread-number	The number of concurrent firmware upgrade operations for RUGGEDCOM WIN base stations.
basestation-upgrade-timeout	The time in milliseconds (ms) allowed for a single a RUGGEDCOM WIN base station firmware upgrade.
basestation-upgrade-wait-interval	The time in milliseconds (ms) to wait before checking the status of a RUGGEDCOM WIN base station firmware upgrade.
bulk-upload-retry	The maximum number of attempts allowed to upload a file to a RUGGEDCOM ROS device.

Attribute	Description
basestation-user	The user name for a RUGGEDCOM WIN base station file transfer.
config-file-location	The directory on the RUGGEDCOM NMS server where RUGGEDCOM device files (configuration files and firmware images) are stored.
config-location	The location of the RUGGEDCOM NMS configuration file.
config-poller-interval	The time in milliseconds (ms) between successive polling and daemon thread executions.
cpe-accumulated-upgrade-failure-percentage	The maximum percentage of failed upgrades to RUGGEDCOM WIN CPE devices allowed. If the overall upgrade failure percentage exceeds the threshold, all pending upgrades are canceled. For example, a value of *50* allows the bulk upgrade process to fail for half of the selected WIN CPE devices. If RUGGEDCOM NMS is unable to upgrade one of the remaining devices, the bulk upgrade process is aborted.
cpe-file-operation-after-wait	The time in milliseconds (ms) to wait between RUGGEDCOM WIN CPE device file operations.
cpe-file-operation-init-wait	The time in milliseconds (ms) to wait before starting a RUGGEDCOM WIN CPE device file operation.
cpe-file-operation-timeout	The time in milliseconds (ms) to wait for a file operation on a RUGGEDCOM WIN CPE device to complete before aborting the operation.
cpe-file-operation-wait-interval	The time in milliseconds (ms) to wait between CPE file operations.
cpe-file-transfer-after-wait	The time in milliseconds (ms) to wait after a file is transferred to a RUGGEDCOM WIN CPE device.
cpe-file-transfer-retry-time	The maximum number times to retry transferring a file to a RUGGEDCOM WIN base station device.
cpe-password	The password for the RUGGEDCOM WIN CPE file transfer.
cpe-password-max-length	The maximum length of the file transfer password that can be used for a RUGGEDCOM WIN CPE device.
cpe-poller-interval	The time in milliseconds (ms) between successive polling and daemon thread executions.
cpe-reboot-timeout	The maximum time in milliseconds (ms) to wait for a RUGGEDCOM WIN CPE to reboot.
cpe-reboot-init-wait	The time in milliseconds (ms) to wait initially for a RUGGEDCOM WIN CPE to reboot.
cpe-reboot-wait-interval	The time in milliseconds to wait between RUGGEDCOM WIN CPE reboots.
cpe-sftp-session-timeout	The maximum time in milliseconds (ms) before SFTP file transfer to RUGGEDCOM WIN CPEs timeout.
cpe-snmp-timeout	The maximum time in milliseconds (ms) that SNMP transactions with RUGGEDCOM WIN CPEs can remain alive.
cpe-ssh-port-number	The SSH port number used for accessing RUGGEDCOM WIN CPEs.
cpe-upgrade-ini-file-name	The name of the upgrade INI file needed for RUGGEDCOM WIN CPE firmware upgrades.
cpe-upgrade-secondary-timeout	The time in milliseconds (ms) to wait for a firmware upgrade to a RUGGEDCOM WIN CPE's secondary partition to complete.
cpe-upgrade-thread-number	The number of concurrent firmware upgrade operations for RUGGEDCOM WIN CPEs.
cpe-upgrade-timeout	The time in milliseconds (ms) allowed for a single a RUGGEDCOM WIN CPE firmware upgrade.
cpe-upgrade-wait-interval	The time in milliseconds (ms) to wait before checking the status of a RUGGEDCOM WIN CPE firmware upgrade.
cpe-user	The user name for a RUGGEDCOM WIN base station SFTP file transfer.
default-password-check	When enabled, default password check will be enforced during login, user creation and password reset. Options include `true` (enabled) or `false` (disabled).
delete-node-option	When enabled, users are alerted to a node-down condition and given the option to either delete or keep the node. Options include `true` (enabled) or `false` (disabled).

Attribute	Description
download-file-list	A list of files on a RUGGEDCOM ROS device to be downloaded when a user attempts to download debug information. For more information about downloading debug information, refer to Section 6.9.1, "Downloading ROS Debug Information" .
gold-config-temp-location	The directory on the RUGGEDCOM NMS server where temporary gold configurations should be stored.
initial-sleep-time	The time in milliseconds (ms) before the polling daemon will commence after RUGGEDCOM NMS is started. This delay allows all the components of RUGGEDCOM NMS to fully initialize before beginning to collect data from RUGGEDCOM devices under management.
ln-sleep	The time in milliseconds (ms) during which the Local Notification dialog checks for updates.
ln-sound-expired	The duration in milliseconds (ms) of the sound played by the Local Notification dialog.
main-location	The directory on the RUGGEDCOM NMS server where firmware image files from RUGGEDCOM ROS devices are stored.
password	The standard administrator account password for RUGGEDCOM devices.
password-complexity	When enabled, password complexity will be enforced during password creation and password reset. Options include `true` (enabled) or `false` (disabled).
password-complexity-pattern	Complex password definition in regular expression.
password-complexity-message	Complex password reminder message.
password-length	The length of passwords generated using the Device Password Management feature. **NOTE** *Some versions of RUGGEDCOM ROS impose a limit of 32 characters.*
reset-time	The time in milliseconds (ms) that RUGGEDCOM NMS waits after a reset before trying to re-establish communications with a device.
reset-time-out	The maximum amount of time in milliseconds (ms) during which RUGGEDCOM NMS tries to re-establish communications with a device after issuing a *reset* request. Upon timeout, RUGGEDCOM NMS declares the device unreachable.
rox-archive-location	The directory on the RUGGEDCOM NMS server where archive files are stored for replaced RUGGEDCOM ROX devices.
ros-config-management-dir	The directory on the RUGGEDCOM NMS server where generic configuration files for RUGGEDCOM ROS devices are stored.
ros-gold-config-location	The directory on the RUGGEDCOM NMS server where gold configurations for RUGGEDCOM ROS devices are stored.
ros-password-max-length	The maximum length of the password that can be used for a RUGGEDCOM ROS device.
rox-backuprestore-time-out	The time in milllseconds (ms) to wait for a RUGGEDCOM ROX **`backuprestore`** command to complete.
rox-config-archive-dir	The directory on the RUGGEDCOM NMS server where archived configuration files for RUGGEDCOM ROX devices are stored.
rox-config-file-location	The directory on the RUGGEDCOM NMS server where current configuration files for RUGGEDCOM ROX devices are stored. on the RUGGEDCOM NMS server for downloaded ROX configuration files.
rox-config-management-dir	The directory on the RUGGEDCOM NMS server where generic archived configuration files for RUGGEDCOM ROX devices are stored.
rox-config-poller-interval	The time in milliseconds (ms) between successive polling executions on RUGGEDCOM ROX devices.

Attribute	Description
rox-config-webmin-dir	The directory on the RUGGEDCOM NMS server where archived Webmin configuration files for RUGGEDCOM ROX devices are stored.
rox-download-file-list	A list of files for miscellaneous downloads, typically log files for RUGGEDCOM ROX devices.
rox-download-misc-time-out	The time in milliseconds (ms) to wait for a miscellaneous file to download.
rox-initial-config-archive-name	The initial file name for archived configuration files from RUGGEDCOM ROX devices.
rox-initial-config-webmin-name	The initial file name for archived Webmin configuration files for RUGGEDCOM ROX devices.
rox-nightbackup-time-out	The time in milliseconds (ms) to wait for the nightly configuration backup operation to complete on RUGGEDCOM ROX devices.
rox-password	The administrator password for RUGGEDCOM ROX devices.
rox-password-max-length	The maximum length of the password that can be used for a RUGGEDCOM ROX device.
rox-reboot-time-out	The time in milliseconds (ms) to wait for RUGGEDCOM ROX devices to reboot.
rox-srs-location	The directory on the RUGGEDCOM NMS server where software repositories for RUGGEDCOM ROX devices are stored.
rox-srs-url	The URL for the RUGGEDCOM ROX software repository server where upgrade packages are stored.
rox-ssh-port-number	The SSH port number used for accessing RUGGEDCOM ROX SSH servers.
rox-upgrade-bandwidth-limit	The bandwidth limit for RUGGEDCOM ROX software upgrades. Options include: 0 (disabled), 1-8 kbps, 2-16 kbps, 3-32 kbps, 4-64 kbps, 5-128 kbps, 6-256 kbps, 7-512 kbps, or 8-1 Mbps.
rox-upgrade-time-out	The time in milliseconds to wait for a RUGGEDCOM ROX software upgrade to complete.
rox-uploadconfig-ack-time-out	The time in milliseconds to wait for acknowledgement from RUGGEDCOM NMS after applying a new configuration and restarting RUGGEDCOM daemons.
rox-uploadconfig-apply-time-out	The time in milliseconds (ms) to wait while applying a partial archived configuration file to a RUGGEDCOM ROX device.
rox-uploadconfig-create-time-out	the time in milliseconds (ms) to wait for a partial archived configuration file to be created for a RUGGEDCOM ROX device.
rox-uploadconfig-list-time-out	The time in milliseconds (ms) to wait for a list of subsystems for a RUGGEDCOM ROX device.
rox-user	The user ID to be used by RUGGEDCOM NMS for administrative access to ROX devices.
rox-wait-reboot-time-out	The time in milliseconds (ms) to wait to re-establish communication with RUGGEDCOM ROX device after a **`reboot`** command.
rox2-app-management-retry	The maximum number of attempts to install/uninstall an app on a RUGGEDCOM ROX II device.
rox2-app-management-exec-interval	The time in milliseconds required for an app to be installed/uninstalled on a RUGGEDCOM ROX II device.
rox2-app-management-wait-interval	The time in milliseconds (ms) to wait before checking the status of the app install/uninstall process on a RUGGEDCOM ROX II device.
rox2-app-management-timeout-interval	The maximum time in milliseconds (ms) allowed for the app install/uninstall process to complete on RUGGEDCOM ROX II devices.
rox2-archive-location	The directory on the RUGGEDCOM NMS server where archived configuration files for RUGGEDCOM ROX II devices are stored.
rox2-config-management-dir	The directory on the RUGGEDCOM NMS server where current configuration files for RUGGEDCOM ROX II devices are stored.
rox2-config-upload-download-retry	The maximum number of attempts to upload/download RUGGEDCOM ROX II NETCONF configuration files.

Attribute	Description
rox2-confirmed-commit-timeout	The time in milliseconds (ms) to complete a RUGGEDCOM ROX II NETCONF confirmed-commit operation.
rox2-debianarm-firmware-url	The URL for the RUGGEDCOM ROX II firmware (ARM device) repository server for firmware upgrades.
rox2-debianarm-firmware-location	The directory on the RUGGEDCOM NMS server where firmware upgrades from the RUGGEDCOM ROX II firmware (ARM device) repository are stored.
rox2-debianppc-firmware-url	The URL for the RUGGEDCOM ROX II firmware (PPC device) repository server for firmware upgrades.
rox2-debianppc-firmware-location	The directory on the RUGGEDCOM NMS server where firmware upgrades from the RUGGEDCOM ROX II firmware (PPC device) repository are stored.
rox2-debian386-firmware-location	The directory on the RUGGEDCOM NMS server where firmware upgrades from the RUGGEDCOM ROX II firmware (x86 device) repository are stored.
rox2-debian386-firmware-url	The URL for the RUGGEDCOM ROX II firmware (x86 device) repository server for firmware upgrades.
rox2-device-location	The directory on the RUGGEDCOM NMS server where downloaded configuration files RUGGEDCOM ROX II devices are stored.
rox2-download-debug-info-location	The directory on the RUGGEDCOM NMS server where debug information for RUGGEDCOM ROX II devices is stored.
rox2-feature-keys-url	The URL for the RUGGEDCOM ROX II feature key repository server for feature key installation.
rox2-feature-keys-location	The directory on the RUGGEDCOM NMS server where feature keys from the RUGGEDCOM ROX II feature key repository are stored.
rox2-feature-keys-retry	The maximum number of attempts to install a RUGGEDCOM ROX II feature key installation.
rox2-gold-config-location	The directory on the RUGGEDCOM NMS server where gold configurations for RUGGEDCOM ROX II devices are stored.
rox2-launch-upgrade-xml	The directory on the RUGGEDCOM NMS server where the RUGGEDCOM ROX II NETCONF *launch upgrade* RPC file is stored.
rox2-netconf-connection-timeout	The time in milliseconds (ms) to wait for a RUGGEDCOM ROX II NETCONF connection operation to complete.
rox2-netconf-port-number	The RUGGEDCOM ROX II NETCONF server port number.
rox2-netconf-session-timeout	The maximum time in milliseconds (ms) to wait for activity on an inactive RUGGEDCOM ROX II NETCONF session. If there is no activity before the time period ends, the session is closed.
rox2-reboot-exec-interval	The time in milliseconds (ms) required to trigger the reboot process on RUGGEDCOM ROX II devices.
rox2-reboot-timeout-interval	The time in milliseconds (ms) to wait for the reboot process to complete for RUGGEDCOM ROX II devices.
rox2-reboot-wait-interval	The time in milliseconds (ms) to wait before checking the status of the reboot process on RUGGEDCOM ROX II devices.
rox2-remote-cli-location	The file path to the CLI configuration file on RUGGEDCOM ROX II devices.
rox2-remote-logs-location	The file path to the debug log file on RUGGEDCOM ROX II devices.
rox2-reset-xml	The directory on the RUGGEDCOM NMS server where the RUGGEDCOM ROX II NETCONF *reset* RPC file is stored.
rox2-sftp-cli-wait-interval	The time in milliseconds (ms) to wait before polling the status of the CLI configuration files on RUGGEDCOM ROX II devices.
rox2-sftp-cli-timeout-interval	The time in milliseconds (ms) allowed for CLI configuration files to download from RUGGEDCOM ROX II devices.

Attribute	Description
rox2-sftp-retry	The maximum number of attempts allowed to download a CLI configuration file from a RUGGEDCOM ROX II device.
rox2-upgrade-exec-interval	The time in milliseconds (ms) required to trigger the firmware upgrade process for RUGGEDCOM ROX II devices.
rox2-upgrade-progress-xml	The directory on the RUGGEDCOM NMS server where the RUGGEDCOM ROX II NETCONF *upgrade status check* RPC file is stored.
rox2-upgrade-retry	The maximum number of attempts allow to upgrade the firmware on a RUGGEDCOM ROX II device.
rox2-upgrade-timeout-interval	The maximum time in milliseconds (ms) the firmware upgrade process to complete on RUGGEDCOM ROX II devices.
rox2-upgrade-wait-interval	The time in milliseconds (ms) to wait before checking the status of a RUGGEDCOM ROX II firmware upgrade.
sb-expired	The time in milliseconds (ms) the last update/error message stays visible in the status bar on the RUGGEDCOM NMS Web interface.
sb-sleep	The time in milliseconds (ms) the status bar on the RUGGEDCOM NMS Web interface checks for updates.
snmp-timeout	The maximum time in milliseconds (ms) that SNMP process threads can remain alive.
temp-location-event	The directory on the RUGGEDCOM NMS server where files temporarily downloaded by the Configuration Management thread are stored.
temp-location-poller	The directory on the RUGGEDCOM NMS server where files temporarily downloaded by the polling daemon are stored.
temp-location-upload	The directory on the RUGGEDCOM NMS server where files uploaded by the Configuration Management thread are stored.
threads	The number of threads that will be spawned to poll RUGGEDCOM devices.
wait-time	The time in milliseconds (ms) between SNMP polls after a RUGGEDCOM device is reset.

3. Save and close the file.

The Configuration Management Log

The configuration management daemon will log all transactions in the following log file:

```
/usr/share/opennms/ruggednms/logs/daemon/configMgtd.log
```

Section 4.7

Configuring a JavaMail Interface

RUGGEDCOM NMS uses JavaMail to send notifications and reports via e-mail.

To configure an interface between RUGGEDCOM NMS and a JavaMail server, do the following:

1. Make sure all users who wish to receive notifications and reports via e-mail have valid e-mail addresses configured in RUGGEDCOM NMS. For more information about configuring a user's profile, refer to Section 4.8.1.2, “Editing a User” .
2. Make sure notifications are enabled. For more information, refer to Section 5.2.4.5, “Enabling/Disabling Notifications” .

3. Make sure the desired notifications are enabled. For more information, refer to Section 5.2.4.6, "Enabling/Disabling Specific Notifications" .
4. Open a terminal application on the RUGGEDCOM NMS server and run the following script:

   `/root/ruggednms_scripts/edit_javamail.sh`

   This script opens the JavaMail configuration file in gedit .

   The following is an example of a JavaMail configuration file:

```
################################################################################
# This file is the configuration for the JavaMailer class.
# It is used to specify the details of the JavaMailer system properties
################################################################################
# Properties are defined but commented out, indicating the default values.
#

# This property defines system sender account.
#
# The default setting is root@[127.0.0.1]
org.opennms.core.utils.fromAddress=RuggedNMS

# These properties define the SMTP Host.
#
org.opennms.core.utils.mailHost=192.168.1.3
org.opennms.core.utils.mailer=smtpsend
org.opennms.core.utils.transport=smtp
org.opennms.core.utils.debug=true
#org.opennms.core.utils.smtpport=25
#org.opennms.core.utils.smtpssl.enable=false
#org.opennms.core.utils.quitwait=true
#
# This property controls the use of the JMTA,
# the default is true
org.opennms.core.utils.useJMTA=false

# These properties define the Mail authentication.
#
org.opennms.core.utils.authenticate=false
org.opennms.core.utils.authenticateUser="user"
org.opennms.core.utils.authenticatePassword="password"
#org.opennms.core.utils.starttls.enable=false

# These properties configure message content
#
#org.opennms.core.utils.messageContentType=text/plain
#org.opennms.core.utils.charset=us-ascii
```

5. Configure the following parameters as required:

> **IMPORTANT!**
> *By default, a # symbol is placed before each parameter. Remove this symbol to enable a parameter.*

Parameter	Description
org.opennms.core.utils.fromAddress	The e-mail address that appears in the From field of all e-mails sent to the server.
org.opennms.core.utils.mailHost	The IP address of the SMTP server used to send e-mail. The recommended value is 127.0.0.1.
org.opennms.core.utils.mailer	The name of the mass mailer used in the X-Mailer header.

Parameter	Description
org.opennms.core.utils.transport	The transport protocol to use. Specify `smtp` unless another transport protocol is required. Do not use if `org.opennms.core.utils.useJMTA` is set to false.
org.opennms.core.utils.debug	**Synopsis:** { true, false } When enabled (true), debug information is displayed.
org.opennms.core.utils.smtpport	**Default:** 25 The port used to connect to the SMTP server.
org.opennms.core.utils.smtpssl.enable	**Synopsis:** { true, false } When enabled (true), SSL is used to connect to the SMTP host.
org.opennms.core.utils.quitwait	**Synopsis:** { true, false } When enabled (true), the e-mail client will wait for a response from the SMTP server to the final QUIT command. Disable (false) if the SMTP server takes too long to respond or does not respond correctly.
org.opennms.core.utils.useJMTA	**Synopsis:** { true, false } When enabled (true), a non-queuing Java-based MTA is used. The MTA looks up Mail eXchanger (MX) records and sends e-mail directly to the appropriate mail server. When disabled (false), emails are delivered to the smart host defined by org.opennms.core.utils.mailHost, which relays the e-mail to the appropriate mail server. If not configured, the default is `true`.
org.opennms.core.utils.authenticate	**Synopsis:** { true, false } When enabled (true), user authentication is required. Make sure the `org.opennms.core.utils.authenticateUser` and `org.opennms.core.utils.authenticatePassword` parameters are configured.
org.opennms.core.utils.authenticateUser	The user name for the user account on the SMTP server. Only required when authentication is enabled.
org.opennms.core.utils.authenticatePass word	The password for the user account on the SMTP server. Only required when authentication is enabled.
org.opennms.core.utils.starttls.enable	**Synopsis:** { true, false } When enabled (true), the STARTTLS command (if supported by the server) is used to switch to a TLS-protected connection before issuing login commands. Requires additional configuration of Java Trust stores.
org.opennms.core.utils.messageContent Type	**Default:** text/plain The MIME type to set when sending the message. When sending HTML in e-mails, set to `text/html`.
org.opennms.core.utils.charset	**Default:** us-ascii The character set encoding used for all e-mails.

6. Save and close the file.
7. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, “Restarting RUGGEDCOM NMS ” .

Section 4.8

Managing Users, Groups and Roles

This section describes how to configure and manage users, groups, roles and authentication in RUGGEDCOM NMS.

CONTENTS

Section 4.8.1

Managing Users

This section describes how to manage and configure users in RUGGEDCOM NMS.

CONTENTS

Section 4.8.1.1

Adding a User

To add a user, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Users**. The **User List** screen appears.

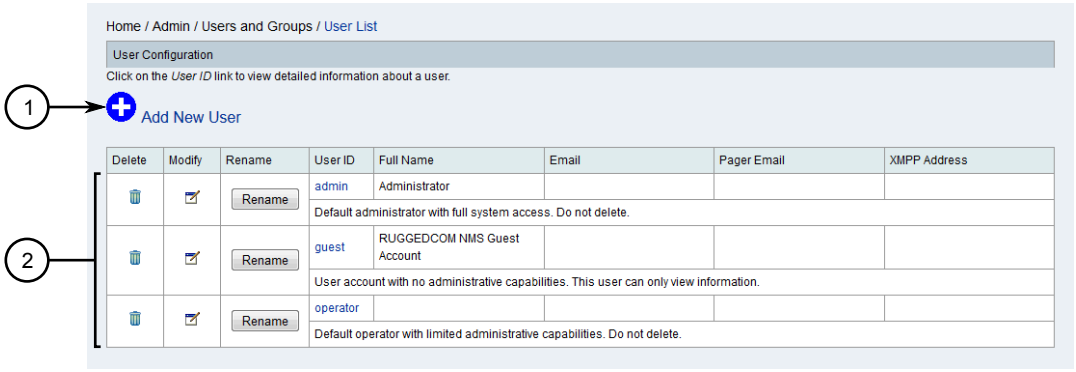


Figure 15: User List Screen

1. Available Users **2.** Add New User Button

2. Click **Add New User**. The **New User** screen appears.

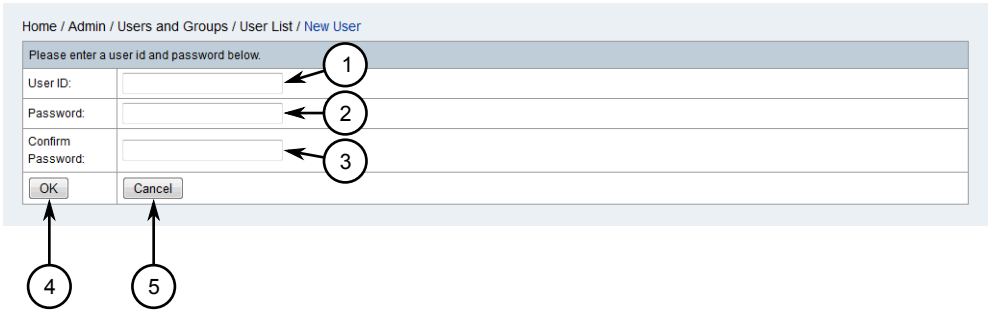


Figure 16: New User Screen

1. User ID Box **2.** Password List **3.** Confirm Password Box **4.** OK Button **5.** Cancel Button

3. Configure the following parameters:

Parameter	Description
User ID	The name of the user.
Password	The user's password. The password must contain at least one lower case letter, one upper case letter and one special character, with a minimum password length of 8 characters.
Confirm Password	The user's password.

4. Click **OK**. The **Modify User** screen appears.

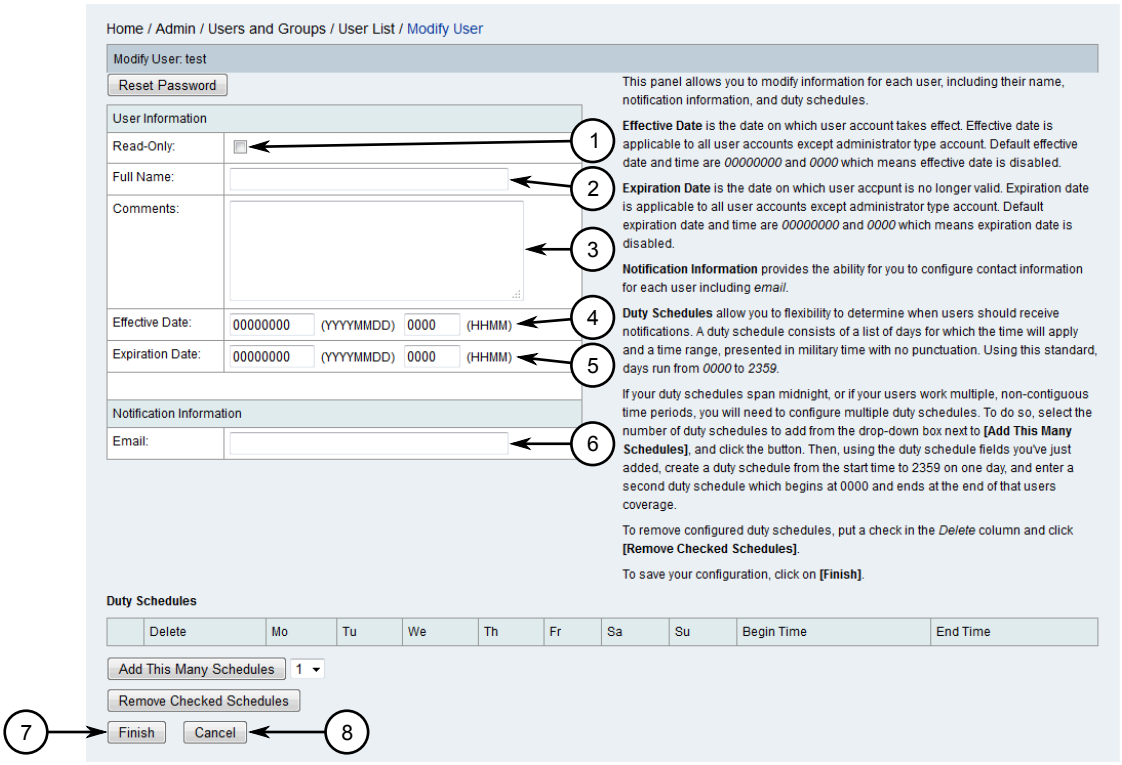


Figure 17: Modify User Screen

1. Read-Only Check Box **2.** Full Name Box **3.** Comments Box **4.** Effective Date Boxes **5.** Expiration Date Boxes **6.** Email Box **7.** Finish Button **8.** Cancel Button

5. Configure the following parameters:

Parameter	Description
Read-Only	When enabled (checked), the user can only view their user profile. Account self-service is only available when **Read-Only** is disabled (cleared).
Full Name	The user's full name. This parameter is optional.
Comments	Additional information related to the user. This parameter is optional.
Effective Date	The date and time when the user account becomes active.
Expiration Date	The date and time at which the user account is deactivated. The user will be unable to start a new Web session following this point in time.
Email	The user's preferred e-mail address.

NOTE
Duty schedules can be added for individual users or to a group of users.

6. [Optional] Configure one or more duty schedules for the user. For more information, refer to Section 4.8.4.1, "Adding/Deleting Duty Schedules for Users" .

> **IMPORTANT!**
> *All new users have limited access rights, similar to the standard guest profile. To expand a user's rights, add them to a user group.*

7. [Optional] Add the user to a user group. For more information, refer to Section 4.8.2.2, "Editing a User Group" .
8. Click **Finish** to create the new user.

Section 4.8.1.2
Editing a User

To add a user, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Users**. The **User List** screen appears.

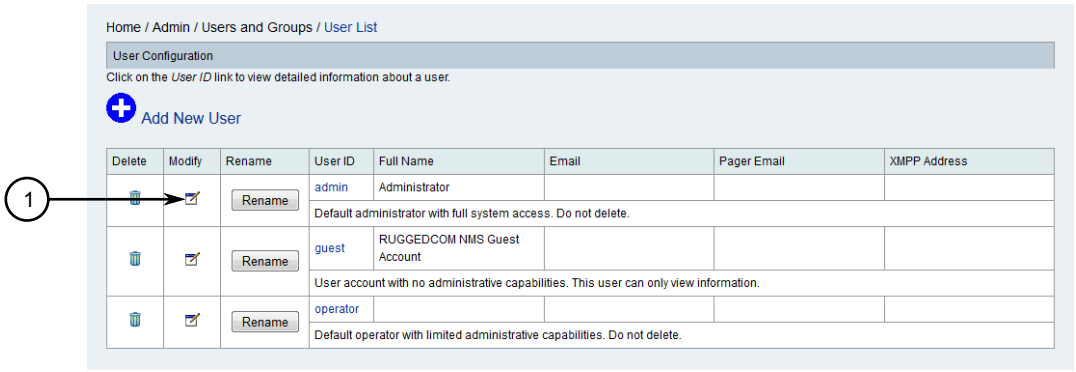


Figure 18: User List Screen

1. Available Users **2.** Modify Icon

2. Click the **Modify** icon next to the chosen user profile. The **Modify User** screen appears.

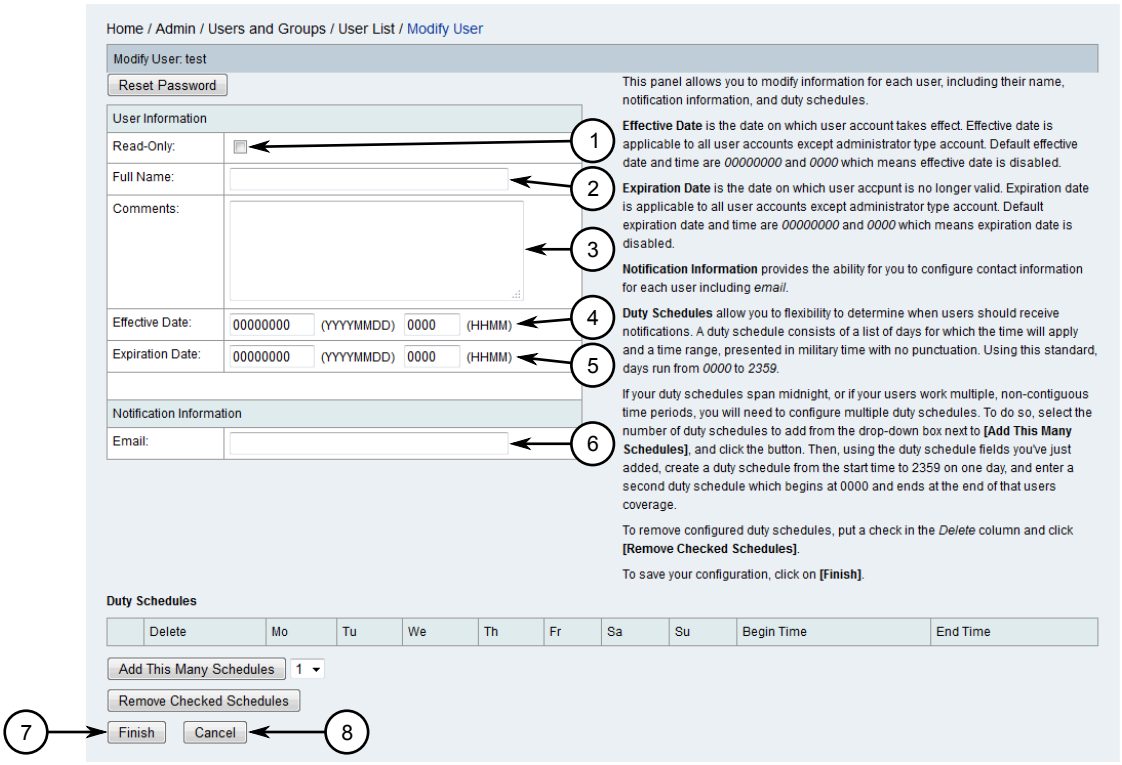


Figure 19: Modify User Screen

1. Read-Only Check Box **2.** Full Name Box **3.** Comments Box **4.** Effective Date Box **5.** Expiration Date Box **6.** Email Box **7.** Finish Button **8.** Cancel Button

3. Configure the following parameters:

Parameter	Description
Read-Only	When enabled (checked), the user can only view their user profile. Account self-service is only available when **Read-Only** is disabled (cleared).
Full Name	The user's full name. This parameter is optional.
Comments	Additional information related to the user. This parameter is optional.
Effective Date	The date and time when the user account becomes active. Not applicable to administrator accounts.
Expiration Date	The date and time at which the user account is deactivated. The user will be unable to start a new Web session following this point in time. Not applicable to administrator accounts.
Email	The user's preferred e-mail address.

4. Configure the user's duty schedule. For more information, refer to Section 4.8.4.1, "Adding/Deleting Duty Schedules for Users" .
5. Click **Finish** to create the new user.

Section 4.8.1.3
Renaming a User

To rename a user, do the following:

> **NOTE**
> *The admin user profile cannot be renamed.*

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Users**. The **User List** screen appears.

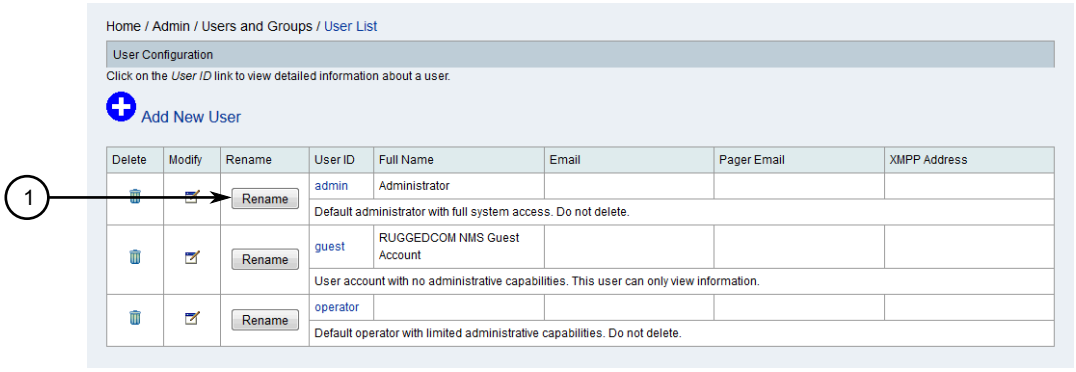


Figure 20: User List Screen

1. Rename Button

2. Click the **Rename** button next to the chosen user profile. A dialog box appears.

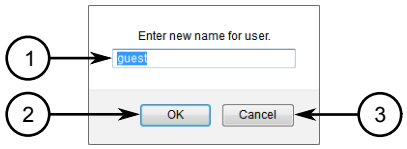


Figure 21: Rename Dialog Box

1. Username Box **2.** OK Button **3.** Cancel Button

3. Enter a new user name.
4. Click **OK** to rename the user.

Section 4.8.1.4
Resetting a User Password

To reset a user password, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Users**. The **User List** screen appears.

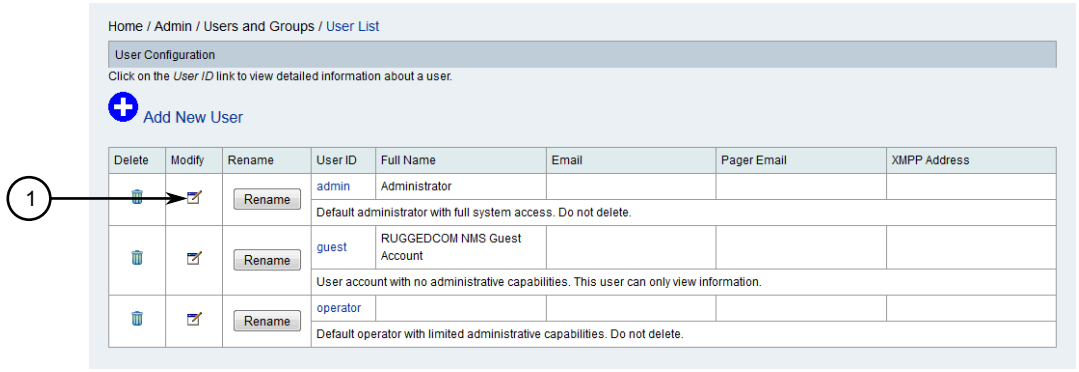


Figure 22: User List Screen

1. Modify Icon

2. Click the **Modify** icon next to the chosen user profile. The **Modify User** screen appears.

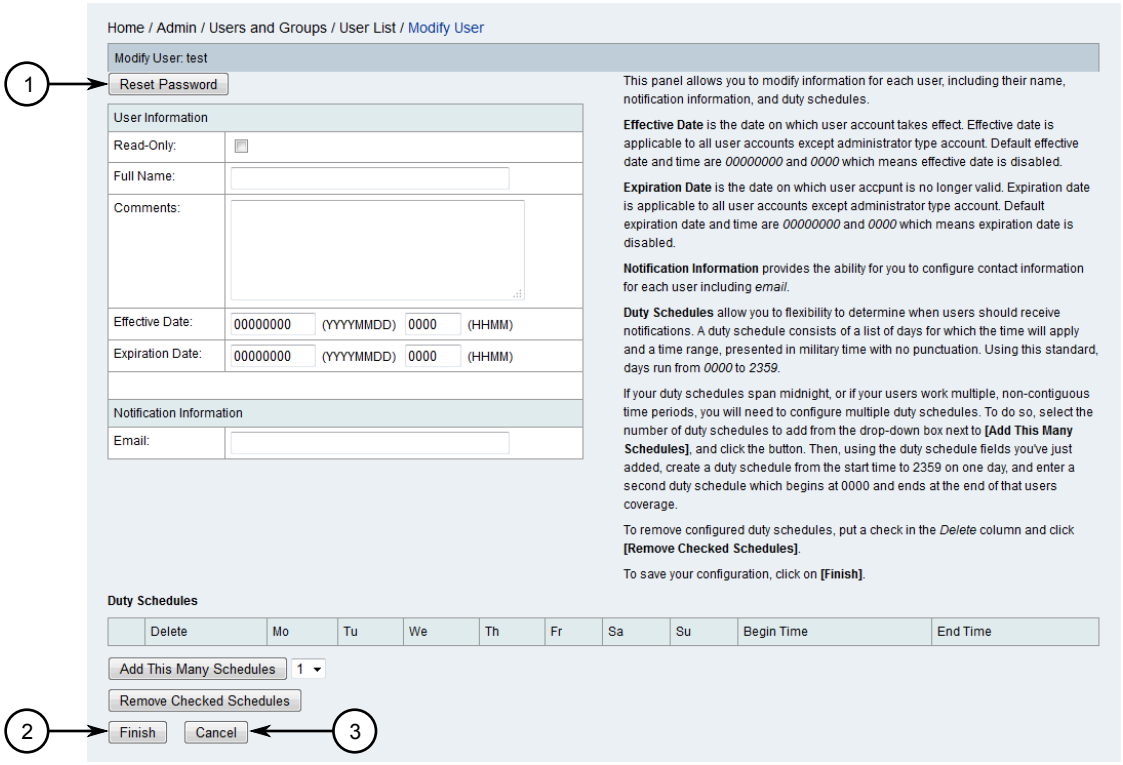


Figure 23: Modify User Screen

1. Reset Password Button **2.** Finish Button **3.** Cancel Button

3. Click **Reset Password**. A dialog box appears.

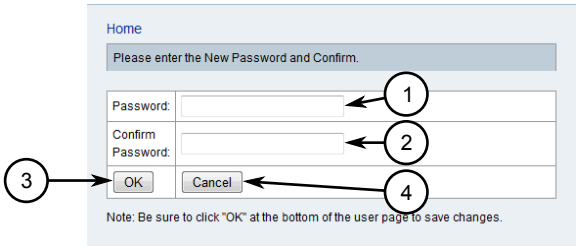


Figure 24: Reset Password Dialog Box

1. User ID Box **2.** Password List **3.** Confirm Password Box **4.** OK Button **5.** Cancel Button

4. Configure the following parameters:

Parameter	Description
Password	The user's password. The password must contain at least one lower case letter, one upper case letter and one special character, with a minimum password length of 8 characters.
Confirm Password	The user's password.

5. Click **OK**.
6. Click **Finish** to save the changes.

Section 4.8.1.5

Deleting a User

To delete a user, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Users**. The **User List** screen appears.

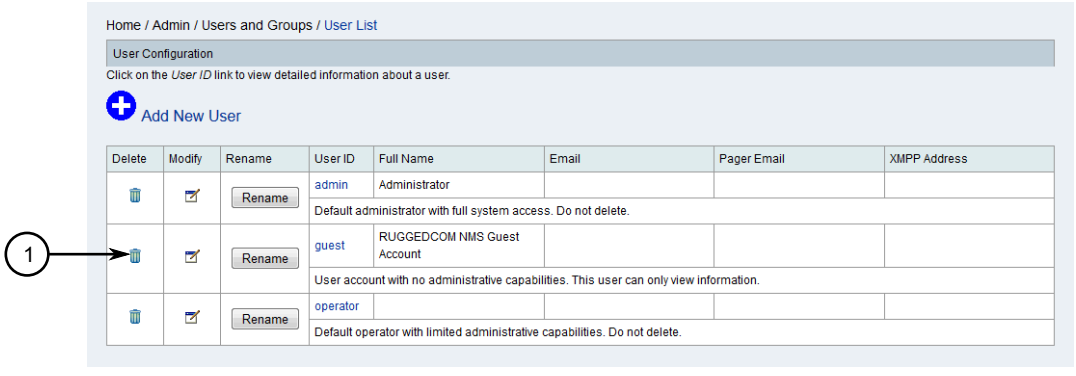


Figure 25: User List Screen

1. Delete Icon

2. Click the **Delete** icon next to the chosen user profile. A confirmation dialog box appears.

3. Click **OK** to delete the user.

Section 4.8.2
Managing User Groups

Assign users to user groups to grant them additional access rights beyond the default rights given to guests, and include them in notifications intended for a select audience. By default, RUGGEDCOM NMS is configured with two groups – *Admin* and *Operator* – used to identify administrators and operators. Additional user groups can be added as suits the organization.

CONTENTS

Section 4.8.2.1
Adding a User Group

To add a user group, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Groups**. The **Group List** screen appears.

Figure 26: Group List Screen

1. Available Groups **2.** Add New Group Link

2. Click **Add new group**. The **New Group** screen appears.

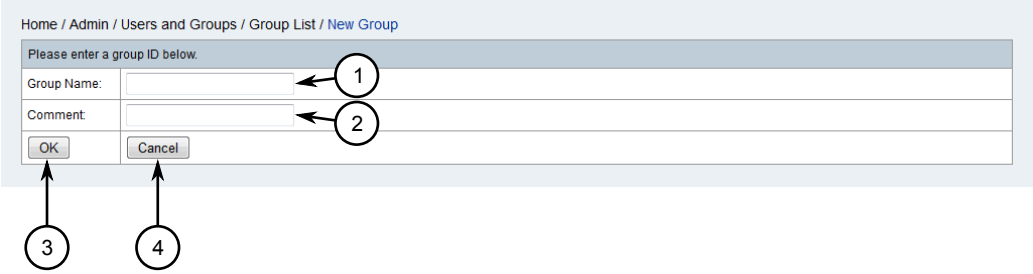


Figure 27: New Group Screen

1. Group Name Box **2.** Comment Box **3.** OK Button **4.** Cancel Button

3. Under **Group Name**, type the name of the new group.
4. [Optional] Under **Comment**, type a description of the new group.
5. Click **OK**. The **Modify Group** screen appears.

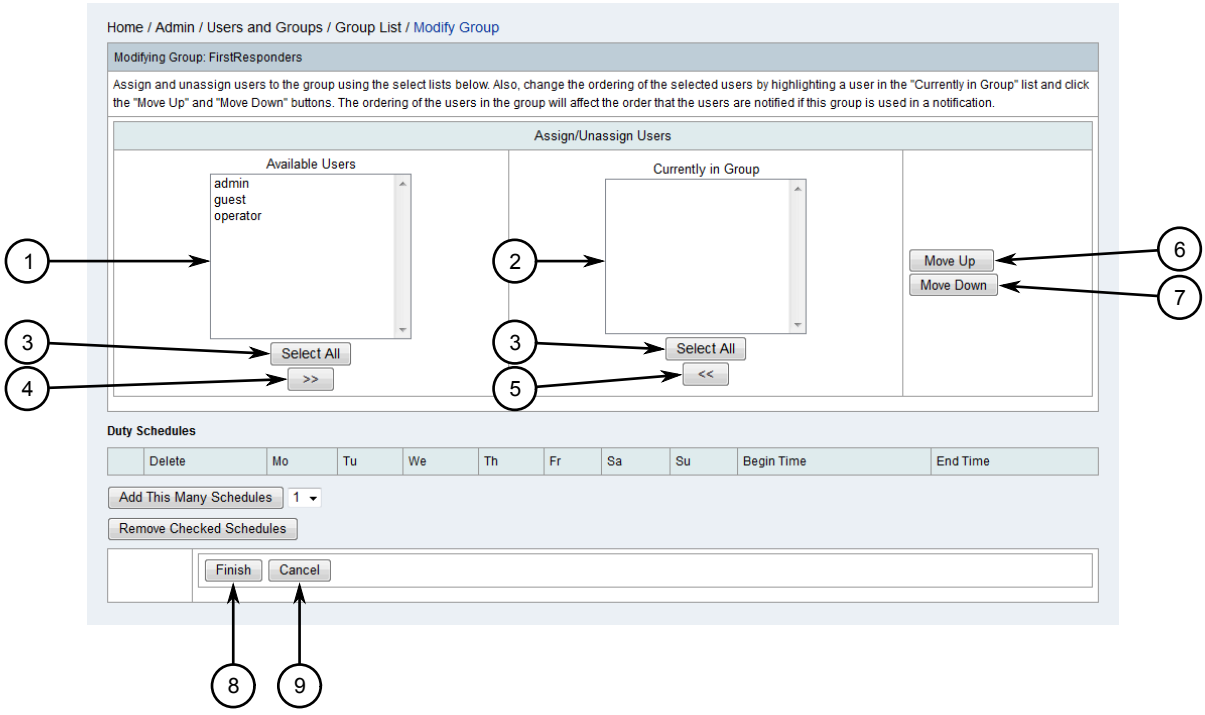


Figure 28: Modify Group Screen

1. Available Users List **2.** Currently In Group List **3.** Select All Button **4.** Add Button **5.** Remove Button **6.** Move Up Button **7.** Move Down Button **8.** Finish Button **9.** Cancel Button

NOTE

*To select consecutive users, click the first user, then hold **Shift** and click the last user. To select specific users, click the first user, and then hold **Ctrl** and select other users from the list.*

6. Select users from the **Available Users** list and then click the **Add** (>>) button. The selected users are moved to the **Currently in Group** list.
7. [Optional] Use the **Move Up** and **Move Down** buttons to change the order of the users in the **Currently in Group** list. Notifications are sent first to users at the top of the list.

> **NOTE**
> *Duty schedules can be added for individual users or to a group of users.*

8. [Optional] Configure one or more duty schedules for the group. For more information, refer to Section 4.8.4.2, "Adding/Deleting Duty Schedules for a Group" .
9. Click **Finish**.

Section 4.8.2.2
Editing a User Group

To edit an existing user group, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Groups**. The **Group List** screen appears.

Figure 29: Group List Screen

1. Available Groups **2.** Modify Icon

2. Click the **Modify** icon next to the chosen group. The **Modify Group** screen appears.

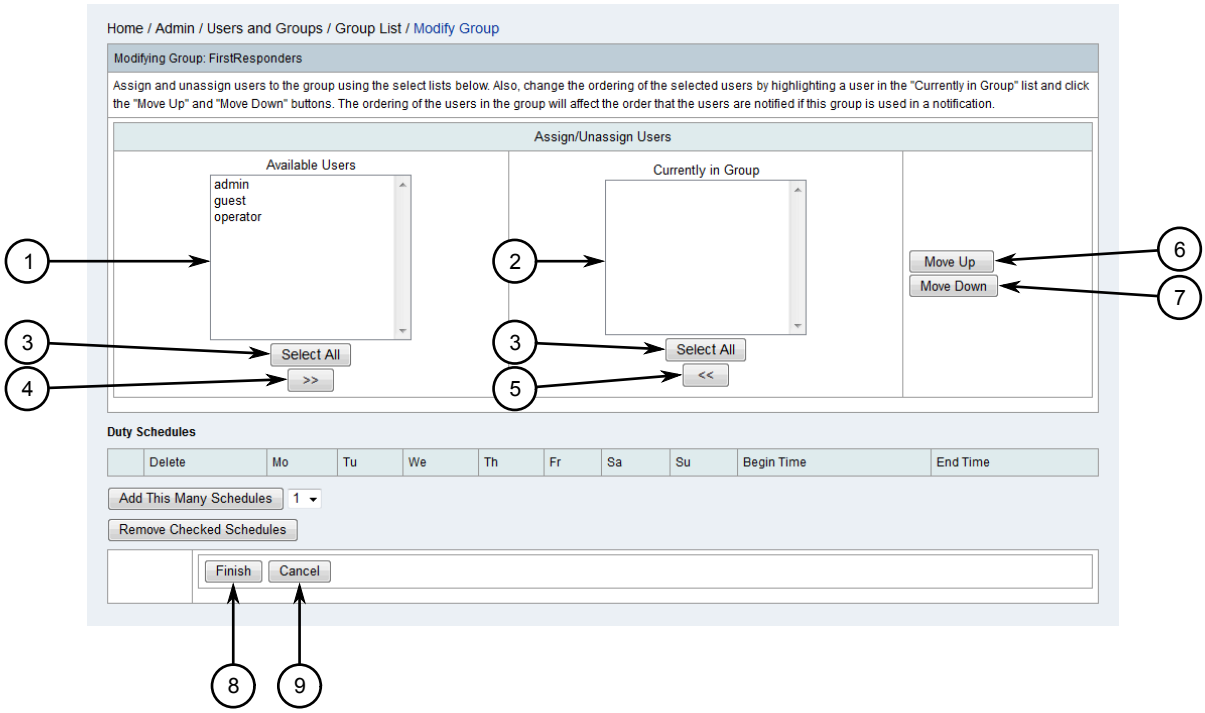


Figure 30: Modify Group Screen

1. Available Users List **2.** Currently In Group List **3.** Select All Button **4.** Add Button **5.** Remove Button **6.** Move Up Button **7.** Move Down Button **8.** Finish Button **9.** Cancel Button

CAUTION!
Risk of removing Administrator login credentials. Make sure not to unassign the last Admin user from the Admin user group, as this will remove their administrator privileges. If this occurs, contact Siemens Customer Support.

NOTE
*To select consecutive users, click the first user, then hold **Shift** and click the last user. To select specific users, click the first user, and then hold **Ctrl** and select other users from the list.*

3. [Optional] Select users from either the **Available Users** or **Currently in Group** lists and use the **Add** (>>) or **Remove** (<<) buttons to move them. The selected users are moved to the opposite list.
4. [Optional] Use the **Move Up** and **Move Down** buttons to change the order of the users in the **Currently in Group** list. Notifications are sent first to users at the top of the list.

NOTE
Duty schedules can be added for individual users or to a group of users.

5. [Optional] Updated the duty schedules for the group. For more information, refer to Section 4.8.4.2, “Adding/Deleting Duty Schedules for a Group” .
6. Click **Finish**.

Section 4.8.2.3
Renaming a User Group

To rename a user group, do the following:

NOTE
The admin group cannot be renamed.

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Groups**. The **Group List** screen appears.

Figure 31: Group List Screen

1. Available Groups **2.** Rename Button

2. Click the **Rename** button next to the chosen group. A dialog box appears.

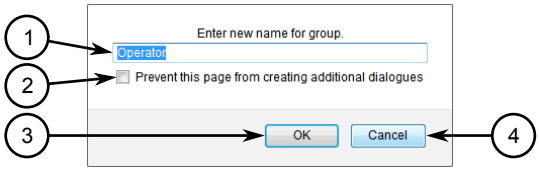


Figure 32: Rename Dialog Box

1. Group Name Box **2.** OK Button **3.** Cancel Button

3. Enter a new name for the group.
4. Click **OK** to rename the group.

Section 4.8.2.4
Deleting a User Group

To delete a user group, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Groups**. The **Group List** screen appears.

Figure 33: Group List Screen

1. Delete Icon **2.** Available Groups

2. Click the **Delete** icon next to the chosen group. A confirmation dialog box appears.
3. Click **OK** to delete the group.

Section 4.8.3

Managing User Roles

Roles are used in combination with destination paths to determine which users should receive a notification when an event occurs. Only users assigned to the selected role(s) who are on-call will be notified initially. If the notification is not acknowledged within the configured time period, the notification will be automatically escalated and sent to the users not on-call or to the configured supervisor that is on-call.

CONTENTS

Section 4.8.3.1

Adding a User Role

To add a user role, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Roles**. The **Role List** screen appears.

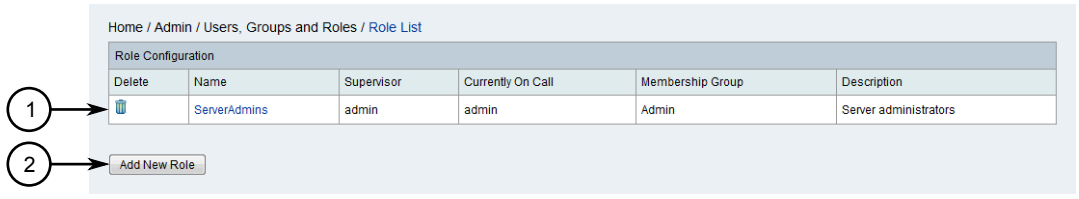


Figure 34: Role List Screen

1. Available Roles **2.** Add New Role Button

2. Click **Add New Role**. The **Edit Role** screen appears.

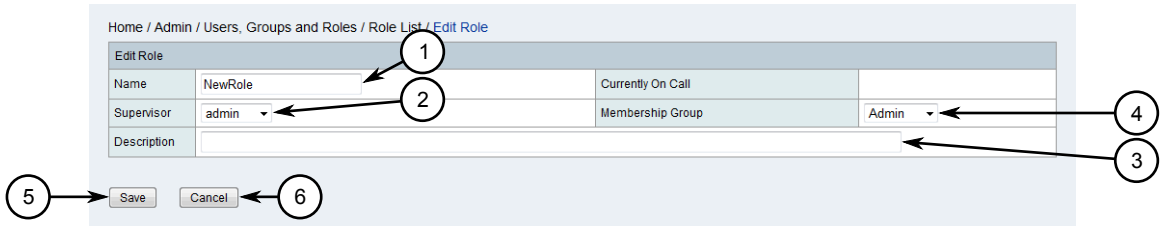


Figure 35: Edit Role Screen

1. Name Box **2.** Supervisor List **3.** Description Box **4.** Membership List **5.** Save Button **6.** Cancel Button

3. Configure the following parameters:

Parameter	Description
Name	The name of the role.
Supervisor	The user who oversees all users that share this role. For information about users, refer to Section 4.8.1, "Managing Users" .
Description	A description of the role.
Membership Group	The user group the role is part of. For more information about groups, refer to Section 4.8.2, "Managing User Groups" .

4. Click **Save**. The **View Role** screen appears.

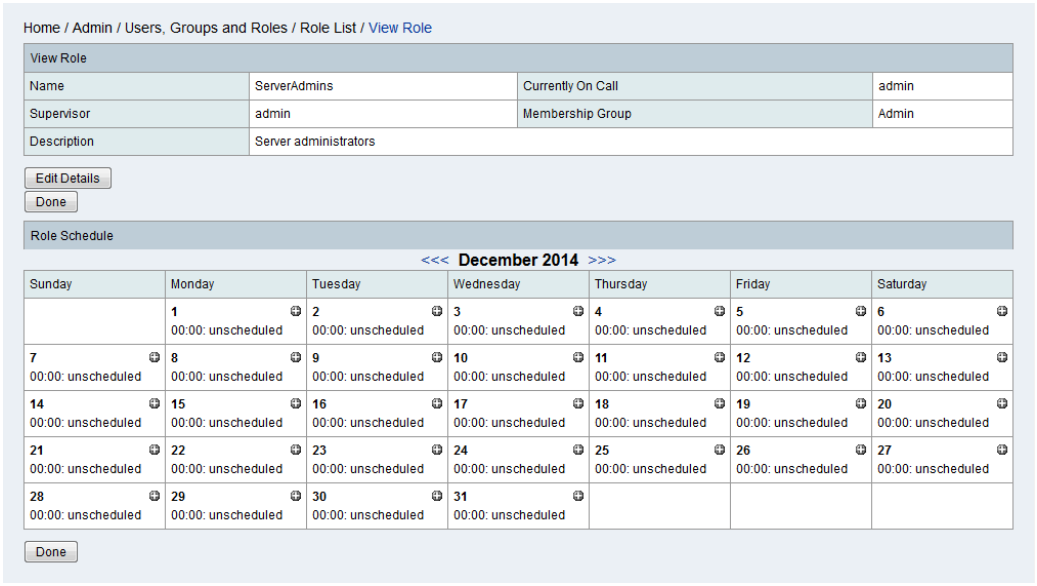


Figure 36: View Role Screen

5. [Optional] Configure the on-call calendar for the new role. For more information, refer to Section 4.8.3.3, "Configuring the On-Call Calendar" .
6. Click **Done**.

Section 4.8.3.2
Editing a User Role

To edit a user role, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Roles**. The **Role List** screen appears.

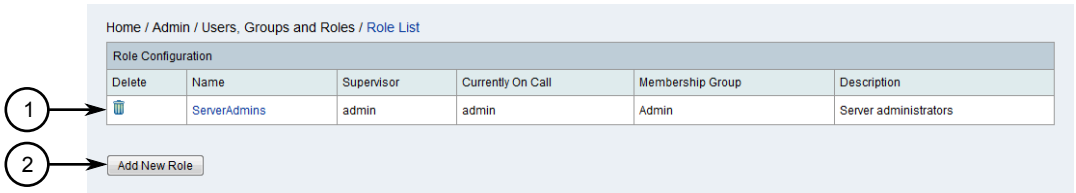


Figure 37: Role List Screen

1. Roles **2.** Add New Role Button

2. Click the name of the chosen role. The **View Role** screen appears.

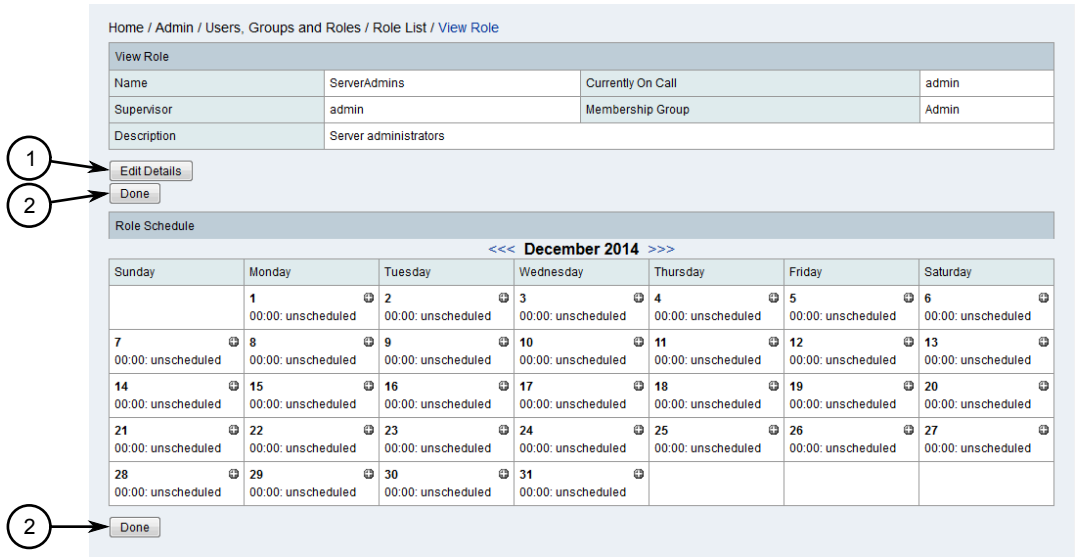


Figure 38: View Role Screen

1. Edit Details Button **2.** Done Button

3. Click **Edit Details**. The **Edit Role** screen appears.

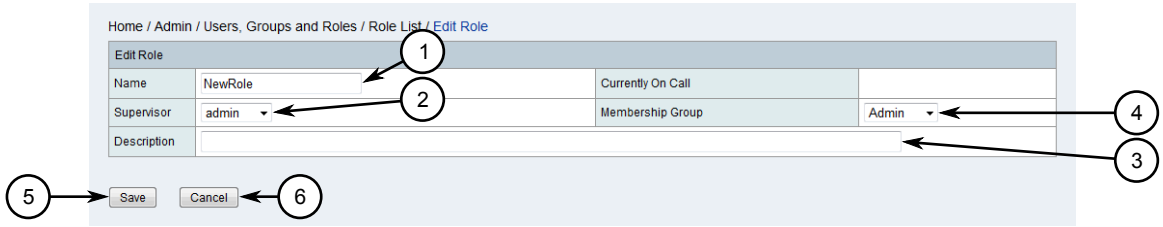


Figure 39: Edit Role Screen

1. Name Box **2.** Supervisor List **3.** Description Box **4.** Membership List **5.** Save Button **6.** Cancel Button

4. Configure the following parameters:

Parameter	Description
Name	The name of the role.
Supervisor	The user who oversees all users that share this role. For information about users, refer to Section 4.8.1, "Managing Users" .
Description	A description of the role.
Membership Group	The user group the role is part of. For more information about groups, refer to Section 4.8.2, "Managing User Groups" .

5. Click **Save**. The **View Role** screen appears. Refer to Figure 38 .

6. [Optional] Configure the on-call calendar for the role. For more information, refer to Section 4.8.3.3, "Configuring the On-Call Calendar" .
7. Click **Done**.

Section 4.8.3.3
Configuring the On-Call Calendar

An on-call calendar can be defined for each user role to control when notifications are sent to the associated users.

To configure the on-call calendar for a user role, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Roles**. The **Role List** screen appears.

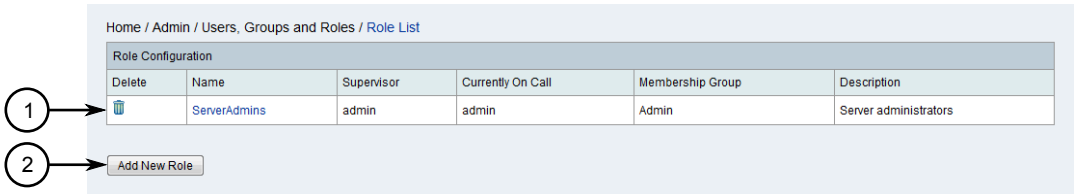


Figure 40: Role List Screen

1. Available Roles **2.** Add New Role Button

For information about adding user roles, refer to Section 4.8.3.1, "Adding a User Role" .

2. Select one of the available user roles. The **View Role** screen appears.

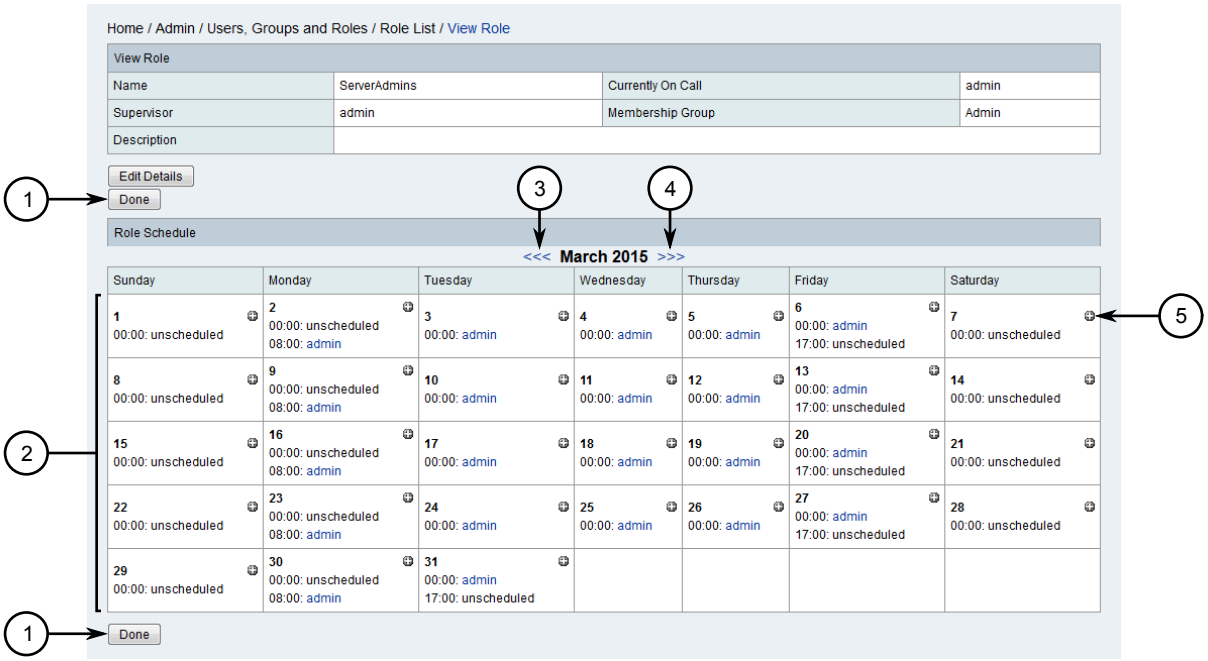


Figure 41: View Role Screen

1. Done Button **2.** Calendar **3.** Previous Month Link **4.** Next Month Link **5.** New Entry Icon

3. [Optional] Use the **<<<** and **>>>** links to change the month.
4. Either click an existing entry or click the **New Entry** icon for the first date in the on-call period. The **Edit Entry** screen appears.

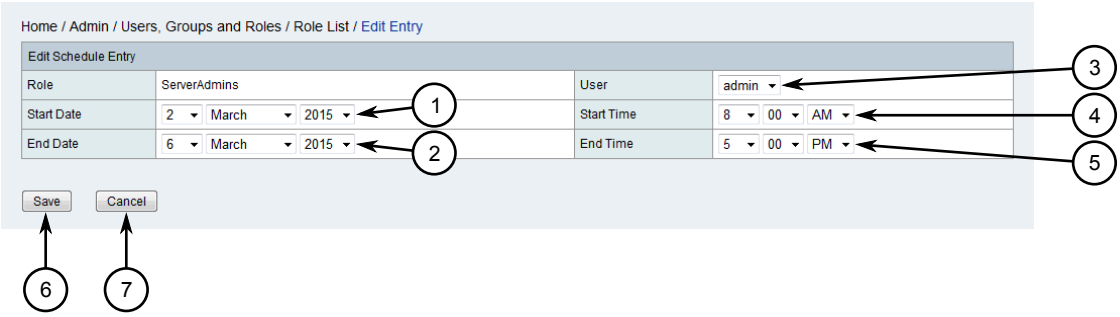


Figure 42: Edit Entry Screen

1. Start Date Boxes **2.** End Date Boxes **3.** User List **4.** Start Time Boxes **5.** End Time Boxes **6.** Save Button **7.** Cancel Button

5. Configure the following parameters as required:

Parameter	Description
Start Date	The first day in the on-call period.
End Date	The last day in the on-call period.

Parameter	Description
User	The affected user.
Start Time	The start time for each day in the on-call calendar.
End Time	The end time for each day in the on-call calendar.

6. Click **Save**.

Section 4.8.3.4
Deleting a User Role

To delete a user role, do the following:

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Roles**. The **Role List** screen appears.

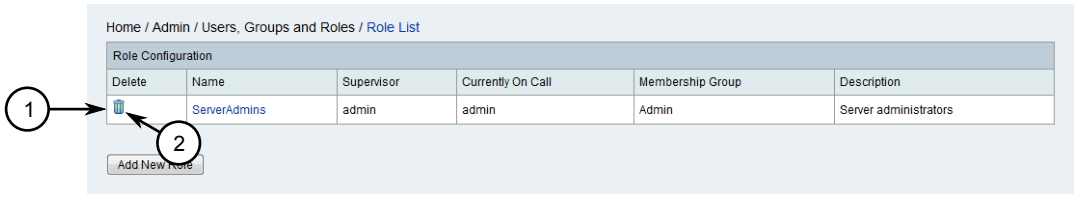


Figure 43: Role List Screen

1. Available Roles **2.** Delete Icon

2. Click the **Delete** icon next to the chosen user role. A confirmation dialog box appears.
3. Click **OK** to delete the user.

Section 4.8.4
Managing Duty Schedules

Duty schedules define when users are available to receive notifications from RUGGEDCOM NMS.

CONTENTS

Section 4.8.4.1
Adding/Deleting Duty Schedules for Users

To add/delete a duty schedule for a user, do the following:

Adding a Duty Schedule

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Users**. The **User List** screen appears.

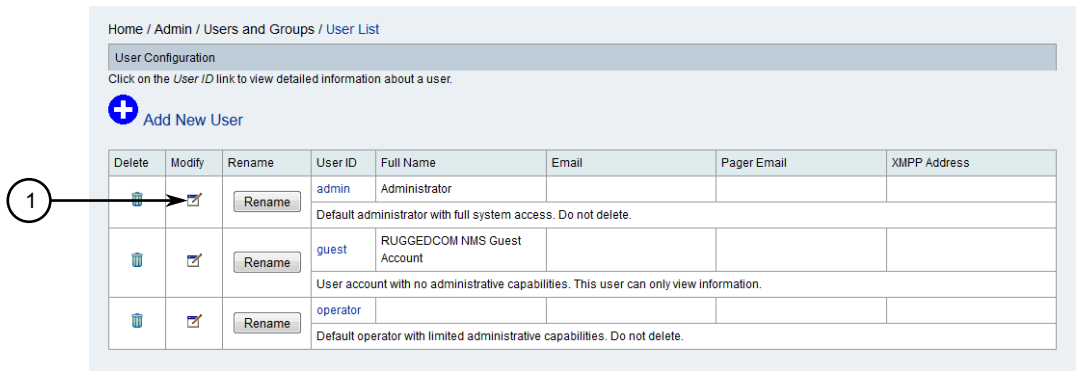


Figure 44: User List Screen

1. Users **2.** Modify Icon

2. Click the **Modify** icon next to the chosen user profile. The **Modify User** screen appears.

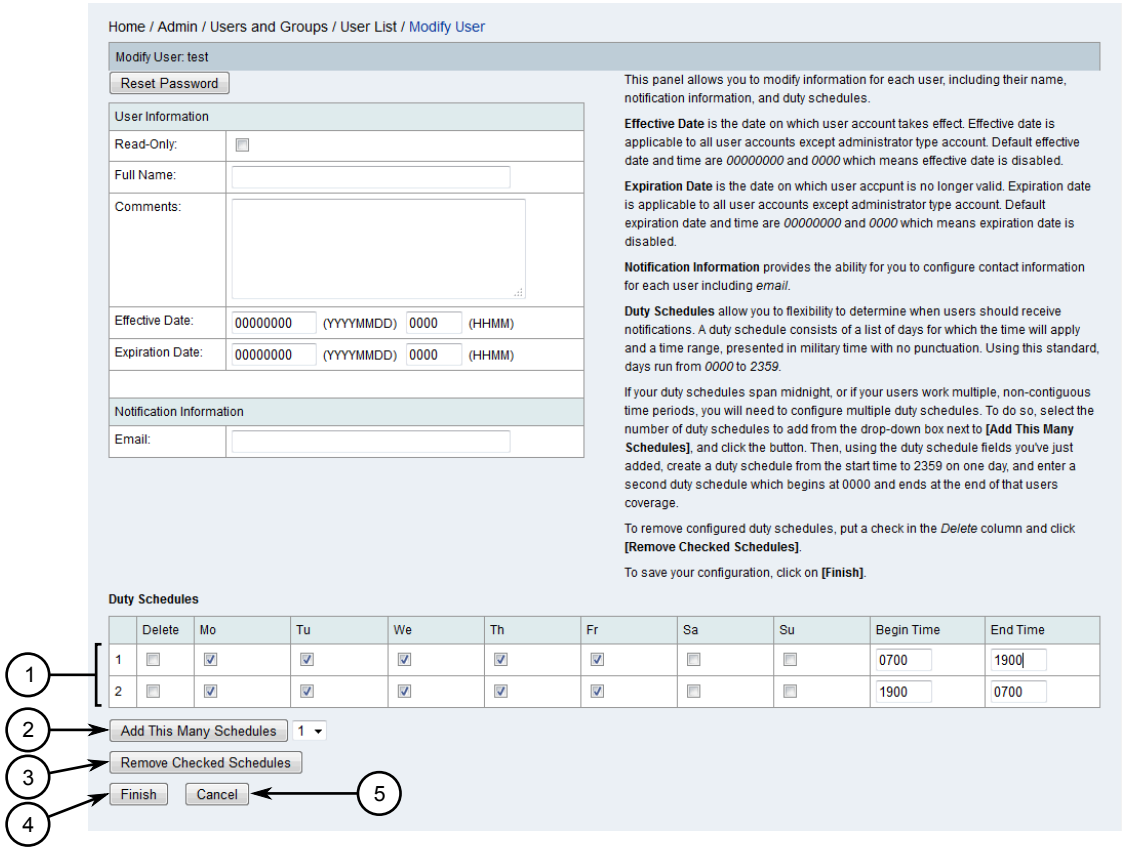


Figure 45: Modify User Screen

1. Duty Schedule **2.** Add This Many Schedules Button **3.** Remove Checked Schedules Button **4.** Finish Button **5.** Cancel Button

3. [Optional] If the user is available past midnight on any given day or only available at certain times during the day, add additional schedules by clicking **Add This Many Schedules**. Use the list next to the button to select more than one schedule.

> **NOTE**
> *Time is based on the 24-hour clock and punctuation is prohibited. Therefore, accepted values are within the range of 0000 and 2359.*

4. Select the days the user is available to receive notifications and define the time period for each under **Begin Time** and **End Time**. For example, if the user is available Monday to Friday, 8:00 AM to 5:00 PM, the begin and end times would be set to 0800 and 1700 respectively.

   If the user is not available at a certain time during the day on a particular day, add two schedules where only that day is selected and the define the begin and end times in each for the times when the user is available. For example, if the user is not available between 11:00 AM and 1:00 PM, set the begin and end time in the first schedule to 0800 and 1100. Then set the begin and end time for the same day in the other schedule to 1300 and 1700.

   Similarly, if a user is available past midnight on a given day, add two schedules where the end time for the first day is set to 2359 and the start time for the second day is 0000.

5. Click **Finish** to save the changes.

» Deleting a Duty Schedule

To remove a duty schedule, do the following:

1. Perform Step 1 to Step 2 in the previous procedure.
2. Select the check box under **Delete** next to the chosen duty schedule(s).
3. Click **Remove Checked Schedules**.
4. Click **Finish** to save the changes.

Section 4.8.4.2

Adding/Deleting Duty Schedules for a Group

To add/delete a duty schedule for a group, do the following:

» Adding a Duty Schedule

1. On the menu bar, click **Admin**, click **Configure Users, Groups and Roles** and then click **Configure Groups**. The **Group List** screen appears.

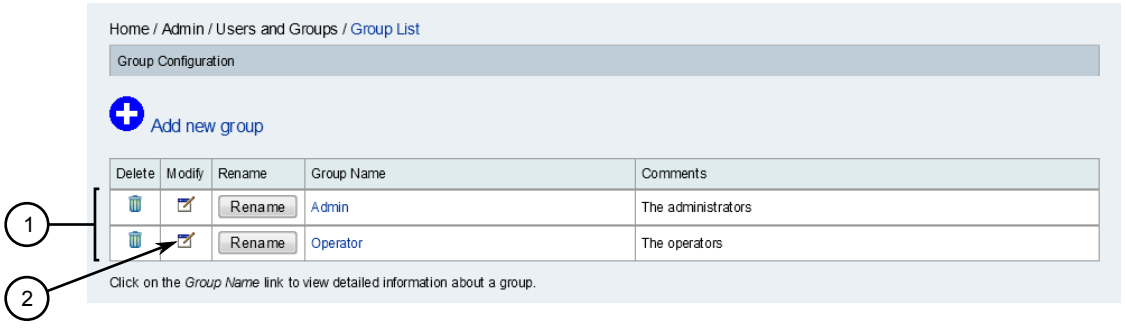


Figure 46: Group List Screen

1. Groups **2.** Modify Icon

2. Click the **Modify** icon next to the chosen group. The **Modify Group** screen appears.

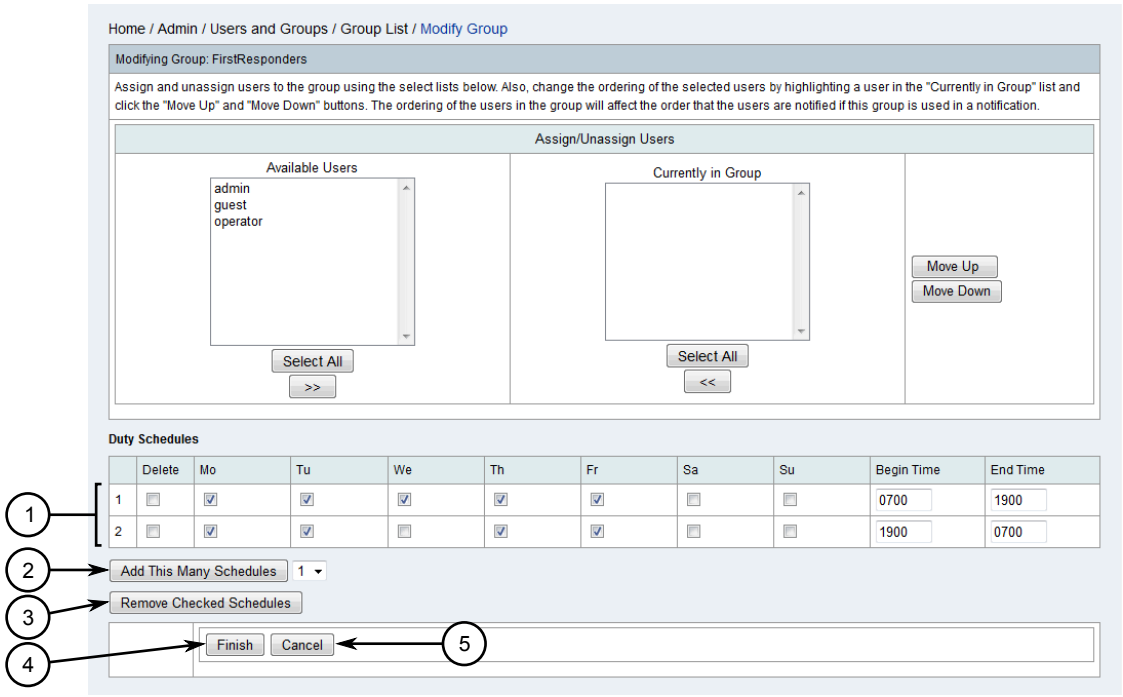


Figure 47: Modify Group Screen

1. Duty Schedule **2.** Add This Many Schedules Button **3.** Remove Checked Schedules Button **4.** Finish Button **5.** Cancel Button

3. [Optional] If the group is available past midnight on any given day or only available at certain times during the day, add additional schedules by clicking **Add This Many Schedules**. Use the list next to the button to select more than one schedule.

> **NOTE**
> *Time is based on the 24-hour clock and punctuation is prohibited. Therefore, accepted values are within the range of 0000 and 2359.*

4. Select the days the group is available to receive notifications and define the time period for each under **Begin Time** and **End Time**. For example, if the group is available Monday to Friday, 8:00 AM to 5:00 PM, the begin and end times would be set to 0800 and 1700 respectively.

   If the group is not available at a certain time during the day on a particular day, add two schedules where only that day is selected and the define the begin and end times in each for the times when the group is available. For example, if the group is not available between 11:00 AM and 1:00 PM, set the begin and end time in the first schedule to 0800 and 1100. Then set the begin and end time for the same day in the other schedule to 1300 and 1700.

   Similarly, if a group is available past midnight on a given day, add two schedules where the end time for the first day is set to 2359 and the start time for the second day is 0000.

5. Click **Finish** to save the changes.

» Deleting a Duty Schedule

To remove a duty schedule, do the following:

1. Perform Step 1 to Step 2 in the previous procedure.

2. Select the check box under **Delete** next to the chosen duty schedule(s).
3. Click **Remove Checked Schedules**.
4. Click **Finish** to save the changes.

Section 4.8.5
Managing User/Group Authentication

RUGGEDCOM NMS can be configured to authenticate users or groups using a remote LDAP (Lightweight Discovery Access Protocol) server.

CONTENTS

Section 4.8.5.1
Enabling/Disabling LDAP Authentication

To enable/disable LDAP authentication in RUGGEDCOM NMS do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and run the following script:

   `/root/ruggednms_scripts/config_ldap_login.sh`

   This script opens the following configuration file in gedit :

   `/usr/share/opennms/ruggednms/jetty-webapps/ruggednms/WEB-INF/applicationContext-spring-security.xml`
2. Remove (enable) or add (disable) the comment tags (<!-- and -->) around the elements between:

   ```
   <!-- ====================== LDAP AUTHENTICATION Part 1 of 2 ====================== -->
   ```

   And:

   ```
   <!--  End of the LDAP Setting Part 1 of 2 -->
   ```
3. Remove (enable) or add (disable) the comment tags (<!-- and -->) around the elements before:

   ```
   <beans:bean id="ldapTemplate" class="org.springframework.ldap.core.LdapTemplate">
   ```

   And after:

   ```
   <!/beans:bean>
   ```
4. Save and close the configuration file.
5. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .
6. If LDAP authentication has been enabled, configure authentication for all users. For more information, refer to Section 4.8.5.2, "Configuring LDAP Authentication" .

Section 4.8.5.2
Configuring LDAP Authentication

To configure LDAP authentication, do the following:

1. Make sure LDAP authentication is enabled. For more information, refer to Section 4.8.5.1, "Enabling/ Disabling LDAP Authentication" .
2. Open a terminal application on the RUGGEDCOM NMS server and run the following script:

   `/root/ruggednms_scripts/config_ldap_login.sh`

   This script opens the following configuration file in gedit :

   `/usr/share/opennms/ruggednms/jetty-webapps/ruggednms/WEB-INF/applicationContext-spring-security.xml`

   NOTE
   The default LDAP configuration file contains placeholders for required values supplied by the user. Each placeholder starts and ends with triple percentage symbols (e.g. %%%) and indicates what type of information is required.
3. Replace `%%%put LDAP server address here%%%` with the IP address of the LDAP server in the form of `ldap://{ip-address}:389`. For example:

   ```
   <beans:value>ldap://172.30.145.90:389</beans:value>
   ```
4. Replace `%%%Base BN HERE%%%` with the DNS name of your domain. For example, if the DNS name of your domain is *rnms.com*:

   ```
   <beans:property name="base" value="DC=rnms,DC=com"/>
   ```
5. Replace `%%%BIND USER HERE%%%` with the name of the principal account to use when binding the LDAP server. For example, if the account name is *ruggednms*:

   ```
   <beans:property name="defaultUser" value="ruggednms@rnms.com"/>
   ```
6. Replace `%%%BIND USER PASSWORD HERE%%%` with the LDAP password for the principal account.
7. Replace `%%%LOCATION OF USERS HERE%%%` with the distinguished name of the location where RUGGEDCOM NMS user records are stored on the LDAP server. For example:

   ```
   <beans:constructor-arg index="0" value="CN=Users"/>
   ```
8. Replace `%%%LOCATION OF YOUR GROUPS HERE%%%` with the distinguished name of the location where RUGGEDCOM NMS user group records are stored on the LDAP server. For example:

   ```
   <beans:constructor-arg value="CN=Users"/>
   ```
9. Make sure all RUGGEDCOM NMS users defined on the LDAP server are associated with one of the following groups in the LDAP server: rnms-user, rnms-operator or rnms-admin.
10. Save and close the configuration file.
11. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 4.9

Managing Thresholds

Thresholding is an important part of automating network management. It allows users to define triggers against data retrieved by the SNMP collector. When a performance metric exceeds the defined threshold, an event, notification or alarm is automatically generated.

For example, events, notifications and alarms can be generated:

- When the response time for a monitored device/service is too high
- When bandwidth utilization exceeds a certain amount
- When the number of CPE devices connected to a Base Station drop below a specified number

CONTENTS

Section 4.9.1

Enabling/Disabling Thresholds

To enable or disable thresholding in RUGGEDCOM NMS, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/collectd-configuration.xml`

2. Locate the *`thresholding-enabled`* parameter key.

```
<?xml version="1.0" encoding="UTF-8"?>
<collectd-configuration xmlns="http://xmlns.opennms.org/xsd/config/collectd" threads="20">
 <package name="RNMS1-collectd">
  <filter>IPADDR != '0.0.0.0'</filter>
  <include-range begin="1.1.1.1" end="254.254.254.254"/>
  <service name="SNMP" interval="300000" user-defined="false"
  status="on">
   <parameter key="collection" value="default"/>
   <parameter key="thresholding-enabled" value="true"/>
   <parameter key="retry" value="2"/>
   <parameter key="timeout" value="1000"/>
  </service>
 </package>
 <collector service="SNMP" classname="org.opennms.netmgt.collectd.SnmpCollector"/>
</collectd-configuration>
```

   If the parameter does not exist, add it.

3. Enable thresholding by setting the *`value`* attribute to `true`, or set the attribute to `false` to disable thresholding.

4. Save and close the file.
5. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 4.9.2
Viewing a List of Threshold Groups

To view a list of configured threshold groups, on the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

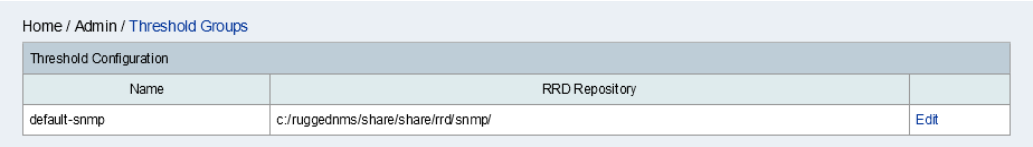


Figure 48: Threshold Groups Screen

The **Threshold Configuration** table lists the configured threshold groups.

Column	Description
Name	The name of the threshold group.
RRD Repository	The physical location of the group.

For information about editing a threshold group, refer to Section 4.9.4, "Viewing/Editing a Threshold Group" .

Section 4.9.3
Adding/Editing a Threshold

Basic thresholds are thresholds applied over a single metric or data source.

Expression-based thresholds are similar to basic thresholds, except they allow users to define mathematical expressions and multiple data sources.

The basic work flow for adding a threshold is as follows:

a. Determine if the target performance metric is being collected by RUGGEDCOM NMS.
b. Define the threshold type.
c. Set the expression (for expression-based thresholds only).
d. Define the expression or data source and type.
e. Define the threshold value that triggers a notification when exceeded.
f. Define the threshold value at which the threshold can be rearmed.
g. Define how many times in a row a threshold can be exceeded it is triggered.
h. Define Unique Event Identifiers (UEIs) for when the threshold is triggered or rearmed.
i. Define resource filters.
j. Define notifications to be sent when the threshold is triggered or rearmed.

To add or edit an existing basic or expression-based threshold, do the following:

1. Open a browser and log in to RUGGEDCOM NMS.
2. On the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

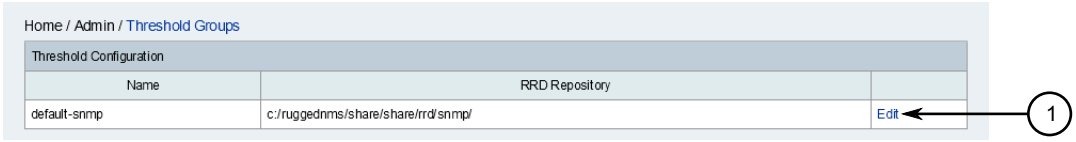


Figure 49: Threshold Groups Screen

1. Edit Hyperlink

3. Choose which group to view or modify and click the **Edit** hyperlink next to it. The **Edit Group** screen appears.

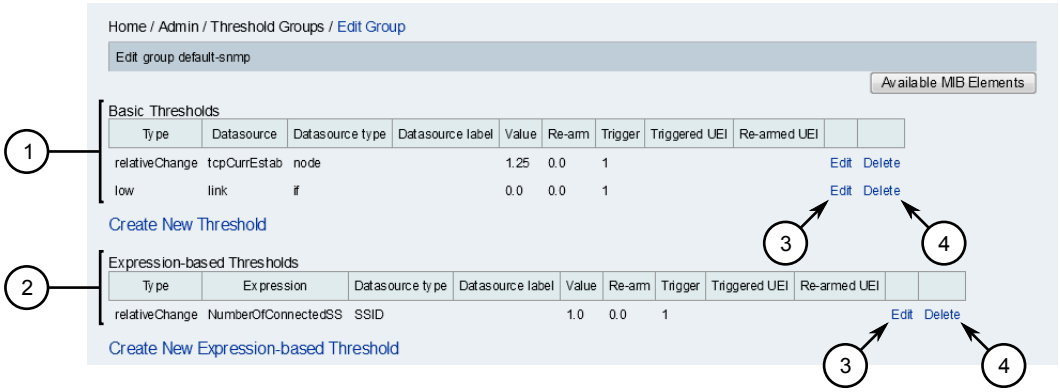


Figure 50: Edit Group Screen

1. Basic Thresholds **2.** Expression-Based Thresholds **3.** Edit Hyperlink **4.** Delete Hyperlink

4. Click **Create New Threshold** to add a basic threshold, click **Create New Expression Threshold** to add an expression-based threshold, or click **Edit** next to an existing threshold. The **Edit Threshold** screen appears.

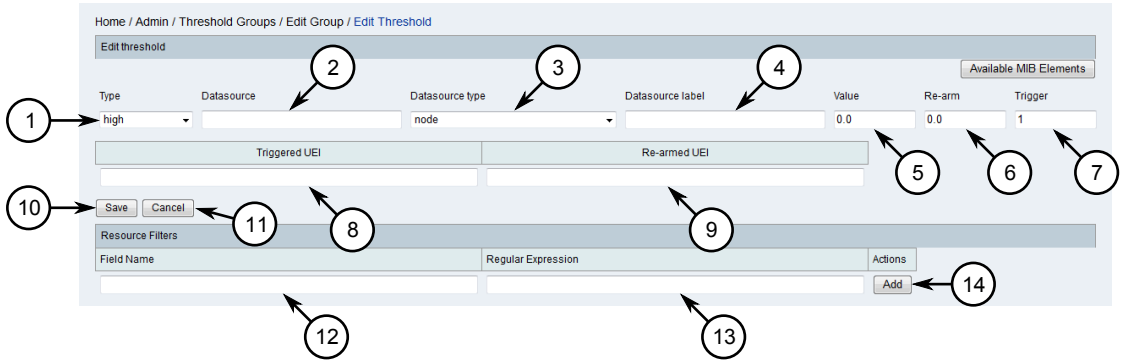


Figure 51: Edit Threshold Screen – Basic Threshold

1. Type List **2.** Datasource Box **3.** Datasource Type List **4.** Datasource Label Box **5.** Value Box **6.** Re-Arm Box **7.** Trigger Box **8.** Triggered UEI Box **9.** Re-Armed UEI Box **10.** Save Button **11.** Cancel Button **12.** Field Name Box **13.** Regular Expression Box **14.** Add Button

5. Configure the following parameters as required:

Parameter	Description
Type	**Synopsis:** { high, low, relativeChange } **Default:** high The threshold type. Options include: • `high` – Triggers when the value of the data source equals or exceeds the value of the threshold. The threshold is re-armed when the value equals or is less than the re-arm value. • `low` – Triggers when the value of the data source equals or is less than the value of the threshold. The threshold is re-armed when the value equals or exceeds the re-arm value. • `relativeChange` – Use to determine the relative difference between two samples. This type uses the *`Value`* parameter to determine in which direction the threshold is exceeded. For example, a value of 0.95 will trigger the threshold if the sample is at least 5% less than the previous sample. Alternatively, a value of 1.05 will trigger the threshold if the sample is at least 5% higher than the previous sample.
Expression	**For expression-based thresholds only.** A mathematical expression involving multiple data source names that will be evaluated and compare to the threshold values. For a list of available expressions based on data source and type, refer to Section 4.9.7, "Available Data Sources, Types and Expressions" .
Datasource	The name of the MIB element to monitor. For a list of available data sources, refer to Section 4.9.7, "Available Data Sources, Types and Expressions" .
Datasource Type	**Synopsis:** { node, if, coolingDeviceIndex, mplsL3VpnVrf, ciscoSlbInstance, cesServerFarmRserverEntry, rttMonCtrlAdminIndex, aixPhysicalVolume, umOrgIndex, CHAN, astChanType, powerUsageIndex, sinifCpuInstance, temperatureProbeIndex, cbgpPeerAddrFamilyPrefixEntry, applIndex, hpuxFSTable, ipuMGCPMsgStatsEntr, ciscoApCntIndex, aixPrintQueue, hrDeviceEntry, sinfNetInstance, netwareDisk, asAppIndex, aixVolumeGroup, msdpPeerEntry, ciscoEnvMonTemperatureStatusIndex,

Parameter	Description
	ciscoEnvMonVoltageStatusIndex, mtxrWlStatIndex, pipePosition, ainfCpuinstance, lgpEnvTemperatureIdDegF, drsChassisIndex, diskIOIndex, juniSystemTempIndex, ltmVSStatName, drsPSUIndex, ciscoMemoryPoolType, aixPagingSpace, ltmPoolStatName, vcPipePosition, mtxrWlRtabAddr, ainfLDskInstance, dskIndex, prtMarkerSuppliesIndex, naDfIndex, bgpPeerEntry, pgmonIndex, hrStorageIndex, f5ifName, SSID, lgpPwrMeasurementPtIndex, pethMainPseGroupIndex, rPDULoadStatusIndex, aixFilesystem, EqVol, ainfNetInstance, junSystemSlot, sinfLDskInstance } **Default:** node The data source type. For a list of data types available for each data source, refer to Section 4.9.7, "Available Data Sources, Types and Expressions" .
Datasource Label	The name of a data item, whose value will be used as a label when reporting the threshold.
Value	The threshold value that will trigger the threshold alarm if exceeded. • For high or low threshold types, the value must be higher or lower respectively to trigger the alarm. • For relativeChange threshold types, this is the relative change in percentage between two samples. A value of 1.5, for example, represents a 50% increase, whereas a value of 0.5 represents a 50% decrease. A value of 1.0 represents no increase or decrease.
Re-Arm	The value at which the threshold will be reset.
Trigger	The number of the times the threshold can be exceeded in a row before the threshold alarm is triggered. Not applicable to relativeChange threshold types.

6. Assign custom Unique Event Identifiers (UEIs) to the threshold by configuring the following parameters:

Parameter	Description
Triggered UEI	A custom Unique Event Identifier (UEI) to use when the threshold is triggered.
Rearmed UEI	A custom Unique Event Identifier (UEI) to use when the threshold is rearmed.

UEIs are linked to notifications that can be sent to other users when the threshold is triggered or rearmed.

A UEI can be any custom string that makes sense to the user. However, most UEIs are modeled after a Universal Resource Indicator (URI), such as uri:{company}.{domain}/{category}/{name}. For example, the following UEI might be used for a threshold that will trigger when disk usage is too high:

```
uri:siemens.com/threshold/disk/utilization/exceeded/
```

The rearmed UEI to go along with this example might be:

```
uri:siemens.com/threshold/disk/utilization/rearmed
```

7. [Optional] Configure one or more resource filters. For more information, refer to Section 4.9.6.2, "Adding/Editing a Resource Filter" .
8. Click **Save**. The **Edit Group** screen appears. Refer to Figure 50 .

   Note the UEI text under **Triggered UEI** and **Re-armed UEI** is hyperlinked.

9. Click the hyperlink under **Triggered UEI** to configure a notification associated with the threshold when it is triggered. For more information, refer to Step 9 in Section 5.2.4.7, "Adding/Editing a Notification".
10. Click the hyperlink under **Re-armed UEI** to configure a notification associated with the threshold when it is rearmed. For more information, refer to Step 9 in Section 5.2.4.7, "Adding/Editing a Notification".

Section 4.9.4
Viewing/Editing a Threshold Group

To view and/or edit a threshold group, do the following:

1. On the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

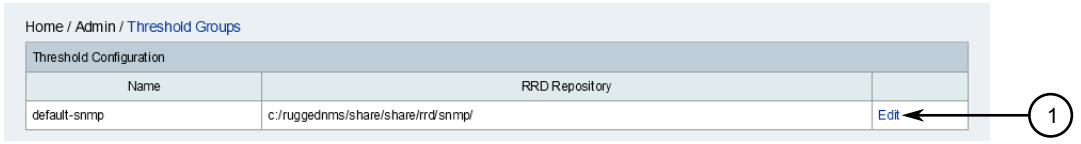


Figure 52: Threshold Groups Screen

1. Edit Hyperlink

2. Choose which group to view or modify and click **Edit**. The **Edit Group** screen appears.

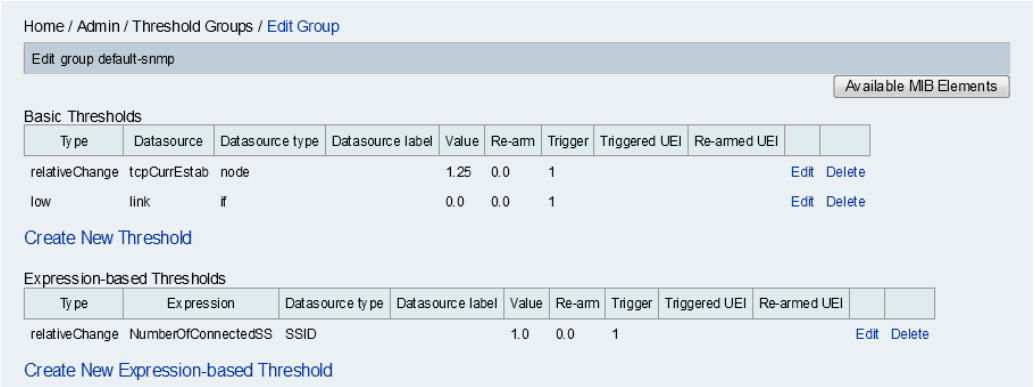


Figure 53: Edit Group Screen

Lists of basic and expression-based thresholds are displayed.

For information about how to add or edit existing thresholds, refer to Section 4.9.3, "Adding/Editing a Threshold".

For information about how to delete a threshold, refer to Section 4.9.5, "Deleting a Threshold".

Section 4.9.5
Deleting a Threshold

To delete either a basic or expression-based threshold, do the following:

1. On the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

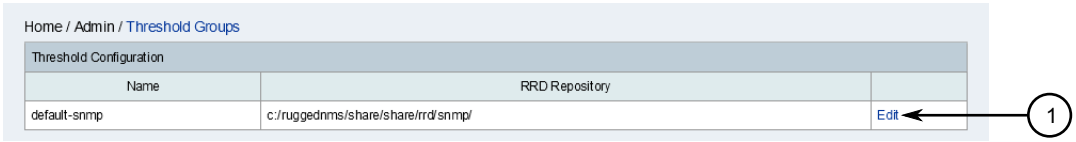


Figure 54: Threshold Groups Screen

1. Edit Hyperlink

2. Choose which group to view or modify and click **Edit**. The **Edit Group** screen appears.

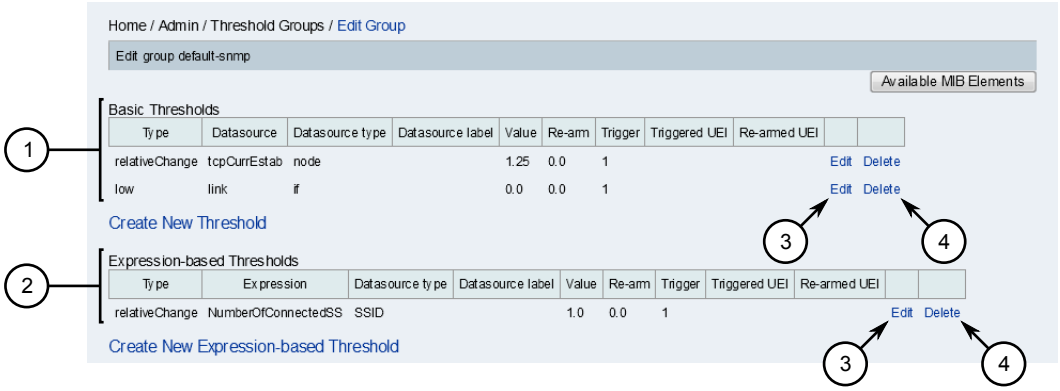


Figure 55: Edit Group Screen

1. Basic Thresholds **2.** Expression-Based Thresholds **3.** Edit Hyperlink **4.** Delete Hyperlink

3. Choose a threshold and click **Delete**. The threshold is removed.

Section 4.9.6

Managing Resource Filters

Resource filters associated with a threshold definition help select which resource should be considered when applying thresholds.

One or more resource filters can be applied to each threshold definition.

CONTENTS

- Section 4.9.6.3, "Deleting a Resource Filter"

Section 4.9.6.1
Sorting Resource Filters

Resource filters are applied in order. If the first filter does not result in a match, RUGGEDCOM NMS then tests the second filter and so on. If none of the filters result in a match, the threshold is not applied.

To sort resource filters, do the following:

1. On the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

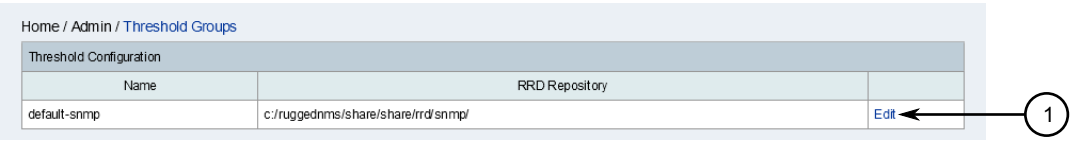


Figure 56: Threshold Groups Screen

1. Edit Hyperlink

2. Choose which group to view or modify and click the **Edit** hyperlink next to it. The **Edit Group** screen appears.

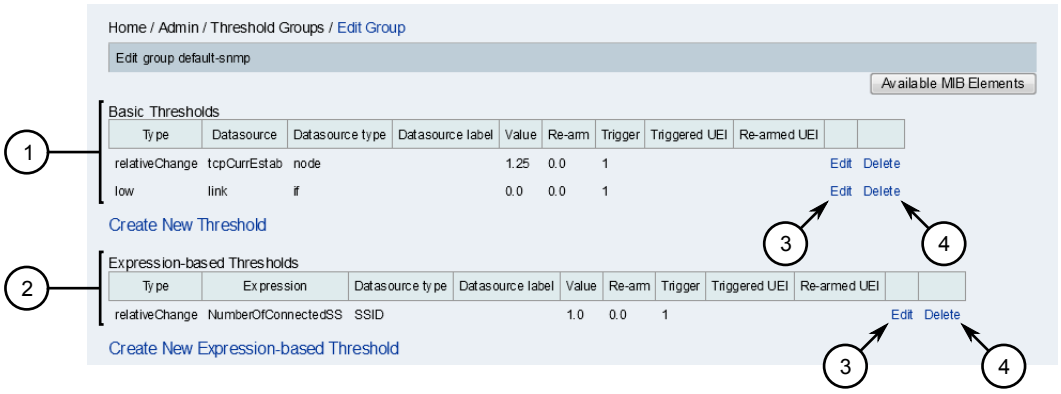


Figure 57: Edit Group Screen

1. Basic Thresholds **2.** Expression-Based Thresholds **3.** Edit Hyperlink **4.** Delete Hyperlink

3. Click **Edit** next to an existing threshold. The **Edit Threshold** screen appears.

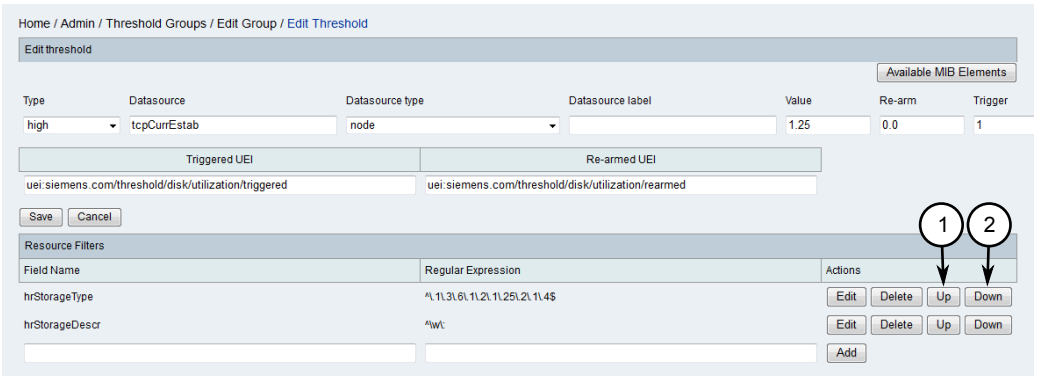


Figure 58: Edit Threshold Screen

1. Up Button **2.** Down Button

4. Make sure two or more resource filters are available. For information about adding resource filters, refer to Section 4.9.6.2, "Adding/Editing a Resource Filter" .
5. Under **Resource Filters**, click the **Up** or **Down** buttons next to the chosen resource filters.

Section 4.9.6.2

Adding/Editing a Resource Filter

To add or edit an existing resource filter, do the following:

1. On the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

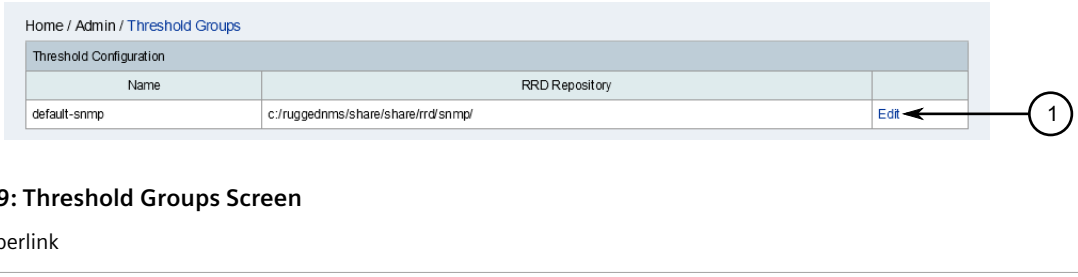


Figure 59: Threshold Groups Screen

1. Edit Hyperlink

2. Choose which group to view or modify and click the **Edit** hyperlink next to it. The **Edit Group** screen appears.

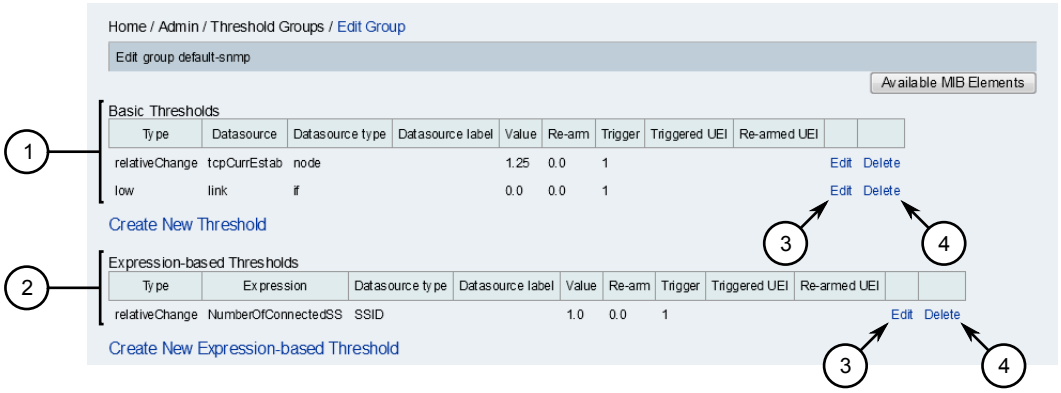


Figure 60: Edit Group Screen

1. Basic Thresholds **2.** Expression-Based Thresholds **3.** Edit Hyperlink **4.** Delete Hyperlink

3. Click **Edit** next to an existing threshold. The **Edit Threshold** screen appears.

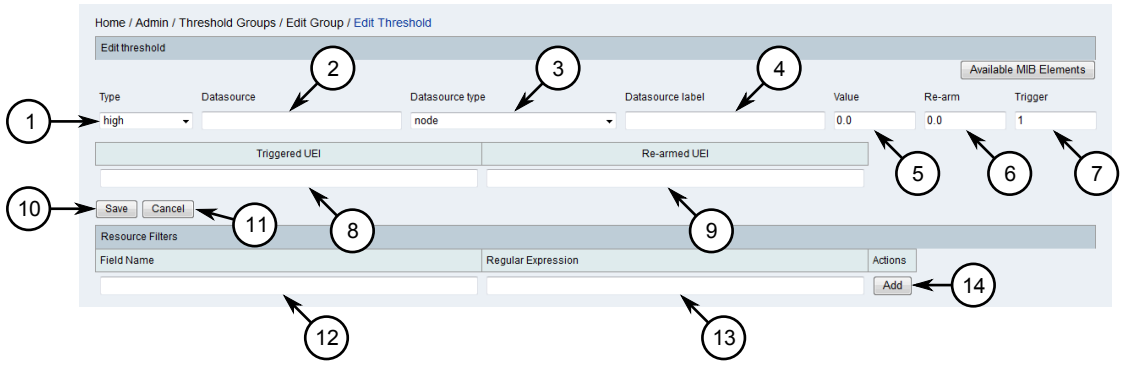


Figure 61: Edit Threshold Screen

1. Type List **2.** Datasource Box **3.** Datasource Type List **4.** Datasource Label Box **5.** Value Box **6.** Re-Arm Box **7.** Trigger Box **8.** Triggered UEI Box **9.** Re-Armed UEI Box **10.** Save Button **11.** Cancel Button **12.** Field Name Box **13.** Regular Expression Box **14.** Add Button

4. If editing an existing resource filter, click **Edit** next to the resource filter definition.
5. Configure the following parameters:

Parameter	Description
Field Name	The name of the resource to consider.
Regular Expression	The regular expression to apply against the resource. If there is a match and the event exceeds the defined threshold, the alarm is triggered.

6. Click **Add** or **Update**.

Section 4.9.6.3

Deleting a Resource Filter

To delete a resource filter, do the following:

1. On the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

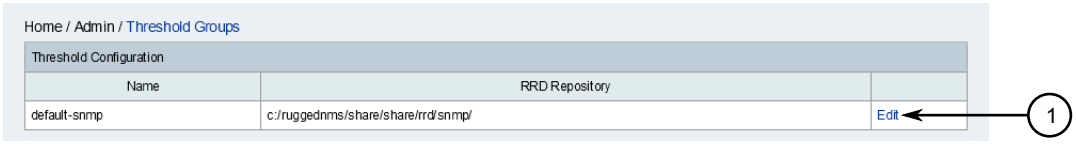


Figure 62: Threshold Groups Screen

1. Edit Hyperlink

2. Choose which group to view or modify and click the **Edit** hyperlink next to it. The **Edit Group** screen appears.

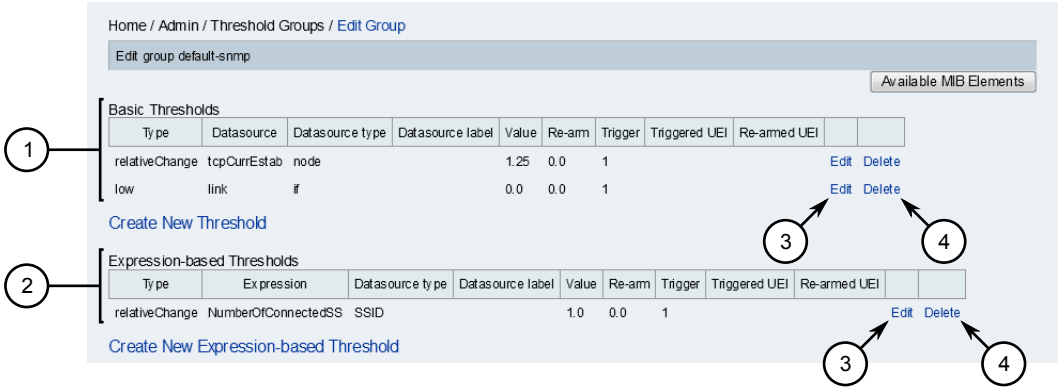


Figure 63: Edit Group Screen

1. Basic Thresholds **2.** Expression-Based Thresholds **3.** Edit Hyperlink **4.** Delete Hyperlink

3. Click **Edit** next to an existing threshold. The **Edit Threshold** screen appears.

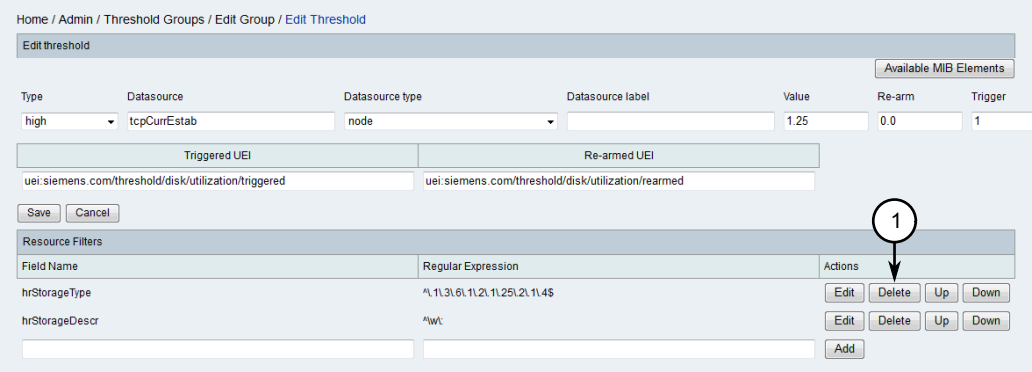


Figure 64: Edit Threshold Screen

1. Delete Button

4. Under **Resource Filters**, click the **Delete** button next to the chosen resource filter.

Section 4.9.7

Available Data Sources, Types and Expressions

The following data sources, types, and expressions, sorted by product relevance, may be used in creating thresholds.

NOTE

Additional SNMP MIBs can be imported into RUGGEDCOM NMS using the free mib2opennms tool. This tool extracts the trap definitions from the MIB and imports them into RUGGEDCOM NMS as events. For more information, refer to https://support.industry.siemens.com/cs/ww/en/view/109482189 .

Data Source	Data Source Type	Expression (MIB Object)	Product					
			ROS	ROX	ROX II	WIN BS	WIN CPE	Other
mib2-interfaces	if	ifDescr, ifSpeed, ifInOctets, ifInUcastpkts, ifInNUcastpkts, ifInDiscards, ifInErrors, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors	✓	✓	✓	✓	✓	✓
mib2-tcp	node	tcpActiveOpens, tcpPassiveOpens, tcpAttemptFails, tcpEstabResets, tcpCurrEstab, tcpInSegs, tcpOutSegs, tcpRetransSegs, tcpInErrors, tcpOutRsts	✓	✓	✓	✓	✓	✓
mib2-icmp	node	icmpInErrors, icmpInDestUnreachs, icmpInTimeExcds, icmpInSrcQuenchs, icmpInRedirects, icmpInEchos, icmpOutErrors, icmpOutDestUnreachs, icmpOutTimeExcds, icmpOutSrcQuenchs, icmpOutRedirects, icmpOutEchos, icmpOutEchoReps, icmpInMsgs,	✓	✓	✓	✓	✓	✓

Data Source	Data Source Type	Expression (MIB Object)	Product					
			ROS	ROX	ROX II	WIN BS	WIN CPE	Other
		icmpInParmProbs, icmpInEchoReps, icmpInTimestamps, icmpInTimestampReps, icmpInAddrMasks, icmpInAddrMaskReps, icmpOutMsgs, icmpOutParmProbs, icmpOutTimestamps, icmpOutTimestmpReps, icmpOutAddrMasks, icmpOutAddrMaskReps						
mib2-X-interfaces	if	ifName, ifHighSpeed, ifHCInOctets, ifHCOutOctets	×	✓	×	×	×	×
mib2-host-resources-storage	hrStorageIndex	hrStorageType, hrStorageDescr, hrStorageAllocUnits, hrStorageSize, hrStorageUsed	×	×	×	×	×	✓
mib2-host-resources-system	node	hrSystemUptime, hrSystemNumUsers, hrSystemProcesses	×	✓	×	×	×	×
mib2-host-resources-memory	node	hrMemorySize	×	✓	×	×	×	×
mib2-host-resources-processor	hrDeviceEntry	hrDeviceIndex, hrDeviceDescr, hrProcessorLoad	×	×	×	×	×	✓
mib2-coffee-rfc2325	node	coffeePotCapacity, coffeePotLevel, coffeePotTemp	×	×	×	×	×	✓
mib2-powerethernet	pethMainPseGroupIndex	pethMainPsePower, pethMainPseConsumptionPower	×	×	×	×	×	✓
mib2-ups-rfc1628	node	upsSecondsOnBattery, upsEstMinsRemain, upsEstChargeRemain, upsBatteryVoltage, upsBatteryCurrent, upsBatteryTemp, upsInputFrequency1, upsInputVoltage1, upsOutputSource, upsOutputFrequency, upsOutputVoltage1, upsOutputCurrent1, upsOutputPower1, upsOutputLoad1	×	×	×	×	×	✓
printer-usage	node	lifeCount, powerOnCount	×	×	×	×	×	✓
printer-mib-supplies	prtMarkerSuppliesIndex	prtMarkerSuppliesDescription, prtMSMaxCapacity, prtMSLevel	×	×	×	×	×	✓
ietf-bgp4-peer-stats	bgpPeerEntry	bgpPeerRemoteAddr, bgpPeerRemoteAs, bgpPeerInUpdates, bgpPeerOutUpdates	×	×	×	×	×	✓
ietf-ipmroute-scalars	node	ifMRouteEntryCount	×	×	×	×	×	✓
ietf-ipmroute-interfaces	if	ifInMcastOctets, ifOutMcastOctets	×	×	×	×	×	✓
ietf-msdp-scalars	if	igmpIfWrongVerQrys, igmpIfJoins, igmpIfGroups	×	×	×	×	×	✓

Data Source	Data Source Type	Expression (MIB Object)	Product					
			ROS	ROX	ROX II	WIN BS	WIN CPE	Other
ietf-igmp-interfaces	node	msdpSACacheEntries	×	×	×	×	×	✓
ietf-msdp-peers	msdpPeerEntry	msdpPeerRemoteAddr, msdpPeerRPFFailures, msdpPeerInSAs, msdpPeerOutSAs, msdpPeerInSAReqs, msdpPeerOutSAReqs, msdpPeerInSARsps, msdpPeerOutSARsps, msdpPeerInCtrlMsgs, msdpPeerOutCtrlMsgs, msdpPeerInDataPkts, msdpPeerOutDataPkts, msdpPeerEstabTrans, msdpPeerLocalAddr, msdpPeerRemotePort, msdpPeerLocalPort, msdpPeerConnAttmpts, msdpPeerInNotifs, msdpPeerOutNotifs	×	×	×	×	×	✓
ietf-mpls-l3vpn-scalars	node	mL3VConfiguredVrfs, mL3VActiveVrfs, mL3VConnectedIfs	×	×	×	×	×	✓
ietf-mpls-l3vpn-vrfs	mplsL3VpnVrf	mL3VVrfName, mL3VVrfDescr, mL3VVrfActiveIfs, mL3VVrfAssocIfs, mL3VVrfPerfRtsAdded, mL3VVrfPerfRtsDeled, mL3VVrfPerfCurRts, mL3VVrfPerfRtsDrpd	×	×	×	×	×	✓
rcom-ros-dev	node	RosCpuUsagePercent, RosAvailableRam, RosTemperature, RosTotalRam	✓	×	×	×	×	×
mib2-ip	node	ipInReceives, ipInHdrErrors, ipInAddrErrors, ipForwDatagrams, ipInUnknownProtos, ipInDiscards, ipInDelivers, ipOutRequests, ipOutDiscards, ipOutNoRoutes, ipReasmTimeout, ipReasmReqds, ipReasmOKs, ipReasmFails, ipFragOKs, ipFragFails, ipFragCreates	✓	✓	×	×	×	×
net-snmp-disk	dskIndex	ns-dskPath, ns-dskTotal, ns-dskAvail, ns-dskUsed, ns-dskPercent	×	✓	×	×	×	×
ucd-loadavg	node	loadavg1, loadavg5, loadavg15	×	✓	×	×	×	×
ucd-memory	node	memTotalSwap, memAvailSwap, memTotalReal, memAvailReal, memTotalFree, memShared, memBuffer, memCached, memSwapError	×	✓	×	×	×	×
ucd-sysstat	node	SwapIn, SwapOut, SysInterrupts, SysContext, CpuRawUser, CpuRawNice, CpuRawSystem, CpuRawIdle, CpuRawWait, CpuRawKernel, CpuRawInterrupt, IORawSent, IORawReceived	×	✓	×	×	×	×

Data Source	Data Source Type	Expression (MIB Object)	Product					
			ROS	ROX	ROX II	WIN BS	WIN CPE	Other
openmanage-coolingdevices	coolingDeviceIndex	coolingDevReading, coolingDeviceLocationName, coolDevLowCritThres	×	✓	×	×	×	×
openmanage-powerusage	powerUsageIndex	powerUsageEntityName, powerUsageWattage, powerUsagePeakWatts	×	✓	×	×	×	×
openmanage-temperatureprobe	temperatureProbeIndex	tempProbeReading, temperatureProbeLocationName, tempProbeUpCrit, tempProbeUpNonCrit, tempProbeLowNonCrit, tempProbeLowCrit	×	✓	×	×	×	×
PRP-HSR-MIB	lreInterfaceStatsIndex	lreInterfaceStatsIndex, lreCntTxA, lreCntTxB, lreCntTxC, lreCntErrWrongLanA, lreCntErrWrongLanB, lreCntErrWrongLanC, lreCntRxA, lreCntRxB, lreCntRxC, lreCntErrorsA, lreCntErrorsB, lreCntErrorsC, lreCntNodes, lreCntProxyNodes, lreCntUniqueA, lreCntUniqueB, lreCntUniqueC, lreCntDuplicateA, lreCntDuplicateB, lreCntDuplicateC, lreCntMultiA, lreCntMultiB, lreCntMultiC, lreCntOwnRxA, lreCntOwnRxB	✓	×	×	×	×	×
rcom-rmax-dev	node	TotDLDroppedPac, TotULDroppedPac, TotalDLPackets, TotalULPackets, TotalULBytes, TotalDLBytes, TotalULCRCFailures, TotalULCRCOK, ULPER, ULBER, ULRate, DLRate, NumberOFConnectedSS, RfTxPower, RfTemp, BSTemperature	×	×	×	✓	×	×
rcom-rmax-filler1	node	filler1, filler2, filler3, filler4	×	×	×	✓	×	×
rcom-rmax-cpe-stats1	SSID	SSID, SSidStr, Link, LinkTime, DlRSSIMin, DlRSSIMax, DlRSSIAvg	×	×	×	✓	×	×
rcom-rmax-cpe-stats2	SSID	SSID, DlCINRMin, DlCINRMax, DlCINRAvg	×	×	×	✓	×	×
rcom-rmax-cpe-stats3	SSID	UlCINRMin, UlCINRMax, UlCINRAvg	×	×	×	✓	×	×
rcom-rmax-cpe-stats4	SSID	DlTotBytes, DlTotPackets, DlTotDropPac, DlTotRateMax, DlTotRateAvg, DlUcastBytes, DlUcastPackets, DlUcastDropPac, DlUcastRateMax, DlUcastRateAvg, UlTotalBytes, UlTotalPac, UlTotDropPac, UlTotRateMax, UlTotRateAvg	×	×	×	✓	×	×

To access this list within RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin** and then click **Manage Thresholds**. The **Threshold Groups** screen appears.

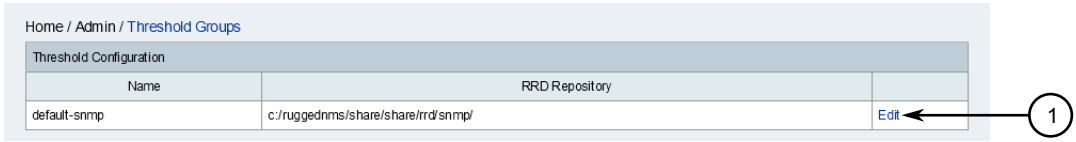


Figure 65: Threshold Groups Screen

1. Edit Hyperlink

2. Choose which group to modify and click the **Edit** hyperlink next to it. The **Edit Group** screen appears.

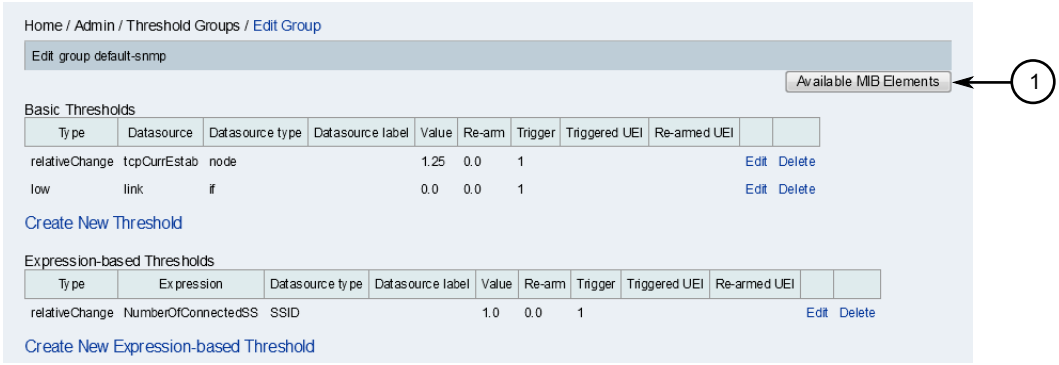


Figure 66: Edit Group Screen

1. Available MIB Elements Button

3. Click **Available MIB Elements**. A new window opens listing the available MIB elements.

Section 4.10

Managing Data Encryption

Information related to SNMP configuration data, and information used by RUGGEDCOM NMS to access devices can be protected by encryption. When encryption is enabled, users are required when launching RUGGEDCOM NMS to enter a specific passphrase, unless the passphrase is stored locally.

CONTENTS

- Section 4.10.4, "Resetting the Encryption Passphrase"

Section 4.10.1
Enabling Data Encryption

To enable data encryption, do the following:

1. On the menu bar, click **Admin**, click **Encryption Passphrase Management**, and then click **Enable Encryption**. The **Enable Encryption** screen appears.

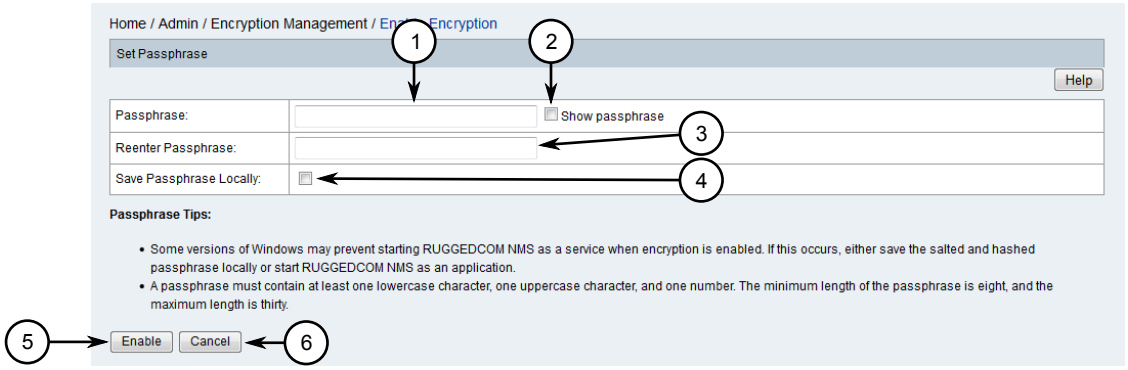


Figure 67: Enable Encryption Screen

1. Passphrase Box **2.** Show Passphrase Check Box **3.** Reenter Passphrase Box **4.** Save Passphrase Locally Check Box **5.** Enable Button **6.** Cancel Button

2. [Optional] Click **Show Passphrase** to display the passphrase on screen in plain text.

IMPORTANT!
The passphrase must meet the following requirements:

- *Length must be between 8 and 30 characters*
- *Must contain at least one lowercase character*
- *Must contain at least one uppercase character*
- *Must contain at least one number*

3. Under **Passphrase**, type a passphrase.
4. Under **Reenter Passphrase**, type the passphrase again.
5. Click **Save Passphrase Locally**. When enabled (checked), the passphrase is stored locally to prevent RUGGEDCOM NMS from requesting the passphrase during launch. For more information, refer to Section 3.2, "Launching RUGGEDCOM NMS " .
6. Click **Enable**. A confirmation dialog box appears.
7. Click **OK** to enable encryption.

Section 4.10.2
Disabling Data Encryption

To disable data encryption, do the following:

1. On the menu bar, click **Admin**, click **Encryption Passphrase Management**, and then click **Disable Encryption**. The **Disable Encryption** screen appears.

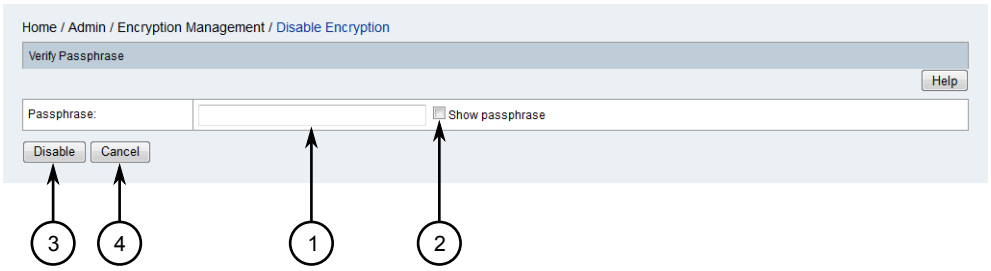


Figure 68: Disable Encryption Screen

1. Passphrase Box **2.** Show Passphrase Check Box **3.** Disable Button **4.** Cancel Button

2. Under **Passphrase**, type the passphrase. If required, click **Show passphrase** to display the passphrase in plain text.
3. Click **Disable**.

Section 4.10.3
Changing the Encryption Passphrase

To change the encryption passphrase, do the following:

1. On the menu bar, click **Admin**, click **Encryption Passphrase Management**, and then click **Change Passphrase**. The **Change Passphrase** screen appears.

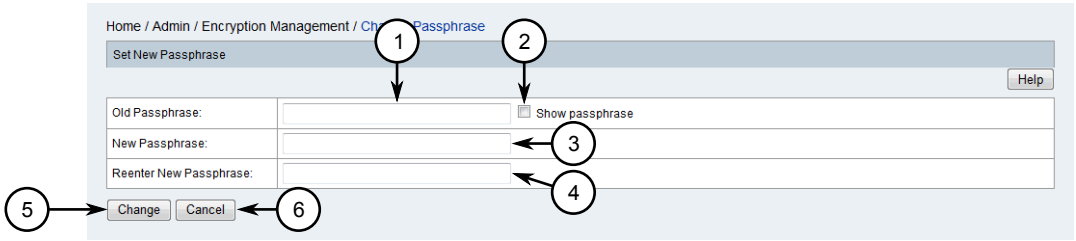


Figure 69: Change Passphrase Screen

1. Old Passphrase Box **2.** Show Passphrase Check Box **3.** New Passphrase Box **4.** Reenter Passphrase Box **5.** Change Button **6.** Cancel Button

2. [Optional] Click **Show Passphrase** to display the passphrase on screen in plain text.
3. Under **Old Passphrase**, type the current passphrase.
4. Under **New Passphrase**, type the new passphrase.

5. Under **Reenter Passphrase**, type the new passphrase again.
6. Click **Change**.

Section 4.10.4
Resetting the Encryption Passphrase

If the encryption passphrase is lost and was not saved locally when encryption was enabled, access to SNMP and device access configuration is blocked, and RUGGEDCOM NMS will be unable to start.

To reset the encryption passphrase, do the following:

CAUTION!
Configuration hazard – risk of data loss. Resetting the encryption passphrase erases all device access passwords and SNMP configuration settings. Device access and SNMP configuration settings will be set back to their default settings.

1. Open a terminal application on the RUGGEDCOM NMS server and run the following script:

   `/root/ruggednms_scripts/start_ruggednms.sh`

   The **Configuration File Encryption** dialog box appears.

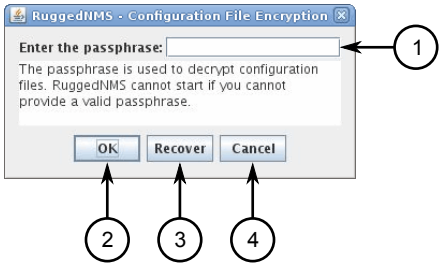


Figure 70: Configuration File Encryption Dialog Box

1. Enter the Passphrase Box **2.** OK Button **3.** Recover Button **4.** Cancel Button

2. Click **Recover**. A confirmation message appears.
3. Click **Yes**. A confirmation message outline the associated risks appears.
4. Click **Accept**. The RUGGEDCOM NMS service starts.
5. Log in to RUGGEDCOM NMS. For more information, refer to Section 3.5, “Logging In/Out” .

Section 4.11
Managing Surveillance Categories

Surveillance categories group devices into logical groups, the information for which can be reviewed and analyzed from the main dashboard.

By default, RUGGEDCOM NMS begins with six suggested categories.

- The *Production*, *Testing* and *Development* categories are intended to group devices based on their current status. The *Production* category would consist of devices deployed in the running infrastructure, while the *Testing* and *Development* categories would consist of devices undergoing evaluation or commissioning.
- The *Routers*, *Servers* and *Switches* categories are intended to group devices by type.

The exact use of these categories can be determined by the user. New categories can also be added as needed.

Surveillance categories can contain multiple members, and a device can be a member of multiple surveillance categories.

CONTENTS

Section 4.11.1

Adding a Surveillance Category

To add a new surveillance category, do the following:

1. On the menu bar, click **Admin**, and then click **Manage Surveillance Categories**. The **Categories** screen appears.

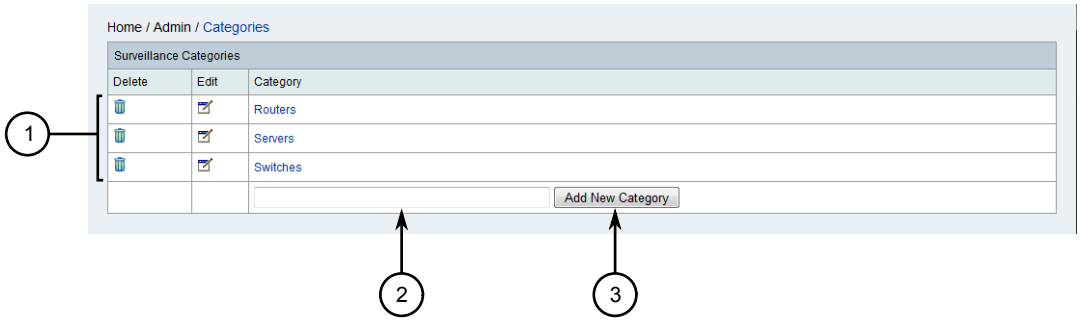


Figure 71: Categories Screen

1. Surveillance Categories **2.** Name Box **3.** Add New Category Button

2. Type the name of the new surveillance category in the **Name** box and then click **Add New Category**. The new category is added.
3. Add one or more nodes to the category. For more information, refer to Section 4.11.3, "Adding/Removing Nodes from Surveillance Categories" .
4. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/surveillance-views.xml`
5. Add a new `<column-def>` or `<row-def>` element as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<surveillance-view-configuration xmlns:this="http://www.opennms.org/xsd/config/surveillance-views"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.opennms.org/
```

```
xsd/config/surveillance-views http://www.opennms.org/xsd/config/surveillance-views.xsd" default-
view="default" >
   <!-- default view here -->
    <view name="default" refresh-seconds="300" >
      <rows>
        <row-def label="Routers" >
          <category name="Routers"/>
        </row-def>
        <row-def label="Switches" >
          <category name="Switches" />
        </row-def>
        <row-def label="Servers" >
          <category name="Servers" />
        </row-def>
        <row-def label="{label}" >
          <category name="{name}" />
        </row-def>
      </rows>
      <columns>
        <column-def label="PROD" >
          <category name="Production" />
        </column-def>
        <column-def label="TEST" >
          <category name="Test" />
        </column-def>
        <column-def label="DEV" >
          <category name="Development" />
        </column-def>
        <column-def label="{label}" >
          <category name="{name}" />
        </column-def>
      </columns>
    </view>
  </views>
</surveillance-view-configuration>
```

Where:

- `{label}` is the name of the surveillance category as it appears in the Surveillance View table on the Dashboard.
- `{name}` is the name of the surveillance category.

6. Save and close the file.

Section 4.11.2

Deleting a Surveillance Category

To delete a surveillance category, do the following:

1. On the menu bar, click **Admin**, and then click **Manage Surveillance Categories**. The **Categories** screen appears.

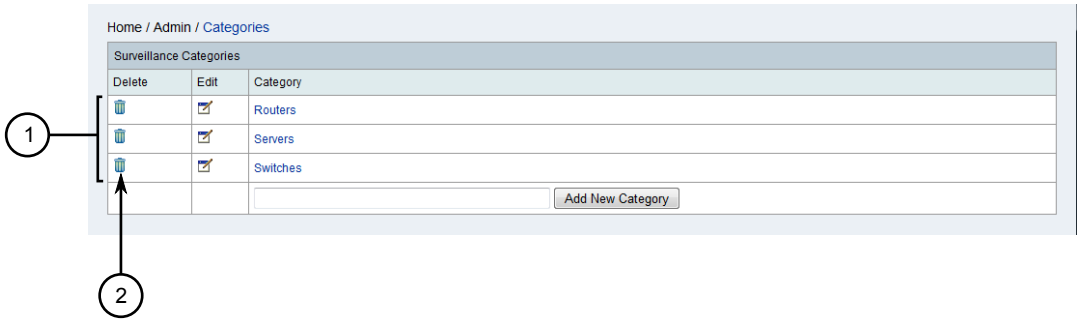


Figure 72: Categories Screen

1. Surveillance Categories **2.** Delete Icon

2. Click the **Delete** icon for the chosen surveillance category. The category is removed from the list, but it still appears in the Surveillance View table on the Dashboard.
3. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/surveillance-view.xml`
4. Remove the `<column-def>` or `<row-def>` elements for the surveillance category:

```
<?xml version="1.0" encoding="UTF-8"?>
<surveillance-view-configuration xmlns:this="http://www.opennms.org/xsd/config/surveillance-views"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.opennms.org/
xsd/config/surveillance-views http://www.opennms.org/xsd/config/surveillance-views.xsd" default-
view="default" >
   <!-- default view here -->
    <view name="default" refresh-seconds="300" >
      <rows>
        <row-def label="Routers" >
          <category name="Routers"/>
        </row-def>
        <row-def label="Switches" >
          <category name="Switches" />
        </row-def>
        <row-def label="Servers" >
          <category name="Servers" />
        </row-def>
        <row-def label="{label}" >
          <category name="{name}" />
        </row-def>
      </rows>
      <columns>
        <column-def label="PROD" >
          <category name="Production" />
        </column-def>
        <column-def label="TEST" >
          <category name="Test" />
        </column-def>
        <column-def label="DEV" >
          <category name="Development" />
        </column-def>
        <column-def label="{label}" >
          <category name="{name}" />
        </column-def>
      </columns>
    </view>
  </views>
```

```
</surveillance-view-configuration>
```

Where:

- `{label}` is the name of the surveillance category as it appears in the Surveillance View table on the Dashboard.
- `{name}` is the name of the surveillance category.

5. Save and close the file.

Section 4.11.3

Adding/Removing Nodes from Surveillance Categories

To add or remove a node form a surveillance category, do the following:

IMPORTANT!
*A node must be added to a **row** type surveillance category and its associated **column** type surveillance category to appear on the Surveillance View table on the Dashboard.*

1. On the menu bar, click **Admin**, and then click **Manage Surveillance Categories**. The **Categories** screen appears.

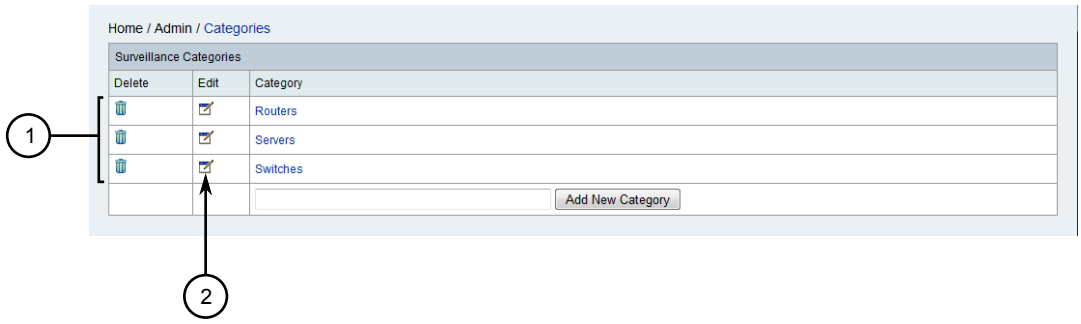


Figure 73: Categories Screen

1. Surveillance Categories **2.** Edit Icon

2. Click the **Edit** icon for the chosen category. The **Show** screen appears.

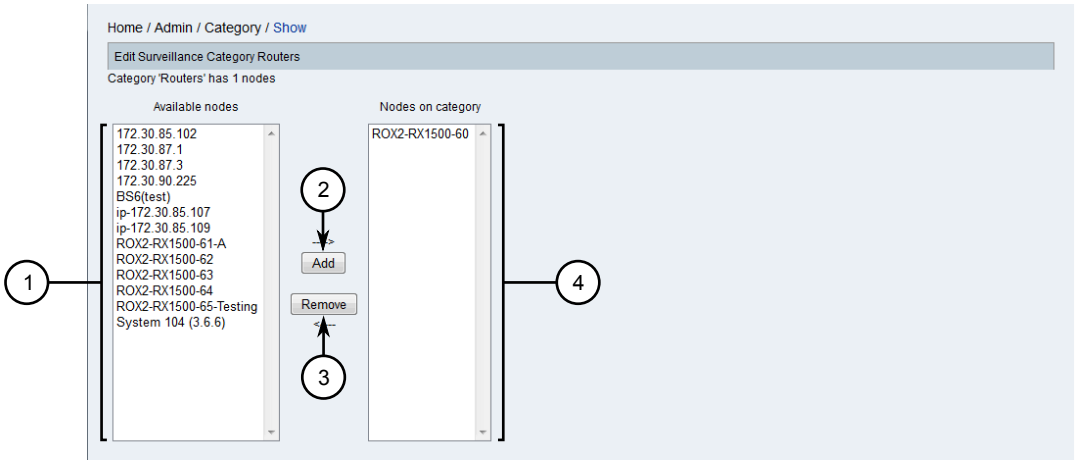


Figure 74: Show Screen

1. Available Nodes List **2.** Add Button **3.** Remove Button **4.** Nodes on Category List

NOTE

*To select consecutive interfaces, click the first interface, then hold **Shift** and click the last interface. To select specific interfaces, click the first interface, and then hold **Ctrl** and select other interfaces from the list.*

3. Select an interface from either the **Available Nodes** or **Nodes on Category** lists, and then click either the **Add** or **Remove** button. **Add** adds selected interfaces to the **Nodes on Category** list, while **Remove** moves interfaces back to the **Available Nodes** list.

5 Monitoring Devices

This chapter describes how to monitor devices managed by RUGGEDCOM NMS.

CONTENTS

Section 5.1

Monitoring Device Availability

The **Home** screen in the RUGGEDCOM NMS Web user interface details the overall availability of all managed devices over the last 24 hours. It also counts the number of outages over the same period.

To view the availability of the network over the last 24 hours, either start a new Web session or click the Siemens logo. The **Home** screen appears.

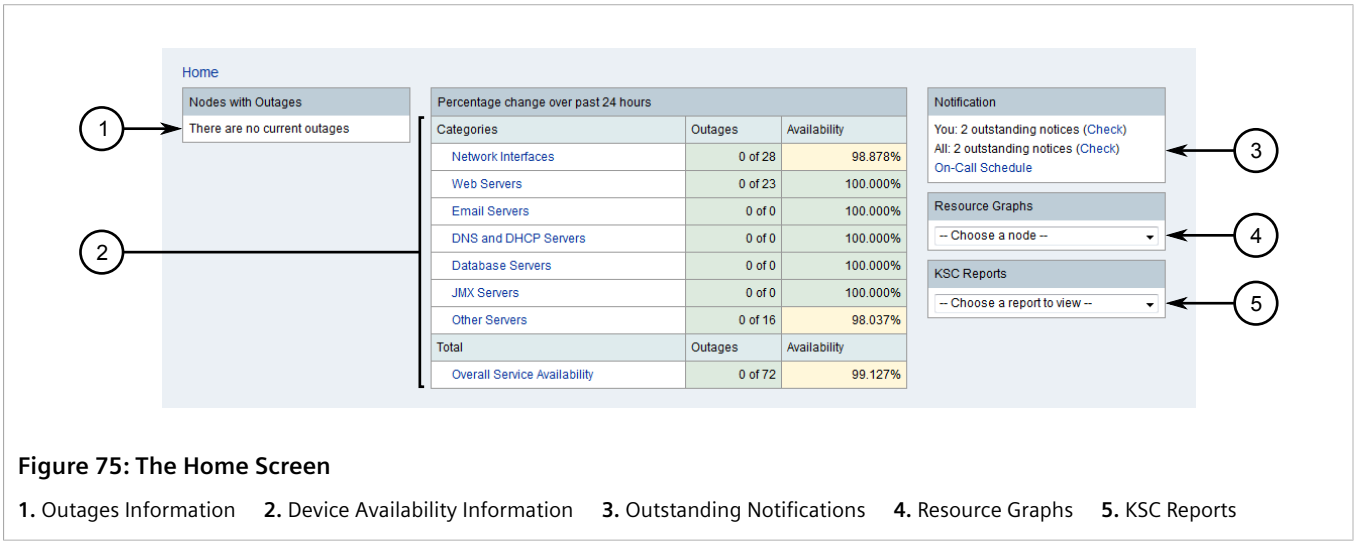


Figure 75: The Home Screen

1. Outages Information **2.** Device Availability Information **3.** Outstanding Notifications **4.** Resource Graphs **5.** KSC Reports

The **Percentage change over the past 24 hours** area details the number of outages and overall availability for each managed device that belongs to a surveillance category. Devices that have not been assigned to a surveillance category are not included in the calculation.

Viewing Details

To view further details about the availability of specific devices, click the related surveillance category. The **Category** screen appears.

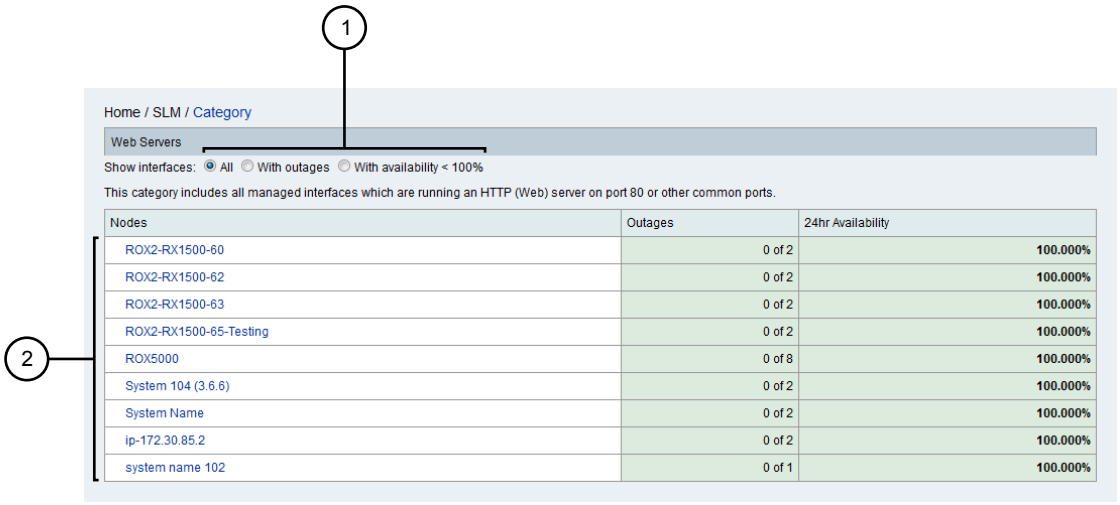


Figure 76: The Home Screen

1. Filter Options **2.** Devices

This screen includes the following filters under **Show interfaces**:

- `All` – Displays all devices.
- `With outages` – Displays only devices that have experience outages.
- `With availability < 100%` – Displays only devices that have been unavailable during the last 24 hours. This is the default view.

Customizing the List

The categories listed in the **Percentage change over the past 24 hours** area are based on surveillance categories, which can be added, modified or removed as needed. It is recommended the default surveillance categories provided by RUGGEDCOM NMS be replaced as needed with categories that are more meaningful to the organization or user. For information about how to add, configure or delete surveillance categories, refer to Section 4.11, “Managing Surveillance Categories” .

Section 5.2

Managing Events, Alarms and Notifications

The primary function of any Network Management System is to monitor the network and report changes or errors it detects to the users. In RUGGEDCOM NMS, this is done through the generation of events, alarms and notifications.

When an event occurs, RUGGEDCOM NMS displays an in-screen pop-up for all active browser sessions to inform users of the new issue.

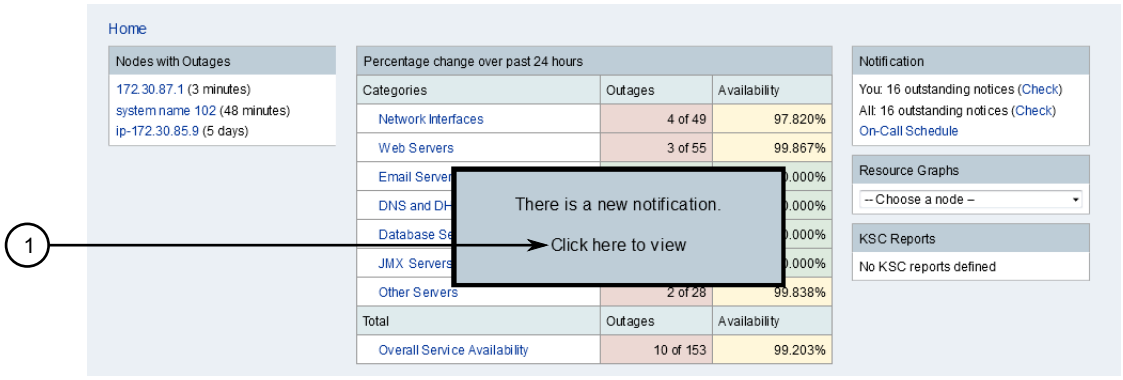


Figure 77: New Notification Pop-Up

1. Click Here to View Link

The pop-up will only disappear for each individual user if the issue is acknowledged or if each user clicks **Click Here to View**. This opens a separate browser window or tab displaying the current list of unacknowledge events. The event in question is at the top of the list.

Based on the configuration of RUGGEDCOM NMS, alarms and/or notifications may also be generated to elevate awareness of the event to other users.

It is important to promptly acknowledge all events, alarms and notifications as they arise to indicate to other users the issue is being addressed. This is particularly important for notifications, as many will be configured to follow an escalation path after a period of time to other users with higher levels of responsibility.

CONTENTS

Section 5.2.1

Understanding Severity Levels

Events, alarms and notifications are color-coded as follows based on their severity to help users quickly identify the most important events.

Color	Severity	Description
	Critical	Urgent attention is required. Multiple devices on the network are affected.
	Major	Immediate attention is required. A device is down or in danger of going down.

Color	Severity	Description
	Minor	Attention is required. Part of a device – an interface, service, power supply, etc. – has stopped functioning.
	Warning	Attention may be required. Indicates a condition that should be logged, but does not necessarily required direct action.
	Indeterminate	No level of severity could be associated with the event.
	Normal	No action required. Indicates an informational message.
	Cleared	No action required. Indicates the prior condition has been corrected and service is restored.

Information about the severity levels and their associated colors is also available through the Web user interface by hovering the mouse cursor over the legend at the top right of an event, alarm or notification list, or by clicking **Severity Legend** to display a dialog box.

Section 5.2.2
Managing Events

Events are the fundamental data structure used by RUGGEDCOM NMS for recording important information about changes to the network or changes to the configuration of RUGGEDCOM NMS. They can be generated externally by, for instance, SNMP traps or remote syslog messages generated by devices under management. But they can also be generated internally, such as upon the detection of a new device or when forcing a capability scan on a device/interface.

Each event generated by RUGGEDCOM NMS details the following:

- The event's unique ID
- The severity of the event
- The time the event occurred
- The device/node affected
- If applicable, the interface and service affected

Events are color-coded to indicate the severity of the issue. For information about the color scheme, refer to Section 5.2.1, “Understanding Severity Levels” .

CONTENTS

- Section 5.2.2.5, “Acknowledging/Unacknowledging Events”

Section 5.2.2.1
Viewing a List of Events

To view a list of current events, do the following:

1. On the menu bar, click **Events**. The **Events** screen appears.

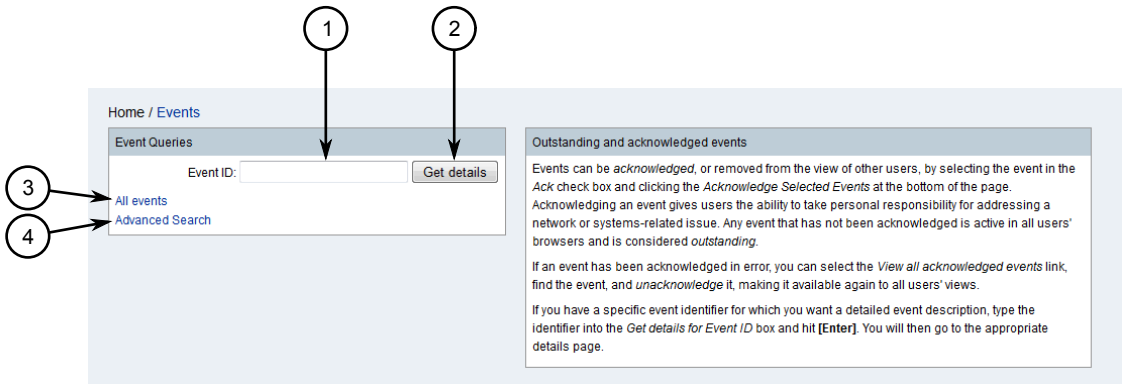


Figure 78: Events Screen

1. Event ID Box **2.** Get Details Button **3.** All Events Link **4.** Advanced Search Link

2. Click **All Events**. The **List** screen appears listing all unacknowledged events.

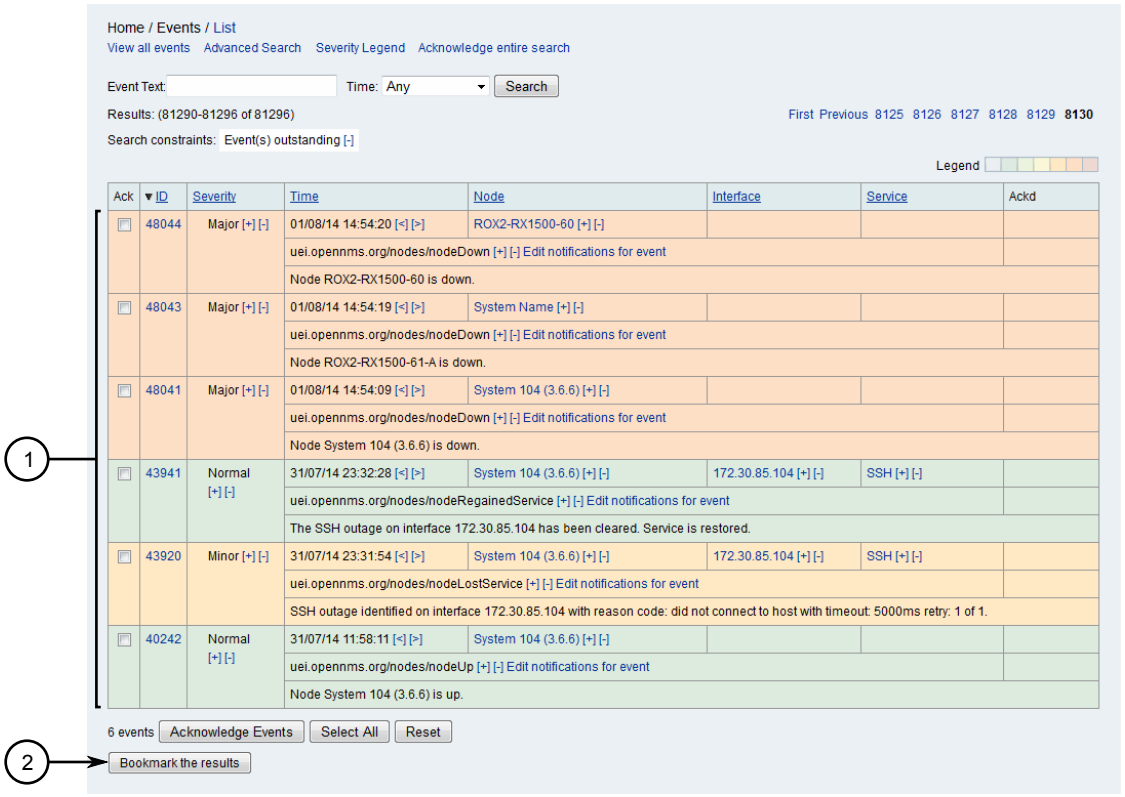


Figure 79: List Screen

1. Events **2.** Bookmark the Results Button

3. [Optional] To create a bookmark, click **Bookmark the Results**. Use the bookmark to quickly access this view at any time.

Section 5.2.2.2

Viewing Event Details

To view more details about a particular event, do one of the following:

» Event ID Is Not Known

1. Display the list of current events. For more information, refer to Section 5.2.2.1, "Viewing a List of Events" .
2. Click the ID of the desired event. The **Detail** screen appears displaying the details of the event.

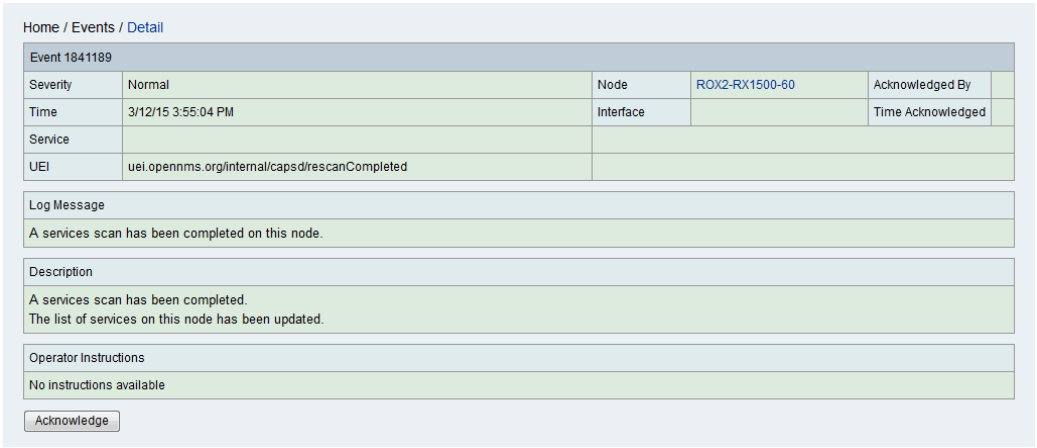


Figure 80: Detail Screen

Event ID Is Known

1. On the menu bar, click **Events**. The **Events** screen appears.

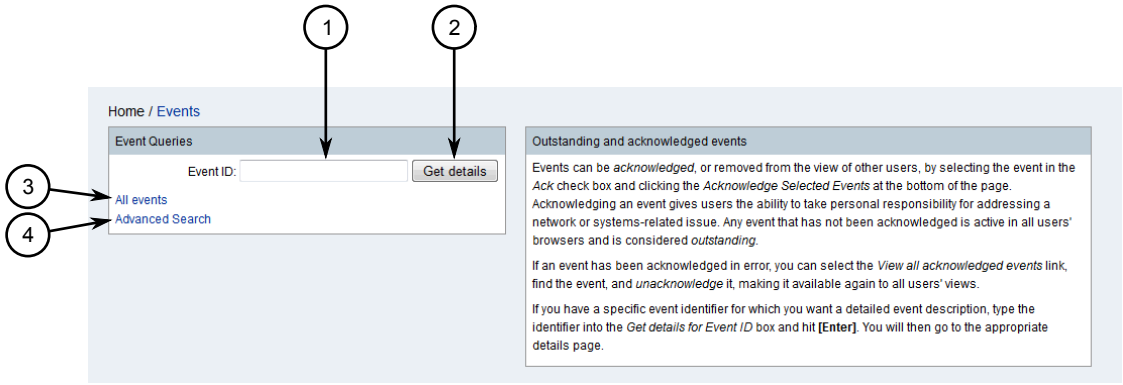


Figure 81: Events Screen

1. Event ID Box **2.** Get Details Button **3.** All Events Link **4.** Advanced Search Link

2. Under **Event ID**, type the exact ID for the desired event, then click **Get Details**. If an event with that ID exists, the **Detail** screen appears displaying the details of the event. Refer to Figure 80 .

Section 5.2.2.3
Searching for Events

To search for a specific event, do the following:

Searching Based on ID

1. On the menu bar, click **Events**. The **Events** screen appears.

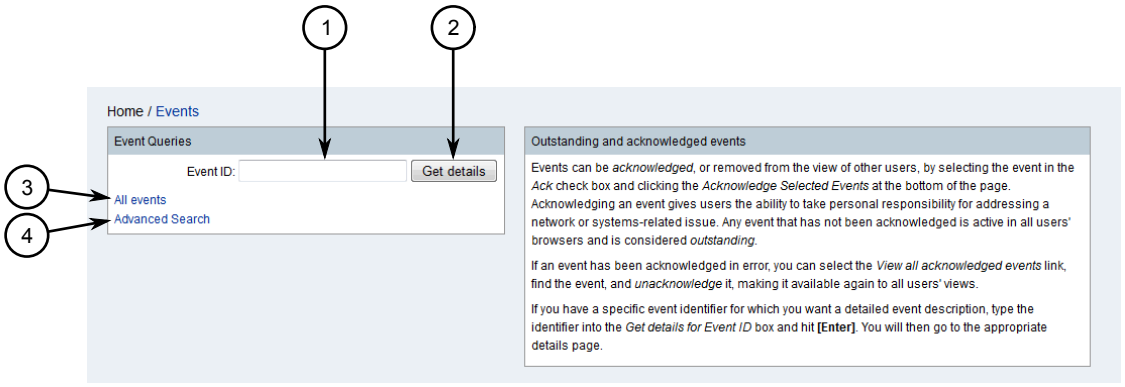


Figure 82: Events Screen

1. Event ID Box **2.** Get Details Button **3.** All Events Link **4.** Advanced Search Link

2. Under **Event ID**, type the exact ID for the event, then click **Get Details**. The **Detail** screen appears displaying the details of the event.

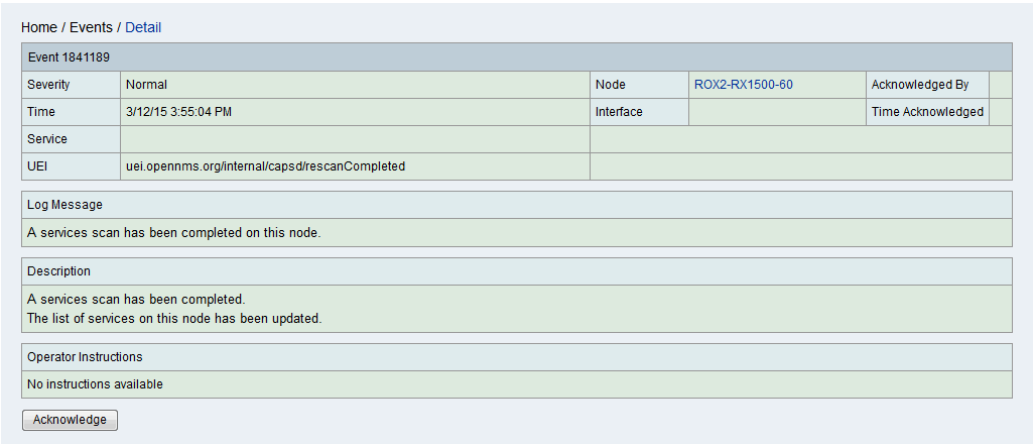


Figure 83: Detail Screen

3. [Optional] Filter the list as required to narrow the search. For more information, refer to Section 5.2.2.4, "Filtering Events" .

Searching Based on Description and Time

1. Display the list of current events. For more information, refer to Section 5.2.2.1, "Viewing a List of Events" .
2. Under **Event Text**, type a string that may appear in the event description.

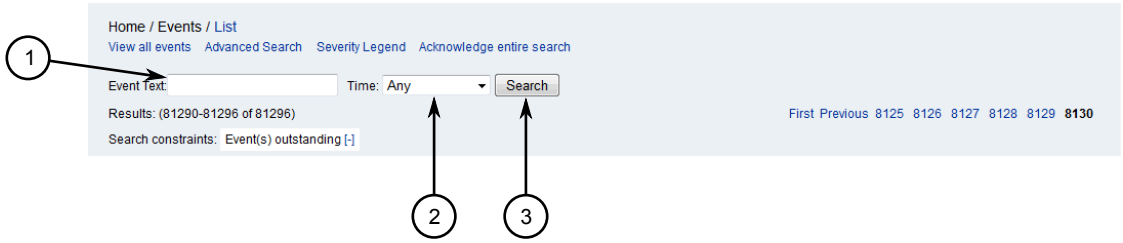


Figure 84: List Screen – Search Criteria

1. Event Text Box **2.** Time List **3.** Search Button

3. Under **Time**, select a time frame in which the event may have occurred.
4. Click **Search**. The **List** screen appears displaying the events that match the search criteria.
5. [Optional] Filter the list as required to narrow the search. For more information, refer to Section 5.2.2.4, "Filtering Events" .

» Performing an Advanced Search

1. On the menu bar, click **Events**. The **Events** screen appears.

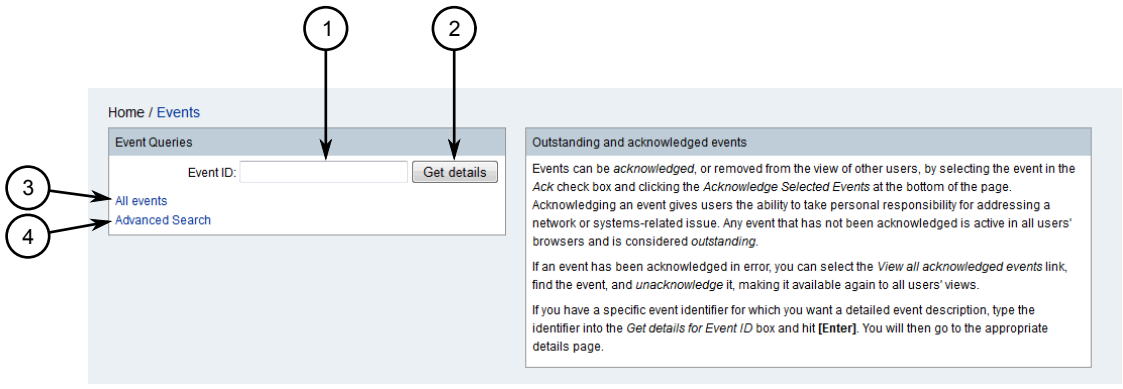


Figure 85: Events Screen

1. Event ID Box **2.** Get Details Button **3.** All Events Link **4.** Advanced Search Link

2. Click **Advanced Search**. The **Advanced Event Search** screen appears.

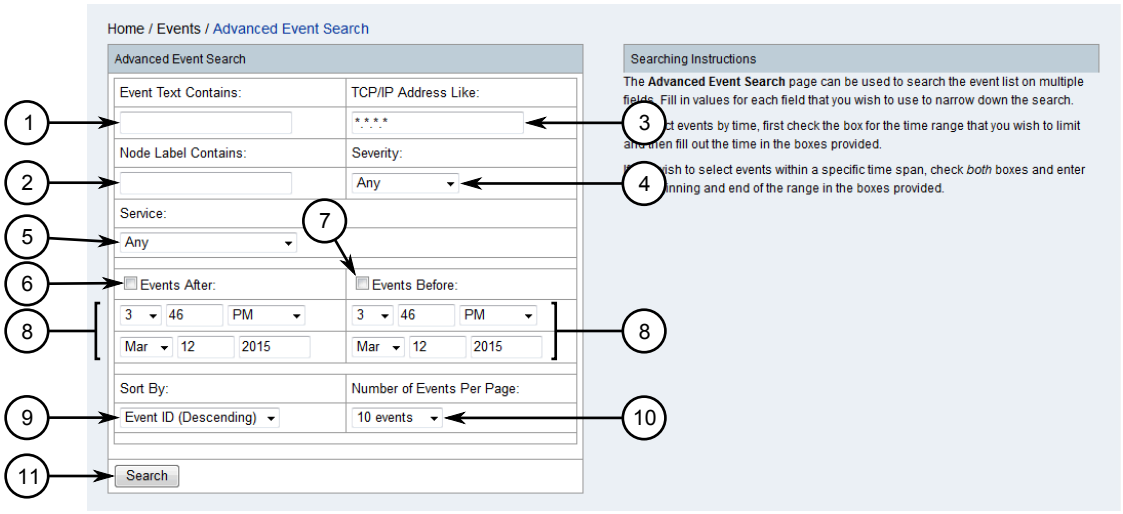


Figure 86: Advanced Event Search Screen

1. Event Text Contains Box **2.** Node Label Contains Box **3.** TCP/IP Address Like Box **4.** Severity List **5.** Service List **6.** Events After Check Box **7.** Events Before Check Box **8.** Time/Date Controls **9.** Sort By List **10.** Number of Events Per Page List **11.** Search Button

3. Set the search criteria:
   - **Event Text Contains** – Type a text string that may appear in the event description.
   - **TCP/IP Address Like** – Type the IP address for the affected device or interface. If needed, use an asterisk (*) as a wild card in place of an octet.
   - **Node Label Contains** – Type the label for the affected device or interface.
   - **Severity** – Select the severity level for the event.
   - **Service** – Select a service offered by the affected device/interface.
   - **Events After** – Select **Events After** and enter a date and time to search for events that occurred after that time.
   - **Events Before** – Select **Events Before** and enter a date and time to search for events that occurred before that time.
4. Under **Sort By**, select the sort order of the events list.
5. Under **Number of Events Per Page**, select the number of events to display per page.
6. Click **Search**. The **List** screen appears listing all the events that match the search criteria.

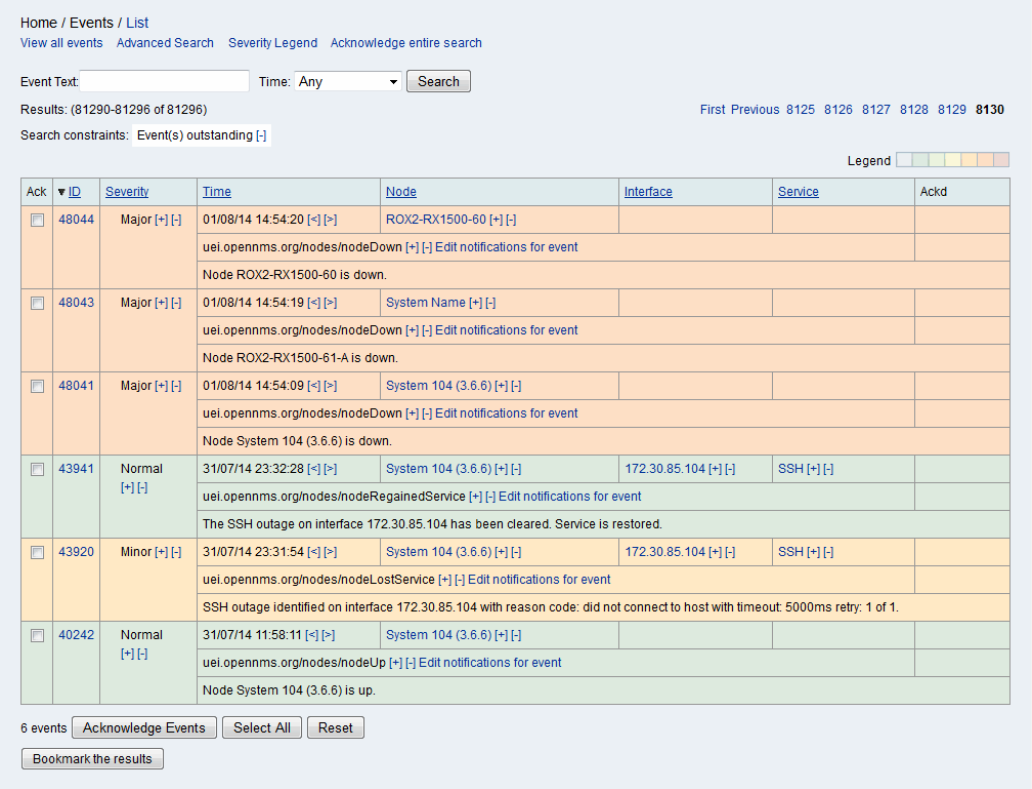


Figure 87: List Screen

7. [Optional] Filter the list as required to narrow the search. For more information, refer to Section 5.2.2.4, "Filtering Events" .

Section 5.2.2.4

Filtering Events

Each list of events features controls for filtering out events and displaying only those that are important to the user. Filtering is also a way of searching for a specific event.

There are two methods for filtering an event list:

- **Filter Based on Description and Time**
  To filter a list of events based on an event's description and the time at which the event occurred, do the following:
  1. Display the list of current events. For more information, refer to Section 5.2.2.1, "Viewing a List of Events" .
  2. Under **Event Text**, type the full description of the event or key words that might appear in the description.

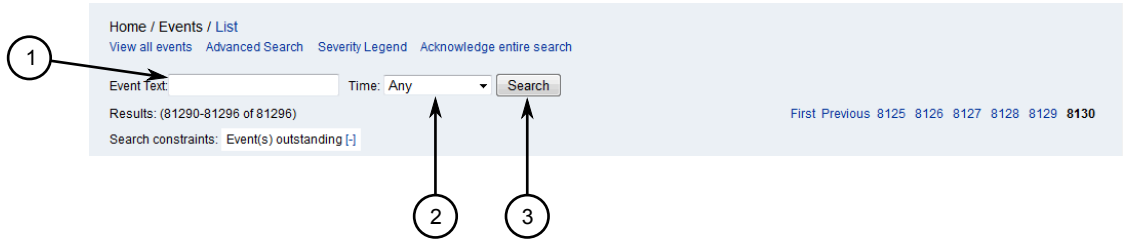


Figure 88: Event Text and Time Controls

1. Event Text Box **2.** Time Box **3.** Search Button **4.** Search Constraints

3. Under **Time**, select a time period at which the event may have occurred.
4. Click **Search**. The search criteria is listed under **Search Constraints** and the list is updated to display the events that match.

   A filter can be removed by clicking **[-]** next to it.

- **Filter Using the Filter Controls**
  Each list of events features controls for removing or adding events of a specific type, that have a specific UEI, ones that occurred before/after a specific time, and more.

  Filters are available in cells under the **Severity** and **Time** columns, as well on the cells that reference the UEI (Unique Event Identifier).

  Controls include the following:

Filter Control	Description
[+]	Only shows events that match the value in the current field. For example, clicking **[+]** in the **Severity** column displays only events that are at the same severity level as the selected event/alarm.
[-]	Hides events that match the value in the current field. For example, in the case of events, clicking **[-]** next to a UEI hides all events that have the same UEI.
[<]	Only shows events that occurred after the selected event/alarm. Only applicable to the time of the event/alarm.
[>]	Only shows events that occurred before the selected event/alarm. Only applicable to the time of the event/alarm.

NOTE
For quick reference in the RUGGEDCOM NMS Web user interface, hover the mouse cursor over any filter control to view a tool tip describing its function.

Once a filter is applied, it appears above the table in the list of search constraints. A filter can be removed by clicking **[-]** next to it.

Section 5.2.2.5
Acknowledging/Unacknowledging Events

Events can be acknowledged or unacknowledged from two areas within RUGGEDCOM NMS:

- **From a List of Events**
  Every list of events includes the option to acknowledge or unacknowledge an item.

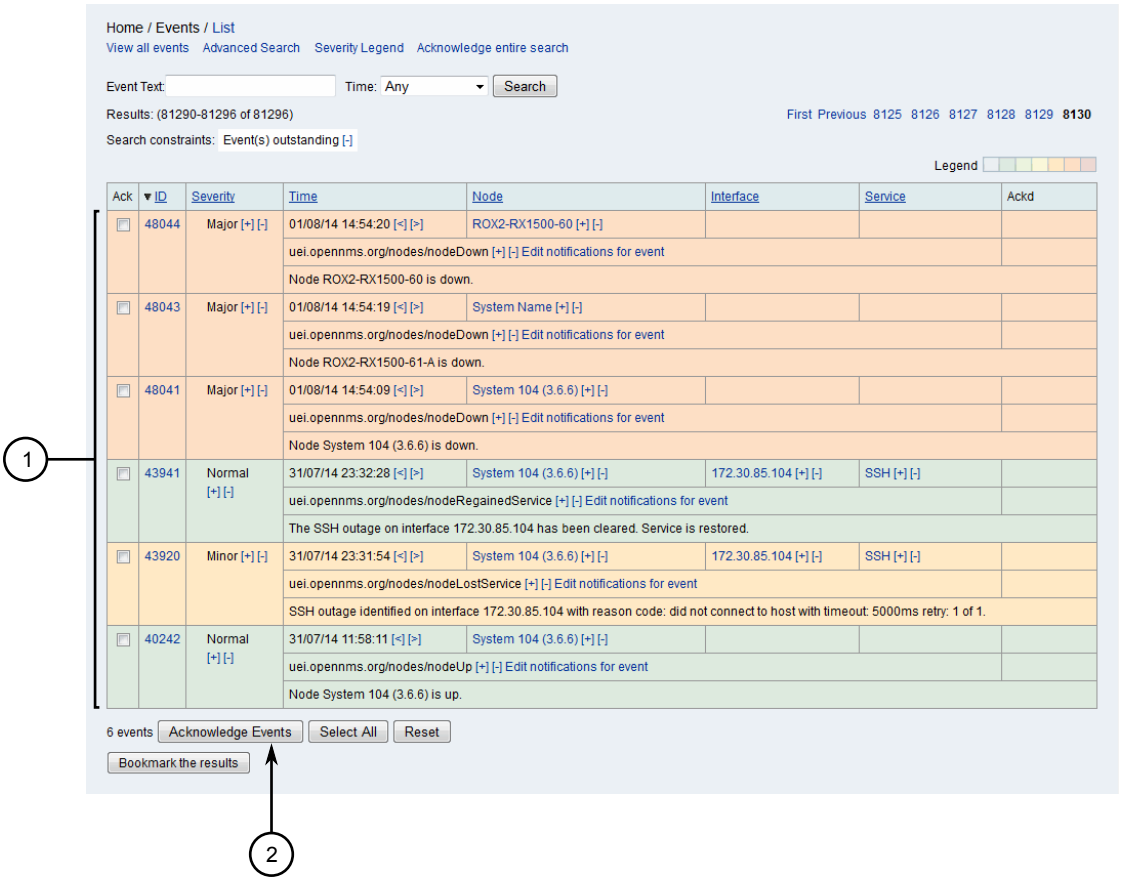


Figure 89: Acknowledge Button on a List of Events

1. Events **2.** Acknowledge Button

Simply select an event and click either **Acknowledge** or **Unacknowledge**, depending on the current status of the event.

- **From the Device Details Screen**
  The details screen for each device includes a **Recent Events** section that lists the recent unacknowledged events. For information about how to acknowledge events from the device details screen, refer to Section 6.4.2.7, "Recent Events" .

Section 5.2.3

Managing Alarms

Alarms are based on events that have been picked specifically during the configuration of RUGGEDCOM NMS to be representative of the current health of the network.

Each alarm generated by RUGGEDCOM NMS details the following:

- The alarms unique ID
- The severity level of the event

- The affected device, interface and/or service
- The number of times the event has occurred
- The times for when the event first occurred and when it last occurred
- A description of the alarm condition

Alarms are color-coded to indicate the severity of the issue. For information about the color scheme, refer to Section 5.2.1, "Understanding Severity Levels" .

CONTENTS

Section 5.2.3.1
Viewing a List of Alarms

To view a list of current alarms, do the following:

1. On the menu bar, click **Alarms**. The **Alarms** screen appears.

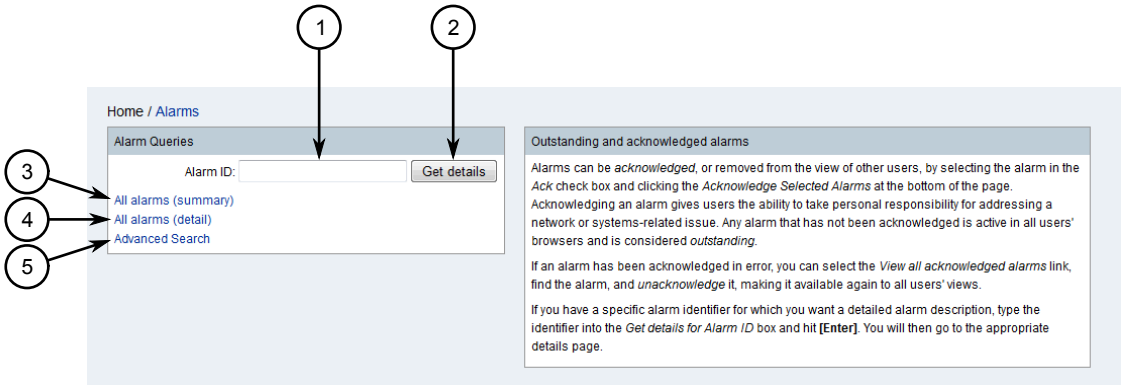


Figure 90: Alarms Screen

1. Alarm ID Box **2.** Get Details Button **3.** All Alarms (Summary) Link **4.** All Alarms (Detail) Link **5.** Advanced Search Link

NOTE
Summary and detailed views are available for alarm lists. The summary view excludes interfaces, services, and the first event time, while the detailed view provides all information.

2. Click either **All Alarms (Summary)** or **All Alarms (Detail)**. The **List** screen appears listing all unacknowledged alarms.

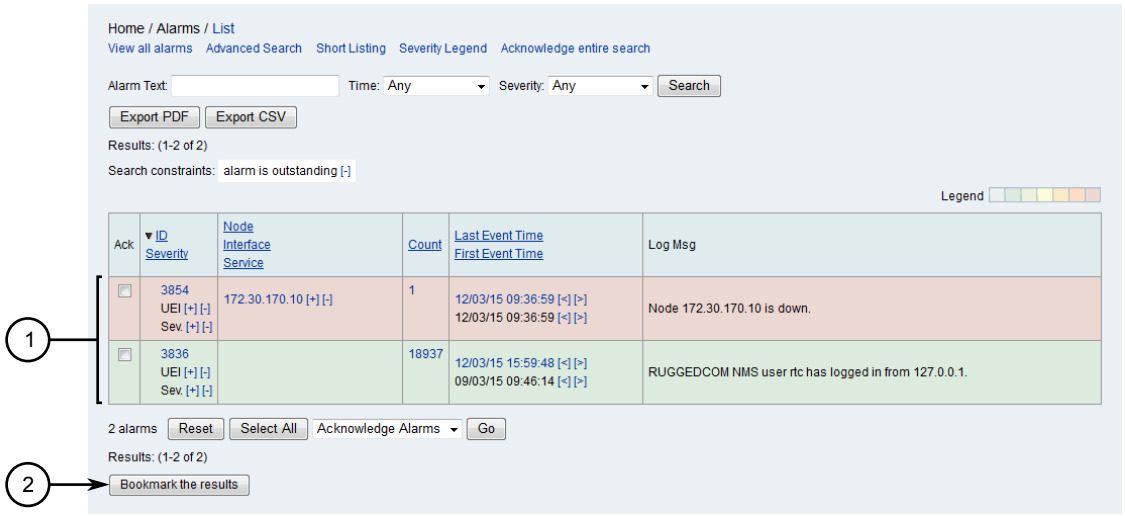


Figure 91: List Screen

1. Alarms **2.** Bookmark the Results Button

3. [Optional] To create a bookmark, click **Bookmark the Results**. Use the bookmark to quickly access this view at any time.

Section 5.2.3.2
Viewing Alarm Details

To view more details about a particular alarm, do one of the following:

» Alarm ID Is Not Known

1. Display the list of current alarms. For more information, refer to Section 5.2.3.1, “Viewing a List of Alarms” .
2. Click the ID of the desired alarm. The **Detail** screen appears displaying the details of the alarm.

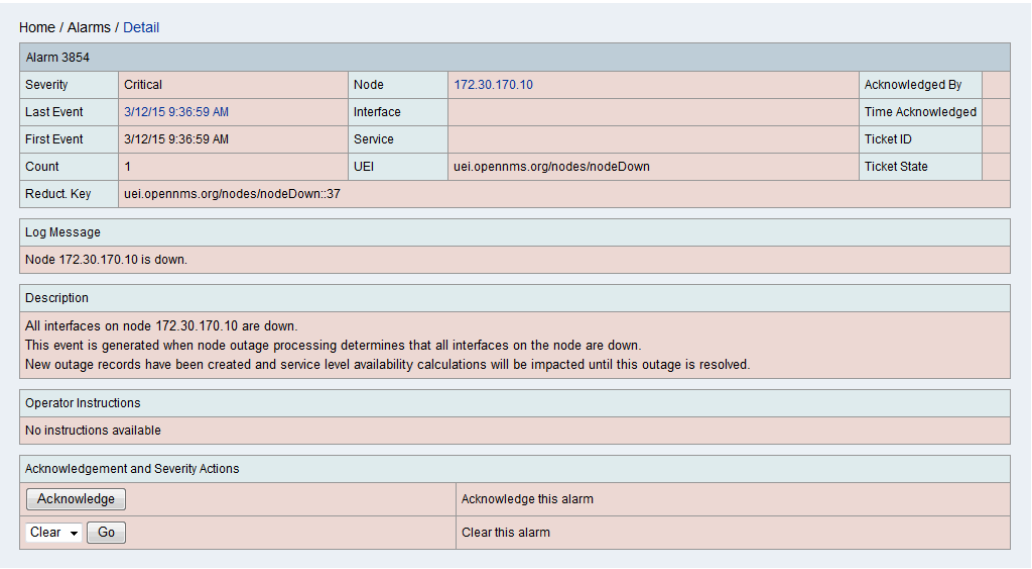


Figure 92: Detail Screen

Alarm ID Is Known

1. On the menu bar, click **Alarms**. The **Alarms** screen appears.

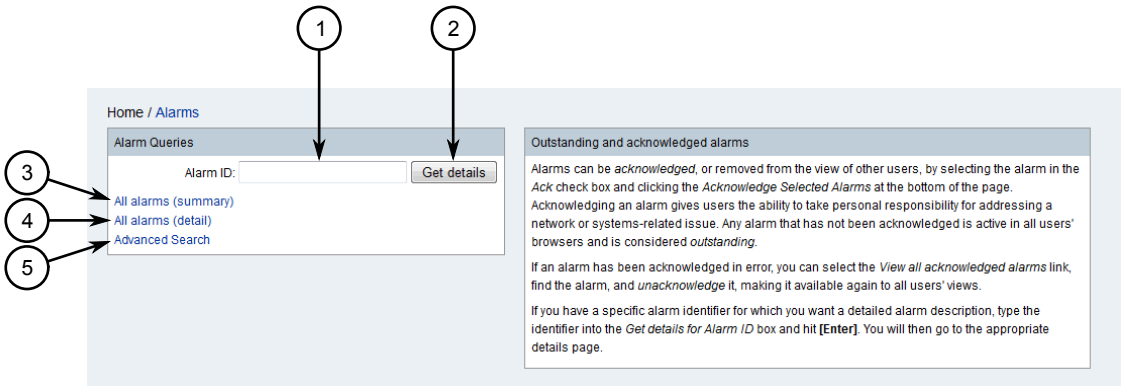


Figure 93: Alarms Screen

1. Alarm ID Box **2.** Get Details Button **3.** All Alarms (Summary) Link **4.** All Alarms (Detail) Link **5.** Advanced Search Link

2. Under **Alarm ID**, type the exact ID for the desired alarm, then click **Get Details**. If an alarm with that ID exists, the **Detail** screen appears displaying the details of the alarm. Refer to Figure 92 .

Section 5.2.3.3
Searching for Alarms

To search for a specific alarm, do the following:

Searching Based on ID

1. On the menu bar, click **Alarms**. The **Alarms** screen appears.

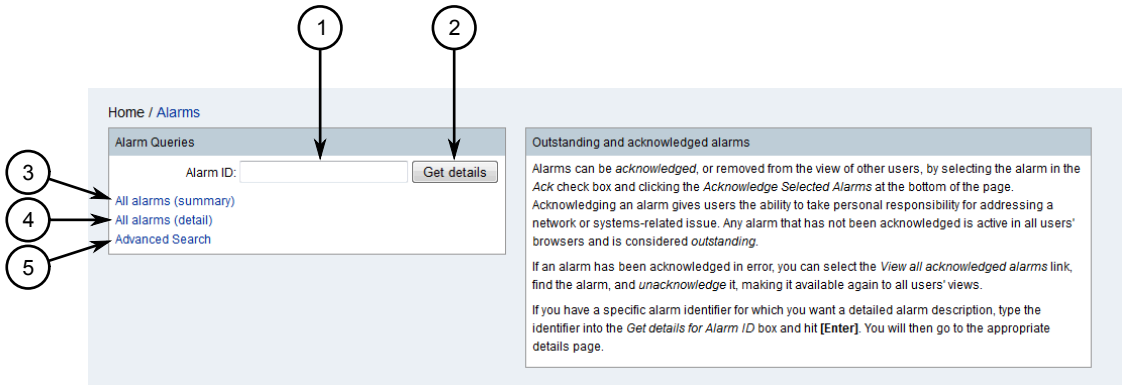


Figure 94: Alarms Screen

1. Alarm ID Box **2.** Get Details Button **3.** All Alarms (Summary) Link **4.** All Alarms (Detail) Link **5.** Advanced Search Link

2. Under **Alarm ID**, type the exact ID for the alarm, then click **Get Details**. The **Detail** screen appears displaying the details of the alarm.

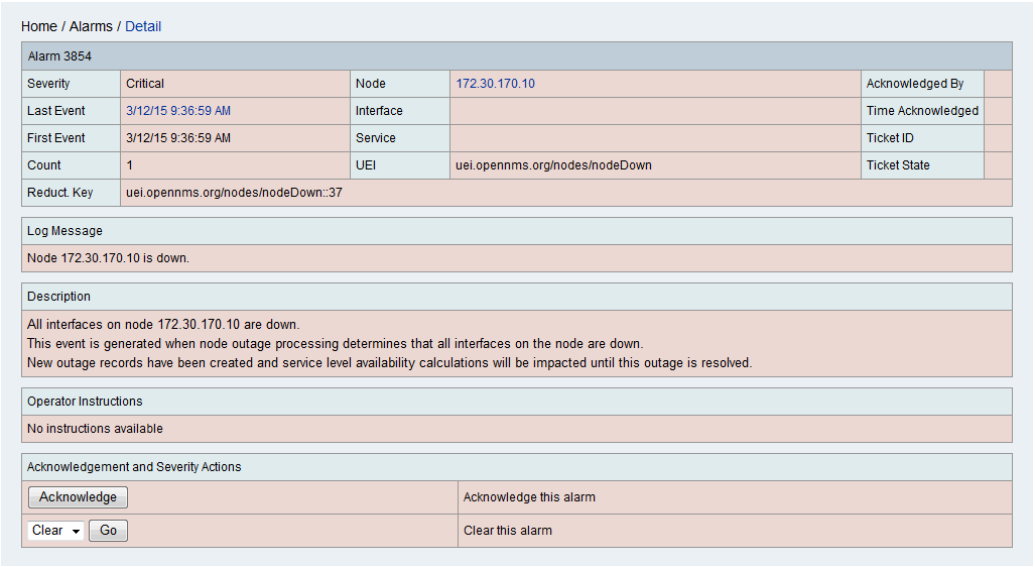


Figure 95: Detail Screen

3. [Optional] Filter the list as required to narrow the search. For more information, refer to Section 5.2.2.4, "Filtering Events" .

Searching Based on Description, Time and Severity

1. Display the list of all current alarms. For more information, refer to Section 5.2.3.1, "Viewing a List of Alarms" .

2. Under **Alarm Text**, type a string that may appear in the event description.

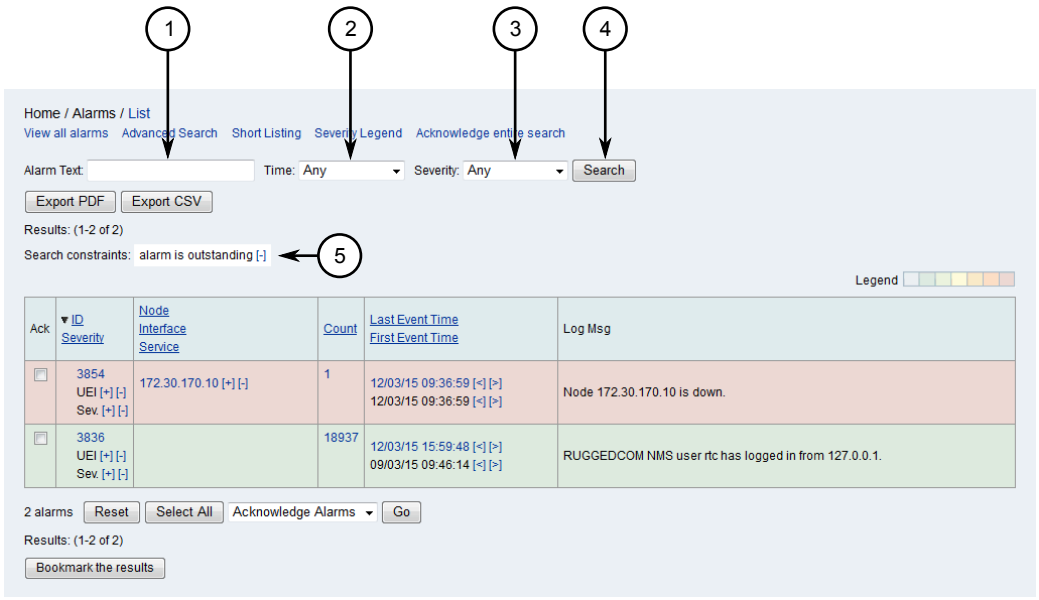


Figure 96: List Screen – Search Criteria

1. Alarm Text Box **2.** Time List **3.** Severity List **4.** Search Button

3. Under **Time**, select a time frame in which the alarm may have occurred.
4. Under **Severity**, select the severity of the alarm.
5. Click **Search**. The **List** screen appears displaying the alarms that match the search criteria.
6. [Optional] Filter the list as required to narrow the search. For more information, refer to Section 5.2.2.4, "Filtering Events" .

» Performing an Advanced Search

1. On the menu bar, click **Alarms**. The **Alarms** screen appears.

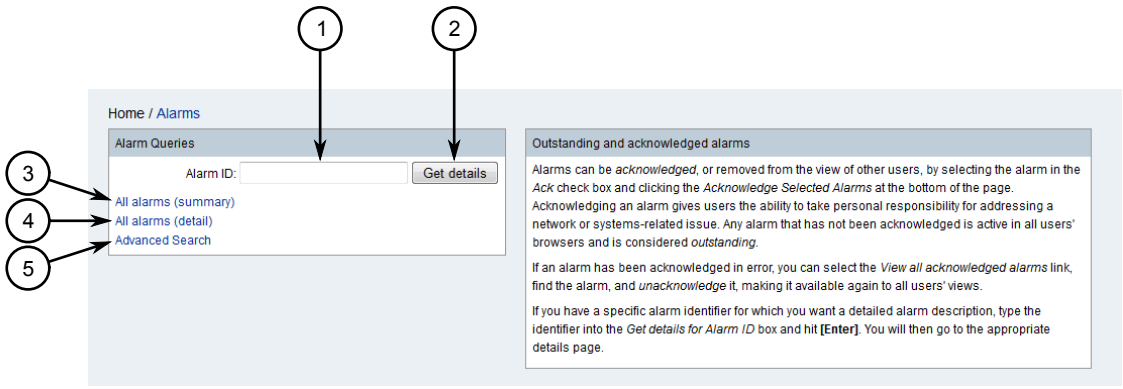


Figure 97: Alarms Screen

1. Alarm ID Box **2.** Get Details Button **3.** All Alarms Link **4.** Advanced Search Link

2. Click **Advanced Search**. The **Advanced Alarm Search** screen appears.

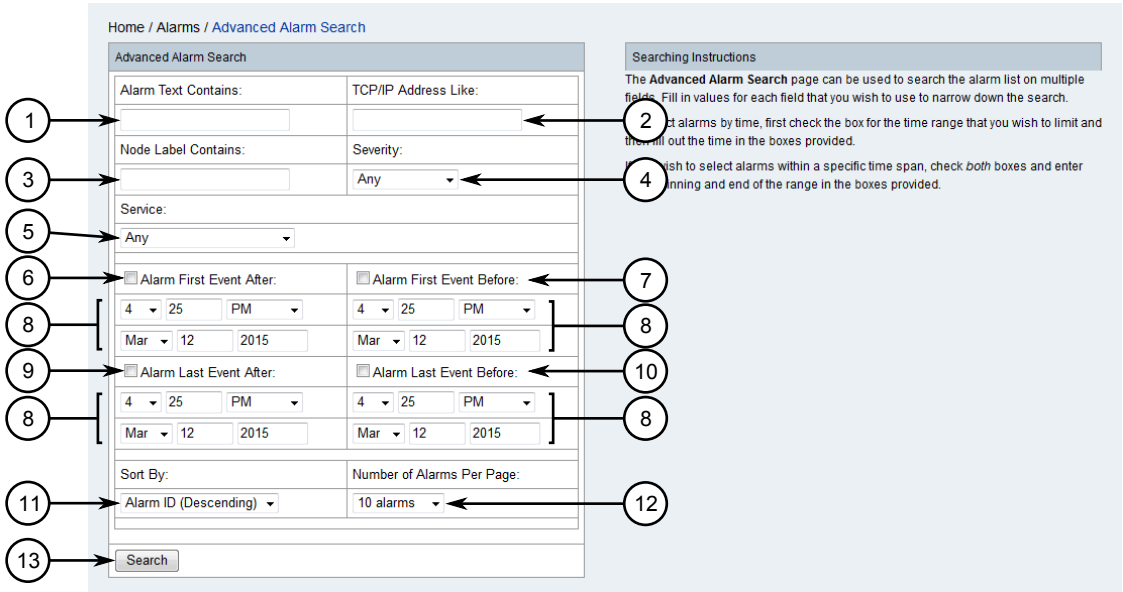


Figure 98: Advanced Alarm Search Screen

1. Alarm Text Contains Box **2.** Node Label Contains Box **3.** TCP/IP Address Like Box **4.** Severity List **5.** Service List **6.** Alarm First Event After Check Box **7.** Alarm First Event Before Check Box **8.** Time/Date Controls **9.** Alarm Last Event After Check Box **10.** Alarm Last Event Before Check Box **11.** Sort By List **12.** Number of Alarms Per Page List **13.** Search Button

3. Set the search criteria:

- **Alarm Text Contains** – Type a text string that may appear in the alarm description.
- **TCP/IP Address Like** – Type the IP address for the affected device or interface. If needed, use an asterisk (*) as a wild card in place of an octet.
- **Node Label Contains** – Type the label for the affected device or interface.

- **Severity** – Select the severity level for the alarm.
- **Service** – Select a service offered by the affected device/interface.
- **Alarm First Event After** – Select **Alarm First Event After** and enter a date and time to search for the first event that occurred after that time.
- **Alarm First Event Before** – Select **Alarm First Event Before** and enter a date and time to search for the first event that occurred before that time.
- **Alarm Last Event After** – Select **Alarm Last Event After** and enter a date and time to search for the last event that occurred after that time.
- **Alarm Last Event Before** – Select **Alarm Last Event Before** and enter a date and time to search for the last event that occurred before that time.

4. Under **Sort By**, select the sort order of the alarms list.
5. Under **Number of Alarms Per Page**, select the number of alarms to display per page.
6. Click **Search**. The **List** screen appears listing all the alarms that match the search criteria..

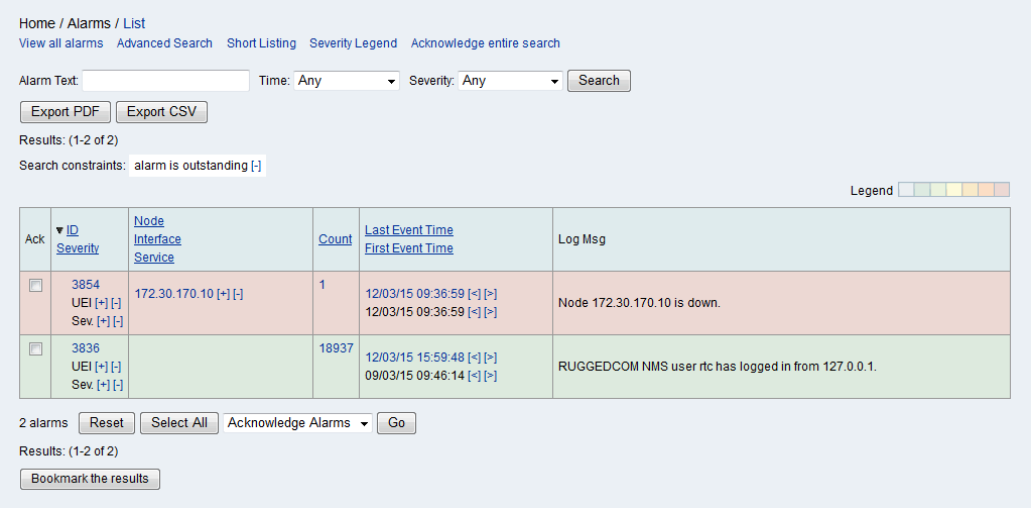


Figure 99: List Screen

7. [Optional] Filter the list as required to narrow the search. For more information, refer to Section 5.2.2.4, "Filtering Events" .

Section 5.2.3.4
Filtering Alarms

Each list of alarms features controls for filtering out alarms and displaying only those that are important to the user. Filtering is also a way of searching for a specific alarm.

There are two methods for filtering an alarm list:

- **Filter Based on Description, Time and Severity**
  To filter a list of alarms based on an alarm's description, the time at which the alarm occurred, and its severity level, do the following:

1. Display the list of current alarms. For more information, refer to Section 5.2.3.1, "Viewing a List of Alarms".
2. Under **Alarm Text**, type the full description of the alarm or key words that might appear in the description.

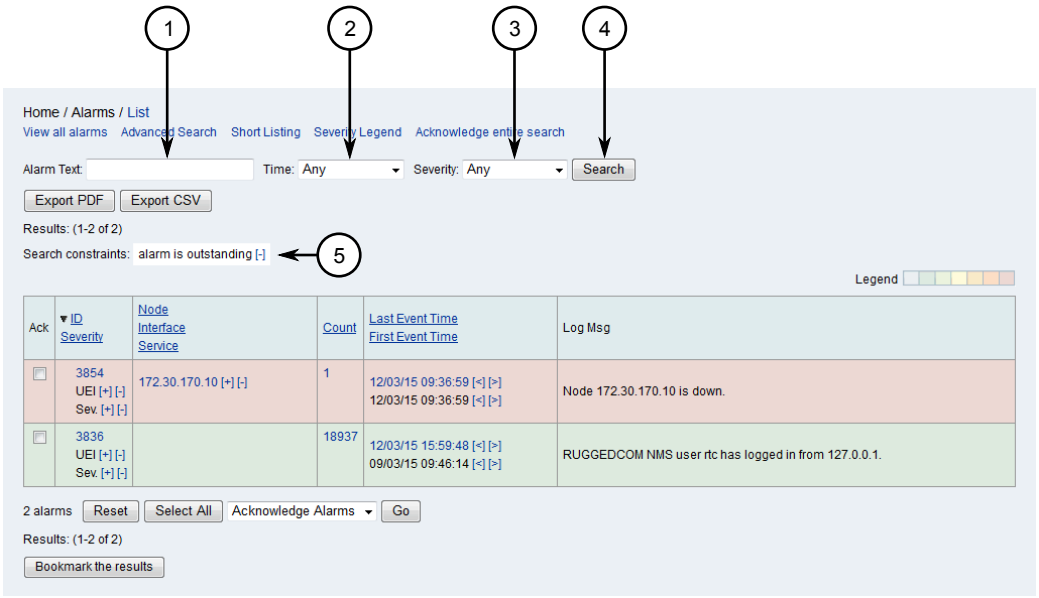


Figure 100: Alarm Text, Time and Severity Controls

1. Alarm Text Box **2.** Time Box **3.** Severity Box **4.** Search Button **5.** Search Constraints

3. Under **Time**, select a time period at which the alarm may have occurred.
4. Under **Severity**, select a severity level.
5. Click **Search**. The search criteria is listed under **Search Constraints** and the list is updated to display the alarms that match.

   A filter can be removed by clicking **[-]** next to it.

- **Filter Using the Filter Controls**

  Each list of alarms features controls for removing or adding alarms of a specific type, that have a specific UEI, ones that occurred before/after a specific time, and more.

  Filters are available in cells under the **ID Severity** and **Last Event Time/First Event Time** columns.

  Controls include the following:

Filter Control	Description
[+]	Only shows alarms that match the value in the current field. For example, clicking **[+]** in the **Severity** column displays only alarms that are at the same severity level as the selected alarm/alarm.
[-]	Hides alarms that match the value in the current field. For example, in the case of alarms, clicking **[-]** next to a UEI hides all alarms that have the same UEI.
[<]	Only shows alarms that occurred after the selected alarm/alarm. Only applicable to the time of the alarm/alarm.
[>]	Only shows alarms that occurred before the selected alarm/alarm. Only applicable to the time of the alarm/alarm.

NOTE
For quick reference in the RUGGEDCOM NMS Web user interface, hover the mouse cursor over any filter control to view a tool tip describing its function.

Once a filter is applied, it appears above the table in the list of search constraints. A filter can be removed by clicking **[-]** next to it.

Section 5.2.3.5
Exporting a List of Alarms

To export a list of alarms to either PDF or a CSV (Comma-Separate Values) file, do the following:

1. Display the list of current alarms or search for specific alarms. For more information, refer to Section 5.2.3.1, "Viewing a List of Alarms" or Section 5.2.3.3, "Searching for Alarms" . The **List** screen appears.

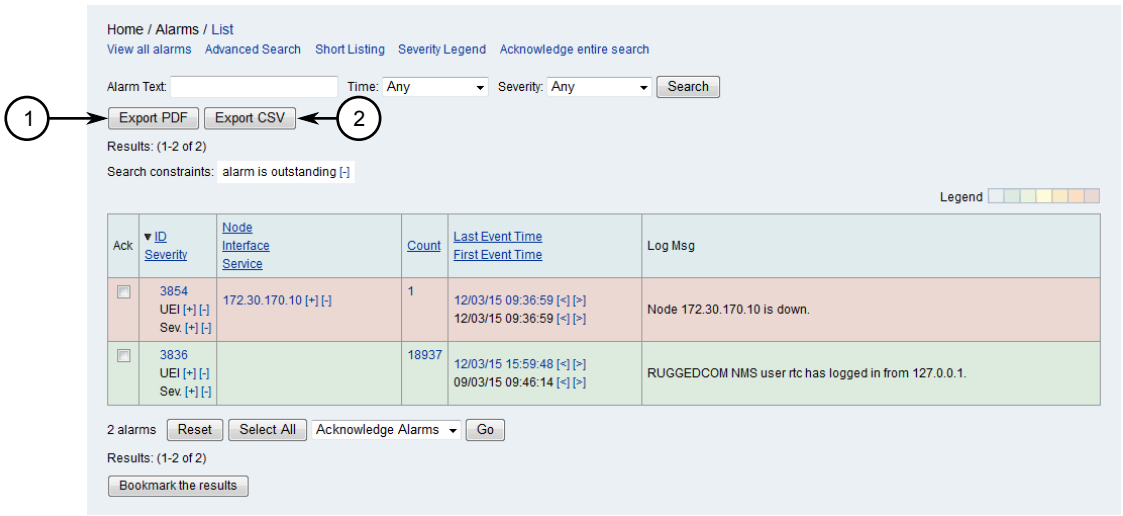


Figure 101: List Screen

1. Export to PDF Button **2.** Export to CSV Button

2. On the **List** screen, click either **Export to PDF** or **Export to CSV**. A dialog box appears.
3. Select where to save the file locally and then click **OK**.

Section 5.2.3.6
Acknowledging, Clearing and Escalating Alarms

Alarms can be acknowledged, cleared or escalated. Acknowledging an alarm simply indicates to other users the issue is being addressed, while clearing an alarm removes the alarm from the list entirely, indicating the issue is resolved. Escalating an alarm raises its severity level, which may prompt RUGGEDCOM NMS to send a notification to another user or group, if such a notification is configured.

To acknowledge, clear or escalate an alarm, do the following:

1. Display the list of current alarms or search for specific alarms. For more information, refer to Section 5.2.3.1, "Viewing a List of Alarms" or Section 5.2.3.3, "Searching for Alarms" . The **List** screen appears.

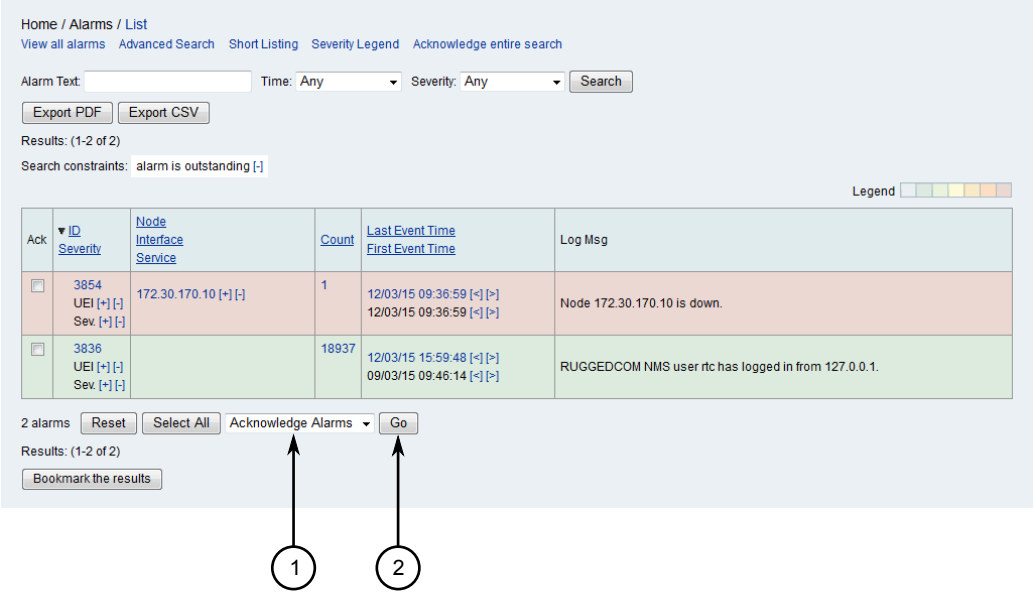


Figure 102: List Screen

1. List **2.** Go Button

2. Select the desired alarm(s).
3. Select the desired action from the list (i.e. Acknowledge Alarms, Clear Alarms or Escalate Alarms), then click **OK**.

Section 5.2.4

Managing Notifications

Notifications, or notices, are messages sent out when particular events occur. RUGGEDCOM NMS can be configured to send these notifications to specific users, groups and/or users who have a specific role.

Each notification generated by RUGGEDCOM NMS details the following:

- The notifications unique ID
- The ID of the related event
- The severity level of the event
- The time the notification was sent
- The name of the user who answered the message
- The time at which the user answered the message
- The affected device, interface and/or service
- A description of the event

Notifications are color-coded to indicate the severity of the issue. For information about the color scheme, refer to Section 5.2.1, "Understanding Severity Levels" .

CONTENTS

Section 5.2.4.1
Viewing a List of Notifications

To view a list of current notifications, do the following:

1. On the menu bar, click **Notifications**. The **Notifications** screen appears.

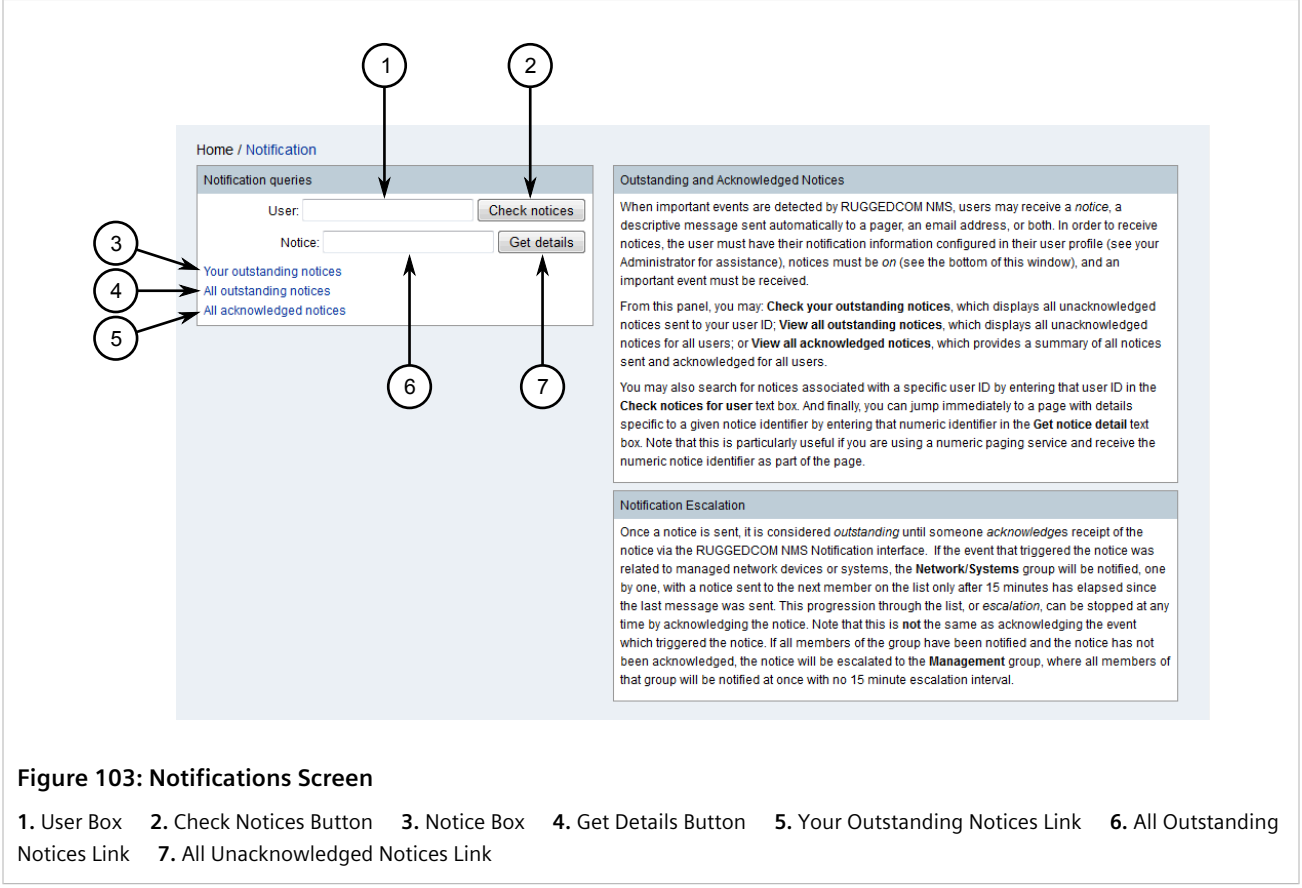


Figure 103: Notifications Screen

1. User Box **2.** Check Notices Button **3.** Notice Box **4.** Get Details Button **5.** Your Outstanding Notices Link **6.** All Outstanding Notices Link **7.** All Unacknowledged Notices Link

2. Click either **Your Oustanding Notices**, **All Outstanding Notices** or **All Unacknowledge Notices**. The **List** screen appears listing the matching notifications.

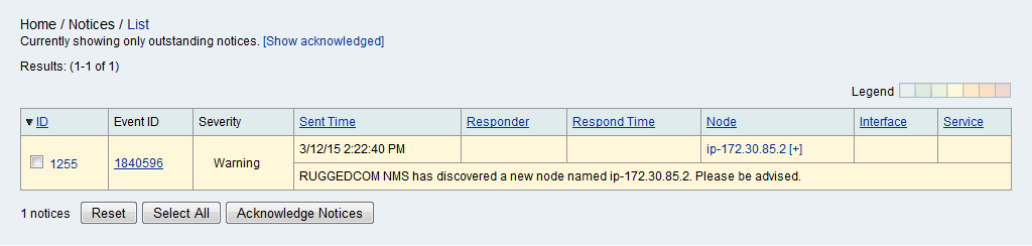


Figure 104: List Screen

Section 5.2.4.2

Viewing Notification Details

To view more details about a particular notification, do one of the following:

» Notification ID Is Not Known

1. Display the list of current notifications. For more information, refer to Section 5.2.4.1, "Viewing a List of Notifications" .
2. Click the ID of the desired notification. The **Detail** screen appears displaying the details of the notification.

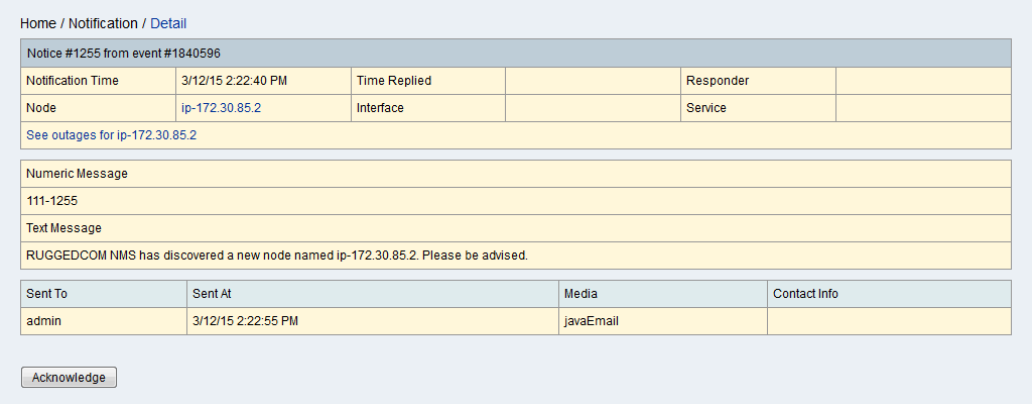


Figure 105: Detail Screen

» Notification ID Is Known

1. On the menu bar, click **Notifications**. The **Notifications** screen appears.

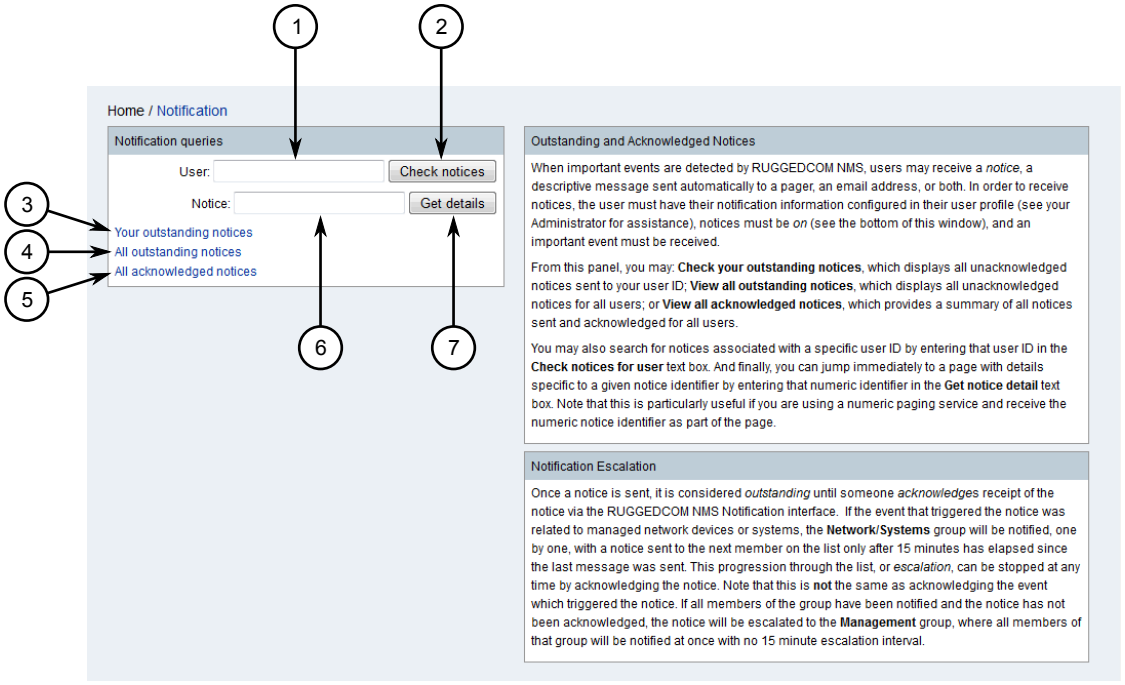


Figure 106: Notifications Screen

1. User Box **2.** Check Notices Button **3.** Notice Box **4.** Get Details Button **5.** Your Outstanding Notices Link **6.** All Outstanding Notices Link **7.** All Unacknowledged Notices Link

2. Under **Notice**, type the exact ID for the desired notification, then click **Get Details**. If a notification with that ID exists, the **Detail** screen appears displaying the details of the notification. Refer to Figure 105 .

Section 5.2.4.3
Searching for Notifications

Notifications can be found based on the user to which they are sent.

To search for a notification sent to a specific user, do the following:

1. On the menu bar, click **Notifications**. The **Notifications** screen appears.

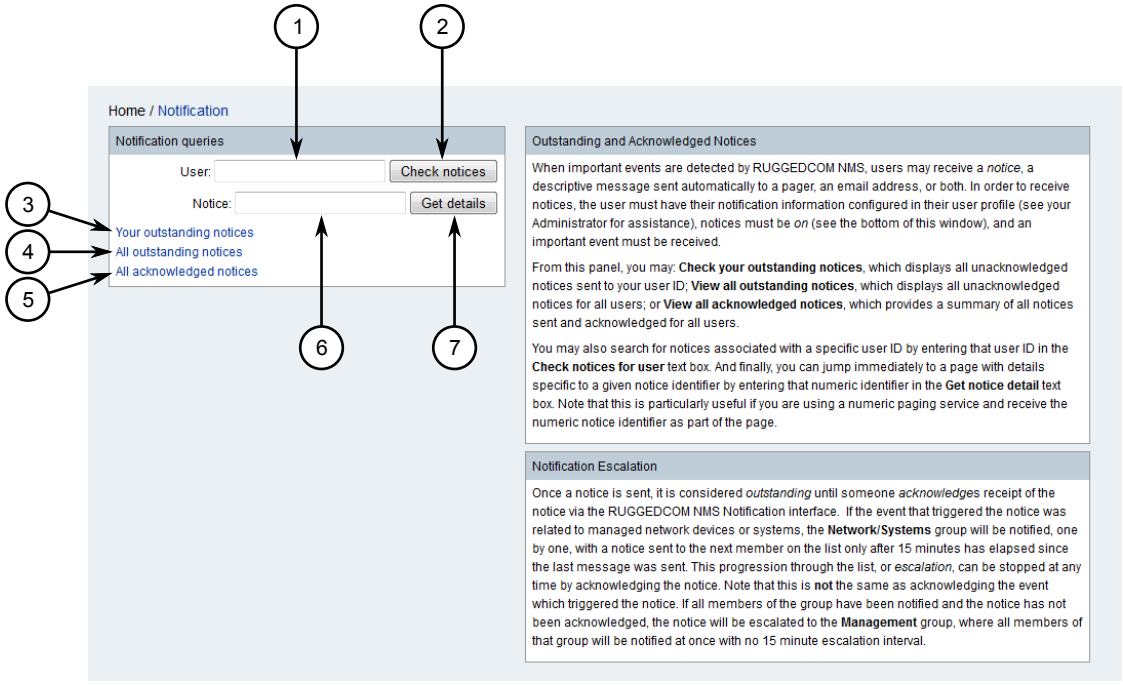


Figure 107: Notifications Screen

1. User Box **2.** Check Notices Button **3.** Notice Box **4.** Get Details Button **5.** Your Outstanding Notices Link **6.** All Outstanding Notices Link **7.** All Unacknowledged Notices Link

2. Under **User**, the type of the name of the user's profile (e.g. admin), then click **Check Notices**. The **List** screen appears displaying all notifications sent to that user.

Section 5.2.4.4

Acknowledging Notifications

To acknowledge a notification, do the following:

1. Display the list of current notifications or search for specific notifications. For more information, refer to Section 5.2.4.1, "Viewing a List of Notifications" or Section 5.2.4.3, "Searching for Notifications" . The **List** screen appears.

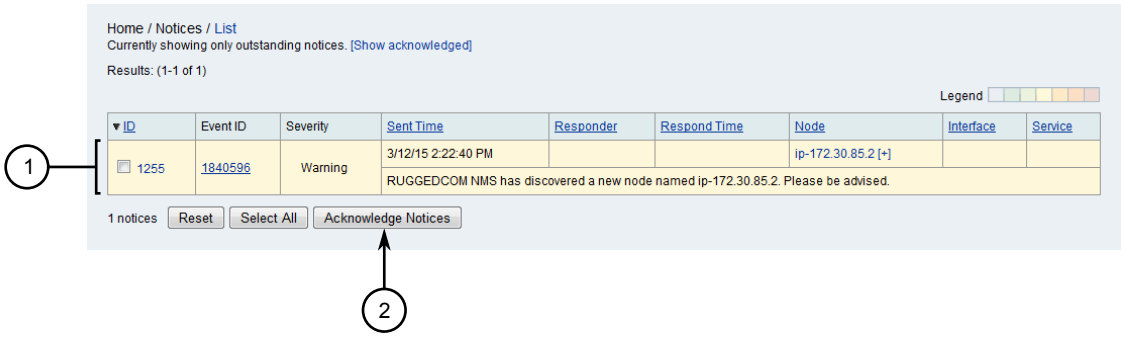


Figure 108: List Screen

1. List **2.** Go Button

2. Select the desired notification(s) and then click **Acknowledge Notices**.

Section 5.2.4.5

Enabling/Disabling Notifications

To enable or disable all notifications, do the following:

1. On the menu bar, click **Admin**. The **Admin** screen appears.

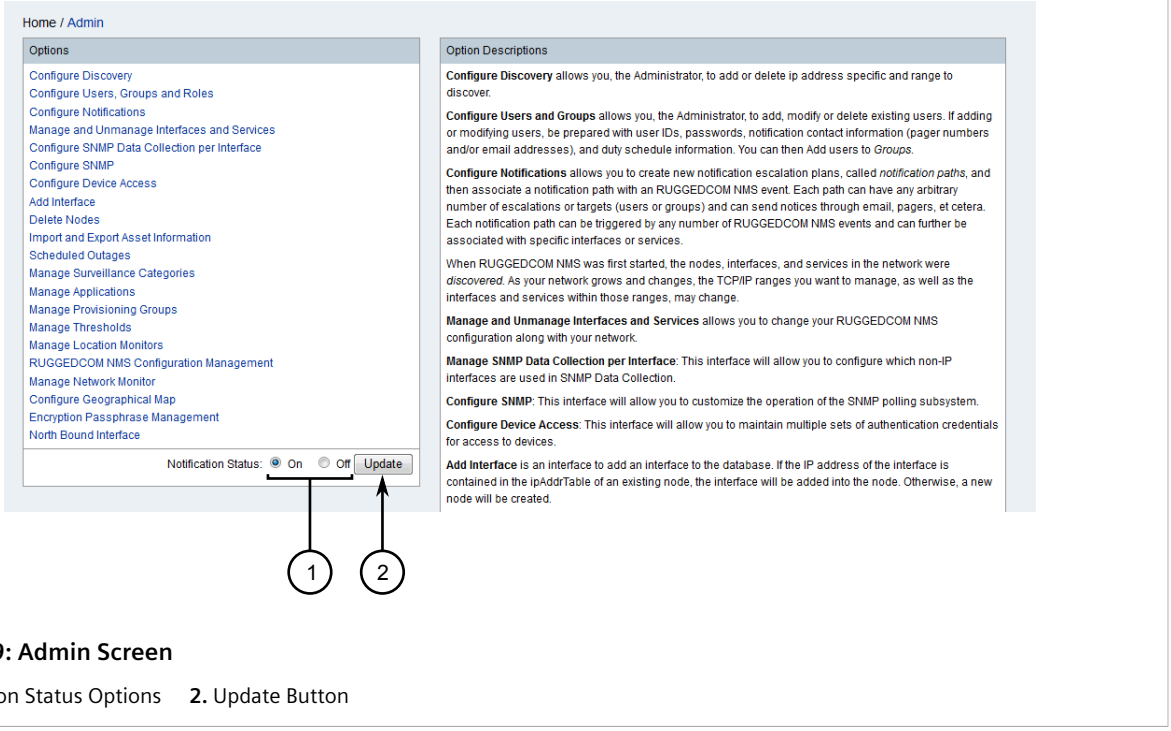


Figure 109: Admin Screen

1. Notification Status Options **2.** Update Button

2. Under **Notification Status**, select `On` to enable notifications or `Off` to disable notifications.
3. Click **Update**.

Section 5.2.4.6
Enabling/Disabling Specific Notifications

To enable or disable specific notifications, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications** and then click **Configure Event Notifications**. The **Event Notifications** screen appears.

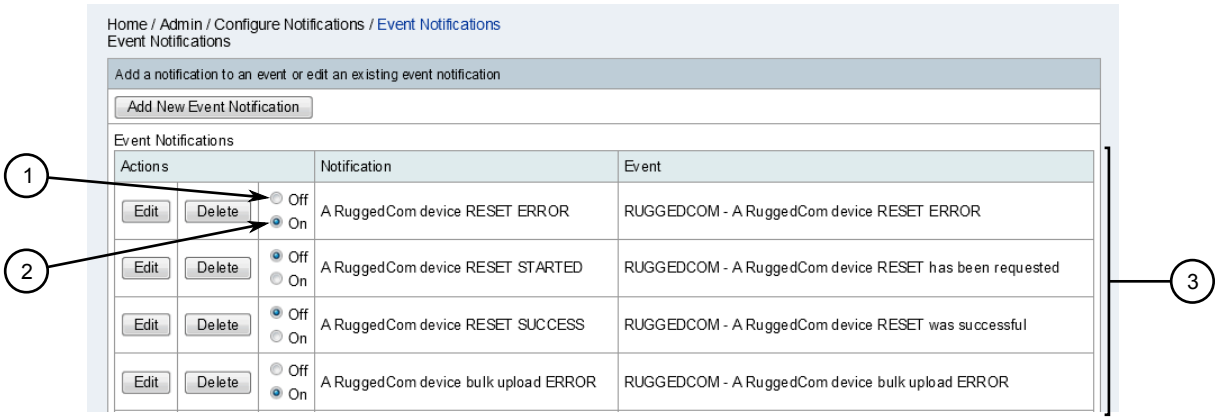


Figure 110: Event Notifications Screen

1. Off Option **2.** On Option **3.** Available Event Notifications

2. For the chosen notification, select `On` to enable the notification or `Off` to disable it. The setting is automatically applied.

Section 5.2.4.7
Adding/Editing a Notification

To add or edit an existing notification, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications** and then click **Configure Event Notifications**. The **Event Notifications** screen appears.

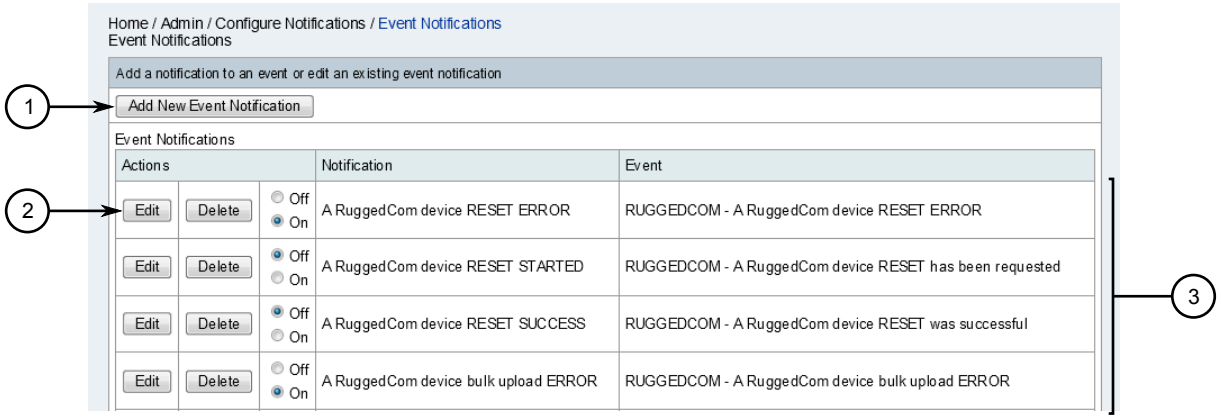


Figure 111: Event Notifications Screen

1. Add New Event Notification Button **2.** Edit Button **3.** Available Event Notifications

2. Click **Add New Event Notification** to add a new notification, or select an existing notification and click **Edit**. The **Choose Event** screen appears.

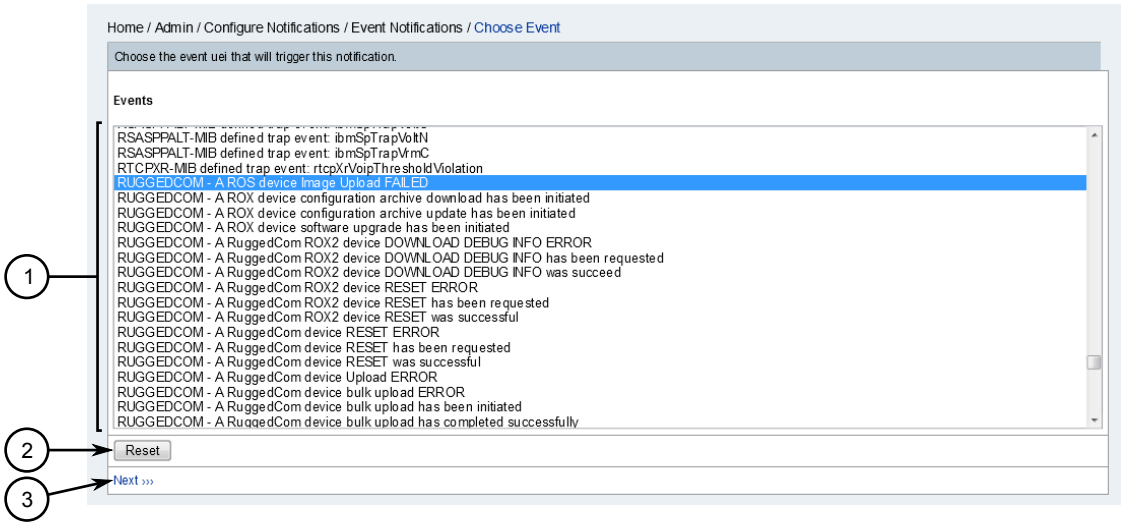


Figure 112: Choose Event Screen

1. List of Unique Event Identifiers (UEIs) **2.** Reset Button **3.** Next Link

This screen lists the available Unique Event Identifiers (UEI).

3. For new notifications or to select a different UEI for an existing notification, select one of the available UEIs.
4. Click **Next**. The **Build Rule** screen appears.

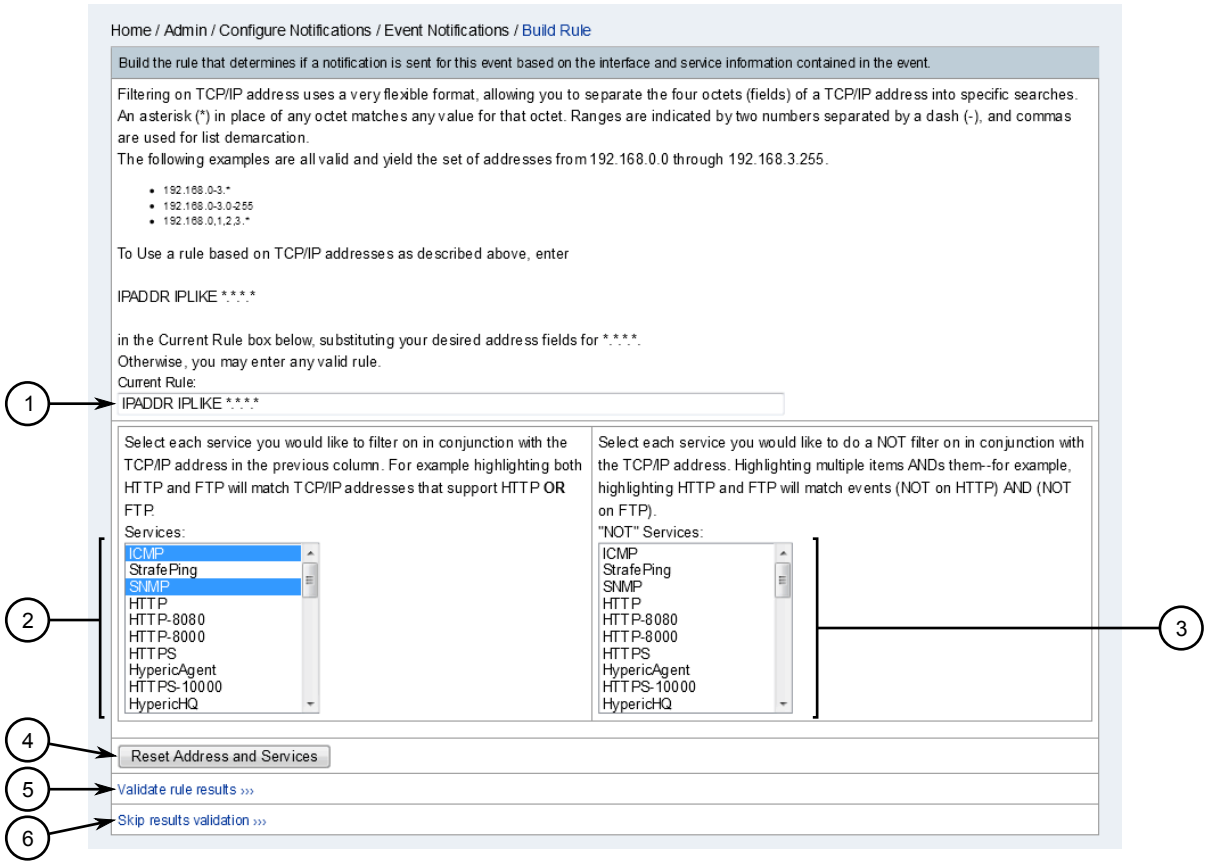


Figure 113: Build Rule Screen

1. Current Rule Box **2.** Services List **3.** Not Services List **4.** Reset Address and Services Button **5.** Validate Rule Results Link **6.** Skip Results Validation Link

5. Under **Current Rule**, define a build rule that looks for the chosen event on one or more interfaces.

   RUGGEDCOM NMS uses the Iplike search format, which allows users to search for interfaces based on any one of the four octets (fields). An asterisk (*) in place of an octet matches any value for that octet. A range (e.g. 0-3, 0-255, etc.) in place of an octet matches any value for that octet that falls within in the specified range. A comma (,) creates a demarcated list (e.g. 0,1,2,3).

   For example, each of the following rules will find interfaces with IP address between 192.168.0.0 and 192.168.3.255:

   ```
   IPADDR IPLIKE 192.168.0-3.*
   IPADDR IPLIKE 192.168.0-3.0-255
   IPADDR IPLIKE 192.168.0,1,2,3.*
   ```

   NOTE
   *To select consecutive services, click the first service, then hold **Shift** and click the last service. To select specific services, click the first service, and then hold **Ctrl** and select other services from the list.*

6. From the list of services and *NOT* services, select the services for which notifications should or should *not* be generated.
7. [Optional] If necessary, click **Reset Address and Services** to reset the build rule and repeat Step 5 to Step 6.
8. [Optional] Click **Validate Rule Results** to test the build rule. The **Validate Rule** screen appears.

> **NOTE**
> *To skip the validation step, click **Skip Results Validation** and proceed to Step 9.*

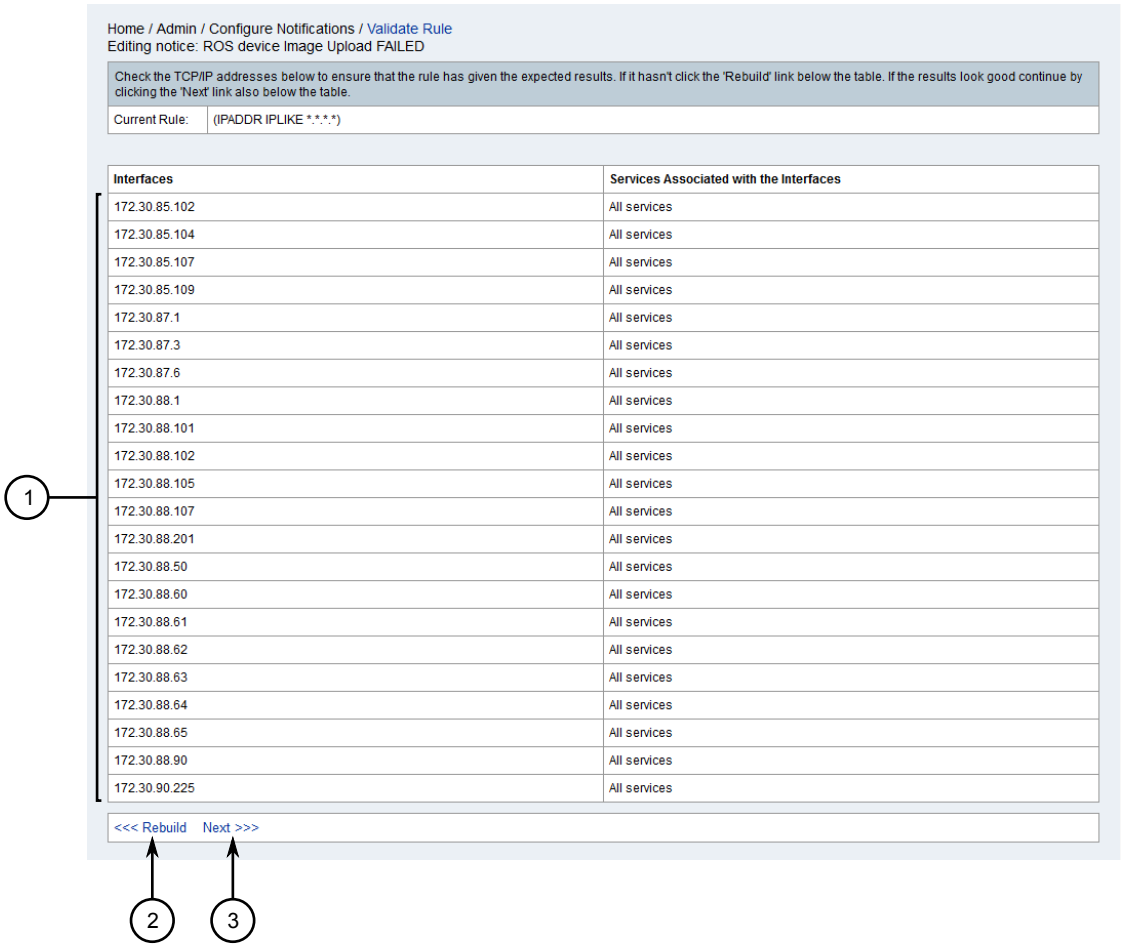


Figure 114: Validate Rule Screen

1. List of IP Addresses **2.** Rebuild Link **3.** Next Link

Review the list of IP addresses to make sure the build rule provides the expected results. If the expected IP addresses are missing from the list, click **Rebuild** and repeat Step 5 to Step 8.

9. On the **Choose Path** screen, configure the following parameters:

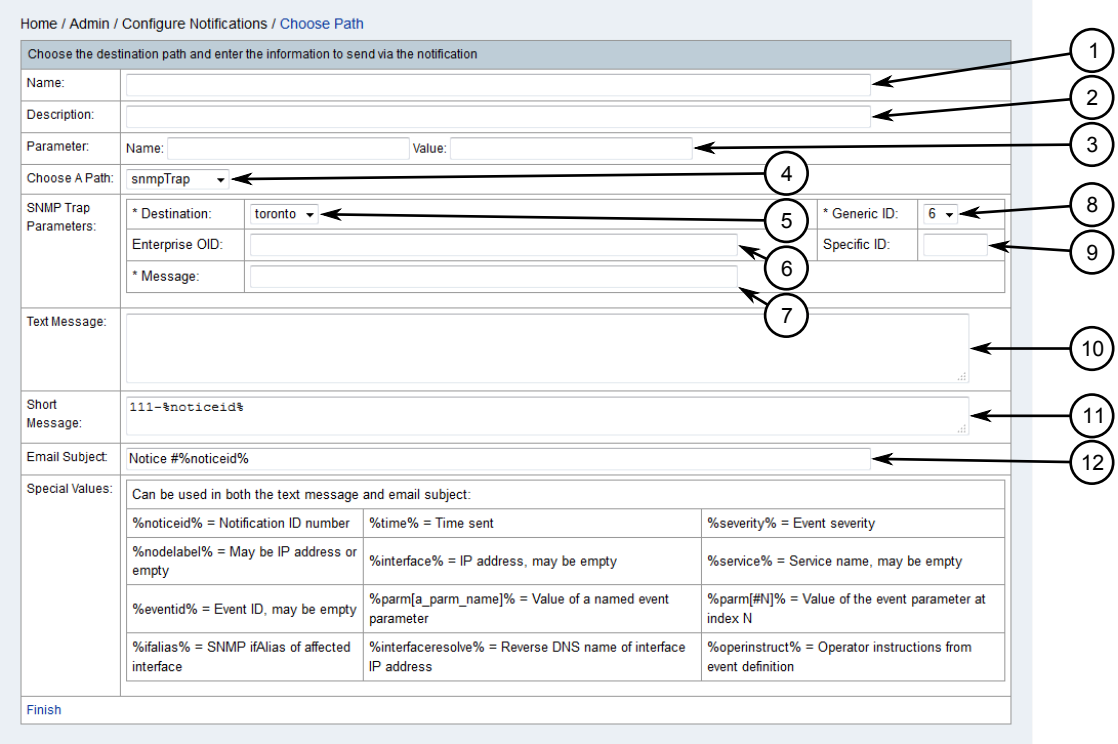


Figure 115: Choose Path Screen

1. Name Box **2.** Description Box **3.** Parameter Boxes **4.** Choose a Path List **5.** Destination List **6.** Enterprise OID Box **7.** Message Box **8.** Generic ID List **9.** Specific ID Box **10.** Text Message Box **11.** Short Message Box **12.** Email Subject Box

NOTE

*Parameters under **SNMP Trap Parameters** only appear when a destination path that has been configured to use the snmpTrap command is chosen. For information about configuring a destination path, refer to Section 5.2.6, "Managing Destination Paths".*

Parameter	Description
Name	A unique name for the notification.
Description	A description of the notification.
Parameter	The parameter – and its value – carried by the event.
Choose a Path	The destination path to which the notification will be sent. For more information about destination paths, refer to Section 5.2.6, "Managing Destination Paths".
Destination	The destination to which to forward the event. For more information about configuring a destination, refer to Section 6.5.6, "Managing SNMP Event Forwarding".
Generic ID	**Synopsis:** { 0, 1, 2, 3, 4, 5, 6 } A generic ID for the trap. Options include: • `0 (coldStart)` – Indicates the SNMP agent is down. • `1 (warmStart)` – Indicates the SNMP agent has reinitialized.

Parameter	Description
	• `2 (linkDown)` – Indicates a device is down. • `3 (linkUp)` – Indicates a device is back up. • `4 (authenticationFailure)` – Indicates someone has queried the SNMP agent using an incorrect community string. • `5 (egpNeighborLoss)` – Indicates an Exterior Gateway Protocol (EGP) neighbor is down. • `6 (enterpriseSpecific)` – Indicates the trap is enterprise-specific. A valid OID must be provided by the *`Specific ID`* parameter.
Enterprise OID	The Object Identifier (OID) for a custom trap. A valid OID includes the enterprise ID of the organization that defined the trap and a specific trap number assigned by that organization. Use only when the *`Generic ID`* value is 6.
Specific ID	The specific ID for the trap.
Message	The description of the notification. The description may be a simple text string, such as *Configuration Change* for a configuration change event, or it may also include event fields (e.g. %*{event}*%). It is recommended to review the events defined in the configuration files under `/usr/share/opennms/etc/events`. Each `<event/>` element in the configuration files contains a `<descr/>` element, whose value can be used as the description.
Text Message	The message sent in the notification. In place of a custom message, use event substitutions to automatically add details from the event into the message.
Short Message	A custom message to briefly describe the event.
Email Subject	The subject of the notification. This appears in the subject line of e-mails sent by RUGGEDCOM NMS for the notification. In place of a custom subject, use event substitutions to automatically add details from the event into the subject.

10. Click **Finish**.

Section 5.2.4.8
Deleting a Notification

To delete a notification, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications** and then click **Configure Event Notifications**. The **Event Notifications** screen appears.

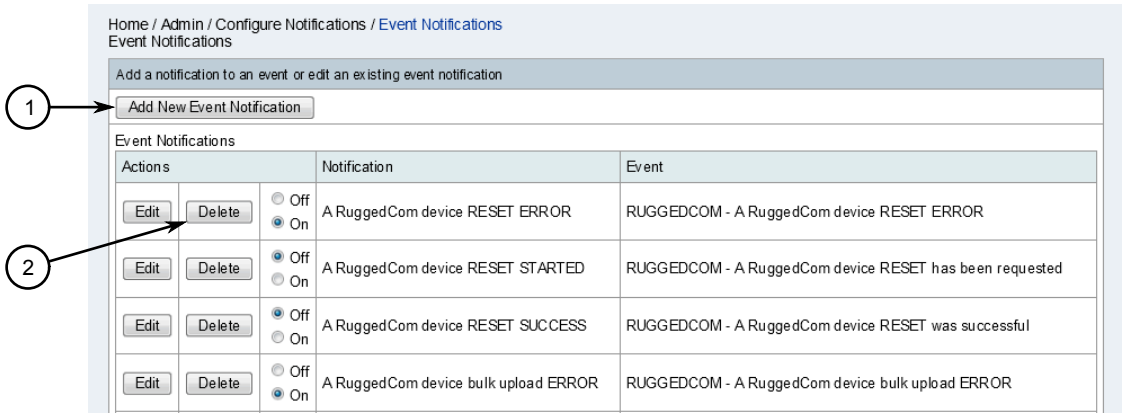


Figure 116: Event Notifications Screen

1. Add New Event Notification Button **2.** Delete Button

2. Click **Delete** next to the chosen notification. A confirmation message appears.
3. Click **OK** to delete the notification.

Section 5.2.5

Managing Outage Notifications

RUGGEDCOM NMS generates an outage notification whenever a network outage occurs.

CONTENTS

Section 5.2.5.1

Viewing a List of Outage Notifications

To view a list of all network outage notifications, do the following:

1. On the menu bar, click **Outages**. The **Outages** screen appears.

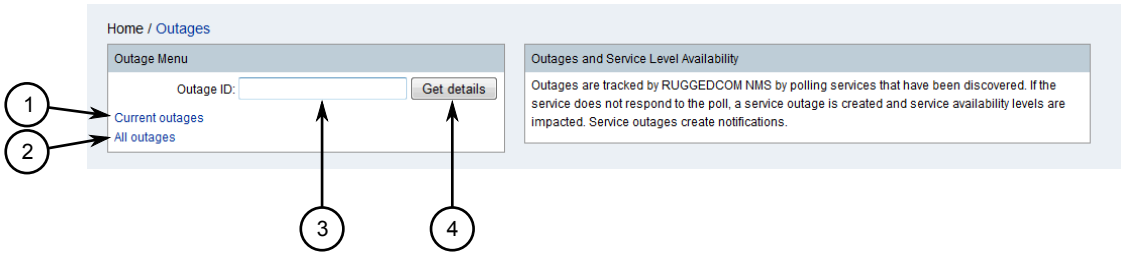
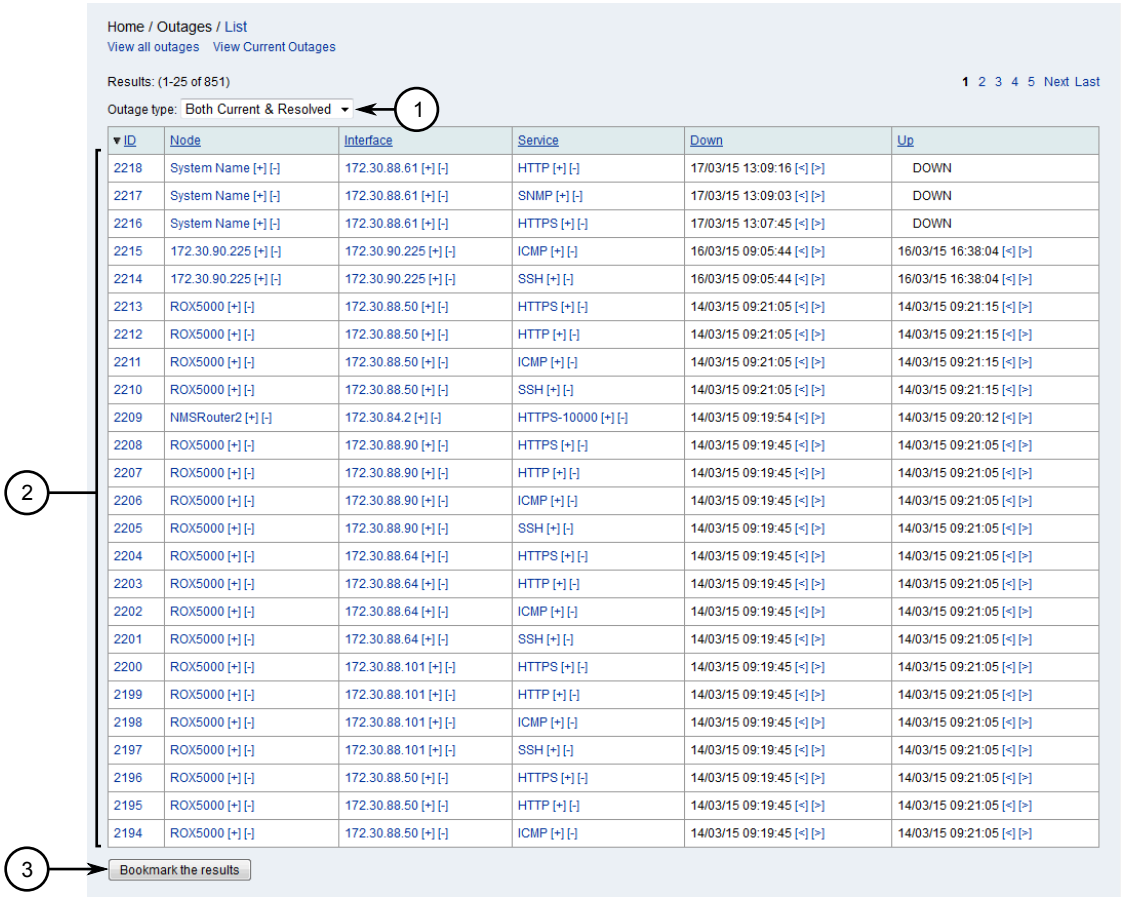


Figure 117: Outages Screen

1. Current Outages Link **2.** All Outages Links **3.** Outage ID Box **4.** Get Details Button

2. Click **All Outages**. The **List** screen appears listing all outage notifications, current and past.



ID	Node	Interface	Service	Down	Up
2218	System Name [+] [-]	172.30.88.61 [+] [-]	HTTP [+] [-]	17/03/15 13:09:16 [<] [>]	DOWN
2217	System Name [+] [-]	172.30.88.61 [+] [-]	SNMP [+] [-]	17/03/15 13:09:03 [<] [>]	DOWN
2216	System Name [+] [-]	172.30.88.61 [+] [-]	HTTPS [+] [-]	17/03/15 13:07:45 [<] [>]	DOWN
2215	172.30.90.225 [+] [-]	172.30.90.225 [+] [-]	ICMP [+] [-]	16/03/15 09:05:44 [<] [>]	16/03/15 16:38:04 [<] [>]
2214	172.30.90.225 [+] [-]	172.30.90.225 [+] [-]	SSH [+] [-]	16/03/15 09:05:44 [<] [>]	16/03/15 16:38:04 [<] [>]
2213	ROX5000 [+] [-]	172.30.88.50 [+] [-]	HTTPS [+] [-]	14/03/15 09:21:05 [<] [>]	14/03/15 09:21:15 [<] [>]
2212	ROX5000 [+] [-]	172.30.88.50 [+] [-]	HTTP [+] [-]	14/03/15 09:21:05 [<] [>]	14/03/15 09:21:15 [<] [>]
2211	ROX5000 [+] [-]	172.30.88.50 [+] [-]	ICMP [+] [-]	14/03/15 09:21:05 [<] [>]	14/03/15 09:21:15 [<] [>]
2210	ROX5000 [+] [-]	172.30.88.50 [+] [-]	SSH [+] [-]	14/03/15 09:21:05 [<] [>]	14/03/15 09:21:15 [<] [>]
2209	NMSRouter2 [+] [-]	172.30.84.2 [+] [-]	HTTPS-10000 [+] [-]	14/03/15 09:19:54 [<] [>]	14/03/15 09:20:12 [<] [>]
2208	ROX5000 [+] [-]	172.30.88.90 [+] [-]	HTTPS [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2207	ROX5000 [+] [-]	172.30.88.90 [+] [-]	HTTP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2206	ROX5000 [+] [-]	172.30.88.90 [+] [-]	ICMP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2205	ROX5000 [+] [-]	172.30.88.90 [+] [-]	SSH [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2204	ROX5000 [+] [-]	172.30.88.64 [+] [-]	HTTPS [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2203	ROX5000 [+] [-]	172.30.88.64 [+] [-]	HTTP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2202	ROX5000 [+] [-]	172.30.88.64 [+] [-]	ICMP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2201	ROX5000 [+] [-]	172.30.88.64 [+] [-]	SSH [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2200	ROX5000 [+] [-]	172.30.88.101 [+] [-]	HTTPS [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2199	ROX5000 [+] [-]	172.30.88.101 [+] [-]	HTTP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2198	ROX5000 [+] [-]	172.30.88.101 [+] [-]	ICMP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2197	ROX5000 [+] [-]	172.30.88.101 [+] [-]	SSH [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2196	ROX5000 [+] [-]	172.30.88.50 [+] [-]	HTTPS [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2195	ROX5000 [+] [-]	172.30.88.50 [+] [-]	HTTP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]
2194	ROX5000 [+] [-]	172.30.88.50 [+] [-]	ICMP [+] [-]	14/03/15 09:19:45 [<] [>]	14/03/15 09:21:05 [<] [>]

Figure 118: List Screen

1. Outage Type List **2.** Outages **3.** Bookmark the Results Button

3. [Optional] Under **Outage Type**, select the type of outages to view. Options include `Both Current & Resolved`, `Resolved` and `Current`.

4. [Optional] To create a bookmark, click **Bookmark the Results**. Use the bookmark to quickly access this view at any time.

To view only notifications for current network outages, do the following:

1. On the menu bar, click **Outages**. The **Outages** screen appears. Refer to Figure 117 .
2. Click **Current Outages**. The **Current By Node** screen appears listing only the current outage notifications. If there are no outages at the time, a message appears indicating that all services are up and running.

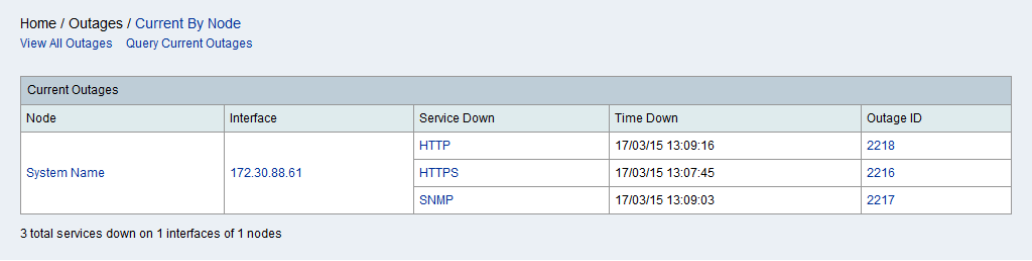


Figure 119: Current By Node Screen

Section 5.2.5.2
Viewing Outage Details

To view further details for any outage notification, do one of the following:

From Within a List of Outage Notifications

View the list of current and/or past outage notifications and click the ID for the desired notification. For more information about viewing a list of outage notifications, refer to Section 5.2.5.1, "Viewing a List of Outage Notifications" .

From the Outages Screen

1. On the menu bar, click **Outages**. The **Outages** screen appears.

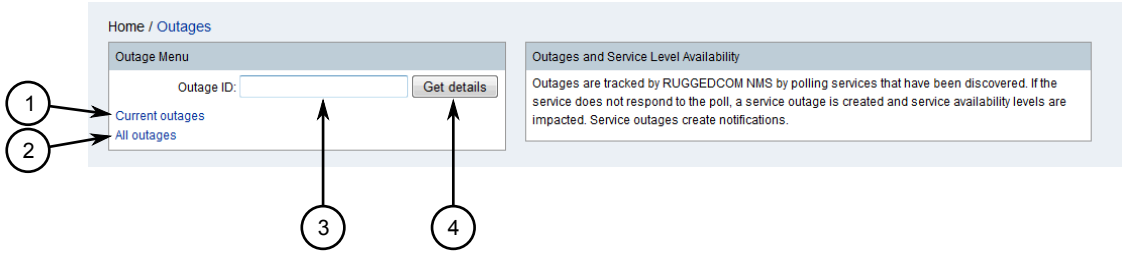


Figure 120: Outages Screen

1. Current Outages Link **2.** All Outages Links **3.** Outage ID Box **4.** Get Details Button

2. Under **Outage ID**, type the ID for the outage notification and then click **Get Details**. The **Detail** screen appears.

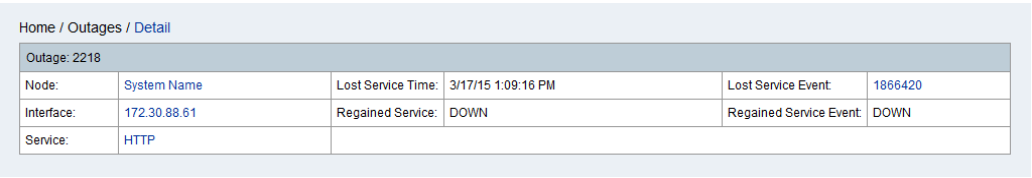


Figure 121: Detail Screen

Section 5.2.5.3
Filtering Outage Notifications

Each list of outage notifications features controls for removing or adding notifications for specific devices, interfaces or services. They can also be customized to only display outages that occurred before or after a specific date and time.

Filters are available in all cells, except those under the **ID** column.

Controls include the following:

Filter Control	Description
[+]	Only shows notifications that match the value in the current field. For example, clicking **[+]** in the **Node** column displays only notifications related to the selected node.
[-]	Hides notifications that match the value in the current field. For example, to exclude notifications related to a specific IP address, click **[-]** next to the desired IP address in the **Interface** column.
[<]	Only shows notifications that occurred after the selected outage. Only applicable to the time of the outage.
[>]	Only shows notifications that occurred before the selected outage. Only applicable to the time of the outage.

NOTE
For quick reference in the RUGGEDCOM NMS Web user interface, hover the mouse cursor over any filter control to view a tool tip describing its function.

Once a filter is applied, it appears above the table in the list of search constraints. A filter can be removed by clicking **[-]** next to it.

Section 5.2.6
Managing Destination Paths

Destination paths determine which user, group or role will receive specific notifications. If configured, the destination path can also escalate the notification to secondary user, group or role to prevent an outage from going unnoticed.

CONTENTS

Section 5.2.6.1
Viewing a List of Destination Paths

To view a list of destination paths, on the menu bar, click **Admin**, click **Configure Notifications**, and then click **Configure Destination Paths**. The **Destination Paths** screen appears.

Figure 122: Destination Paths Screen

Available destination paths are listed under **Existing Paths**. For more information about adding or editing a destination path, refer to Section 5.2.6.2, “Adding a Destination Path” .

Section 5.2.6.2
Adding a Destination Path

To add a new destination path, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications**, and then click **Configure Destination Paths**. The **Destination Paths** screen appears.

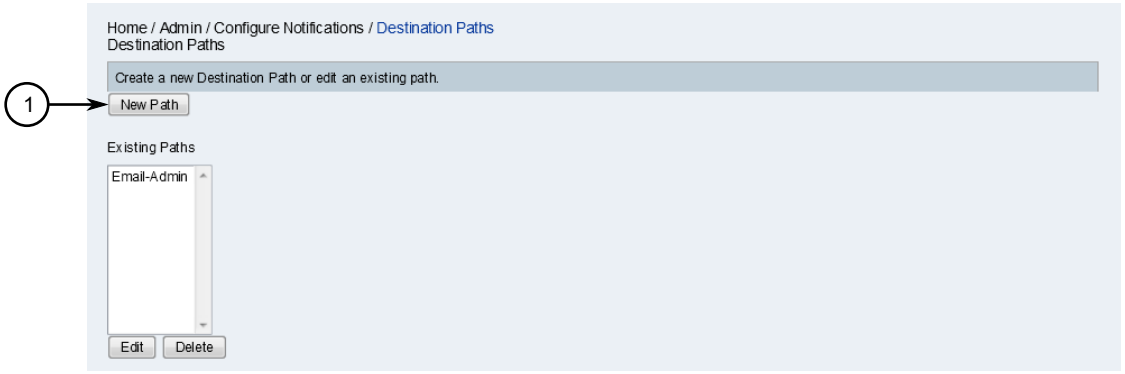


Figure 123: Destination Paths Screen

1. New Path Button

2. Click **New Path** to add a new destination Path. The **Path Outline** screen appears.

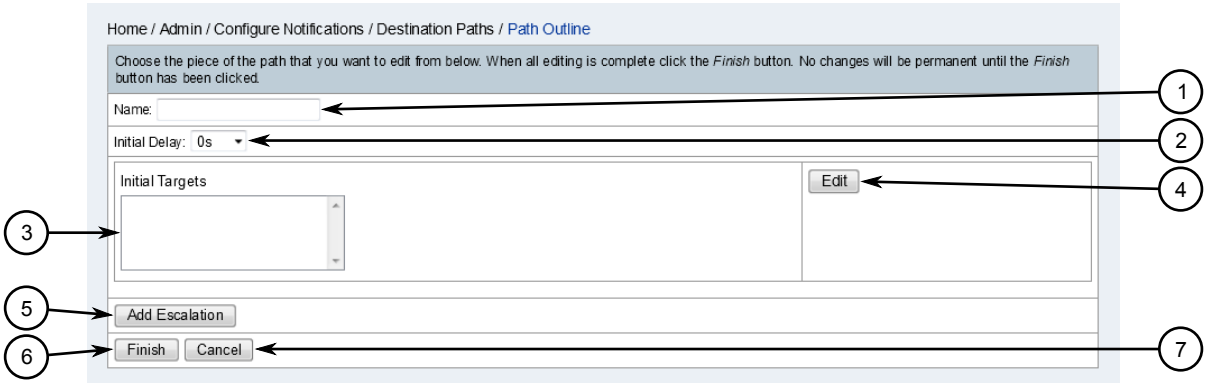


Figure 124: Path Outline Screen

1. Name Box **2.** Initial Delay List **3.** Initial Targets **4.** Edit Button **5.** Add Escalation Button **6.** Finish Button **7.** Cancel Button

3. Under **Name**, type a name for the new destination path.
4. [Optional] Under **Initial Delay**, select the desired delay period. Notifications will not be sent until the time period expires, allowing services the opportunity to restore.
5. Click **Edit** to define the initial/primary target for the notification. The **Choose Targets** screen appears.

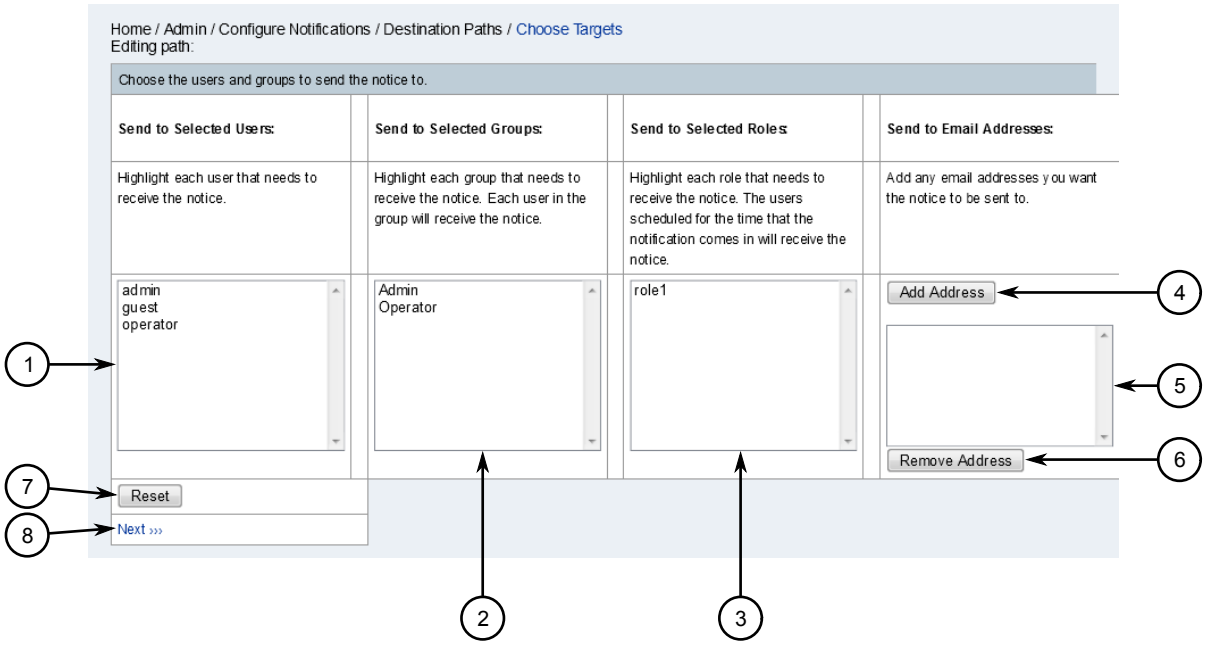


Figure 125: Choose Targets Screen

1. Available Users **2.** Available Groups **3.** Available Roles **4.** Add Address Button **5.** Available E-Mail Addresses **6.** Remove Address Button **7.** Reset Button **8.** Next Link

6. Select the users, groups, roles or e-mail addresses who should receive the initial notifications. For more information, refer to:
   - Step 4 to Step 7 in Section 5.2.6.3, "Editing a Destination Path to Users or Roles"
   - Step 4 to Step 6 in Section 5.2.6.4, "Editing a Destination Path to a Group"
   - Step 6 to Step 8 in Section 5.2.6.5, "Editing a Destination Path to an E-Mail Address"
7. Click **Add Escalation** to add an escalation path should the initial notification not be acknowledged by the recipient(s). The **Choose Targets** screen appears. Refer to Figure 125 .
8. Repeat Step 6 .
9. Repeat Step 7 to Step 8 to add additional escalation paths.
10. [Optional] For each escalation path, under **Delay**, select the desired delay period. This allows the users on that path time to acknowledge and address the notification before the notification is sent on the next escalation path.
11. Click **Finish**.

Section 5.2.6.3
Editing a Destination Path to Users or Roles

To edit a destination path to one or more users or roles, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications**, and then click **Configure Destination Paths**. The **Destination Paths** screen appears.

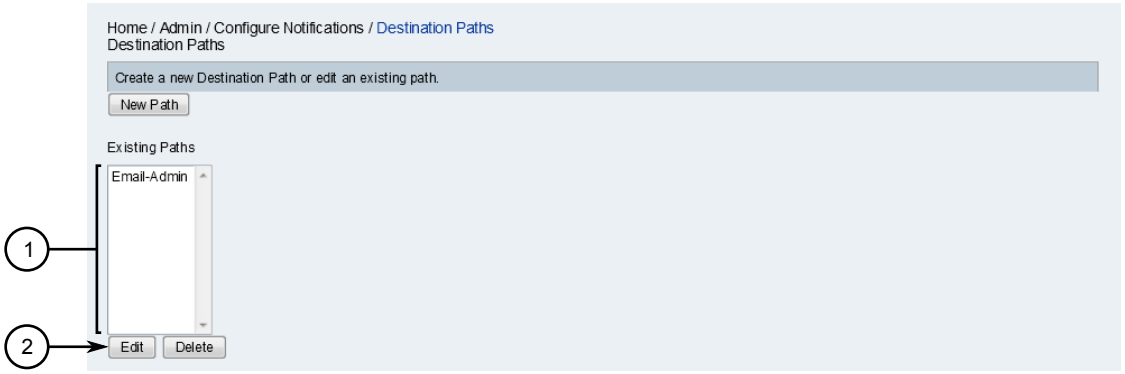


Figure 126: Event Notifications Screen

1. Existing Paths List **2.** Edit Button

2. Select a path from the **Existing Paths** list and then click **Edit**. The **Path Outline** screen appears.

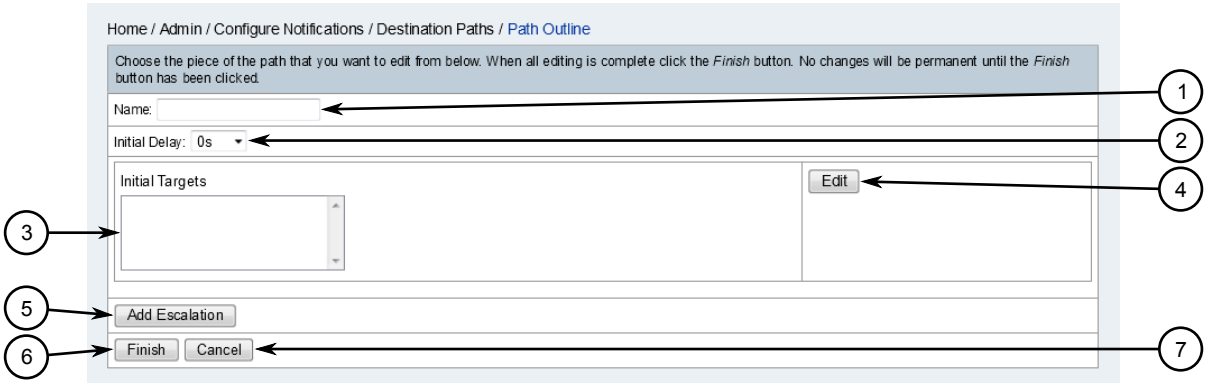


Figure 127: Path Outline Screen

1. Name Box **2.** Initial Delay List **3.** Initial Targets **4.** Edit Button **5.** Add Escalation Button **6.** Finish Button **7.** Cancel Button

3. Click **Edit**. The **Choose Targets** screen appears.

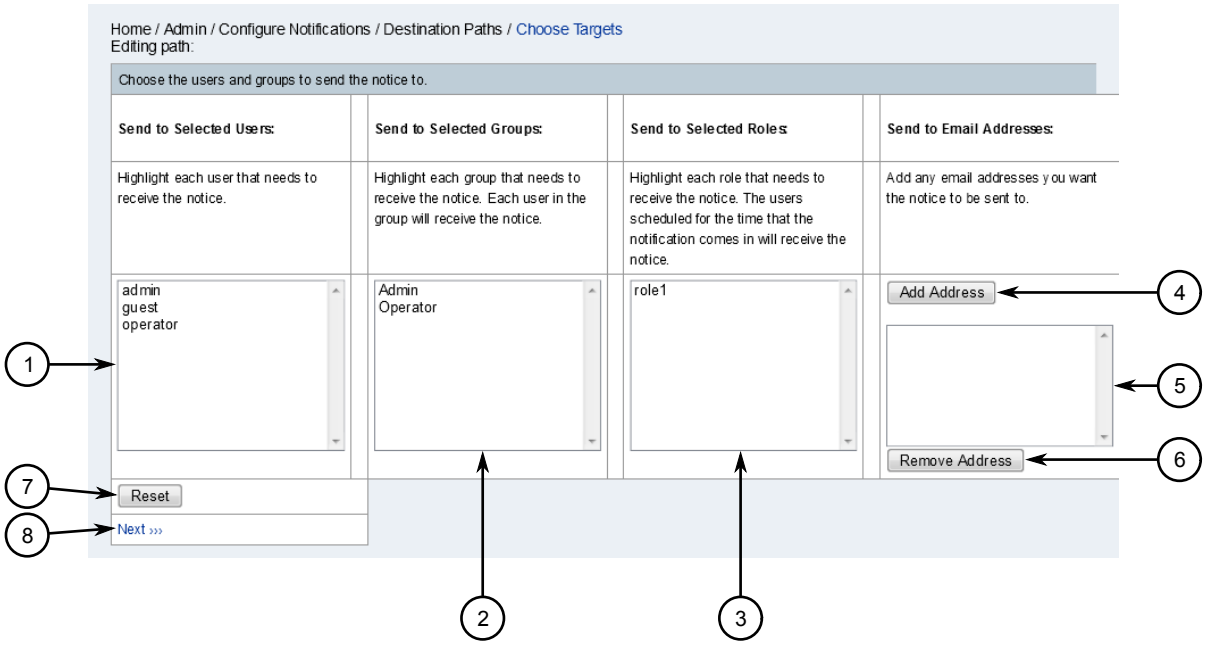


Figure 128: Choose Targets Screen

1. Available Users **2.** Available Groups **3.** Available Roles **4.** Add Address Button **5.** Available E-Mail Addresses **6.** Remove Address Button **7.** Reset Button **8.** Next Link

NOTE

*To select consecutive users/roles, click the first user/role, then hold **Shift** and click the last user/role. To select specific users/roles, click the first user/role, and then hold **Ctrl** and select other users/roles from the list.*

4. Select one or more users/roles, and then click **Next**. The **Choose Commands** screen appears.

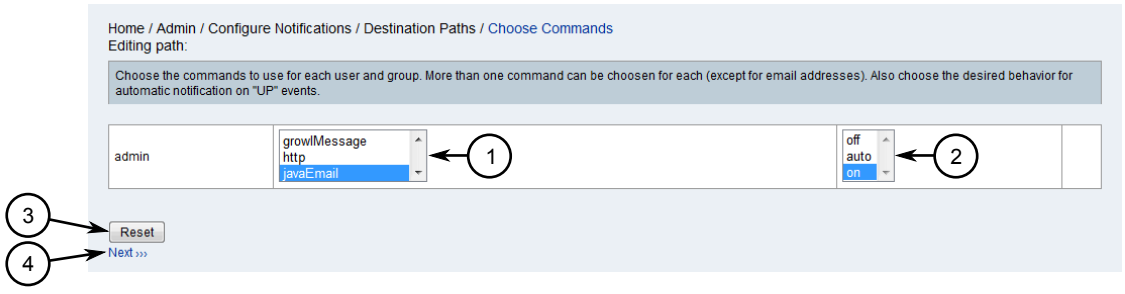


Figure 129: Choose Commands Screen

1. Available Commands **2.** Available Behaviors **3.** Reset Button **4.** Next Link

NOTE
*To select consecutive commands, click the first command, then hold **Shift** and click the last command. To select specific commands, click the first command, and then hold **Ctrl** and select other commands from the list.*

5. Select one or more notification methods to use from the list of available commands. Options include:
   - `email` – Sends notifications to the defined e-mail address
   - `growlMesage` – Sends notifications in Growl format for Mac OS X
   - `http` – Sends notifications as SNMP traps
   - `javaEmail` – Sends notifications to the defined e-mail address
   - `javaPagerEmail` – Sends notifications to the defined pager e-mail
   - `numericPage` – Sends the defined phone number to a pager
   - `pagerEmail` – Sends notifications to the defined pager e-mail address
   - `snmpTrap` – Sends notifications as SNMP traps
   - `syslog` – Logs notifications in the RUGGEDCOM NMS server system log
   - `textPage` – Sends the notification to a pager
   - `xmppGroupMessage` – Sends group xmppMessage notifications to an external jabber (XMPP) server
   - `xmppMessage` – Sends xmppMessage notifications to an external jabber (XMPP) server
6. Select a behavior to perform when an event occurs:
   - `On` – Notifications are sent to the users/roles on the path
   - `Off` – Notifications are *not* sent to the users/roles on the path
   - `Auto` – Notifications are automatically acknowledged
7. Click **Next**. The **Path Outline** screen appears (refer to Figure 127), now with the select users/roles listed in the **Initial Targets** list.
8. Click **Finish**.

Section 5.2.6.4
Editing a Destination Path to a Group

To edit a destination path to one or more groups, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications**, and then click **Configure Destination Paths**. The **Destination Paths** screen appears.

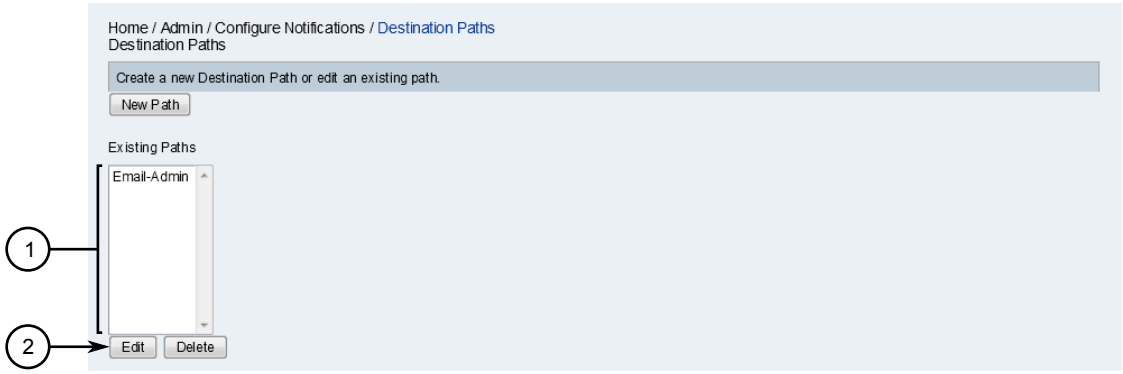


Figure 130: Event Notifications Screen

1. Existing Paths List **2.** Edit Button

2. Select a path from the **Existing Paths** list and then click **Edit**. The **Path Outline** screen appears.

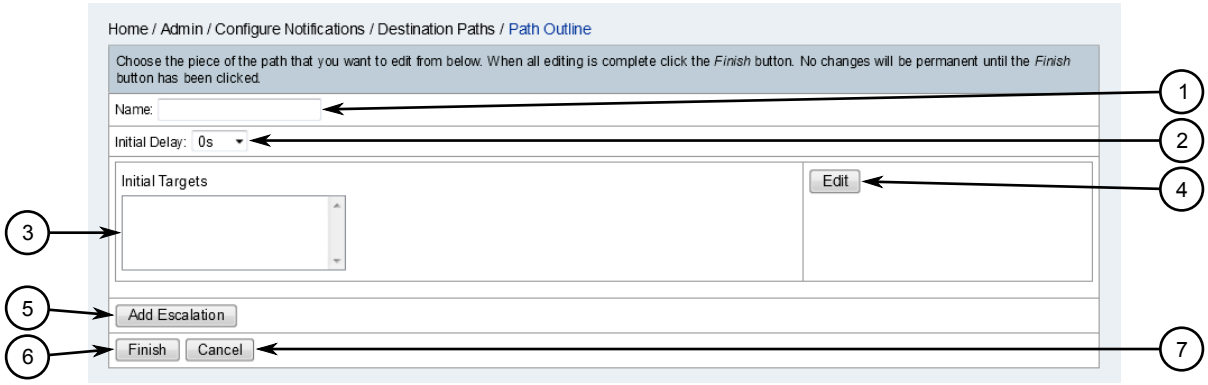


Figure 131: Path Outline Screen

1. Name Box **2.** Initial Delay List **3.** Initial Targets **4.** Edit Button **5.** Add Escalation Button **6.** Finish Button **7.** Cancel Button

3. Click **Edit**. The **Choose Targets** screen appears.

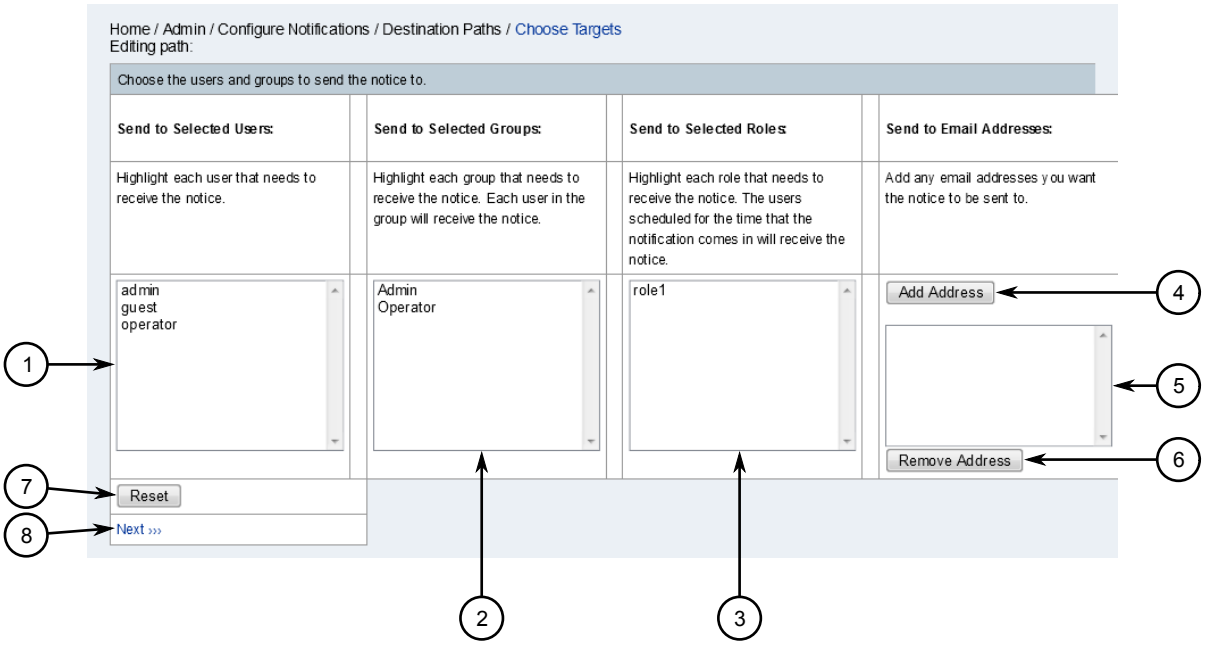


Figure 132: Choose Targets Screen

1. Available Users **2.** Available Groups **3.** Available Roles **4.** Add Address Button **5.** Available E-Mail Addresses **6.** Remove Address Button **7.** Reset Button **8.** Next Link

NOTE
*To select consecutive groups, click the first group, then hold **Shift** and click the last group. To select specific groups, click the first group, and then hold **Ctrl** and select other groups from the list.*

4. Select one or more groups, and then click **Next**. The **Group Intervals** screen appears.

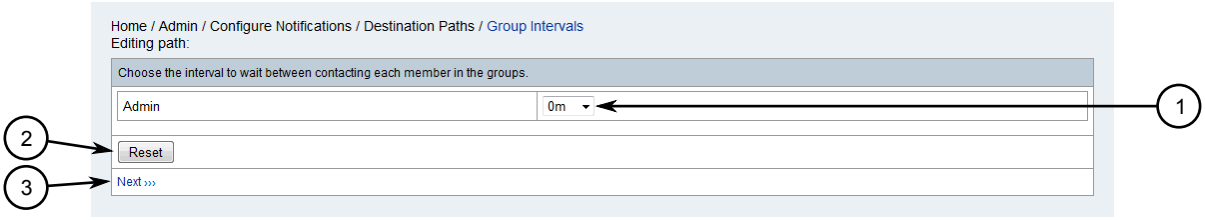


Figure 133: Group Intervals Screen

1. Interval List **2.** Reset Button **3.** Next Link

5. Select an interval from the list. This represents the amount of time RUGGEDCOM NMS will wait before contacting each group member.
6. Click **Next**. The **Path Outline** screen appears (refer to Figure 131), now with the select groups listed in the **Initial Targets** list.
7. Click **Finish**.

Section 5.2.6.5
Editing a Destination Path to an E-Mail Address

To edit a destination path to a specific e-mail address, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications**, and then click **Configure Destination Paths**. The **Destination Paths** screen appears.

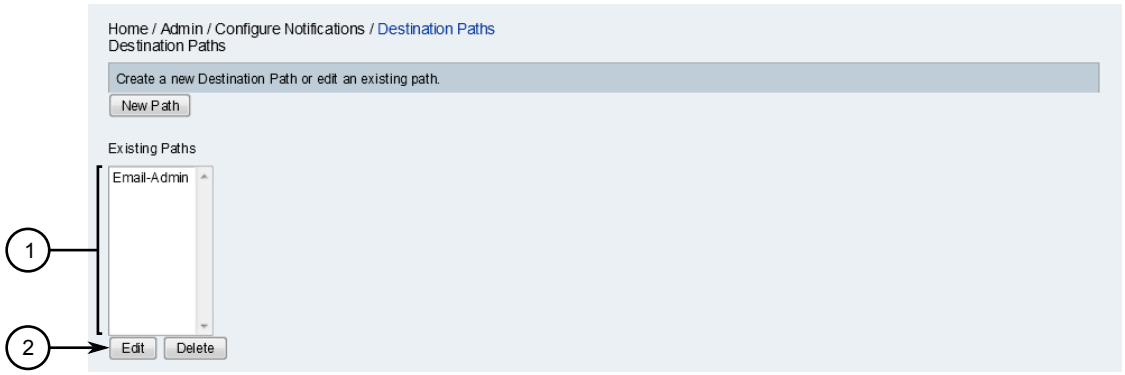


Figure 134: Event Notifications Screen

1. Existing Paths List **2.** Edit Button

2. Select a path from the **Existing Paths** list and then click **Edit**. The **Path Outline** screen appears.

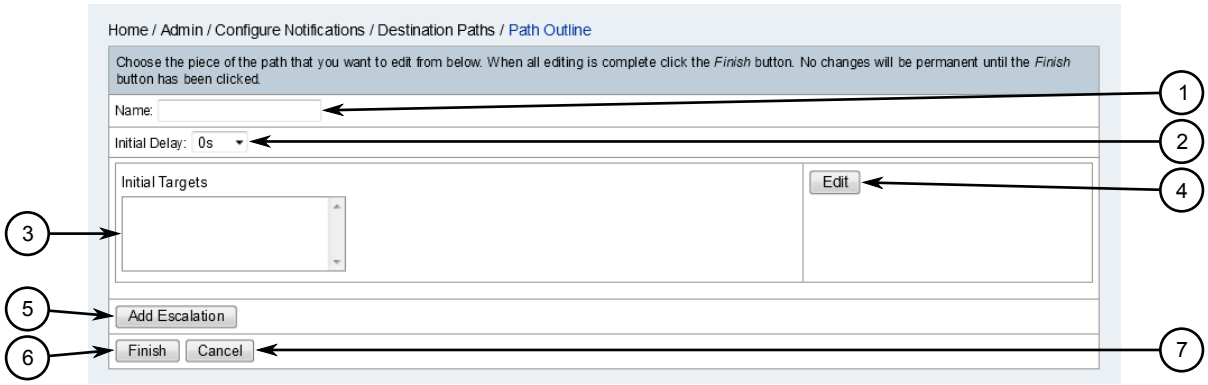


Figure 135: Path Outline Screen

1. Name Box **2.** Initial Delay List **3.** Initial Targets **4.** Edit Button **5.** Add Escalation Button **6.** Finish Button **7.** Cancel Button

3. Click **Edit**. The **Choose Targets** screen appears.

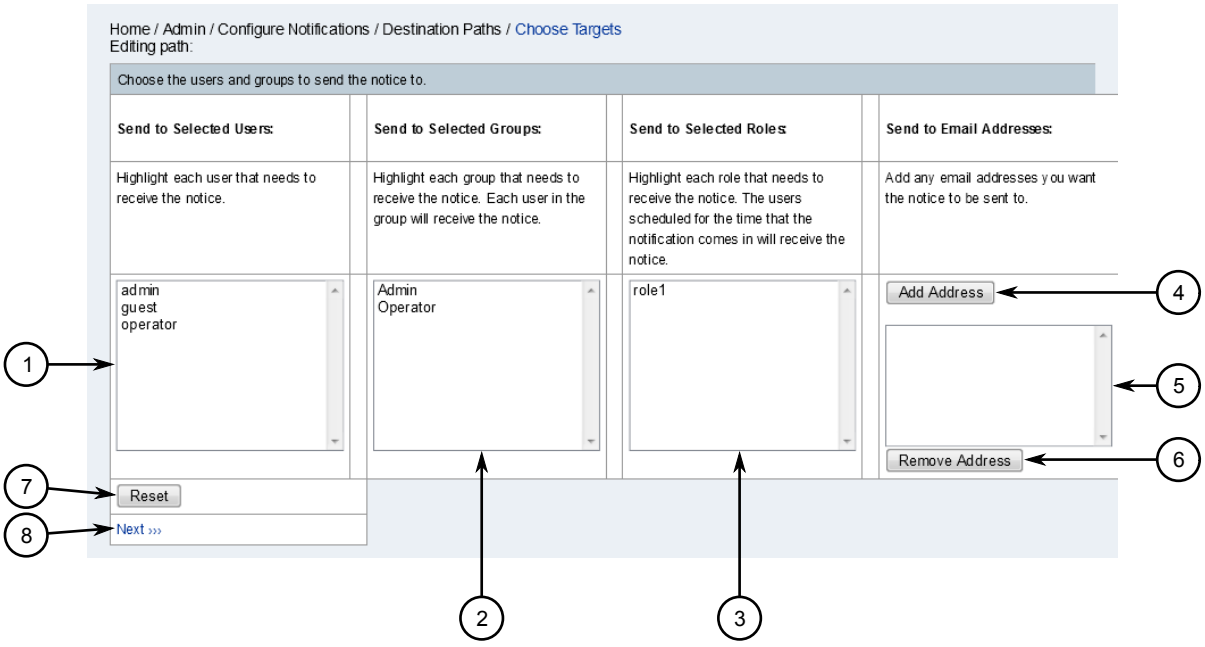


Figure 136: Choose Targets Screen

1. Available Users **2.** Available Groups **3.** Available Roles **4.** Add Address Button **5.** Available E-Mail Addresses **6.** Remove Address Button **7.** Reset Button **8.** Next Link

4. Click **Add Address**. A dialog box appears.

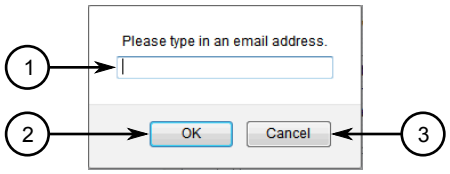


Figure 137: Add Address Dialog Box

1. ? Box **2.** OK Button **3.** Cancel Button

5. Type an e-mail address and then click **OK**.
6. Click **Next**. The **Choose Commands** screen appears.

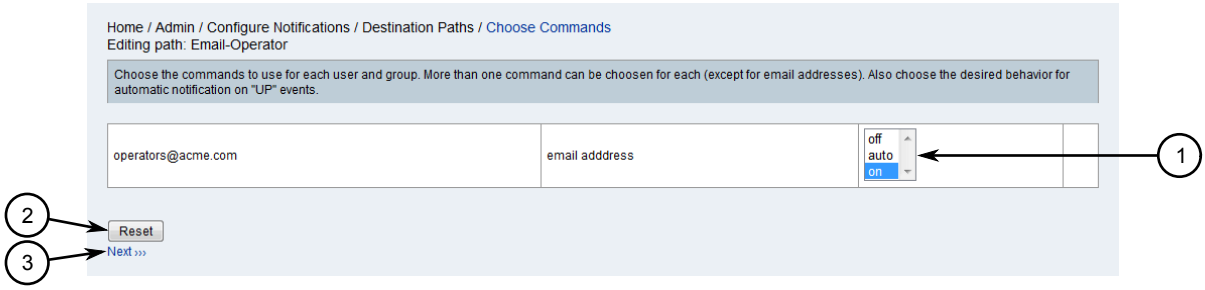


Figure 138: Choose Commands Screen

1. Available Behaviors **2.** Reset Button **3.** Next Link

7. Select a behavior to perform when an event occurs:
   - `On` – Notifications are sent to the e-mail address on the path
   - `Off` – Notifications are *not* sent to the e-mail address on the path
   - `Auto` – Notifications are automatically acknowledged
8. Click **Next**. The **Path Outline** screen appears (refer to Figure 135), now with the select users/roles listed in the **Initial Targets** list.
9. Click **Finish**.

Section 5.2.6.6

Deleting a Destination Path

To delete a destination path, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications**, and then click **Configure Destination Paths**. The **Destination Paths** screen appears.

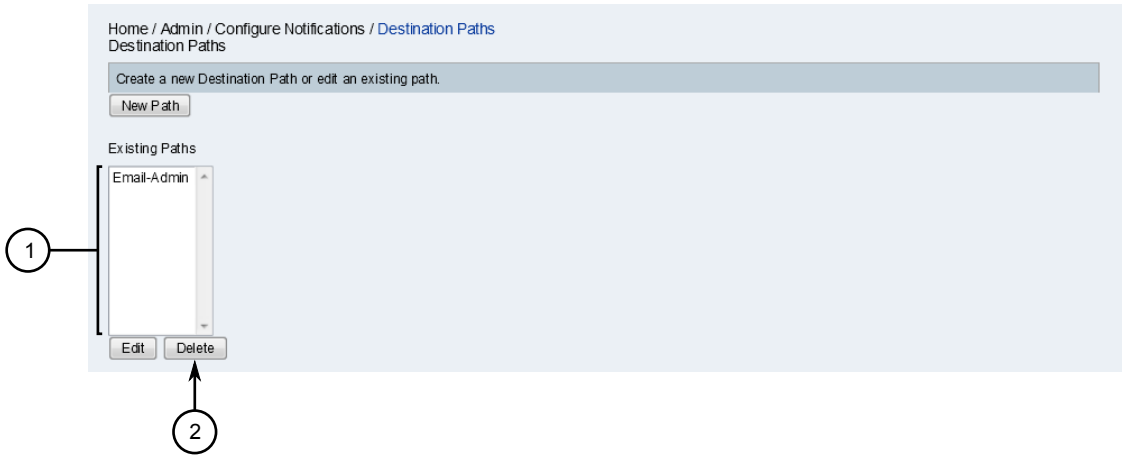


Figure 139: Event Notifications Screen

1. Available Destination Paths **2.** Delete Button

2. Select a destination path from the list and click **Delete**. A confirmation message appears.
3. Click **OK** to delete the notification.

Section 5.2.7
Managing Path Outages

Path outages suppress unwanted notifications from nodes in a group that appear to RUGGEDCOM NMS to be down, when in fact it is the primary node that services the group that is down. In cases such as this, only the notification that the primary node is down is required.

Path outages are defined by a critical path (i.e. an IP address and service pair) that tests a specified primary node when a node from its group is down. If no response is received from the primary node, all notifications from the nodes it services are automatically suppressed.

In addition to the critical path, a rule (typically an IPADDR IPLIKE rule) can also be configured to search for other primary nodes that should be tested.

CONTENTS

Section 5.2.7.1
Viewing a List of Path Outages

To view a list of path outages configured for RUGGEDCOM NMS, click **Path Outages** on the menu bar. The **Path Outages** screen appears.

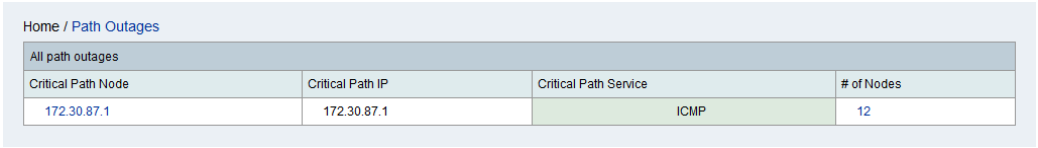


Figure 140: Path Outages Screen

This screen details the critical path node, IP address, service (ICMP), and the number of nodes discovered under the critical path.

For information about changing the critical path and/or expanding the rule to include other nodes in the path, refer to Section 5.2.7.2, "Configuring a Path Outage" .

Section 5.2.7.2
Configuring a Path Outage

To define a path outage, do the following:

1. On the menu bar, click **Admin**, click **Configure Notifications**, and then click **Configure Path Outages**. The **Configure Path Outages** screen appears.

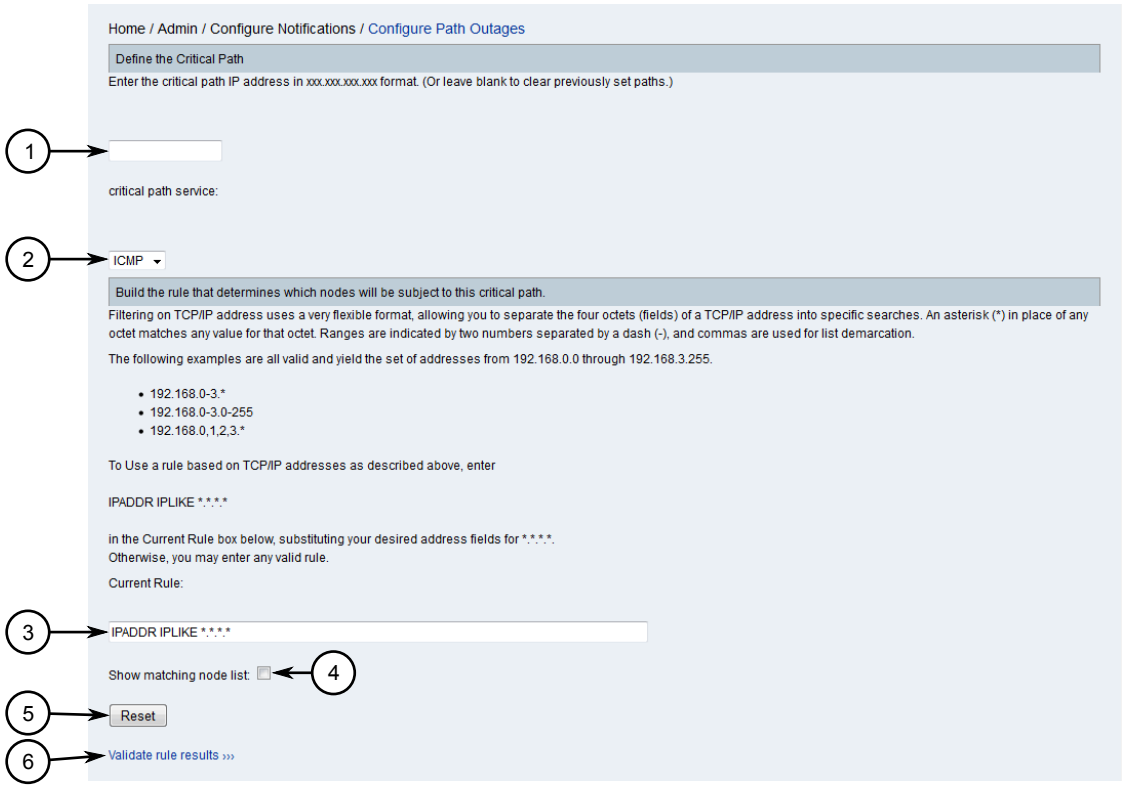


Figure 141: Configure Path Outages Screen

1. IP Address Box **2.** Critical Path Service List **3.** Current Rule Box **4.** Show Matching Node List Check Box **5.** Reset Button **6.** Validate Rule Results Link

2. In the first box, type the IP address for the primary node that services the target group, or leave it blank to clear a previously configured critical path.
3. [Optional] Under **Current Rule**, define a build rule that looks for the chosen node on one or more interfaces.

   RUGGEDCOM NMS uses the Iplike search format, which allows users to search for interfaces based on any one of the four octets (fields). An asterisk (*) in place of an octet matches any value for that octet. A range (e.g. 0-3, 0-255, etc.) in place of an octet matches any value for that octet that falls within in the specified range. A comma (,) creates a demarcated list (e.g. 0,1,2,3).

   For example, each of the following rules will find interfaces with IP address between 192.168.0.0 and 192.168.3.255:

   ```
   IPADDR IPLIKE 192.168.0-3.*
   IPADDR IPLIKE 192.168.0-3.0-255
   IPADDR IPLIKE 192.168.0,1,2,3.*
   ```

4. [Optional] Click **Show Matching Node List**. During validation, a list of nodes matching the rule will be shown.

5. [Optional] If necessary, click **Reset** to reset the build rule and repeat Step 3 .
6. Click **Validate Rule Results** to test the build rule. The **Validate Rule** screen appears.

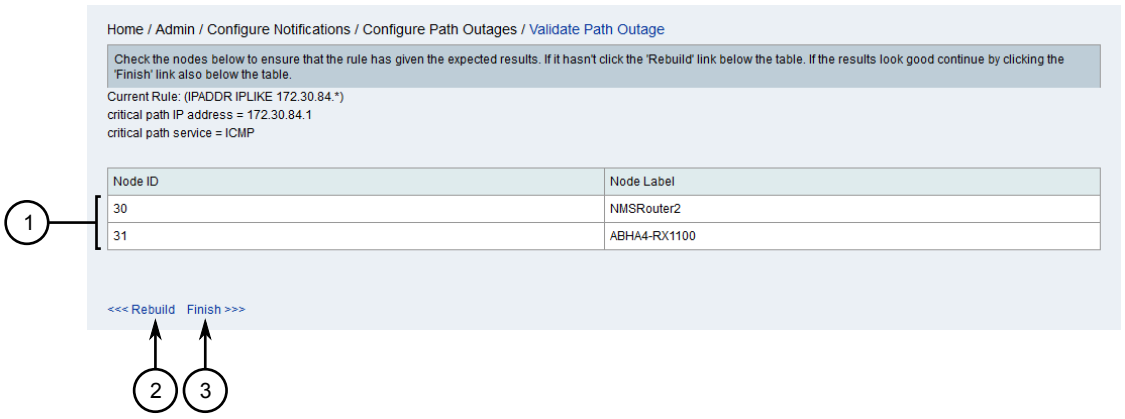


Figure 142: Validate Rule Screen

1. List of Matching Nodes **2.** Rebuild Link **3.** Next Link

Review the list of IP addresses to make sure the build rule provides the expected results. If the expected IP addresses are missing from the list, click **Rebuild** and repeat Step 3 to Step 6 .

IMPORTANT!
If a critical path was not defined, any critical path that was configured previously will be erased.

7. Click **Finish**. The new path outage appears on the **Path Outages** screen. For more information about viewing the **Path Outages** screen, refer to Section 5.2.7.1, "Viewing a List of Path Outages" .

Section 5.2.7.3
Configuring a Critical Path for a Device

To configure a critical path for a specific device, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. From the **Node** screen, click **Admin** and then click **Configure Path Outage**. The **Configure Path Outage** screen appears.

Figure 143: Configure Path Outage Screen

1. IP Address Box **2.** Submit Button **3.** Cancel Button **4.** Delete Button

3. In the first box, type the IP address for the primary node that services the device.
4. Click **Submit**.

Section 5.2.7.4

Deleting a Critical Path for a Device

The delete a critical path configured for a specific device, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, “Viewing Device Details” .
2. From the **Node** screen, click **Admin** and then click **Configure Path Outage**. The **Configure Path Outage** screen appears.

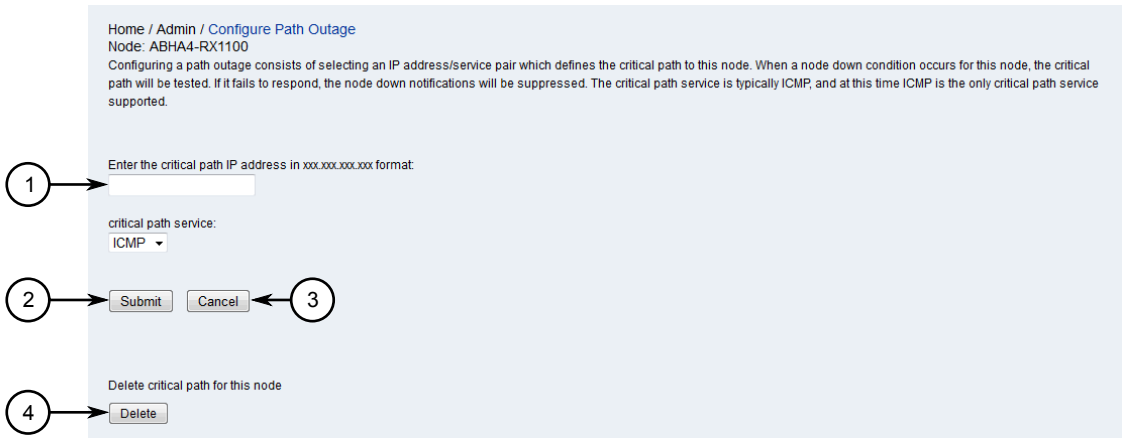


Figure 144: Configure Path Outage Screen

1. IP Address Box **2.** Submit Button **3.** Cancel Button **4.** Delete Button

3. Click **Delete**. A confirmation message appears.
4. Click **OK**.

Section 5.3
Managing Scheduled Outages

When one or more devices managed by RUGGEDCOM NMS are scheduled to be unavailable for a period of time, schedule an outage within RUGGEDCOM NMS to control how the device is managed. In some instances, for example, it may be desirable to continue polling a device, but not monitor thresholding.

CONTENTS

Section 5.3.1
Viewing a List of Scheduled Outages

To view a list of scheduled outages, on the menu bar, click **Admin** and then click **Schedule Outages**. The **Scheduled Outages** screen appears.

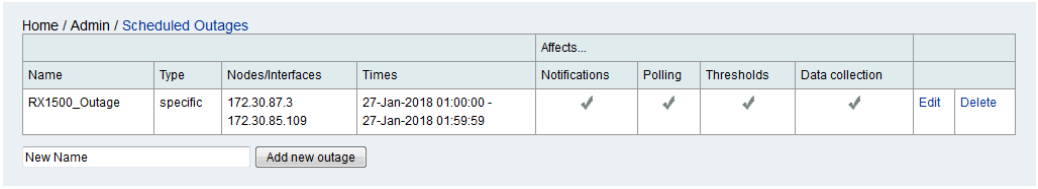


Figure 145: Scheduled Outages Screen

For information about adding, editing or deleting a scheduled outage, refer to Section 5.3.2, "Scheduling an Outage", Section 5.3.3, "Editing a Scheduled Outage" or Section 5.3.4, "Deleting a Scheduled Outage".

Section 5.3.2
Scheduling an Outage

To schedule an outage for one or more devices managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin** and then click **Schedule Outages**. The **Scheduled Outages** screen appears.

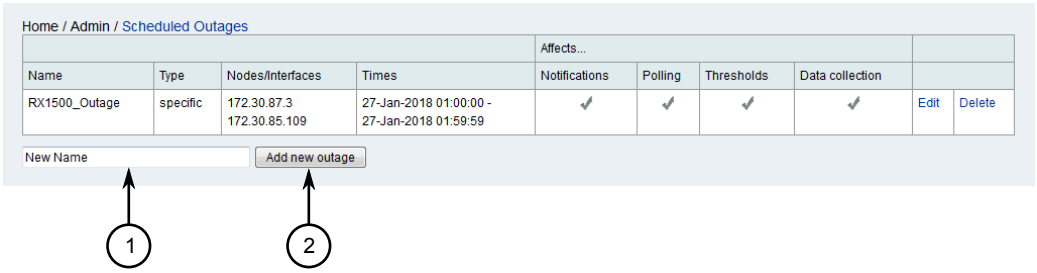


Figure 146: Scheduled Outages Screen

1. Add New Outage Box **2.** Add New Outage Button

2. In the **Add New Outage** box, type the name of the new scheduled outage and then click **Add New Outage**. The **Edit** screen appears.

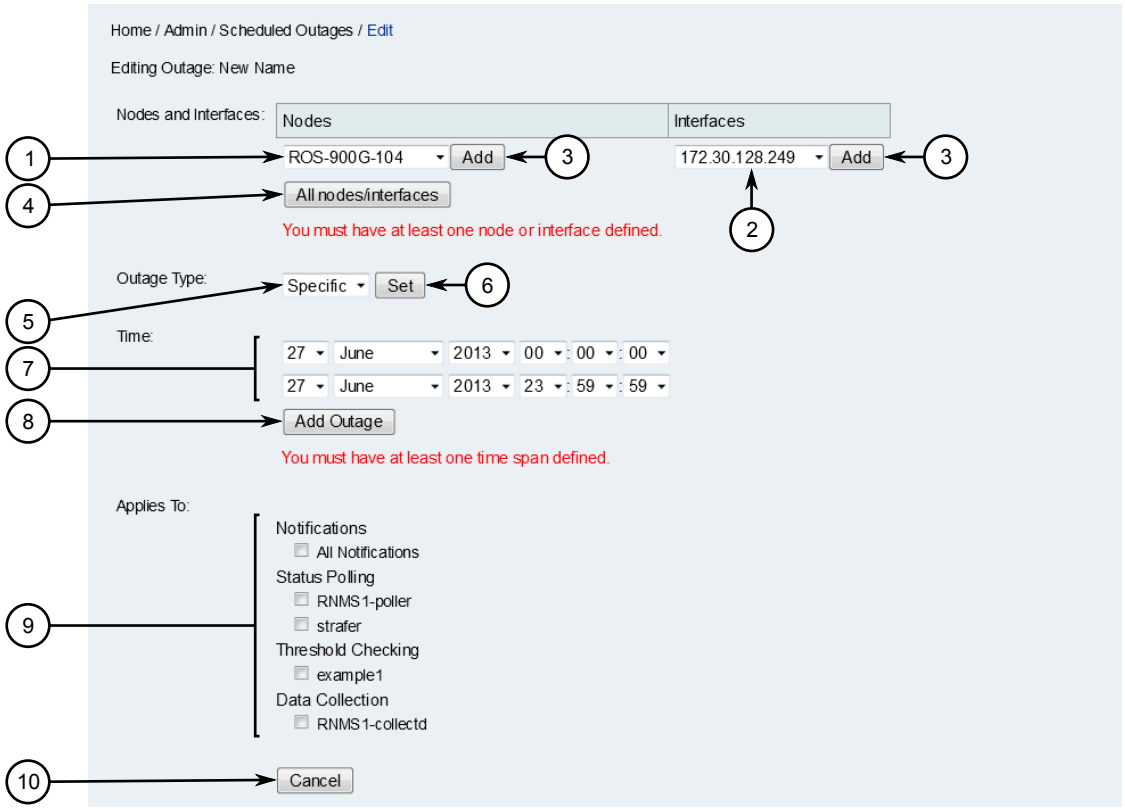


Figure 147: Edit Screen

1. Nodes List **2.** Interfaces List **3.** Add Button **4.** All Nodes/Interfaces Button **5.** Type List **6.** Set Button **7.** Time Boxes **8.** Add Outage Button **9.** Action Options **10.** Cancel Button

3. Under **Nodes and Interfaces**, click **All Nodes/Interfaces** or select specific nodes or interfaces and click the associated **Add** buttons.

4. Under **Outage Type**, select the outage type and click **Set**. The outage type specifies whether the outage occurs on a regular basis or only on a specific date. Options include `daily`, `weekly`, `monthly` and `specific`.
5. Under **Time**, configure the start and end time for the outage and then click **Add**. Repeat this step to add different outage periods for the selected node(s) and/or interface(s).
6. Under **Applies to**, select the features that should be disabled for the selected node(s) and/or interface(s) during the outage. For example, to prevent notifications from being generated, select **All Notifications**.

> **NOTE**
> *The **Save** button appears once all requirements are met.*

7. Click **Save**.

Section 5.3.3
Editing a Scheduled Outage

To edit a scheduled outage, do the following:

1. On the menu bar, click **Admin** and then click **Schedule Outages**. The **Scheduled Outages** screen appears.

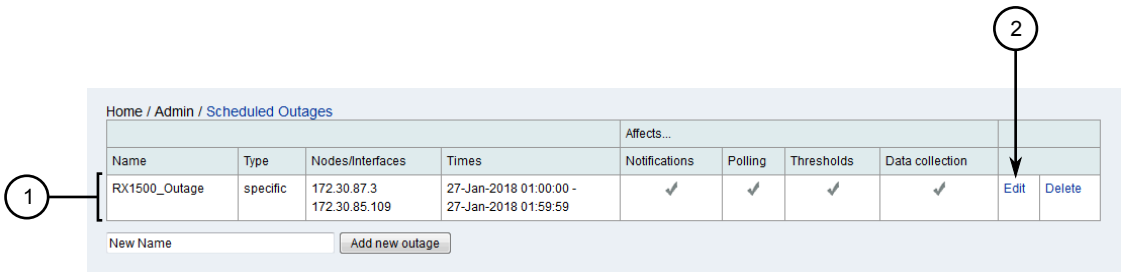


Figure 148: Scheduled Outages Screen

1. Scheduled Outages **2.** Edit Link

2. Click **Edit** next to the chosen scheduled outage. The **Edit** screen appears.

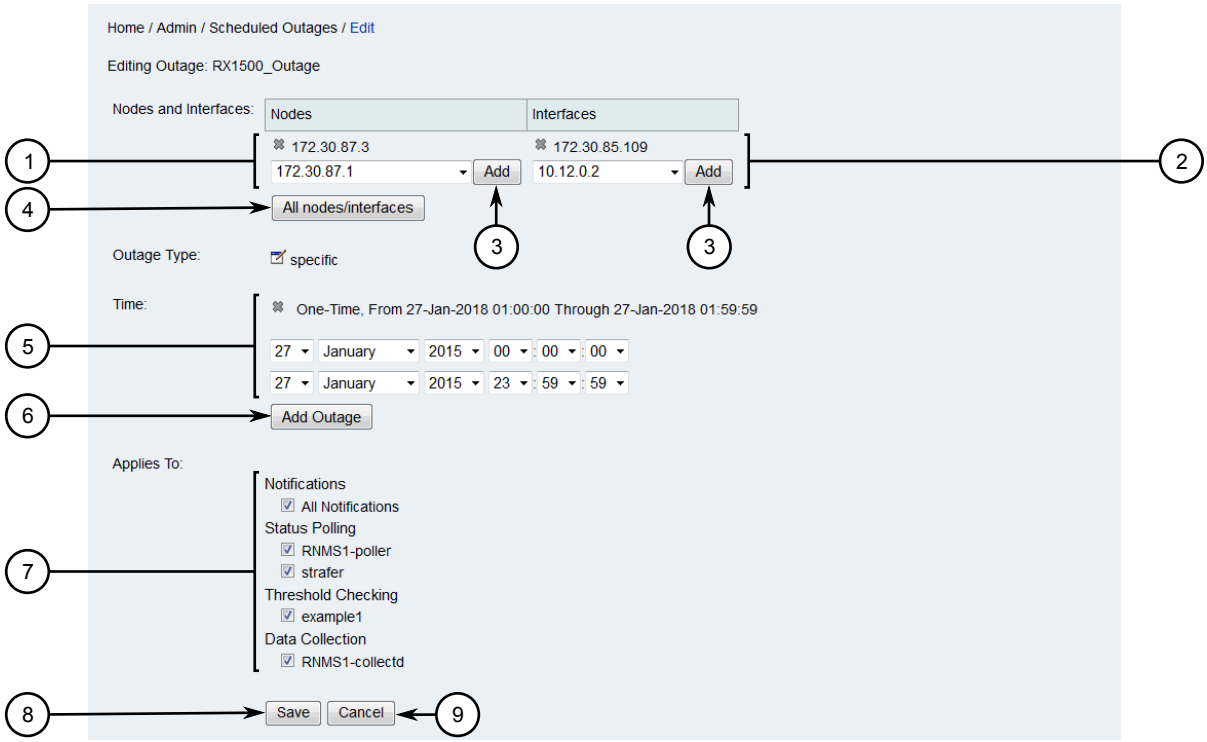


Figure 149: Edit Screen

1. Nodes List **2.** Interfaces List **3.** Add Button **4.** All Nodes/Interfaces Button **5.** Time Boxes **6.** Add Outage Button **7.** Action Options **8.** Save Button **9.** Cancel Button

3. [Optional] Under **Nodes and Interfaces**, add or remove nodes/interfaces as required.
   - Add nodes/interfaces by either clicking **All Nodes/Interfaces** or select specific nodes or interfaces and click the associated **Add** buttons.
   - Delete a node or interface by clicking the **×** symbol next to it.
4. [Optional] Under **Outage Type**, click the **Modify** icon, select a different outage type, and then click **Set**. The outage type specifies whether the outage occurs on a regular basis or only on a specific date. Options include `daily`, `weekly`, `monthly` and `specific`.
5. [Optional] Under **Time**, add or remove outage periods.
   - Add an outage period by configuring the start and end time for the outage and then clicking **Add**. Repeat this step to add different outage periods for the selected node(s) and/or interface(s).
   - Delete an outage period by clicking the **×** symbol next to it.
6. [Optional] Under **Applies to**, select the features that should be disabled for the selected node(s) and/or interface(s) during the outage. For example, to prevent notifications from being generated, select **All Notifications**.
7. Click **Save**.

Section 5.3.4
Deleting a Scheduled Outage

To delete a scheduled outage, do the following:

1. On the menu bar, click **Admin** and then click **Schedule Outages**. The **Scheduled Outages** screen appears.

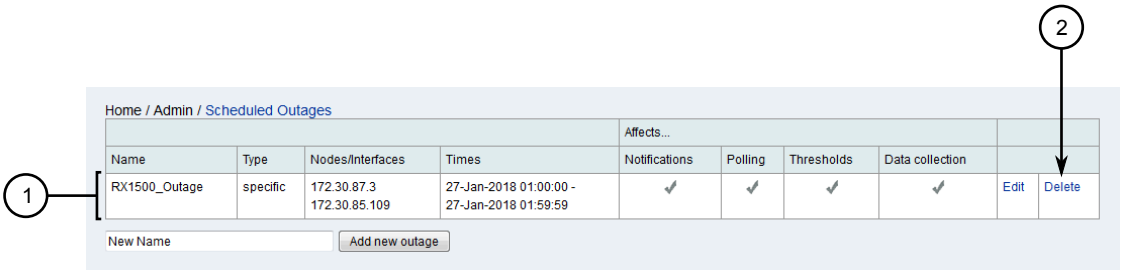


Figure 150: Scheduled Outages Screen

1. Scheduled Outages **2.** Delete Link

2. Click **Delete** next to the chosen scheduled outage. A confirmation message appears.
3. Click **OK** to delete the scheduled outage.

Section 5.4
Managing Performance Reports

Four types of reports can be generated from RUGGEDCOM NMS to outline the current and historical health of the network. Performance reports provide the tools needed to pro-actively detect issues and correct them before an outage or unacceptable network latency occurs.

CONTENTS

Section 5.4.1
Generating an Availability Report

An availability report details the availability of devices, services or connectivity.

To generate an availability report, do the following:

1. Make sure an e-mail is configured for the user. The availability report will be e-mailed to the user when it is ready. For more information about setting an e-mail for a user, refer to Section 4.8.1.2, "Editing a User" .
2. On the menu bar, click **Reports** and then click **Availability**. The **Availability** screen appears.

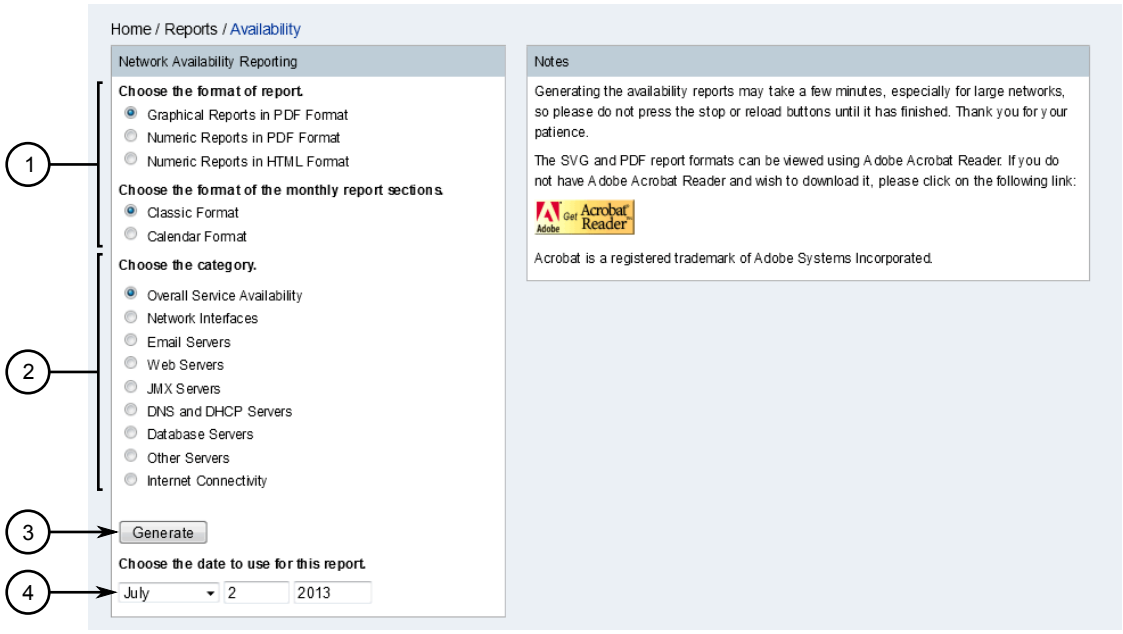


Figure 151: Availability Screen

1. Format Options **2.** Category Options **3.** Generate Button **4.** Date Boxes

3. Under **Choose the format of report**, select the output format.
4. Under **Choose the format of the monthly report sections**, select the style for the report.
5. Under **Choose the category**, select a category.
6. [Optional] Change the date that is displayed on the report.
7. Click **Generate**. The availability report is generated and e-mailed to the user.

Section 5.4.2

Managing Resource Performance Reports

Resource performance reports present SNMP data in a graphical format. Users can generate standard reports or create their own custom reports.

CONTENTS

Section 5.4.2.1

Generating Standard Reports

A standard resource performance report details stock reports based on node-oriented SNMP data.

To generate a standard report, do the following:

1. On the menu bar, click **Reports** and then click **Resource Graphs**. The **Resource Graphs** screen appears.

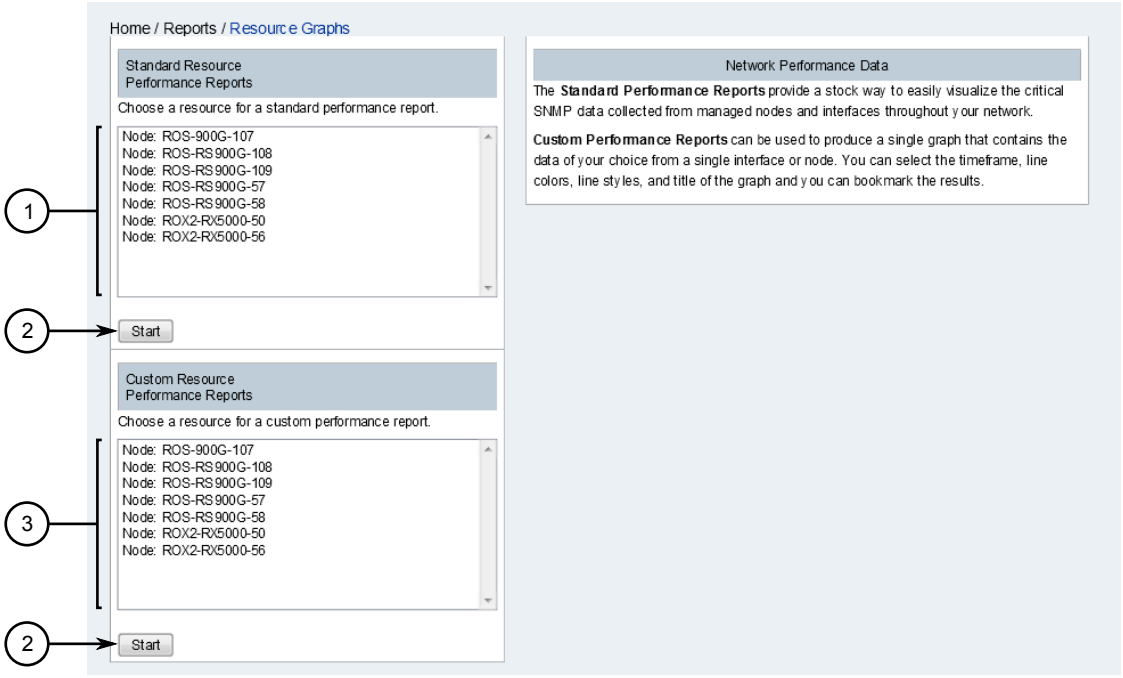


Figure 152: Resource Graphs Screen

1. Resource List for Standard Reports **2.** Start Button **3.** Resource List for Custom Reports

2. Under **Standard Resource Performance Reports**, select a resource and then click **Start**. The **Choose** screen appears.

> **NOTE**
> *Interface data is only available when SNMP data collection is configured for the selected device. For more information, refer to* *Section 6.5.2.1, "Configuring SNMP Data Collection"*.

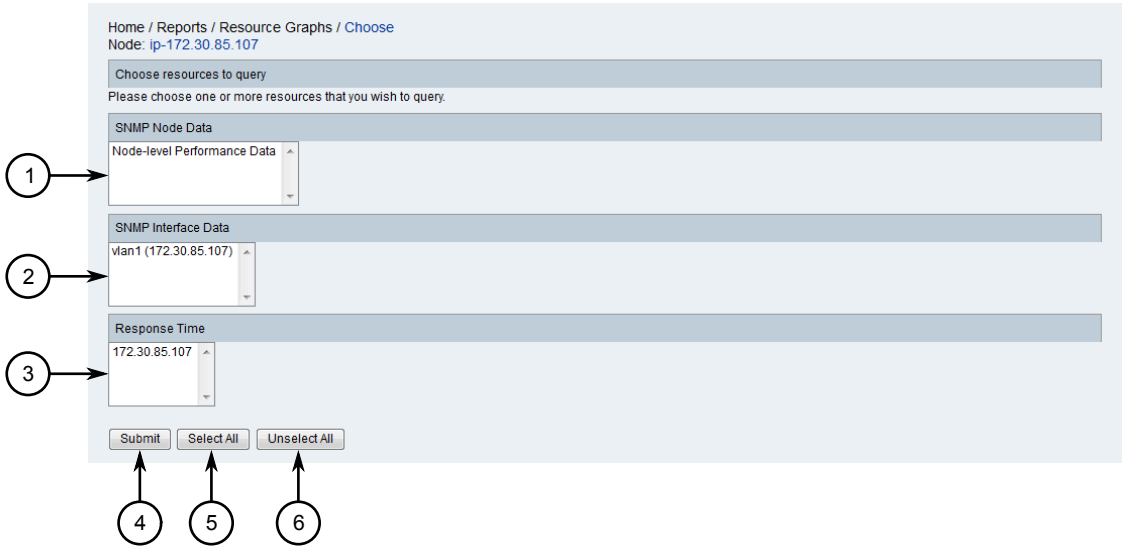


Figure 153: Choose Screen

1. SNMP Node Data List **2.** SNMP Interface Data List **3.** Response Time List **4.** Submit Button **5.** Select All Button **6.** Unselect All Button

NOTE
*To de-select a resource, hold **Ctrl** and select the resource.*

3. Select one or more resources to query.
4. Click **Submit**. The **Results** screen appears displaying a series of graphs.

Figure 154: Results Screen

1. Time Period List **2.** Start Time Lists and Boxes **3.** End Time Lists and Boxes **4.** Apply Custom Time Period Button **5.** Graphs

5. [Optional] Select a time period from which to display data. If **Custom** is selected, define the time period under **Start Time** and **End Time** and then click **Apply Custom Time Period**.
6. [Optional] Right-click and save one or more graphs, or click a graph to display it on its own for further analysis.

   Once a graph is displayed on its own, the sampling period can be further refined by defining a start and end time, or by clicking within the graph itself and dragging across the time period of interest.

Section 5.4.2.2

Generating Custom Reports

A custom resource performance report details specific node-oriented SNMP data chosen by the user. Only one resource can be selected at time, but up to four data choices can be chosen.

Custom resource performance reports can be bookmarked in a user's browser, allowing the report to be regenerated again.

To generate a custom report, do the following:

1. On the menu bar, click **Reports** and then click **Resource Graphs**. The **Resource Graphs** screen appears.

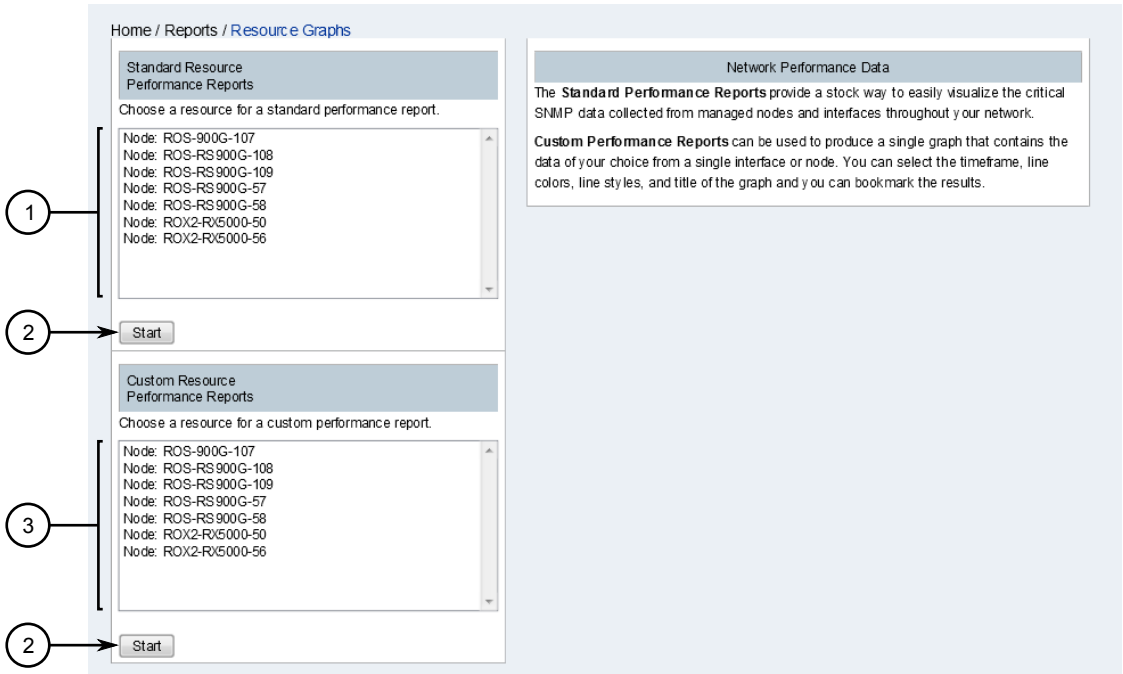


Figure 155: Resource Graphs Screen

1. Resource List for Standard Reports **2.** Start Button **3.** Resource List for Custom Reports

2. Under **Custom Resource Performance Reports**, select a resource and then click **Start**. The **Choose** screen appears.

> **NOTE**
> *Interface data is only available when SNMP data collection is configured for the selected device. For more information, refer to* *Section 6.5.2.1, "Configuring SNMP Data Collection"* .

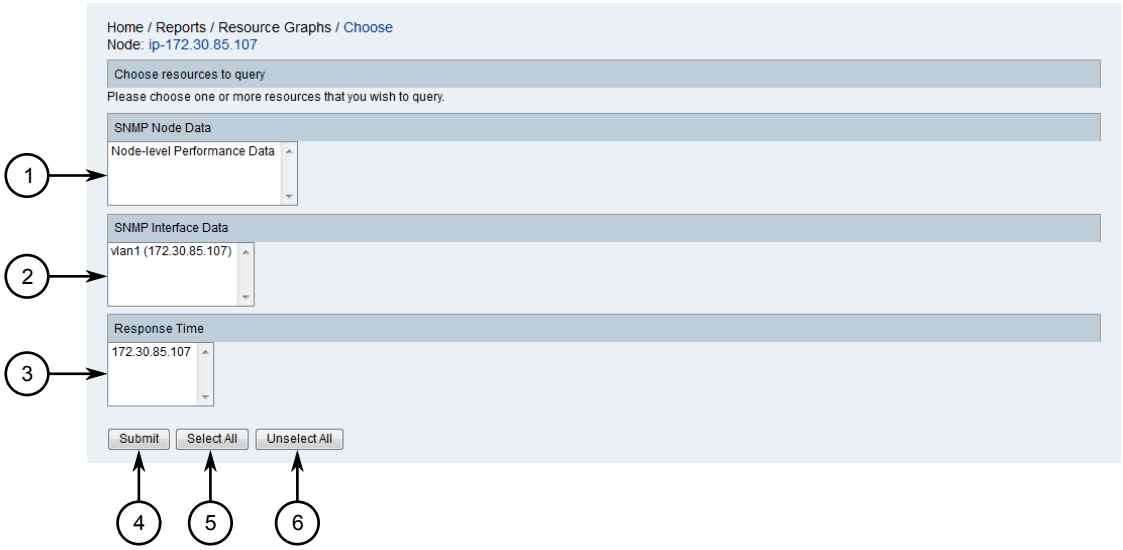


Figure 156: Choose Screen

1. SNMP Node Data List **2.** SNMP Interface Data List **3.** Response Time List **4.** Submit Button **5.** Select All Button **6.** Unselect All Button

NOTE
*To de-select a resource, hold **Ctrl** and select the resource.*

3. Select a resource to query.
4. Click **Submit**. The **Custom** screen appears displaying parameters for four data sources.

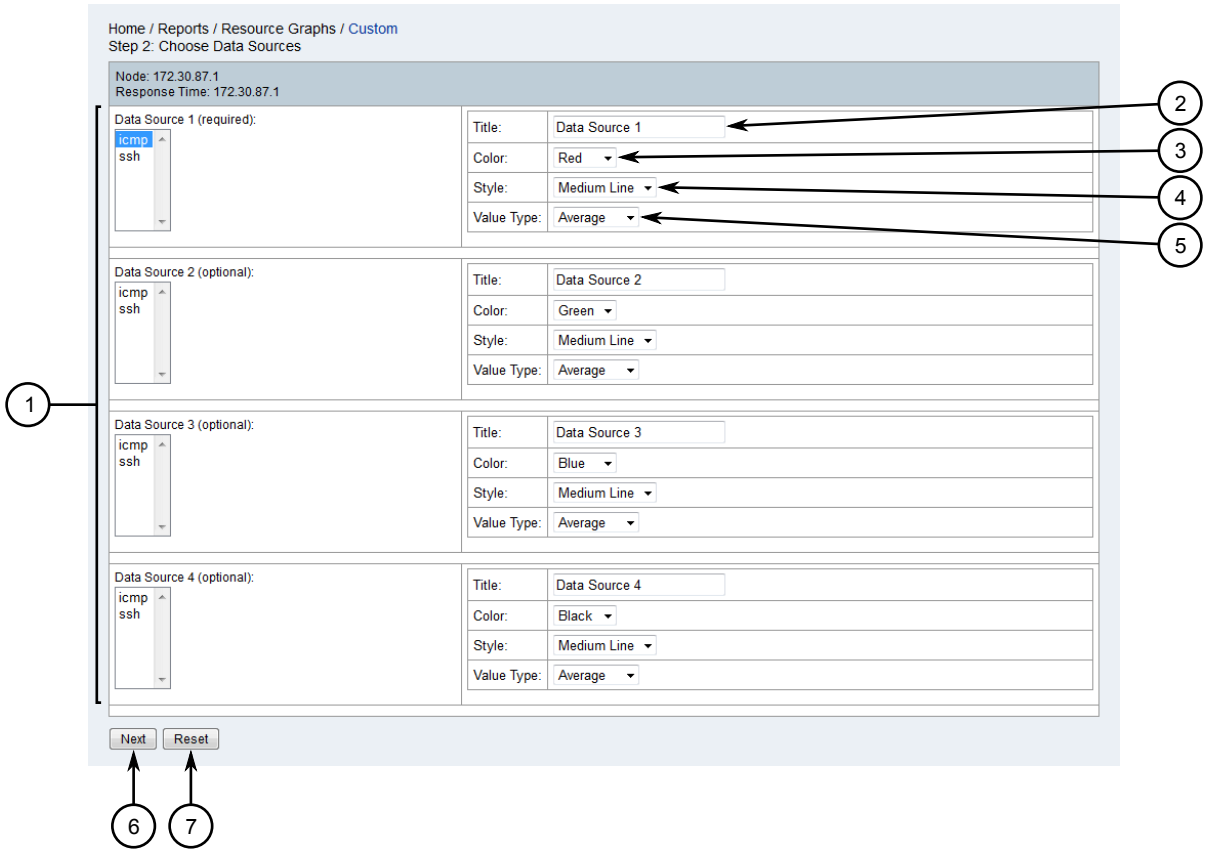


Figure 157: Custom Screen

1. Data Sources **2.** Title Box **3.** Color List **4.** Style List **5.** Value Type List **6.** Next Button **7.** Reset Button

5. For each data source, configure the following parameters:

Parameter	Description
Title	A custom name for the data source.
Color	**Synopsis:** { Red, Green, Blue, Black } **Default:** Red The color that represents the data in the performance report.
Style	**Synopsis:** { Thin Line, Medium Line, Thick Line, Area } **Default:** Medium Line The style of the line.
Value Type	**Synopsis:** { Average, Minimum, Maximum } **Default:** Average Determines whether the data displayed is the average, minimum or maximum.

6. Click **Next**. The **Custom** screen appears displaying a series of graphs.

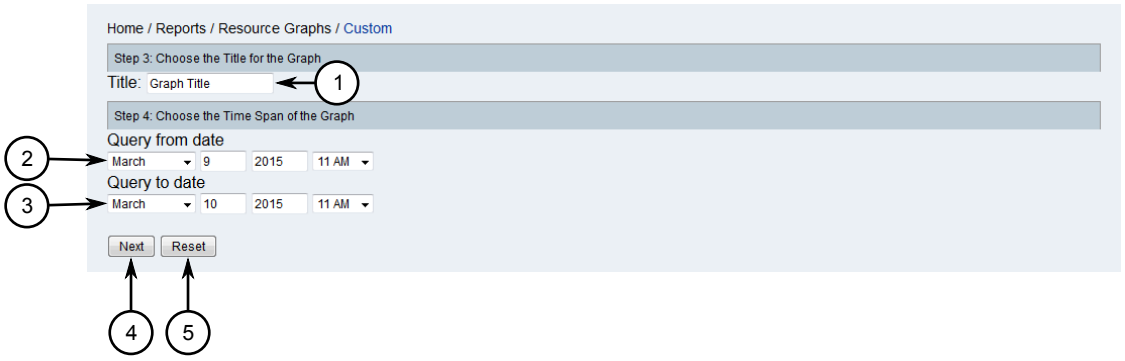


Figure 158: Custom Screen

1. Title Box **2.** Query From Date Lists and Boxes **3.** Query To Date Lists and Boxes **4.** Next Button **5.** Reset Button

7. Click **Next**. The **Custom** screen appears displaying the resulting graph.

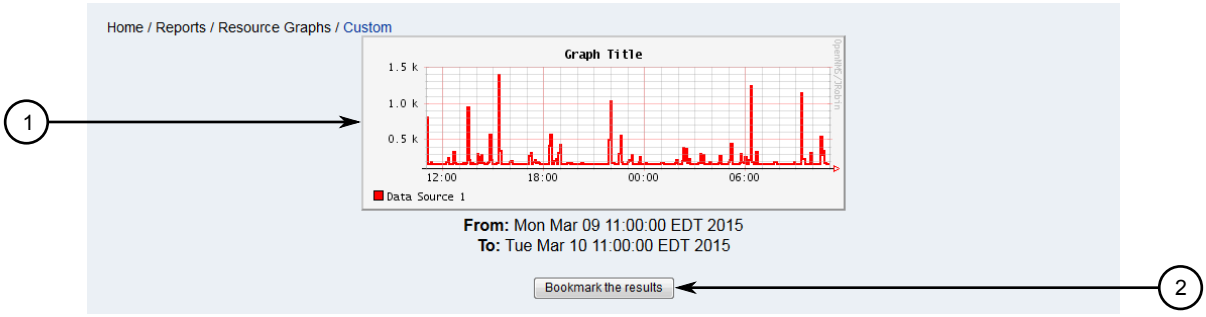


Figure 159: Results Screen

1. Graph **2.** Bookmark the Results Button

8. [Optional] Click **Bookmark the Results** to add a bookmark to the custom report.

Section 5.4.3

Managing KSC Reports

KSC (Key SNMP Customized) reports are user-defined views of SNMP performance data that use prefabricated graph types. Each report shows SNMP data for all SNMP interfaces on a selected device.

CONTENTS

- Section 5.4.3.6, “Deleting a KSC Report”

Section 5.4.3.1
Viewing a KSC Report

To view a saved KSC report, do the following:

1. On the menu bar, click **Reports** and then click **KSC Performance, Nodes, Domain**. The **KSC Report** screen appears.

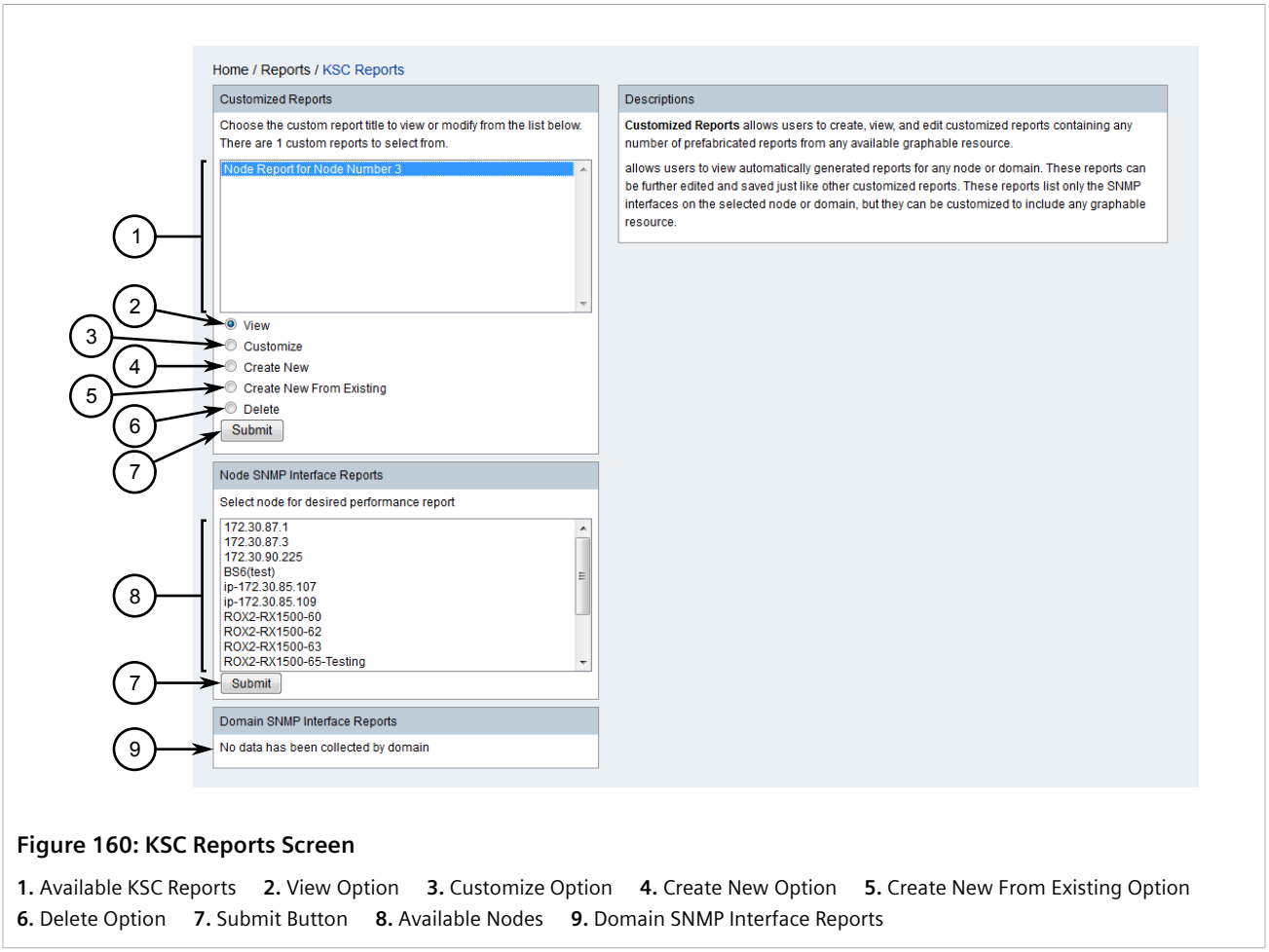


Figure 160: KSC Reports Screen

1. Available KSC Reports **2.** View Option **3.** Customize Option **4.** Create New Option **5.** Create New From Existing Option **6.** Delete Option **7.** Submit Button **8.** Available Nodes **9.** Domain SNMP Interface Reports

2. Select an existing report, select **View**, and then click **Submit**. The KSC report appears.

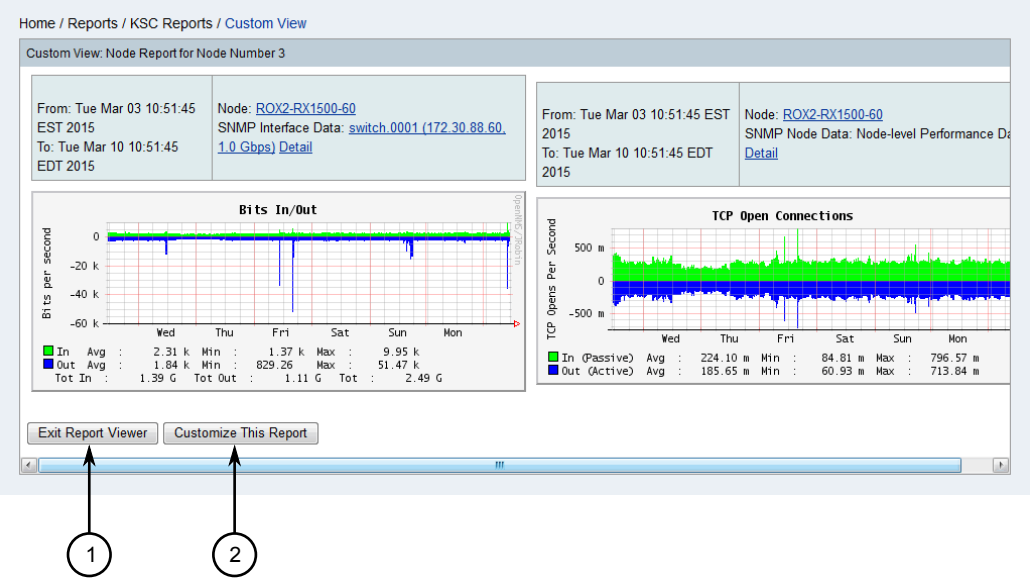


Figure 161: Sample KSC Report

1. Exit Report Viewer Button **2.** Customize This Report Button

Each KSC report features options for exiting and customizing the report. If configured, options for overriding the graph settings may also appear.

- **Exiting the Report**
  Click **Exit Report Viewer** to return to the **KSC Reports Screen**. Refer to Figure 160 .
- **Overriding the Graph Settings**
  1. Under **Override Graph Timespan**, select a time span.
  2. Under **Override Graph Type**, select a graph type.
  3. Click **Update Report View**. Each graph in the report is updated.
- **Customizing the Report**
  Click **Customize This Report** to customize the KSC report. The **Custom Report** screen appears. For more information about customizing a KSC Report, refer to Section 5.4.3.3, "Customizing a KSC Report" .

Section 5.4.3.2
Adding a KSC Report

To add a new KSC report, do the following:

1. On the menu bar, click **Reports** and then click **KSC Performance, Nodes, Domain**. The **KSC Report** screen appears.

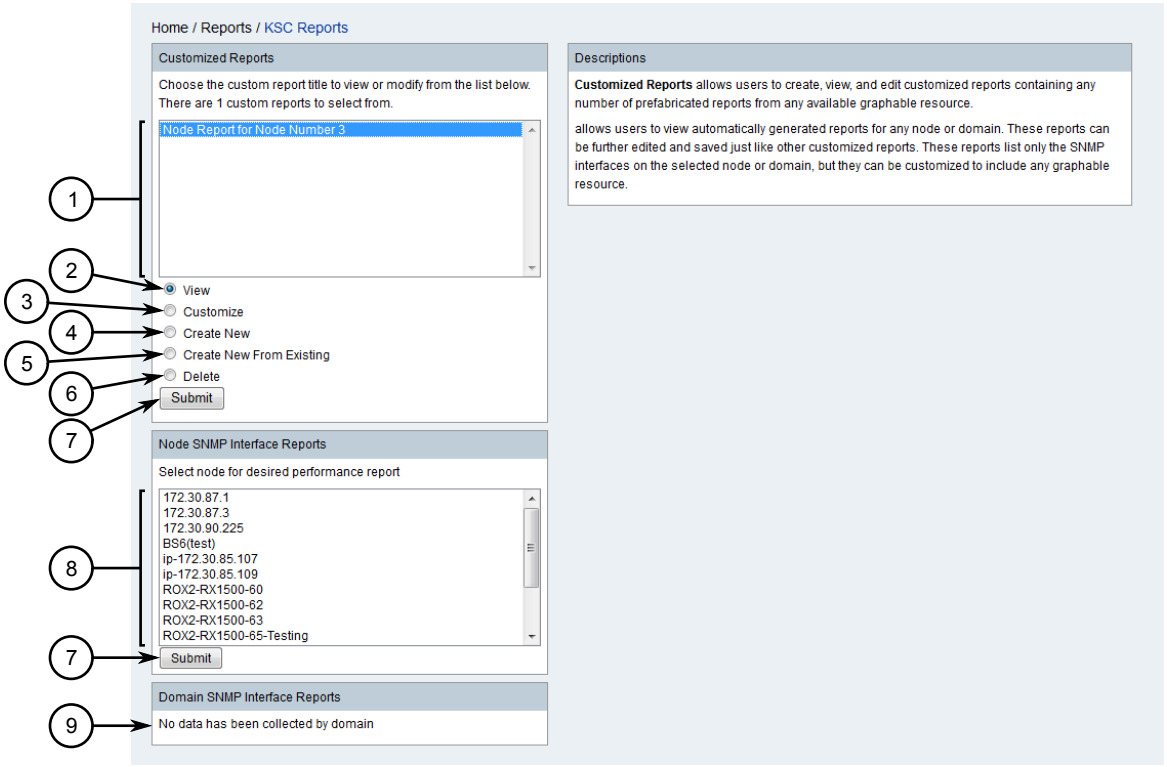


Figure 162: KSC Reports Screen

1. Available KSC Reports **2.** View Option **3.** Customize Option **4.** Create New Option **5.** Create New From Existing Option **6.** Delete Option **7.** Submit Button **8.** Available Nodes **9.** Domain SNMP Interface Reports

2. Select **Create New** to create a new KSC report, or select an existing KSC report and click **Create New From Existing**.
3. Click **Submit**. The **Custom Report** screen appears.

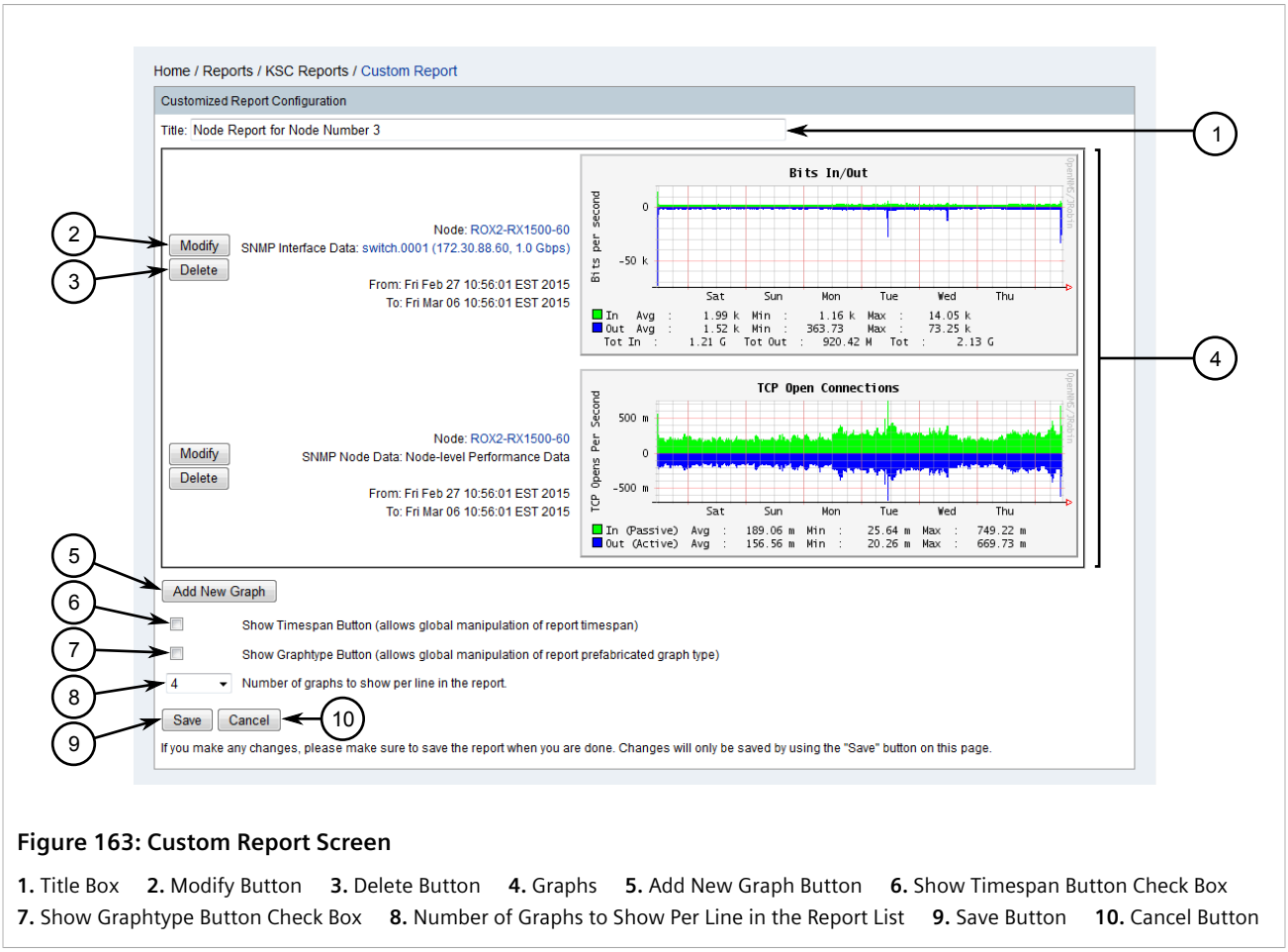


Figure 163: Custom Report Screen

1. Title Box **2.** Modify Button **3.** Delete Button **4.** Graphs **5.** Add New Graph Button **6.** Show Timespan Button Check Box **7.** Show Graphtype Button Check Box **8.** Number of Graphs to Show Per Line in the Report List **9.** Save Button **10.** Cancel Button

4. [Optional] If the report is based on an existing report, click **Delete** next to any unwanted graphs.
5. [Optional] If the report is based on an existing report, click **Modify** next to a graph to modify it. For more information, refer to Section 5.4.3.5, “Modifying a Graph” .
6. [Optional] Click **Add New Graph** to add a new graph. For more information, refer to Section 5.4.3.4, “Adding a Graph” .
7. Click **Save**. The new report is added to the list of available KSC reports.

Section 5.4.3.3
Customizing a KSC Report

To customize an existing KSC report, do the following:

1. On the menu bar, click **Reports** and then click **KSC Performance, Nodes, Domain**. The **KSC Report** screen appears.

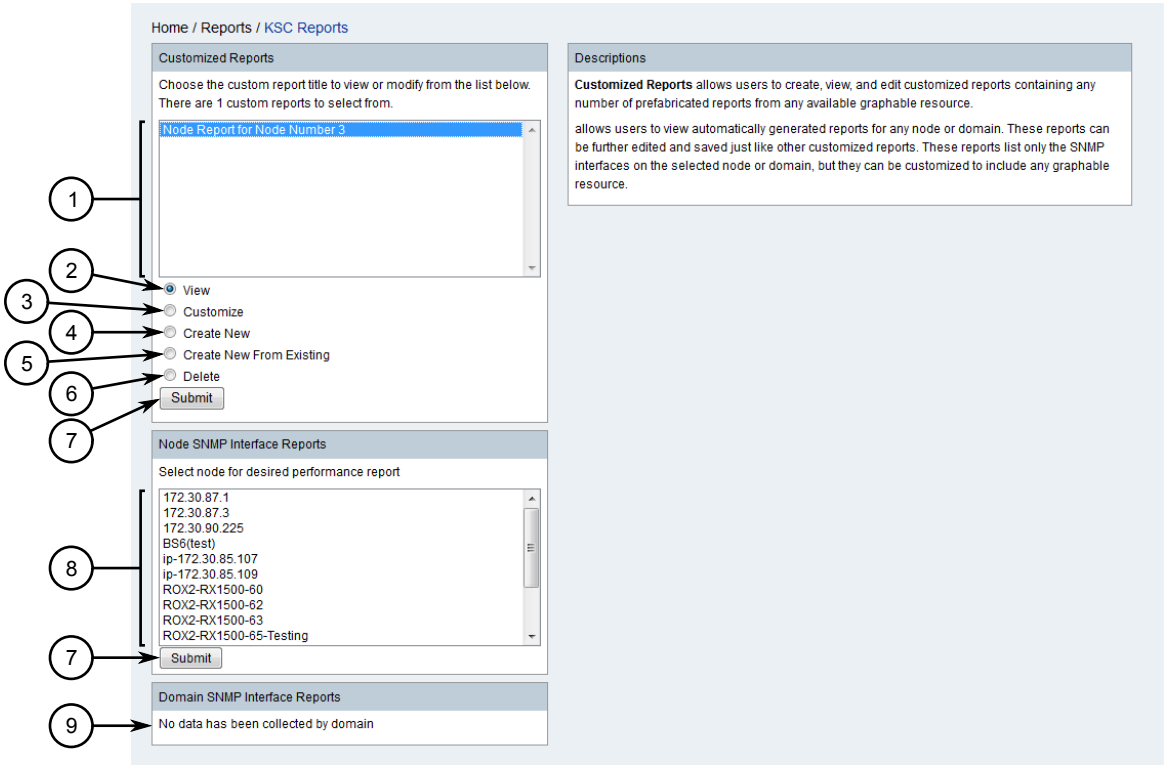


Figure 164: KSC Reports Screen

1. Available KSC Reports **2.** View Option **3.** Customize Option **4.** Create New Option **5.** Create New From Existing Option **6.** Delete Option **7.** Submit Button **8.** Available Nodes **9.** Domain SNMP Interface Reports

2. Select an existing report, select **Customize**, and then click **Submit**. The **Custom Report** screen appears.

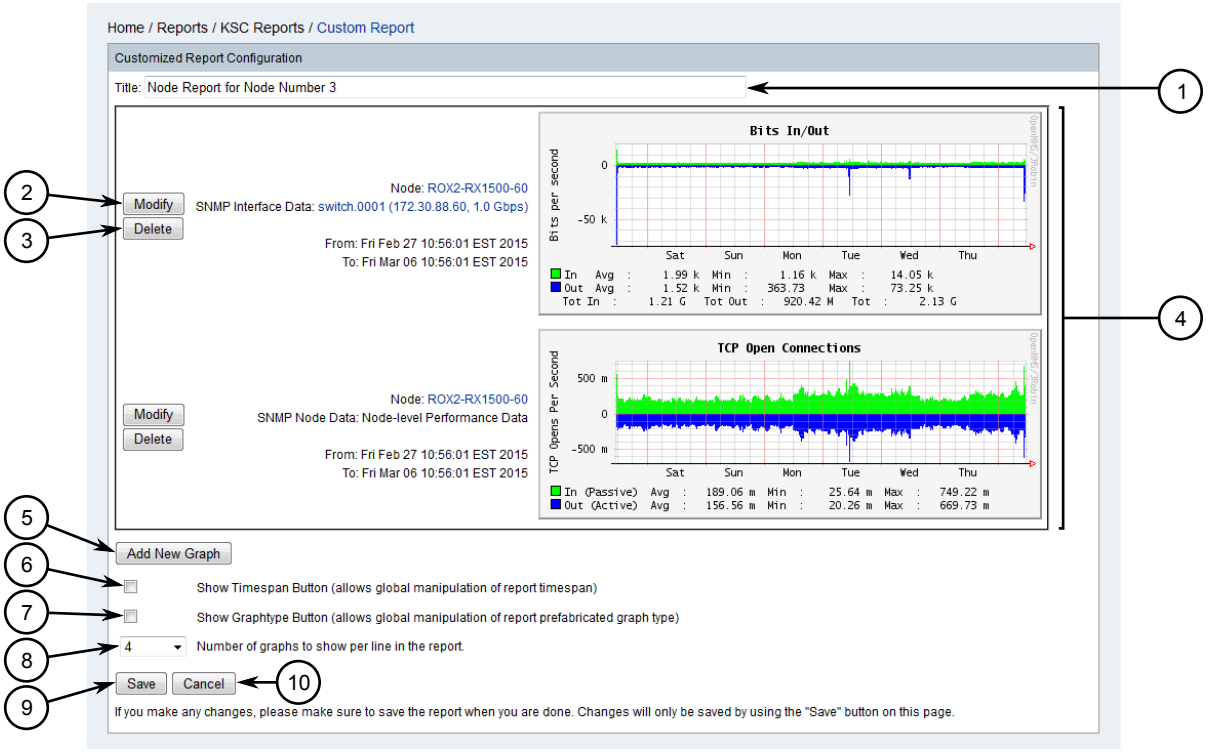


Figure 165: Custom Report Screen

1. Title Box **2.** Modify Button **3.** Delete Button **4.** Graphs **5.** Add New Graph Button **6.** Show Timespan Button Check Box **7.** Show Graphtype Button Check Box **8.** Number of Graphs to Show Per Line in the Report List **9.** Save Button **10.** Cancel Button

3. Configure the following parameters as required:

Parameter	Description
Title	The name of the KSC report.
Show Timespan Button	When selected, the **Override Graph Timespan** list appears at the bottom of the report, allowing the user to change the sampling period.
Show Graphtype Button	When selected, the **Override Graph Type** list appears at the bottom of the report, allowing the user to select a different prefabricated graph type.
Number of Graphs to Show Per Line in the Report	**Synopsis:** { 1, 2, 3, 4, 5, 6 } The number of graphs to show on each line, side-by-side, in the KSC report.

4. [Optional] Click **Delete** next to any unwanted graphs.
5. [Optional] Click **Modify** next to a graph to modify it. For more information, refer to Section 5.4.3.5, “Modifying a Graph” .
6. [Optional] Click **Add New Graph** to add a new graph. For more information, refer to Section 5.4.3.4, “Adding a Graph” .
7. Click **Save**.

Section 5.4.3.4
Adding a Graph

Graphs can be added for any graph-able resource, such as SNMP data, response time data or distribution response time data.

Available resources are listed first by top-level resources, such as nodes or domains (if enabled), and then by child resources, such as SNMP node-level data, response time data, etc.

To add a graph to a new or existing KSC report, do the following:

1. During the procedures for adding or customizing a KSC report, click **Add New Graph**. The **Custom Graph** screen appears.

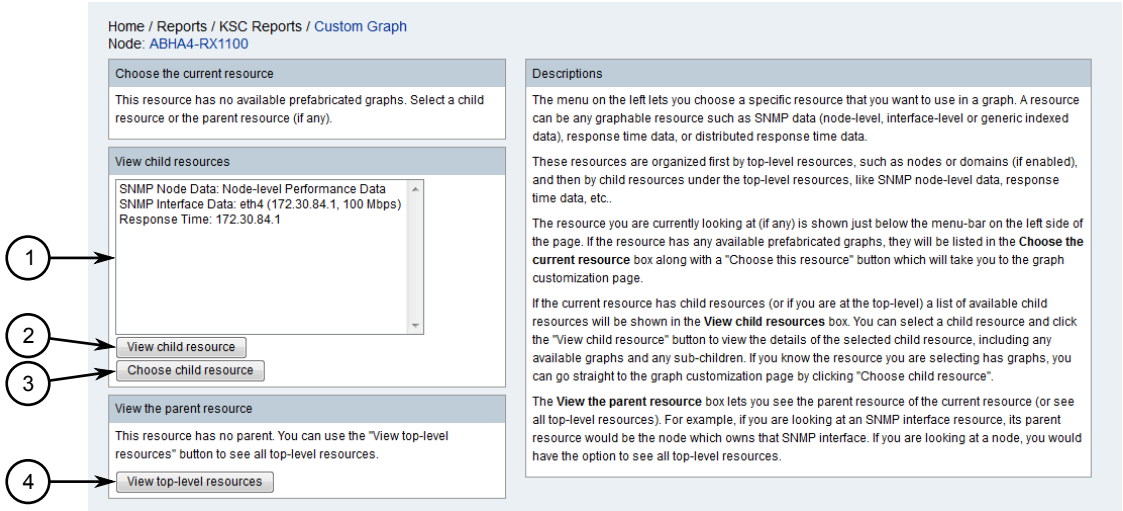


Figure 166: Custom Graph Screen

1. Child Resources List **2.** View Child Resources Button **3.** Choose Child Resource Button **4.** View Top-Level Resources Button

2. Select a top-level resource and then click **View Child Resource** to display its child resources. Repeat this step until the desired resource is found.

   If necessary, click **View Top-Level Resources** to return to the top-level resources again.

3. Click **Choose Child Resource**. The **Custom Graph** screen appears.

Figure 167: Custom Graph Screen

1. Sample Graph **2.** Title Box **3.** Timespan List **4.** Prefabricated Report List **5.** Graph Index List **6.** Cancel Edits to this Graph Button **7.** Refresh Sample View Button **8.** Choose Different Resource Button **9.** Done With Edits to this Graph Button

4. Configure the following parameters:

Parameter	Description
Title	The name of the graph.
Timespan	**Synopsis:** { 1_hour, 2_hour, 4_hour, 6_hour, 8_hour, 12_hour, 1_Day, 2_Day, 7_Day, 1_month, 3_month, 6_month, 1_year, Today, Yesterday, Yesterday 9am-5pm, Yesterday 5pm-10pm, This Week, Last Week, This Month, Last Month, This Quarter, Last Quarter, This Year, Last Year } **Default:** 7_Day The data sampling period.
Prefabricated Report	**Synopsis:** { mib2.bits, mib2_percentdiscards, mib2.percenterrors, mib2.discards, mib2.errors, mib2.packets, mib2.traffic-inout } **Default:** mib2.bits The prefabricated graph to use.
Graph Index	**Synopsis:** { 1, 2, 3 } **Default:** 3 The desired position in the report where the graph will be inserted next to other graphs.

5. [Optional] Click **Refresh Sample View** to update the sample graph based on the changes made.
6. [Optional] Click **Choose Different Resource** to return to **Custom Graph** screen and select a different resource and repeat Step 1 to Step 4 .
7. Click **Done With Edits to this Graph**. The new graph is added to the KSC report.

Section 5.4.3.5
Modifying a Graph

To modify a graph in an existing KSC report, do the following:

1. On the menu bar, click **Reports** and then click **KSC Performance, Nodes, Domain**. The **KSC Report** screen appears.

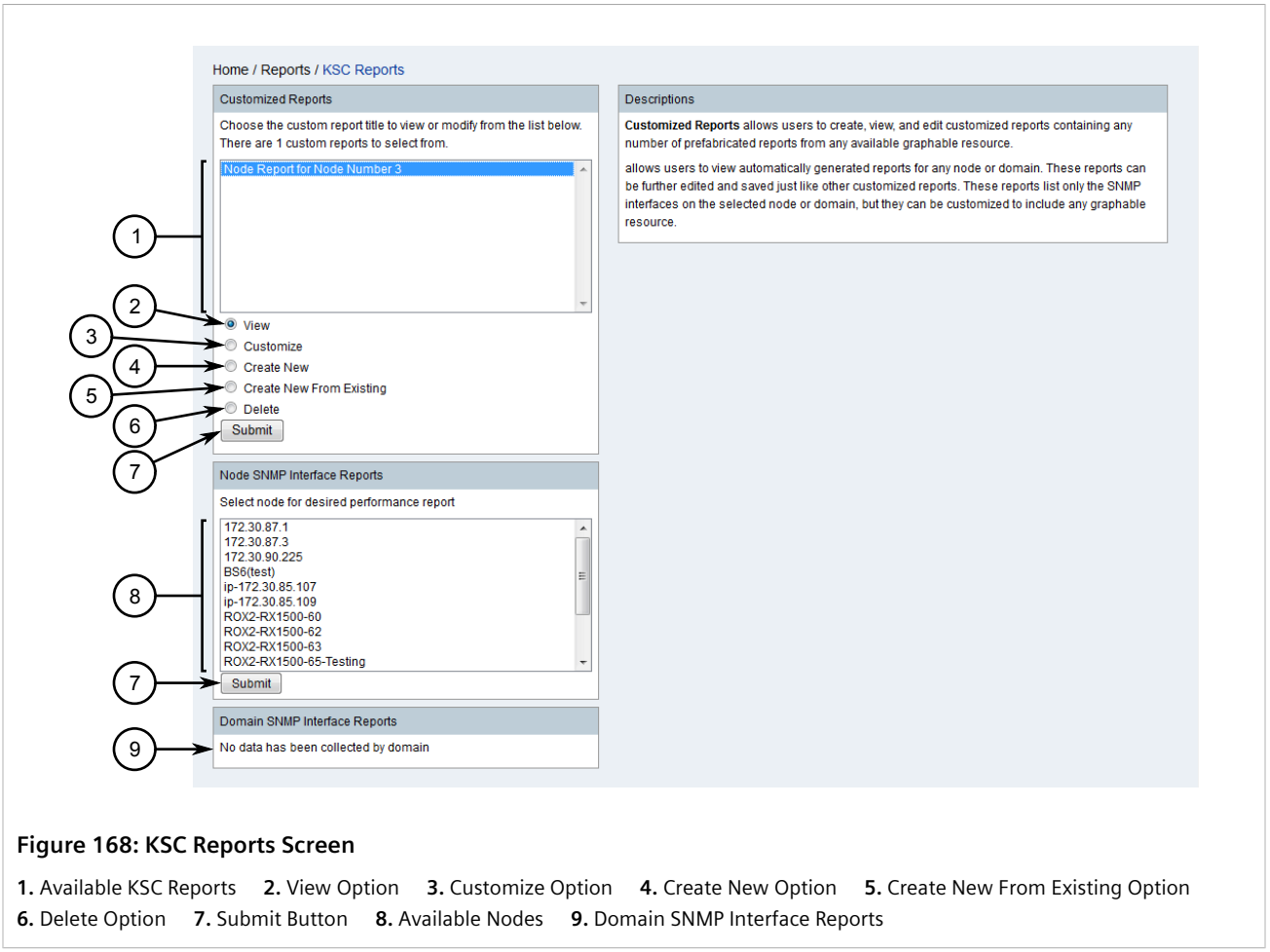


Figure 168: KSC Reports Screen

1. Available KSC Reports **2.** View Option **3.** Customize Option **4.** Create New Option **5.** Create New From Existing Option **6.** Delete Option **7.** Submit Button **8.** Available Nodes **9.** Domain SNMP Interface Reports

2. Select an existing report, select **Customize**, and then click **Submit**. The **Custom Report** screen appears.

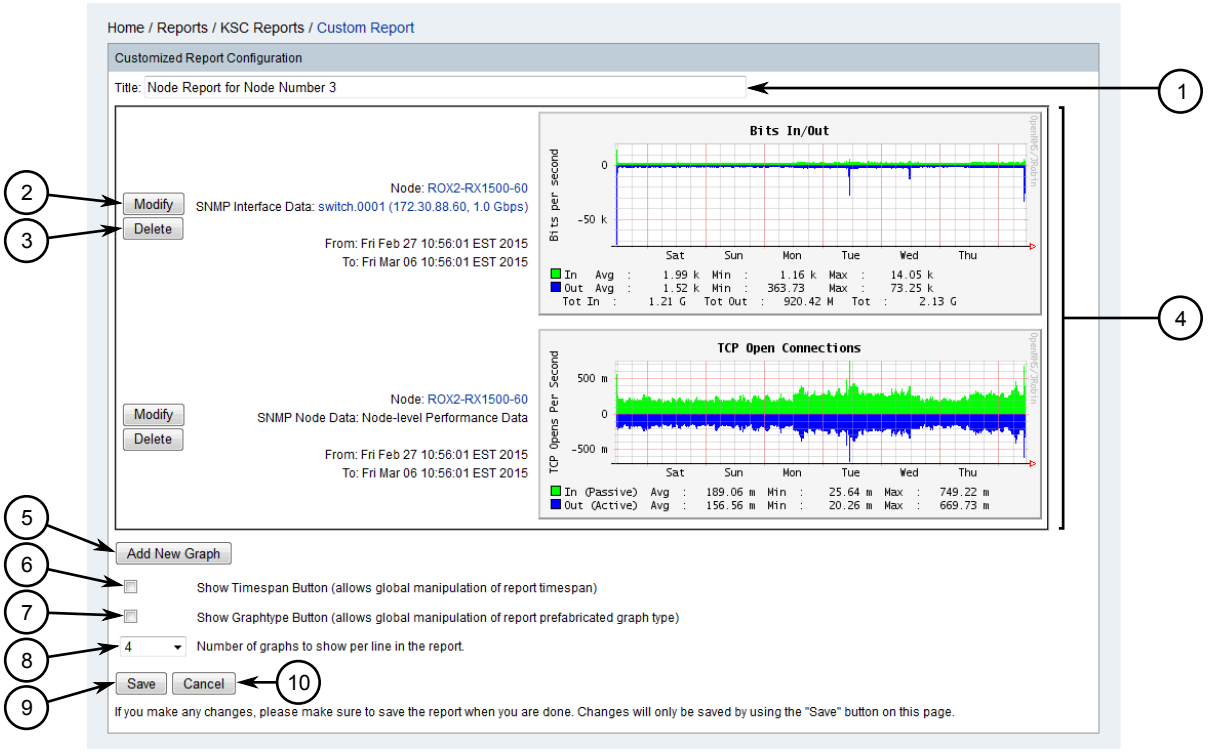


Figure 169: Custom Report Screen

1. Title Box **2.** Modify Button **3.** Delete Button **4.** Graphs **5.** Add New Graph Button **6.** Show Timespan Button Check Box **7.** Show Graphtype Button Check Box **8.** Number of Graphs to Show Per Line in the Report List **9.** Save Button **10.** Cancel Button

3. Click **Modify** next to the chosen graph. The **Custom Graph** screen appears.

Figure 170: Custom Graph Screen

1. Sample Graph **2.** Title Box **3.** Timespan List **4.** Prefabricated Report List **5.** Graph Index List **6.** Cancel Edits to this Graph Button **7.** Refresh Sample View Button **8.** Choose Different Resource Button **9.** Done With Edits to this Graph Button

4. Configure the following parameters:

Parameter	Description
Title	The name of the graph.
Timespan	**Synopsis:** { 1_hour, 2_hour, 4_hour, 6_hour, 8_hour, 12_hour, 1_Day, 2_Day, 7_Day, 1_month, 3_month, 6_month, 1_year, Today, Yesterday, Yesterday 9am-5pm, Yesterday 5pm-10pm, This Week, Last Week, This Month, Last Month, This Quarter, Last Quarter, This Year, Last Year } **Default:** 7_Day The data sampling period.
Prefabricated Report	**Synopsis:** { mib2.bits, mib2_percentdiscards, mib2.percenterrors, mib2.discards, mib2.errors, mib2.packets, mib2.traffic-inout } **Default:** mib2.bits The prefabricated graph to use.
Graph Index	**Synopsis:** { 1, 2, 3 } **Default:** 3 The desired position in the report where the graph will be inserted next to other graphs.

5. [Optional] Click **Refresh Sample View** to update the sample graph based on the changes made.
6. [Optional] Click **Choose Different Resource** to select a different resource. For more information, refer to Step 1 to Step 4 in Section 5.4.3.4, “Adding a Graph” .
7. Click **Done With Edits to this Graph**. The **Custom Report** screen appears displaying the updated graph.

Section 5.4.3.6
Deleting a KSC Report

To delete a KSC report, do the following:

1. On the menu bar, click **Reports** and then click **KSC Performance, Nodes, Domain**. The **KSC Report** screen appears.

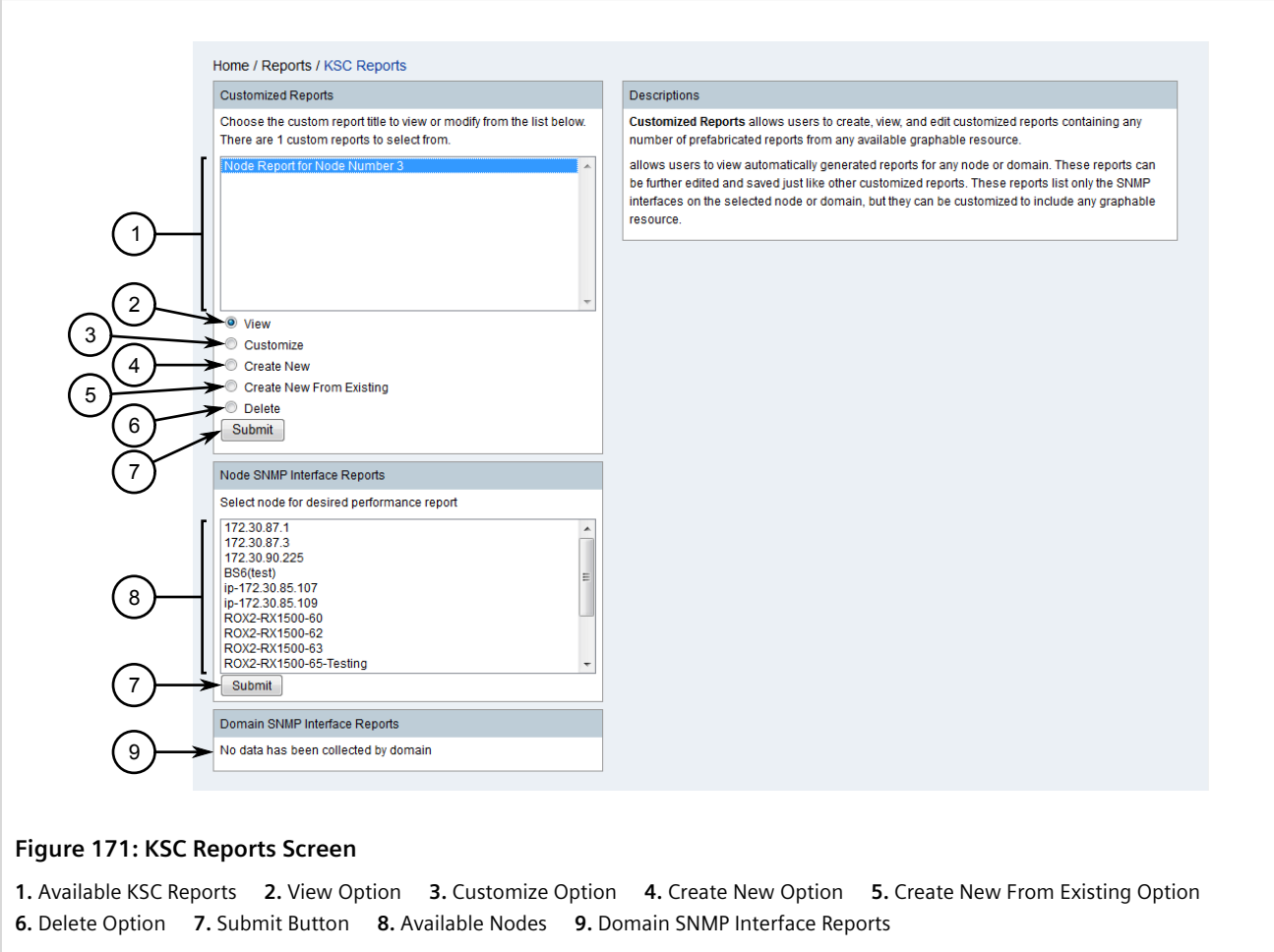


Figure 171: KSC Reports Screen

1. Available KSC Reports **2.** View Option **3.** Customize Option **4.** Create New Option **5.** Create New From Existing Option **6.** Delete Option **7.** Submit Button **8.** Available Nodes **9.** Domain SNMP Interface Reports

2. Select one or more KSC reports, select **Delete**, and then click **Submit**. A confirmation message appears.
3. Click **OK**.

Section 5.4.4
Managing Statistics Reports

Statistics reports list and detail the top IP interfaces within a specific time frame that have the highest number of input octets (ifInOctet). Reports are generated automatically at regular intervals.

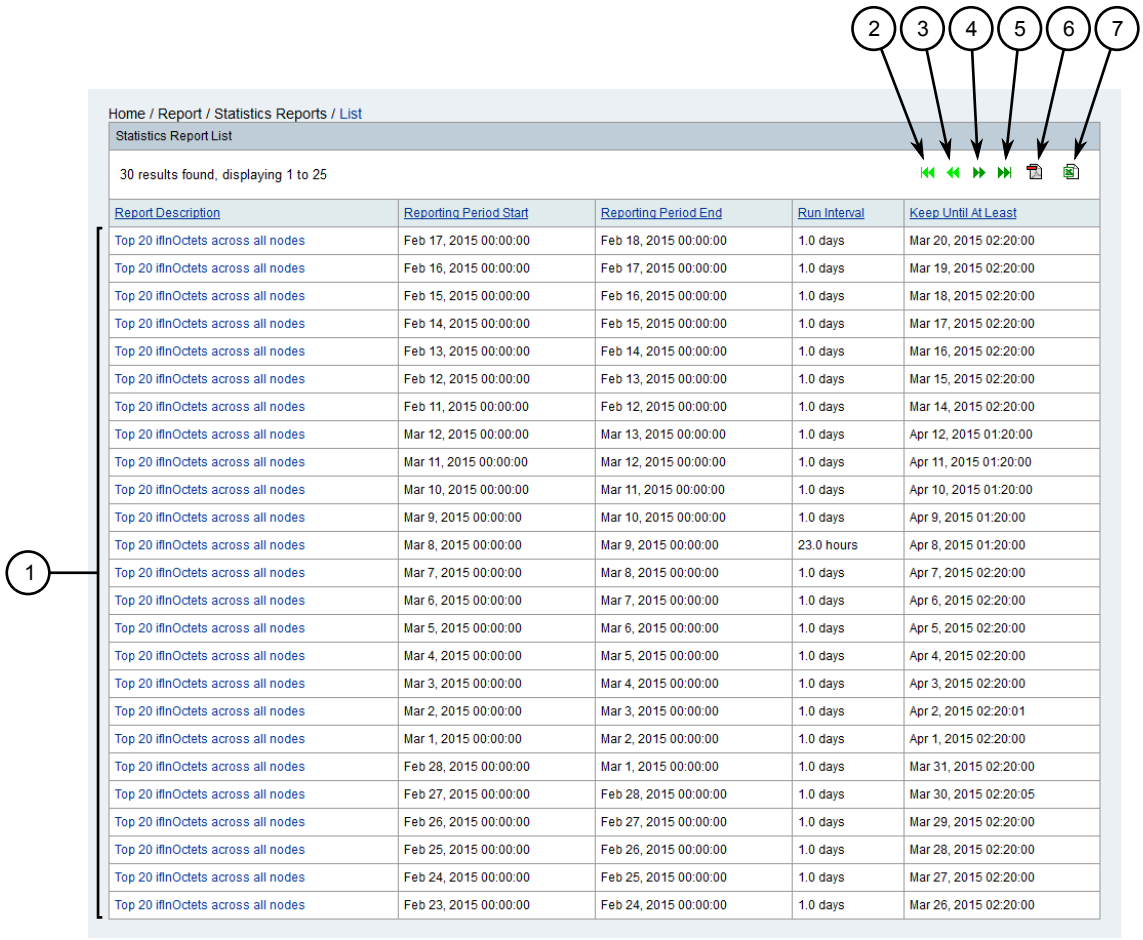
The title of reports, when they are generated, how long they are retained, and much more, is customizable by the user.

CONTENTS

Section 5.4.4.1

Viewing/Exporting a List of Statistics Reports

To view a list of available statistics reports, click **Reports** on the menu bar, then click **Statistics Reports**. The **List** screen appears



Report Description	Reporting Period Start	Reporting Period End	Run Interval	Keep Until At Least
Top 20 ifInOctets across all nodes	Feb 17, 2015 00:00:00	Feb 18, 2015 00:00:00	1.0 days	Mar 20, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 16, 2015 00:00:00	Feb 17, 2015 00:00:00	1.0 days	Mar 19, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 15, 2015 00:00:00	Feb 16, 2015 00:00:00	1.0 days	Mar 18, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 14, 2015 00:00:00	Feb 15, 2015 00:00:00	1.0 days	Mar 17, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 13, 2015 00:00:00	Feb 14, 2015 00:00:00	1.0 days	Mar 16, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 12, 2015 00:00:00	Feb 13, 2015 00:00:00	1.0 days	Mar 15, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 11, 2015 00:00:00	Feb 12, 2015 00:00:00	1.0 days	Mar 14, 2015 02:20:00
Top 20 ifInOctets across all nodes	Mar 12, 2015 00:00:00	Mar 13, 2015 00:00:00	1.0 days	Apr 12, 2015 01:20:00
Top 20 ifInOctets across all nodes	Mar 11, 2015 00:00:00	Mar 12, 2015 00:00:00	1.0 days	Apr 11, 2015 01:20:00
Top 20 ifInOctets across all nodes	Mar 10, 2015 00:00:00	Mar 11, 2015 00:00:00	1.0 days	Apr 10, 2015 01:20:00
Top 20 ifInOctets across all nodes	Mar 9, 2015 00:00:00	Mar 10, 2015 00:00:00	1.0 days	Apr 9, 2015 01:20:00
Top 20 ifInOctets across all nodes	Mar 8, 2015 00:00:00	Mar 9, 2015 00:00:00	23.0 hours	Apr 8, 2015 01:20:00
Top 20 ifInOctets across all nodes	Mar 7, 2015 00:00:00	Mar 8, 2015 00:00:00	1.0 days	Apr 7, 2015 02:20:00
Top 20 ifInOctets across all nodes	Mar 6, 2015 00:00:00	Mar 7, 2015 00:00:00	1.0 days	Apr 6, 2015 02:20:00
Top 20 ifInOctets across all nodes	Mar 5, 2015 00:00:00	Mar 6, 2015 00:00:00	1.0 days	Apr 5, 2015 02:20:00
Top 20 ifInOctets across all nodes	Mar 4, 2015 00:00:00	Mar 5, 2015 00:00:00	1.0 days	Apr 4, 2015 02:20:00
Top 20 ifInOctets across all nodes	Mar 3, 2015 00:00:00	Mar 4, 2015 00:00:00	1.0 days	Apr 3, 2015 02:20:00
Top 20 ifInOctets across all nodes	Mar 2, 2015 00:00:00	Mar 3, 2015 00:00:00	1.0 days	Apr 2, 2015 02:20:01
Top 20 ifInOctets across all nodes	Mar 1, 2015 00:00:00	Mar 2, 2015 00:00:00	1.0 days	Apr 1, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 28, 2015 00:00:00	Mar 1, 2015 00:00:00	1.0 days	Mar 31, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 27, 2015 00:00:00	Feb 28, 2015 00:00:00	1.0 days	Mar 30, 2015 02:20:05
Top 20 ifInOctets across all nodes	Feb 26, 2015 00:00:00	Feb 27, 2015 00:00:00	1.0 days	Mar 29, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 25, 2015 00:00:00	Feb 26, 2015 00:00:00	1.0 days	Mar 28, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 24, 2015 00:00:00	Feb 25, 2015 00:00:00	1.0 days	Mar 27, 2015 02:20:00
Top 20 ifInOctets across all nodes	Feb 23, 2015 00:00:00	Feb 24, 2015 00:00:00	1.0 days	Mar 26, 2015 02:20:00

Figure 172: List Screen

1. Available Statistics Reports **2.** First Page Icon **3.** Previous Page Icon **4.** Next Page Icon **5.** Last Page Icon **6.** PDF Icon **7.** Excel Icon

Only 25 reports are displayed at a time. Use the **First Page**, **Previous Page**, **Next Page** or **Last Page** controls to the next/previous list.

To export the full list as an Adobe PDF (*.pdf) or Microsoft Excel (*.xls) file, do the following:

1. Click either the **PDF** or **Excel** icon. A dialog box appears.
2. Select where to save the file locally and then click **OK**.

Section 5.4.4.2

Viewing/Exporting a Statistics Report

To view and export a statistics report, do the following:

1. On the menu bar, click **Reports**, then click **Statistics Reports**. The **List** screen appears

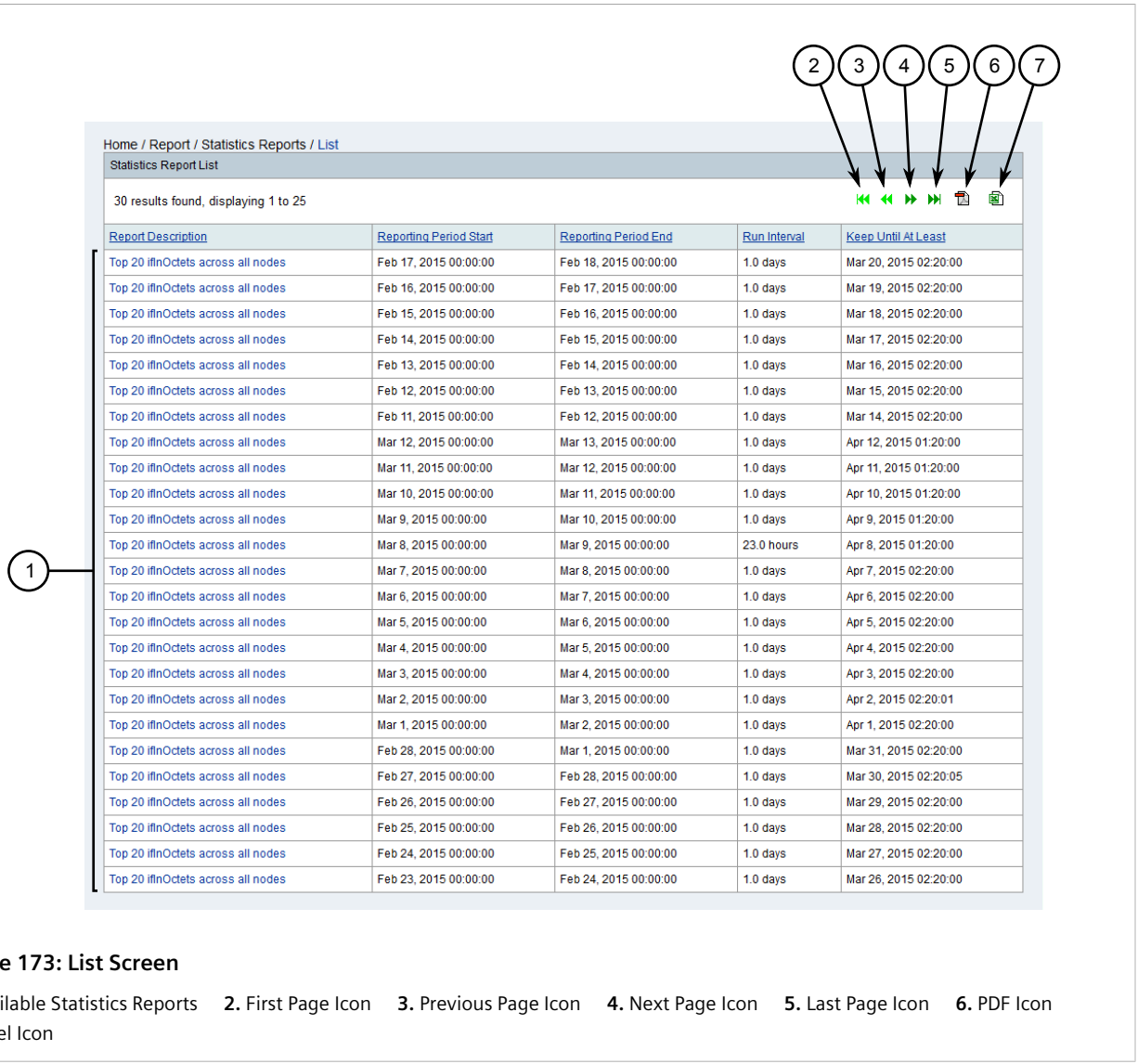


Figure 173: List Screen

1. Available Statistics Reports **2.** First Page Icon **3.** Previous Page Icon **4.** Next Page Icon **5.** Last Page Icon **6.** PDF Icon **7.** Excel Icon

NOTE
Only 25 reports are displayed at a time.

2. Only 25 reports are displayed at a time. Use the **First Page**, **Previous Page**, **Next Page** or **Last Page** controls to find the desired report.
3. Select the desired statistics report. The **Report** screen appears:

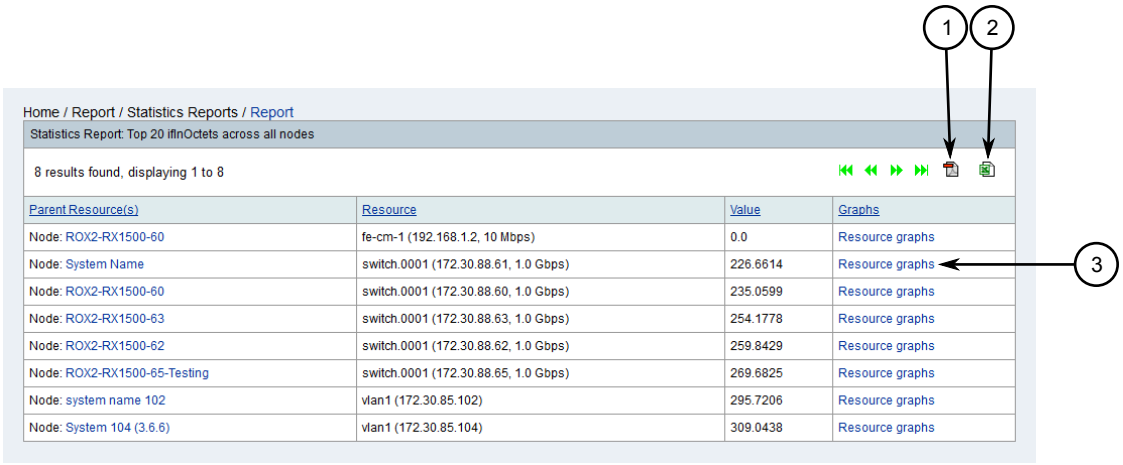


Figure 174: List Screen

1. PDF Icon **2.** Excel Icon **3.** Resource Graphs Link

4. To export the full list as an Adobe PDF (*.pdf) or Microsoft Excel (*.xls) file, click either the **PDF** or **Excel** icon. A dialog box appears.
5. Select where to save the file locally and then click **OK**.
6. [Optional] Click **Resource Graphs** to view the resource graphs for the associated interface.

Figure 175: Results Screen

1. Time Period List **2.** Start Time Lists and Boxes **3.** End Time Lists and Boxes **4.** Apply Custom Time Period Button **5.** Graphs

Section 5.4.4.3

Customizing the Generation of Statistics Reports

To customize the generation of statistics reports, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/statsd-configuration.xml`

   The following is an example of standard `statsd-configuration.xml` file:

```
<?xml version="1.0"?>
<statistics-daemon-configuration
  xmlns:this="http://www.opennms.org/xsd/config/statsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opennms.org/xsd/config/statsd http://www.opennms.org/xsd/config/
statistics-daemon-configuration.xsd ">

  <package name="example1">
    <packageReport name="TopN" description="Top 20 ifInOctets across all nodes"
                   schedule="0 20 1 * * ?" retainInterval="2592000000"
                   status="on">
      <parameter key="count" value="20"/>
      <parameter key="consolidationFunction" value="AVERAGE"/>
      <parameter key="relativeTime" value="YESTERDAY"/>
      <parameter key="resourceTypeMatch" value="interfaceSnmp"/>
      <parameter key="attributeMatch" value="ifInOctets"/>
    </packageReport>
  </package>

  <report name="TopN" class-name="org.opennms.netmgt.dao.support.TopNAttributeStatisticVisitor"/>
```

```
</statistics-daemon-configuration>
```

2. Create a copy of an existing `<package>` element (including its children), or modify an existing element.
3. Customize the `<package>` element as required:

   ```
   <package name="{name}">
   ```

   Where:

   - `name` is the name of the report package.
4. Configure the basic settings for the report by customizing the `<packageReport>` element:

   ```
   <packageReport name="{name}" description="{description}" schedule="{schedule}"
    retainInterval="{interval}" status="{status}"/>
   ```

   Where:

   - `name` is the name of the report.
   - `description` is a description of the report. The description appears in the list of statistics reports.
   - `schedule` is a cron-like statement that defines when to create the report.
   - `retainInterval` is the total time in milliseconds (ms) to keep the report. Once the time expires, the report is deleted automatically.
   - `status` enables/disables report generation. Accepted values include `on` and `off`.
5. Configure the maximum number of nodes counted included in the report by customizing the `count` parameter as required:

   ```
   <parameter key="count" value="{value}"/>
   ```

   Where:

   - `value` is the number of nodes to count.
6. Control how data is consolidated over the collection period by customizing the `consolidationFunction` parameter:

   ```
   <parameter key="consolidationFunction" value="{value}"/>
   ```

   Where:

   - `value` is one of the following:
     - `AVERAGE` – Averages all the values.
     - `MAX` – Stores the maximum value collected.
     - `MIN` – Stores the minimum value collected.
     - `LAST` – Stores the last value collected.
7. Define the sampling period by customizing the `relativeTime` parameter as required:

   ```
   <parameter key="relativeTime" value="{value}"/>
   ```

   Where:

   - `value` is one of the following:
     - `YESTERDAY` – Present data from the previous day.
     - `LASTSEVENDAYS` – Present data from over the last seven days.

    - `LASTTHIRTYONEDAYS` – Present data from over the last 31 days.
    - `TODAY` – Present data from today.

8. Define the resource type by customizing the `resourceTypeMatch` parameter as required:

   ```
   <parameter key="resourceTypeMatch" value="{value}"/>
   ```

   Where:

   - `value` is one of the following:
     - `nodeSnmp` – Node-level data.
     - `interfaceSnmp` – Interface-level data.

9. Define the data source by customizing the `attributeMatch` parameter as required:

   ```
   <parameter key="attributeMatch" value="{value}"/>
   ```

   Where:

   - `value` is the data source, such as *ifInOctets* or *ifOutOctets*.

10. Save and close the file.
11. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS".

Section 5.5

Managing Logical Maps

Logical mapping provides powerful, flexible, Web-based mapping of network devices managed by RUGGEDCOM NMS.

RUGGEDCOM NMS can automatically map and lay out a selected set of devices, save and restore custom map views, perform live updates, display map updates in real-time, and much more.

Each map uses data collected from each device to display network nodes, links and other important information. Devices discovered by RUGGEDCOM NMS are placed automatically on the map in the order in which they are discovered. They can be laid out in either a *hierarchical* or *organic* style.

Other features include:

- Customize map content, filtered by IP address and device name
- Display multiple maps simultaneously
- Designate a *home* map
- Edit, save and restore network maps
- Use node and link colors to quickly asses the state of the network
- Use network links to view live statistical data
- Group/ungroup devices
- Customize the look of each map, including device icons
- Export images of each map in either PNG or JPEG format

IMPORTANT!
The Adobe Flash Player browser plug-in must be installed to use logical maps. For more information about which version of Flash is supported, refer to *Section 1.2, "System Requirements"*.

IMPORTANT!
Admin and Operator users can create and edit logical maps. Guest users can only view logical maps.

NOTE
RUGGEDCOM NMS supports a maximum of five simultaneous logical map sessions.

NOTE
Pop-up windows must be enabled in the user's Web browser for some map features to work properly.

CONTENTS

Section 5.5.1
Enabling Logical Maps

Before using logical maps in RUGGEDCOM NMS, the following DNS entry must first be added to either the DNS server or to the HOST file on each user's workstation:

```
rnms.ruggedcomnms.com
```

For information about how to add a DNS entry to a DNS server, contact the DNS server administrator or refer to the DNS server documentation.

Section 5.5.2

Logical Map Controls

Each logical map features a toolbar that provides the following controls:

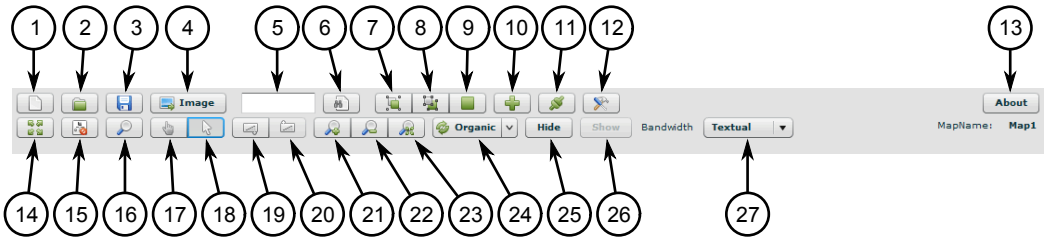


Figure 176: Logical Map Toolbar

1. New Map Button **2.** Load Map Button **3.** Save Map Button **4.** Export Map Button **5.** Device to Find Box **6.** Find Device Button **7.** Group Selection Button **8.** Ungroup Selection Button **9.** Fold/Unfold Button **10.** Add Device Button **11.** Synchronize Button **12.** Configuration Button **13.** About Button **14.** Full Screen Button **15.** Toggle Navigation Panel Button **16.** Magnifier Button **17.** Move Tool Button **18.** Edit Tool Button **19.** Enter Group Button **20.** Exit Group Button **21.** Zoom In Button **22.** Zoom Out Button **23.** Zoom Fit Button **24.** Refresh Map and Recalculate Layout List **25.** Hide Button **26.** Show Button **27.** Bandwidth Button

NOTE

*When logical mapping is launched for the first time in a session, only the **New Map** and **Load Map** buttons are available in the toolbar.*

Icon	Name	Description
	New Map	Creates a new map. This button appears for administrative users only. For more information, refer to Section 5.5.5, “Adding a Logical Map” .
	Load Map	Loads an existing map saved on the RUGGEDCOM NMS server. For more information, refer to Section 5.5.4, “Opening a Logical Map” .
	Save Map	Saves a map. This button appears for administrative users only. For more information, refer to Section 5.5.7, “Saving/Copying a Logical Map” .
Image	Export	Exports the current map as a PNG or JPG image. For more information, refer to Section 5.5.11, “Exporting a Logical Map as an Image” .
	Find Device	Finds a device based on its visible name and locates it in the center of the screen. For more information, refer to Section 5.5.17.2, “Searching for Devices in a Logical Map” .
	Group	Groups selected devices into a single object. For more information, refer to Section 5.5.18.1, “Assigning Devices to a Group” .
	Ungroup	Ungroups a selected group of devices. For more information, refer to Section 5.5.18.4, “Ungrouping Devices” .
	Fold/Unfold	Collapses or expands a selected group of devices. For more information, refer to Section 5.5.18.3, “Displaying Devices Within Groups” .
	Add Devices	Adds additional devices to the current map. For more information, refer to Section 5.5.17.1, “Adding Devices to a Logical Map” .
	Synchronize	Synchronizes the map with data from the RUGGEDCOM NMS server. For more information, refer to Section 5.5.10, “Synchronizing a Logical Map” .

Icon	Name	Description
	Configure	Displays controls for configuring automatic data updates, a *home* map, and enabling the network monitor gage. For more information, refer to Section 5.5.6, "Configuring a Logical Map" .
	About	Displays the mapping application version and support information.
	Full Screen	Switches the map to full-screen mode. In full screen mode, the map hides the navigation panel and toolbar. Keyboard shortcuts are also disabled. To exit from full-screen mode, press **Esc**.
	Toggle Navigation Panel	Displays or hides the gray navigation panel at the top-left of the map. To move the logical map around in the screen, click and drag inside the navigation panel.
	Magnifier	Displays or hides a circular region on the map that enlarges objects on the map. Move the magnifier over the map to inspect objects. Click the **Magnifier** button again to close the magnifier.
	Move Tool	Use this control to reposition the map by clicking and dragging on the map itself.
	Edit Tool	Enables users to select and manipulate nodes/links on the map. To select a node or link, click on the object. To move a node or link, click and drag the object. To select multiple objects, click and drag to draw a bounding box around the objects.
	Enter Group	Displays the contents of a group of nodes. For more information, refer to Section 5.5.18.3, "Displaying Devices Within Groups" .
	Exit Group	Exits a group of nodes and returns to the main map. For more information, refer to Section 5.5.18.3, "Displaying Devices Within Groups" .
	Zoom In	Zooms in on the map.
	Zoom Out	Zooms out from the map.
	Zoom Fit	Fits the map to the size available in the browser window.
	Refresh Map and Recalculate layout	Displays the map in Organic or Hierarchical mode. For more information, refer to Section 5.5.9, "Selecting a Layout" .
	Hide	Hides selected items – other than groups – on the map. Items can also be hidden by seleting them and then pressing **Delete**.
	Show	Shows items on the map that have been hidden.
	Bandwidth	Shows and hides link labels. To display graphical labels, select **Graphical**. To display text labels, select **Textual**. To hide link labels, select **None**. For more information on link labels, refer to Section 5.5.19, "Managing Links" .

Section 5.5.3

Icons and OID Mapping

Each device is represented on a map by an icon (standard or custom) that indicates the status of the device as follows:

Color	Status	Description
	New Device	The device has been newly discovered. Events related to the discovery of the new device must be acknowledged before the device's up/down/alarm status is displayed on the logical map. For more information about viewing events for a

Color	Status	Description
		device on a logical map, refer to Section 5.5.17.4, "Viewing Events, Reports and Assets Information" .
	Device Down	The device is unavailable.
	Alarm	The device has outstanding notifications that have not yet been acknowledged/ cleared.
	Device Up	The device is a normal state.

Each device type is assigned, by default, a unique standard icon which maps to a specific OID (Object Identifier). The registered RUGGEDCOM OID is .1.3.6.1.4.1.15004.

NOTE
Standard icons can be replaced with custom icons, as suits the organization, on a device-by-device basis. For more information about changing the icon for a device, refer to Section 5.5.17.6, "Customizing Device Icons" .

The following are the standard icons associated with each device type, along with the OID suffices appended to the RUGGEDCOM OID.

Device Group	Device System OID Suffix	Icon Name	Icon
Generic		generic	
Switches	.1.3.6.1.4.1.15004.2.1	switch	
RS950G		prphsr	
RUGGEDCOM Access Point	.1.3.6.1.4.1.15004.2.10	rugged_air	
Serial Server	.1.3.6.1.4.1.15004.2.2	serial_server	
Spanning Tree Protocol (STP) Root		stproot	

Device Group	Device System OID Suffix	Icon Name	Icon
Media Converters	.1.3.6.1.4.1.15004.2.3	media_converter	
ROX-based Routers	.1.3.6.1.4.1.15004.2.4.*	router	
RX1000 models (ROX)	.1.3.6.1.4.1.15004.2.4.1		
RX1100 models (ROX)	.1.3.6.1.4.1.15004.2.4.2		
RX1400	.1.3.6.1.4.1.15004.2.8.14	ucp_RX1400	
RX5000	.1.3.6.1.4.1.15004.2.5.*	ucp_5000	
RX5000 model (ROX II)	.1.3.6.1.4.1.15004.2.5.1		
	.1.3.6.1.4.1.15004.2.5.2		
WIN	.1.3.6.1.4.1.15004.2.6.*	rmax_base	
WIN Base Station	.1.3.6.1.4.1.15004.2.6.1		
WIN Base Station	.1.3.6.1.4.1.15004.2.6.2		
WIN	.1.3.6.1.4.1.15004.2.7.*	rmax_cpe	
WIN CPE	.1.3.6.1.4.1.15004.2.7.1		
WIN CPE	.1.3.6.1.4.1.15004.2.7.2		
WIN CPE	.1.3.6.1.4.1.15004.2.7.3		
RX1500	.1.3.6.1.4.1.15004.2.8.*	ucp_1500	
RX1500 models	.1.3.6.1.4.1.15004.2.8.1		
	.1.3.6.1.4.1.15004.2.8.2		
	.1.3.6.1.4.1.15004.2.8.11		
	.1.3.6.1.4.1.15004.2.8.12		
	.1.3.6.1.4.1.15004.2.8.13		
RX1000 models (ROX II)	.1.3.6.1.4.1.15004.2.9.1	rox2_router	
RX1100 models (ROX II)	.1.3.6.1.4.1.15004.2.9.2		
RUGGEDCOM NMS		nms	
Obsolete router	.1.3.6.1.4.1.15004.3.1	router	

Device Group	Device System OID Suffix	Icon Name	Icon
Scalance	.1.3.6.1.4.1.4196.1.1 .1.3.6.1.4.1.4329.20.1 .1.3.6.1.4.1.4329.6.1	scalance	

Section 5.5.4
Opening a Logical Map

To open an existing logical map, do the following:

1. On the menu bar, click **Map**. A new browser window or tab appears displaying either the *home* map or a blank map with a simplified toolbar.
2. Click the **Open Map** button. The **Load Saved Map** dialog box appears.

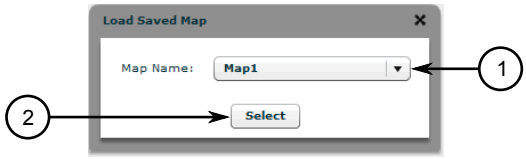


Figure 177: Load Saved Map Dialog Box

1. Map Name List **2.** Select Button

3. Under **Map Name**, select a saved map and then click **Select**. The selected map is loaded.

Section 5.5.5
Adding a Logical Map

To add new logical map, do the following:

1. On the menu bar, click **Map**. A new browser window or tab appears displaying either the *home* map or a blank map with a simplified toolbar.
2. Click the **New Map** button. The **Create New Map** dialog box appears.

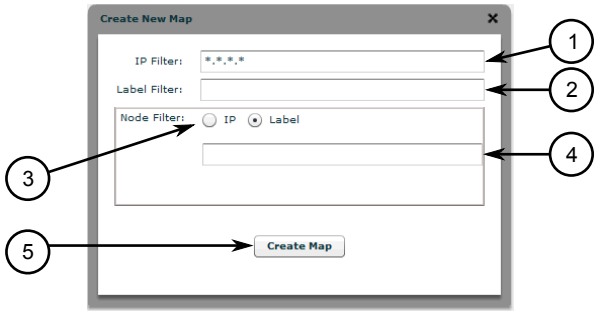


Figure 178: Create New Map Dialog Box

1. IP Filter Box **2.** Label Filter Box **3.** Node Filter Options **4.** Node Filter Box **5.** Create Map Button

NOTE
All filter criteria is retained and applied to new devices discovered by RUGGEDCOM NMS after the map is created.

3. Under **IP Filter**, type the IP address for a device. Only devices managed by RUGGEDCOM NMS that are within the specified IP address range will appear in the map. Use an asterisk (*) as a wildcard to represent all numbers from 0 to 255.

   For example, `10.100.*.*` selects all devices in the range of addresses beginning with *10.100*.

4. Under **Label Filter**, type a full or partial device name. If required, use a percent sign (%) as a wildcard to match device names that begin and/or end with the specified string. Only devices with a matching name appear in the map.

   For example, `%switch%` matches all device names that include *switch*, such as *my_**switch*** , ***switch**_123*, but not *sw* or *swt*.

5. Under **Node Filter**, select either **IP** or **Label** and then type the exact IP address or name (label) of a device managed by RUGGEDCOM NMS. Only devices matching the specific criterion – and devices linked to them – will appear in the map.

   NOTE
   Pattern matches are not supported.

   NOTE
   The search criteria does not need to match the IP Filter or Label Filter criteria.

   For example, `switch_123` matches *switch_123*, but not *switch_1234*. Similarly, `10.100.10.111` matches *10.100.10.111*, but not *10.100.10.112*.

6. Click **Create Map**. A map is created displaying the devices that match the selected criteria.

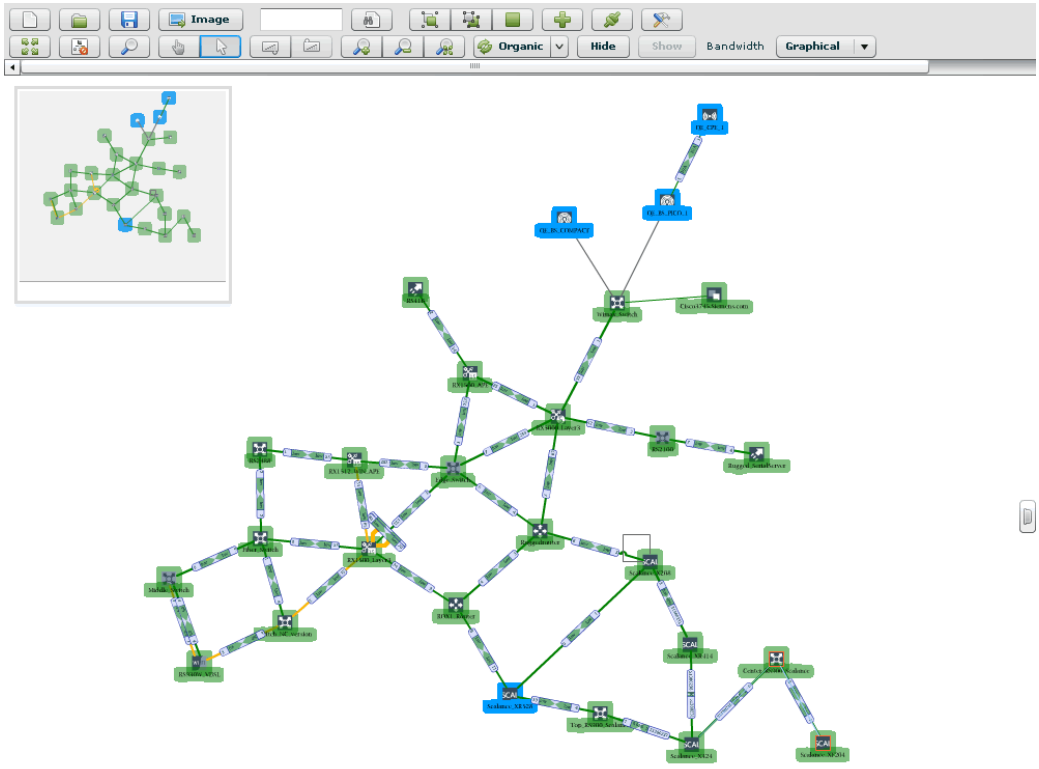


Figure 179: Example of a Logical Map

NOTE
Logical maps are not limited to mapping only the device(s) chosen during their initial creation. Multiple devices can be added to a map at any time.

7. [Optional] Add additional devices as needed. For more information, refer to Section 5.5.17.1, "Adding Devices to a Logical Map" .

Section 5.5.6

Configuring a Logical Map

To configure a logical map, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .
2. Click the **Configure** button. The **General Configuration** dialog box appears.

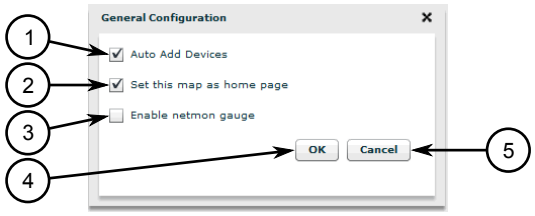


Figure 180: General Configuration Dialog Box

1. Auto Add Devices Check Box **2.** Set This Map As Home Page Check Box **3.** Enable Netmon Gauge Check Box **4.** OK Button **5.** Cancel Button

3. Enable or disable the following parameters as required:

Parameter	Description
Auto Add Device	When selected, devices discovered by RUGGEDCOM NMS will be added to the logical map automatically.
Set This Map As Home Page	Sets the current map as the *home* map. The home map will open automatically when the user logs in to RUGGEDCOM NMS. A home map is associated with the user's credentials. If two users with the same credentials log in at the same time, the same home map will open for both. **NOTE** *In some browsers, pop-up windows are blocked by default. When setting the home map, make sure your browser is configured to allow pop-up windows, otherwise the home map may not display.*
Enable Netmon Gauge	When selected, a gage for monitoring network bandwidth appears in the top right corner of the logical map. For more information about the network monitor gage, refer to Section 5.5.14, "Monitoring Bandwidth Usage" .

4. Click **OK**.

To configure advanced settings, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/netmap-config.xml`

   The following is an example of a typical `netmap-config.xml` file:

```
<netmap-configuration>
  <butil_threshold>
    <butil color="green" threshold="0.0"/>
    <butil color="yellow" threshold="33.3"/>
    <butil color="red" threshold="66.6"/>
  </butil_threshold>
  <link_styles>
   <link ltype="10000000" width="2.0"/>
    <link ltype="100000000" width="4.0"/>
  <link ltype="1000000000" width="6.0"/>
  <link ltype="10000000000" width="8.0"/>
  <link ltype="up" width="0" style="green"/>
    <link ltype="down" width="0" style="red"/>
    <link ltype="blocking" width="0" style="haloorange"/>
```

```
  <link ltype="new" width="0" style="haloblue"/>
  <link ltype="netmon" width="0" style="blue"/>
  </link_styles>
 <params>
    <param name="animation" value="false" />
    <param name="butil_units_bps" value="false" />
  <param name="trace" value="false" />
   <param name="node-filter-update-timer" value="900000" />
   <param name="auto-delete-node" value="true" />
  </params>
</netmap-configuration>
```

2. Configure the following parameters as required:

Parameter	Description
`<butil color="{color}" threshold="{threshold}"/>`	Controls the color that appears around icons when the bandwidth exceeds the specified threshold percentage.
`<link ltype="{type}" width="{width}" style="{color}"/>`	Controls the color and width of link lines based on the speed or status of the connection.
`<param name="animation" value="{boolean}"/>`	**Synopsis:** { true, false } **Default:** false Enables/disables animations.
`<param name="butil_units_bps" value="{boolean}"/>`	**Synopsis:** { true, false } **Default:** false When enabled (true), traffic is displayed on link labels in bits/second (bps). Otherwise, traffic is displayed as a percentage.
`<param name="node-filter-update-timer" value="{age}"/>`	**Default:** 900000 For node filter aging of new auto-added devices.
`<param name="auto-delete-node" value="{boolean}"/>`	**Synopsis:** { true, false } **Default:** false When enabled (true), connected nodes are deleted from the map when they age out and the node filter is applied.

3. Save and close the file.
4. Restart any open logical map sessions.

Section 5.5.7

Saving/Copying a Logical Map

To save or copy a logical map, do the following:

1. On the toolbar, click the **Save** button. The **Save Map** screen appears.

Figure 181:

1. Map Name Box **2.** Save Map Button

2. To copy the existing map, under **Map Name**, type a new name for the duplicate map. Otherwise, proceed to the next step.
3. Click **Save Map**. The existing map or a copy of the existing map is saved.

Section 5.5.8

Deleting Logical Maps

To delete a logical map, do the following:

1. Log on to the RUGGEDCOM NMS server.
2. Navigate to the following directory:

   `/usr/share/opennms/ruggednms/netmap/maps`
3. Delete the following two files:
   - {name}.graphml
   - {name}.xml

   Where *{name}* is the name of the map.

Section 5.5.9

Selecting a Layout

Devices on a logical map can be arranged manually by the user or automatically by RUGGEDCOM NMS in one of two layouts: *Organic* or *Hierarchical*. Each layout arranges the devices according to the data collected from them using mathematical data graphic techniques. Neither layout attempts to represent the physical arrangement or location of the devices.

- **Organic Layout**
  Organic layouts show a free-form and balanced schematic view of the devices. Organic layouts are best for illustrating clusters and relative relationships between network nodes.

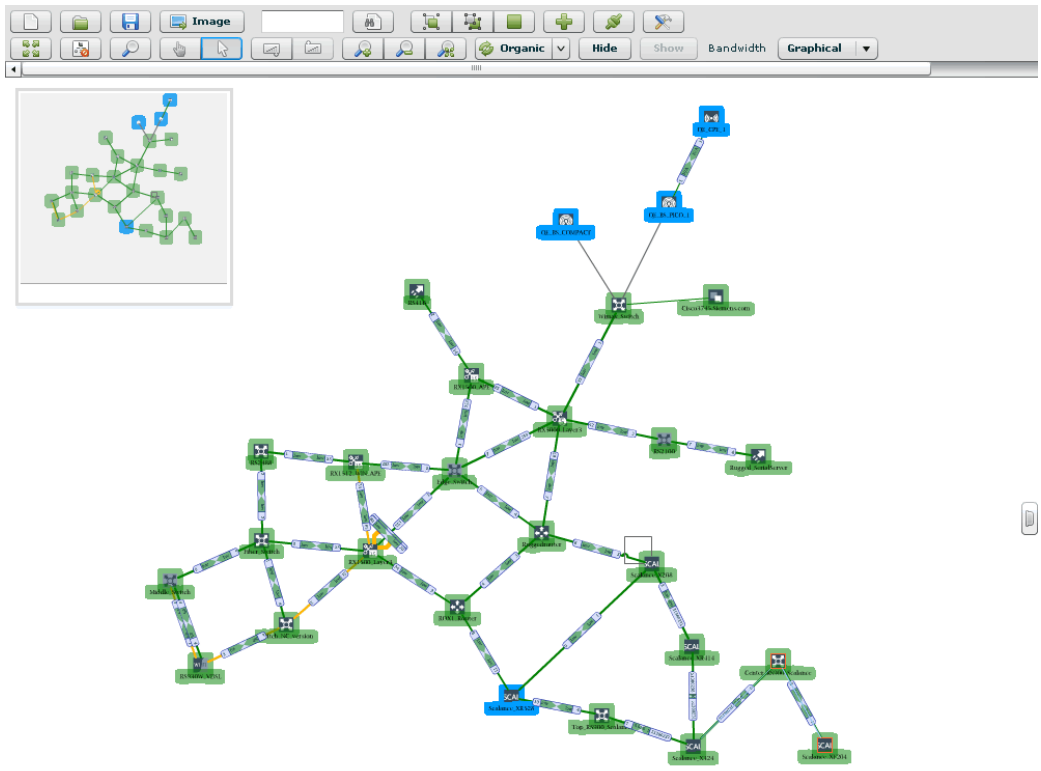


Figure 182: Example Organic Layout

- **Hierarchical Layout**
  Hierarchical layouts show an arbitrarily structured schematic view of the devices. Hierarchical view arrange nodes in distinct levels, roughly based on the number of nodes and their links.

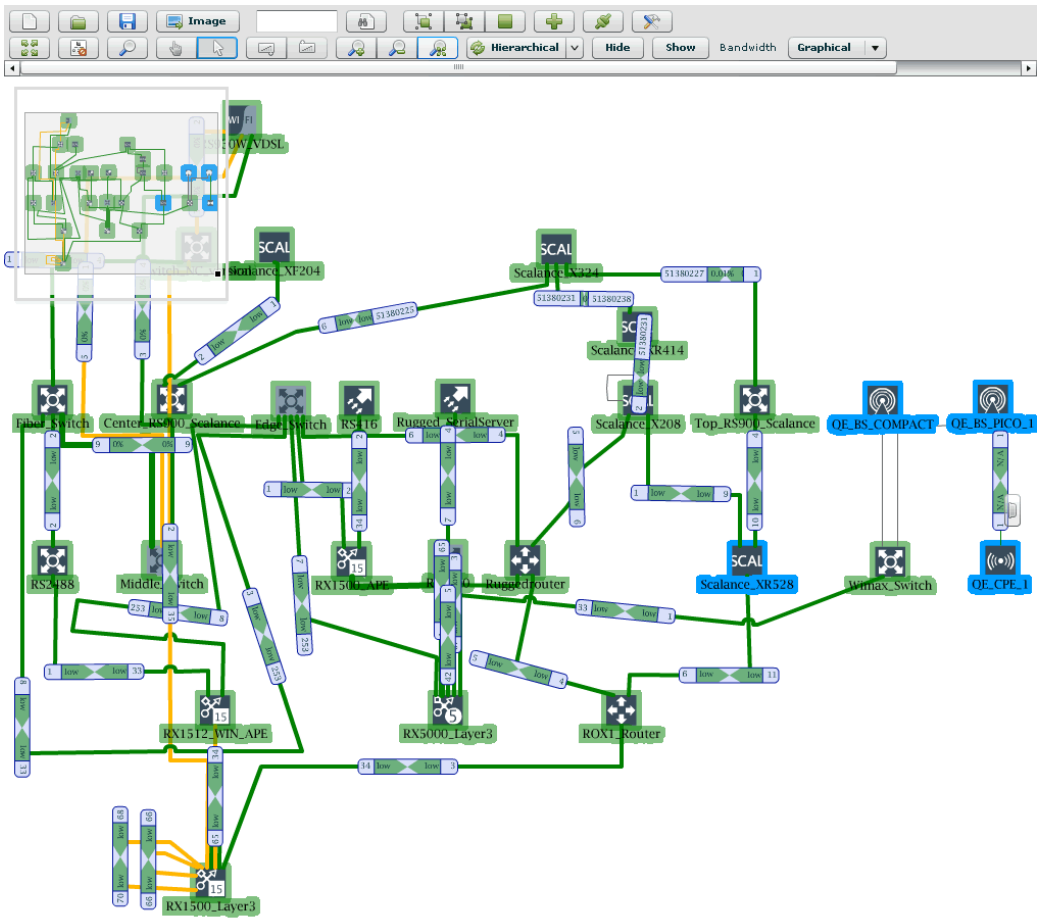


Figure 183: Example Hierarchical Layout

To apply a layout to an existing logical map, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .

   NOTE
   Refreshing a logical map may cause the map to be redrawn based on the current data available for each device. To avoid changing the arrangement of devices on a map, consider synchronizing it instead. For more information, refer to Section 5.5.10, "Synchronizing a Logical Map" .

2. Select the **Refresh Map and Recalculate Layout** control and choose either `Organic` or `Hierarchical`. The map is refreshed and all devices are rearranged.

Section 5.5.10

Synchronizing a Logical Map

Synchronizing a logical map updates the map with data collected by RUGGEDCOM NMS, and updates device and link status information for each device on the map. In comparison to refreshing a map, as described in Section 5.5.9, "Selecting a Layout" , synchronizing does not change the arrangement of the map.

Synchronization is typically done automatically by RUGGEDCOM NMS and in real-time. However, synchronizing a map manually can be done at any time if it is suspected the map is out-of-sync with the RUGGEDCOM NMS server.

To synchronize a logical map, click the **Synchronize** button on the toolbar.

Section 5.5.11

Exporting a Logical Map as an Image

To export a logical map as a PNG (Portable Network Graphic) or JPEG (Joint Photographic Experts Group) file, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .
2. Click **Export** on the toolbar. The **Export Image** dialog box appears.

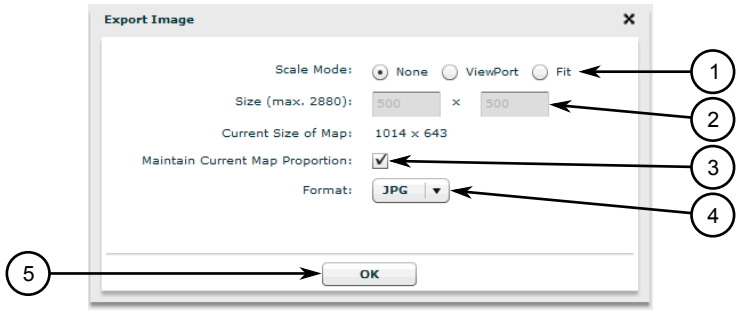


Figure 184: Export Image Dialog Box

1. Scale Mode Options **2.** Size Box **3.** Maintain Current Map Proportion Check Box **4.** Format List **5.** OK Button

3. Configure the following parameters as required:

Parameter	Description
Scale Mode	**Synopsis:** { none, ViewPort, Fit } **Default:** none The scale mode. Options include: • `none` – the image is not scaled • `ViewPort` – the image is scaled to the size of the view port • `Fit` – the image is scaled to fit
Size	The width and height of the image in pixels (px).
Maintain Current Map Proportion	When selected, the current proportions of the map are maintained.
Format	**Synopsis:** { JPG, PNG } **Default:** JPG The output format.

4. Click **OK**. A **Save As** dialog box appears.
5. Choose where to save the file and then click **Save**.

Section 5.5.12
Backing Up Logical Maps

Logical maps can be retrieved directly from the RUGGEDCOM NMS server's file system. Simply copy the following files from `/usr/share/opennms/ruggednms/netmap/maps` and save them in the desired location:

- {name}.graphml
- {name}.xml

Where *{name}* is the name of the map.

Section 5.5.13
Navigating a Logical Map

Navigating a large logical map is made easy using the following tools:

Using the Navigation Panel

The navigation panel appears in the upper left corner of the map, displaying a small-scale overview of the entire map. The gray box inside the panel indicates the portion of the logical map that is currently displayed on screen.

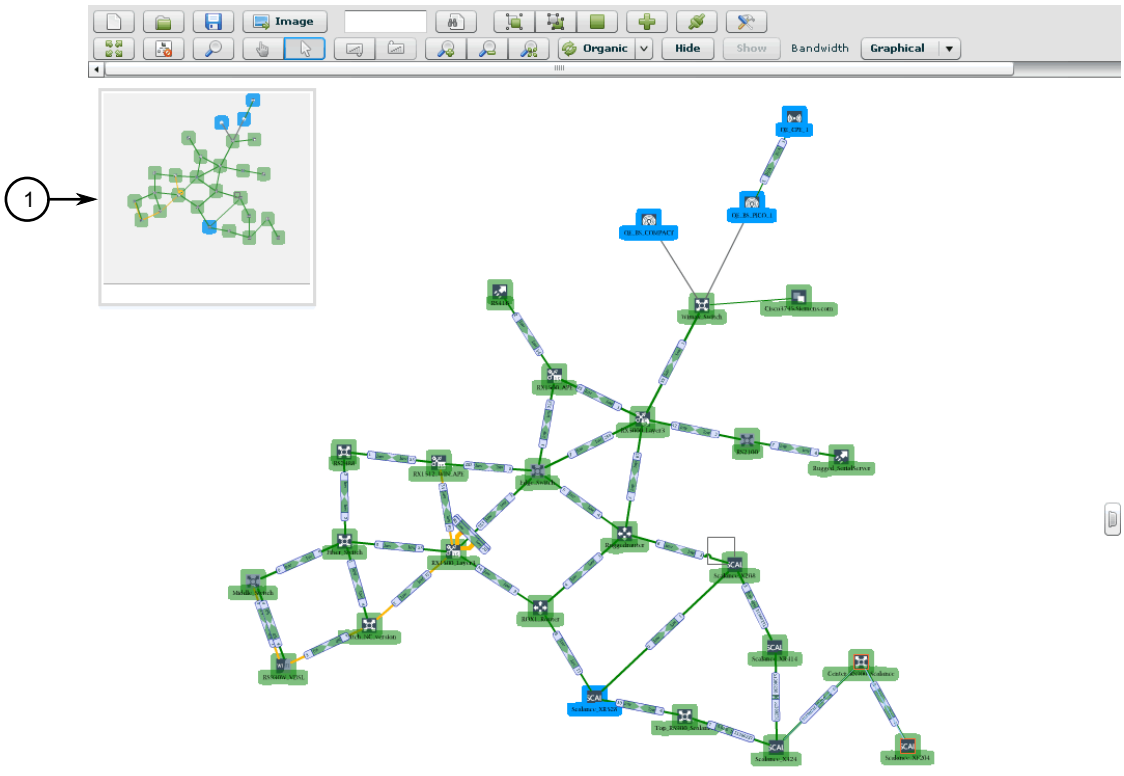


Figure 185: Navigation Panel

Dragging the gray box around the navigation panel moves the logical map on the screen. This allows users to quickly navigate from one side of a logical map to the other.

The navigation panel appears by default for all new logical maps. To hide or display the navigation panel, click the **Navigation Panel** button on the toolbar. For more information, refer to Section 5.5.2, "Logical Map Controls" .

» Using the Move Tool

Click the **Move Tool** button on the toolbar to change the mouse cursor to a pointer, then click and drag the logical map in the desired direction. When done, click the **Edit Tool** button.

For more information about the **Move Tool** and **Edit Tool** buttons, refer to Section 5.5.2, "Logical Map Controls" .

Section 5.5.14

Monitoring Bandwidth Usage

Part of RUGGEDCOM NMS's network monitoring feature, a network monitor gage can be displayed on each logical map to indicate the overall bandwidth usage of the network. When enabled for a map, a graphical gage appears in the upper-right corner of the logical map. The gage displays the percentage of bandwidth currently in use using the dial and also displays a numeric value.

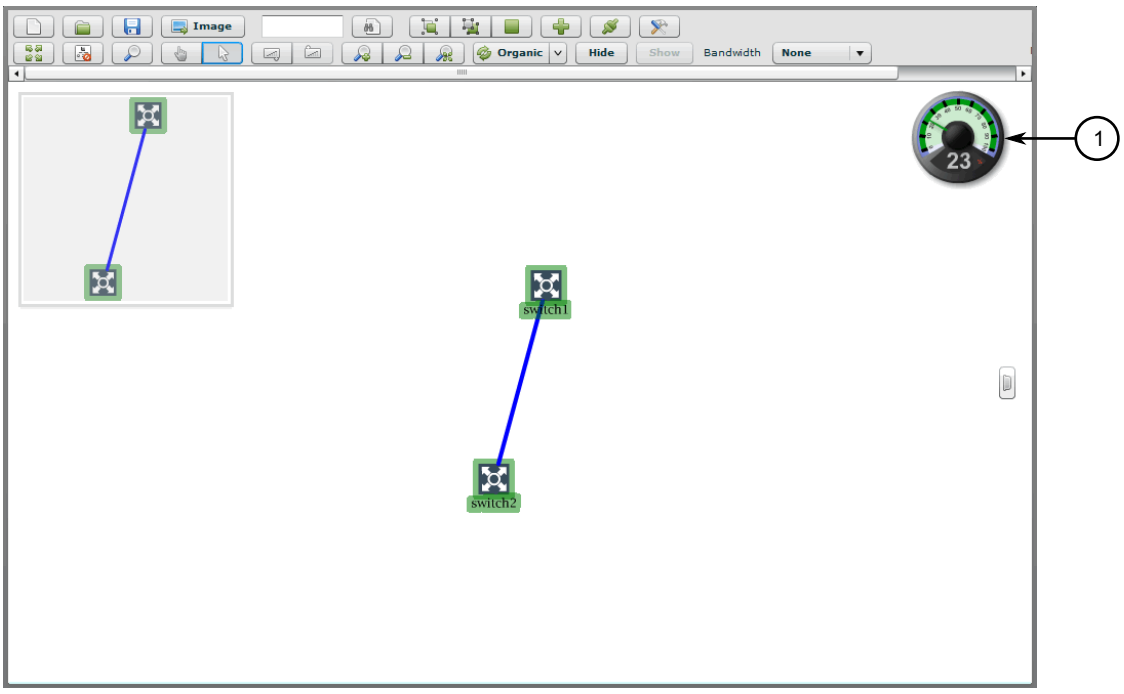


Figure 186: Network Monitor Gage

1. Network Monitor Gage

The network monitor gage can be displayed when configuring a logical map. For information about how to display/hide the network monitor gage, refer to Section 5.5.6, "Configuring a Logical Map" .

IMPORTANT!
The network monitor gage only shows when network monitoring is enabled and running. For more information about enabling network monitoring, refer to *Section 6.9.3, "Managing Network Monitoring"* .

The background color of the gage indicates the current bandwidth usage:

- Green – bandwidth usage is low. The default threshold range is 0 to 29%.
- Yellow – bandwidth usage is moderate. The default threshold is 30 to 60%.
- Red – bandwidth usage is high. The default threshold is 61% or higher.

The bandwidth usage thresholds are user configurable. For more information about changing the thresholds, refer to Section 6.9.3.4, "Configuring Network Monitoring" .

Section 5.5.15
Configuring the Datafeeder Polling Interval

To configure the interval at which RUGGEDCOM NMS updates link labels, do the following:

CAUTION!
Configuration hazard – risk of reduced performance. Reducing the polling interval may affect system performance.

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/datafeeder-config.xml`

2. Change the value for the *`snmp_poll_interval`* parameter. The default value is *`300000`* milliseconds (ms).

```
<?xml version="1.0" encoding="UTF-8"?>
<datafeeder-configuration
    max_threads="10"
    initial_sleep_time="60000"
    snmp_poll_interval="300000"
  butil="true"
  low="0.00001"
/>
```

3. Save and close the file.
4. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 5.5.16
Changing a Map Background

To replace the background of an existing logical map with an image or color, do the following:

IMPORTANT!
Background images must be resized to fit the map ***before*** *they are saved on the RUGGEDCOM NMS server. The size of the image cannot be larger than the map.*

1. For background images only, save the desired image on the RUGGEDCOM NMS server in the following directory:

```
/usr/share/opennms/ruggednms/netmap/images
```

2. Open an existing logical map. For more information, refer to Section 5.5.4, “Opening a Logical Map” .
3. Right-click the background of the map to open the shortcut menu and then click **Set Map Background**. The **Set Background** dialog box appears.

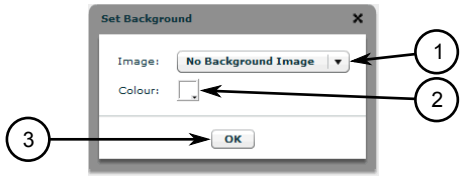


Figure 187: Set Background Dialog Box

1. Image List **2.** Color Selector **3.** OK Button

4. Either select a background image or select a color. The color can be one of the many pre-defined colors or a hex value.
5. Click **OK**.
6. Save the logical map. For more information, refer to Section 5.5.7, “Saving/Copying a Logical Map” .

Section 5.5.17

Managing Devices in a Logical Map

This section describes how to add, manage and customize devices in a logical map.

CONTENTS

Section 5.5.17.1

Adding Devices to a Logical Map

To add devices to an existing logical map, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, “Opening a Logical Map” .
2. On the toolbar, click **Add Device**. The **Add Device** dialog box appears.

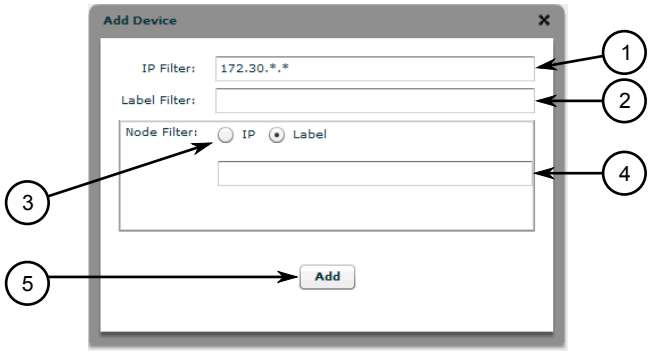


Figure 188: Add Device Dialog Box

1. IP Filter Box **2.** Label Filter Box **3.** Node Filter Options **4.** Node Filter Box **5.** Add Device Button

3. Under **IP Filter**, type the IP address for a device. Only devices managed by RUGGEDCOM NMS that are within the specified IP address range will appear in the map. Use an asterisk (*) as a wildcard to represent all numbers from 0 to 255.

   For example, `10.100.*.*` selects all devices in the range of addresses beginning with *10.00*.

4. Under **Label Filter**, type a full or partial device name. If required, use a percent sign (%) as a wildcard to match device names that begin and/or end with the specified string. Only devices with a matching name appear in the map.

   For example, `%switch%` matches all device names that include *switch*, such as *my_**switch*** , ***switch**_123*, but not *sw* or *swt*.

5. Under **Node Filter**, select either **IP** or **Label** and then type the exact IP address or name (label) of a device managed by RUGGEDCOM NMS. Only devices matching the specific criterion – and devices linked to them – will appear in the map.

   NOTE
   Pattern matches are not supported.

   NOTE
   The search criteria does not need to match the IP Filter or Label Filter criteria.

   For example, `switch_123` matches *switch_123*, but not *switch_1234*. Similarly, `10.100.10.111` matches *10.100.10.111*, but not *10.100.10.112*.

6. Click **Add**. The devices that match the selected criteria are added to the logical map.

Section 5.5.17.2
Searching for Devices in a Logical Map

To search for devices in a logical map, do the following:

NOTE
*Devices are found based on their device label. For example, search for the term **switch** will match **switch101** and **ip-192.168.0.50-switch**.*

» Searching for Devices at the Map Level

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .

   NOTE
   Devices in a group are hidden from the search until the group is unfolded.

2. [Optional] Make sure all groups are unfolded.
3. On the toolbar, type a value in the search field and then click the **Find Device** button. The map focuses on and highlights the first device on the map whose label matches the search criteria.
4. [Optional] Click the **Find Device** button again to search for the next device.

» Searching for Devices Within a Group

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .
2. Select the desired group and then click the **Enter Group** icon.
3. On the toolbar, type a value in the search field and then click the **Find Device** button. The map focuses on and highlights the first device in the group whose label matches the search criteria.
4. [Optional] Click the **Find Device** button again to search for the next device.

Section 5.5.17.3
Moving Devices on a Logical Map

To move a device on a logical map, do the following:

1. Select the device.
2. Place the cursor over the selected device until the *move* cursor appears.

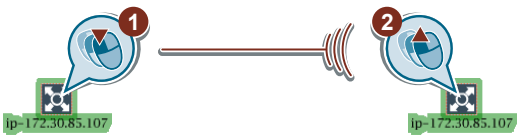


Figure 189: Moving a Device

3. Click and drag the device.

Section 5.5.17.4
Viewing Events, Reports and Assets Information

To view events, reports and asset information for a device on a logical map, do the following:

Viewing Events

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map".
2. Right-click the device to open the shortcut menu and click **View Events**. The **List** screen appears in a new browser window or tab listing the all notifications and events related to the device.

   For more information about events, refer to Section 5.2.2, "Managing Events".

Viewing Reports

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map".
2. Right-click the device to open the shortcut menu and click **Show Available Reports**. The **Choose** screen appears in a new browser window or tab offering a resource to graph.
3. Perform Step 2 to Step 4 in Section 5.4.2.1, "Generating Standard Reports" to generate the standard resource report.

Viewing Asset Information

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map".
2. Right-click the device to open the shortcut menu and click **Show Assets**. The **Modify** screen appears in a new browser window or tab detailing the asset information for the device.

   For more information about asset information, refer to Section 6.4.9, "Managing Asset Information".

Section 5.5.17.5
Changing the Device Label

Each device is automatically assigned a label for quick identification. The label can be used in whole or in part to search for the device within RUGGEDCOM NMS and on a logical map.

To customize the label for a device, the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map".
2. Right-click the desired device to open the shortcut menu and then click **Change Device Label**. The **Node Label** screen appears in a new browser window or tab.

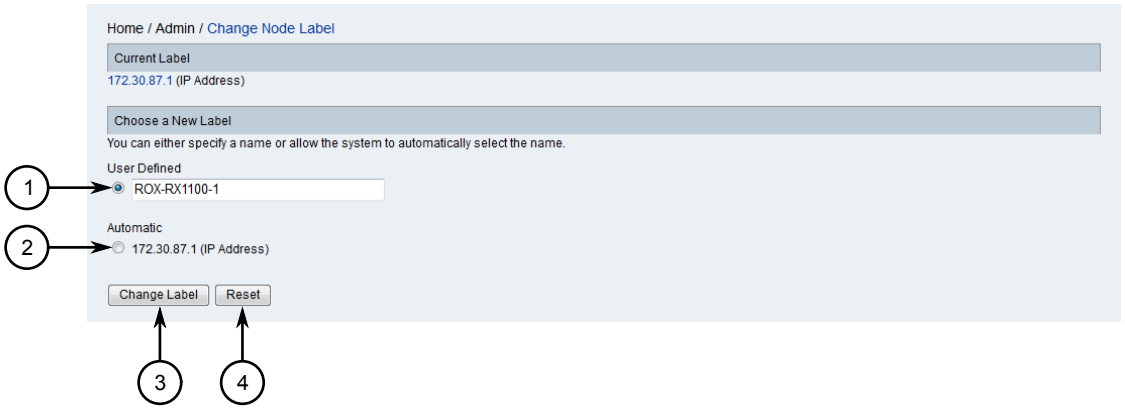


Figure 190: Node Label

1. User Defined Box and Option **2.** Automatic Option **3.** Change Label Button **4.** Reset Button

3. Select either the **User Defined** or **Automatic** option.
4. If the **User Defined** option is selected, type a custom name for the device.
5. Click **Change Label**.

Section 5.5.17.6

Customizing Device Icons

Each type of device is represented by a standard icon on a logical map, which can be customized to suit the user or organization's needs. For information about the standard icons, refer to Section 5.5.3, "Icons and OID Mapping".

To customize the icon for a device, do the following:

IMPORTANT!
The dimensions of custom icons must not exceed 125 pixels in height or width.

1. [Optional] If using a custom icon, save the desired image on the RUGGEDCOM NMS server in the following directory:

   `/usr/share/opennms/ruggednms/netmap/icons`

   The image will appear in the list of available icons.
2. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map".
3. Right-click the desired device to open the shortcut menu and then click **Change Icon**. The **Change Device Icon** dialog box appears.

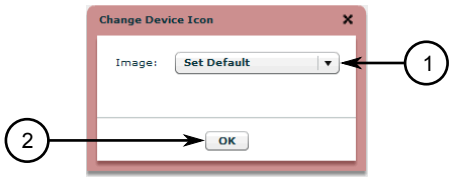


Figure 191: Change Device Icon Dialog Box

1. Image List **2.** OK Button

4. Under **Image**, select an icon and then click **OK**. The selected icon is applied to the device.

Section 5.5.17.7

Pinging a Device

To ping a device from a logical map, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .
2. Right-click a device to open the shortcut menu and then click **Ping**. A dialog box opens.

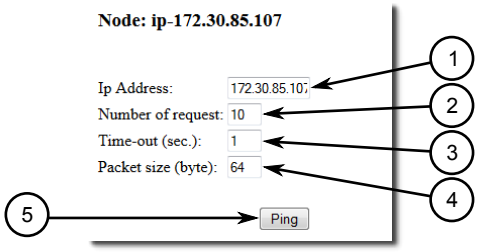


Figure 192: Ping Dialog Box

1. IP Address Box **2.** Number of Request Box **3.** Time-Out Box **4.** Packet Size Box **5.** Ping Button

3. Configure the following parameters as required:

Parameter	Description
Number of Request	**Default:** 10 The maximum number of times to ping the device.

Parameter	Description
Time-Out	**Default:** 1 The time in seconds (s) to wait for a response from the device after each ping.

Parameter	Description
Packet Size	**Default:** 64

Parameter	Description
	The size of the packet – in bytes – to send to the device with each ping.

4. Click **Ping**. The dialog box closes and new dialog box opens displaying the results of the ping request.

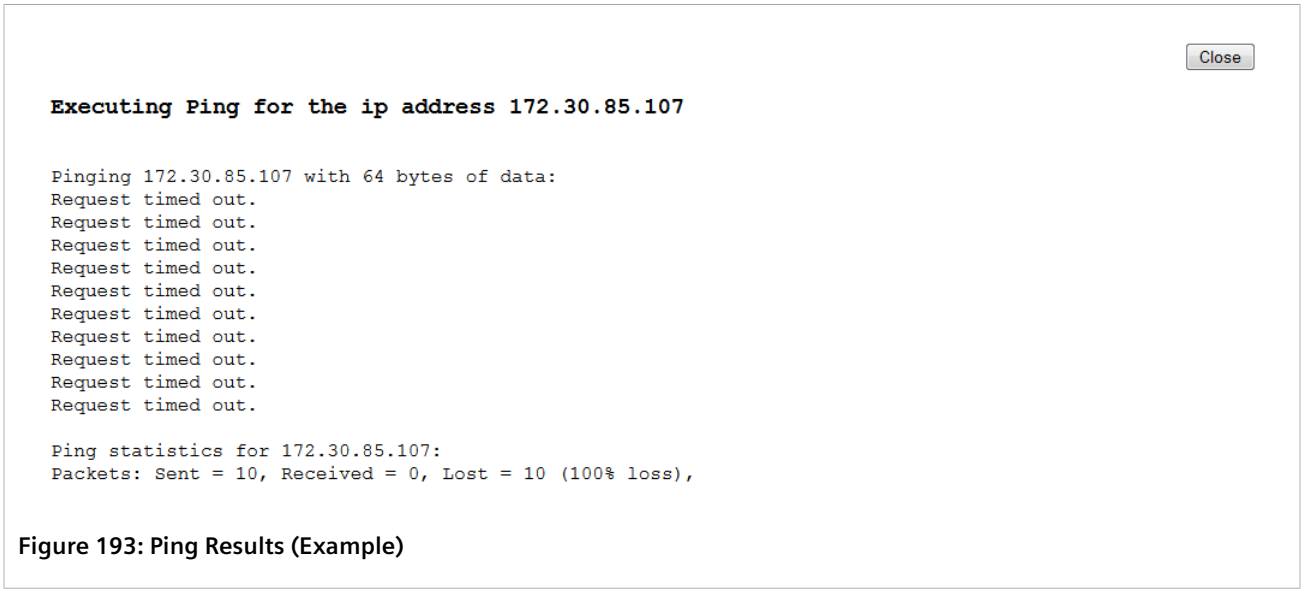


Figure 193: Ping Results (Example)

Section 5.5.17.8
Tracing a Device

To trace the route between the RUGGEDCOM NMS server and a device, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .
2. Right-click a device to open the shortcut menu and then click **Traceroute**. A dialog box opens.

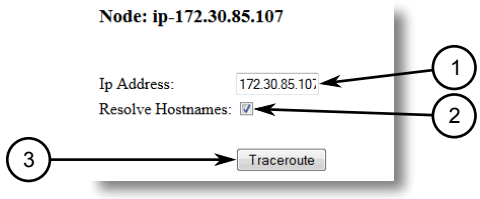


Figure 194: Trace Route Dialog Box

1. IP Address Box **2.** Resolve Hostnames Check Box **3.** Traceroute Button

3. [Optional] Select or clear **Resolve Hostnames**.
4. Click **Traceroute**. The dialog box closes and new dialog box opens displaying the results of the trace.

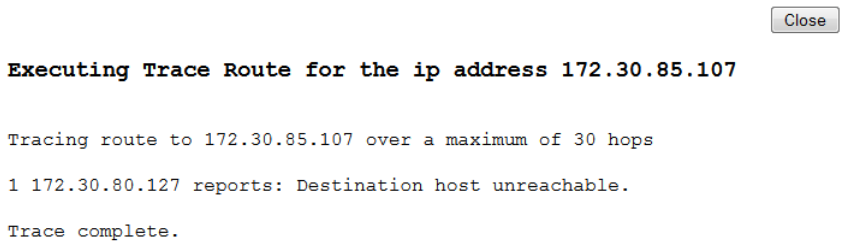


Figure 195: Trace Results (Example)

Section 5.5.17.9
Repositioning a Device Label

Device labels can be repositioned around the device icon to make it easier for devices to fit on a logical map.

To reposition a device label, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, “Opening a Logical Map” .
2. Select the label for a device.
3. Click and drag the label to any one of the eight positions that appear on screen.

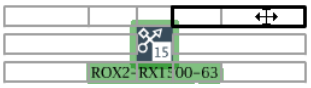


Figure 196: Repositioning a Device Label

Section 5.5.18
Managing Device Groups

Complex maps are made easier to work with when multiple devices are represented by a device group, which can be placed on a map as a single point. Device groups are also used in other areas of RUGGEDCOM NMS, such as configuring gold configurations.

On a logical map, a device group is represented by a group icon.

Figure 197: Group Icon

The group icon displays the most severe status indication of all the devices in the group as the status of the entire group. For example, if one device in the group is down, the status of the entire group is shown as *Node Down*. For

more information about how the status of devices is displayed on a logical map, refer to Section 5.5.3, "Icons and OID Mapping" .

To status of individual devices within the group can be determined by *unfolding* the group and viewing the icons for the individual nodes.

Groups can also be combined into super groups or broken up into subgroups. This provides great flexibility to simplify complex logical maps.

IMPORTANT!
A device can only belong to one group. However, if that group is part of a super group, the super group can reference the device. Assigning a device to a different group will remove it from its current group.

CONTENTS

Section 5.5.18.1
Assigning Devices to a Group

To assign devices to a group, do the following:

1. Open an existing logical map or add a new map. For more information, refer to Section 5.5.4, "Opening a Logical Map" or Section 5.5.5, "Adding a Logical Map" .
2. Using the **Edit** tool, click and drag a bounding box around the devices to include in the group.
3. Click the **Group** button. The **Assign to Logic Group** dialog box appears, with the default name *ungrouped* as the name of the group.

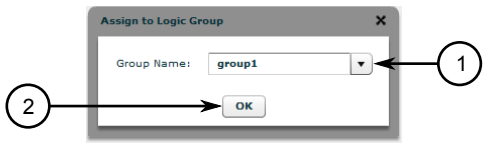


Figure 198: Assign to Logic Group Dialog Box

1. Group Name Box **2.** OK Button

IMPORTANT!
*Do not use the default word **ungrouped** as the name of the group. All devices will be removed from the group.*

4. Under **Group Name**, either type a name for a new group or select an existing group from the list.
5. Click **OK**. The selected devices collapse into a single icon on the map. The name of the group appears below the icon.

Section 5.5.18.2
Creating a Super Group

In addition to placing individual devices into groups, groups themselves can also be assigned to a group referred to as a *super group*.

There are two methods for creating a super group.

Method 1: Assign Existing Groups to a Super Group

To assign existing groups to a super group, do the following:

1. Open an existing logical map or add a new map. For more information, refer to Section 5.5.4, "Opening a Logical Map" or Section 5.5.5, "Adding a Logical Map" .
2. Make sure more than one group is available on the map. For more information about adding groups, refer to Section 5.5.18.1, "Assigning Devices to a Group" .
3. Using the **Edit** tool, click and drag a bounding box around the groups to include in the super group.
4. Click the **Group** button. The **Assign to Logic Group** dialog box appears.

Figure 199: Assign to Logic Group Dialog Box

1. Group Name Box **2.** OK Button

5. Under **Group Name**, either type a name for a new super group or select an existing super group from the list.
6. Click **OK**. The selected groups collapse into a single icon on the map. The name of the super group appears below the icon.

Method 2: Group Devices Within a Group

To take devices already grouped together in a large group and group them into smaller groups, do the following:

1. Open an existing logical map or add a new map. For more information, refer to Section 5.5.4, "Opening a Logical Map" or Section 5.5.5, "Adding a Logical Map" .
2. Unfold the desired group to display the devices it contains. For more information, refer to Section 5.5.18.3, "Displaying Devices Within Groups" .
3. Using the **Edit** tool, click and drag a bounding box around the desired groups.
4. Click the **Group** button. The **Assign to Logic Group** dialog box appears. Refer to Figure 199 .
5. Under **Group Name**, either type a name for a new super group or select an existing super group from the list.
6. Click **OK**. The selected groups collapse into a single icon within the main group, which is now a super group. The name of the new group appears below the icon.

Section 5.5.18.3
Displaying Devices Within Groups

The following describe the methods for accessing/viewing devices that are grouped together.

- **Folding/Unfolding Groups**
  Folding and *unfolding* are the terms used to describe collapsing and expanding groups to show/hide the devices or groups within.

  To fold (collapse) or unfold (expand) a group, select the group icon on the map and then click the **Fold/Unfold** button.

  When unfolded (expanded), all the devices belonging to the group sit on a blue background.

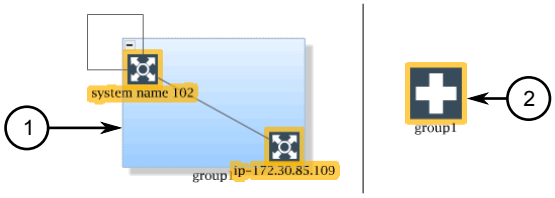


Figure 200: Folded and Unfolded Group Icons

1. Unfolded Group **2.** Folded Group

- **Using the Group Filter**
  Click the tab on the right-side of the map to display the **Group Filter** side menu. This menu lists the available groups.

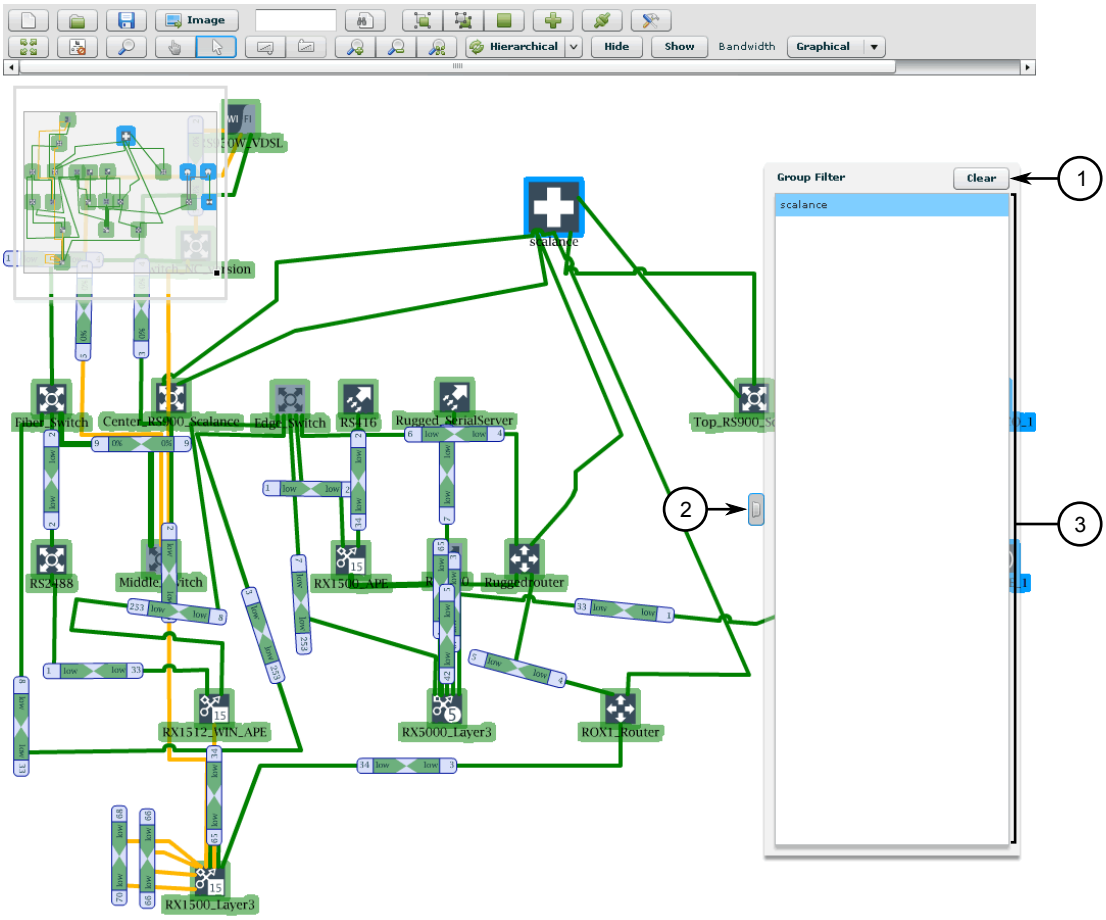


Figure 201: Group Filter

1. Clear Button **2.** Tab **3.** Available Groups

To view the devices in one of the groups, simply select the group from the list. An individual map of the devices in the group is displayed.

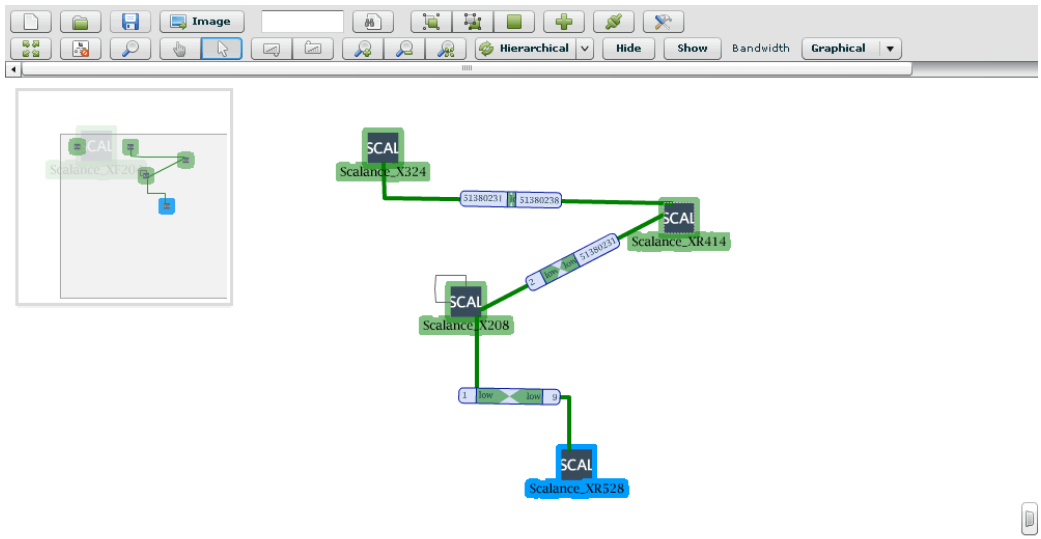


Figure 202: Displaying Only the Devices Within a Group

To display the main map, click **Clear**.

To close the **Group Filter** side menu, click the tab.

- **Entering/Exiting Groups**
  Similar to using the **Group Filter**, the **Enter Group** and **Exit Group** buttons on the toolbar can be used to display and close an individual map of the devices in a group.

  To display an individual map of the devices within a group, select group and then click the **Enter Group** button. Refer to Figure 202 .

  To display the main map, click **Exit Group**.

Section 5.5.18.4
Ungrouping Devices

To ungroup a set of devices, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, “Opening a Logical Map” .
2. If the desired group is part of a super group, first unfold the super group. For more information about unfolding groups, refer to Section 5.5.18.3, “Displaying Devices Within Groups” .
3. Select the desired group and then click the **Ungroup** button.

Section 5.5.19
Managing Links

Lines connecting devices on a logical map represent links between those devices. Each link conveys the connection status and displays the network traffic as either a percentage or in bits/second (bps).

For information about how to change the unit of measure used to display network traffic, refer to Section 5.5.6, "Configuring a Logical Map" .

NOTE
When several devices are grouped together and folded, some links extending from the group may overlap one another. Simply refresh the map to correct the problem.

CONTENTS

Section 5.5.19.1
Link Colors, Labels and Tool Tips

Links provide information with line color, graphical labels, textual labels and tool tips.

Link Colors

The color of a link indicates the current status of the connection between two devices.

NOTE
At least one device in the pair must support a standard interface MIB for RUGGEDCOM NMS to detect the status of their connection with one another.

Link Color	Condition	Description
Red	Link Down	Indicates the link between the devices is down. This can be detected with a trap if NSMP is configured on the device, or through a regular scan. RUGGEDCOM NMS also regularly scans the network to detect such outages.
Yellow	Blocking Link	Indicates the link does not transfer any data (reserved link).
Green	Link Up	Indicates the link is fully functional.
Blue	Link Event	Indicates there is a new network monitor event.

Link colors can be customized to suit the needs of the organization or user. For more information, refer to Section 5.5.6, "Configuring a Logical Map" .

Graphical Labels

Graphical link labels display the bandwidth utilization between the ports of each device. For the map to display this information, devices must have SNMP enabled.

Link labels are displayed only when a link has a status of *Link Up* and the database contains information for calculating the bandwidth utilization. Graphical labels can display bandwidth usage between 0.00001% to 100%

of the port's capacity. Bandwidth usage below 0.00001% of the port's capacity will not appear in the label. The bandwidth utilization is calculated dynamically by RUGGEDCOM NMS every five minutes for all devices that provide the required information via SNMP. For information about changing this polling period, refer to Section 5.5.15, "Configuring the Datafeeder Polling Interval" .

To display graphical link labels, select `Graphical` from the **Bandwidth** list on the logical map toolbar. For more information, refer to Section 5.5.2, "Logical Map Controls" .

The following is an example of a graphical link label:

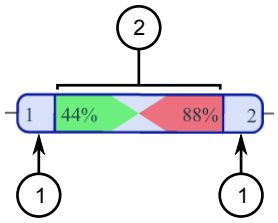


Figure 203: Graphical Link Label

1. Ports **2.** Outgoing/Incoming Bandwidth

The label displays the connected ports (based on the SNMP Interface Index or ifIndex) and the bandwidth utilization in both directions.

In this example, the bandwidth utilization is read as follows:

- At port 1, the outgoing bandwidth is 44% and the incoming bandwidth is 88%
- At port 2, the outgoing bandwidth is 88% and the incoming bandwidth is 44%

Colors also indicate when the bandwidth exceeds specific usage thresholds. For instance:

- **Green** – indicates 0 to 10% usage
- **Yellow** – indicates 10 to 20% usage
- **Red** – indicates 20% or higher usage

For very low utilization levels, graphical labels display bandwidth utilization as follows:

- For usage lower than 0.00001%, the label displays 0%
- For usage higher than 0.00001%, but less than 0.01%, the label displays *low*

Figure 204: Graphical Link Label Indicating Very Low Usage

- For usage higher than 0.01%, the label displays the usage percentage in each direction

Bandwidth utilization colors and thresholds can be customized to suit the organization or user. For more information, refer to Section 5.5.6, "Configuring a Logical Map" .

Textual Labels

Textual link labels display the highest current bandwidth utilization between the two devices and its direction.

The following is an example of a textual link label:

Figure 205: Textual Link Label

This label indicates the bandwidth utilization is highest in the direction indicated by the < character and is currently 0.04% of the total link capacity.

When the bandwidth utilization is the same in both directions, the label displays both < and > characters (e.g. > 0% <).

Textual link labels display bandwidth usage as follows:

- For usage lower than 0.00001%, the label displays 0%
- For usage higher than 0.00001%, but less than 0.01%, the label displays < *low*
- For usage higher than 0.01%, the label displays the usage percentage

The thickness of the line will also increase/decrease if the label knows the speed of the physical connection between the two devices.

The thickness of textual link labels and thresholds can be customized to suit the organization or user. For more information, refer to Section 5.5.6, “Configuring a Logical Map” .

Tool Tips

Tool tips appear when the mouse cursor is placed over a link label (graphical or textual). By default, the tool tip details the link speed, port number and interface name, bandwidth utilization, and link type information.

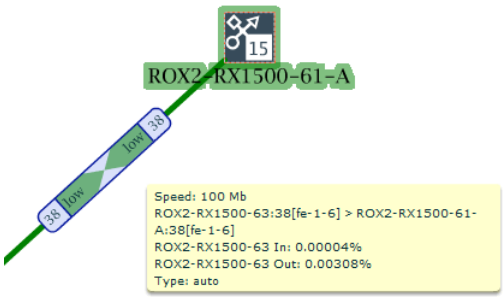


Figure 206: Tool Tip

Section 5.5.19.2

Adding a Link Manually

When RUGGEDCOM NMS is unable to detect the link between two devices, a link can be drawn manually on a logical map by dragging a line between the two devices.

NOTE
At least one device in the pair must support a standard interface MIB for RUGGEDCOM NMS to detect the status of their connection with one another.

To manually create a link between two devices, do the following:

1. Open an existing logical map. For more information, refer to Section 5.5.4, "Opening a Logical Map" .
2. Select the center of the first device and drag a line to the center of the second point.

Figure 207: Drawing a Link Between Two Devices

   A thin black line appears between the two devices. This line is temporary until the map is saved.
3. Save the logical map. For more information, refer to Section 5.5.7, "Saving/Copying a Logical Map" .

Each manually created link is unmanaged, meaning it will not display the link status or bandwidth utilization.

To convert an unmanaged link to a managed link that does display the link status and bandwidth utilization, do the following:

IMPORTANT!
At least one of the devices must support SNMP.

1. Right-click the link to open the shortcut menu and then click **Configure Manual Link**. The **Manual Link Configuration** dialog box appears.

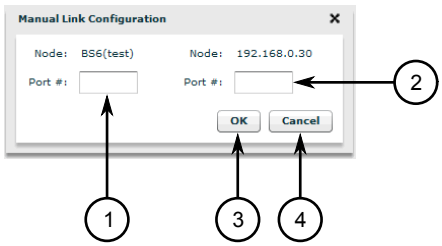


Figure 208: Manual Link Configuration Dialog Box

1. Port # Box **2.** OK Button **3.** Cancel Button

2. Under **Port #** for both devices, enter the ifIndex of the device's management port. The ifIndex is listed in the device details under RUGGEDCOM NMS. For information about viewing the device details, refer to Section 6.4.2, "Viewing Device Details" .
3. Click **OK**.

Section 5.5.19.3

Bending a Link

When several nodes are grouped and folded in a logical map, some links extending from the group may overlap each other. These links can cleaned up by *bending* them along a different path and making the map more presentable.

To bend a link in a logical map, click anywhere along the link and drag the line in the desired direction. A node is created at the point where the line is selected and the line will bend as needed at that point.

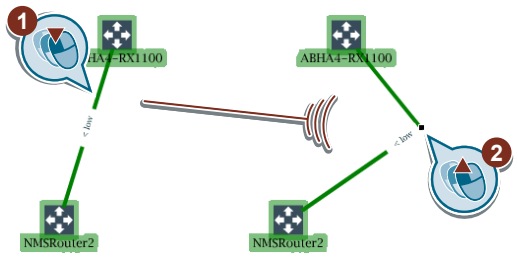


Figure 209: Bending Links

Section 5.5.19.4

Removing a Link Manually

To remove a link that was added manually, select the link and press **Delete**.

NOTE
When selecting a link, select the ends of the link rather than the middle. Clicking on the center of a link may select an invisible bandwidth utilization label instead.

Section 5.6

Managing Geographical Maps

Use the geographical mapping feature to map the physical location of each RUGGEDCOM WIN base station controlled by RUGGEDCOM NMS and view their current status. Simply upload one or more map images in BMP, JPG, GIF or PNG format and then add base stations.

The base station icons indicate the status of each base station by changing their background color. Green indicates the base stations are running normally, amber indicates the base station has notifications to view, and red indicates the base station has been de-registered.

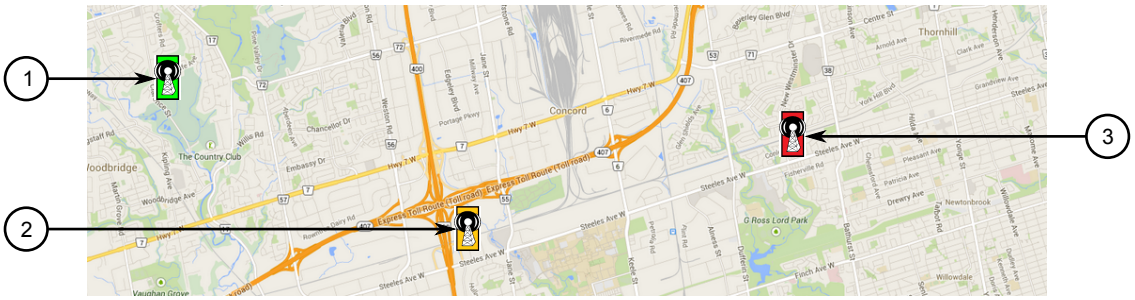


Figure 210: Base Station Status Icons

1. Green (Normal) **2.** Amber (Notifications) **3.** Red (De-Registered)

Multiple maps can be saved and shared with other users.

CAUTION!
Configuring hazard – risk of data loss. Multiple users can view and modify the same map at the same time. If two users are modifying the same map, the last user to save their changes will overwrite the changes made by the other user. Always modify maps in cooperation with other users to prevent the loss of data.

CONTENTS

Section 5.6.1

Geographical Map Controls

Each geographical map features a toolbar that provides the following controls:

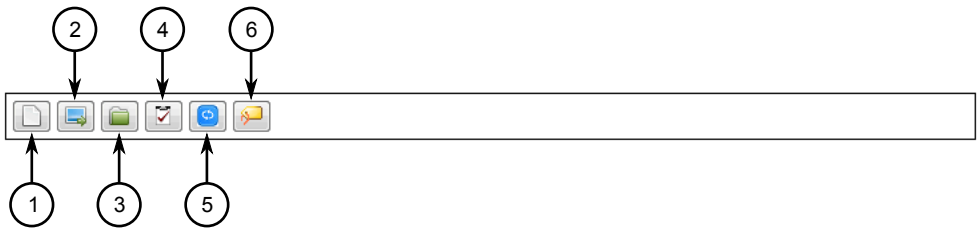


Figure 211: Geographical Map Toolbar

1. Create Map Button **2.** Open Map Image Button **3.** Open Map Button **4.** List Unassociated Base Stations Button **5.** Refresh Button **6.** Display Site Name Labels Button

Icon	Name	Description
	Create Map	Creates a new geographical map.
	Open Map Image	Opens a dialog box that allows users to add, delete and upload map images.

Icon	Name	Description
	Open Map	Opens a dialog box that allows users to open, delete and save maps.
	List Unassociated Base Stations	Opens a dialog box that lists base stations that do not have a site ID configured.
	Refresh	Refreshes/reloads the current map. Use this if another user has modified the map.
	Display Site Name Labels	Hides or displays site name labels for base stations on the map.

Section 5.6.2

Configuring Default Settings

To configure the default settings for new geographical maps, do the following:

NOTE
Changes to the default settings only affect new geographical maps. Settings for existing maps must be changed individually.

1. On the toolbar, click **Admin** and click **Configure Geographical Map**. The **Configure Geographical Map** screen appears.

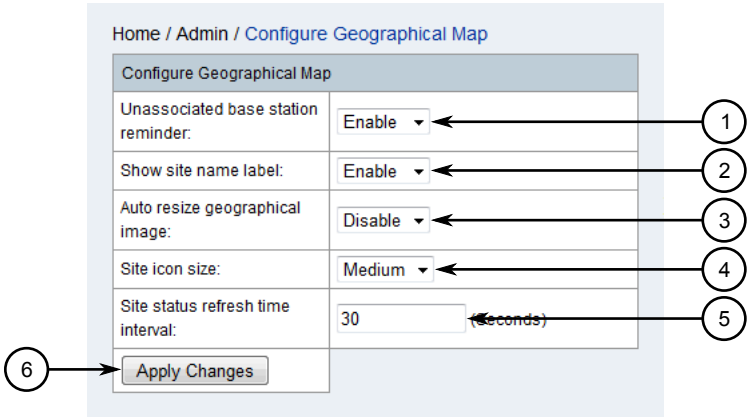


Figure 212: Configure Geographical Map Screen

1. Unassociated Base Station Reminder List **2.** Show Site Name Label List **3.** Auto Resize Geographical Image List **4.** Site Icon Size List **5.** Site Status Refresh Time Interval Box **6.** Apply Changes Button

2. Configure the following parameter(s) as required:

> **NOTE**
> *If the **Unassociated base station reminder** parameter is enabled and one or more base stations have not been assigned a site ID, RUGGEDCOM NMS displays a notice each time geographical mapping is launched listing the base stations that have not been assigned a site ID. Site IDs are assigned individually through the RUGGEDCOM WIN BST Web Manager. For more information, refer to the RUGGEDCOM WIN BST Web Manager User Guide for the base station.*

Parameter	Description
Unassociated base station reminder	**Synopsis:** { Enable, Disable } **Default:** Enable Enables/disables the unassociated base station reminder. When enabled, the reminder will appear when the Geographical Map feature is launched.
Show site name label	**Synopsis:** { Enable, Disable } **Default:** Enable Enables/disables the default for the site name label display setting for new geographical maps.
Auto resize geographical image	**Synopsis:** { Enable, Disable } **Default:** Disable Enables/disables automatic resizing of the geographical image to fit the screen. Using this option may alter the general look of the original image.
Site icon size	**Synopsis:** { Small, Medium, Large } **Default:** Medium Allows the user to select the site icon size on the map.
Site status refresh time interval	**Synopsis:** 1 to 2147483647 s **Default:** 30 s Sets the time interval to update site status information from the base stations.

3. Click **Apply Changes**.

Section 5.6.3
Opening a Geographical Map

To open a geographical map, do the following:

1. On the menu bar, click **Geographical Map**. The **RUGGEDCOM NMS Geographical Map** screen appears in a new window.
2. Click the **Open Map** button on the geographical map toolbar. A dialog box appears.

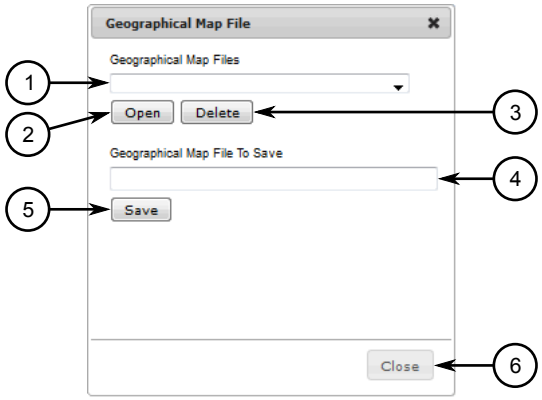


Figure 213: Dialog Box

1. Geographical Map Files List **2.** Open Button **3.** Delete Button **4.** Geographical Map File to Save Box **5.** Save Button

3. Select a map from the **Geographical Map Files** list and then click **Open**.

Section 5.6.4
Adding a Geographical Map

To add a new geographical map, do the following:

1. If already viewing an existing map, click the **Create Map** button on the geographical map toolbar. A blank map workspace appears.

   Otherwise, on the menu bar, click **Geographical Map**. The **RUGGEDCOM NMS Geographical Map** screen appears in a new window.
2. Add a map image. For more information, refer to Section 5.6.5, "Selecting, Uploading and Deleting Map Images" .
3. Add base station sites to the map. For more information, refer to Section 5.6.9.1, "Adding Sites" .
4. Save the map. For more information, refer to Section 5.5.7, "Saving/Copying a Logical Map" .

Section 5.6.5
Selecting, Uploading and Deleting Map Images

To select, upload or delete a map image, first select the **Open Map Image** button from the geographical map toolbar. A dialog box appears.

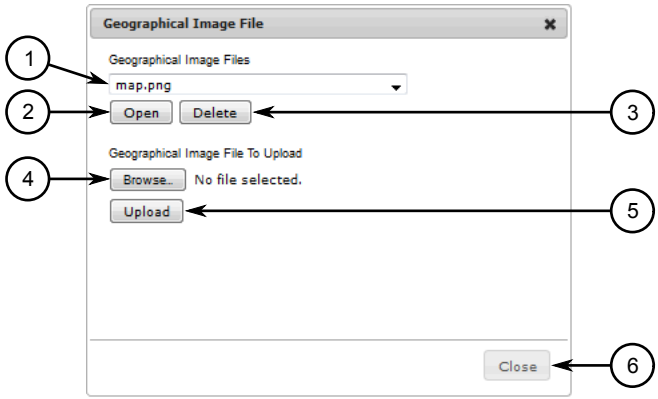


Figure 214: Dialog Box

1. Geographical Images List **2.** Open Button **3.** Delete Button **4.** Geographical Image File to Upload **5.** Browse Button **6.** Upload Button

NOTE
Map images cannot be removed or replaced once added to a map.

Selecting a Map Image

To select a map image for a new map, do the following:

1. Select a map image from the **Geographical Images** list.
2. Click **Open**.

Uploading a Map Image

To upload a map image, do the following:

1. Click **Browse** and select the map image to upload. Only BMP, JPG, GIF and PNG formats are permitted.
2. Click **Upload**.

Deleting a Map Image

To delete a map image, do the following:

1. Select a map image from the **Geographical Images** list.
2. Click **Delete**. A confirmation dialog box appears.
3. Click **Yes** to delete the image, or click **No** to cancel.

Section 5.6.6

Saving and Deleting Geographical Maps

To save or delete a geographical map, first select the **Open Map** button from the geographical map toolbar. A dialog box appears.

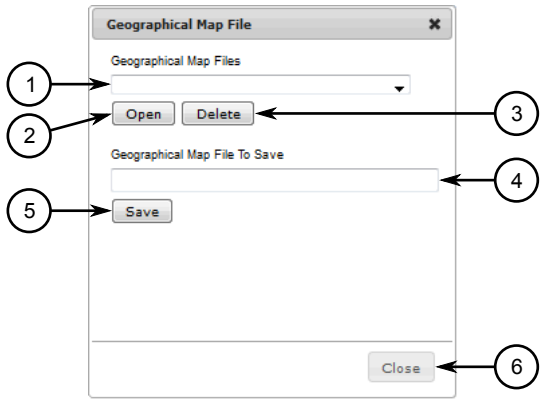


Figure 215: Dialog Box

1. Geographical Map Files List **2.** Open Button **3.** Delete Button **4.** Geographical Map File to Save Box **5.** Save Button

Saving a Map

To save a map, do the following:

1. In the **Geographical Map File To Save** box, type a unique name for the map.
2. Click **Save**. A confirmation dialog box appears.
3. Click **Yes** to save the map, or click **No** to cancel.

Deleting a Map

To delete a map, do the following:

1. Select the map from **Geographical Map Files** list.
2. Click **Delete**. A confirmation dialog box appears.
3. Click **Yes** to delete the map, or click **No** to cancel.

Section 5.6.7

Display/Hiding Site Labels

To display site labels on a geographical map, click the **Display Site Name Labels** button in the geographical map toolbar.

NOTE
Site labels can also be set to display by default when a new map is created. For more information, refer to *Section 5.6.2, "Configuring Default Settings"* .

Section 5.6.8
Identifying Unassociated Base Stations

Click the **List Unassociated Base Stations** button on the geographical map toolbar to display a list of base stations that do not been assigned a site ID. A site ID is required for RUGGEDCOM NMS to add the base station to a map. Site IDs are assigned individually through the RUGGEDCOM WIN BST Web Manager. For more information, refer to the *RUGGEDCOM WIN BST Web Manager User Guide* for the base station.

Section 5.6.9
Managing Sites

Sites on a geographical map represent the physical locations of base stations managed by RUGGEDCOM NMS. They indicate the status of each base station and allow for quick access to important information about the site.

CONTENTS

Section 5.6.9.1
Adding Sites

To add a base station site to a geographical map, do the following:

1. Open the geographical map. For more information, refer to Section 5.6.3, "Opening a Geographical Map" .
2. Right-click on the map in the area where the site is located. A dialog box appears.

Figure 216: Adding a Site

1. Site Names List **2.** OK Button **3.** Close Button

3. Under **Site Names**, select a site and then click **OK**.

Section 5.6.9.2
Moving Sites

To move a base station site on a geographical map, left-click and drag the icon to a new location on the map.

Section 5.6.9.3
Viewing the Status of Base Stations

At a high-level, the overall status of a base station is indicated by the background color of its site icon. Green indicates the base station is running normally, amber indicates the base station has notifications to view, and red indicates the base station has been de-registered.

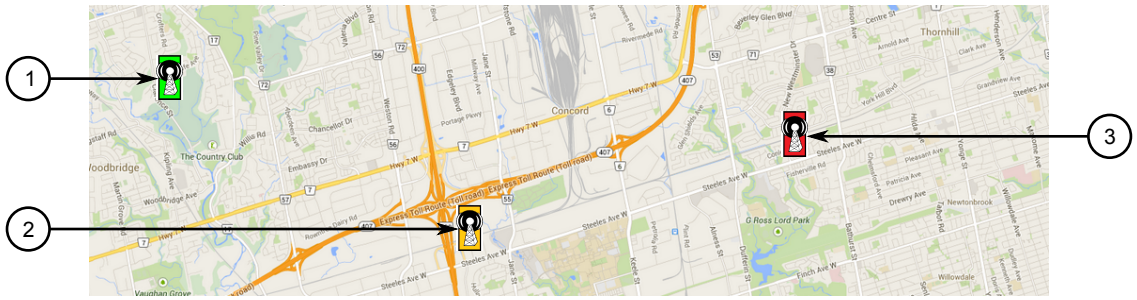


Figure 217: Base Station Status Icons

1. Green (Normal) **2.** Amber (Notifications) **3.** Red (De-Registered)

For further information, right-click on the site icon to display a shortcut menu. The shortcut menu provides the following links:

- **Notifications** – Links to a list of notifications associated with the base station.
- **Base Station Information** – Links to the base station's node information.
- **Logical Map** – Links to a hierarchical or organic map showing the logical arrangement of the base station and other nodes. For more information about logical maps, refer to Section 5.5, "Managing Logical Maps" .

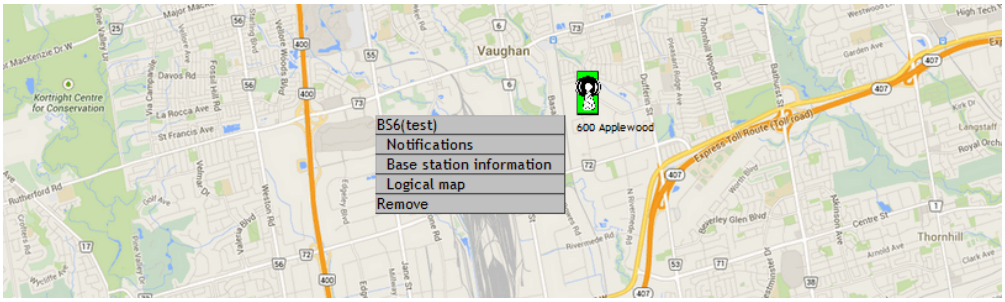


Figure 218: Shortcut Menu

Section 5.6.9.4
Deleting Sites

To delete a base station site from a geographical map, do the following:

1. Open the geographical map. For more information, refer to Section 5.6.3, "Opening a Geographical Map" .
2. Right-click on the site icon. A shortcut menu appears.
3. Select **Remove**. The site icon is deleted from the map.

6 Managing/Configuring Devices

This chapter describes how to setup and configure devices managed by RUGGEDCOM NMS.

CONTENTS

Section 6.1

Viewing the Configuration Management Log

The Configuration Management Log file displays in chronological order (oldest to latest) the upload, download, upgrade, gold configuration conflicts, and error history for all devices managed by RUGGEDCOM NMS.It is a useful tool for verifying/monitoring configuration changes and troubleshooting errors.

To view the log file, on the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **View Log File**. The **Configuration Management Log File** screen appears in a separate window.

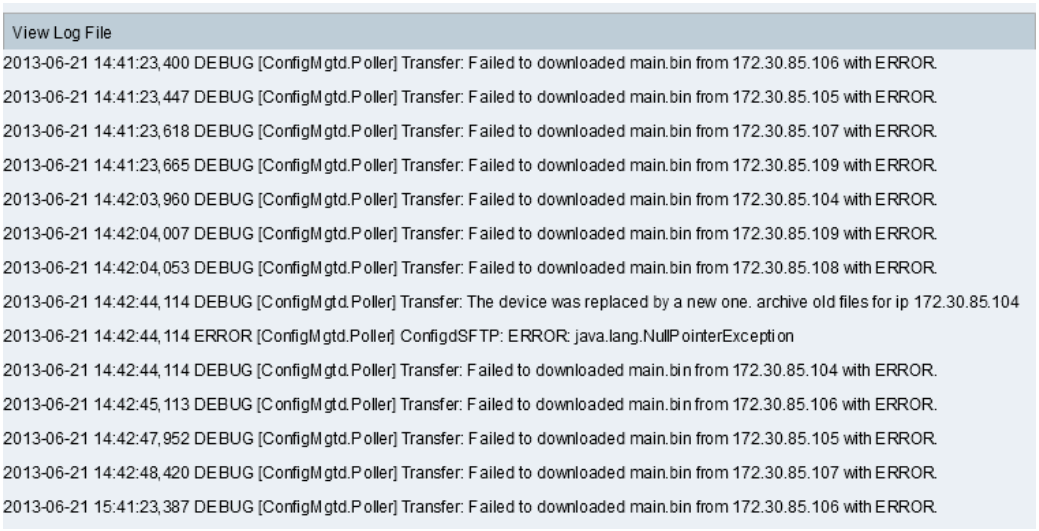


Figure 219: Configuration Management Log File Screen

Section 6.2

Managing Provisioning Groups

Provisioning groups offer the ability to bring a set of devices under the management of RUGGEDCOM NMS before they are available on the network. RUGGEDCOM NMS can then be used to fully pre-configure the devices down to the level of available IP interfaces and services for each. Allowing RUGGEDCOM NMS to auto-discover IP interfaces and services on a device is considerably faster by comparison, but provisioning groups provider finer-grain control of how RUGGEDCOM NMS monitors devices.

CONTENTS

Section 6.2.1

Viewing a List of Provisioning Groups

To view a list of available provisioning groups, click **Admin** on the menu bar, and then click **Manage Provisioning Groups**. The **Provisioning Groups** screen appears.

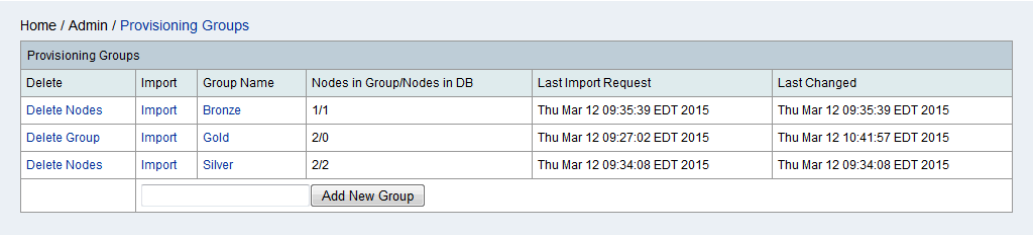


Figure 220: Provisioning Groups Screen

Section 6.2.2

Adding a Provisioning Group

To add a provisioning group, do the following:

NOTE
Each provisioning group counts towards the maximum number of devices RUGGEDCOM NMS can manage as defined by the product license.

1. On the menu bar, click **Admin** and then click **Manage Provisioning Groups**. The **Provisioning Groups** screen appears.

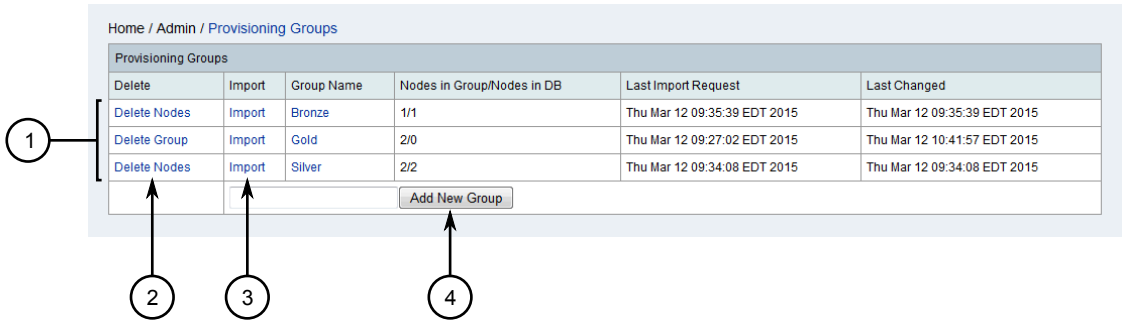


Figure 221: Provisioning Groups Screen

1. Available Provisioning Groups **2.** Delete Link **3.** Import Link **4.** Add New Group Button

2. Type the name of the new provisioning group next to **Add New Group**.
3. Click **Add New Group**. The new group is added to the list.
4. Add one or more nodes to the new provisioning group, as well as IP interfaces, services and/or node categories as needed. For more information, refer to Section 6.2.3, "Adding/Editing Nodes, Interfaces and Services" .
5. Click **Import** next to the new provisioning group. RUGGEDCOM NMS scans the new nodes and adds the specified IP interfaces and services to its database.

Section 6.2.3

Adding/Editing Nodes, Interfaces and Services

To add or edit nodes, IP interfaces and services within a provisioning group, do the following:

Adding/Editing a Node

1. On the menu bar, click **Admin** and then click **Manage Provisioning Groups**. The **Provisioning Groups** screen appears.

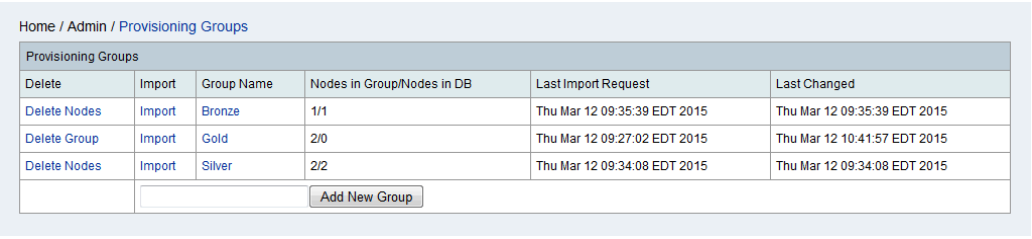


Figure 222: Provisioning Groups Screen

2. Select an existing provisioning group. The **Edit** screen appears.

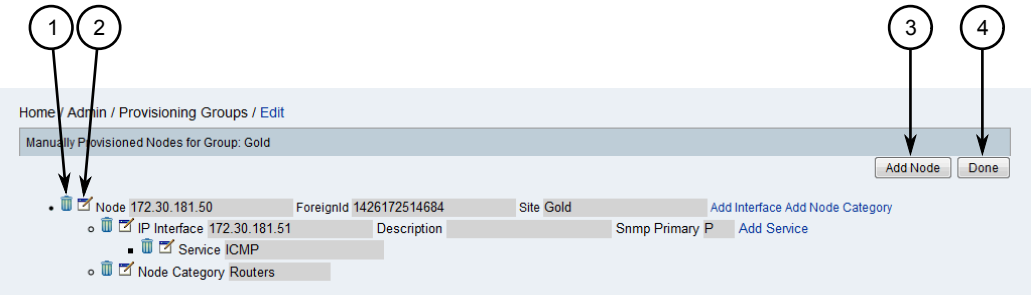


Figure 223: Edit Screen

1. Delete Icon **2.** Edit Icon **3.** Add Node Button **4.** Done Button

3. [Optional] To add a new node, click **Add Node**. Parameters for configuring a new node appear.

Figure 224: Adding a Node

1. Edit Icon **2.** Add Interface Link **3.** Add Node Category Link

4. Click the **Edit** icon for the new or existing node and configure the following parameters.

Figure 225: Editing a Node

1. Node Box **2.** ForeignID Box **3.** Site Box **4.** Save Button **5.** Cancel Button

Parameter	Description
Node	The name of the device.
ForeignID	A unique, auto-generated ID for the external (foreign) system.
Site	The building/site where the device is located. The name provided will be added to the device's asset information.

5. Click **Save**.

Adding/Editing an IP Interface (Optional)

1. Click the **Edit** next to an existing IP interface, or add a new IP interface by clicking **Add Interface**. Parameters for configuring the IP interface appear.

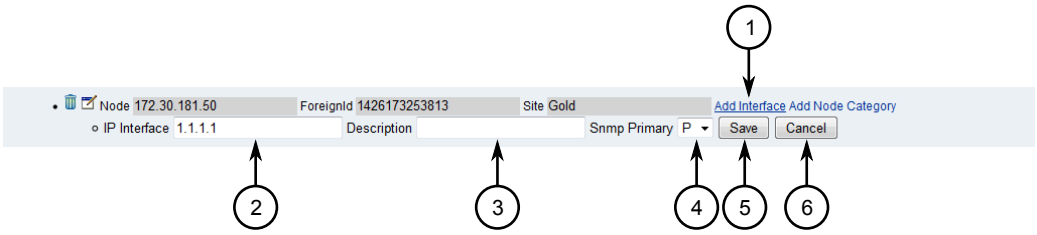


Figure 226: Adding/Editing an IP Interface

1. Add Interface Link **2.** IP Interface Box **3.** Description Box **4.** SNMP Primary List **5.** Save Button **6.** Cancel Button

2. Configure the following parameters as required:

Parameter	Description
IP Interface	The IP address of the IP interface.
Description	A description of the IP interface.
SNMP Primary	**Synopsis:** { P, S, C, N } The primary attribute. Options include: • `P` – Primary • `S` – Secondary • `C` – Collected • `N` – Not Collected

3. Click **Save**.

Adding/Editing a Service (Optional)

1. Click the **Edit** next to an existing service, or add a new service by clicking **Add Service**. Parameters for configuring the service appear.

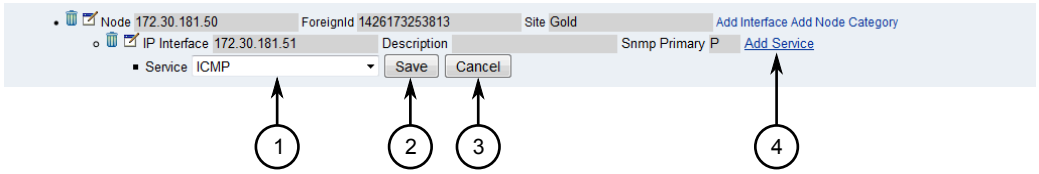


Figure 227: Adding/Editing a Service

1. Service List **2.** Save Button **3.** Cancel Button **4.** Add Service Link

2. Configure the following parameters as required:

Parameter	Description
Service	**Synopsis:** { ICMP, StrafePing, SNMP, HTTP, HTTP-8080, HTTP-8000, HTTPS, HypericAgent, HTTPS-1000, HypericHQ, FTP, Telnet, DNS, DHCP, IMAP, MSExchange, SMTP, POP3, SSH, MySQL, SQLServer, Oracle, Postgres, Router, HP Insight Manager, Dell-OpenManage, NSClient, NSClientpp, NRPE, NRPE-NoSSL, Windows-Task-Scheduler } **Default:** ICMP The service type.

3. Click **Save**.

Adding/Editing a Node Category (Optional)

NOTE
Node categories relate directly to surveillance categories. For more information about surveillance categories, including how to add, edit or delete them, refer to *Section 4.11, "Managing Surveillance Categories"*.

1. Click the **Edit** next to an existing node category, or add a new node category by clicking **Add Node Category**. Parameters for configuring the node category appear.

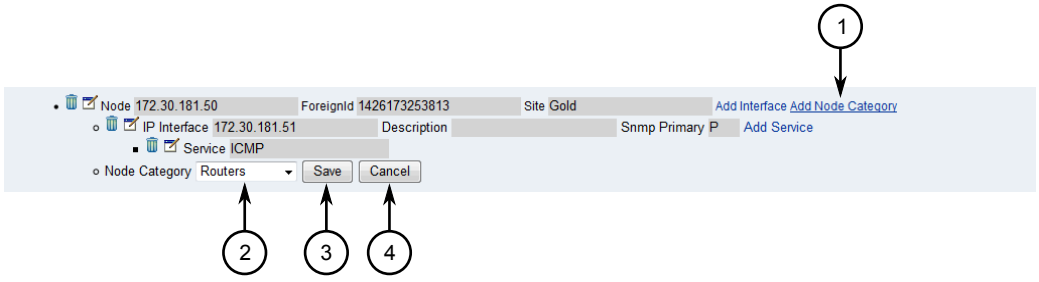


Figure 228: Editing a Node Category

1. Add Node Category Link **2.** Node Category List **3.** Save Button **4.** Cancel Button

Parameter	Description
Node Category	The node category. For a list of available categories, refer to Section 4.11, "Managing Surveillance Categories" .

2. Click **Save**.

» Completing the Configuration

Once all nodes have been added and configured, click **Done**.

Section 6.2.4

Deleting a Node, Interface, Service or Category

To delete a node, IP interface, service and/or node category from a provisioning group, do the following:

1. On the menu bar, click **Admin** and then click **Manage Provisioning Groups**. The **Provisioning Groups** screen appears.

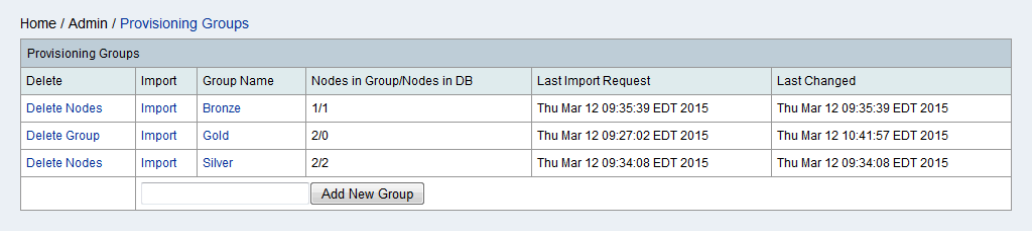


Figure 229: Provisioning Groups Screen

2. Select an existing provisioning group. The **Edit** screen appears.

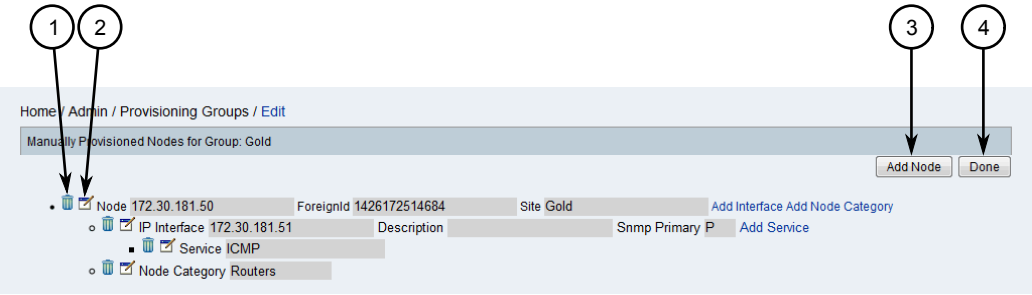


Figure 230: Edit Screen

1. Delete Icon **2.** Edit Icon **3.** Add Node Button **4.** Done Button

3. Click the **Delete** icon next to the desired node, IP interface, service or node category. The node, IP interface, service or node category is removed instantly.

Section 6.2.5
Deleting a Provisioning Group

To delete a provisioning group, do the following:

1. On the menu bar, click **Admin** and then click **Manage Provisioning Groups**. The **Provisioning Groups** screen appears.

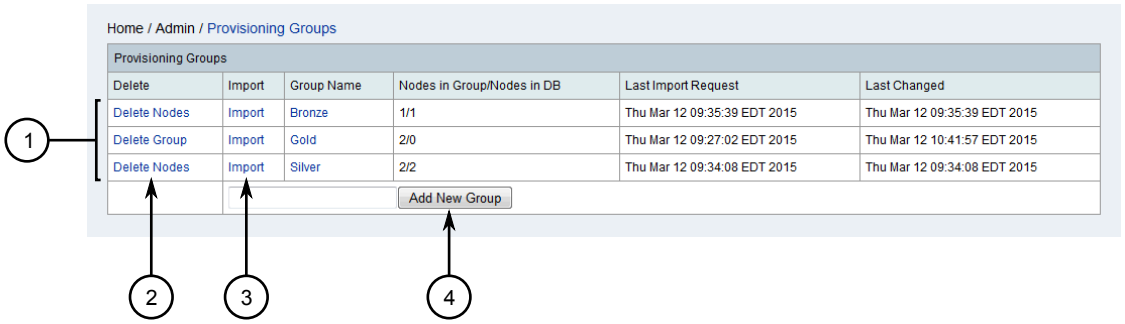


Figure 231: Provisioning Groups Screen

1. Available Provisioning Groups **2.** Delete Node Link **3.** Delete Group Link **4.** Import Link **5.** Add New Group Button

NOTE
*A provisioning group cannot be deleted until all its nodes have been removed from the RUGGEDCOM NMS database. The **Nodes in Group/Nodes in DB** column indicates how many nodes are configured for the group and how many nodes are in the database.*

2. If the group has nodes in the RUGGEDCOM NMS database, click **Delete Node** next to the desired provisioning group and then click **Import** to update the database.

   Once all nodes have been deleted from the database, the **Delete Node** link changes to **Delete Group**.

3. Click **Delete** next to the desired provisioning group and then click **Import** to update the database. The group is removed.

Section 6.3
Managing Nodes, Interfaces and Services

Layer 3 nodes and interfaces represent IP addresses monitored by RUGGEDCOM NMS. Services are mapped to IP interfaces, and interfaces discovered to be on the same device are grouped together as a node.

CONTENTS

- Section 6.3.3, "Clearing/Deleting a Node"

Section 6.3.1

Enabling/Disabling Nodes, Interfaces and Services

When RUGGEDCOM NMS is first started, it discovers the nodes, interfaces and services in the network. As the network grows and changes, the TCP/IP ranges to be managed, as well as the interfaces and services within those ranges, may change.

Each node, interface and associated service is enabled by default and actively managed by RUGGEDCOM NMS. These can be disabled as needed and later re-enabled when needed, allowing the user to adapt the configuration of RUGGEDCOM NMS to the network.

Once a node, interface or service is disabled, no further data is collected. However, existing data is retained in the database.

To enable or disable a node, interface or service, do the following:

1. On the menu bar, click **Admin** and then click **Manage and Unmanage Interfaces and Services**. The **Manage/Unmanage Interfaces** screen appears.

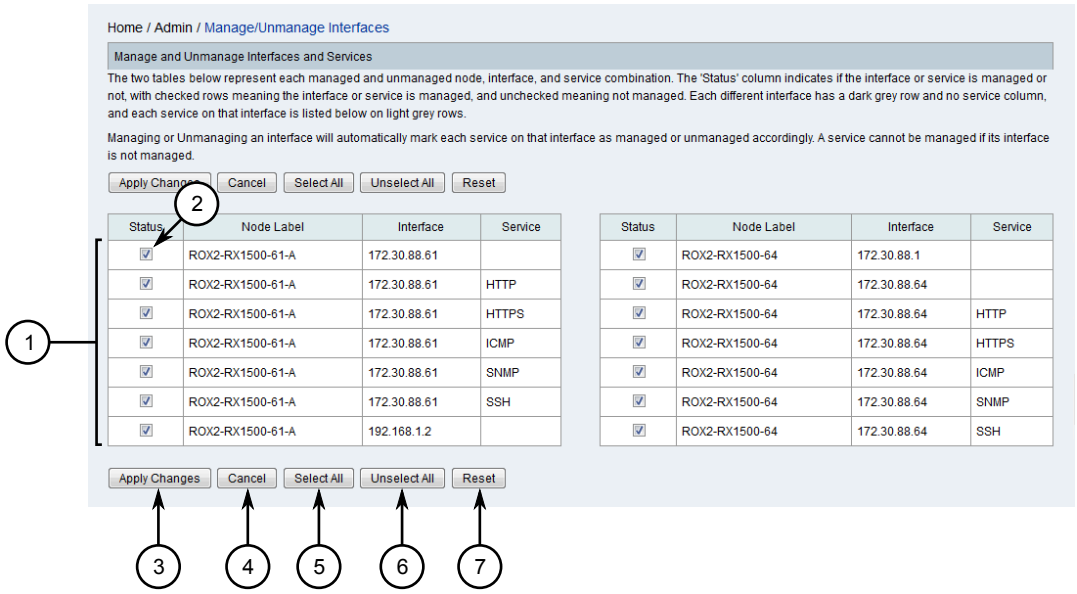


Figure 232: Manage/Umanage Interfaces Screen

1. Nodes, Interfaces and Services **2.** Enable Check Box **3.** Apply Changes Button **4.** Cancel Button **5.** Select All Button **6.** Unselect All Button **7.** Reset Button

This screen displays the known nodes, interfaces and the services associated with them.

> **NOTE**
> *Enabling or disabling a single node (one without a service associated to it) enables/disables all related interfaces and services.*

2. Select (enable) or clear (disable) individual nodes or node/interface/service combinations. The **Select All** and **Unselect All** buttons can also be used to enable or disable all node/interface/service combinations at once.

3. Click **Apply Changes** to save changes.

Section 6.3.2
Adding an Interface

IP interfaces (or devices) can be added to the RUGGEDCOM NMS database manually by providing a valid IP address. If the IP address for the interface already exists in the table for an existing, managed node, the interface is added to that node. Otherwise, a new node is generated for the interface.

To add an individual IP interface, do the following:

1. On the menu bar, click **Admin** and then click **Add Interface**. The **Add Interface** screen appears.

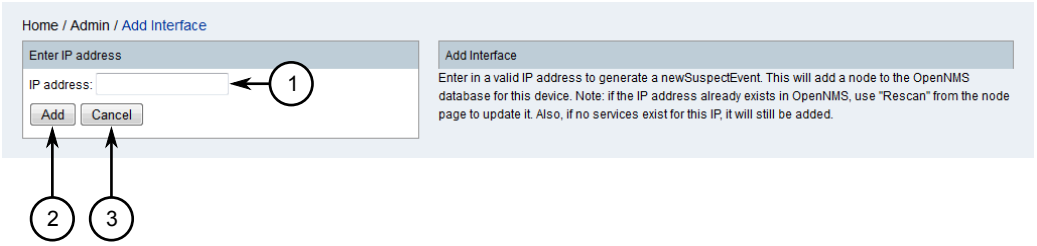


Figure 233: Add Interface Screen

1. IP Address Box **2.** Add Button **3.** Cancel Button

2. Under **IP Address**, type the IP address for the interface and then click **Add**.

Section 6.3.3
Clearing/Deleting a Node

Nodes and/or their associated data can be manually removed from RUGGEDCOM NMS as needed.

IMPORTANT!
A node previously removed from the database may be rediscovered later on during the discovery process. To permanently delete a node, it must also be either removed from the device discovery configuration or explicitly unmanaged. For more information, refer to *Section 6.4.10, "Managing Device Discovery"* *and/or* *Section 6.3.1, "Enabling/Disabling Nodes, Interfaces and Services"* .

To delete one or more nodes, or simply clear the data associated with them, do the following:

1. On the menu bar, click **Admin** and then click **Delete Nodes**. The **Delete Nodes** screen appears.

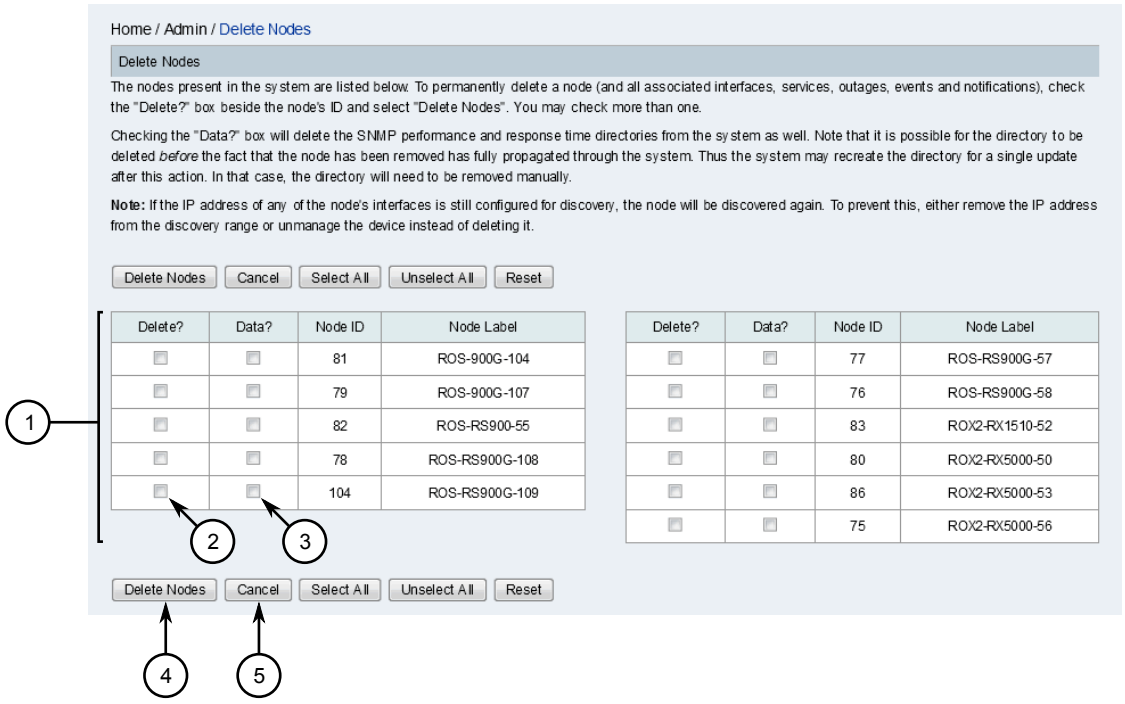


Figure 234: Delete Nodes Screen

1. Available Nodes **2.** Delete Check Box **3.** Data Check Box **4.** Delete Nodes Button **5.** Cancel Button

2. Select whether to delete and/or clear the desired node(s). The check box under **Delete?** marks the node for deletion. The check box under **Data?** marks only the data associated with the node for deletion.
3. Click **Delete Nodes**.

Alternatively, navigate to the device details for a specific node and do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. From the **Node** screen, click **Admin** and then **Delete Node**. The **Node Management** screen appears.

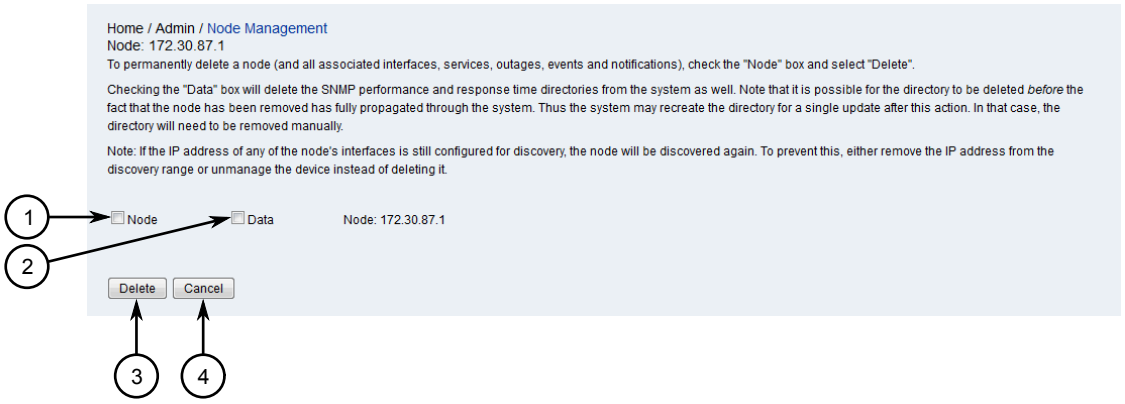


Figure 235: Node Management Screen

1. Node Check Box **2.** Data Check Box **3.** Delete Button **4.** Cancel Button

3. Select whether to delete and/or clear the desired node.
   - Select **Node** to mark the node for deletion
   - Select **Data** to mark the node's data for deletion
4. Click **Delete**.

Section 6.4

Managing Devices

This section describes how to discover and access devices managed by RUGGEDCOM NMS.

CONTENTS

- Section 6.4.12, “Managing Device Passwords”

Section 6.4.1
Searching for Devices within RUGGEDCOM NMS

To search for a device managed by RUGGEDCOM NMS, start by clicking **Search** on the menu bar. The **Search** screen appears.

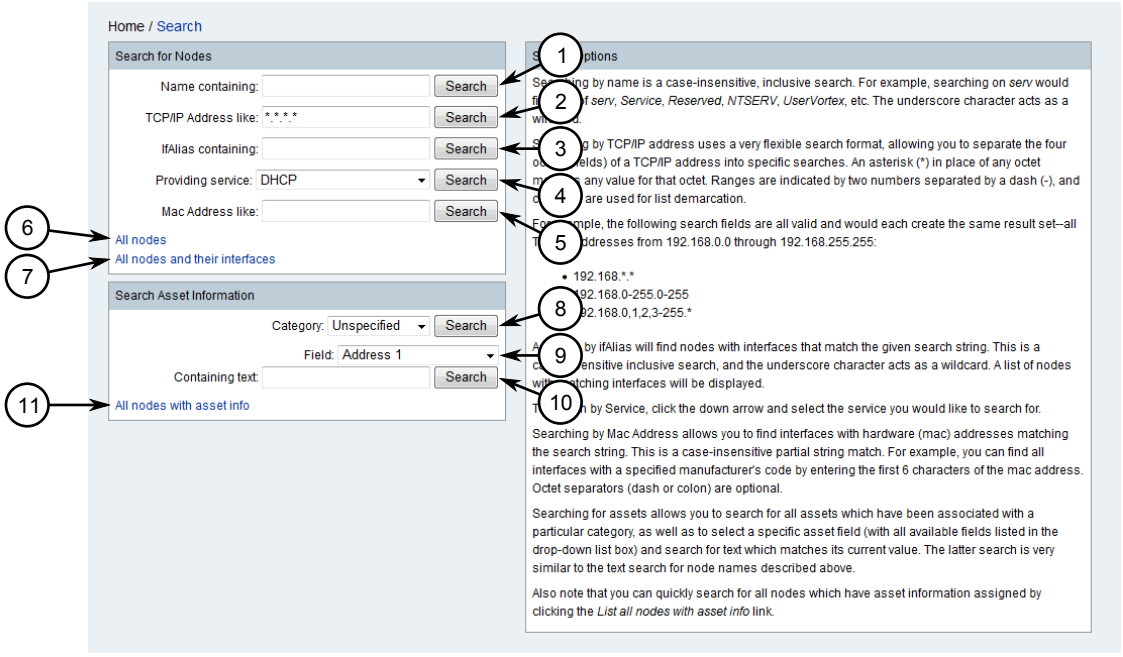


Figure 236: Search Screen

1. Name Containing Box and Search Button **2.** TCP/IP Address Like Box and Search Button **3.** IfAlias Containing Box and Search Button **4.** Providing Service List and Search Button **5.** MAC Address Like Box and Search Button **6.** All Nodes Link **7.** All Nodes and Their Interfaces Link **8.** Category List and Search Button **9.** Field List **10.** Containing Text and Search Button **11.** All Nodes With Asset Info Link

From here, devices can be found based on their name, IP address, interfaces, services, or MAC address. Asset information can also be used to find devices of a specific type, in a specific location, operated by a specific department or contractor, etc.

- **Searching by Name**
  To search for a device by its name, type the full or partial name of the device under **Name Containing** and then click **Search**. A list of all devices matching that name is displayed.

  Searching by name is a case-insensitive, inclusive search. For example, searching for *serv* will find *serv*, *Service*, *Reserved*, *NETSERV*, *UserVortex*, etc. The underscore (_) character acts as a wildcard.

- **Searching by IP Address**
  To search for a device by its IP address, type the IP address under **TCP/IP Address Like** and then click **Search**. A list of all devices matching that IP address is displayed.

  Each octet in the IP address can be replaced with an asterisk (*) character (e.g. 192.168.*.*), a demarcated list of values (e.g. 192.168.1,2,3.*), or a range (e.g. 192.168.1,2,3.10-255) to expand the search criteria.

- **Searching by Interface**
  To search by interface, type the name of the interface under **ifAlias Containing** and then click **Search**. A list of all devices that have matching interfaces appears.

  Searching by interface name is a case-insensitive, inclusive search. Use the underscore (_) character as a wildcard.
- **Searching by Service**
  To search by service, select a service from **Providing Service** and then click **Search**. A list of devices that provide matching services appears.
- **Searching by MAC Address**
  To search for devices based on their MAC addresses, type the full or partial MAC address under **MAC Address Like** and then click **Search**. All devices that have similar MAC addresses appear.

  Searching by MAC address is a case-insensitive, inclusive search that allows for partial matches. Use the dash (-) or colon (:) characters as octet separators if needed.
- **Searching by Category**
  To search by asset category, select a category under **Category** and then click **Search**. All devices belonging to the selected category are displayed.
- **Searching by Asset Field**
  To search based on a specific field in a device's asset information, select a field under **Field**, type the value for the field under **Containing Text**, and then click **Search**. All devices that contain the specified text string in their asset information appear.

When devices are found that match the search criteria, the **Node List** screen appears.

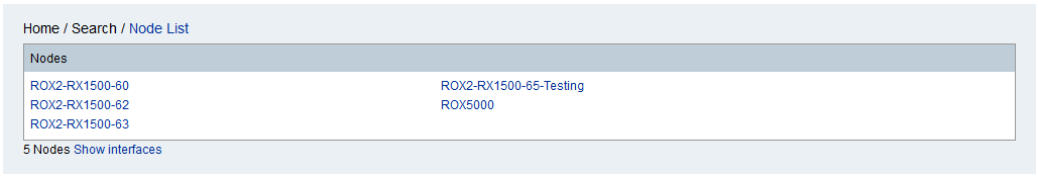


Figure 237: Node List Screen

Click the desired device to access its device details. For more information about device details, refer to Section 6.4.2, “Viewing Device Details” .

Section 6.4.2

Viewing Device Details

To view detailed information about a device, do one of the following:

- Search for the device by label or IP address. For more information, refer to Section 6.4.1, “Searching for Devices within RUGGEDCOM NMS ” .
- On the menu bar, click **Node List** and then select the device from the list.

Both methods lead to the **Node** screen for the selected device.

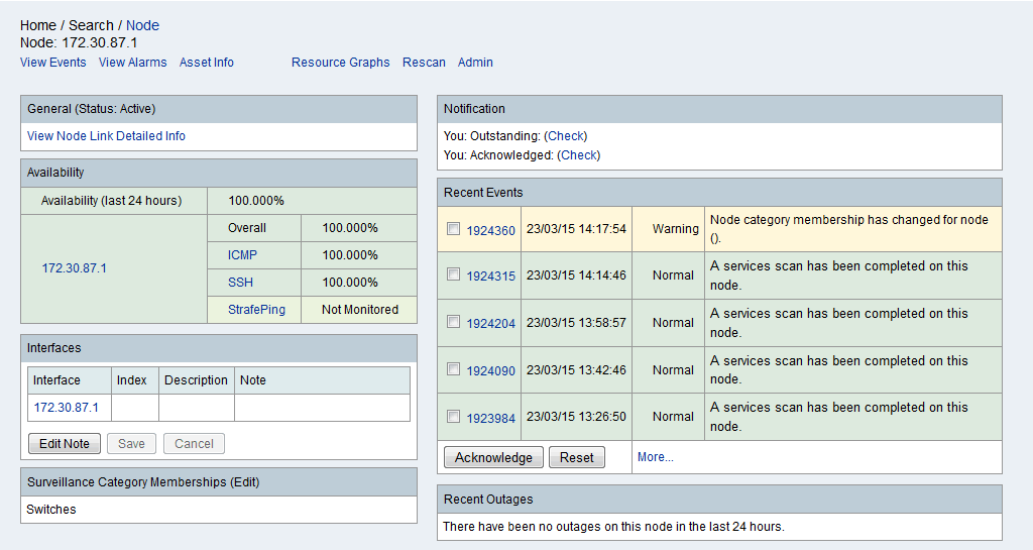


Figure 238: Node Screen (Example)

This screen presents a detailed summary of current data collected from the device. It also provides tools for managing the device configuration within RUGGEDCOM NMS.

CONTENTS

Section 6.4.2.1

Important Links

The following links may appear along the top of the **Node** screen depending on the device type and configuration:

- **View Events** – Displays a list of all events related to the device. For more information about events, refer to Section 5.2, “Managing Events, Alarms and Notifications”
- **View Alarms** – Displays a list of all alarms related to the device. For more information about alarms, refer to Section 5.2, “Managing Events, Alarms and Notifications”
- **Asset Information** – Displays the asset information configured in RUGGEDCOM NMS for the device. For more information, refer to Section 6.4.9, “Managing Asset Information” .
- **Telnet** – Opens a telnet session to the device. This link only appears for devices that support telnet sessions. The browser must also be configured to open a telnet terminal based on the telnet::// URL prefix.

- **HTTP/HTTPS** – Opens the device's Web-based user interface in a new browser window or tab.
- **HTTPS-10000** – Opens the device's Web-based user interface in a new browser window or tab. For RUGGEDCOM ROX devices only.
- **SSH** – Opens an SSH session to the device. This link only appears for devices that support SSH sessions. The browser must be configured to open an SSH terminal based on the ssh://URL prefix.
- **Resource Graphs** – Begins the process for generating a standard performance graph for the device. For more information, refer to Section 5.4.2.1, "Generating Standard Reports" .
- **Rescan** – Rescans the device for available services. For more information about rescanning a device, refer to Section 6.4.7.4, "Scanning a Device/Interface for Services" .
- **Admin** – Opens a management menu for:
  - Changing the node label
  - Managing interfaces and services
  - Configuring SNMP data collection
  - Deleting the device and/or device data
  - Configuring a critical path to the device for path outages
- **Update SNMP** – Refreshes the SNMP data collected from the device.

Section 6.4.2.2
General

The **General** section of the **Node** screen contains links to information based on the device type. Links include:

Figure 239: General Section

- **View Node Bridge/STP Info** – Displays detailed information about the device's bridge/STP configuration. For more information, refer to Section 6.4.3, "Viewing Bridge/STP Information" .
- **View Node IP Route Info** – Displays the device's IP routing table. Only for devices that support Layer 3 networking, such as routers. For more information, refer to Section 6.4.4, "Viewing the IP Routing Table" .
- **View Node Link Detailed Info** – Displays detailed information about the device's network links. Information about adjacent devices is also displayed if they are managed by RUGGEDCOM NMS. For more information, refer to Section 6.4.8.1, "Viewing a List of Device Links" .

Section 6.4.2.3
Availability

The **Availability** section of the **Node** screen displays:

- The availability of services on the device as a percentage value over the last 24 hours
- The overall availability of the device and that of each monitored service

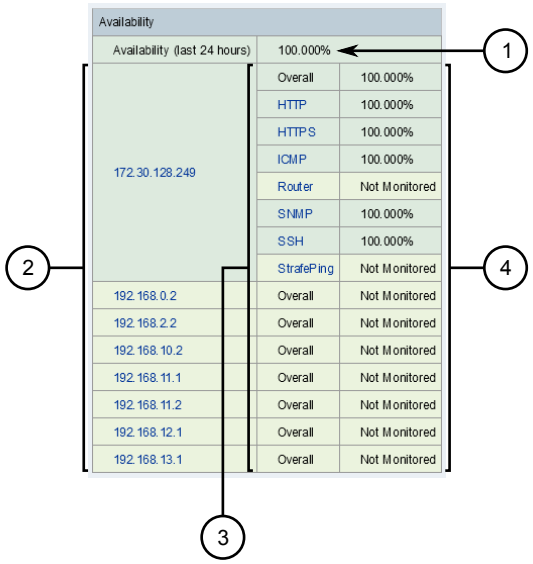


Figure 240: Availability Section

1. Overall Availability **2.** Interfaces **3.** Services **4.** Availability of Services

NOTE
By default, defined services are monitored only via the primary IP interface for the device.

Only managed services are displayed. For information about how to control which services are managed, refer to Section 6.4.7.3, "Selecting Interfaces/Services Managed by Devices" .

The color of each row in the table indicates the overall availability of the device and its monitored services.

- *Green* – Indicates 100% availability over the last 24 hours
- *Yellow* – Indicates 97 to 100% availability, suggesting the service was interrupted briefly
- *Red* – Indicates less than 97% availability, suggesting a serious problem

Section 6.4.2.4
SNMP Attributes

The **SNMP Attributes** section of the **Node** screen displays system-level SNMP information for the selected device. The information is taken specifically from the MIB-2 System management group.

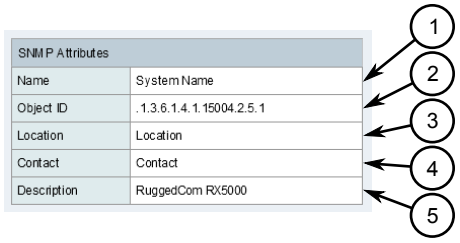


Figure 241: SNMP Attributes Section

1. Name **2.** Object ID **3.** Location **4.** Contact **5.** Description

Section 6.4.2.5
Surveillance Category Membership

The **Surveillance Category Membership** section of the **Node** screen lists the surveillance categories to which the device belongs.

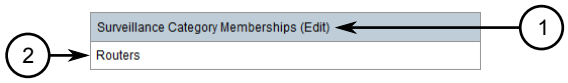


Figure 242: Surveillance Category Membership Section

1. Edit Link **2.** Memberships

Click **Edit** to assign a surveillance category to the device. For more information, refer to Section 4.11.1, "Adding a Surveillance Category" .

For information about surveillance categories in general, refer to Section 4.11, "Managing Surveillance Categories" .

Section 6.4.2.6
Notification

The **Notification** section of the **Node** screen provides links to lists of outstanding and acknowledged notifications specific to the user.

NOTE
Only notifications marked as outstanding or acknowledged during the current RUGGEDCOM NMS session are listed.

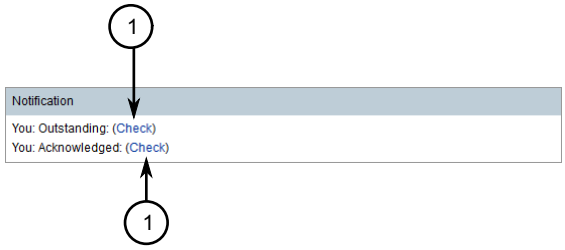


Figure 243: Notification Section

1. Check Link

Click **Check** to view the associated list.

Section 6.4.2.7

Recent Events

The **Recent Events** section of the **Node** screen lists the most recent events still outstanding for the selected device.

NOTE
Only the latest five events are listed.

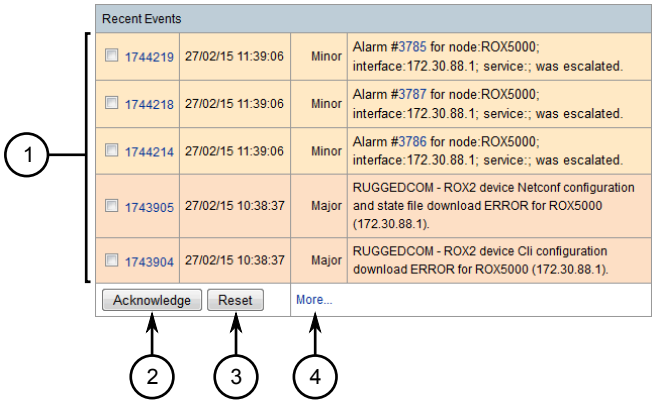


Figure 244: Recent Events Section

1. Outstanding Events **2.** Acknowledge Button **3.** Reset Button **4.** More Link

To acknowledge an event from the **Recent Events** section, select the events to acknowledge and then click **Acknowledge**. The selected events are removed from the list.

To refresh the list, click **Reset**.

To view all outstanding events related to the device, click **More**.

Section 6.4.2.8
Recent Outages

The **Recent Outages** section of the **Node** screen lists detected service outages on the selected device over the past 24 hours. The list details which services were lost, at what time, for which interface on the device, and at what time the service was restored.

If an outage has not yet been restored, the background of the table row is red and *DOWN* appears in the **Regained** column.

NOTE
Only the latest five events are listed.

Recent Outages

Interface	Service	Lost	Regained	Outage ID
172.30.131.4	SSH	6/3/13 13:12:07	DOWN	52002
172.30.131.4	SNMP	6/3/13 13:12:07	DOWN	52003
172.30.131.4	ICMP	6/3/13 13:12:07	DOWN	52004
172.30.131.4	Telnet	6/3/13 13:12:07	DOWN	52005
172.30.131.4	HTTP	6/3/13 13:12:07	DOWN	52006
172.30.131.4	HTTPS	6/3/13 13:12:07	DOWN	52007

Figure 245: Recent Events Section

Section 6.4.3
Viewing Bridge/STP Information

To view bridge/STP information for a device managed by RUGGEDCOM NMS, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. Under **General**, click **View Node Bridge/STP Info**. The **Bridge Info** screen appears.

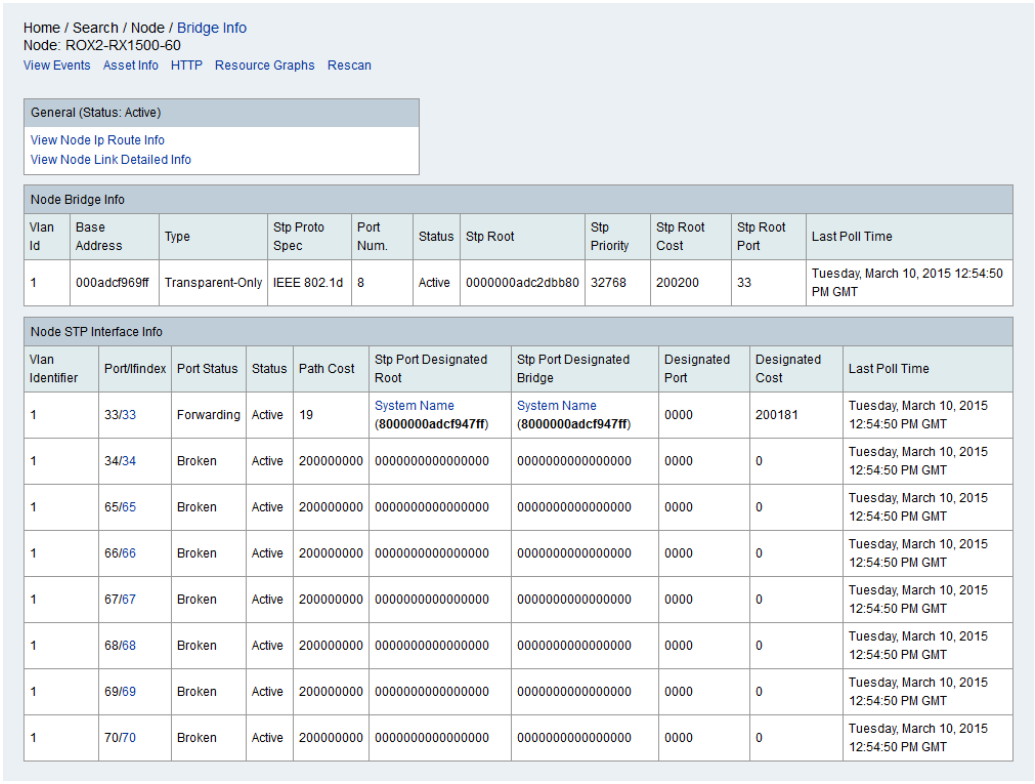


Figure 246: Bridge Info Screen

Section 6.4.4

Viewing the IP Routing Table

To view IP routing table for a device managed by RUGGEDCOM NMS, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. Under **General**, click **View Node IP Route Info**. The **Bridge Info** screen appears.

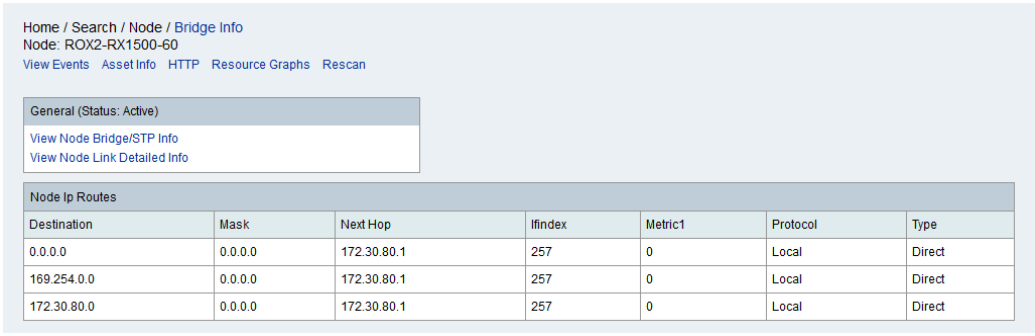


Figure 247: Bridge Info Screen

Section 6.4.5
Renaming a Device

Each device is automatically assigned a label for quick identification within RUGGEDCOM NMS. The label can be used in whole or in part to search for the device within RUGGEDCOM NMS and on a logical map.

NOTE
Renaming a device only changes its name within RUGGEDCOM NMS, not on the device itself.

To rename a device, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details".
2. From the **Node** screen, click **Admin** and then **Change Node Label**. The **Change Node Label** screen appears.

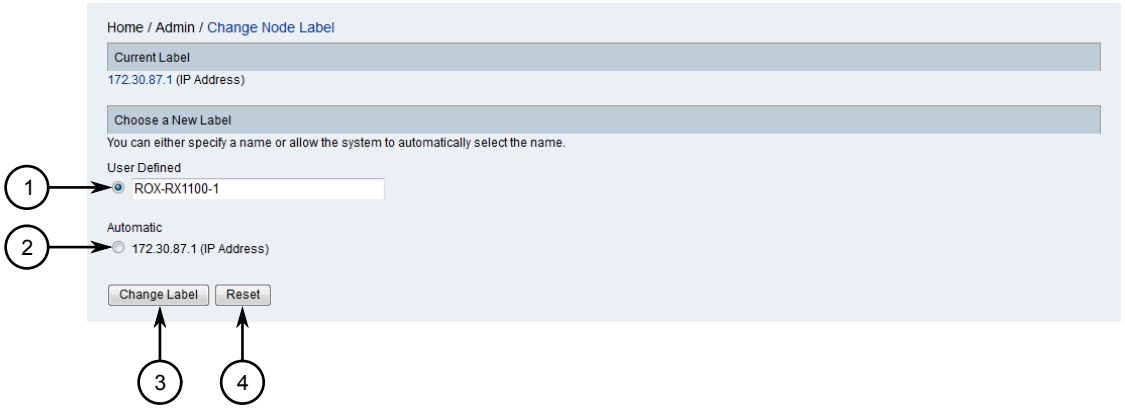


Figure 248: Change Node Label Screen

1. User Defined Box and Option **2.** Automatic Option **3.** Change Label Button **4.** Reset Button

3. Select either the **User Defined** or **Automatic** option.
4. If the **User Defined** option is selected, type a custom name for the device.
5. Click **Change Label**.

Section 6.4.6
Deleting a Device and/or Device Data

To delete a device and/or its data from RUGGEDCOM NMS, do the following:

NOTE
If the IP address of of any of the node's interface is still discovered for discovery, the node will be discovered again. To permanently delete the device, follow this procedure, then remove the IP address from the discovery range. For more information about managing device discovery, refer to Section 6.4.10, "Managing Device Discovery".

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details".
2. Click **Admin** and then click **Delete Node**. The **Node Management** screen appears.

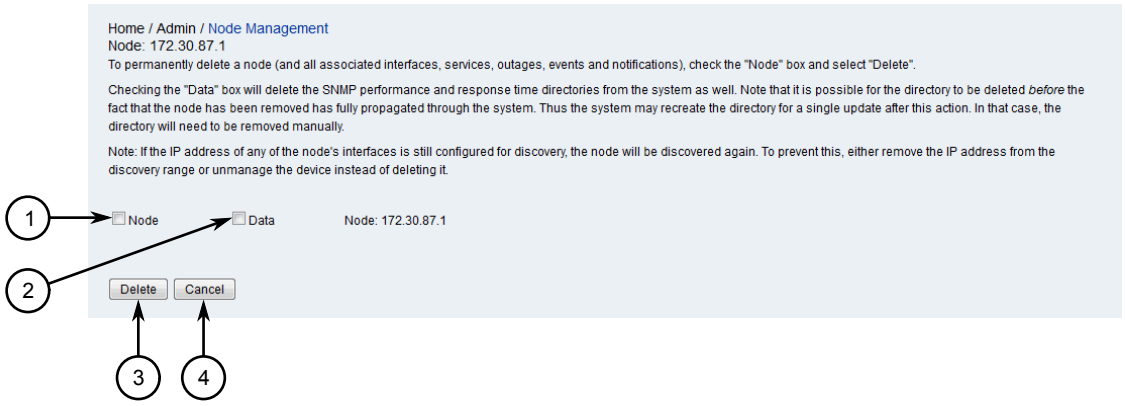


Figure 249: Links Screen

1. Node Check Box **2.** Data Check Box **3.** Delete Button **4.** Cancel Button

3. [Optional] Select **Node** to delete the device.
4. [Optional] Select **Data** to delete the data for the device.
5. Click **Delete**. A confirmation message appears.
6. Click **OK**.

Section 6.4.7

Managing Interfaces and Services

Whenever RUGGEDCOM NMS is launched, it automatically discovers the devices, interfaces and services available on the network. As the network grows and changes, the TCP/IP ranges to be managed, as well as the interfaces and services within those ranges, may change as well. As such, it may be necessary to control which interfaces and/or services are managed or force RUGGEDCOM NMS to scan the network for new interfaces and services.

CONTENTS

Section 6.4.7.1

Viewing Interface Details

To view details about the interfaces owned by a device managed by RUGGEDCOM NMS, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, “Viewing Device Details” .

2. Click the desired interface. The **Interface** screen appears.

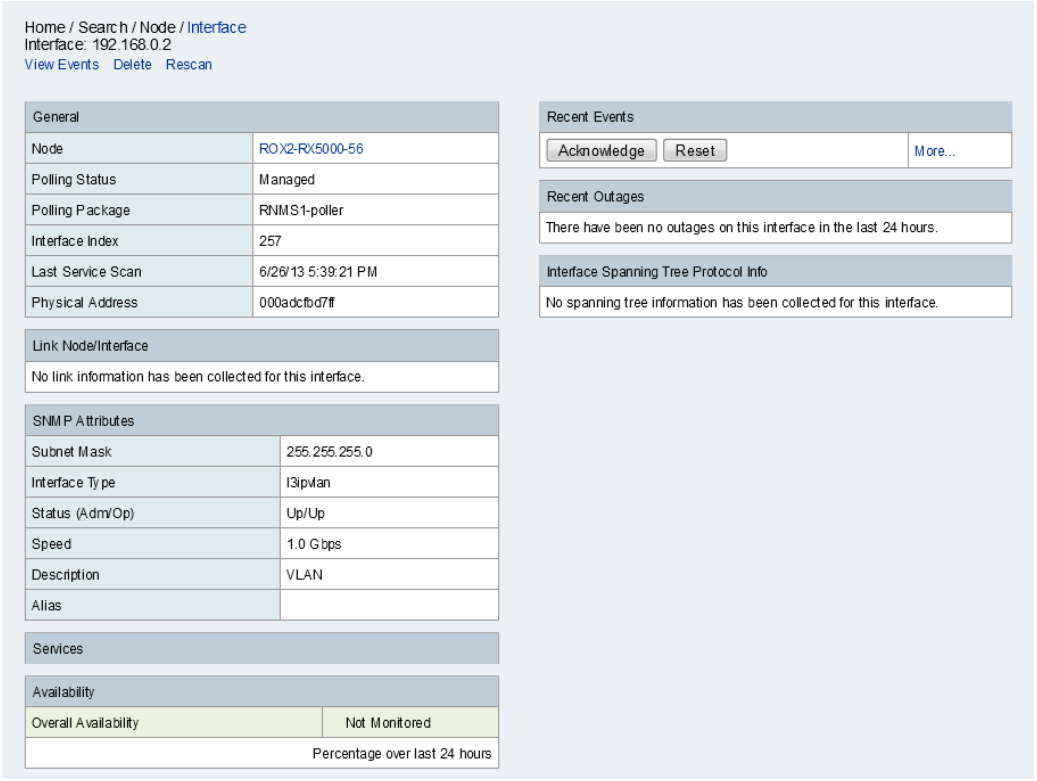


Figure 250: Interface Screen

Section 6.4.7.2

Viewing Service Details

To view details about the services offered by an interface, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. Under **Availability**, select the desired service for one of the available interfaces. The **Service** screen appears.

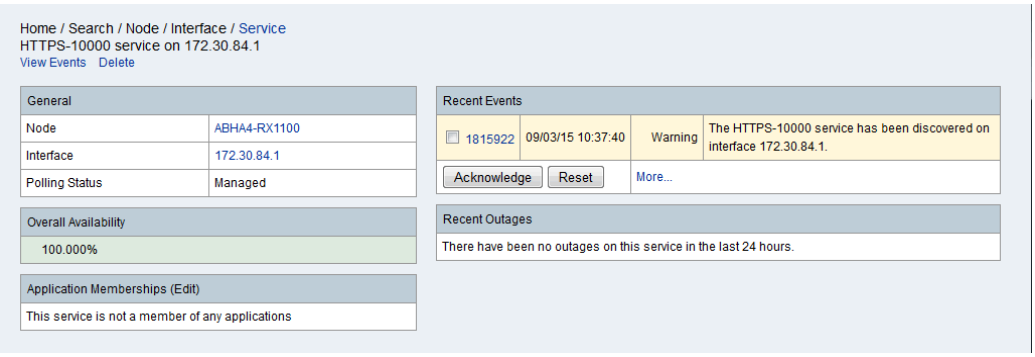


Figure 251: Service Screen

Section 6.4.7.3

Selecting Interfaces/Services Managed by Devices

Interfaces and services managed by devices can be selectively enabled or disabled.

NOTE
Once an interface or service is no longer managed, no further data is collected or stored in the RUGGEDCOM NMS database. However, existing data is retained.

Managing Interfaces/Services for a Specific Device

To control which interfaces/services are managed by a specific device, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. From the **Node** screen, click **Admin** and then **Manage and Unmanage Interfaces and Services**. The **Node Management** screen appears.

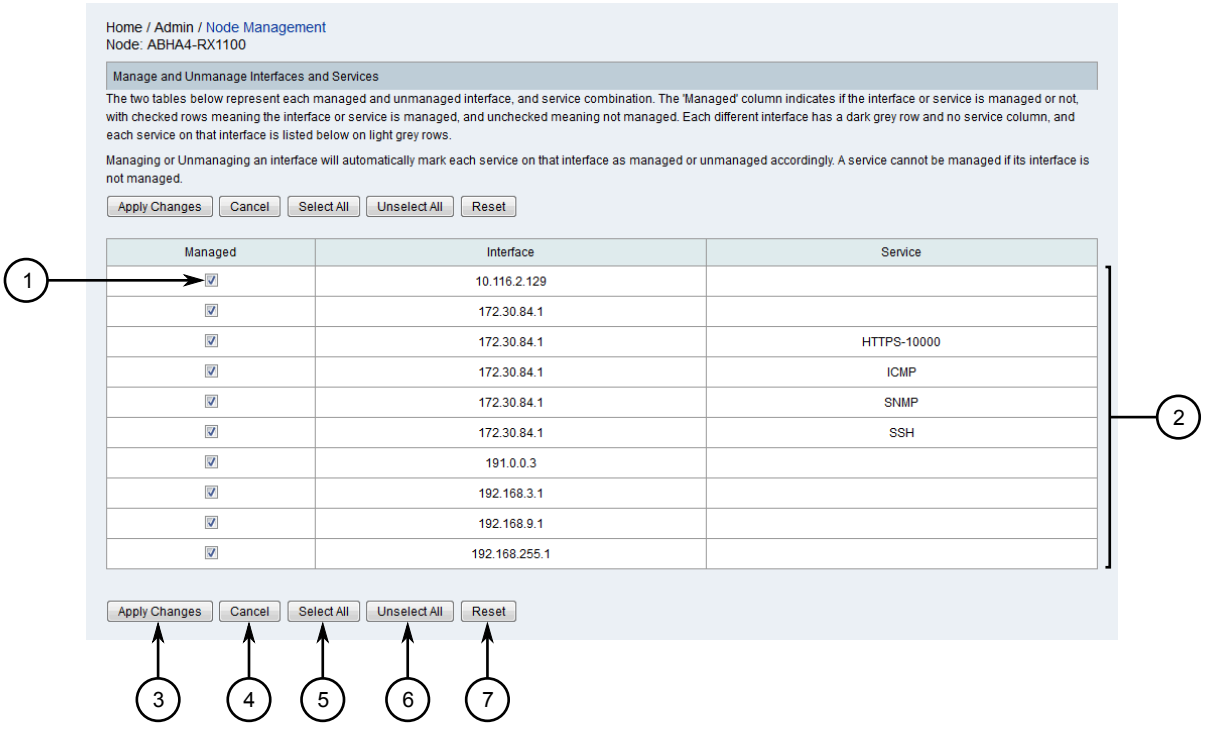


Figure 252: Node Management Screen

1. Managed Check Box **2.** Available Nodes and Services **3.** Apply Changes Button **4.** Cancel Button **5.** Select All Button **6.** Unselect All Button **7.** Reset Button

3. Select the interfaces and interface/service pairs to be managed by the device. Clear the **Managed** check box to de-select an interface or interface/service pair.
4. Click **Apply Changes**. A confirmation message appears.
5. Click **OK**.
6. Scan the device for the changes to take effect. For more information, refer to Section 6.4.7.4, "Scanning a Device/Interface for Services" .

» Managing Interfaces/Services for All Devices

To control which interfaces/services are managed by all devices, do the following:

1. On the menu bar, click **Admin** and then click **Manage and Unmanage Interfaces and Services**. The **Manage/Unmanage Interfaces** screen appears.

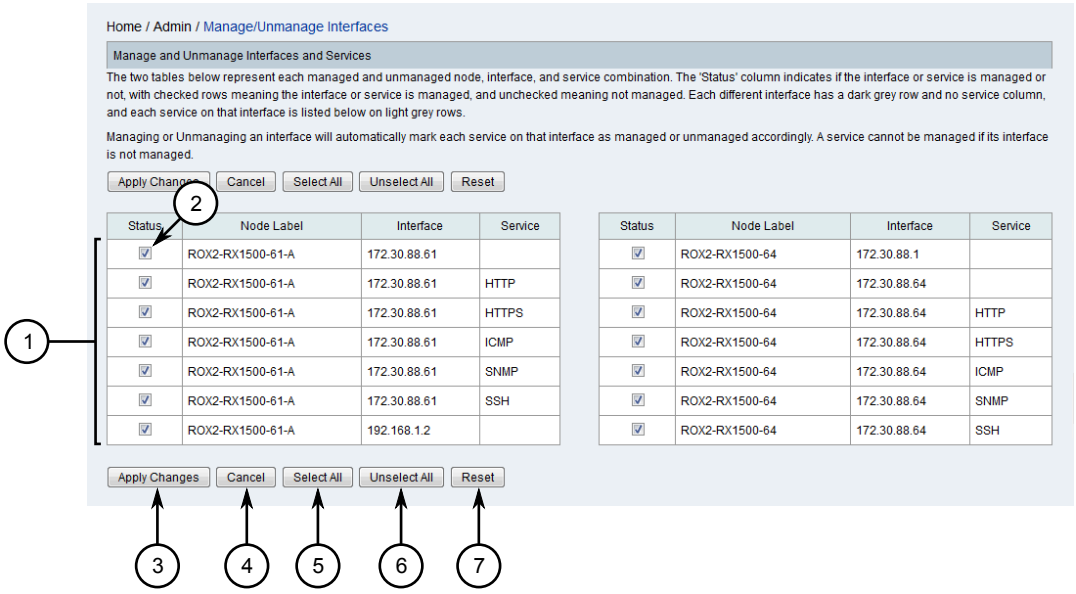


Figure 253: Managing/Unmanage Interfaces Screen

1. Managed Check Box **2.** Available Nodes and Services **3.** Apply Changes Button **4.** Cancel Button **5.** Select All Button **6.** Unselect All Button **7.** Reset Button

2. Select the interfaces and interface/service pairs to be managed by the device. Clear the **Managed** check box to de-select an interface or interface/service pair.
3. Click **Apply Changes**. A confirmation message appears.
4. Click **OK**.
5. Scan the devices for the changes to take effect. For more information, refer to Section 6.4.7.4, "Scanning a Device/Interface for Services" .

Section 6.4.7.4

Scanning a Device/Interface for Services

By default, RUGGEDCOM NMS scans devices and interfaces every 15 minutes to determine their capabilities, or whenever it suspects a device/interface may have previously unidentified services.

To force RUGGEDCOM NMS to rescan a device or interface, do the following:

» Rescanning a Device

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. From the **Node** screen, click **Rescan**. The **Rescan** screen appears.

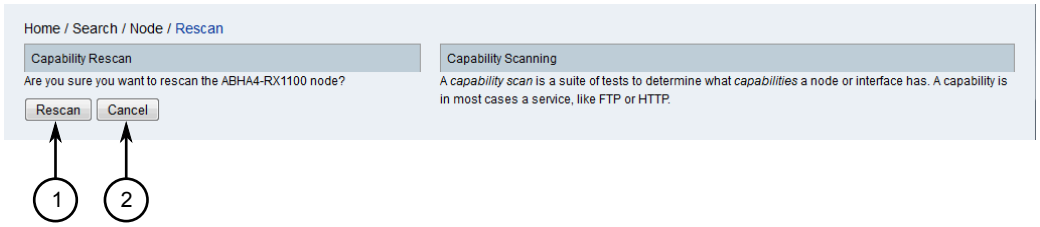


Figure 254: Rescan Screen

1. Rescan Button **2.** Cancel Button

3. Click **Rescan**. A notification is generated to indicate the start of the scan.

Rescanning an Interface

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. From the **Node** screen, select the desired interface. The **Interface** screen.

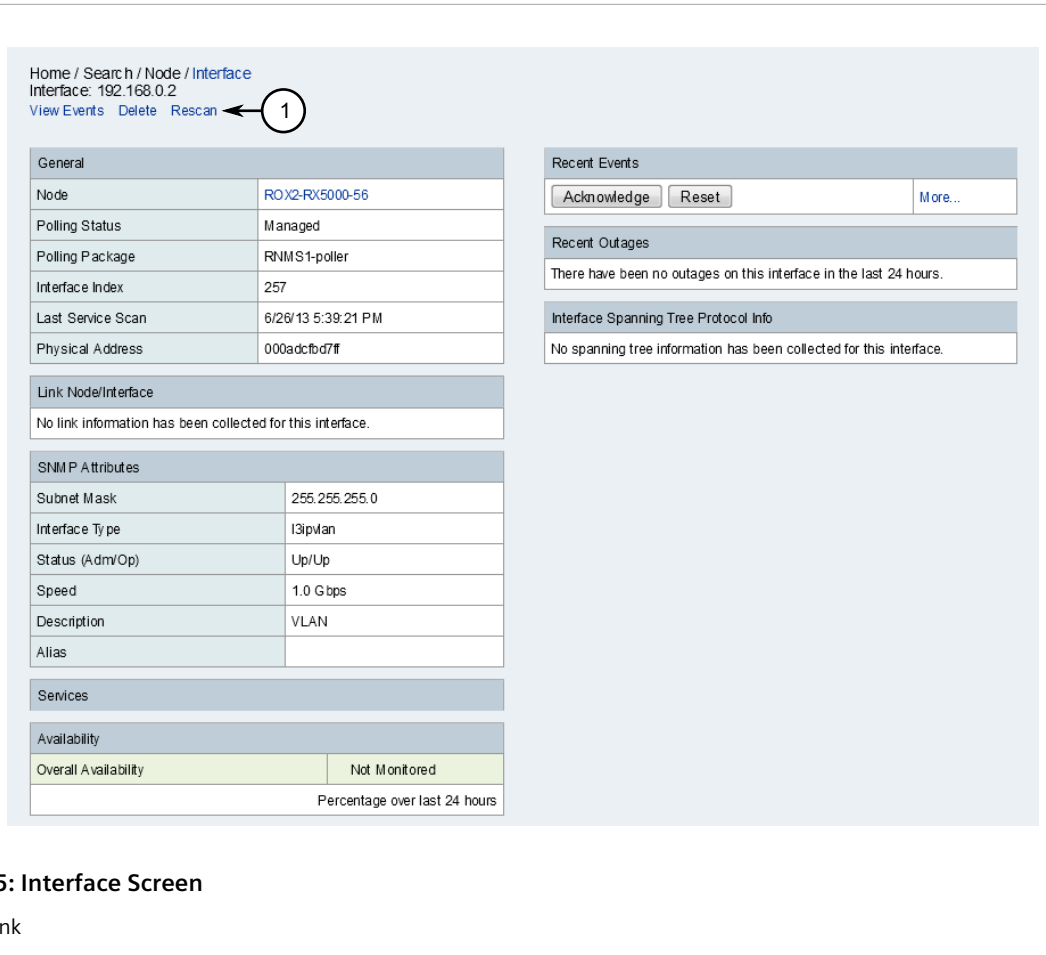


Figure 255: Interface Screen

1. Rescan Link

3. Click **Rescan**. The **Rescan** screen appears.

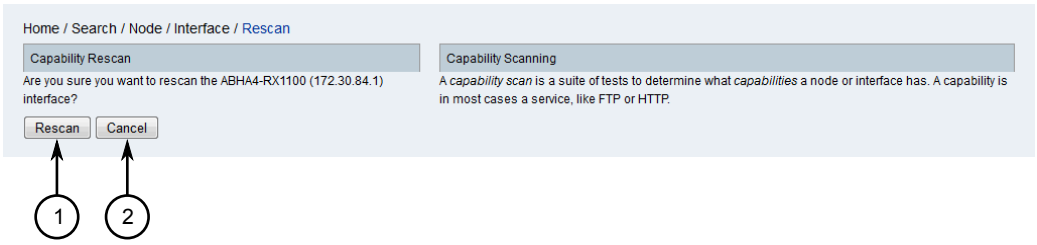


Figure 256: Rescan Screen

1. Rescan Button **2.** Cancel Button

4. Click **Rescan**. A notification is generated to indicate the start of the scan.

Section 6.4.7.5
Deleting an Interface

To delete an interface from a device managed by RUGGEDCOM NMS, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. Under **Availability**, select an interface. The **Interface** screen appears.

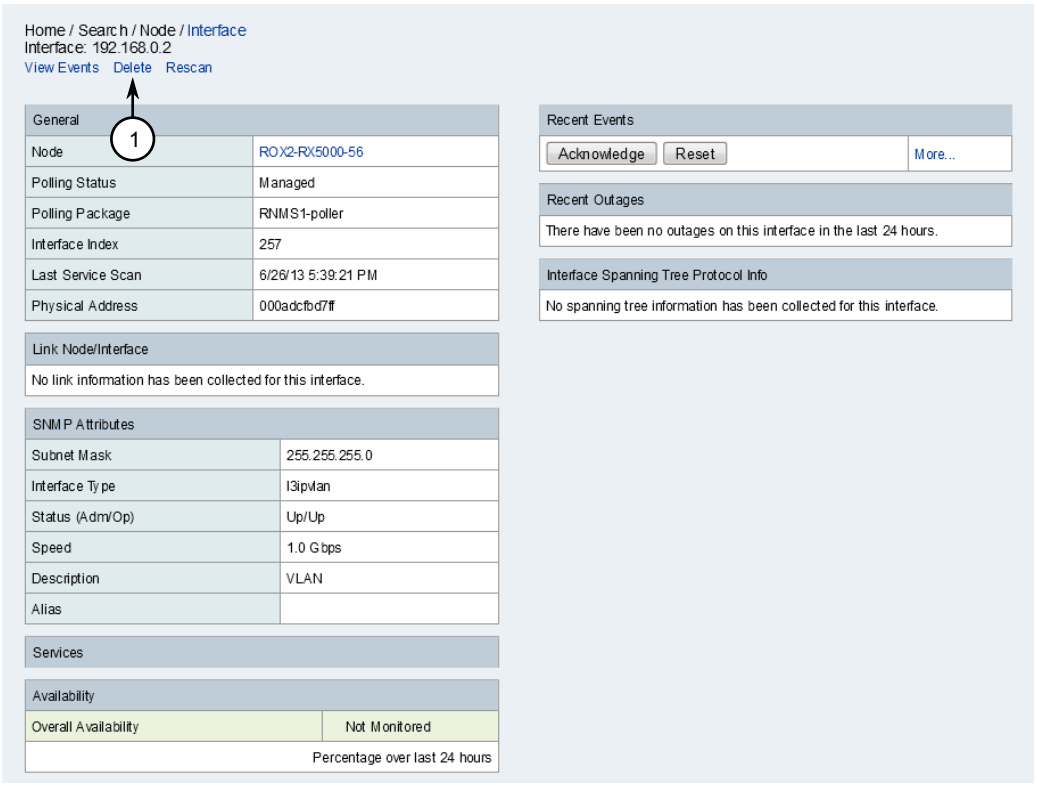


Figure 257: Links Screen

1. Delete Link

3. Click **Delete**. A confirmation message appears.
4. Click **OK**.

Section 6.4.7.6

Deleting a Service

To delete a service from an interface, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. Under **Availability**, select an interface. The **Interface** screen appears.

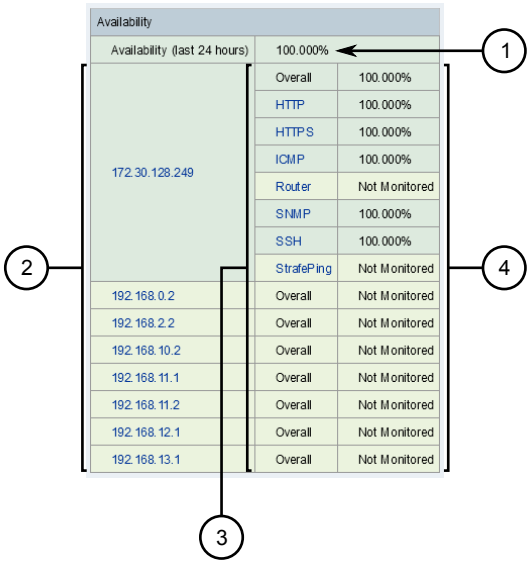


Figure 258: Availability Section

1. Overall Availability **2.** Interfaces **3.** Services **4.** Availability of Services

3. Select a service. The **Service** screen appears.

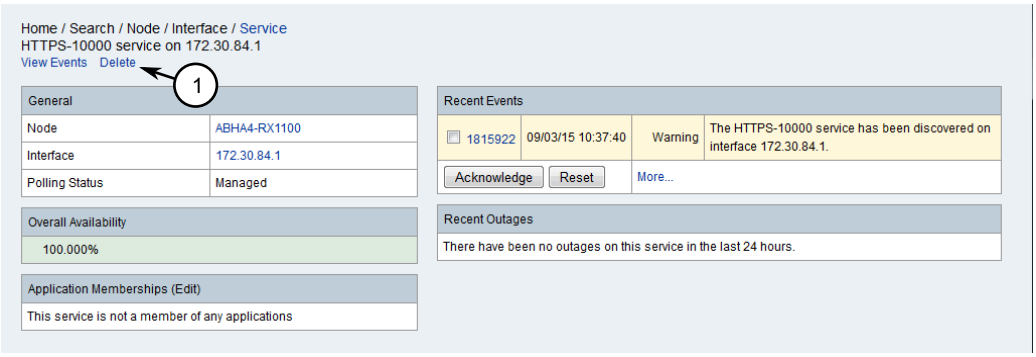


Figure 259: Service Screen

1. Delete Link

4. Click **Delete**. A confirmation message appears.
5. Click **OK**.

Section 6.4.8

Managing Device Links

This section describes how to manage device links for devices managed by RUGGEDCOM NMS.

CONTENTS

Section 6.4.8.1

Viewing a List of Device Links

To view a list of device links, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. From the **Node** screen, click **View Node Link Detailed Info**. The **Links** screen appears.

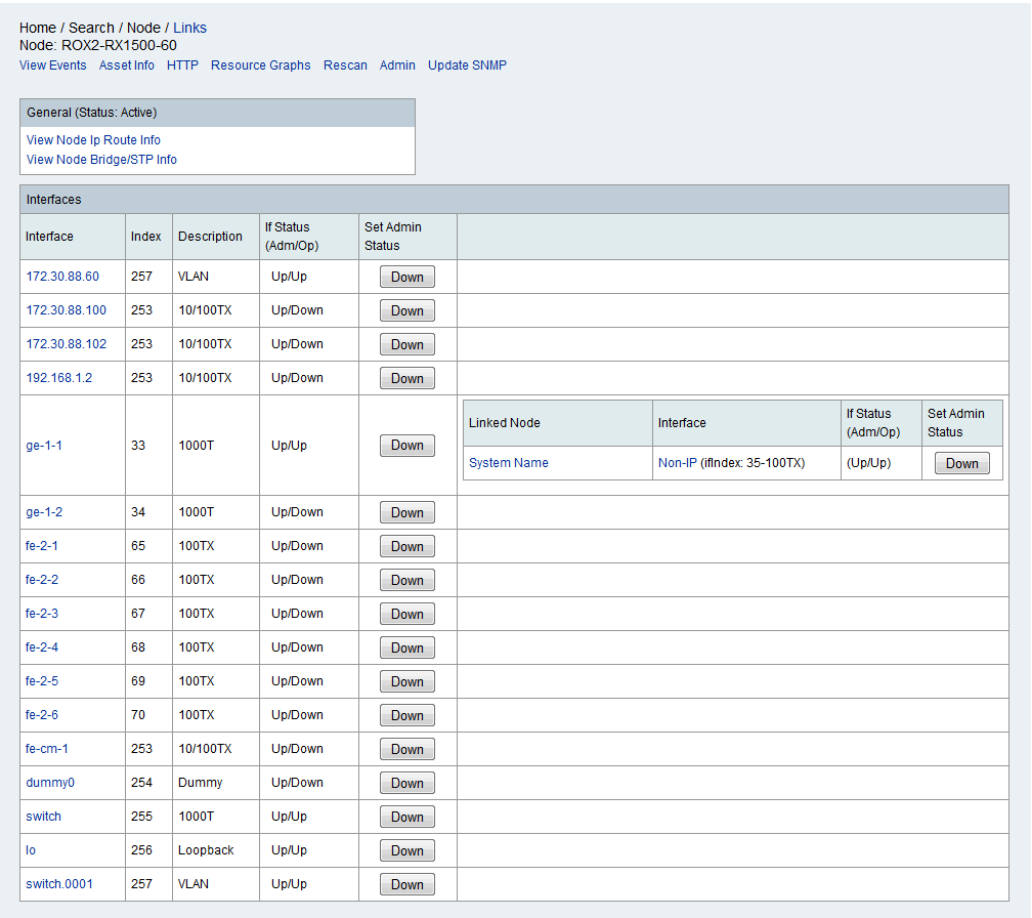


Figure 260: Links Screen

The **Interfaces** table displays the following information:

Column	Description
Interface	The IP address or label for the interface.
Linked Node	The label for the linked node.
Index	The SNMP index associated with the interface.
Description	The name associated with the interface.
If Status (Adm/Op)	The administrative and current operational status of the interface or linked node. For example, *Up/Down* indicates the administrative status is UP, but the operational status is DOWN.
Set Admin Status	Controls for manually setting the administrative status of the interface or linked node.

The table for linked nodes displays the following information:

Column	Description
Linked Node	The label for the linked node.
Interface	The IP address or label for the interface followed by the SNMP interface index and name in the form of *(ifIndex: N-name)*, where *N* is the SNMP interface index, and *name* is the associated name.
If Status (Adm/Op)	The administrative and current operational status of the interface or linked node. For example, *Up/Down* indicates the administrative status is UP, but the operational status is DOWN.
Set Admin Status	Controls for manually setting the administrative status of the interface or linked node.

Section 6.4.8.2
Setting the Administrative Status of Interfaces and Linked Nodes

To set the administrative status of an interface or linked node to either UP or DOWN, do the following:

IMPORTANT!
SNMP must be properly configured on the target device for RUGGEDCOM NMS to successfully send **`set`** *commands.*

1. Display details for the chosen device. For more information, refer to Section 6.4.2, "Viewing Device Details" .
2. From the **Node** screen, click **View Node Link Detailed Info**. The **Links** screen appears.

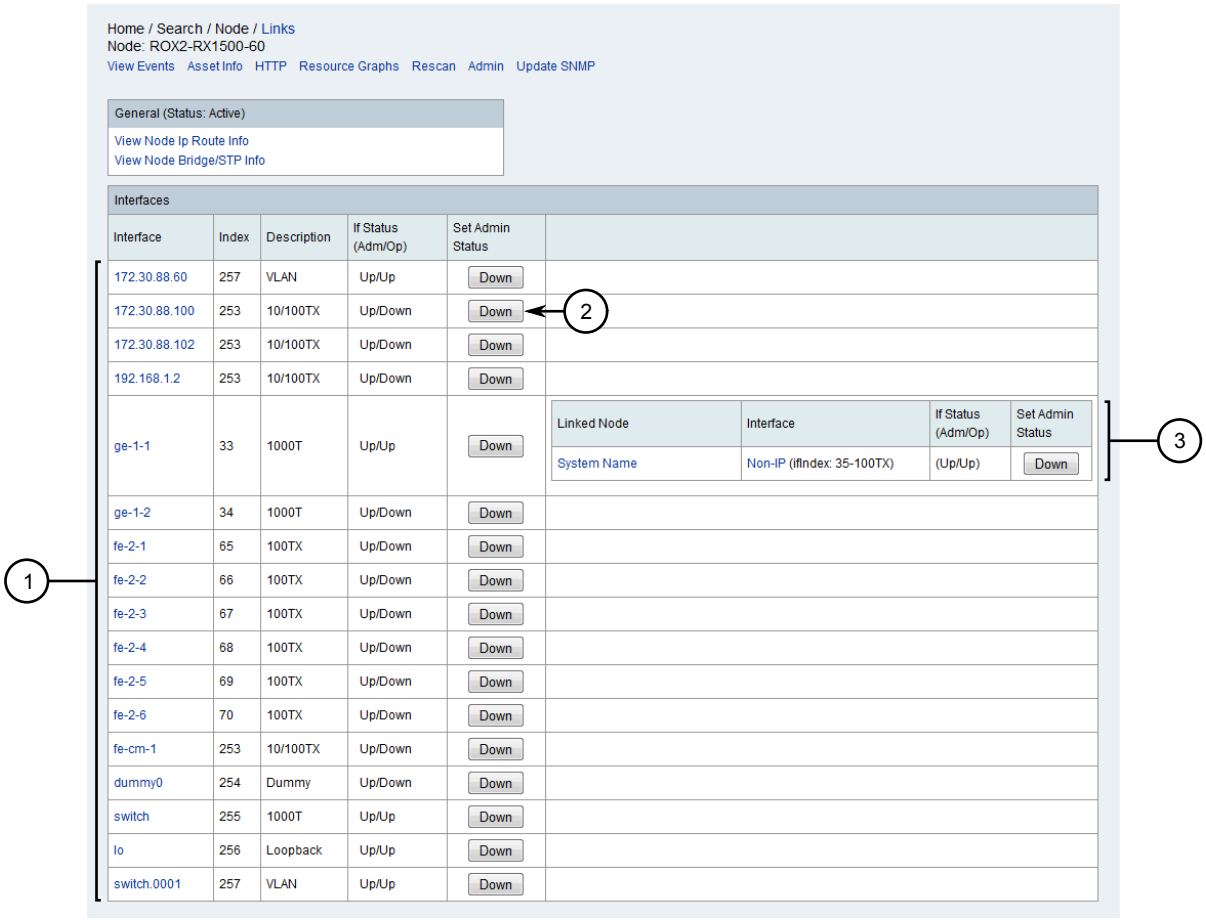


Figure 261: Links Screen

1. Available Interfaces **2.** Down/Up Button **3.** Available LInked Nodes

The **If Status** column indicates the administrative and current operational status of the interface or linked node.

NOTE
A user must have SNMP Write Community access to a device to change the status, otherwise a notification will appear. For more information about configuring SNMP, refer to *Section 6.5.1, "Configuring SNMP Globally"* *.*

3. Under **Set Admin Status**, for the desired interfaces and/or linked nodes, click **Up** to bring the interface up, or click **Down** to bring the interface down, depending on its current administrative status.

Section 6.4.9

Managing Asset Information

Information about each device, or asset, managed by RUGGEDCOM NMS should be maintained within RUGGEDCOM NMS for quick reference. RUGGEDCOM NMS allows information about a device's :

- serial number
- manufacturer
- installation date
- physical location
- vendor
- ...and much more

Devices can also be assigned to one of the pre-defined categories to help better organize asset information.

CONTENTS

Section 6.4.9.1

Editing Asset Information

To edit the asset information for a device managed by RUGGEDCOM NMS, do the following:

NOTE

The following procedure describes how to define the asset information for a single device. If asset information is the same or similar for multiple devices, consider first defining the information in a Comma-Separated Value (CSV) file and importing it for each device. Unique information can be added/modified afterwards using this procedure.

For more information about importing asset information, refer to Section 6.4.9.2, "Importing/Exporting Device Information".

1. On the menu bar, click **Assets**. The **Assets** screen appears.

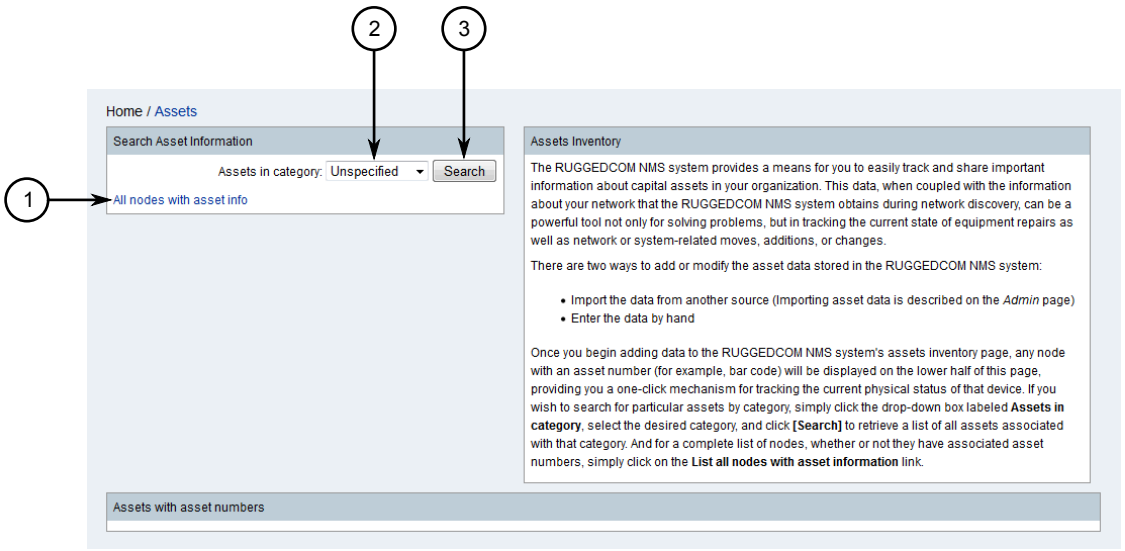


Figure 262: Assets Screen

1. All Nodes With Asset Information Link **2.** Assets In Category List **3.** Search Button

2. Search for the required device using the search tools. If the asset information already exists for the node, click **All Nodes With Asset Information** to display a list of devices that have asset information. Or select a category from the **Assets in Category List** and click **Search** to display a list of devices that fall under the selected category. The **Asset List** screen appears.

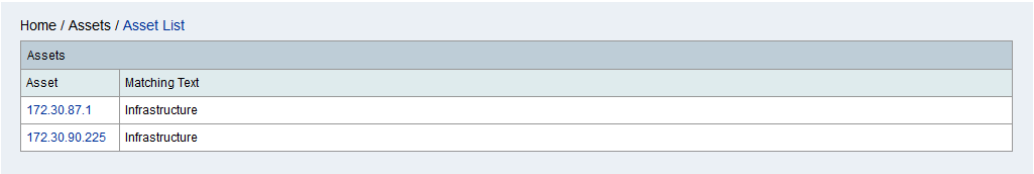


Figure 263: Asset List Screen

3. Select a device. The **Modify** screen appears.

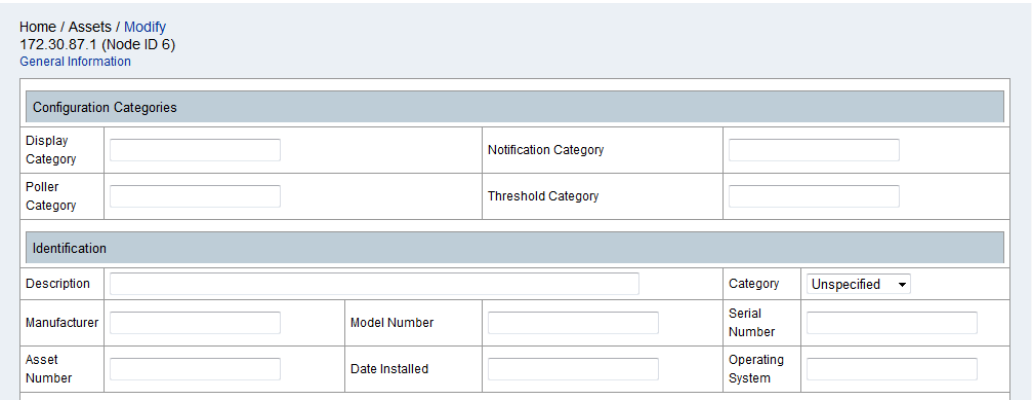


Figure 264: Modify Screen

4. Under **Configuration Categories**, configure the following parameters as required:

> **NOTE**
> *The name of each category is user-defined.*

Parameter	Description
Display Category	A custom display category associated with the asset.
Notification Category	A custom notification category associated with the asset.
Poller Category	A custom poller category associated with the asset.
Threshold Category	A custom threshold category associated with the asset.

5. Under **Identification**, configure the following parameters as required:

Parameter	Description
Description	A description of the device.
Category	**Synopsis:** { Unspecified, Infrastructure, Server, Desktop, Laptop, Printer, Telephony, Other } **Default:** Unspecified The category to which the device belongs. Use categories to better sort and find asset information.
Manufacturer	The name of the device's manufacturer.
Model Number	The device's model number.
Serial Number	The device's serial number.
Asset Number	The device's asset number.
Date Installed	The date the device was installed.
Operating System	The operating system installed on the device.

6. Under **Location**, configure the following parameters as required:

Parameter	Description
Region	The region where the device is located.
Division	The division within the company responsible for the device.
Department	The department within the company responsible for the device.
Address 1 Address 2	The address where the device is located.
City	The city where the device is located
State	The state/province where the device is located.
ZIP	The ZIP/postal code for the location.
Building	The name of the building where the device is located.
Floor	The floor name or number where the device is located.
Room	The room name or number where the device is located.
Rack	The rack name or number where the device is located.
Slot	The slot in the rack where the device is installed.
Port	The port used at the facility.
Circuit ID	The ID of the circuit used at the facility.

7. Under **Vendor**, configure the following parameters as required:

Parameter	Description
Name	The name of the vendor responsible for the device.
Phone	The vendor's phone number.
Fax	The vendor's fax number.
Lease	Details of the lease agreement.
Lease Expires	The expiry date for the lease.
Vendor Asset	The vendor's asset information.
Main Contract	Details of the main contract.
Contract Expires	The expiry date for the vendor's contract.
Maint Phone	The vendor's support phone number.

8. Under **Comments**, type additional information about the asset.
9. Click **Submit**.

Section 6.4.9.2
Importing/Exporting Device Information

To import or export information about a device, or asset, managed by RUGGEDCOM NMS, do the following:

Importing Asset Information

1. On the menu bar, click **Admin**, click **Import and Export Asset Information** and then click **Import Assets**. The **Import Assets** screen appears.

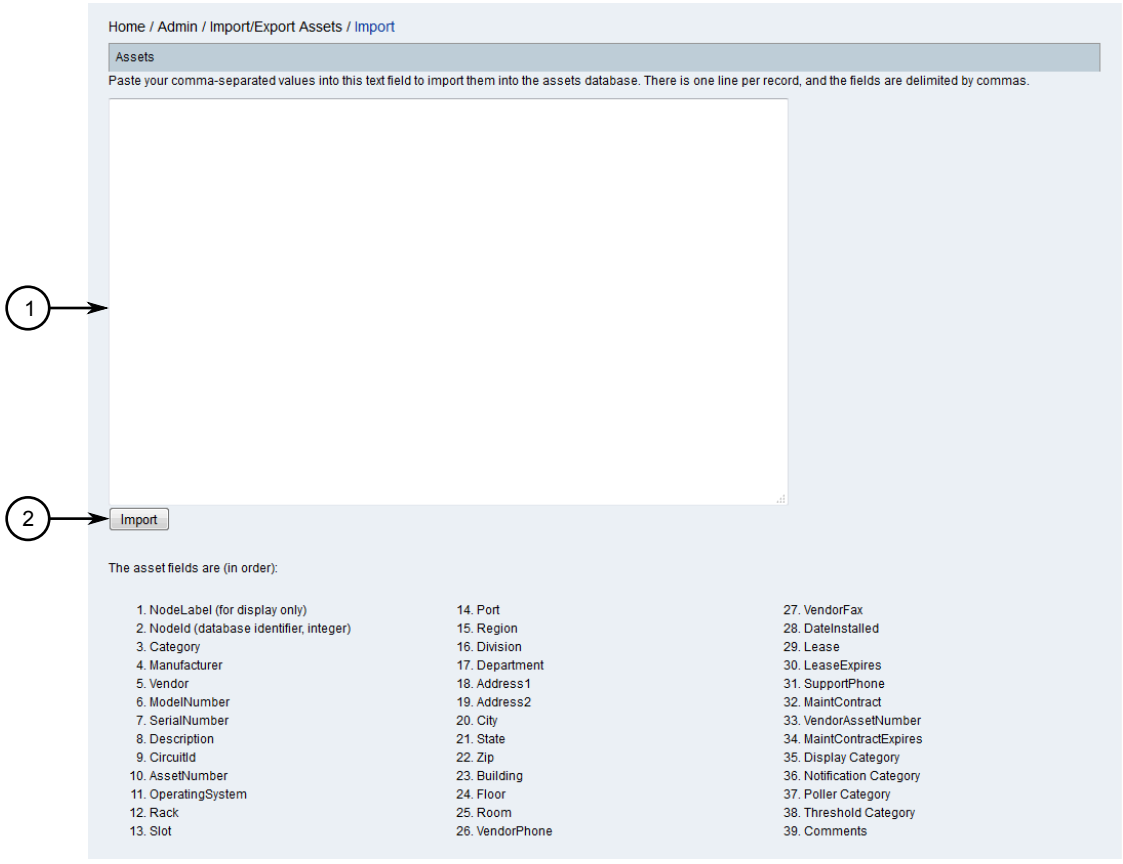


Figure 265: Import Assets Screen

1. Asset Information Box **2.** Import Button

2. Make sure the asset information to be imported includes only the following parameters:

Address1	Description	NodeId (Database Identifier, Integer)	Slot
Address2	Display Category	NodeLabel (Display Only)	State
AssetNumber	Division	Notification Category	SupportPhone
Building	Floor	OperatingSystem	Threshold Category
Category	Lease	Poller Category	Vendor
CircuitId	LeaseExpires	Port	VendorAssetNumber
City	MaintContract	Rack	VendorFax
Comments	MaintContractExpires	Region	VendorPhone
DateInstalled	Manufacturer	Room	Zip
Department	ModelNumber	SerialNumber	

3. Paste asset information into the box under **Assets**, making sure it is in Common-Separate Value (CSV) format.

» Exporting Asset Information

1. On the menu bar, click **Admin**, click **Import and Export Asset Information** and then click **Export Assets**. Information about each asset is displayed in Comma-Separated Value (CSV) format.
2. Save the file (`assets.csv`) or copy and paste the information into a spreadsheet editor and save the file as a CSV (*.csv) file.

Section 6.4.10

Managing Device Discovery

Device discovery is both a passive and purposeful process whereby devices on the network are discovered and added to the RUGGEDCOM NMS database, and polled for information about the services they may support.

- **Passive Discovery**
  During regular operation, RUGGEDCOM NMS actively listens for SNMP trap and syslog messages. If it receives a message of either type from a device that is not in its database, the device's IP address is automatically added to the database and the device is polled for information.

  NOTE
  Devices discovered passively are only added to the live database and not permanently added to the RUGGEDCOM NMS configuration. Their IP addresses are also not added to the list of IP address to be probed during the user-initiated discovery process.

- **Active Discovery**
  At launch, when initiated by a user, and at configured intervals, RUGGEDCOM NMS automatically seeks out active devices on the network. Devices that respond to RUGGEDCOM NMS's ICMP Echo request (ping) within the configured time period are added to database and polled for information about the services they support.

  IMPORTANT!
  Each ping is associated with a user-configurable timeout period. As such, device discovery should be configured carefully to prevent RUGGEDCOM NMS, whenever possible, from pinging non-existent devices.

Since passive discovery requires no configuration, this section focuses only on configuring and starting the active discovery process.

CONTENTS

- Section 6.4.10.6, “Starting Device Discovery”

Section 6.4.10.1
Configuring Device Discovery

To configure device discovery, do the following:

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

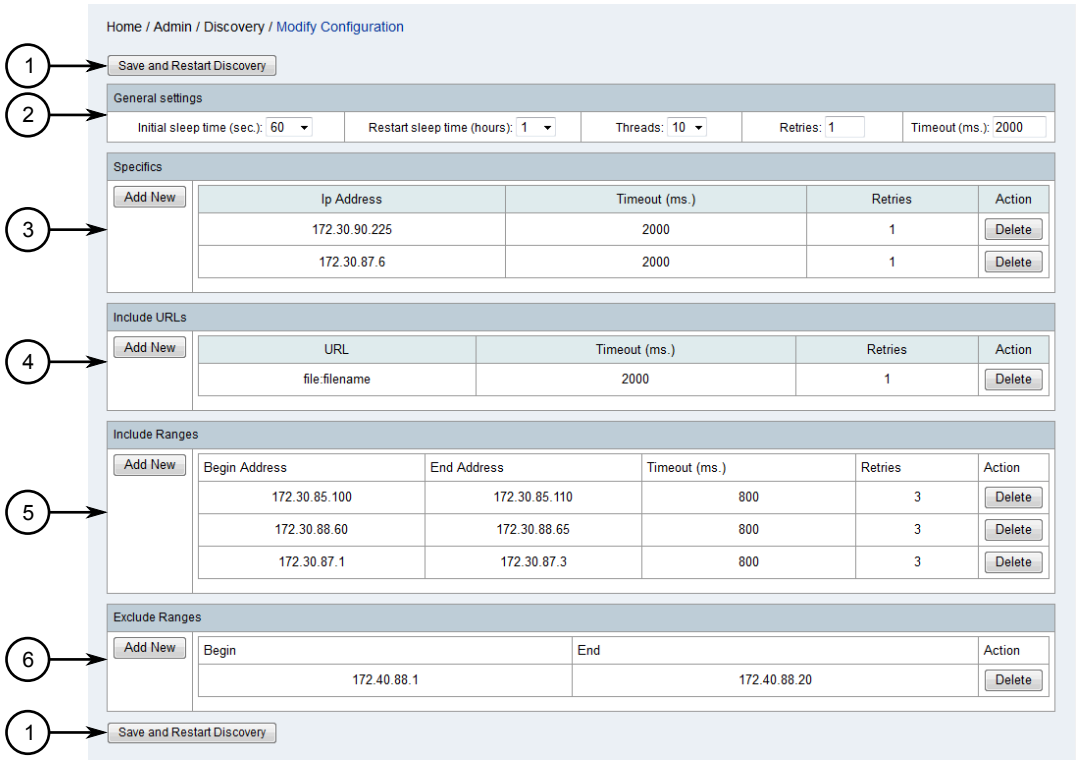


Figure 266: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **General Settings**, configure the following parameters:

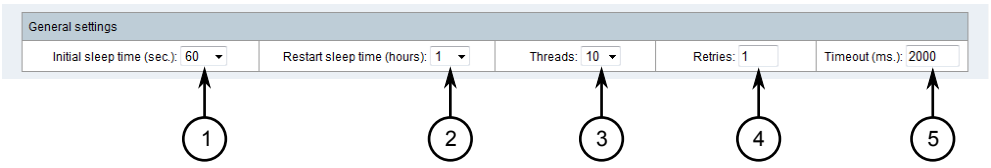


Figure 267: General Settings

1. Initial Sleep Time List **2.** Restart Sleep Time List **3.** Threads List **4.** Retries Box **5.** Timeout Box

Parameter	Description
Initial Sleep Time	**Synopsis:** { 30, 60, 90, 120, 150, 300, 600 } **Default:** 60 The time in seconds (s) to wait after RUGGEDCOM NMS starts before scanning known nodes for available services. A value of 30000, for example, will start the device discovery process 30 seconds after RUGGEDCOM NMS is started.
Restart Sleep Time	**Synopsis:** { 1, 2, 3, 4, 5, 6, 12, 24, 36, 72 } **Default:** 1 The time in hours (h) to wait after the device discovery process begins before starting again.
Threads	**Synopsis:** { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15 } **Default:** 10 The number of threads used by the discovery process.
Retries	**Default:** 1 The maximum number of attempts to query a given device. **IMPORTANT!** *A higher timeout value coupled with a larger number of retries can create significant overhead to the system. This is because non-responding IP addresses cause RUGGEDCOM NMS to wait for the timeout period to end for each retry before declaring the device nonexistent and moving on to the next IP address for discovery. Making the timeout too short and/or specifying too small a number of retries may cause RUGGEDCOM NMS to miss an active device, possibly every time the discovery process runs.*
Timeout	**Default:** 2000 The time in milliseconds (ms) the discovery process will wait for a response from a device.

3. [Optional] Add or delete specific IP addresses. For more information, refer to Section 6.4.10.2, "Adding/Deleting Specific IP Addresses" .
4. [Optional] Add or delete IP ranges. For more information, refer to Section 6.4.10.3, "Adding/Deleting IP Ranges" .
5. [Optional] Add or delete external lists of IP addresses. For more information, refer to Section 6.4.10.4, "Adding/Deleting External Lists of IP Addresses" .
6. [Optional] Add or delete excluded IP ranges. For more information, refer to Section 6.4.10.5, "Adding/Deleting IP Range Exclusions" .
7. Click **Save and Restart Discovery**. The discovery process begins using the new configuration settings.

Section 6.4.10.2
Adding/Deleting Specific IP Addresses

The device discovery process can be configured to scan specific IP addresses on the network for available services.

To add or delete a specific IP address, do the following:

Adding an IP Address

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

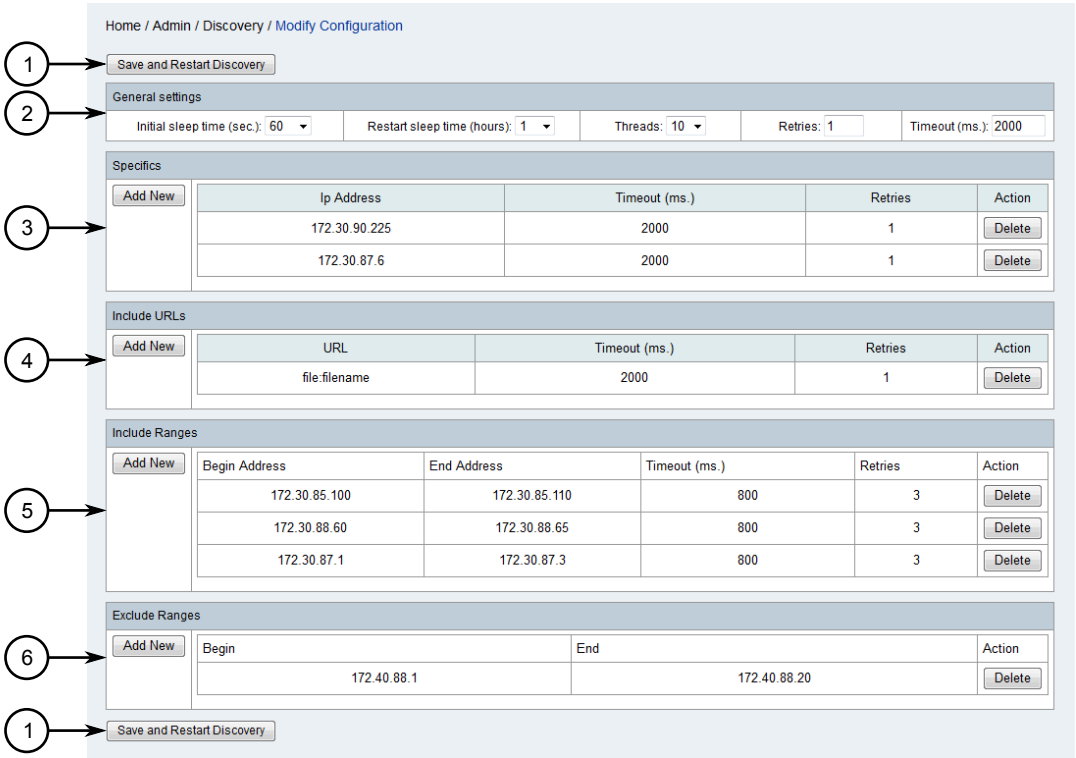


Figure 268: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **Specifics**, click **Add New**. A dialog box appears.

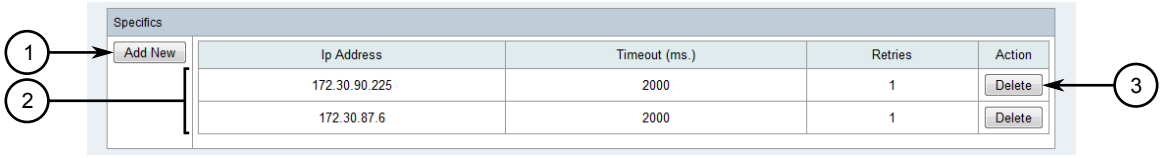


Figure 269: Specifics

1. Add New Button **2.** IP Addresses **3.** Delete Button

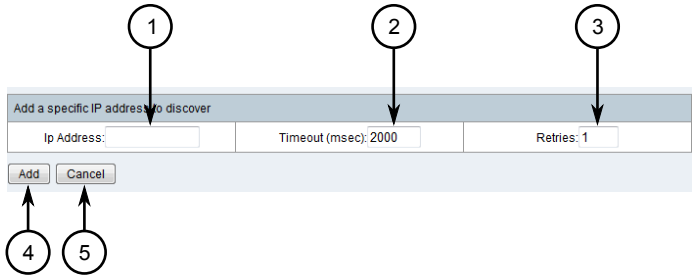


Figure 270: Dialog Box

1. IP Address Box **2.** Timeout Box **3.** Retries Box **4.** Add Button **5.** Cancel Button

3. Configure the following parameters:

Parameter	Description
IP Address	The IP address of the device to scan for available services each time device discovery is initiated.
Timeout	**Default:** 20000 The time in milliseconds (ms) to wait for a response from the device.
Retries	**Default:** 1 The maximum number of attempts to query the device.

4. Click **Add** to add the IP address.

» Deleting an IP Address

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

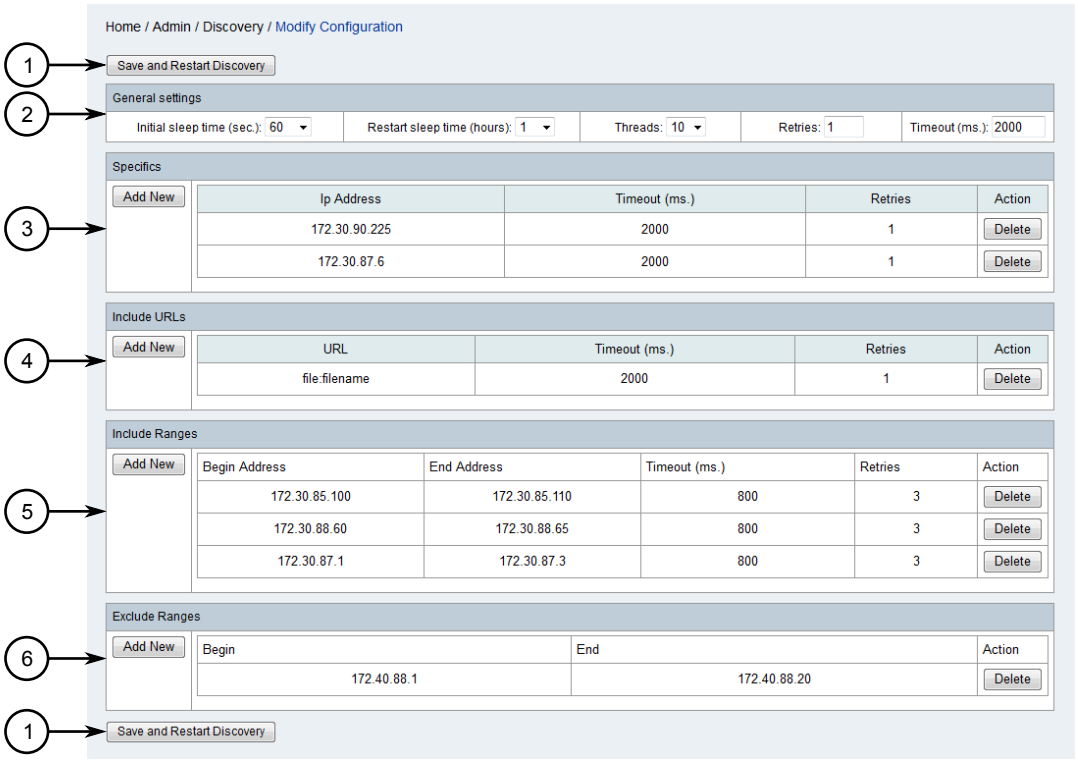


Figure 271: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **Specifics**, click **Delete** next to the chosen IP address. A confirmation dialog box appears.

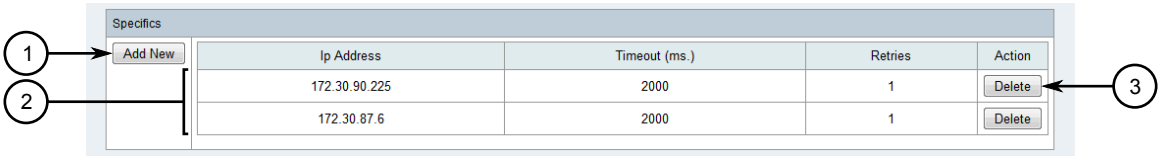


Figure 272: Specifics

1. Add New Button **2.** IP Addresses **3.** Delete Button

3. Click **OK** to delete the IP address.

Section 6.4.10.3

Adding/Deleting IP Ranges

The device discovery process can be configured to scan specific range of IP addresses on the network for available services.

To add or delete an IP address range, do the following:

Adding an IP Address Range

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

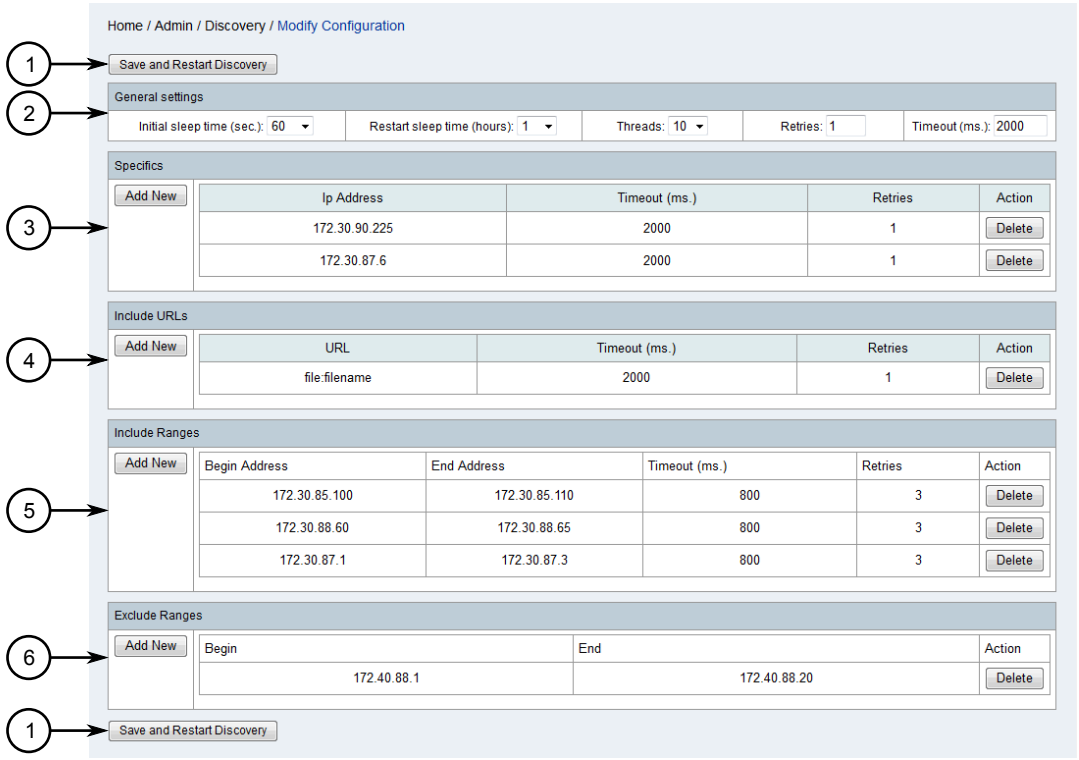


Figure 273: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **Include Ranges**, click **Add New**. A dialog box appears.

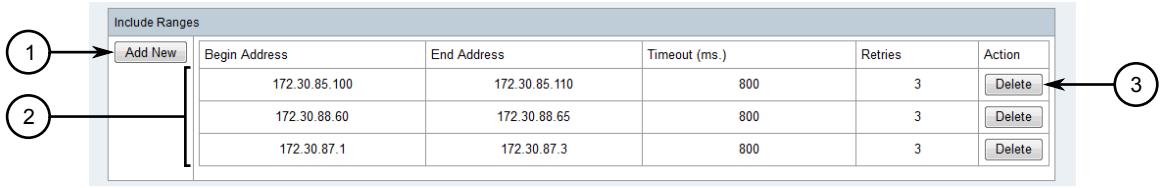


Figure 274: Include Ranges

1. Add New Button **2.** IP Address Ranges **3.** Delete Button

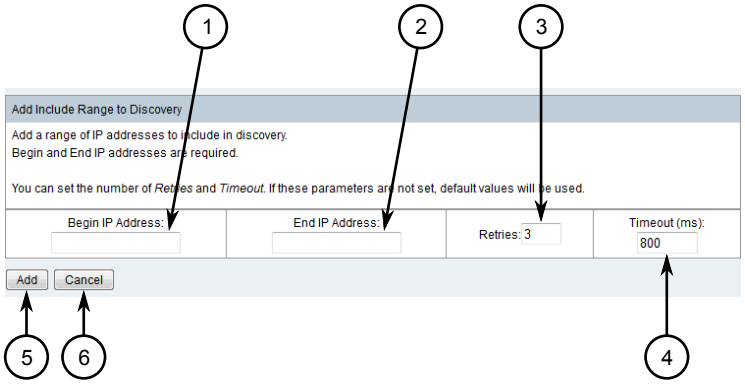


Figure 275: Dialog Box

1. Begin IP Address Box **2.** End IP Address Box **3.** Retries Box **4.** Timeout Box **5.** Add Button **6.** Cancel Button

3. Configure the following parameters:

Parameter	Description
Begin IP Address	The first IP address in the range.
End IP Address	The last IP address in the range.
Retries	**Default:** 3 The maximum number of attempts to query the devices in the IP address range.
Timeout	**Default:** 800 The time in milliseconds (ms) to wait for a response from the devices in the IP address range.

4. Click **Add** to add the IP address range.

» Deleting an IP Address Range

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

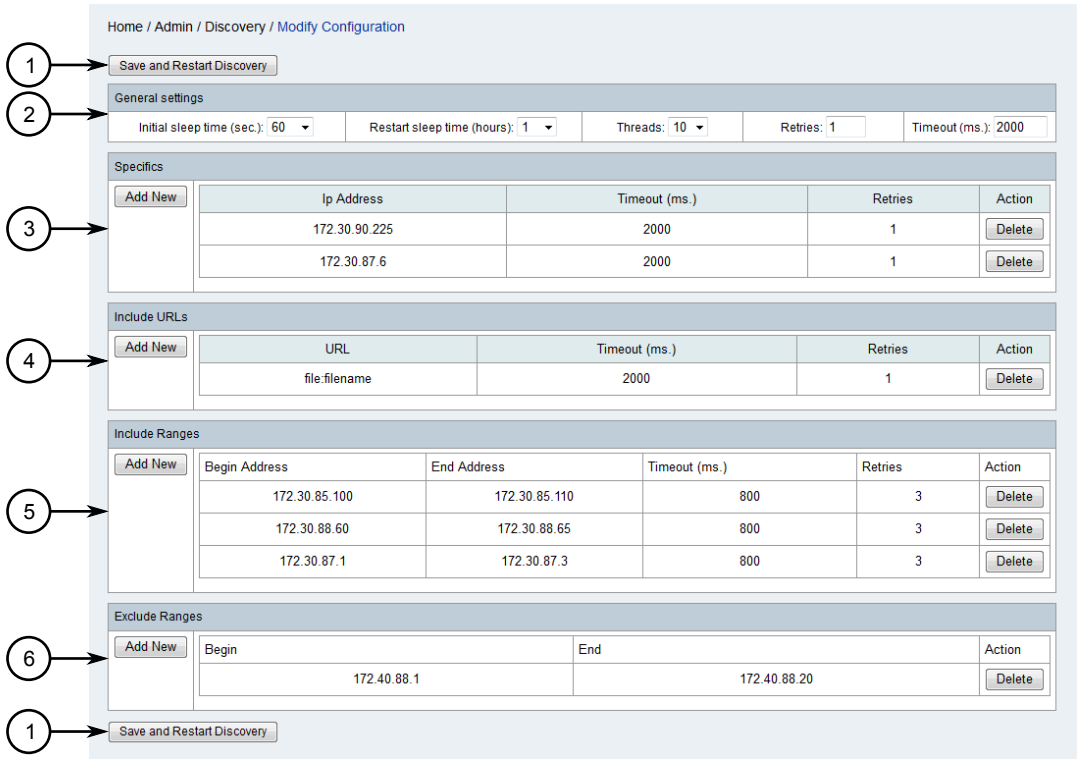


Figure 276: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **Include Ranges**, click **Delete** next to the chosen IP address range. A confirmation dialog box appears.

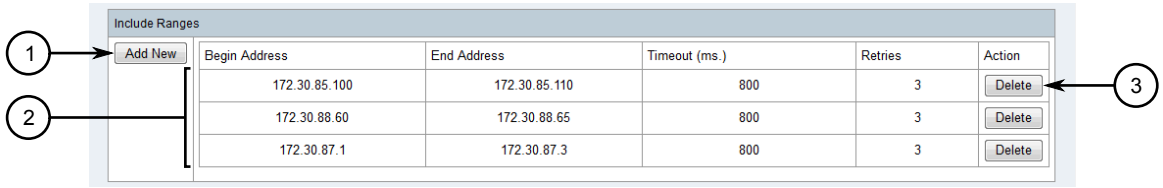


Figure 277: Include Ranges

1. Add New Button **2.** IP Addresses **3.** Delete Button

3. Click **OK** to delete the IP address range.

Section 6.4.10.4

Adding/Deleting External Lists of IP Addresses

The device discovery process can be configured to scan devices for available services based on an external list of IP addresses. The list must be saved as a plain text (*.txt) file.

```
# IP Address 172.30.185.2 172.30.185.5 172.30.88.10
```

NOTE
The text file can contain comments. Any line that begins with a # character, or is followed by a space a # character, is ignored.

To add or delete an external list of IP addresses, do the following:

Adding a List of IP Addresses

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

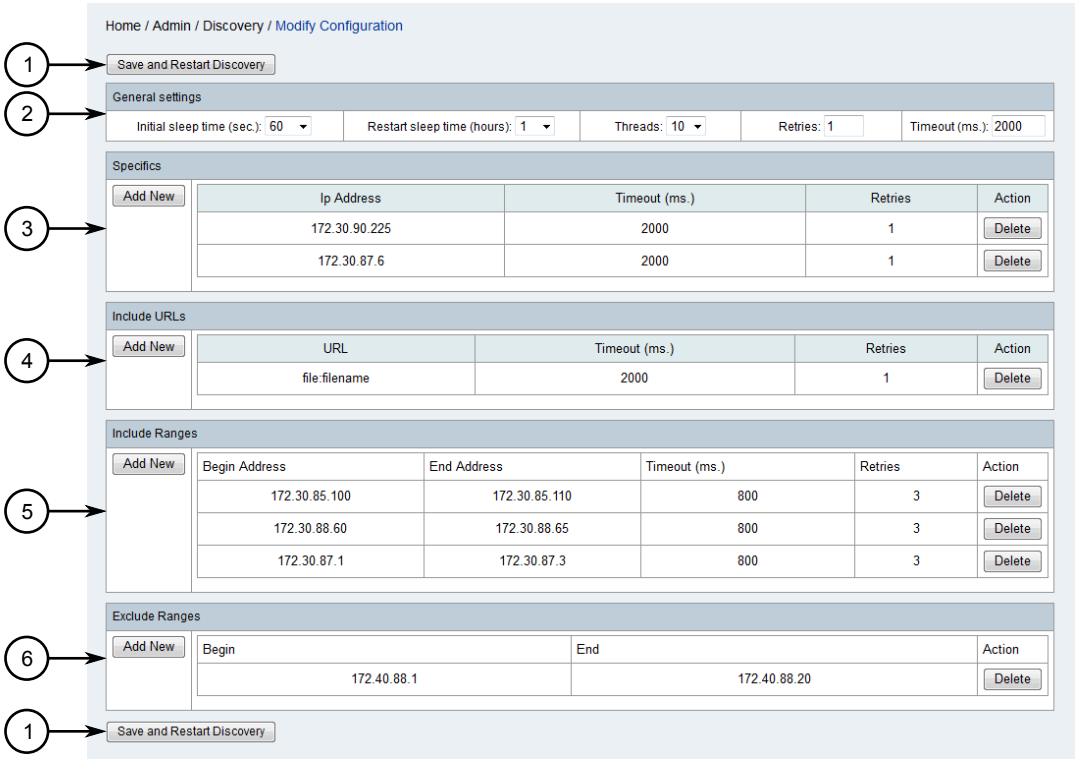


Figure 278: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **URLs**, click **Add New**. A dialog box appears.

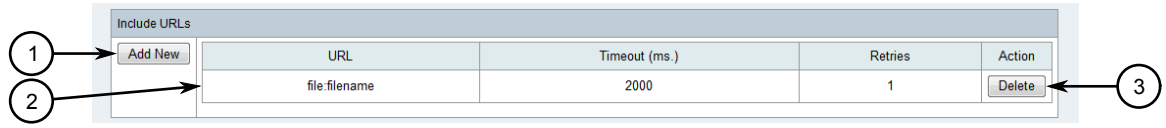


Figure 279: URLs

1. Add New Button **2.** URLs **3.** Delete Button

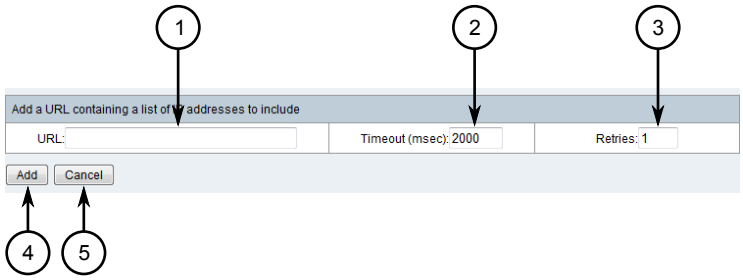


Figure 280: Dialog Box

1. URL Box **2.** Timeout Box **3.** Retries Box **4.** Add Button **5.** Cancel Button

3. Configure the following parameters:

Parameter	Description
URL	The full network path or Web address of the text file.
Timeout	**Default:** 20000 The time in milliseconds (ms) to wait for a response from each device in the list.
Retries	**Default:** 1 The maximum number of attempts to query each device in the list.

4. Click **Add** to add the list.

» Deleting a List of IP Addresses

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

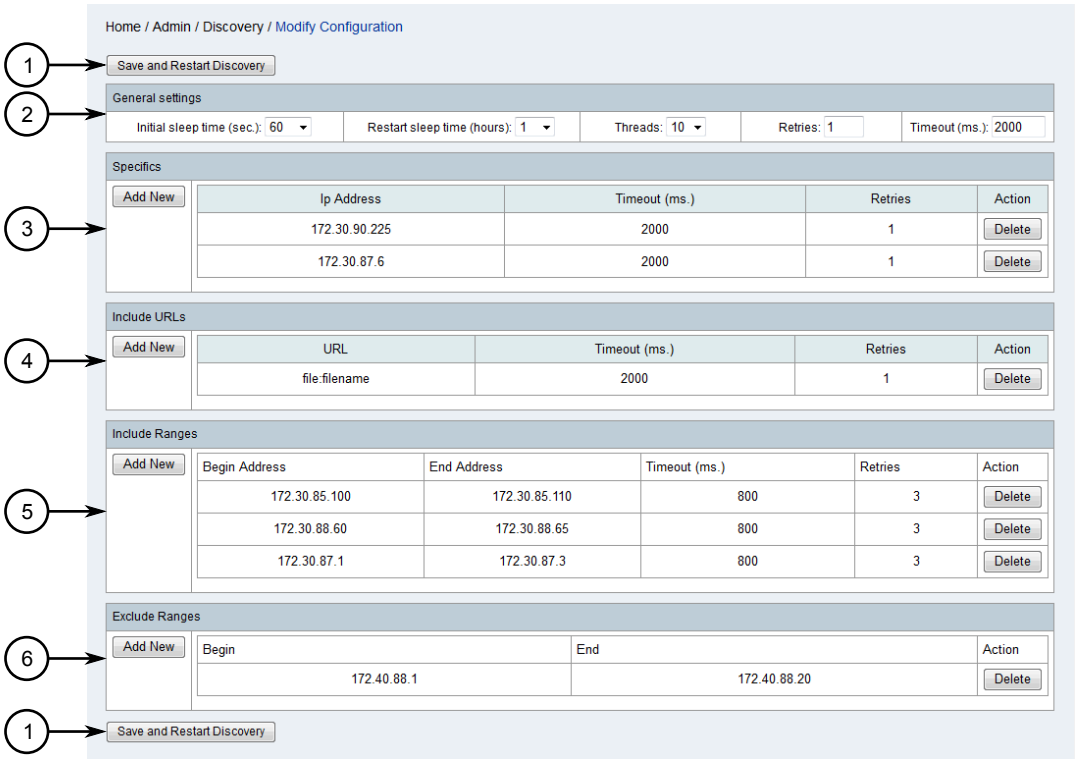


Figure 281: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **URLs**, click **Delete** next to the chosen list. A confirmation dialog box appears.

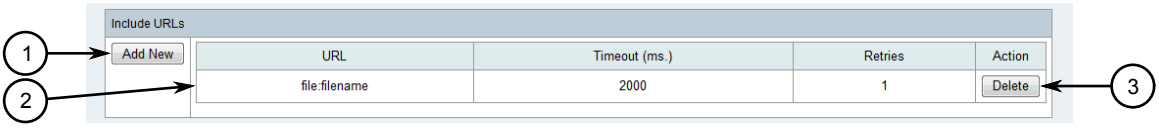


Figure 282: Include Ranges

1. Add New Button **2.** URLs **3.** Delete Button

3. Click **OK** to delete the list.

Section 6.4.10.5

Adding/Deleting IP Range Exclusions

The device discovery process can be configured to ignore or exclude IP addresses in a specific range.

To add or delete an IP address exclusion, do the following:

Adding an IP Address Exclusion

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

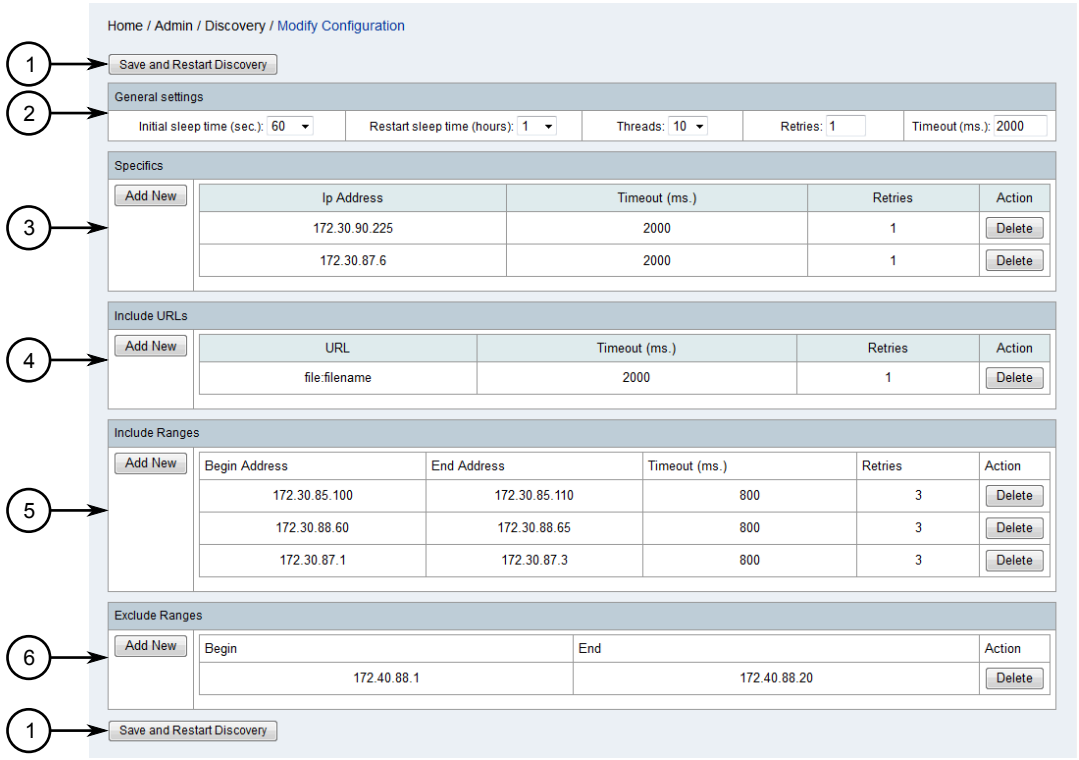


Figure 283: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **Exclude Ranges**, click **Add New**. A dialog box appears.

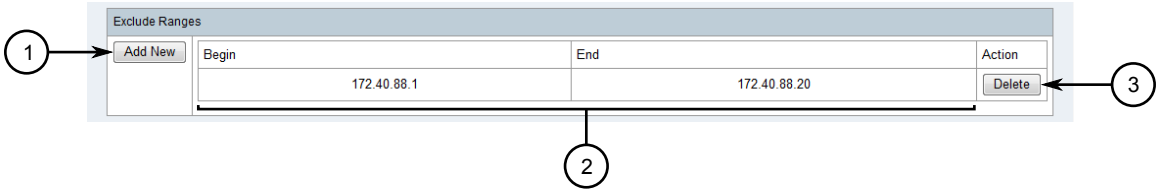


Figure 284: Exclude Ranges

1. Add New Button **2.** IP Address Ranges **3.** Delete Button

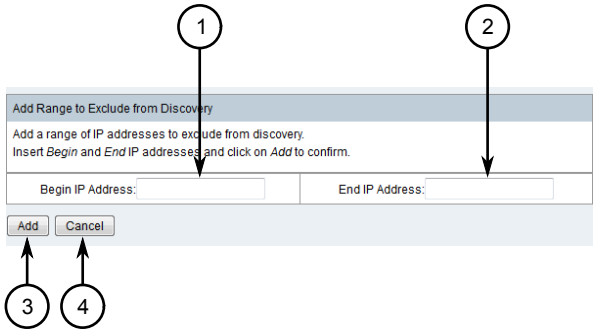


Figure 285: Dialog Box

1. Begin IP Address Box **2.** End IP Address Box **3.** Add Button **4.** Cancel Button

3. Configure the following parameters:

Parameter	Description
Begin IP Address	The first IP address in the range.
End IP Address	The last IP address in the range.

4. Click **Add** to add the IP address exclusion.

» Deleting an IP Address Range

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

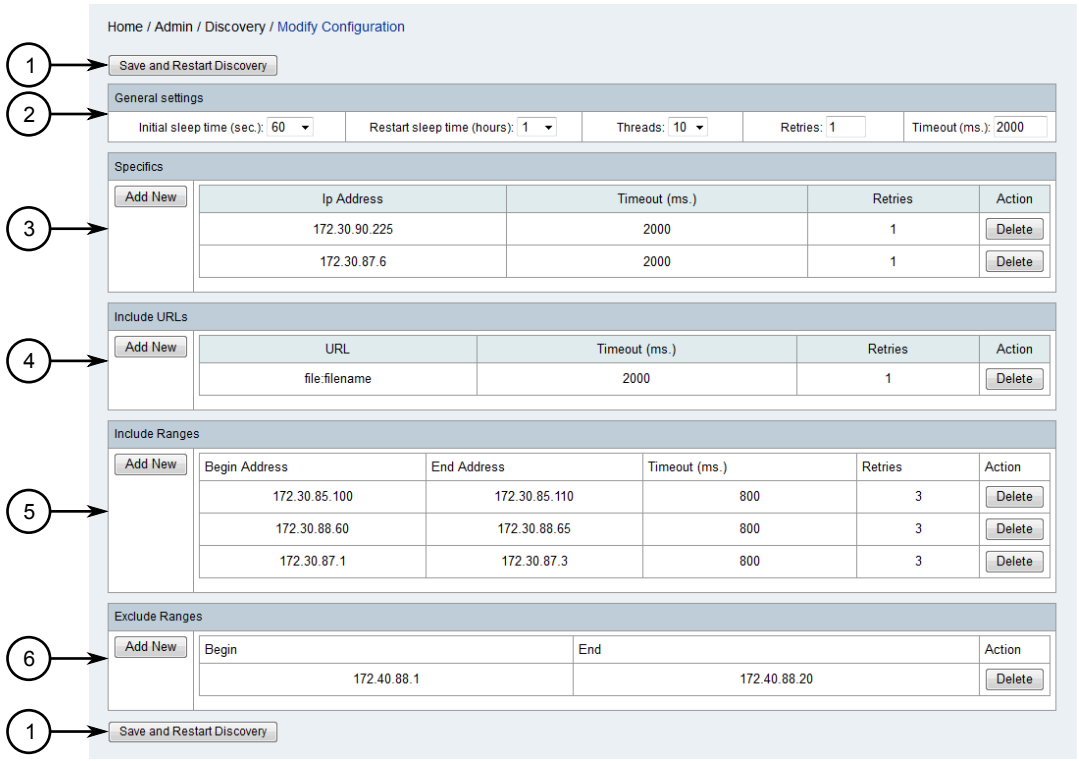


Figure 286: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Under **Exclude Ranges**, click **Delete** next to the chosen IP address exclusion. A confirmation dialog box appears.

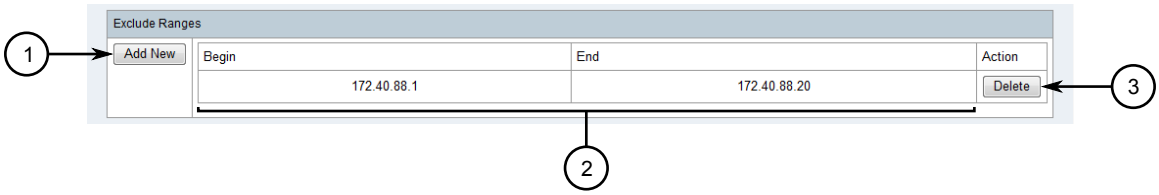


Figure 287: Exclude Ranges

1. Add New Button **2.** IP Addresses **3.** Delete Button

3. Click **OK**.

Section 6.4.10.6
Starting Device Discovery

The device discovery process is designed to initiate after launch and at set intervals thereafter. However, it must be restarted after the configuration settings have been modified, and can be initiated manually at any time.

To start the device discovery process manually, do the following:

1. On the menu bar, click **Admin**, click **Configure Discovery** and then click **Modify Configuration**. The **Modify Configuration** screen appears.

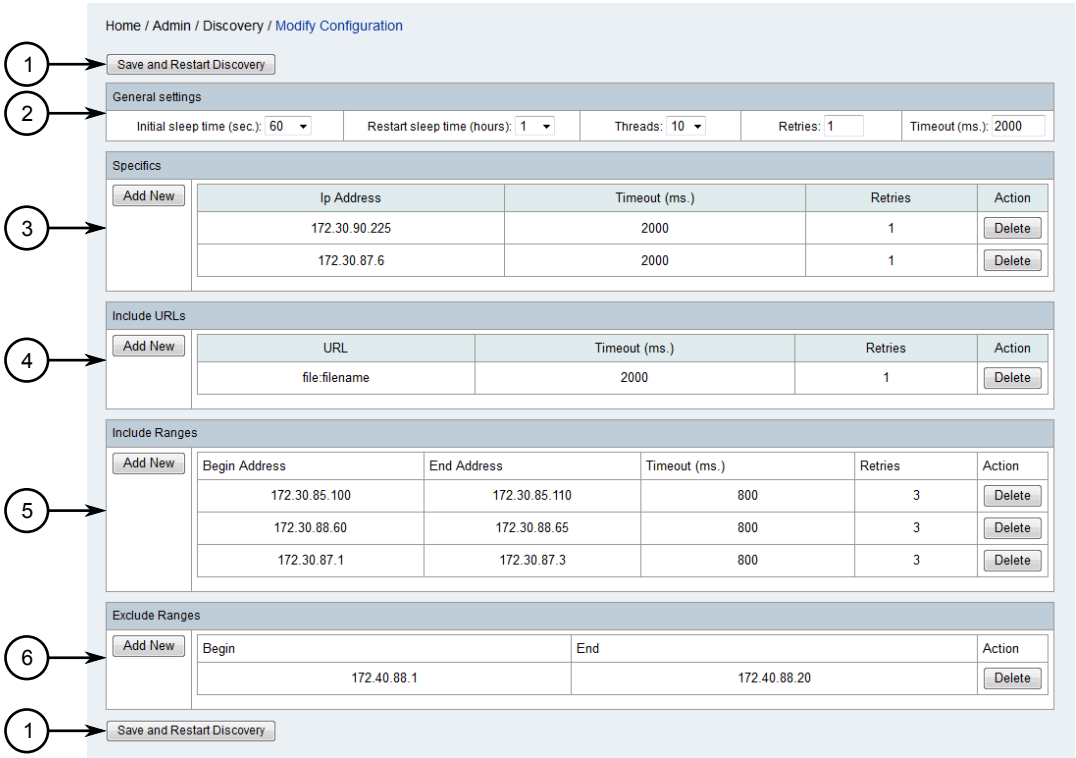


Figure 288: Modify Configuration Screen

1. Save and Restart Discovery Button **2.** General Settings **3.** Specific IP Address **4.** Specific URLs **5.** Specific IP Ranges **6.** Excluded IP Ranges

2. Click **Save and Restart Discovery**. The current settings are saved and the device discovery process begins.

Section 6.4.11
Managing Device Access

For RUGGEDCOM NMS to access the devices it manages, it must be supplied with a valid user profile and password/passphrase to use when configuring or polling the device(s). A user profile and password/passphrase

can be configured individual devices based on their IP addresses, or for a group of devices by specifying a range of IP addresses.

CONTENTS

Section 6.4.11.1

Viewing Device Access Information

To view access information for devices managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin** and then click **Configure Device Access**. The **Device Access** screen appears.

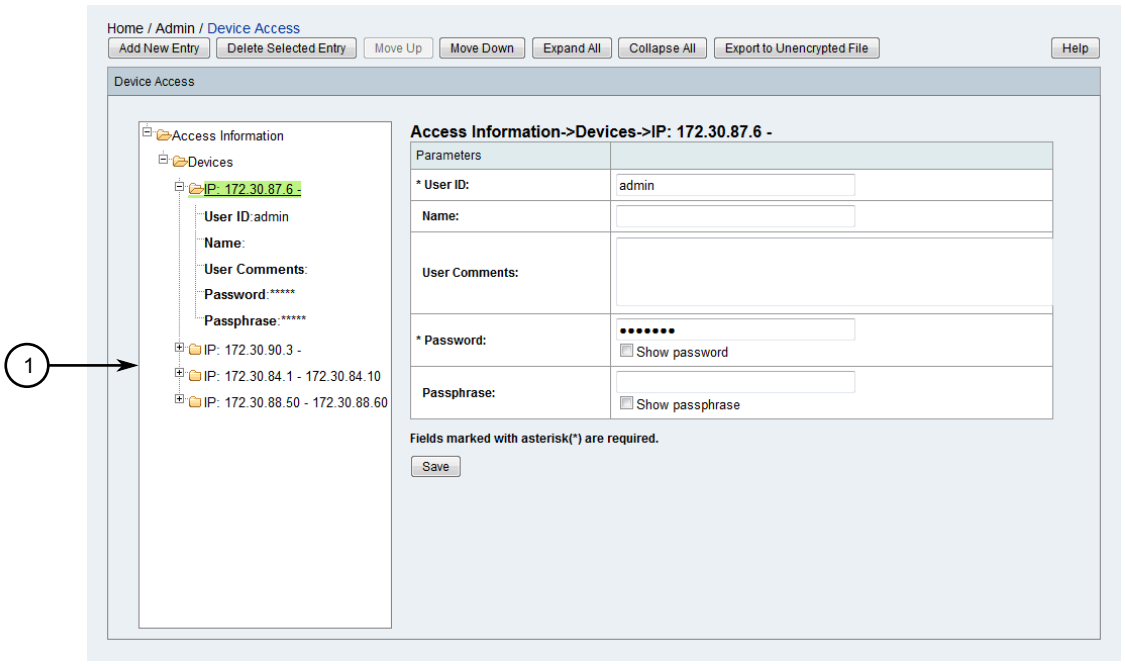


Figure 289: Device Access Screen

1. Tree Menu

2. In the tree menu, click **Access Information** and then click **Devices**. IP addresses for each device or IP ranges for multiple devices are displayed.
3. [Optional] Click an IP address or IP address range to display its configuration information in the tree menu and in a form layout.

Section 6.4.11.2
Adding/Editing Device Access Information

To add a device(s) or edit the existing access information for a device, do the following:

IMPORTANT!
For devices that have multiple IP address configured, a single entry for each IP address or an IP range entry for all IP addresses must be created.

1. On the menu bar, click **Admin** and then click **Configure Device Access**. The **Device Access** screen appears.

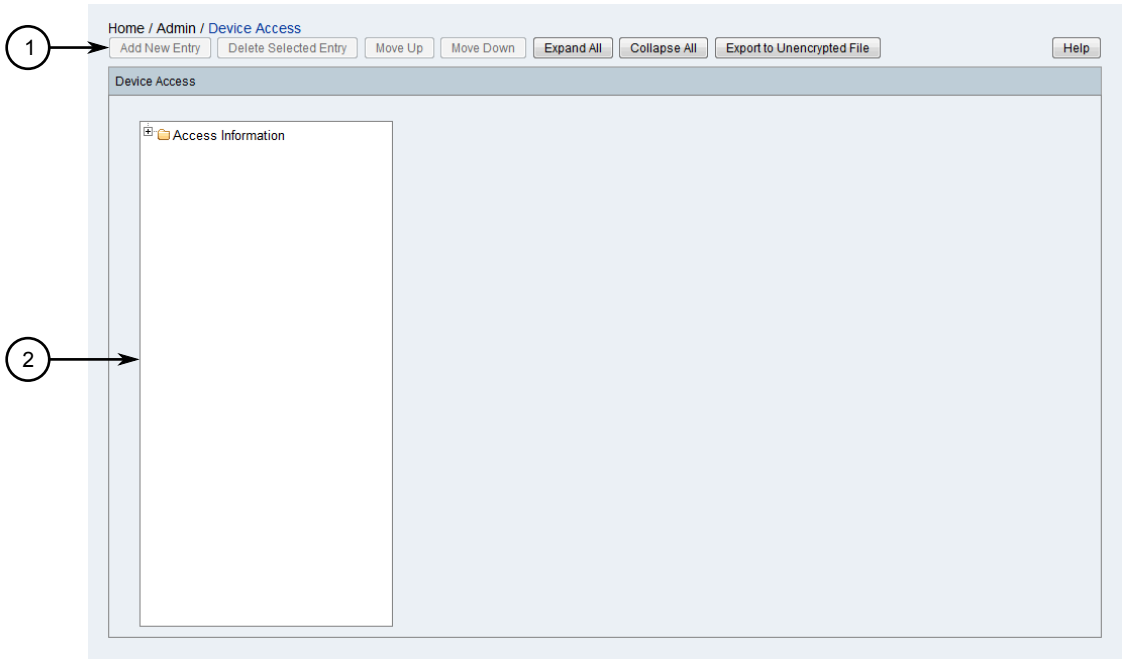


Figure 290: Device Access Screen

1. Add New Entry Button **2.** Tree Menu

2. In the tree menu, click **Access Information** and then click **Devices**.
3. Click **Add New Entry**, select an existing device by its IP address, or select multiple devices as represented by an IP range. A form appears.

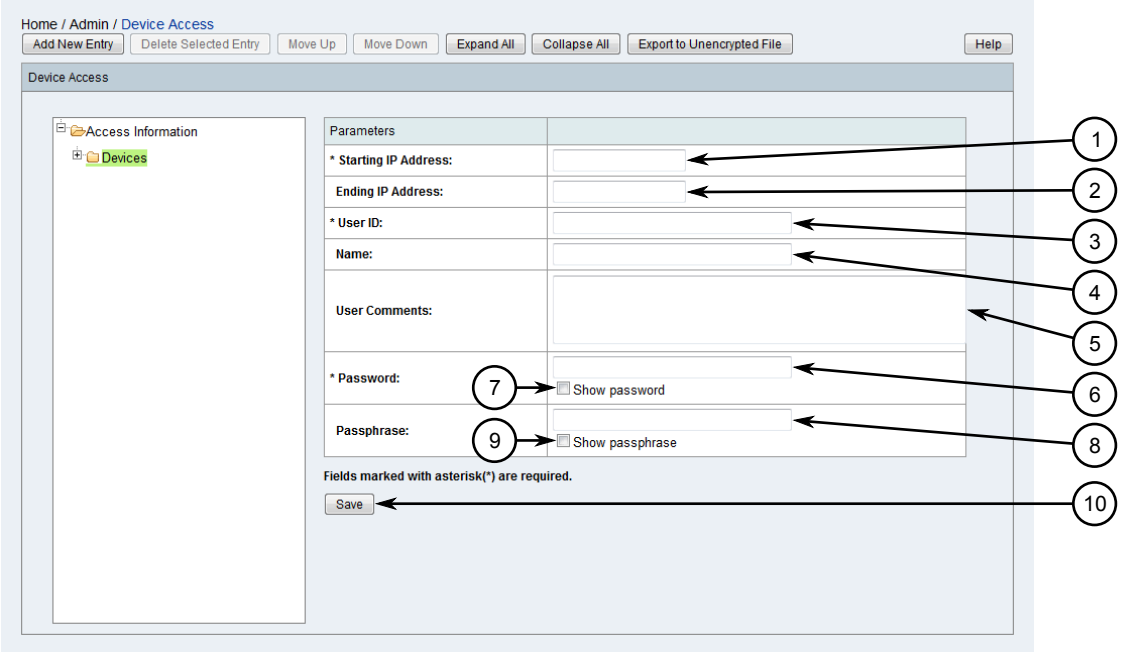


Figure 291: Device Access Form

1. Starting IP Address Box **2.** Ending IP Address Box **3.** User ID Box **4.** Name Box **5.** User Comments Box **6.** Password Box **7.** Show Password Check Box **8.** Passphrase Box **9.** Show Passphrase Check Box **10.** Save Button

4. [Optional] Select **Show Password** and/or **Show Passphrase** to display passwords/passphrases in plain text.
5. Configure the following parameters as required:

Parameter	Description
Starting IP Address	The IP address for the device or the first IP address in a range of IP addresses for multiple devices.
Ending IP Address	The last IP address in a range of IP addresses for multiple devices.
User ID	The name for the user profile to use to access the device(s). This is typically an administrator account.
Name	A unique name for the device(s).
User Comments	A comment or description related to the device(s).
Password	The password associated with the user ID.
Passphrase	The passphrase, if applicable, associated with the user ID. Only required for RUGGEDCOM ROS devices that have data storage encryption enabled.

6. Click **Save**.

NOTE
Different access information for the same device can be added if needed by adding multiple entries with different user names and passwords/passphrases configured. RUGGEDCOM NMS will

attempt to access the device with this information in sequential order. If RUGGEDCOM NMS is unable to access the device with the first set of credentials, it will try the next set of credentials.

*The order of the access information can be controlled using the **Move Up** and **Move Down** buttons.*

7. [Optional] Select the IP address or IP range and then click either **Move Up** or **Move Down** as needed.

Section 6.4.11.3

Deleting Device Access information

To delete access information for a device(s), do the following:

1. On the menu bar, click **Admin** and then click **Configure Device Access**. The **Device Access** screen appears.

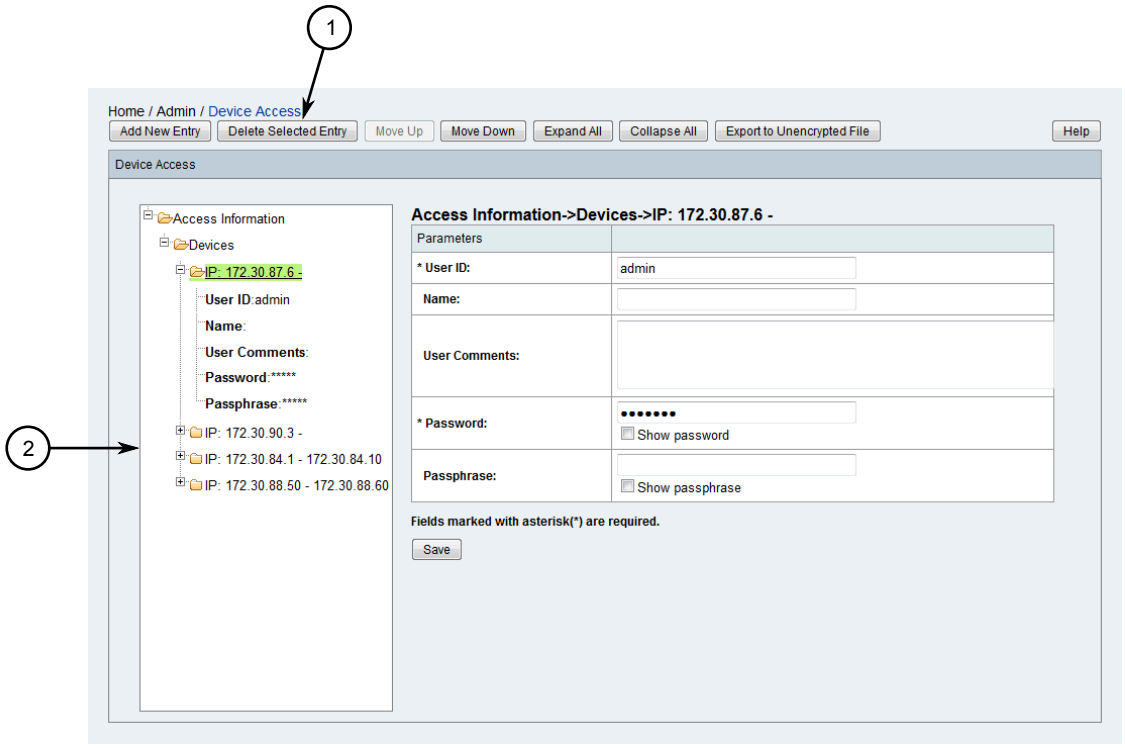


Figure 292: Device Access Screen

1. Delete Selected Entry Button **2.** Tree Menu

2. In the tree menu, click **Access Information** and then click **Devices**.
3. Select a device or IP range (for multiple devices) and then click **Delete Selected Entry**. A confirmation message appears.
4. Click **OK** to delete the device(s).

Section 6.4.11.4
Exporting Device Access Information

To export access information for all devices managed by RUGGEDCOM NMS to an unencrypted XML file, do the following:

1. On the menu bar, click **Admin** and then click **Configure Device Access**. The **Device Access** screen appears.

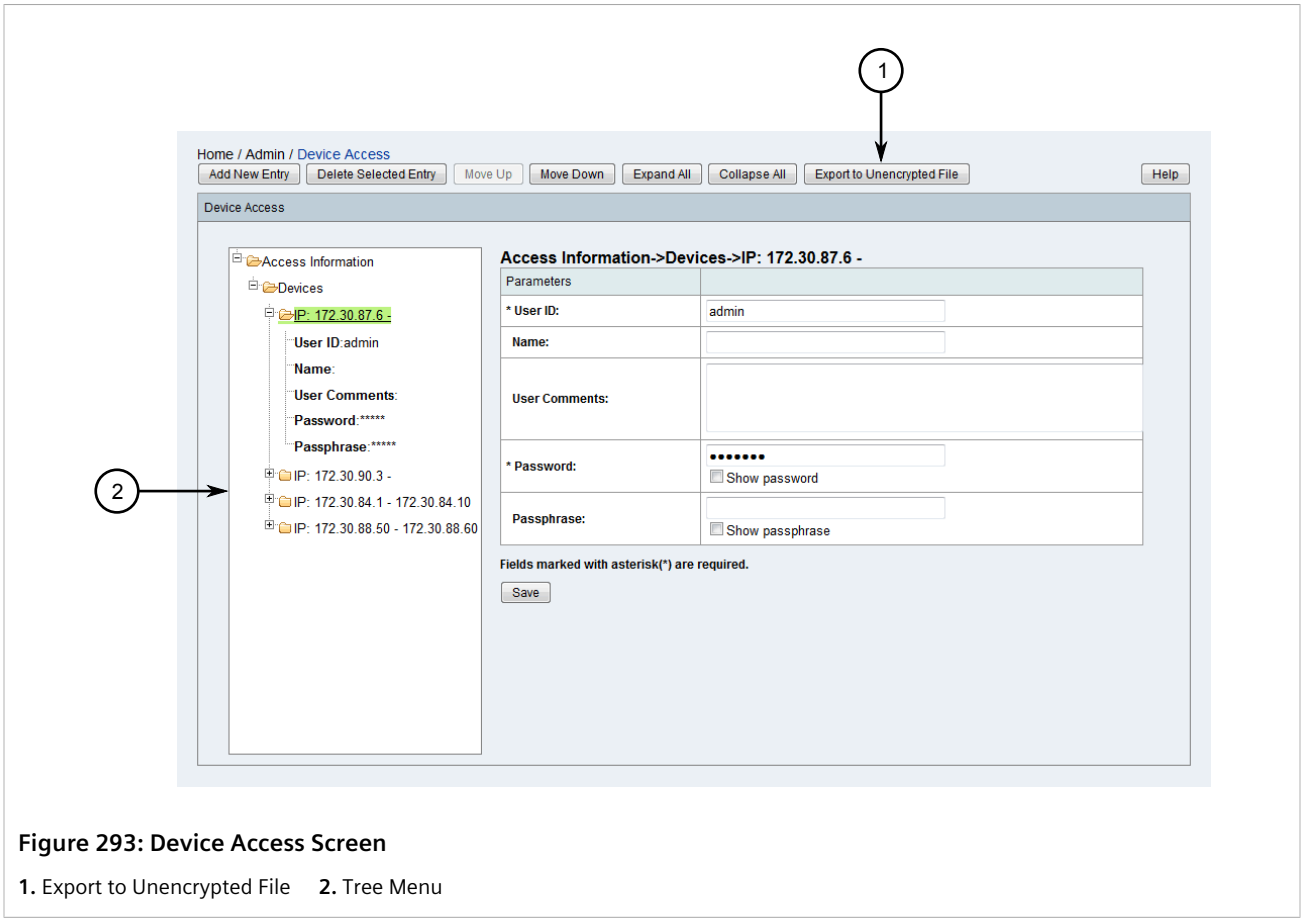


Figure 293: Device Access Screen

1. Export to Unencrypted File **2.** Tree Menu

2. Click **Export to Unencrypted File**. A dialog box appears.
3. Choose to open or save the generated XML file and then click **OK**.

Section 6.4.12
Managing Device Passwords

Passwords for each managed device (excluding ROX II based devices) can be controlled centrally by RUGGEDCOM NMS using the device password management utility. The utility applies the password to all devices of the same type, such as ROS, ROX or WIN devices.

All passwords are stored by RUGGEDCOM NMS in an XML file that can be encrypted for added security. For more information, refer to Section 4.10, “Managing Data Encryption” .

To troubleshoot connection problems, the XML file that contains device access passwords can be validated to identify devices whose passwords have been changed manually since they were last synchronized with the device password management utility.

IMPORTANT!
Support for device password management is only available for WIN devices that have the version 4.4 (or higher) operating system installed.

CONTENTS

Section 6.4.12.1
Validating Device Passwords

Device passwords stored by RUGGEDCOM NMS for managed ROS, ROX and WIN devices, can be validated to verify they are still correct.

The validation process also helps RUGGEDCOM NMS analyze IP ranges to determine which device types are within range. This information is used when updating passwords for a specific device type. For example, when updating the passwords for ROS devices, if an IP range includes ROX devices, RUGGEDCOM NMS will only apply the new password to the ROS-based devices.

IMPORTANT!
For RUGGEDCOM NMS to manage devices properly, failed passwords should be addressed immediately.

NOTE
A typical reason for a validation failure would be that RUGGEDCOM NMS has discovered a device on the network for which no access credentials have been configured. For more information about configure credentials for devices, refer to Section 6.4.11.2, "Adding/Editing Device Access Information" .

To validate the stored passwords for managed ROS, ROX and WIN devices, do the following:

1. Make sure valid device access is configured for each RUGGEDCOM device managed by RUGGEDCOM NMS. For more information, refer to Section 6.4.11.2, "Adding/Editing Device Access Information" .
2. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Device Password Management**. The **Device Password** screen appears.

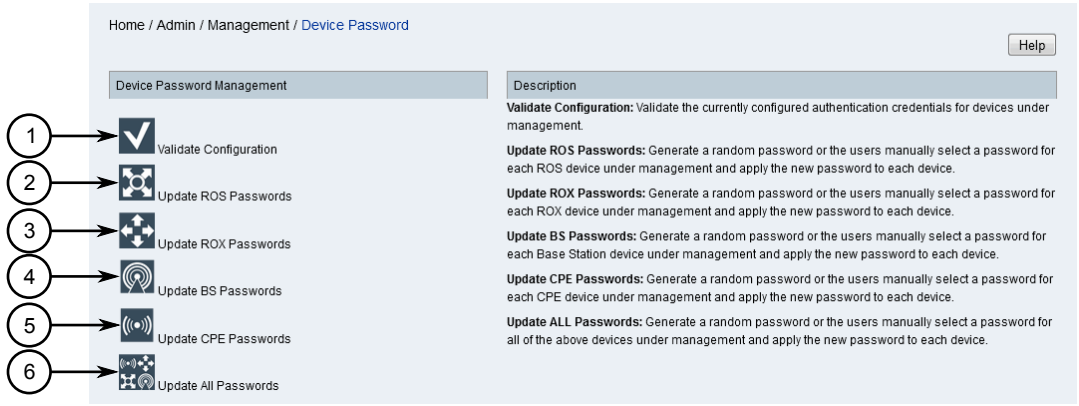


Figure 294: Device Password Screen

1. Validate Configuration Icon **2.** Update ROS Passwords Icon **3.** Update ROX Passwords Icon **4.** Update BS Passwords Icon **5.** Update CPE Passwords Icon **6.** Update All Passwords Icon

3. Click the **Validate Configuration** icon. A confirmation dialog box appears.
4. Click **OK**. The validation process begins, after which the **Validate** screen appears.

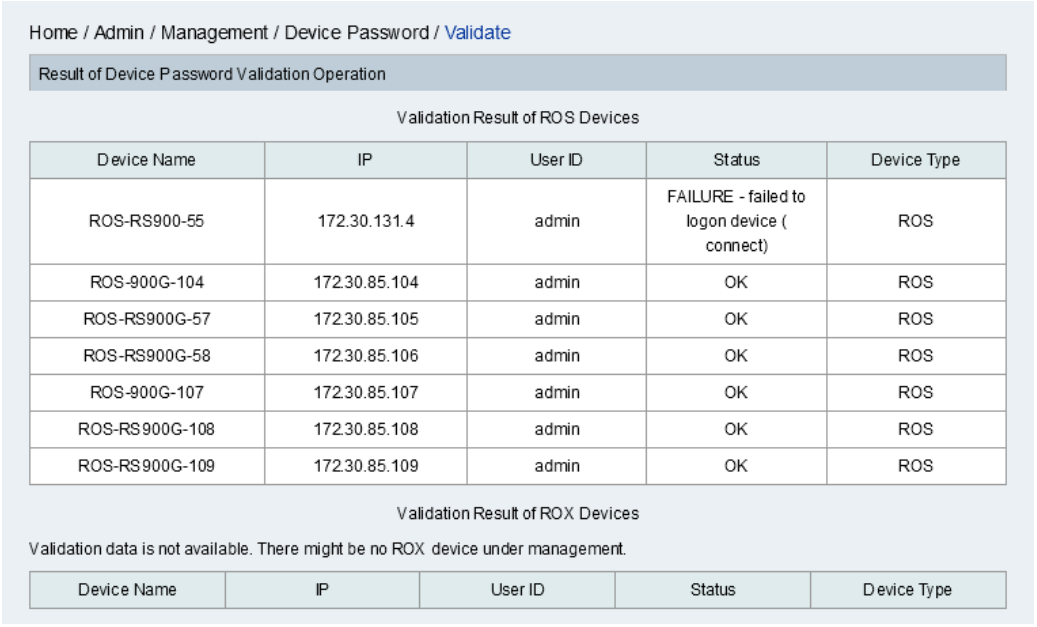


Figure 295: Validate Screen

The **Validate** screen displays separate tables for each type of supported RUGGEDCOM device. The tables list the following for each device managed by RUGGEDCOM NMS:

Parameter	Description
Device Name	The name of the device.
IP	The IP address of the device.

Parameter	Description
User ID	The name of the administrator profile on the device.
Status	Indicates if the password used by RUGGEDCOM NMS is valid for the device. If the password is rejected, an error message is displayed.
Device Type	The type of RUGGEDCOM device.

Section 6.4.12.2
Applying an Auto-Generated Password

To apply an auto-generated password to all supported RUGGEDCOM devices, or a specific device type, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Device Password Management**. The **Device Password** screen appears.

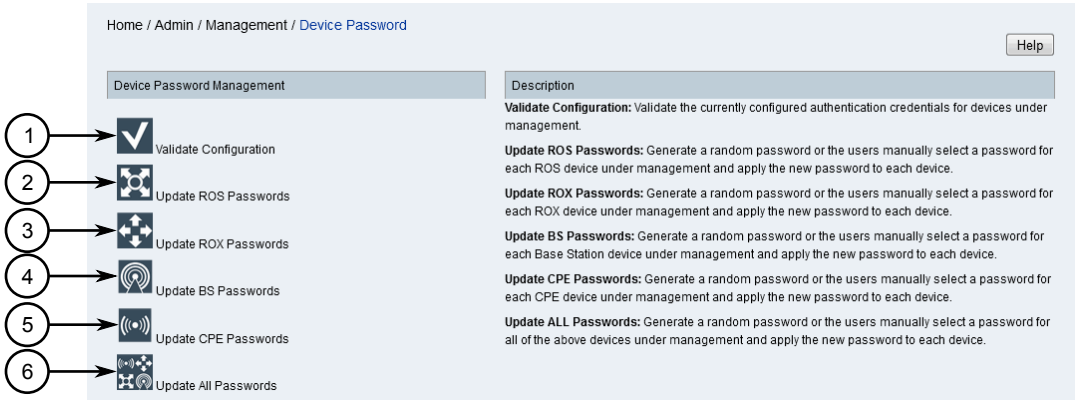


Figure 296: Device Password Screen

1. Update ROS Passwords Icon **2.** Update ROX Passwords Icon **3.** Update BS Passwords Icon **4.** Update CPE Passwords Icon **5.** Update All Passwords Icon

2. Click the desired **Update {Type} Passwords** icon, where *{Type}* is either `ROS`, `ROX`, `BS`, `CPE` or `All`. The **Update Passwords** dialog box appears.

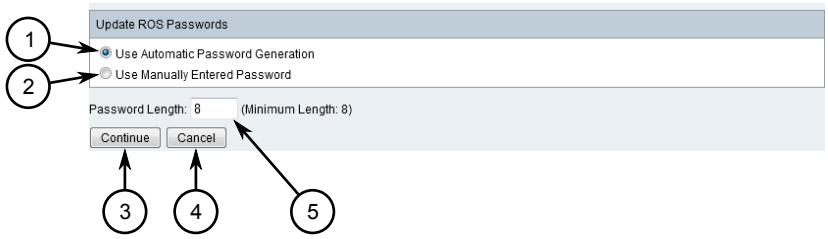


Figure 297: Updated Passwords Dialog Box

1. Use Automatic Password Generation Option **2.** Use Manually Entered Password Option **3.** Continue Button **4.** Cancel Button **5.** Required Length Box

3. Select **Use Automatic Password Generation** and then click **Continue**. A confirmation dialog box appears.

CAUTION!
Configuration hazard – risk of data loss. During the password update process, the RUGGEDCOM NMS Web interface is locked. Avoid the following:

- *Do not close the browser window*
- *Do not start any other configuration management processes*
- *Do not start the password validation process*

4. Click **OK**. The password update process begins, after which the **Update** screen appears.

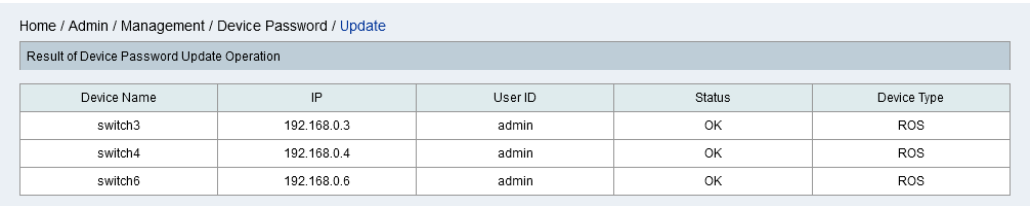


Figure 298: Update Screen

This screen summarizes the results of the password update process. The table list the following for each device managed by RUGGEDCOM NMS:

Parameter	Description
Device Name	The name of the device.
IP	The IP address of the device.
User ID	The name of the administrator profile on the device.
Status	Indicates if the password used by RUGGEDCOM NMS is valid for the device. If the password is rejected, an error message is displayed.
Device Type	The type of RUGGEDCOM device.

IMPORTANT!
For RUGGEDCOM NMS to manage devices properly, failed passwords should be addressed immediately.

If RUGGEDCOM NMS was unable to update the password for any device, do the following:

- Make sure device access is configured for the device(s). For more information, refer to Section 6.4.11.2, "Adding/Editing Device Access Information" .
- Make sure RUGGEDCOM NMS can connect to the device(s). Error messages such as *No route to host* or *Network is unreachable* indicate a network-related failure.

Section 6.4.12.3
Applying a Custom Password

To apply a custom password to selected RUGGEDCOM devices, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Device Password Management**. The **Device Password** screen appears.

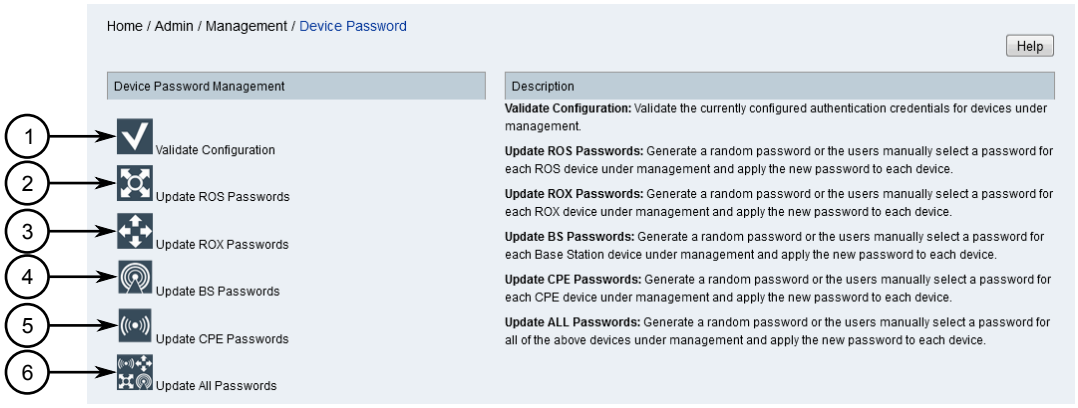


Figure 299: Device Password Screen

1. Validate Configuration Icon **2.** Update ROS Passwords Icon **3.** Update ROX Passwords Icon **4.** Update BS Passwords Icon **5.** Update CPE Passwords Icon **6.** Update All Passwords Icon

2. Click the desired **Update {Type} Passwords** icon, where *{Type}* is either `ROS`, `ROX`, `BS`, `CPE` or `All`. The **Update Passwords** dialog box appears.

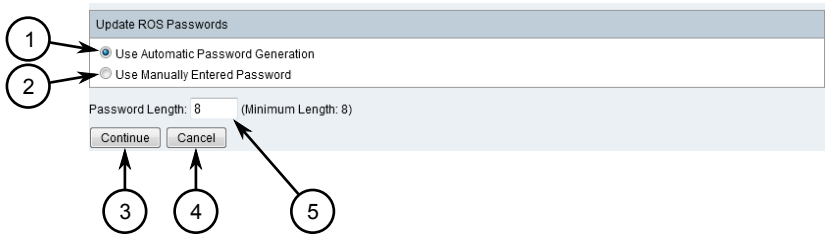


Figure 300:

1. Use Automatic Password Generation Option **2.** Use Manually Entered Password Option **3.** Continue Button **4.** Cancel Button **5.** Required Length Box

3. Select **Use Manually Entered Password**.
4. Click **Continue**. The **Update Passwords** dialog box updates to display the IP ranges that will be updated and form fields for applying a custom password for each.

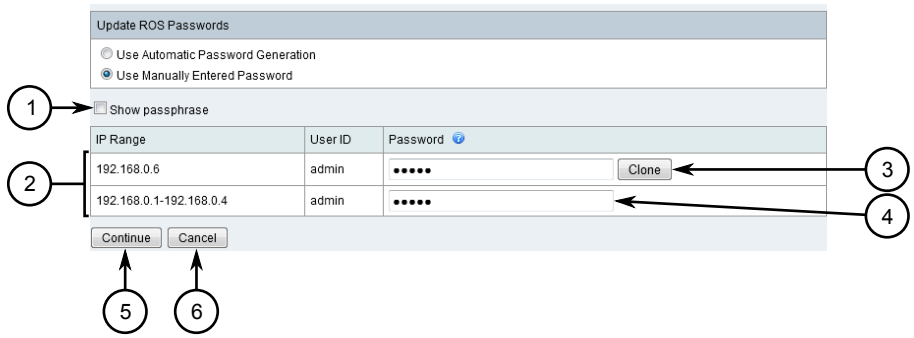


Figure 301:

1. Show Passphrase Check Box **2.** IP Ranges **3.** Password Box **4.** Clone Button **5.** Continue Button **6.** Cancel Button

5. [Optional] Select **Show Passphrase** to display passwords in plain text.

IMPORTANT!
All passwords must be at least eight characters long. For added security, they should also contain at least one lowercase letter, one uppercase letter, one numeric character, and one special character.

IMPORTANT!
Passwords for all devices can include the following characters:

- *English uppercase characters: A-Z*
- *English lower characters: a-z*
- *Basic 10 digits: 0-9*
- *Non-alphabetic characters: ~!@#$%^&*()-_=+[{}]|\;:<>/?.,*

6. Under **Password**, type a custom password for each IP range. To reuse a password for another IP range, click **Clone**.
7. Click **Continue**. A confirmation dialog box appears.

CAUTION!
Configuration hazard – risk of data loss. During the password update process, the RUGGEDCOM NMS Web interface is locked. Avoid the following:

- *Do not close the browser window*
- *Do not start any other configuration management processes*
- *Do not start the password validation process*

8. Click **OK**. The password update process begins, after which the **Update** screen appears.

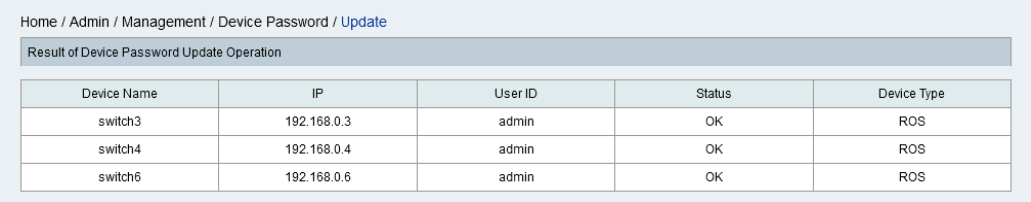


Figure 302: Update Screen

This screen summarizes the results of the password update process. The table list the following for each device managed by RUGGEDCOM NMS:

Parameter	Description
Device Name	The name of the device.
IP	The IP address of the device.
User ID	The name of the administrator profile on the device.
Status	Indicates if the password used by RUGGEDCOM NMS is valid for the device. If the password is rejected, an error message is displayed.
Device Type	The type of RUGGEDCOM device.

IMPORTANT!
For RUGGEDCOM NMS to manage devices properly, failed passwords should be addressed immediately.

If RUGGEDCOM NMS was unable to update the password for any device, do the following:

- Make sure device access is configured for the device(s). For more information, refer to Section 6.4.11.2, "Adding/Editing Device Access Information" .
- Make sure RUGGEDCOM NMS can connect to the device(s). Error messages such as *No route to host* or *Network is unreachable* indicate a network-related failure.

Section 6.4.12.4
Viewing the Password Update History

All device passwords are recorded in the file `deviceusers.xml` on the RUGGEDCOM NMS server. When the device access information is updated, a copy of the previous information is archived under `/usr/share/opennms/ruggednms/confighistory/deviceusers.{number}` , where *{number}* is a three-digit sequential number (e.g. 001, 002, 003, etc.).

To view the update history for device passwords, compare the information in the current `deviceusers.xml` file with the archived files.

NOTE
If data encryption is enabled, all archived versions of `deviceusers.xml` *(renamed as* `deviceusers.{number}`*) are protected. To access the information in one of the archived files, copy the file to* `/usr/share/opennms/ruggednms/etc` *and change the extension to* ***xml****. For example, change* `deviceusers.001` *to* `deviceusers.xml`.

Section 6.5

Managing SNMP

This section describes how to configure and manage SNMP for RUGGEDCOM NMS.

CONTENTS

Section 6.5.1

Configuring SNMP Globally

When configured, RUGGEDCOM NMS can apply a default configuration to all SNMP targets that do not have a specific configuration already defined.

To configure global settings for all SNMP targets, do the following:

1. On the menu bar, click **Admin** and then click **Configure SNMP**. The **SNMP** screen appears.

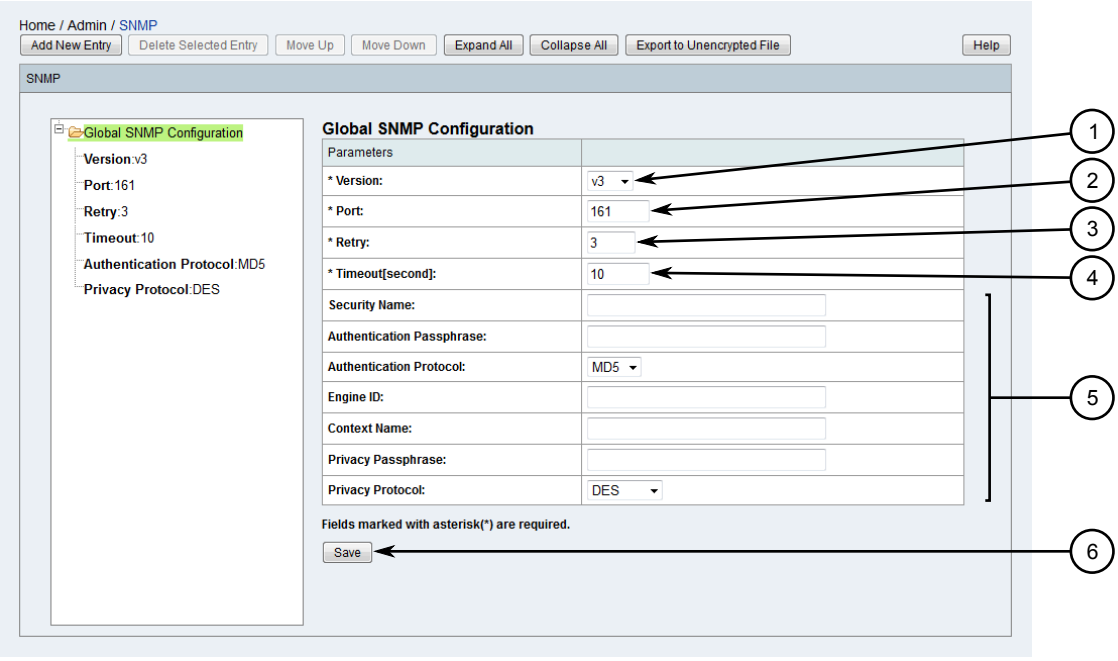


Figure 303: SNMP Screen

1. Version List **2.** Port Box **3.** Retry Box **4.** Timeout Box **5.** SNMP Version-Specific Parameters **6.** Save Button

2. In the tree menu, select **Global SNMP Configuration**. The **Global SNMP Configuration** table appears.
3. Configure the following common parameters as required:

Parameter	Description
Version	**Synopsis:** { v1, v2c, v3 } **Default:** v2c The SNMP version. Available parameters are dependent on the selection.
Port	**Default:** 161 The port the SNMP agent will listen on for SNMP requests.
Retry	**Default:** 3 The maximum number of attempts allowed for connecting to the SNMP agent.
Timeout	**Default:** 10 The time in seconds (s) to wait for a response from the SNMP agent.

4. Configure the following version-specific parameters as required:

For SNMPv1 and SNMPv2 Only

Parameter	Description
Read Community	**Default:** public The default *read* community string for SNMP queries.
Write Community	**Default:** private The default *write* community string for SNMP queries.

For SNMPv3 Only

Parameter	Description
Security Name	The system-wide security name.
Authentication Passphrase	The passphrase to use for SNMPv3 authentication.
Authentication Protocol	**Synopsis:** { MD5, SHA } **Default:** MD5 The authentication protocol to use for SNMPv3 authentication.
Engine ID	The engine ID for the target agent.
Context Name	The name of the context to obtain data from on the target agent. This parameter applies to RUGGEDCOM WIN devices only. Always set to `Public`.
Privacy Passphrase	The passphrase to used to encrypt the contents of SNMPv3 packets.
Privacy Protocol	**Synopsis:** { DES, AES, AES192, AES256 } **Default:** DES The protocol to use to encrypt the contents of SNMPv3 packets.

5. Click **Save**. A confirmation message appears.
6. Click **OK**.

7. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 6.5.2
Managing SNMP Data Collection

This section describes how to configure SNMP data collection and exclude primary and/or secondary SNMP interfaces as necessary.

CONTENTS

Section 6.5.2.1
Configuring SNMP Data Collection

By default, RUGGEDCOM NMS automatically collects data via SNMP from each interface on a managed device that is associated with an IP address. The interface with the lowest IP address is considered the default, or *primary*, for the device that will be used for SNMP data collection.

RUGGEDCOM NMS can also be configured to poll other interfaces on a device that are not associated with an IP address. Selecting or deselecting interfaces for data collection will notify RUGGEDCOM NMS to actively poll these interfaces for data, and to store this information in the database for later viewing. For more information about viewing reports, refer to Section 5.4, "Managing Performance Reports" .

IMPORTANT!
*If two interfaces on a managed device (from which RUGGEDCOM NMS has already been gathering data) are collected into an **aggregate link**, RUGGEDCOM NMS will retain outdated information for the older, secondary link. For example, if interfaces A and B are aggregated, SNMP will supply information for link A but not for link B (the switch will skip port B when a MIB **walk** is executed). RUGGEDCOM NMS, at this point, still erroneously believes interface B to be present on the device.*

To correct this situation, the devices that have been configured with aggregated links must be deleted in RUGGEDCOM NMS (including the device entry and all associated data) and then rediscovered for the correct link information to be captured. If these devices are not configured during the device discovery process, they will have to be added manually.

To configure RUGGEDCOM NMS to collect SNMP data from non-IP interfaces on a RUGGEDCOM device, do the following:

NOTE
By default, interfaces marked as Primary or Secondary in the SNMP Status column will be selected for data collection. If alternate interfaces are to be selected, the Primary or Secondary IP address range(s) to be excluded must be updated in a separate configuration file. For more information, refer to Section 6.5.2.2, "Excluding Primary and/or Secondary SNMP Interfaces" .

1. On the menu bar, click **Admin** and then click **Configure SNMP Data Collection per Interface**. The **Manage SNMP By Interface** screen appears.

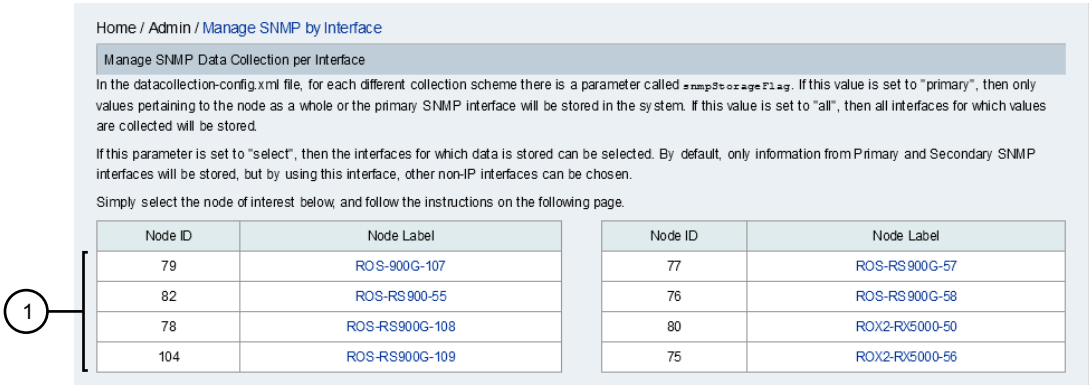


Figure 304: Manage SNMP By Interface Screen

1. Available Nodes

2. Click the desired node. The **Select SNMP Interfaces** screen appears.

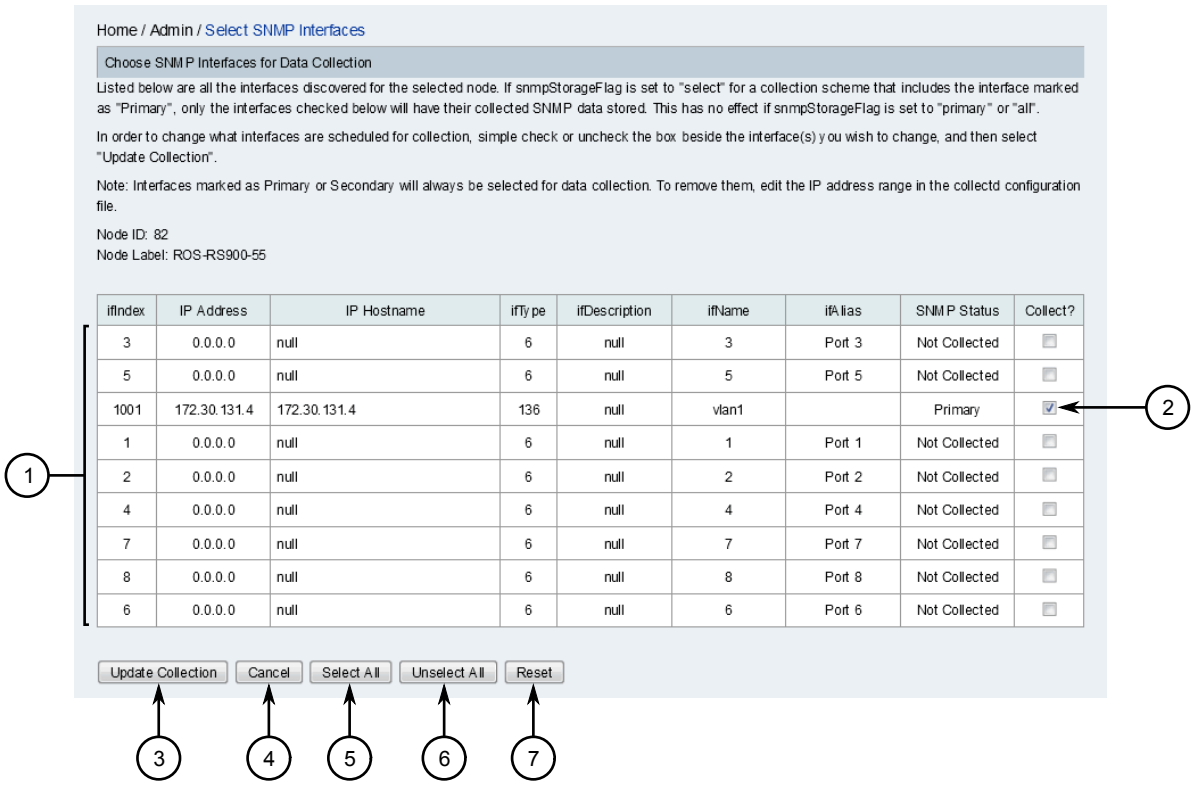


Figure 305: Select SNMP Interfaces Screen

1. Available Interfaces **2.** Collect Check Box **3.** Update Collection Button **4.** Cancel Button **5.** Select All Button **6.** Unselect All Button **7.** Reset Button

3. Under the **Collect** column, select one or more non-IP interfaces from which to collect data.
4. Click **Update Collection**. A confirmation message appears.

5. Click **OK** to apply the changes.

Section 6.5.2.2
Excluding Primary and/or Secondary SNMP Interfaces

By default, SNMP interfaces marked as Primary or Secondary will be selected for data collection. If alternate interfaces are to be selected for data collection, a configuration file can be modified to exclude a specified range of IP addresses.

To exclude primary and/or secondary SNMP interfaces, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and open the following file in a text editor:

   `/usr/share/opennms/etc/collectd-configuration.xml`

2. Navigate to the end of the following line, then press **Enter**:

   ```
   <include-range begin="1.1.1.1" end="254.254.254.254" />
   ```

3. Add the following line:

   ```
   <exclude-range begin="*.*.*.*" end="*.*.*.*" />
   ```

   where *.*.*.* is the primary/secondary interface IP or an IP range.

   For example:

   ```
   <include-range begin="1.1.1.1" end="254.254.254.254" />
   <exclude-range begin="172.30.85.15" end="172.30.85.15" />
   ```

   NOTE
   Users can add multiple exclude-range entries in this configuration file.

4. Save and close the file
5. Restart RUGGEDCOM NMS.

Section 6.5.3
Updating SNMP Data Per Device

By default, RUGGEDCOM NMS automatically collects data via SNMP from each interface on a managed device that is associated with an IP address. However, the user can force RUGGEDCOM NMS to collect SNMP data from a device's interfaces at any time.

To initiate SNMP data collection on a device, do the following:

1. Display details for the chosen device. For more information, refer to Section 6.4.2, “Viewing Device Details” . If SNMP is supported and enabled on the device, the **Update SNMP** link is available.

Figure 306: Device Details Screen (Example)

1. Update SNMP Link

2. Click **Update SNMP**. The **Update SNMP Information** screen appears indicating the SNMP data for the device's interfaces have been updated.

Section 6.5.4

Managing SNMP Targets

This section describes how to configure and manage SNMP targets.

CONTENTS

Section 6.5.4.1

Adding an SNMP Target

To add and configure a specific SNMP target, do the following:

1. On the menu bar, click **Admin** and then click **Configure SNMP**. The **SNMP** screen appears.

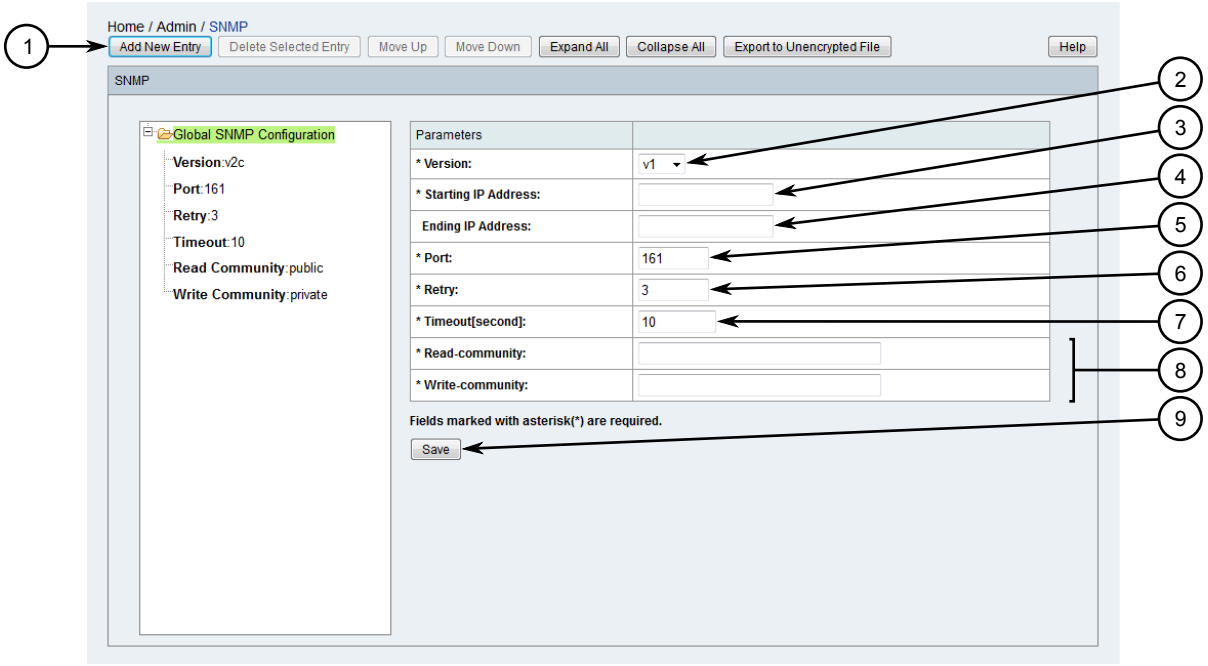


Figure 307: SNMP Screen

1. Add New Entry Button **2.** Version List **3.** Starting IP Address **4.** Ending IP Address **5.** Port Box **6.** Retry Box **7.** Timeout Box **8.** SNMP Version-Specific Parameters **9.** Save Button

2. Select an existing SNMP target from the tree menu. The **Add New Entry** button is enabled.
3. Click **Add New Entry**. The required and optional parameters appear.
4. Configure the following common parameters as required:

Parameter	Description
Version	**Synopsis:** { v1, v2c, v3 } **Default:** v2c The SNMP version. Available parameters are dependent on the selection.
Port	**Default:** 161 The port the SNMP agent will listen on for SNMP requests.
Retry	**Default:** 3 The maximum number of attempts allowed for connecting to the SNMP agent.
Timeout	**Default:** 10 The time in seconds (s) to wait for a response from the SNMP agent.

5. Configure the following version-specific parameters as required:

For SNMPv1 and SNMPv2 Only

Parameter	Description
Read Community	**Default:** public The default *read* community string for SNMP queries.
Write Community	**Default:** private The default *write* community string for SNMP queries.

For SNMPv3 Only

Parameter	Description
Security Name	The system-wide security name.
Authentication Passphrase	The passphrase to use for SNMPv3 authentication.
Authentication Protocol	**Synopsis:** { MD5, SHA } **Default:** MD5 The authentication protocol to use for SNMPv3 authentication.
Engine ID	The engine ID for the target agent.
Context Name	The name of the context to obtain data from on the target agent. This parameter applies to RUGGEDCOM WIN devices only. Always set to `Public`.
Privacy Passphrase	The passphrase to used to encrypt the contents of SNMPv3 packets.
Privacy Protocol	**Synopsis:** { DES, AES, AES192, AES256 } **Default:** DES The protocol to use to encrypt the contents of SNMPv3 packets.

6. Click **Save**. A confirmation message appears.
7. Click **OK**.
8. [Optional] Change the order in which SNMP targets are processed by selecting them from the tree menu and using **Move Up** or **Move Down**.
9. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, “Restarting RUGGEDCOM NMS ” .

Section 6.5.4.2
Exporting an SNMP Target Configuration

To export SNMP configuration information for a specific target, do the following:

1. On the menu bar, click **Admin** and then click **Configure SNMP**. The **SNMP** screen appears.

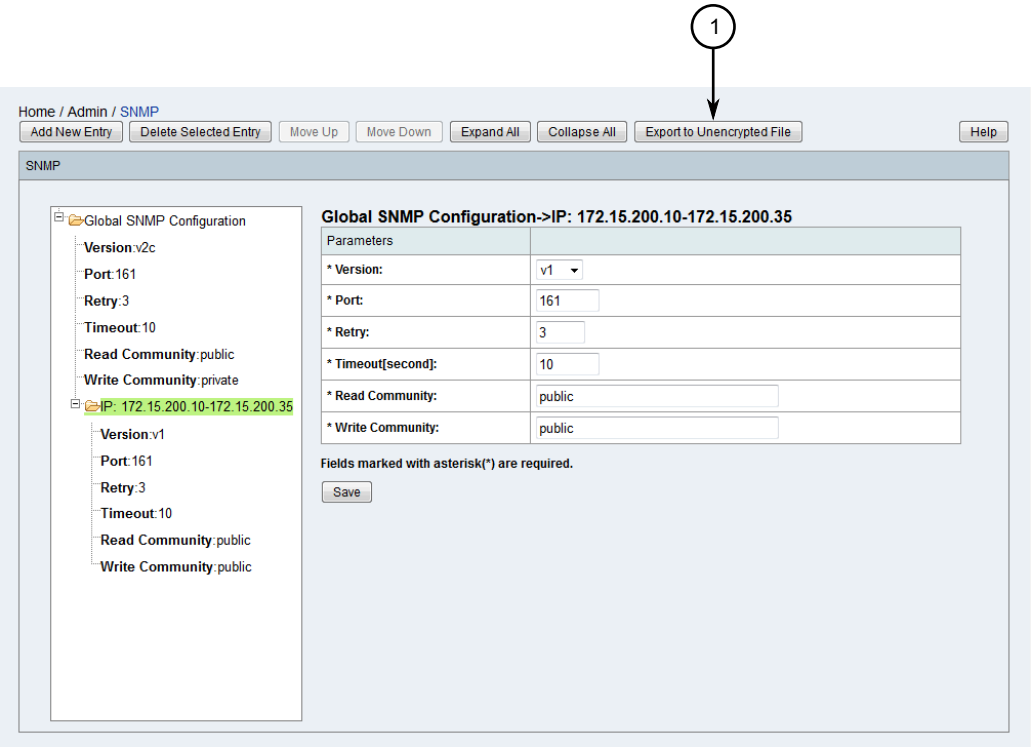


Figure 308: SNMP Screen

1. Export to Unencrypted File Button

2. In the tree menu, select an SNMP target and then click **Export to Unencrypted File**. A dialog box appears.
3. Choose to open or save the generated XML file and then click **OK**.

Section 6.5.4.3

Deleting an SNMP Target

To delete a specific SNMP target, do the following:

1. On the menu bar, click **Admin** and then click **Configure SNMP**. The **SNMP** screen appears.

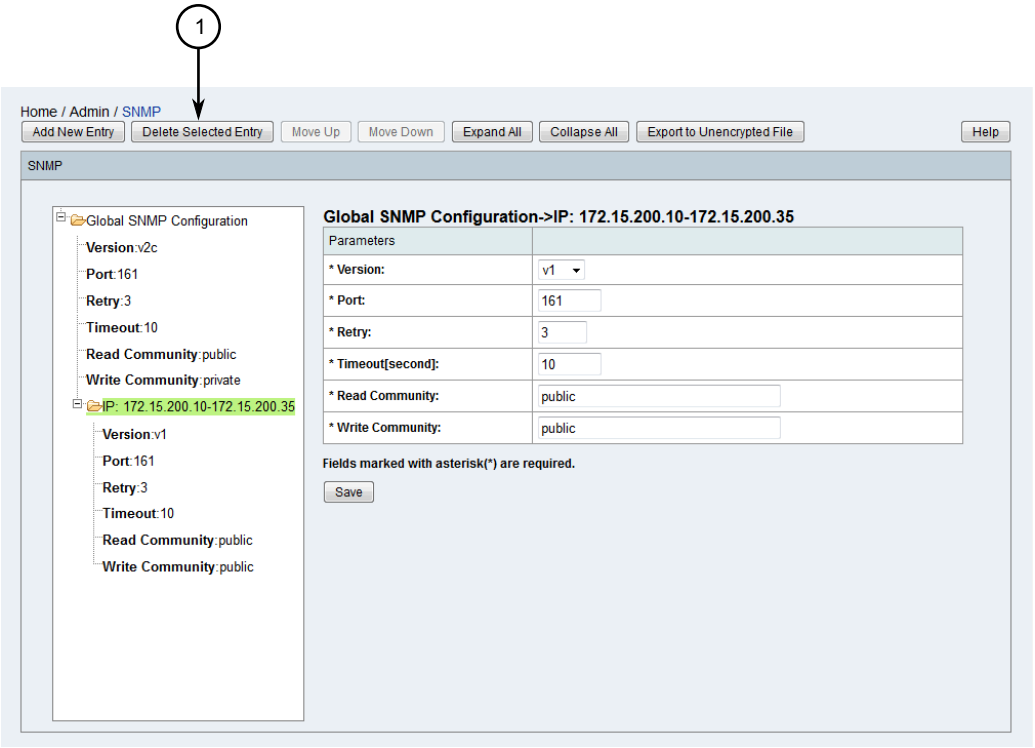


Figure 309: SNMP Screen

1. Delete Selected Entry Button

2. Select an existing SNMP target from the tree menu and then click **Delete Selected Entry**. A confirmation message appears.
3. Select **OK** to delete the target.
4. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 6.5.5

Managing SNMP Trap Forwarding

RUGGEDCOM NMS employs a northbound interface for forwarding SNMP traps to SNMP trap receivers, allowing other systems to monitor RUGGEDCOM NMS remotely.

NOTE
The format of all SNMP traps is retained when they are forwarded.

CONTENTS

- Section 6.5.5.2, "Deleting a Trap Destination"

Section 6.5.5.1
Adding/Editing a Trap Destination

To add or edit the destination for an SNMP trap, do the following:

1. On the menu bar, click **Admin**, click **Northbound Interface**, and then click **SNMP Trap Forwarding**. The **Trap Forwarding** screen appears.

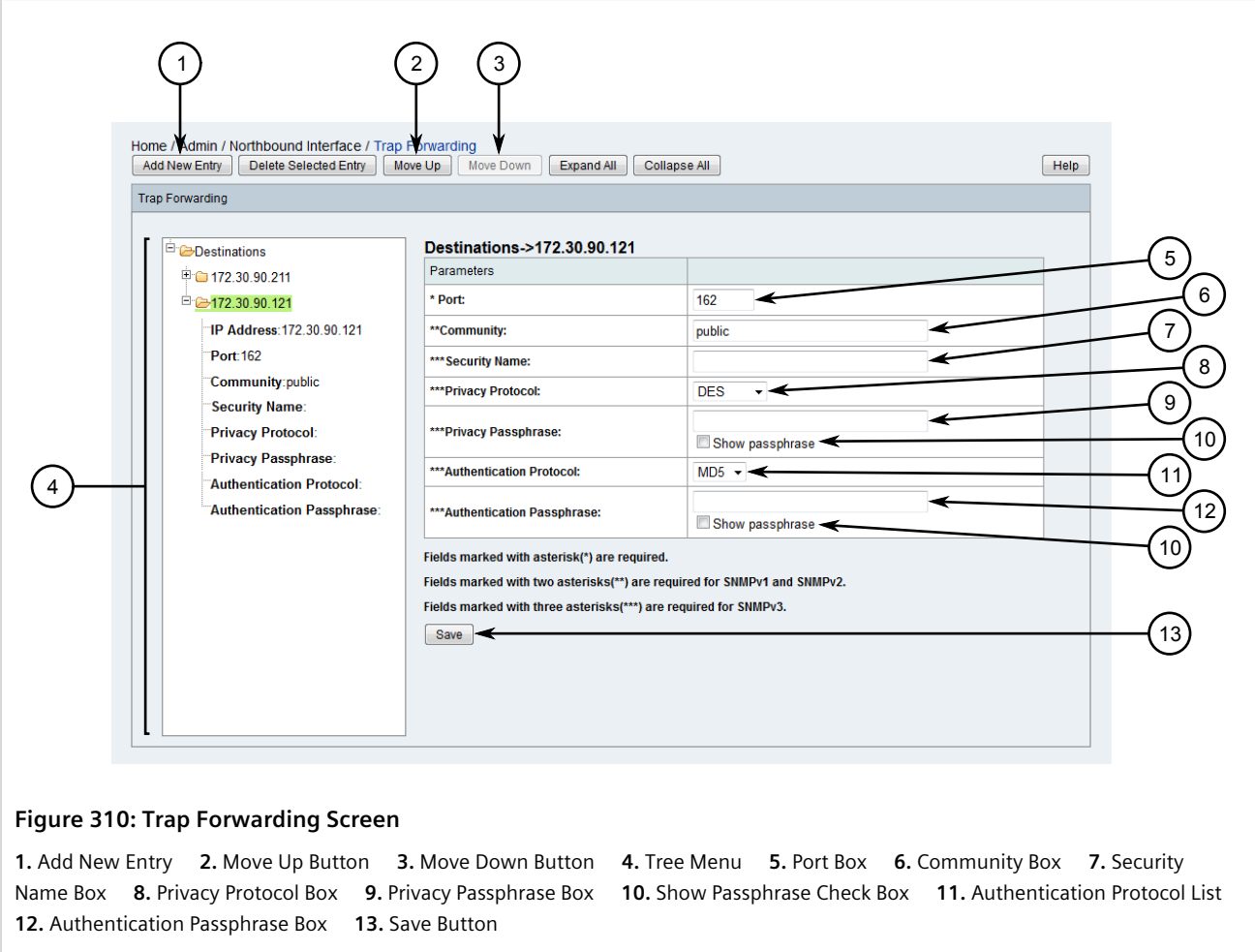


Figure 310: Trap Forwarding Screen

1. Add New Entry **2.** Move Up Button **3.** Move Down Button **4.** Tree Menu **5.** Port Box **6.** Community Box **7.** Security Name Box **8.** Privacy Protocol Box **9.** Privacy Passphrase Box **10.** Show Passphrase Check Box **11.** Authentication Protocol List **12.** Authentication Passphrase Box **13.** Save Button

2. In the tree menu, click **Destinations**.
3. Select either **Destinations** or an existing destination from the tree menu. If an existing destination is selected, the new destination will be placed after it.
4. Click **Add New Entry** or select an existing destination. A form appears.
5. [Optional] Select **Show Passphrase** to display passwords/passphrases in plain text.
6. Configure the following parameters as required:

Parameter	Description
Community	The default community string for SNMP queries.

Parameter	Description
Security Name	The system-wide security name.
Privacy Protocol	**Synopsis:** { DES, AES, AES192, AES256 } **Default:** DES The protocol to use to encrypt the contents of SNMPv3 packets.
Privacy Passphrase	The passphrase to used to encrypt the contents of SNMPv3 packets.
Authentication Protocol	**Synopsis:** { MD5, SHA } **Default:** MD5 The authentication protocol to use for SNMPv3 authentication.
Authentication Passphrase	The passphrase to use for SNMPv3 authentication.

7. Click **Save**. A confirmation message appears.
8. Click **OK**.
9. [Optional] Change the order in which destinations are processed by selecting them from the tree menu and using **Move Up** or **Move Down**.
10. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 6.5.5.2
Deleting a Trap Destination

To delete the destination for an SNMP trap, do the following:

1. On the menu bar, click **Admin**, click **Northbound Interface**, and then click **SNMP Trap Forwarding**. The **Trap Forwarding** screen appears.

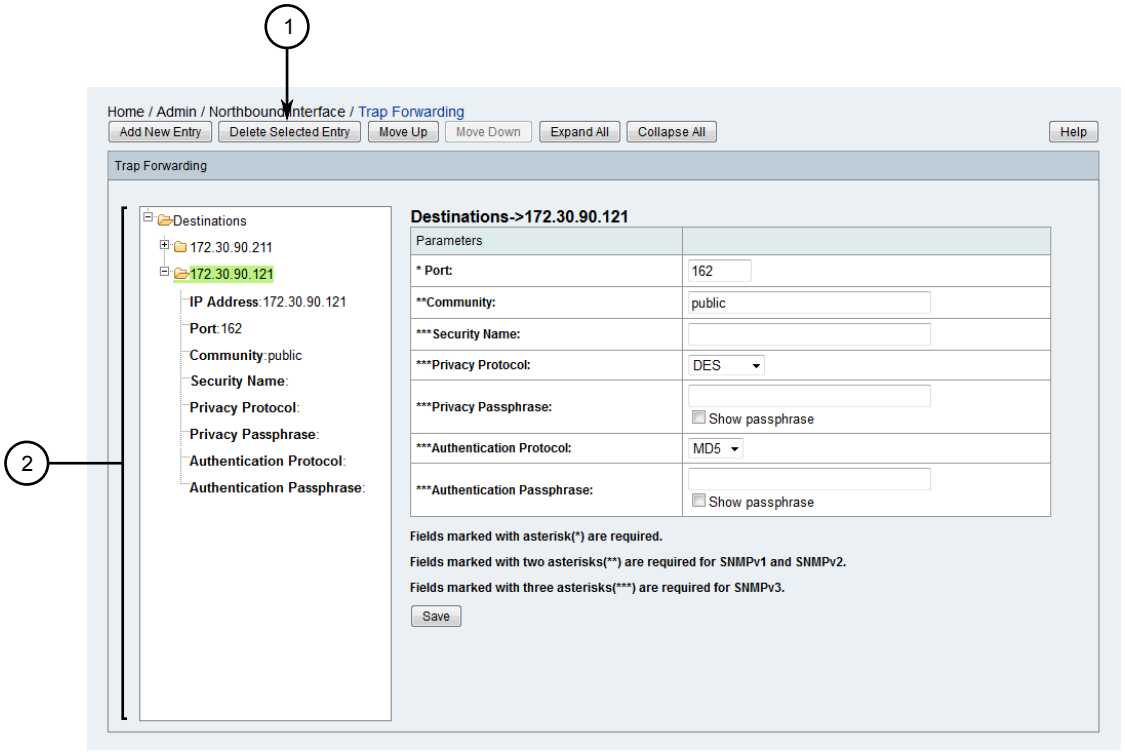


Figure 311: Trap Forwarding Screen

1. Delete Selected Entry **2.** Tree Menu

2. In the tree menu, click **Destinations**.
3. Select a destination from the tree menu and click **Delete**. A confirmation message appears.
4. Click **OK** to delete the notification.
5. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 6.5.6

Managing SNMP Event Forwarding

RUGGEDCOM NMS employs a northbound interface for forwarding events generated by RUGGEDCOM NMS to SNMP trap receivers, allowing other systems to monitor RUGGEDCOM NMS remotely.

NOTE
Only one SNMP version can be used per destination.

CONTENTS

- Section 6.5.6.2, “Deleting an Event Destination”

Section 6.5.6.1
Adding/Editing an Event Destination

To add or edit the destination for an event, do the following:

1. On the menu bar, click **Admin**, click **Northbound Interface**, and then click **SNMP Event Forwarding**. The **Event Forwarding** screen appears.

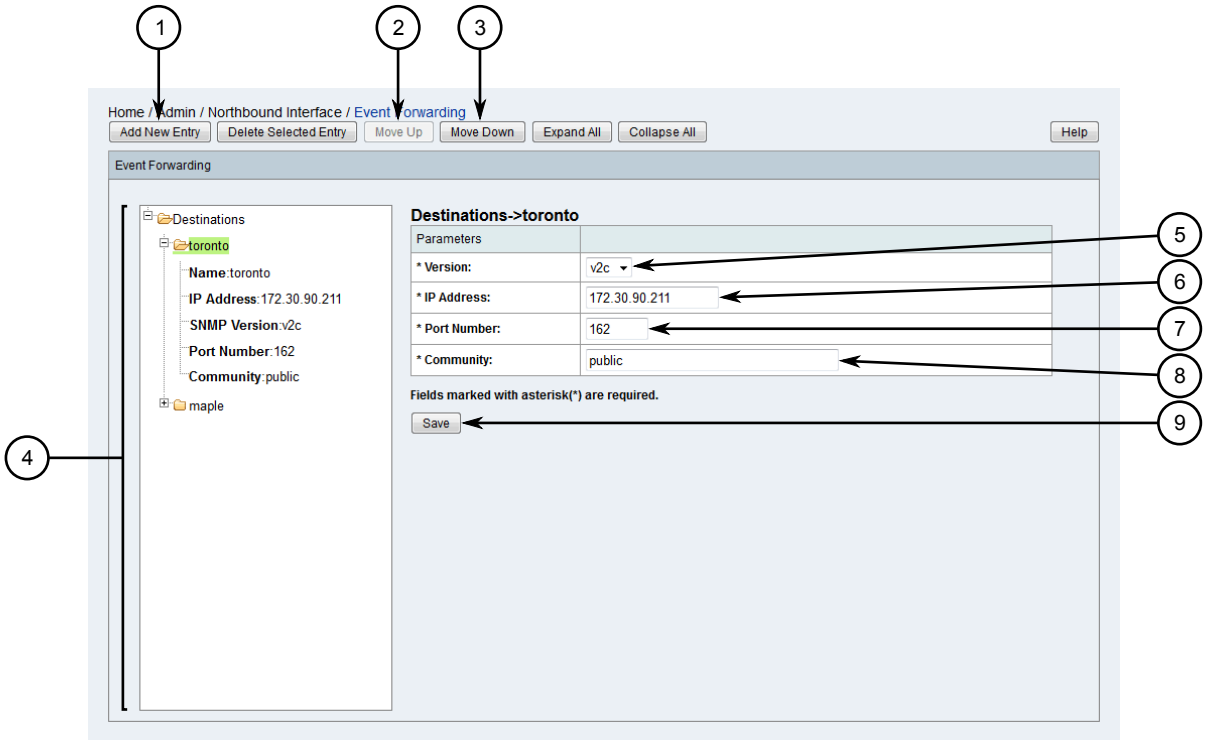


Figure 312: Event Forwarding Screen

1. Add New Entry **2.** Move Up Button **3.** Move Down Button **4.** Tree Menu **5.** Version List **6.** IP Address Box **7.** Port Number Box **8.** Community Box **9.** Save Button

2. In the tree menu, click **Destinations**.
3. Select either **Destinations** or an existing destination from the tree menu. If an existing destination is selected, the new destination will be placed after it.
4. Click **Add New Entry** or select an existing destination. A form appears.
5. Configure the following parameters as required:

Parameter	Description
Version	**Synopsis:** { v1, v2c } **Default:** v2c The SNMP version.

Parameter	Description
IP Address	The IP address of the SNMP trap receiver.
Port Number	The port number associated with the SNMP trap receiver.
Community	The default community string for SNMP queries.

6. Click **Save**. A confirmation message appears.
7. Click **OK**.
8. [Optional] Change the order in which destinations are processed by selecting them from the tree menu and using **Move Up** or **Move Down**.
9. Add/edit one or more notifications to use the new destination. For more information, refer to Section 5.2.4.7, "Adding/Editing a Notification" .
10. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 6.5.6.2

Deleting an Event Destination

To delete the destination for an event, do the following:

1. On the menu bar, click **Admin**, click **Northbound Interface**, and then click **SNMP Event Forwarding**. The **Event Forwarding** screen appears.

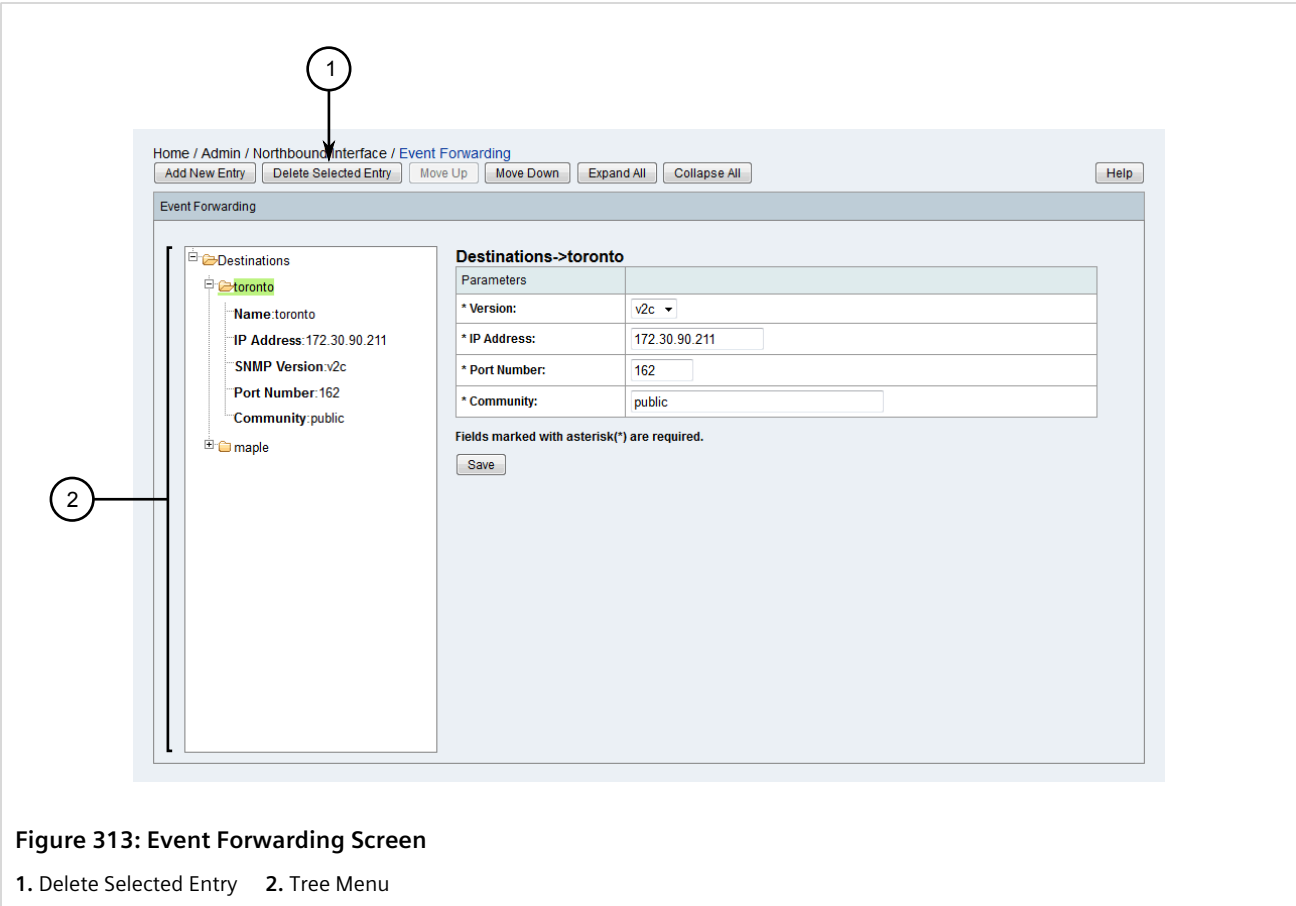


Figure 313: Event Forwarding Screen

1. Delete Selected Entry **2.** Tree Menu

2. In the tree menu, click **Destinations**.
3. Select a destination from the tree menu and click **Delete**. A confirmation message appears.
4. Click **OK** to delete the notification.
5. Restart RUGGEDCOM NMS. For more information, refer to Section 3.3, "Restarting RUGGEDCOM NMS " .

Section 6.6

Managing Archived Configuration Files

This section describes how to upload, export and otherwise manage archived configuration files for RUGGEDCOM devices.

CONTENTS

Section 6.6.1

Uploading an Archived Configuration File to a Device

To upload an archived configuration file to a RUGGEDCOM device managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Archived Configuration File Upload**. The **Configuration Upload** screen appears.

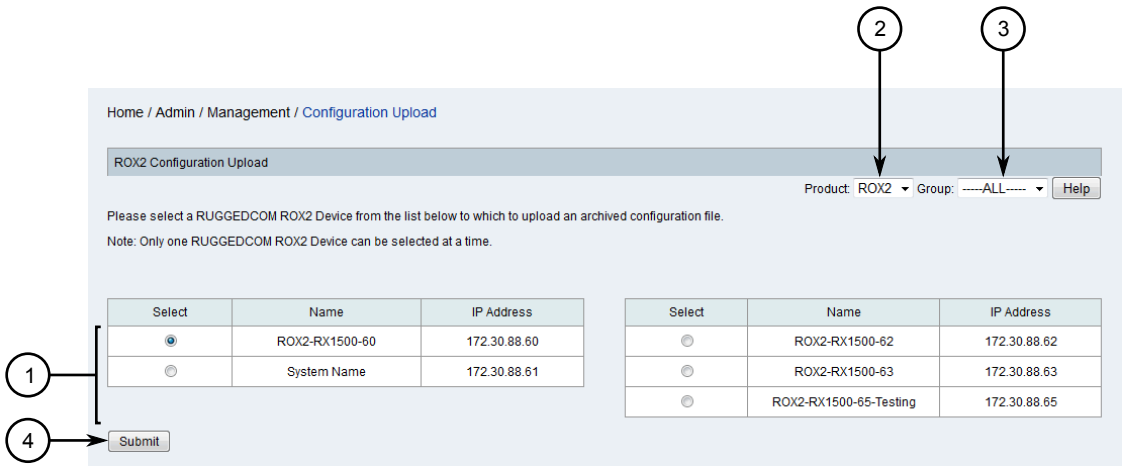


Figure 314: Configuration Upload Screen

1. Available Devices **2.** Product List **3.** Group List **4.** Submit Button

2. Use the **Product** and **Group** lists to filter the list of available devices.
3. Select a device and then click **Submit**. If previously archived configuration files are available for the chosen device, **Configuration Upload** screen appears.

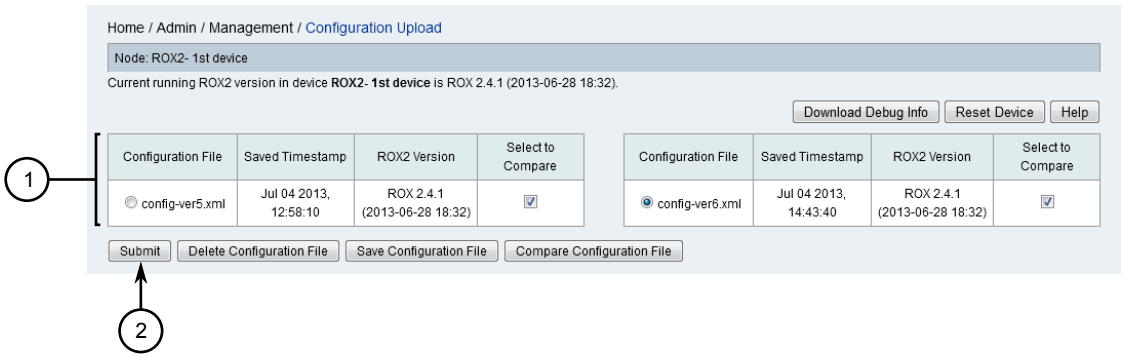


Figure 315: Configuration Upload Screen

1. Available Configuration Files **2.** Submit Button

4. [Optional] Compare the available configuration files to determine which one to upload. For more information, refer to Section 6.6.3, "Comparing Archived Configuration Files (ROX II Only)" .
5. Select the desired configuration file and click **Submit**. The configuration file currently in use is saved and the archived configuration file is uploaded to the device.
6. [Optional] View the Configuration Management Log to determine if the upload was successful. For more information, refer to Section 6.1, "Viewing the Configuration Management Log" .

Section 6.6.2

Exporting an Archived Configuration File

To export an archived configuration file to a local file system or network, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Archived Configuration File Upload**. The **Configuration Upload** screen appears.

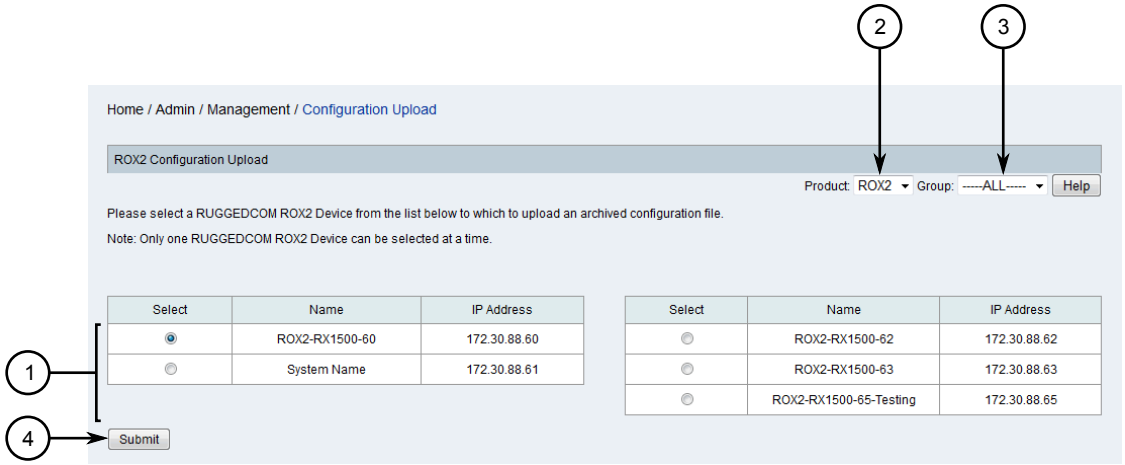


Figure 316: Configuration Upload Screen

1. Available Devices **2.** Product List **3.** Group List **4.** Submit Button

2. Use the **Product** and **Group** lists to filter the list of available devices.
3. Select a device and then click **Submit**. If previously archived configuration files are available for the chosen device, **Configuration Upload** screen appears.

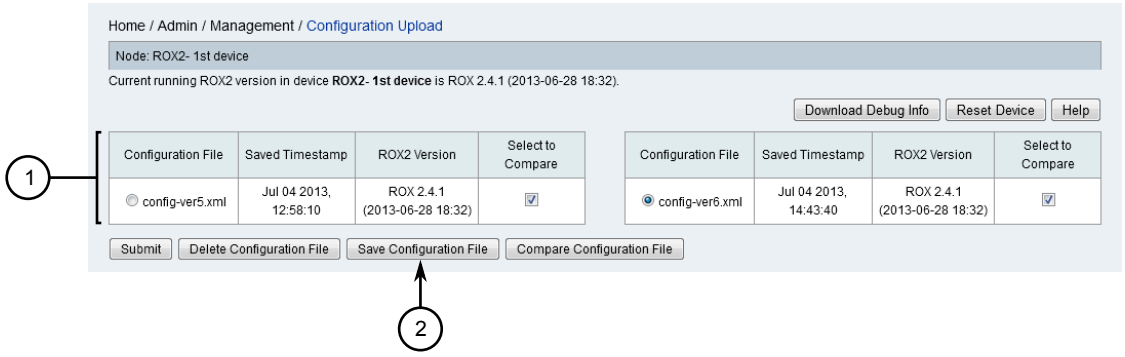


Figure 317: Configuration Upload Screen

1. Available Configuration Files **2.** Save Configuration File Button

4. [Optional] Compare the available configuration files to determine which one to export. For more information, refer to Section 6.6.3, "Comparing Archived Configuration Files (ROX II Only)" .
5. Select the desired configuration file and click **Save Configuration File**. A dialog box appears. If possible, select the location to save the file and then click **OK**. The file is saved in XML format.

Section 6.6.3

Comparing Archived Configuration Files (ROX II Only)

To compare two or more archived configuration files taken from a RUGGEDCOM ROX II device managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Archived Configuration File Upload**. The **Configuration Upload** screen appears.

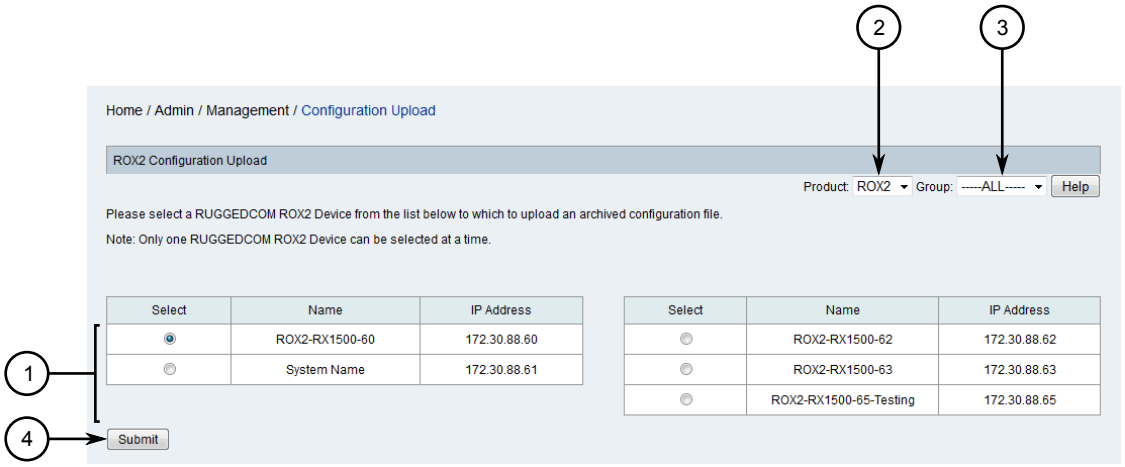


Figure 318: Configuration Upload Screen

1. Available Devices **2.** Product List **3.** Group List **4.** Submit Button

2. Use the **Product** and **Group** lists to filter the list of available ROX II devices.
3. Select a device and then click **Submit**. If previously archived configuration files are available for the chosen device, **Configuration Upload** screen appears.

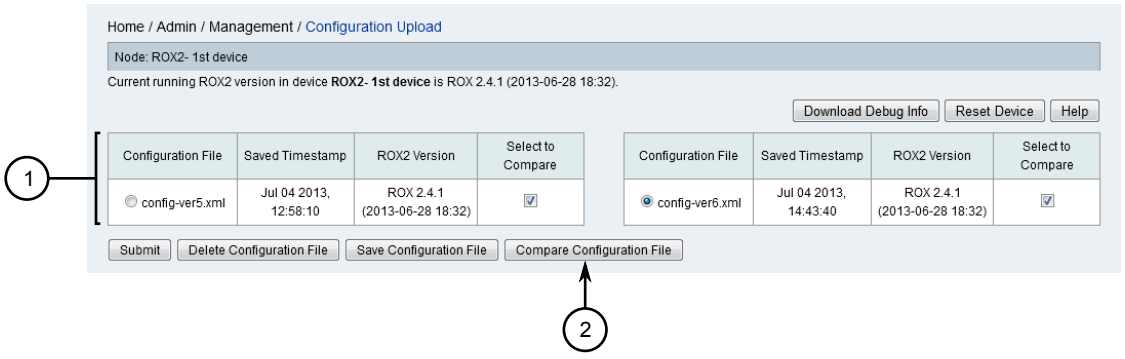


Figure 319: Configuration Upload Screen

1. Available Configuration Files **2.** Compare Configuration File Button

4. Select two or more configuration files and click **Compare Configuration File**. The **Compare** screen appears.

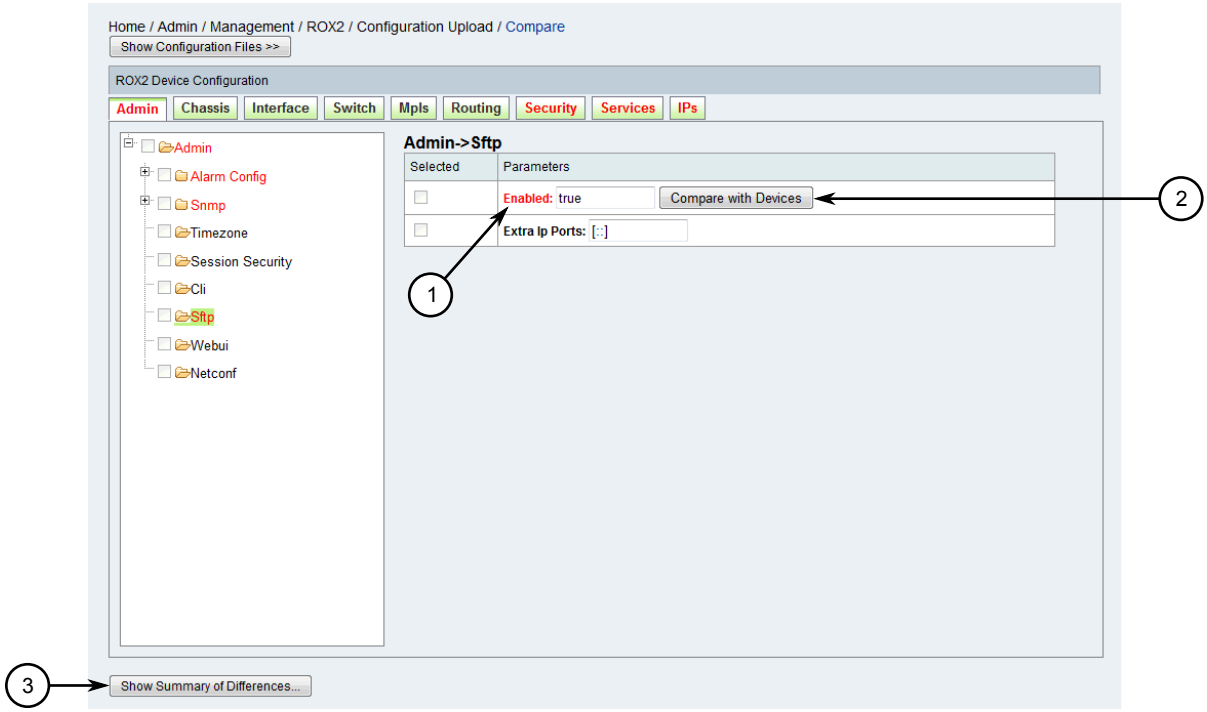
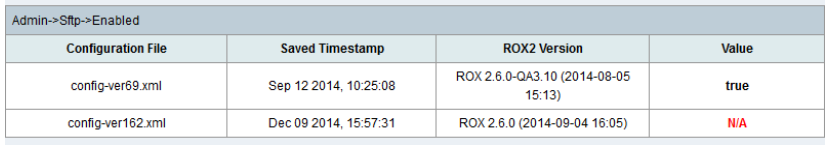


Figure 320: Compare Screen

1. Parameter Value is Different in Configuration Files **2.** Compare with Devices Button **3.** Show Summary of Differences Button

5. Review the parameters under each tab. Parameters that have different values in the configuration files are highlighted in red and are accompanied by a **Compare with Devices** button.
6. [Optional] To compare the different values available for a specific parameter, click **Compare with Devices**. A dialog box appears displaying the target name (i.e. configuration file), the software version and the different values.



Admin->Sftp->Enabled

Configuration File	Saved Timestamp	ROX2 Version	Value
config-ver69.xml	Sep 12 2014, 10:25:08	ROX 2.6.0-QA3.10 (2014-08-05 15:13)	true
config-ver162.xml	Dec 09 2014, 15:57:31	ROX 2.6.0 (2014-09-04 16:05)	N/A

Figure 321: Parameter Value Comparison Dialog Box

7. [Optional] To display a summary of all differences between the configuration files, click **Show Summary of Differences**. A dialog box appears displaying the path, parameters and target name (i.e. configuration file).

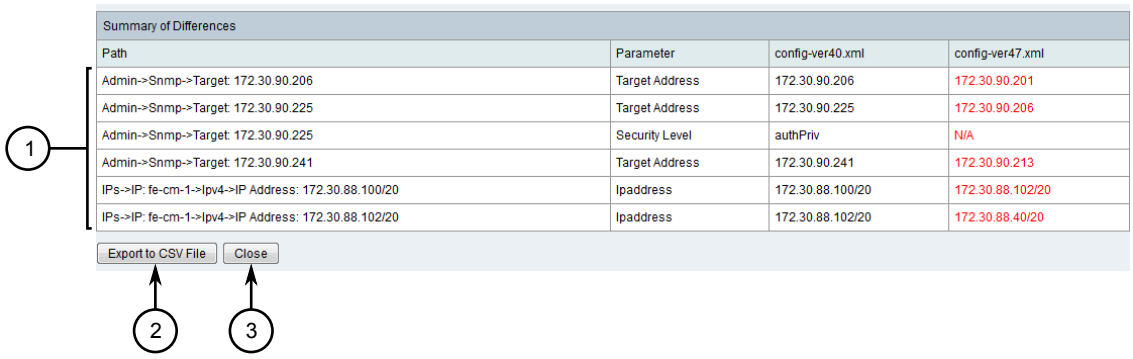


Figure 322: Show Differences Dialog Box

1. Export to CSV File Button **2.** Close Button

8. [Optional] Click **Export to CSV File** to export the list of differences to a CSV (*.csv) file, or click **Close**.

Section 6.6.4

Deleting an Archived Configuration File

To delete an archived configuration file taken from a RUGGEDCOM device from the RUGGEDCOM NMS server, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Archived Configuration File Upload**. The **Configuration Upload** screen appears.

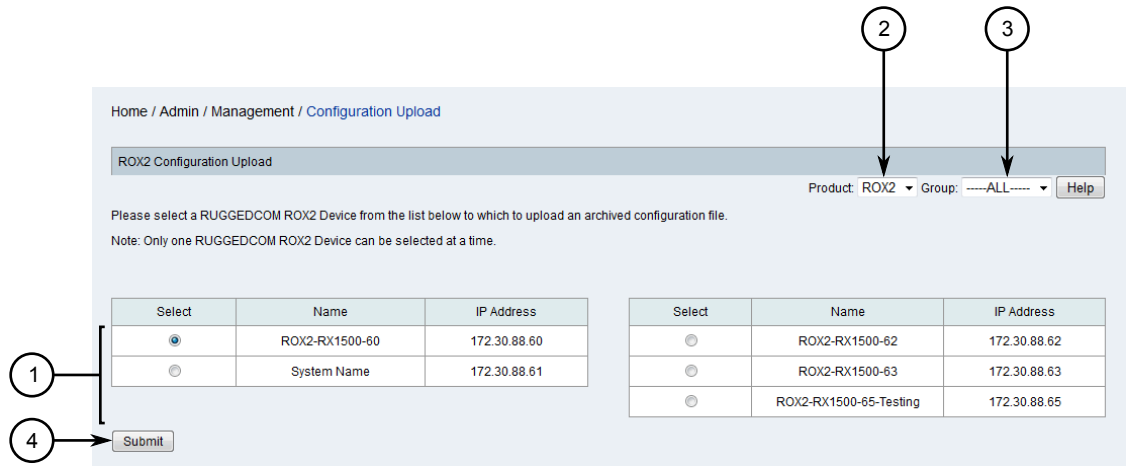


Figure 323: Configuration Upload Screen

1. Available Devices **2.** Product List **3.** Group List **4.** Submit Button

2. Use the **Product** and **Group** lists to filter the list of available devices.
3. Select a device and then click **Submit**. If previously archived configuration files are available for the chosen device, **Configuration Upload** screen appears.

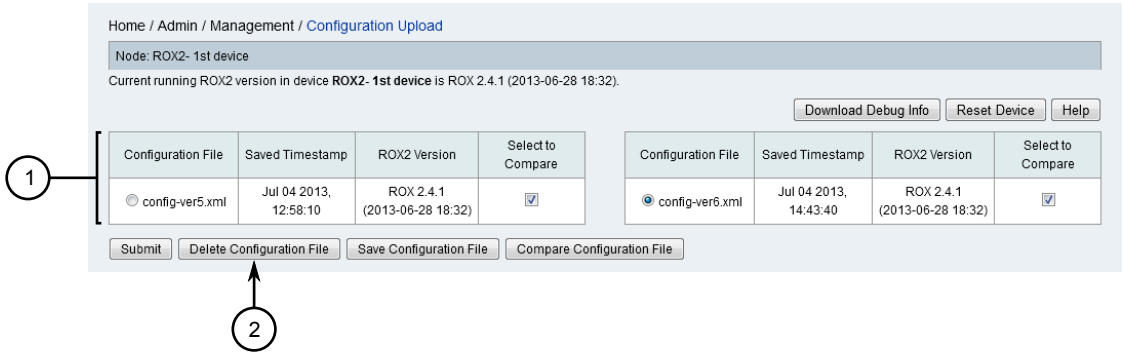


Figure 324: Configuration Upload Screen

1. Available Configuration Files **2.** Delete Configuration File Button

4. Select the desired configuration file and click **Delete Configuration File**. A confirmation dialog box appears.
5. Click **OK**.

Section 6.7

Managing Gold Configurations

Gold configuration management allows users to monitor specific parameters for consistency across a set of ROS and ROX II based devices. If the settings for the selected parameters deviate outside their defined boundaries, RUGGEDCOM NMS will send a notification. At that point, the current configuration for a device can be compared to the gold configuration to identify the deviations.

Gold configuration management is a useful tool for identifying potential problems early:

- It can catch invalid configuration changes on a device that could lead to network performance degradation
- It can catch malicious configuration changes on a device that could compromise network performance and stability

Multiple gold configurations can be created for different ROS and ROX II device groups.

CONTENTS

Section 6.7.1

Adding a Gold Configuration File

To add a gold configuration, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management** click **Gold Configuration** and then **Create Gold Configuration**. The **Create Gold Configuration** screen appears.

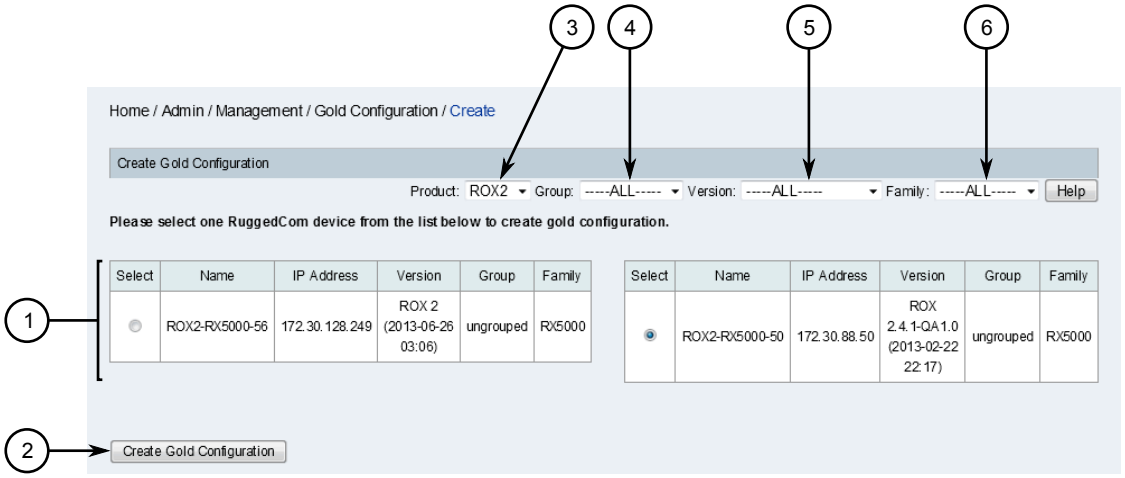


Figure 325: Create Gold Configuration Screen

1. Available Devices **2.** Create Gold Configuration Button **3.** Product List **4.** Group List **5.** Version List **6.** Family List

2. Use the **Product**, **Group**, **Version** and **Family** lists to filter the list of available devices.
3. Select one of the available devices and then click **Create Gold Configuration**. Once the gold configuration is ready, the **Edit** screen appears.

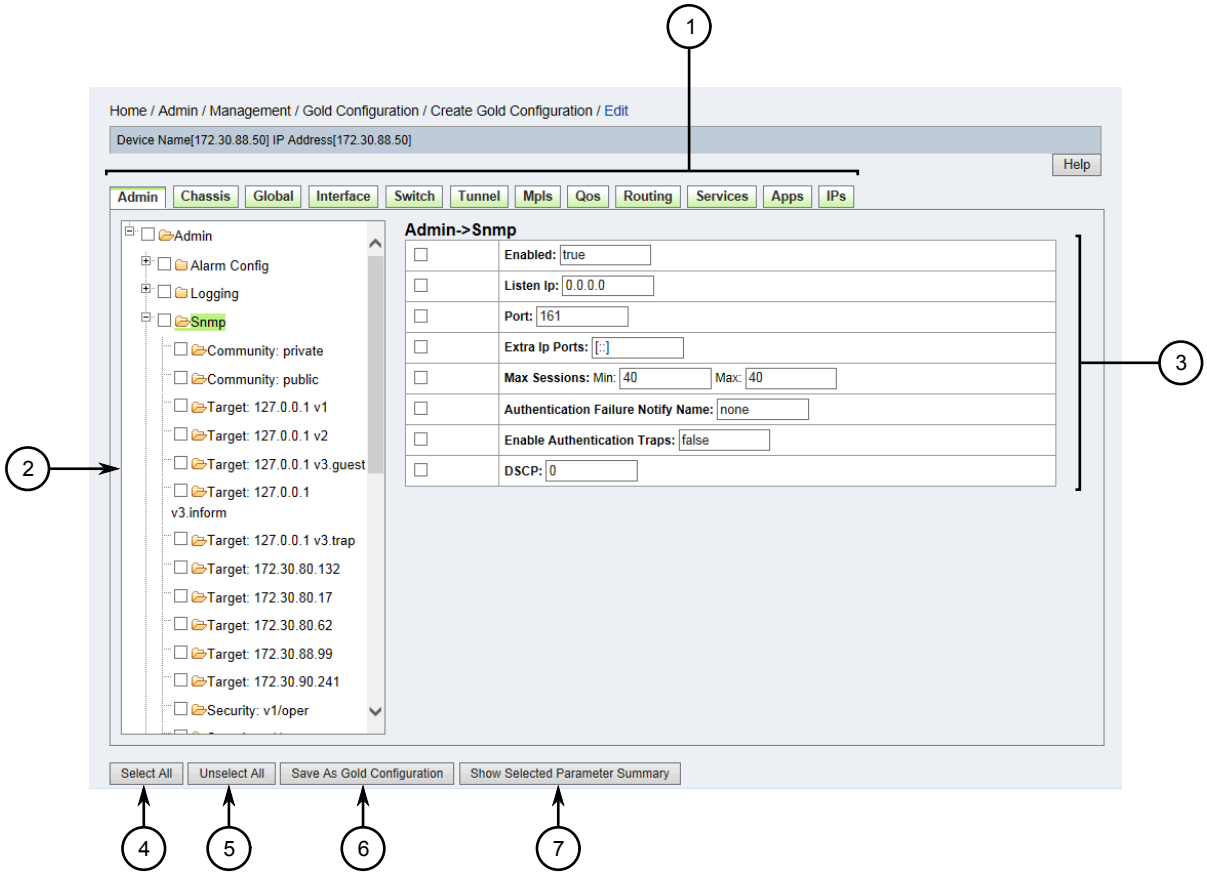


Figure 326: Edit Screen

1. Tabs **2.** Tree Menu **3.** Parameters **4.** Select All Button **5.** Unselect All Button **6.** Save As Gold Configuration Button **7.** Show Selected Parameter Summary Button

Parameters for the device are organized first by general categories, represented by the tabs at the top of the screen. Parameters are then organized into sub-groups, which can be accessed through the tree menu.

4. Locate the desired parameters in the configuration file structure and apply changes as required.

   Select the check box next to a parameter to monitor it, or clear the check box to stop monitoring the parameter. By default, all parameters are selected.

   Parameter values can also be changed. Any changes made will be applied to all associated devices.

5. [Optional] Click **Show Selected Parameter Summary** to list the parameters that will be included in the gold configuration. The **Selected Parameter Summary** screen appears in a new window, displaying the path, parameter and value for each selected parameter.

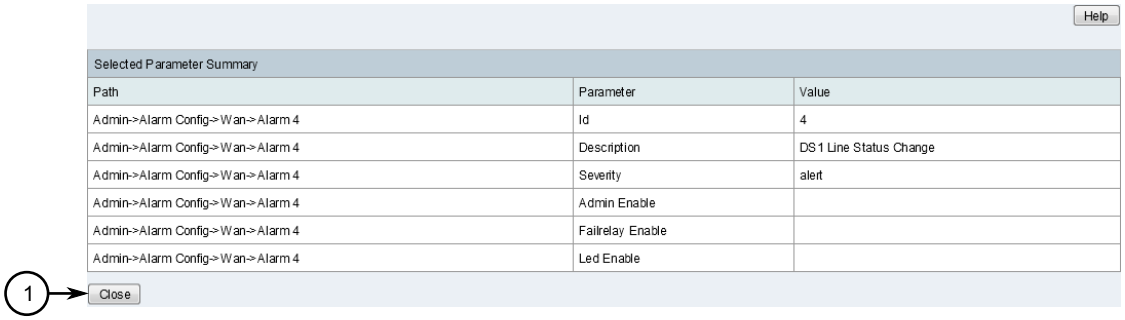


Figure 327: Selected Parameter Summary Window

1. Close

Click **Close** when done reviewing the parameters.

6. Click **Save as Gold Configuration**. If the configuration for any device in the associated group conflicts with the gold configuration, a confirmation message appears. Click **OK**.

   Otherwise, the **Gold Configuration Info** screen appears in a new window.

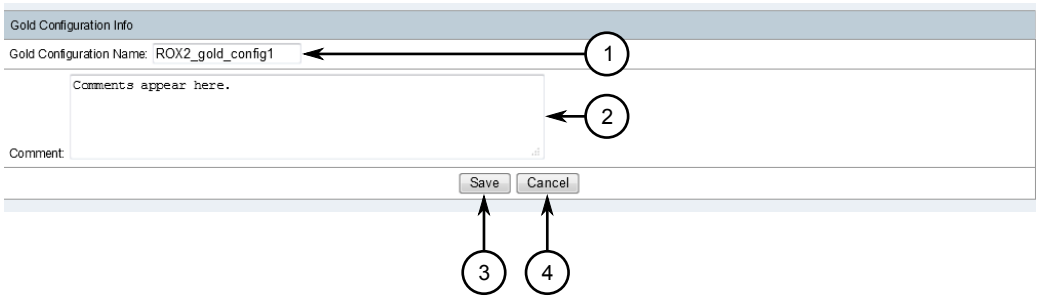


Figure 328: Gold Configuration Info Window

1. Gold Configuration Name Box **2.** Comment Box **3.** Save Button **4.** Cancel Button

7. Under **Gold Configuration Name**, type a new name for the gold configuration.
8. [Optional] Under **Comment**, type a comment related to the gold configuration.
9. Click **Save**. If the name of the gold configuration was not changed, a confirmation message appears asking for permission to overwrite the current gold configuration. Click **OK**.

   If the gold configuration was successfully saved, a confirmation message appears. However, if any errors were detected in the configuration, an error message appears and the gold configuration is not saved. Repeat Step 4 to Step 9 to review and update the configuration.
10. [Optional] To monitor more than one device and compare configurations, associate a group of devices with the new gold configuration. For more information, refer to Section 6.7.4, "Adding/Removing a Group Association" .

Section 6.7.2

Editing a Gold Configuration

To edit a gold configuration, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **Gold Configuration** and then click **Manage Gold Configuration**. The **Manage** screen appears.

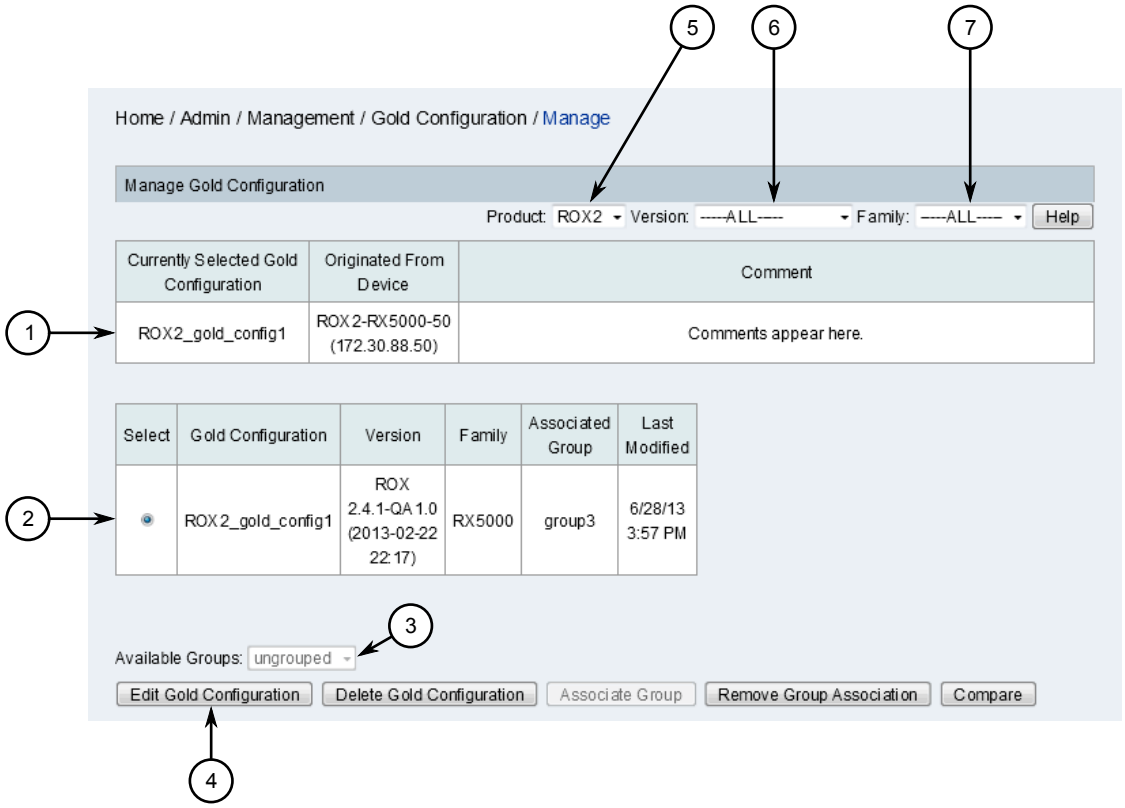


Figure 329: Manage Screen

1. Selected Gold Configuration **2.** Available Gold Configurations **3.** Available Groups List **4.** Edit Gold Configuration Button
5. Product List **6.** Version List **7.** Family List

2. Use the **Product**, **Version** and **Family** lists to filter the list of available devices.
3. Select a gold configuration from the list. Information about the selected configuration is displayed in the table above the list.

   If necessary, compare gold configuration files to determine which one to edit. For more information, refer to Section 6.7.5, "Comparing Gold Configuration Files" .
4. Click **Edit Gold Configuration**. The **Edit** screen appears.

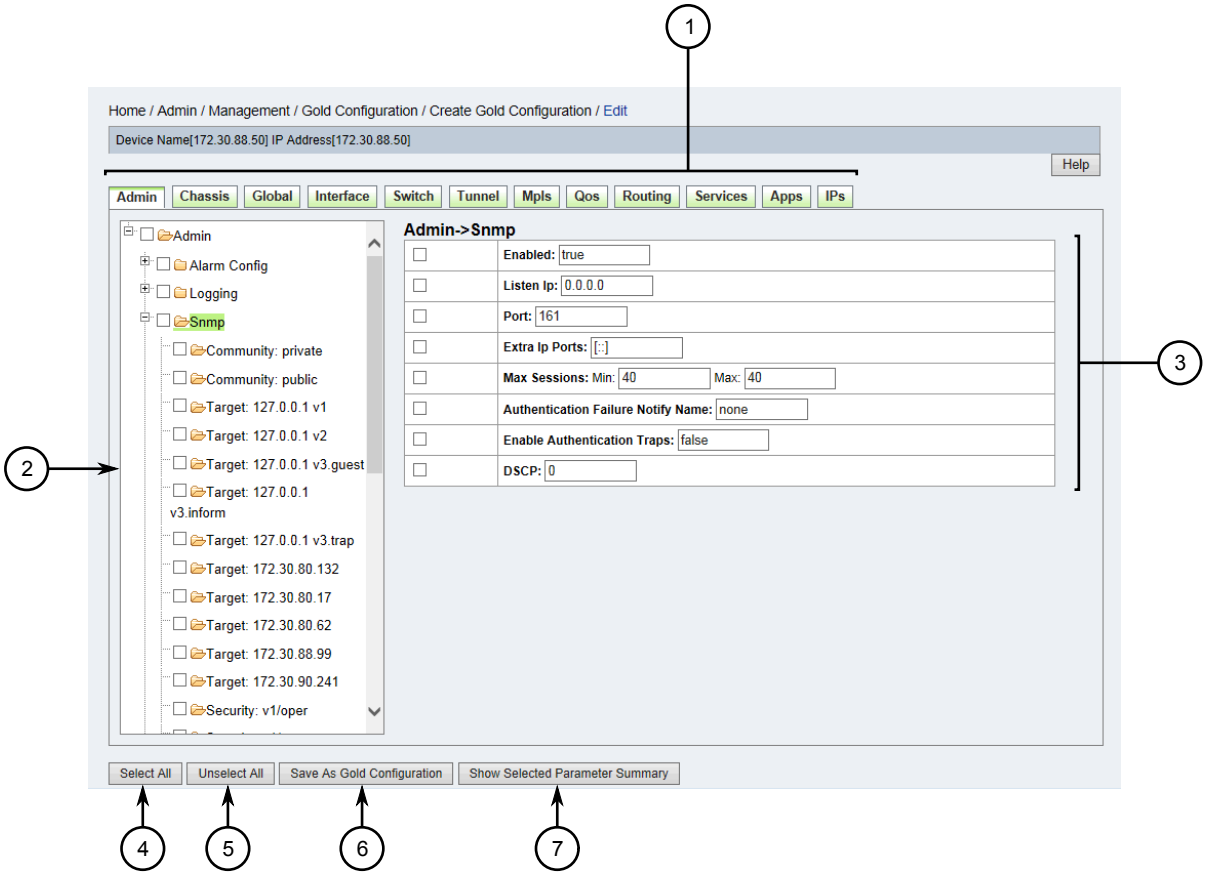


Figure 330: Edit Screen

1. Tabs **2.** Tree Menu **3.** Parameters **4.** Select All Button **5.** Unselect All Button **6.** Save As Gold Configuration Button **7.** Show Selected Parameter Summary Button

Parameters for the device are organized first by general categories, represented by the tabs at the top of the screen. Parameters are then organized into sub-groups, which can be accessed through the tree menu.

5. Locate the desired parameters in the configuration file structure and apply changes as required.

   Select the check box next to a parameter to monitor it, or clear the check box to stop monitoring the parameter. By default, all parameters are selected.

   Parameter values can also be changed. Any changes made will be applied to all associated devices.

6. [Optional] Click **Show Selected Parameter Summary** to list the parameters that will be included in the gold configuration. The **Selected Parameter Summary** screen appears in a new window, displaying the path, parameter and value for each selected parameter.

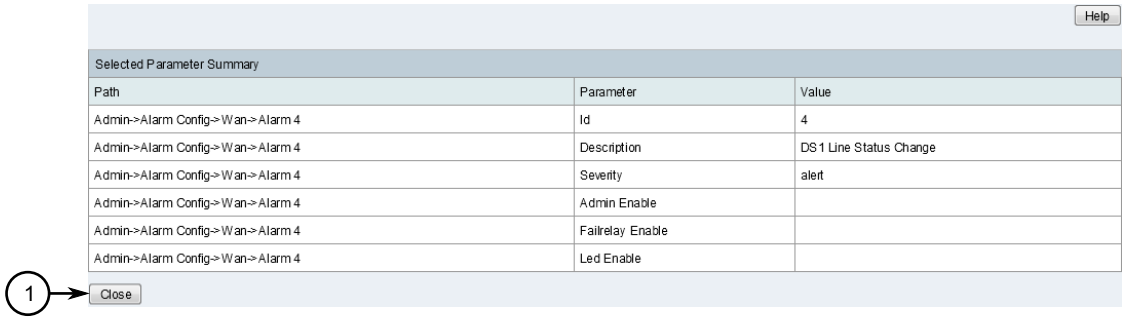


Figure 331: Selected Parameter Summary Window

1. Close Button

Click **Close** when done reviewing the parameters.

7. Click **Save as Gold Configuration**. If the configuration for any device in the associated group conflicts with the gold configuration, a confirmation message appears. Click **OK**.

   Otherwise, the **Gold Configuration Info** screen appears in a new window.

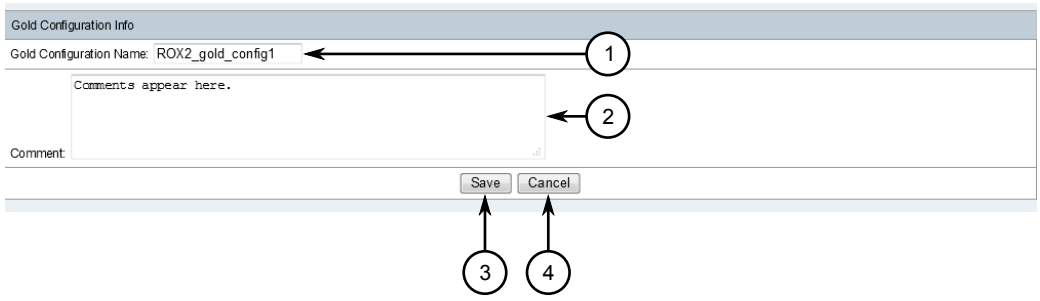


Figure 332: Gold Configuration Info Window

1. Gold Configuration Name Box **2.** Comment Box **3.** Save Button **4.** Cancel Button

8. [Optional] Under **Gold Configuration Name**, type a new name for the gold configuration.
9. [Optional] Under **Comment**, type a comment related to the gold configuration.
10. Click **Save**. If the name of the gold configuration was not changed, a confirmation message appears asking for permission to overwrite the current gold configuration. Click **OK**.

    If the gold configuration was successfully saved, a confirmation message appears. However, if any errors were detected in the configuration, an error message appears and the gold configuration is not saved. Repeat Step 5 to Step 10 to review and update the configuration.

Section 6.7.3
Deleting a Gold Configuration

To delete a gold configuration, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **Gold Configuration** and then click **Manage Gold Configuration**. The **Manage** screen appears.

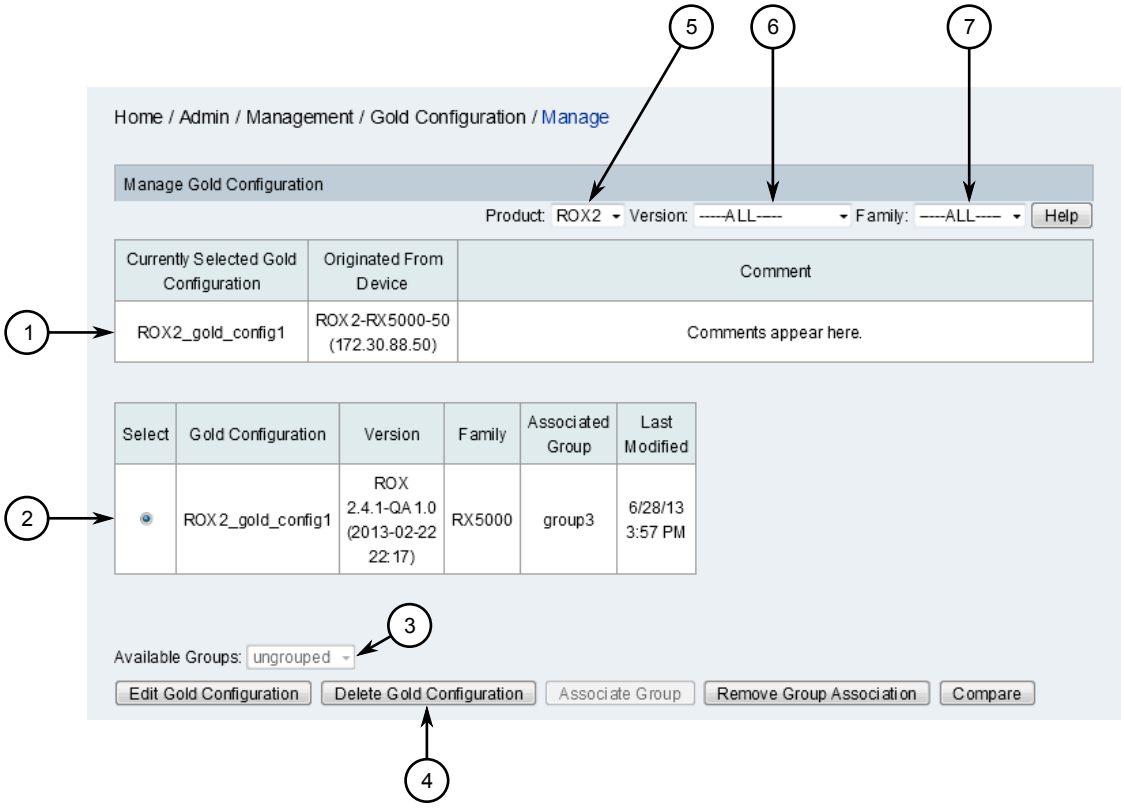


Figure 333: Manage Screen

1. Selected Gold Configuration **2.** Available Gold Configurations **3.** Available Groups List **4.** Edit Gold Configuration Button **5.** Product List **6.** Version List **7.** Family List

2. Use the **Product**, **Version** and **Family** lists to filter the list of available devices.
3. Select a gold configuration from the list. Information about the selected configuration is displayed in the table above the list.

   If necessary, compare gold configuration files to determine which one to delete. For more information, refer to Section 6.7.5, "Comparing Gold Configuration Files" .
4. Click **Delete Gold Configuration**. A confirmation message appears.
5. Click **OK** to confirm.

Section 6.7.4

Adding/Removing a Group Association

For a gold configuration to monitor more than one device and compare their configurations, a group must be associated with the gold configuration.

To add a group association or remove an existing association, do the following:

1. If associating a group with the gold configuration, make sure the desired group is available. For more information, refer to Section 5.5.18, "Managing Device Groups" .
2. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **Gold Configuration** and then click **Manage Gold Configuration**. The **Manage** screen appears.

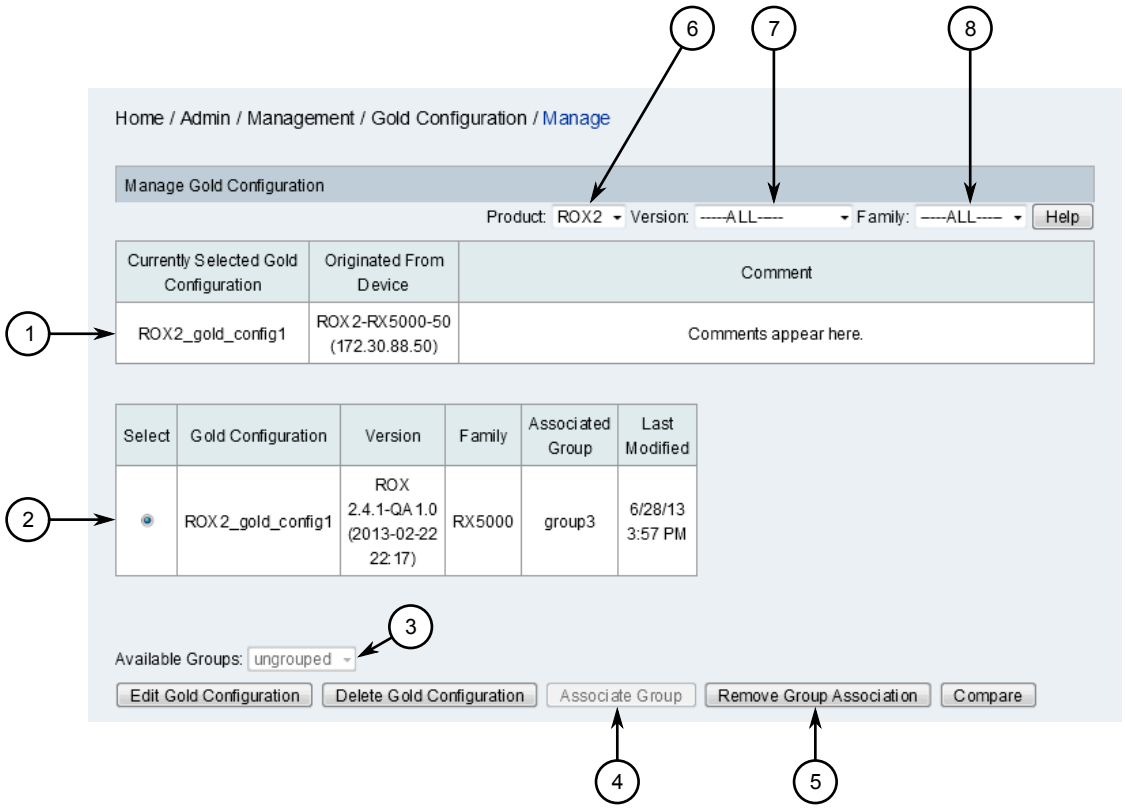


Figure 334: Manage Screen

1. Selected Gold Configuration **2.** Available Gold Configurations **3.** Available Groups List **4.** Associate Group Button **5.** Remove Group Association Button **6.** Product List **7.** Version List **8.** Family List

3. Use the **Product**, **Version** and **Family** lists to filter the list of available devices.
4. Select a gold configuration from the list. Information about the selected configuration is displayed in the table above the list.
5. If associating a group with the gold configuration, select a group from the **Available Groups** list.
6. Click either **Associate Group** or **Remove Group Association**. A confirmation message appears.
7. Click **OK** to confirm.

Section 6.7.5

Comparing Gold Configuration Files

Notifications that announce a change to a monitored parameter include a link that – when clicked – shows the difference between the current parameter value and the previous value.

Admin->Logging->Diagnostics->Developer Log->Enabled				
Device Name	**IP Address**	**Version**	**Family**	**Value**
ROX2_gold_config	172.30.88.60	ROX 2.6.1 (2014-10-31 15:12)	RX15XX	**false**
ROX2-RX1500-60	172.30.88.60	ROX 2.6.1 (2014-10-31 15:12)	RX15XX	**false**
ROX5000	172.30.88.50	N/A	RX5000	**true**

Figure 335: Parameter Level Comparison

To further explore the differences between a gold configuration and the devices in its associated group, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **Gold Configuration** and then click **Manage Gold Configuration**. The **Manage** screen appears.

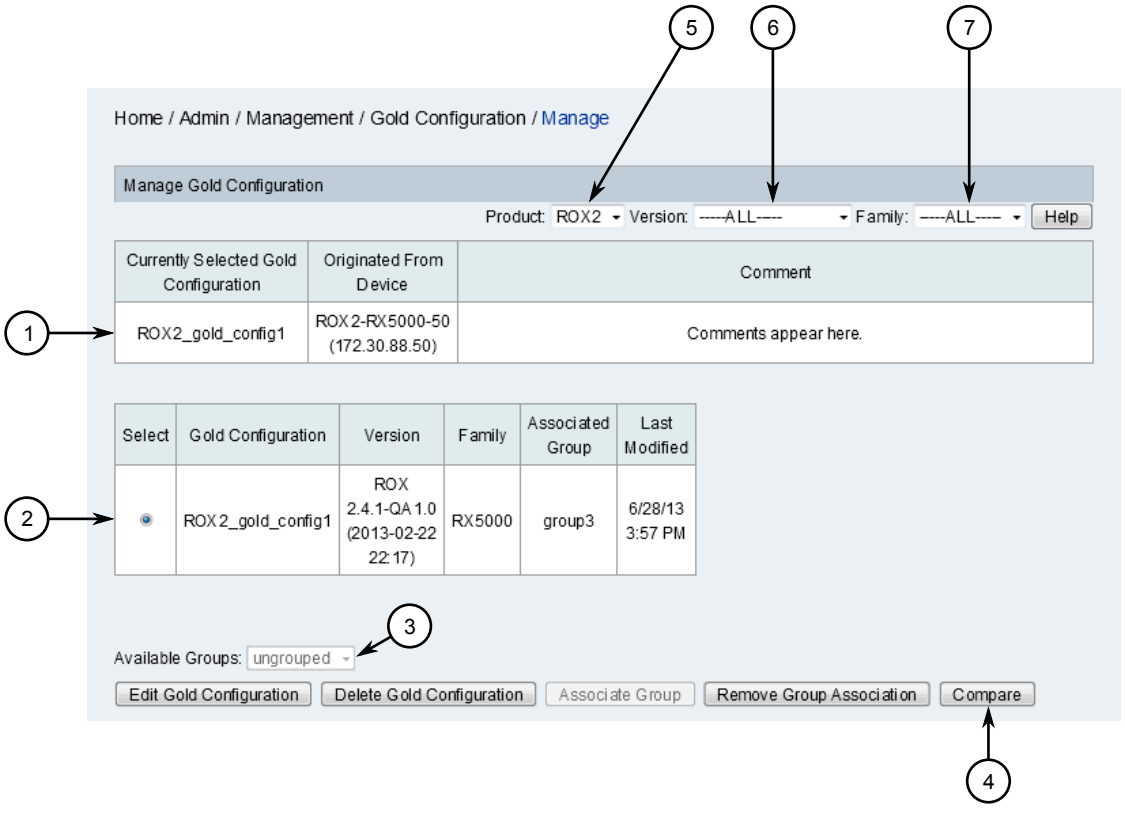


Figure 336: Manage Screen

1. Selected Gold Configuration **2.** Available Gold Configurations **3.** Available Groups List **4.** Compare Button **5.** Product List **6.** Version List **7.** Family List

2. Use the **Product**, **Version** and **Family** lists to filter the list of available devices.
3. Select a gold configuration from the list. Information about the selected configuration is displayed in the table above the list.
4. Click **Compare**. The **Compare Result** screen appears.

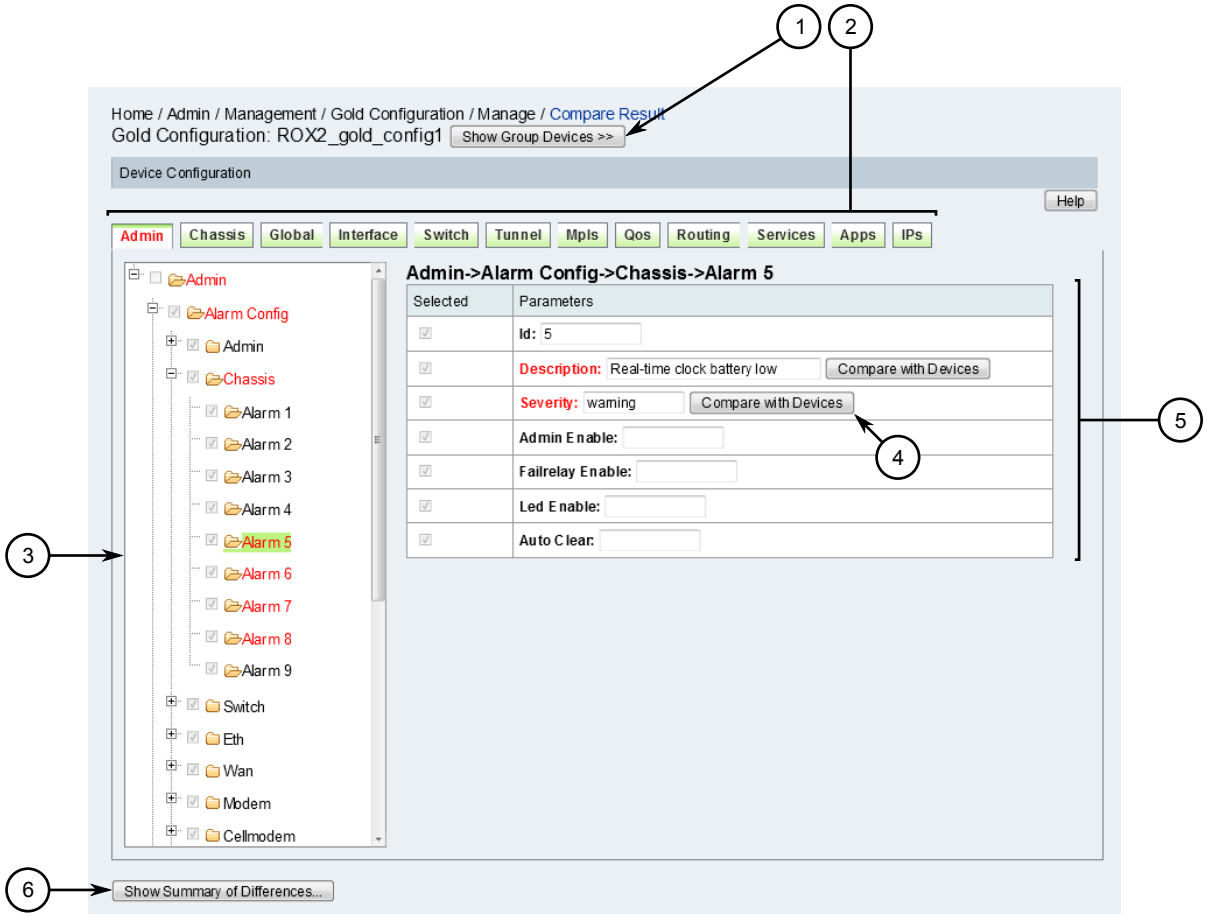


Figure 337: Compare Result

1. Show Group Devices Button **2.** Tabs **3.** Tree Menu **4.** Compare With Devices Button **5.** Parameters **6.** Show Summary of Differences Button

Parameters for the device are organized first by general categories, represented by the tabs at the top of the screen. Parameters are then organized into sub-groups, which can be accessed through the tree menu.

Categories, groups and parameters highlighted in red indicate parameter settings on the device that differ from the other devices associated with the gold configuration.

5. [Optional] To display the list of devices in the group, click **Show Group Devices**. Click **Hide Group Devices** to hide the list.
6. [Optional] Compare parameters individually by locating parameters highlighted in red and clicking **Compare With Devices**. A new window appears listing all ROS or ROX II devices in the group and their values for the parameter. Refer to Figure 335 .

   Click **Close** when done reviewing the differences.
7. Click **Show Summary of Differences** to display a list of differences between all ROS or ROX II devices in the group. The **Summary of Differences** screen appears in a new window.

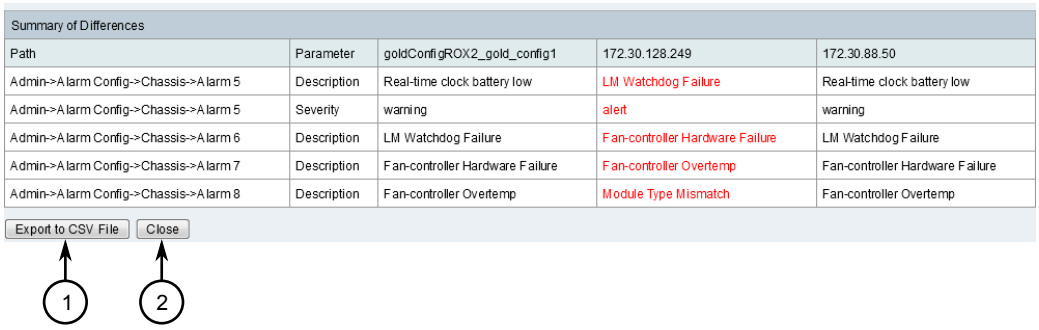


Figure 338: Summary of Differences Screen

1. Export to CSV File Button **2.** Close Button

8. [Optional] Click **Export to CSV File** to export the summary of differences to a CSV (Comma-Separate Value) file. A dialog box appears.
9. Click **Save**. The CSV file is saved with the default filename `diffs.csv`.

Section 6.8

Managing the Dynamic Configuration of ROS/ROX II Devices

RUGGEDCOM NMS uses a template approach to updating, comparing, and validating (ROX II only) the current configurations for multiple RUGGEDCOM ROS and RUGGEDCOM ROX II devices. The template is based on either one of the target devices or a template the user has saved based on another configuration. This allows for the application of common settings, allowing users to create consistent configurations and update new devices quickly.

IMPORTANT!
Configuration files can only be updated if all target ROS devices are v4.2.0 or higher, and all target ROX II devices are running ROX v2.3.0 or higher.

CONTENTS

- Section 6.8.5, "Comparing Configuration Files"

Section 6.8.1
Creating a Configuration Template

To create a configuration template, do the following:

NOTE
*Use the **Product** list to select either ROS or ROX II devices.*

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Dynamic Configuration**. The **Dynamic Configuration** screen appears.

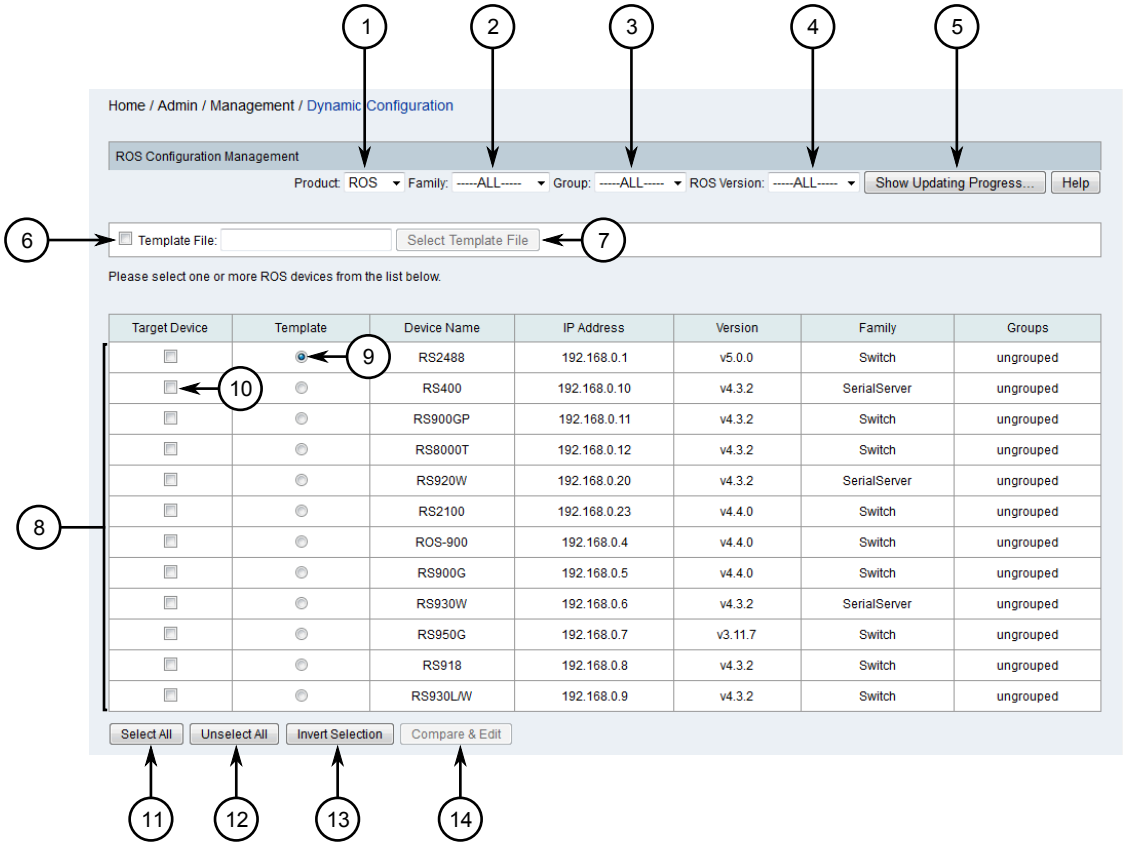


Figure 339: Dynamic Configuration Screen

1. Product List **2.** Family List **3.** Group List **4.** Version List (ROS or ROX2) **5.** Show Updating Progress Button **6.** Template File Check Box **7.** Select Template Button **8.** Available Devices **9.** Template Option **10.** Target Device Check Box **11.** Select All Button **12.** Unselect All Button **13.** Invert Selection Button **14.** Compare & Edit Button

2. Use the **Product**, **Family**, **Group** and **Version** lists to filter the list of available ROS or ROX II devices.
3. Select the device whose configuration will be saved as a template, and then click **Compare & Edit**. The **Configuration** screen appears.

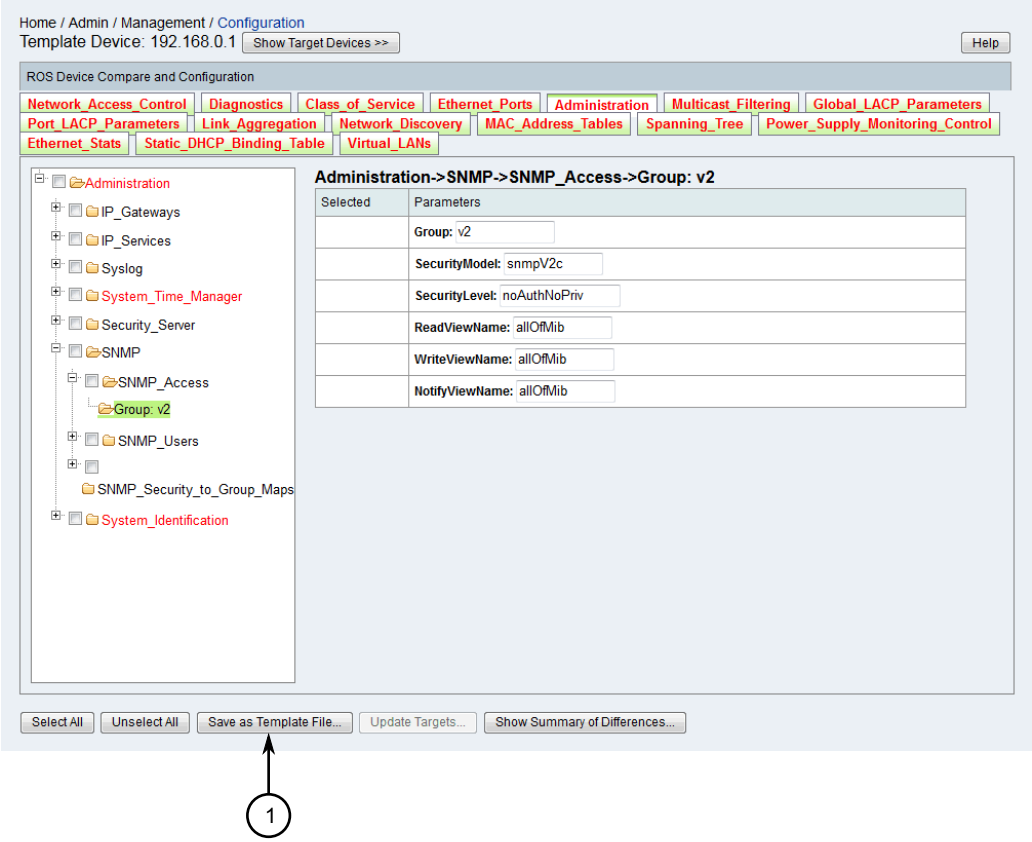


Figure 340: Configuration Screen

1. Save as Template File Button

4. Click **Save as Template File**. A dialog box appears.

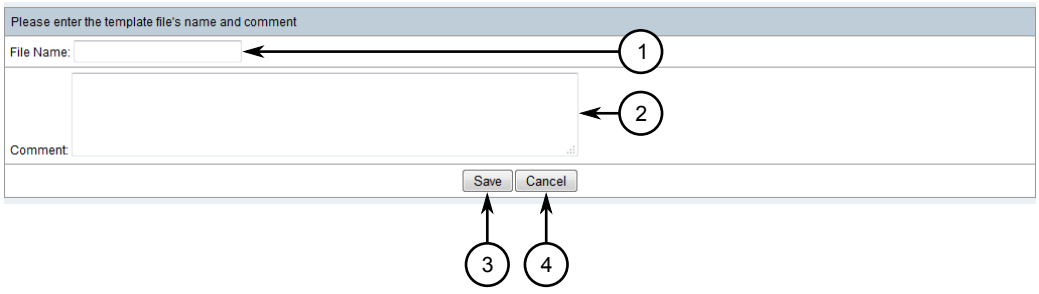


Figure 341: Dialog Box

1. File Name Box **2.** Comment Box **3.** Save Button **4.** Cancel Button

5. Under **File Name**, type the name of the new configuration template.
6. [Optional] Under **Comment**, type a description or comment related to the new configuration template.
7. Click **Save**. A confirmation dialog box appears.

8. Click **OK**.

Section 6.8.2
Selecting a Saved Configuration Template

To select a saved configuration template to use as the base for one or more RUGGEDCOM NMS ROS or ROX II devices, do the following:

NOTE
*Use the **Product** list to select either ROS or ROX II devices.*

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Dynamic Configuration**. The **Dynamic Configuration** screen appears.

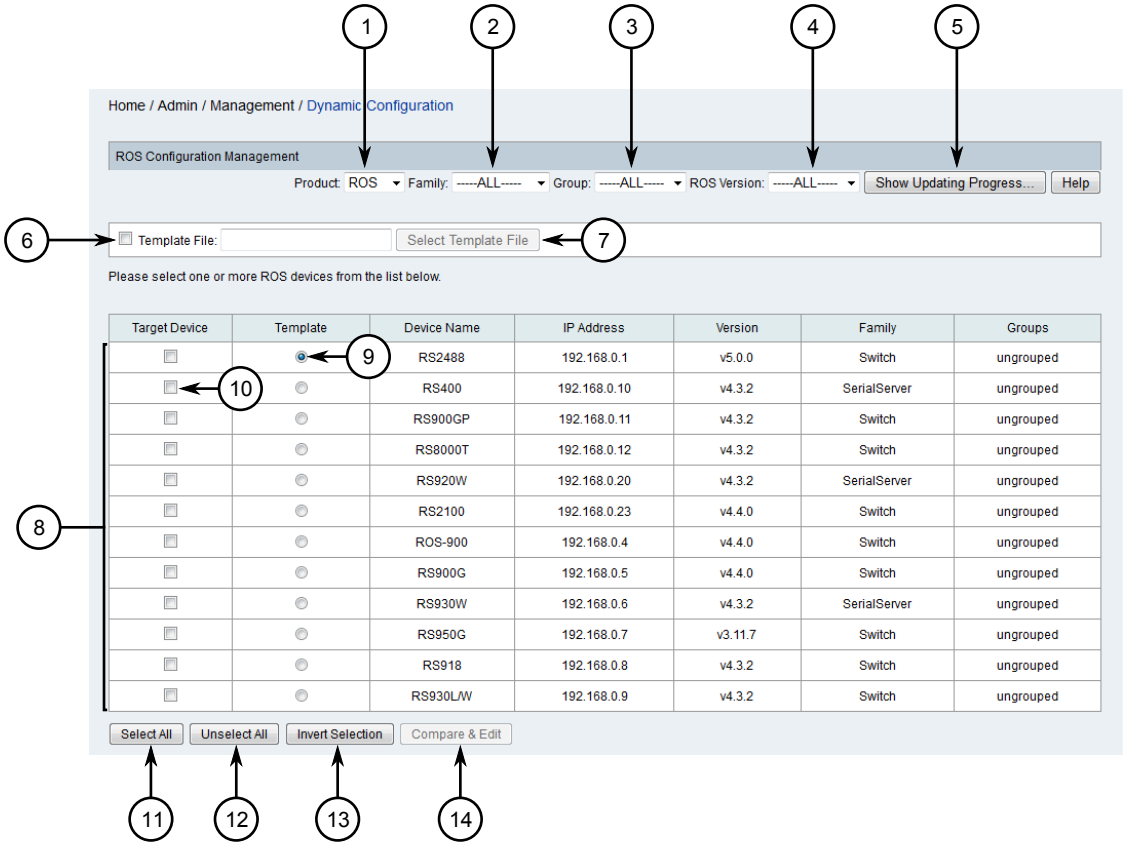


Figure 342: Dynamic Configuration Screen

1. Product List **2.** Family List **3.** Group List **4.** Version List (ROS or ROX2) **5.** Show Updating Progress Button **6.** Template File Check Box **7.** Select Template Button **8.** Available Devices **9.** Template Option **10.** Target Device Check Box **11.** Select All Button **12.** Unselect All Button **13.** Invert Selection Button **14.** Compare & Edit Button

2. Use the **Product**, **Family**, **Group** and **Version** lists to filter the list of available ROS or ROX II devices.
3. Select **Template File** and then click **Select Template File**. A dialog box appears.

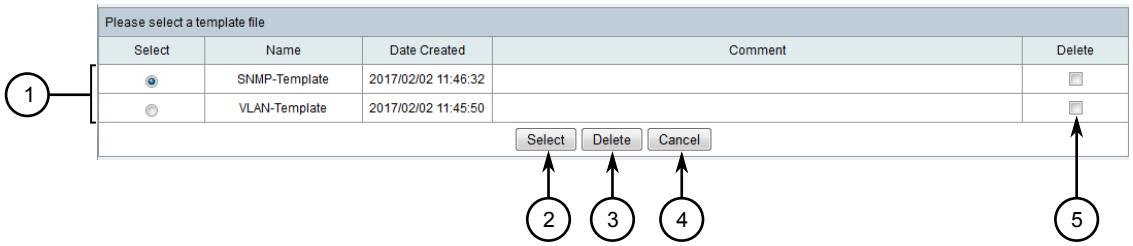


Figure 343: Dialog Box

1. Available Template Files **2.** Delete Check Box **3.** Select Button **4.** Delete Button **5.** Cancel Button

4. Select a configuration template.
5. Click **Select**. The dialog box closes and the name of the selected configuration template appears in the box next to the **Select Template**.

Section 6.8.3

Deleting a Saved Configuration Template

To delete a saved configuration template, do the following:

NOTE
*Use the **Product** list to select either ROS or ROX II devices.*

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Dynamic Configuration**. The **Dynamic Configuration** screen appears.

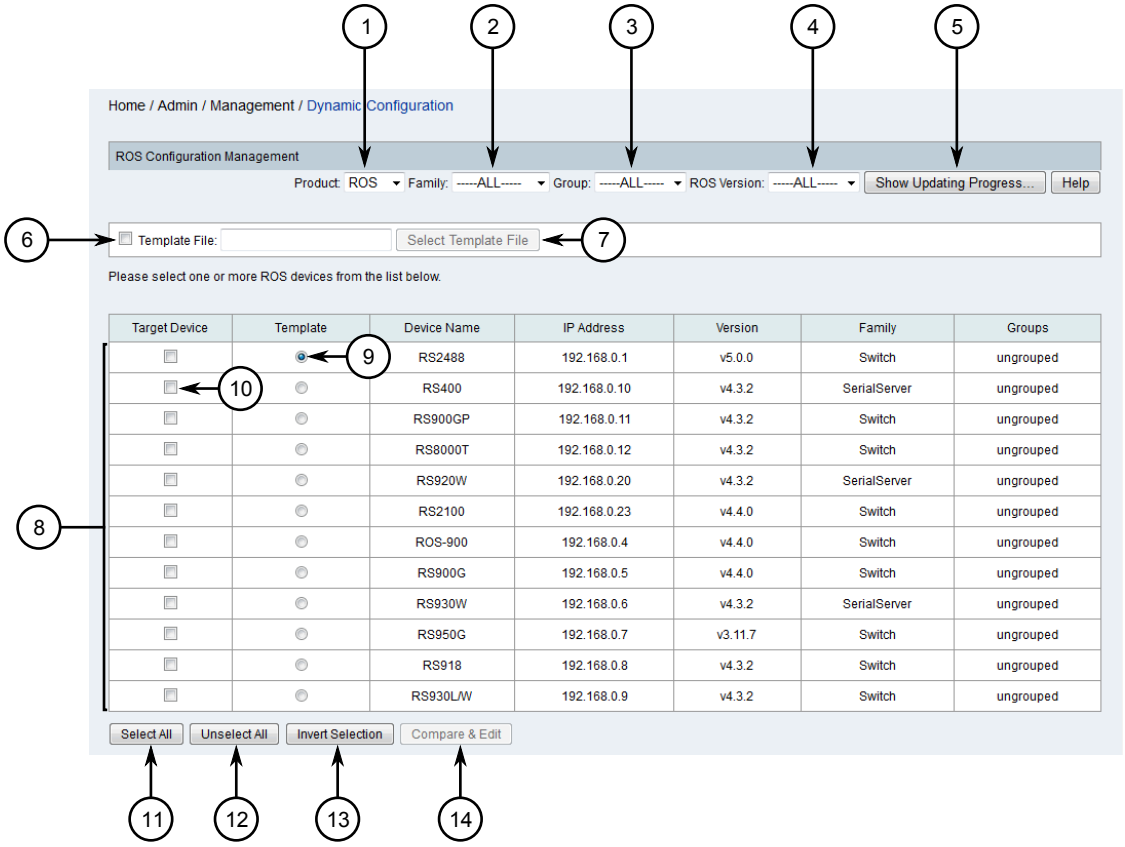


Figure 344: Dynamic Configuration Screen

1. Product List **2.** Family List **3.** Group List **4.** Version List (ROS or ROX2) **5.** Show Updating Progress Button **6.** Template File Check Box **7.** Select Template Button **8.** Available Devices **9.** Template Option **10.** Target Device Check Box **11.** Select All Button **12.** Unselect All Button **13.** Invert Selection Button **14.** Compare & Edit Button

2. Use the **Product**, **Family**, **Group** and **Version** lists to filter the list of available ROS or ROX II devices.
3. Select **Template File** and then click **Select Template File**. A dialog box appears.

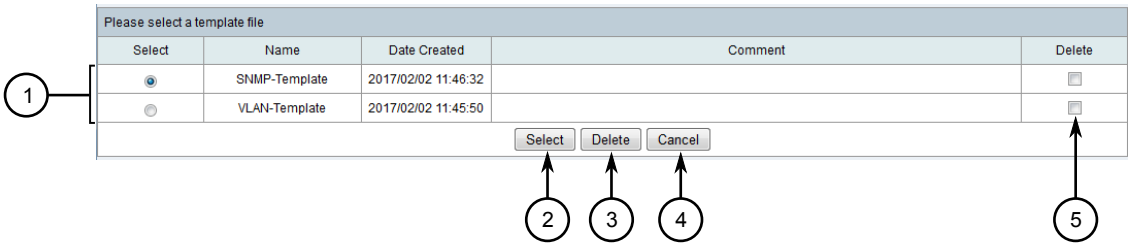


Figure 345: Dialog Box

1. Available Template Files **2.** Select Button **3.** Delete Button **4.** Cancel Button **5.** Delete Check Box

4. Select **Delete** next to one or more saved configuration templates.
5. Click **Delete**. A confirmation dialog box appears.

6. Click **OK**.

Section 6.8.4
Updating the Configuration of Devices

To update the configuration for one or more RUGGEDCOM ROS or RUGGEDCOM ROX II devices managed by RUGGEDCOM NMS, do the following:

NOTE
*Use the **Product** list to select either ROS or ROX II devices.*

NOTE
Make sure to choose devices with similar architecture and configuration when comparing and applying configurations to target devices.

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Dynamic Configuration**. The **Dynamic Configuration** screen appears.

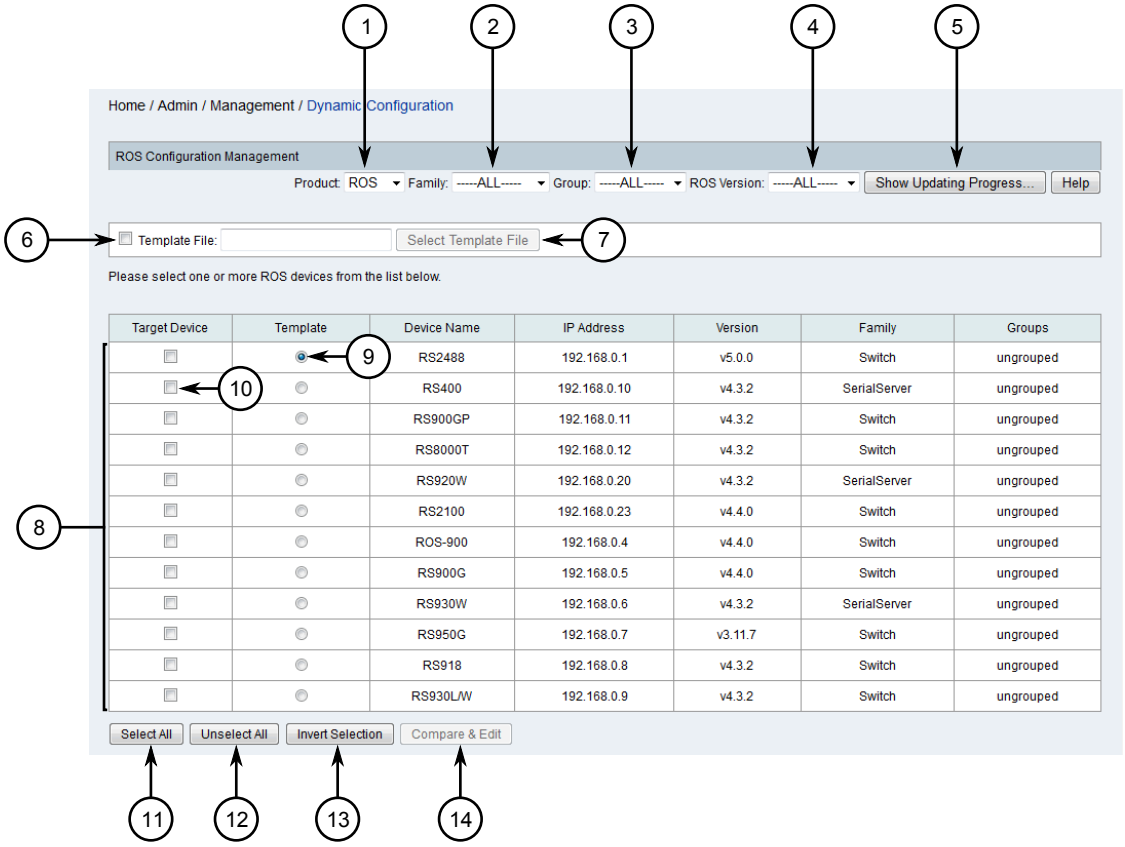


Figure 346: Dynamic Configuration Screen

1. Product List **2.** Family List **3.** Group List **4.** Version List (ROS or ROX2) **5.** Show Updating Progress Button **6.** Template File Check Box **7.** Select Template Button **8.** Available Devices **9.** Template Option **10.** Target Device Check Box **11.** Select All Button **12.** Unselect All Button **13.** Invert Selection Button **14.** Compare & Edit Button

2. Use the **Product**, **Family**, **Group** and **Version** lists to filter the list of available ROS or ROX II devices.
3. Select **Target Device** for one or more devices.
4. Select one of the selected devices to be the template or select a saved template. For information about how to select a saved template, refer to Section 6.8.2, “Selecting a Saved Configuration Template” .
5. Click **Compare & Edit**. The **Configuration** screen appears.

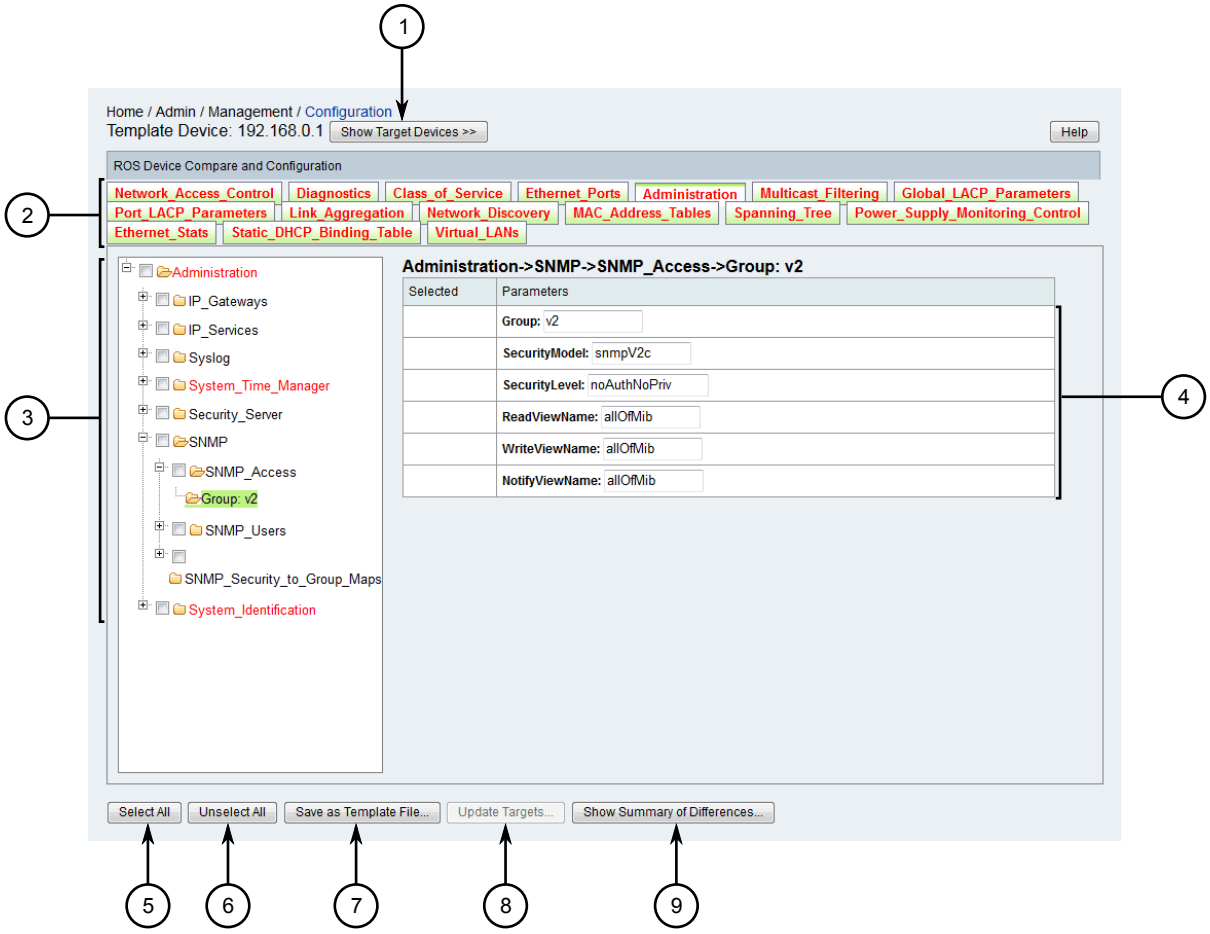


Figure 347: Configuration Screen

1. Show Target Devices Button **2.** Tabs **3.** Tree Menu **4.** Parameters **5.** Select All Button **6.** Unselect All Button **7.** Save As Template File Button **8.** Update Targets Button **9.** Show Summary of Differences Button

Parameters for the device are organized first by general categories, represented by the tabs at the top of the screen. Parameters are then organized into sub-groups, which can be accessed through the tree menu.

Categories, groups and parameters highlighted in red indicate parameter settings from the template device that differ from the other targets.

6. Select individual parameters to apply to the target devices or click **Select All** to select all parameters.
7. Update the values for the selected parameters as required.
8. [Optional] On RUGGEDCOM ROX II devices , it is possible validate changes.

   To validate the changes, click **Validate**. A dialog box appears.

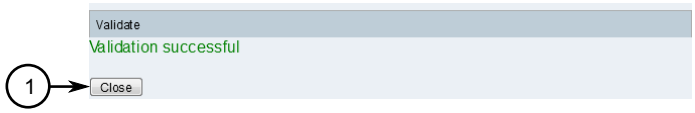


Figure 348: Dialog Box

1. Close Button

Once validation is complete, a message appears indicating whether or not the configuration passed.

Click **Close**. If the configuration did not pass validation, repeat Step 6 to Step 8 .

9. Click **Update Targets**. A dialog box appears.

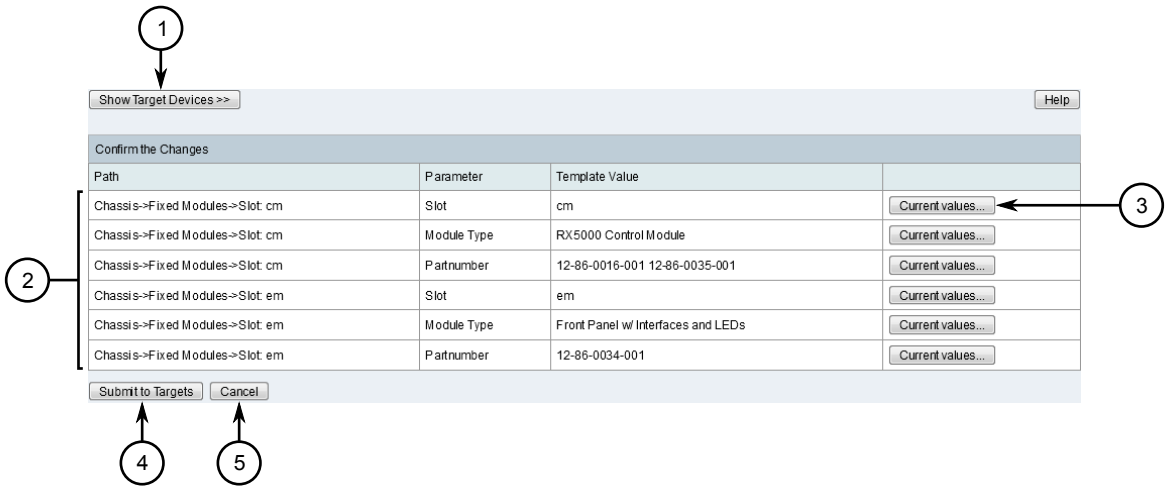


Figure 349: Dialog Box

1. Show Target Devices Button **2.** Changes to be Applied **3.** Current Values Button **4.** Submit to Targets Button **5.** Cancel Button

10. Click **Submit to Targets**. A confirmation dialog box appears.
11. Click **OK**. A dialog box appears displaying the progress of the update.
12. When the update is complete, click **Continue**, then click **Close**.

Section 6.8.5

Comparing Configuration Files

To compare two or more archived configuration files taken from a RUGGEDCOM ROX II device managed by RUGGEDCOM NMS, do the following:

NOTE
*Use the **Product** list to select either ROS or ROX II devices.*

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Dynamic Configuration**. The **Dynamic Configuration** screen appears.

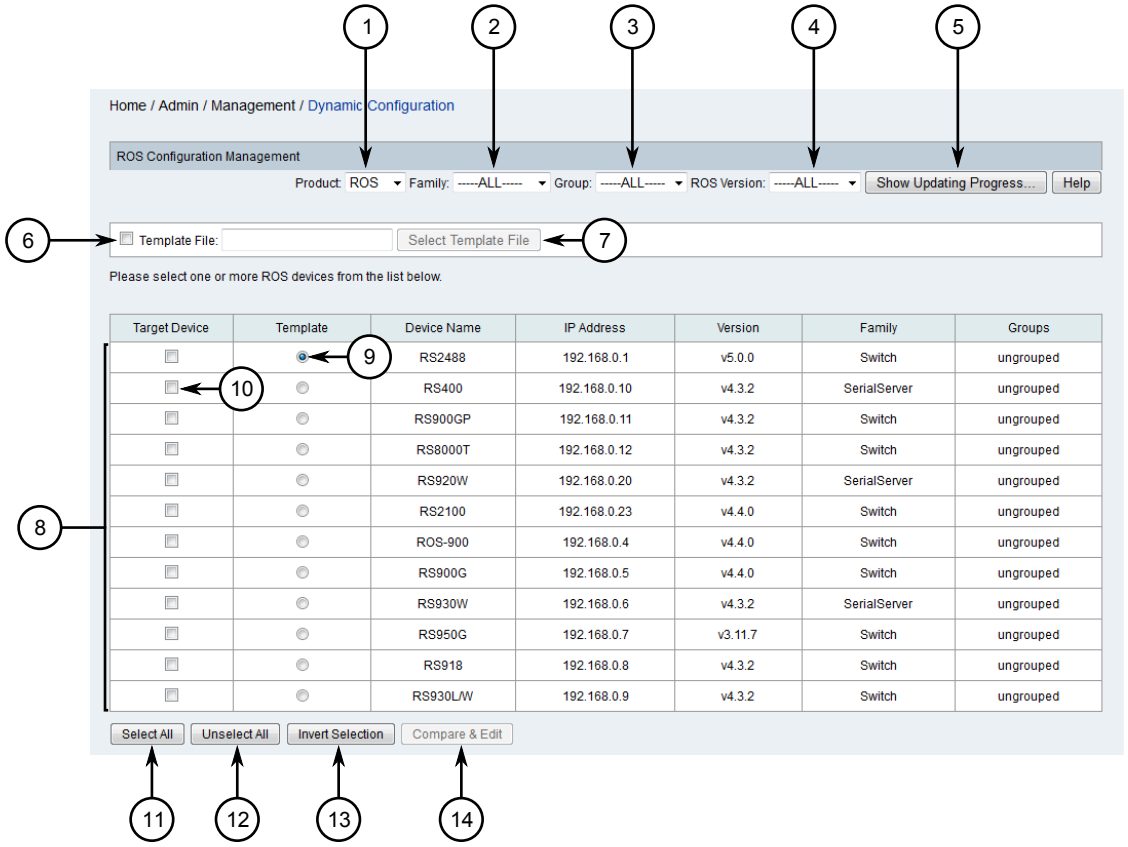


Figure 350: Dynamic Configuration Screen

1. Product List **2.** Family List **3.** Group List **4.** Version List (ROS or ROX2) **5.** Show Updating Progress Button **6.** Template File Check Box **7.** Select Template Button **8.** Available Devices **9.** Template Option **10.** Target Device Check Box **11.** Select All Button **12.** Unselect All Button **13.** Invert Selection Button **14.** Compare & Edit Button

2. Use the **Product**, **Family**, **Group** and **Version** lists to filter the list of available ROS or ROX II devices.
3. Select **Target Device** for one or more devices and then click **Compare & Edit**. The **Configuration** screen appears.

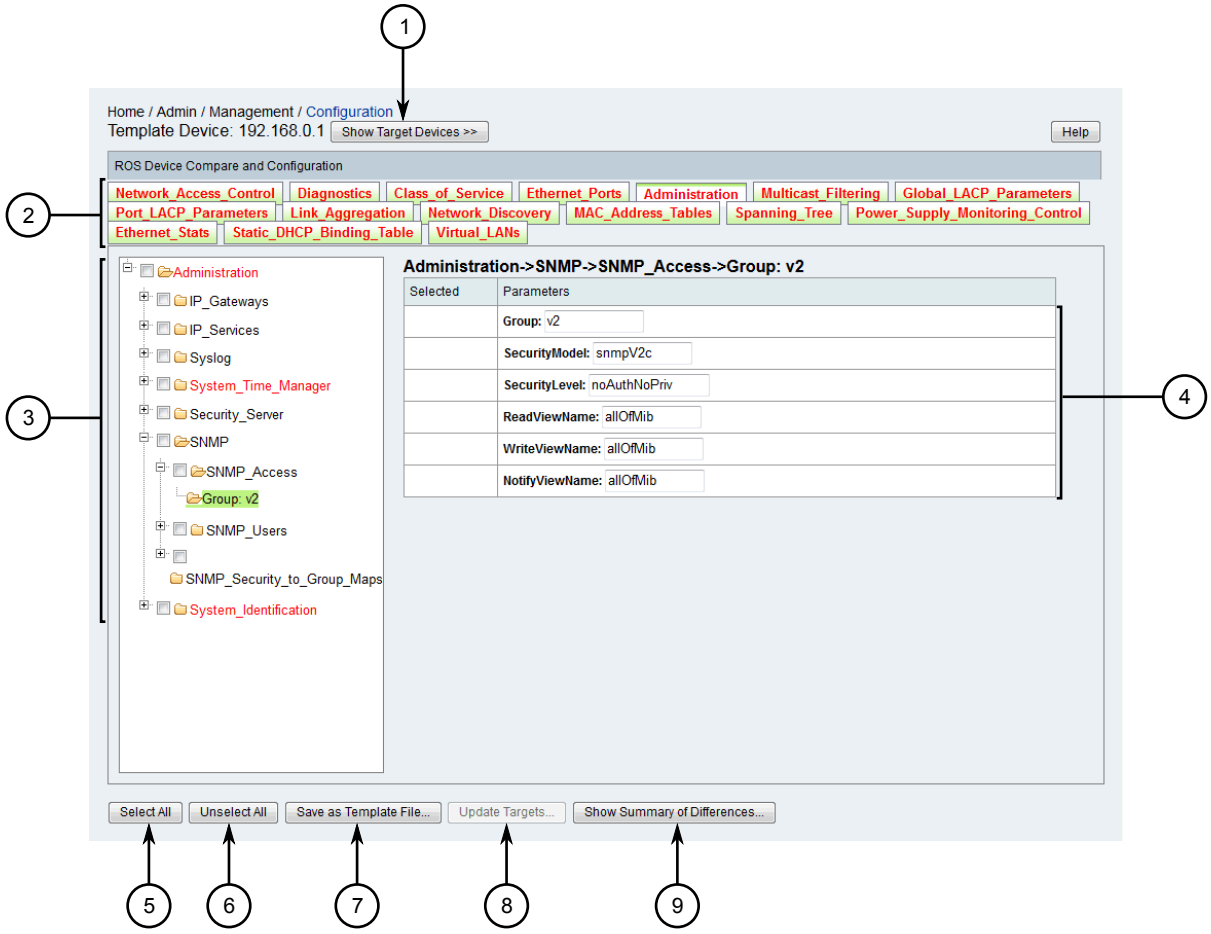


Figure 351: Configuration Screen

1. Show Target Devices Button **2.** Tabs **3.** Tree Menu **4.** Parameters **5.** Select All Button **6.** Unselect All Button **7.** Save As Template File Button **8.** Update Targets Button **9.** Show Summary of Differences Button

4. Review the parameters under each tab. Parameters that have different values in the configuration files are highlighted in red and are accompanied by a **Compare with Targets** button.
5. [Optional] To compare the different values available for a specific parameter, click **Compare with Targets**. A dialog box appears displaying the target name (i.e. configuration file), the software version and the different values.

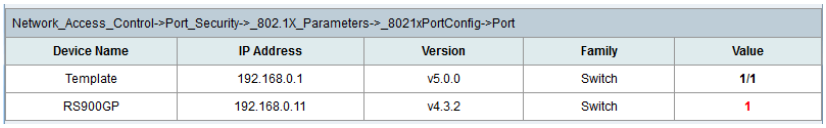


Figure 352: Parameter Value Comparison Dialog Box

6. [Optional] To display a summary of all differences between the configuration files, click **Show Summary of Differences**. A dialog box appears displaying the path, parameters and target name (i.e. configuration file).

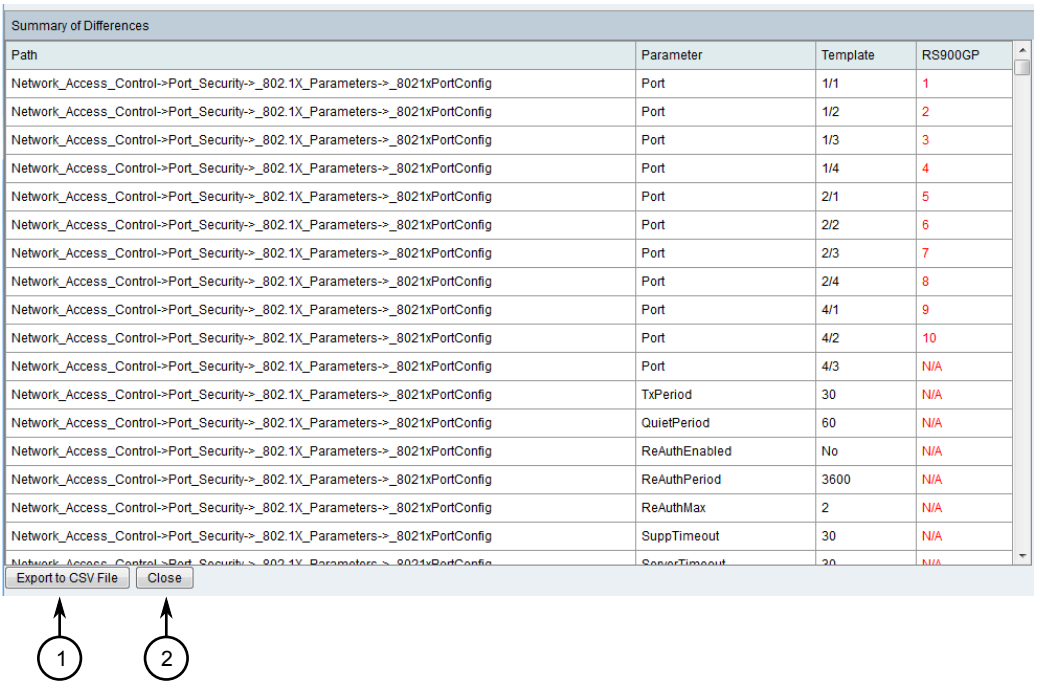


Figure 353: Show Differences Dialog Box

1. Export to CSV File Button **2.** Close Button

7. [Optional] Click **Export to CSV File** to export the list of differences to a CSV (*.csv) file, or click **Close**.

Section 6.9

Managing ROS Devices

This section describes how to manage RUGGEDCOM ROS devices managed by RUGGEDCOM NMS.

NOTE
For information about how to download, upload, compare, save and delete configuration files for RUGGEDCOM ROS devices, refer to *Section 6.6, "Managing Archived Configuration Files"* .

CONTENTS

- Section 6.9.3, "Managing Network Monitoring"

Section 6.9.1
Downloading ROS Debug Information

RUGGEDCOM ROS devices managed by RUGGEDCOM NMS actively report device crashes and alarm conditions that require user intervention. In addition to triggering an event in RUGGEDCOM NMS, a ROS device will also generate a debug log file in non-volatile memory, which is automatically collected by RUGGEDCOM NMS.

Debug log files are stored by RUGGEDCOM NMS with the following naming convention:

```
DebugKit_X.X.X.X_YYYYMMDD-HHMM.tar.gz
```

Where:

- `X.X.X.X` is the IP address for the ROS device
- `YYYYMMDD-HHMM` is the date and time when the log file was downloaded from the ROS device (e.g. 20150202-1112)

When RUGGEDCOM NMS downloads a debug file, it generates a secondary event with the following UEI:

```
uei.opennms.org/ruggedcom/RNMSMiscDownloadSuccess
```

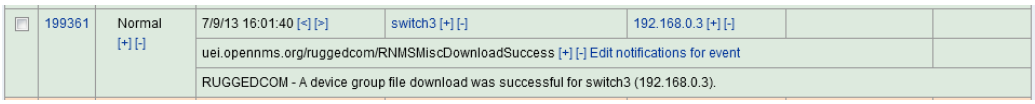


Figure 354: Example RNMSMiscDownloadSuccess Event

For more information about viewing these events, refer to Section 5.2.2.1, "Viewing a List of Events" .

IMPORTANT!
Debug logs should be forwarded to Siemens Customer Support for analysis. The detailed information will allow Siemens to diagnose the cause of the abnormal operation or system fault that triggered the event.

To retrieve a debug log from RUGGEDCOM NMS, do the following:

1. Open a terminal application on the RUGGEDCOM NMS server and run the following script:

   `/root/ruggednms_scripts/get_ros_debugkit.sh`

   The script archives all available ROS debug data under /usr/share/opennms/scripts/ros_debugkit.tar.gz. .
2. Locate the debug log on the server and forward it to RUGGEDCOM NMS Customer Support for troubleshooting.

To retrieve a debug log from RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Archived Configuration File Upload**. The **Configuration Upload** screen appears.

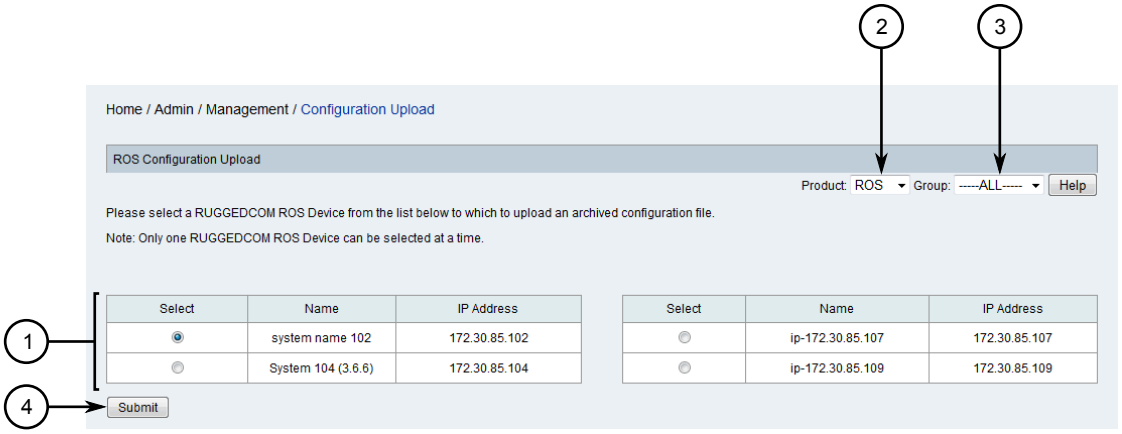


Figure 355: Configuration Upload Screen

1. Available Devices **2.** Product List **3.** Group List **4.** Submit Button

2. Use the **Product** and **Group** lists to filter the list of available devices.
3. Select a device and then click **Submit**. If previously archived configuration files are available for the chosen device, the **Configuration Upload** screen appears.

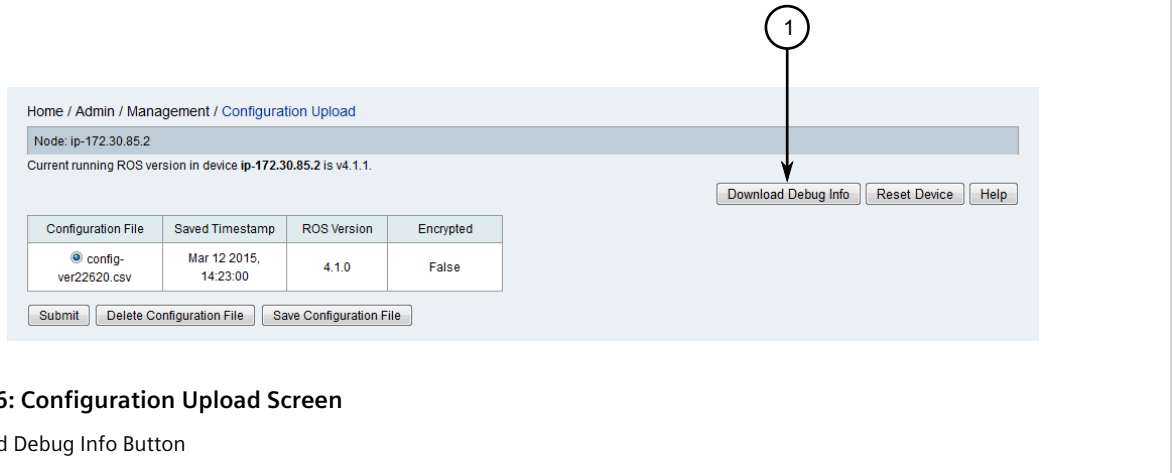


Figure 356: Configuration Upload Screen

1. Download Debug Info Button

4. Click **Download Debug Info**. A confirmation message appears.
5. Click **OK**. A dialog box appears.
6. Select where to save the file locally and then click **OK**.
7. Forward the debug log file to RUGGEDCOM NMS Customer Support for troubleshooting.

Section 6.9.2

Managing Files on ROS Devices

The following file types can be uploaded to a ROS device managed by RUGGEDCOM NMS:

File Type	Description
Configuration Files	Partial configuration files can be uploaded to ROS devices to configure a common facility or attribute.
Binary Files	Upload binary files to change the main firmware (main.bin) or boot loader (boot.bin) on ROS devices.
System File	Upload FPGA files. Only applicable to RUGGEDCOM RS950G devices.

CONTENTS

Section 6.9.2.1

Uploading Files to RUGGEDCOM NMS

To upload a file to RUGGEDCOM NMS that will later be uploaded to ROS devices managed by RUGGEDCOM NMS, do the following:

NOTE

Compressed binary files (.zb), typically provided by Siemens Support for firmware images, can only be added to the RUGGEDCOM NMS server manually. For more information, refer to Section 6.9.2.2, "Adding a Compressed Firmware Image to RUGGEDCOM NMS" .*

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Firmware Upgrade**. The **Firmware Upgrade** screen appears.

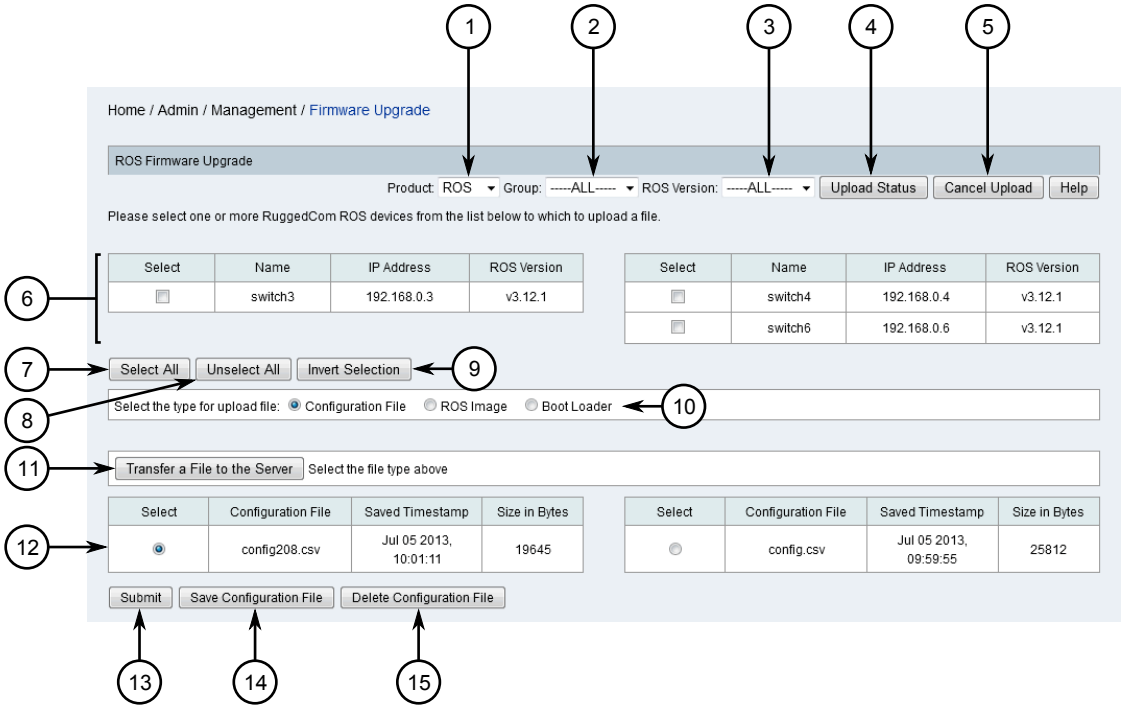


Figure 357: Firmware Upgrade Screen

1. Product List **2.** Group List **3.** ROS Version **4.** Upload Status **5.** Cancel Upload **6.** Available ROS Devices **7.** Select All Button **8.** Unselect All Button **9.** Invert Selection Button **10.** File Type Options **11.** Transfer a File to the Server Button **12.** Available Files **13.** Submit Button **14.** Save Configuration File Button **15.** Delete Configuration File Button

2. Use the **Product**, **Group** and **ROS Version** lists to filter the list of available ROS devices.
3. Select the file type that will be uploaded. A list of files available on the RUGGEDCOM NMS server that match the file type appear. For more information about the available file types, refer to Section 6.9.2, "Managing Files on ROS Devices" .
4. Select a file and then click **Transfer a File to the Server**. A dialog box appears.

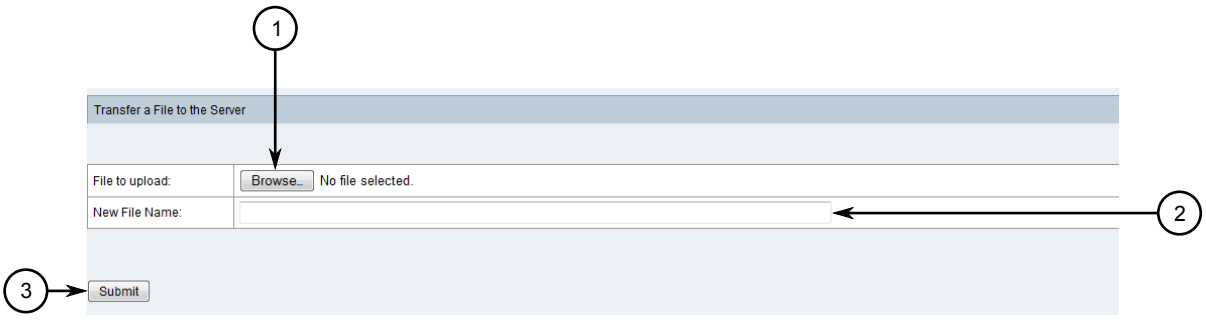


Figure 358: Dialog Box

1. Browse Button **2.** New File Name Box **3.** Submit Button

5. Click **Browse** to navigate to and select the file.

6. For configuration files only, under **New File Name**, type **`config.csv`**.
7. Click **Submit**. The file is uploaded from the local workstation to the RUGGEDCOM NMS server.

Section 6.9.2.2
Adding a Compressed Firmware Image to RUGGEDCOM NMS

Firmware images are sometimes provided by Siemens Customer Support in a compressed file format (*.zb). Such files can not be uploaded to the RUGGEDCOM NMS server via the RUGGEDCOM NMS Web interface, as described in Section 6.9.2.1, "Uploading Files to RUGGEDCOM NMS " . These files must be copied directly to the RUGGEDCOM NMS server manually by the user.

To copy a compressed firmware image to the RUGGEDCOM NMS server, do the following:

1. On the RUGGEDCOM NMS server, copy the compressed firmware image file to `/usr/share/opennms/configMgtd/ROS` .
2. Open a terminal application and open the following file in a text editor:

   `/usr/share/opennms/ruggednms/configMgtd/ROS/ROSVersions.txt`
3. Add the file name to the end of the file.
4. Save and close the file. The compressed firmware image is now available for upload to a ROS device.

Section 6.9.2.3
Uploading Files to ROS Devices

To upload configuration files, binary files or system files to one or more RUGGEDCOM ROS devices managed by RUGGEDCOM NMS, do the following:

CAUTION!
Configuration hazard – risk of data loss. Uploading a new boot loader or system file should be done with extreme caution and only under instructions from an authorized Siemens Customer Support representative. Uploading an improper boot loader could render the device inoperable.

IMPORTANT!
Before uploading a configuration file to multiple devices, it is critical to remove device specific data – parameters that must be unique to every device, such as the IP address and system ID. To reduce the chance of errors and for ease of management, consider removing all sections other than those specific to the configuration changes that need to be applied. Be sure to give these modified files descriptive names and retain them for future use.

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Firmware Upgrade**. The **Firmware Upgrade** screen appears.

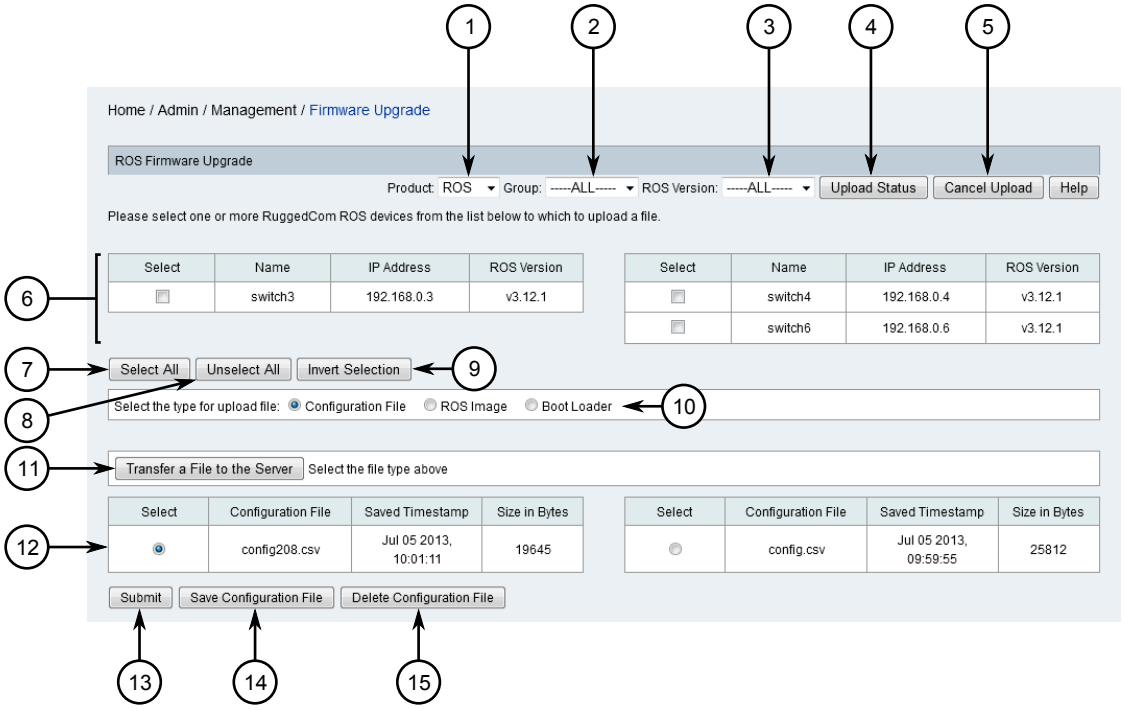


Figure 359: Firmware Upgrade Screen

1. Product List **2.** Group List **3.** ROS Version List **4.** Upgrade Status Button **5.** Cancel Upgrade Button **6.** Available ROS Devices **7.** Select All Button **8.** Unselect All Button **9.** Invert Selection Button **10.** File Type Options **11.** Transfer a File to the Server Button **12.** Available File Types **13.** Submit Button **14.** Save Configuration File Button **15.** Delete Configuration File Button

2. Use the **Product**, **Group** and **ROS Version** lists to filter the list of available ROS devices.
3. Select one or more ROS devices.
4. Select the file type that will be uploaded. A list of files available on the RUGGEDCOM NMS server that match the file type appear. For more information about the available file types, refer to Section 6.9.2, "Managing Files on ROS Devices" .
5. Select a file and then click **Submit**. A confirmation message appears.
6. Click **OK**. The **List** screen appears listing all recent events, including a new event signaling the upload of the selected file to the first target device. As the upload process continues in the background, a new event of the type *RNMSSingleUploadSuccess* is generated for each ROS device that is updated.

   All event information is recorded in the log file. For more information about the viewing the Configuration Management log file, refer to Section 6.1, "Viewing the Configuration Management Log" .

   Another method for tracking the upload process is to return to the **Firmware Upgrade** screen and click **Upload Status**. The **Bulk Upload/Operation Status** dialog box appears indicating the current status.

Figure 360: Bulk Upload/Operation Status Dialog Box

To cancel the upload process, do the following:

1. Return to the **Configuration Upload** screen and click **Cancel Upgrade**. A confirmation message appears.
2. Click **OK**. The upload process is stopped after the current upload has either completed or failed.

Section 6.9.3

Managing Network Monitoring

When network monitoring is enabled, RUGGEDCOM NMS continuously learns the traffic characteristics of all RMON-enabled RUGGEDCOM ROS devices on the network. For those ROS devices that display consistent traffic patterns with little variation, RUGGEDCOM NMS is able to determine a statistical baseline and watch for deviations based on user-configured thresholds. Such deviations indicate a potential change to the network that an administrator should be aware of, such as:

- Generic service attacks
- Faulty devices on the network
- New devices on the network
- Network traffic bursts
- Electromagnetic or other interference affecting a device
- A twisted or improperly connected cable
- Power is removed from a device or a device goes down
- Unstable traffic

Depending on the event, RUGGEDCOM NMS may adjust the baseline over time to account for a natural event, such as a gradual increase in overall network traffic, or trigger a notification. Event notifications are sent to the network administrator and it is the administrator's responsibility to investigate further.

IMPORTANT!
The network must have stable, predictable traffic flows, such as in an industrial setting where the network is used for monitoring processes.

IMPORTANT!
Devices other than RUGGEDCOM ROS devices that do not support SNMP or RMON 2 are automatically excluded (blacklisted) from network monitoring.

IMPORTANT!
Devices with frequently unstable network traffic should be blacklisted from network monitoring to avoid generating a high number of meaningless events and false indications.

CONTENTS

Section 6.9.3.1
Network Monitoring Concepts

The following describes some of the concepts important to the implementation of network monitoring in RUGGEDCOM NMS:

NOTE
For more advanced information about the network monitoring feature, including important use cases, refer to https://support.industry.siemens.com/cs/ww/en/view/109477329 .

Network Monitoring Process

Network monitoring is done in two stages:

- **Stage 1: Baseline Calculation**
  In this stage, RUGGEDCOM NMS configures all RMON-enabled devices under its control and begins analyzing device data and traffic flows. RUGGEDCOM NMS looks specifically at InOctets, InPkts, InBroadcast and InMulticast data to determine thresholds and a statistical baseline.

Data	Description
InOctets	The number of octets in good packets (Unicast+Multicast+Broadcast) and dropped packets received.
InPkts	The number of good packets (Unicast+Multicast+Broadcast) and dropped packets received.
InBroadcasts	The number of broadcast packets received.
InMulticasts	The number of multicast packets received.

  The time allotted for establishing a suitable baseline and thresholds is by default six hours, but this can be changed by the user. For more information about changing the calculation period, Section 6.9.3.4, "Configuring Network Monitoring" .

- **Stage 2: Monitoring**
  After establishing thresholds and a baseline, RUGGEDCOM NMS begins collecting data from each monitored device and compares it to the baseline. If rising or falling thresholds are crossed, RUGGEDCOM NMS generates events and notifications at the end of the polling interval (15 minutes). RUGGEDCOM NMS also continuously calculates and adjusts the baseline (which may continue growing) based on gradual changes in traffic throughput. If the revised baseline crosses a rising or falling threshold a new threshold is set and a baseline change event is generated.

NOTE
RUGGEDCOM NMS distinguishes between gradual and sharp changes in traffic flow using a standard deviation value. The default value is 3 Sigma, but this can be modified by the user. The standard deviation controls how much deviation is acceptable.

NOTE
While events and notifications are not generated until after the polling interval, RUGGEDCOM NMS also works with RMON on each monitored device to detect problems earlier. If RMON detects a

deviation outside the configured thresholds, it will use SNMP to notify RUGGEDCOM NMS, which will trigger an event or notification.

In both stages, RUGGEDCOM NMS also monitors network utilization and errors. If either crosses their threshold values, RUGGEDCOM NMS generates events and notifications.

» Adding a New Device

Each device added to the network is polled by RUGGEDCOM NMS to determine if RMON is configured. This occurs before any data collection takes place. If RUGGEDCOM NMS receives *OID not found*, RMON is not configured on the device. RUGGEDCOM NMS then configures RMON on the device.

Section 6.9.3.2

Monitoring the Network

To view the status of the network, click **Network Monitor** on the toolbar. The **Network Status** screen appears with the **Events** tab displayed by default. This tab displays the total number of outstanding network warnings and errors.

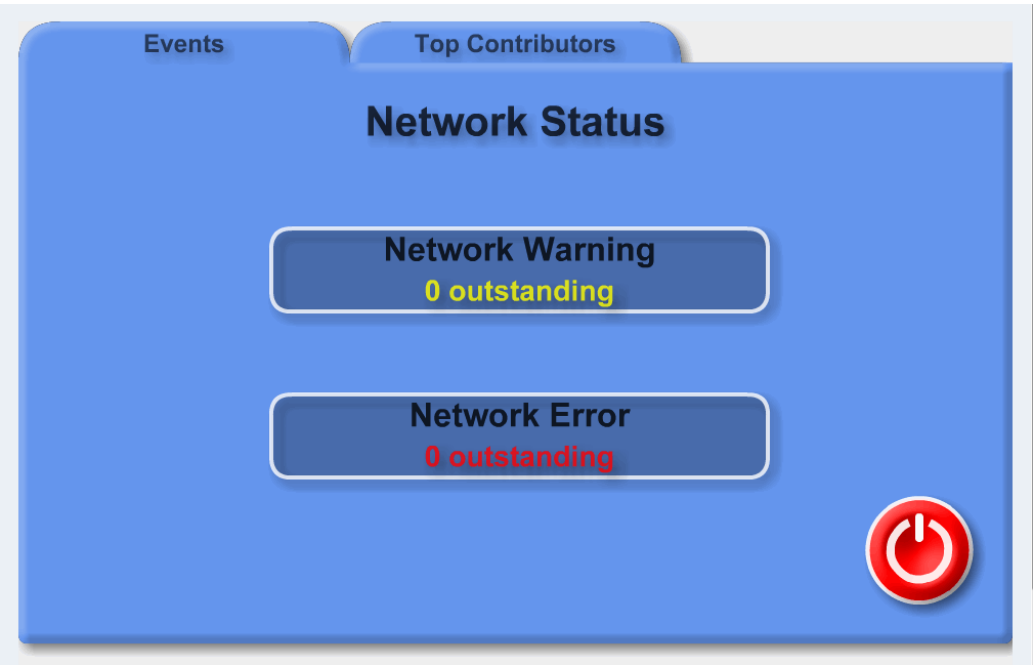


Figure 361: Network Status Screen

Click either **Network Warnings** or **Network Errors** to display the events list. For more information, refer to Section 5.2.2, "Managing Events" .

The status icon also indicates the status of the network monitoring function.

	Network monitoring is enabled.

	Network monitoring is calculating baselines and thresholds.
	Network monitoring is disabled.

Section 6.9.3.3
Enabling, Restarting or Disabling Network Monitoring

To enable/restart or disable network monitoring, do the following:

Enabling or Restarting Network Monitoring

1. On the toolbar, click **Admin**, click **Manage Network Monitor**, and then click **Enable Network Monitor**. The **Enable Network Monitor** screen appears.

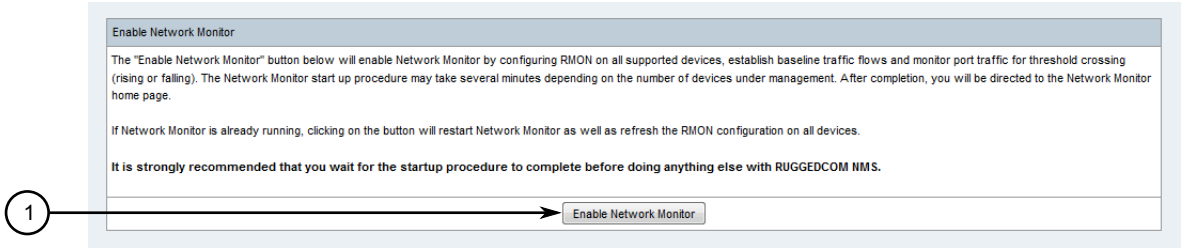


Figure 362: Enable Network Monitor Screen

1. Enable Network Monitor Button

IMPORTANT!
After enabling/restoring network monitoring, avoid making any changes to RUGGEDCOM NMS or the network until the calculation period ends. The calculation period is set by the ***Threshold baseline calculation period*** *parameter, but it also depends on the number of devices on the network. For more information about configuring the calculation period, refer to* *Section 6.9.3.4, "Configuring Network Monitoring"* .

2. Click **Enable Network Monitor**. Once network monitoring is fully initialized, the **Network Monitor** screen appears. For more information about, refer to Section 6.9.3.2, "Monitoring the Network" .

Disabling Network Monitoring

1. On the toolbar, click **Admin**, click **Manage Network Monitor**, and then click **Disable Network Monitor**. The **Disable Network Monitor** screen appears.

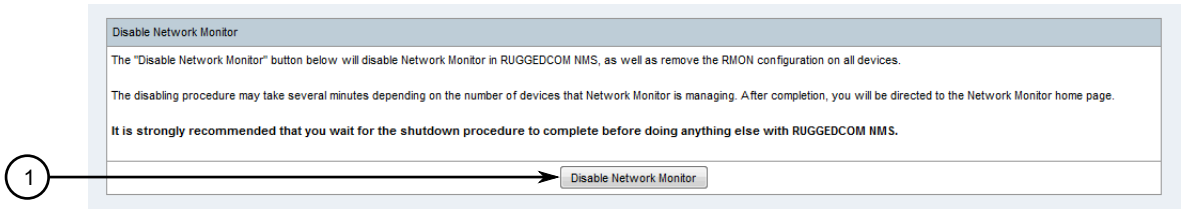


Figure 363: Disable Network Monitor Screen

1. Disable Network Monitor Button

IMPORTANT!
After disabling network monitoring, avoid making any changes to RUGGEDCOM NMS until the shutdown period ends.

2. Click **Disable Network Monitor**. Once network monitoring is disabled, the **Network Monitor** screen appears. For more information about, refer to Section 6.9.3.2, “Monitoring the Network” .

Section 6.9.3.4
Configuring Network Monitoring

To configure network monitoring, do the following:

NOTE
The default settings for network monitoring are recommended for initial setup. These settings can be adjusted later if required.

1. On the toolbar, click **Admin**, click **Manage Network Monitor** and then click **Configure Network Monitor**. The **Configure Network Monitor** screen appears.

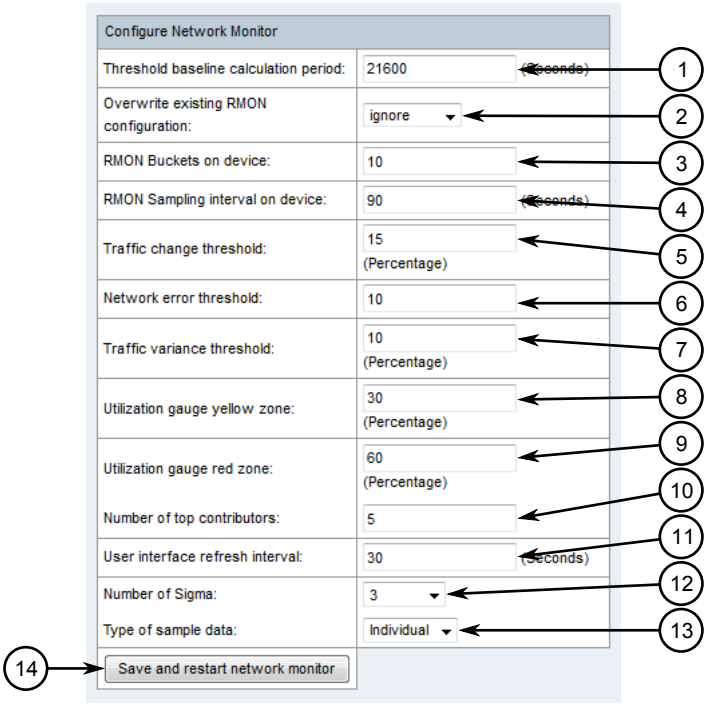


Figure 364: Configure Network Monitor Screen

1. Threshold Baseline Calculation Period Box **2.** Overwrite Existing RMON Configuration List **3.** RMON Buckets on Device Box **4.** RMON Sampling Interval on Device Box **5.** Traffic Change Threshold Box **6.** Network Error Threshold Box **7.** Traffic Variance Threshold Box **8.** Utilization Gauge Yellow Zone Box **9.** Utilization Gauge Red Zone Box **10.** Number of Top Contributors Box **11.** User Interface Refresh Interval Box **12.** Number of Sigma List **13.** Type of Sample Data List **14.** Save and Restart Network Monitor Button

2. Configure the following parameter(s) as required:

Parameter	Description
Threshold baseline calculation period	**Synopsis:** 1 to 2147483647 **Default:** 21600 s The learning period used to calculate statistical baseline and thresholds. A longer learning period will result in a more accurate baseline and thresholds.
Overwrite existing RMON configuration	**Synopsis:** { overwrite, ignore } **Default:** ignore When set to **overwrite**, the network monitor overwrites any existing RMON configuration on each monitored device. Devices that do not have RMON configured are skipped and blacklisted.
RMON Buckets on device	**Synopsis:** 1 to 1000 **Default:** 10 The number of traffic statistic samples to be kept on a device.
RMON Sampling interval on device	**Synopsis:** 1 to 2147483647 **Default:** 90 The interval (in seconds) to sample traffic statistics from a device.
Traffic change threshold	**Synopsis:** 0 to 100

Parameter	Description
	Default: 15 The maximum change in traffic as a percentage of the calculated baseline. A traffic change event is generated if the change crosses this threshold in either direction (rising or falling).
Network error threshold	**Synopsis:** 1 to 2147483647 **Default:** 10 The maximum number of network errors that can be reported by a device. An error event is generated if the number of network errors exceeds this threshold.
Traffic variance threshold	**Synopsis:** 0 to 100 **Default:** 10 The maximum allowed increase in sample traffic measured in percentage. Thresholds are automatically re-based if traffic volume exceeds this percentage.
Utilization gauge yellow zone	**Synopsis:** 0 to 100 **Default:** 30 The threshold (measured as a percentage) at which the background of the network monitor gage on maps turns yellow. If the bandwidth usage is less than this value, the background is green.
Utilization gauge red zone	**Synopsis:** 0 to 100 **Default:** 60 The threshold (measured as a percentage) at which the background of the network monitor gage on maps turns red. If the bandwidth usage is less than this value, the background is yellow or green.
Number of top contributors	**Synopsis:** 1 to 10 **Default:** 5 The number of top traffic contributors shown on the **Top Contributors** screen. For more information, refer to Section 6.9.3.8, "Viewing a List of Top Contributors" .
User interface refresh interval	**Synopsis:** 1 to 2147483647 **Default:** 30 The interval (in seconds) at which charts and gages are refreshed from the RUGGEDCOM NMS server.
Number of Sigma	**Synopsis:** { Disable, 1, 2, 3, 4, 5, 6 } **Default:** 3 The distribution limit for calculating the standard deviation (Sigma). The value of this parameter is used to determine how much deviation (rising or falling) in traffic flow is acceptable. If 3 Sigma (3 × Sigma) is within the configured threshold, the traffic is considered stable and under control. If 3 sigma, however, is outside the threshold, RUGGEDCOM NMS blacklists all history statistics, generates a warning event, and stops monitoring until network monitoring is restarted. Select `Disable` to prevent history statistics from being blacklisted.
Type of sample data	**Synopsis:** { Individual, Average } **Default:** Individual Determines if individual or average data points can be used when calculating the standard deviation (Sigma).

3. Click **Save and restart network monitor**.

Section 6.9.3.5
Enabling or Disabling Monitoring for Specific Ports

To enable or disable network monitoring on a specific port, do the following:

1. On the toolbar, click **Admin**, click **Manage Network Monitor**, and then click **Disable/Enable Monitoring on a Port**. The **Disable/Enable Port Monitoring - Device List** form appears.

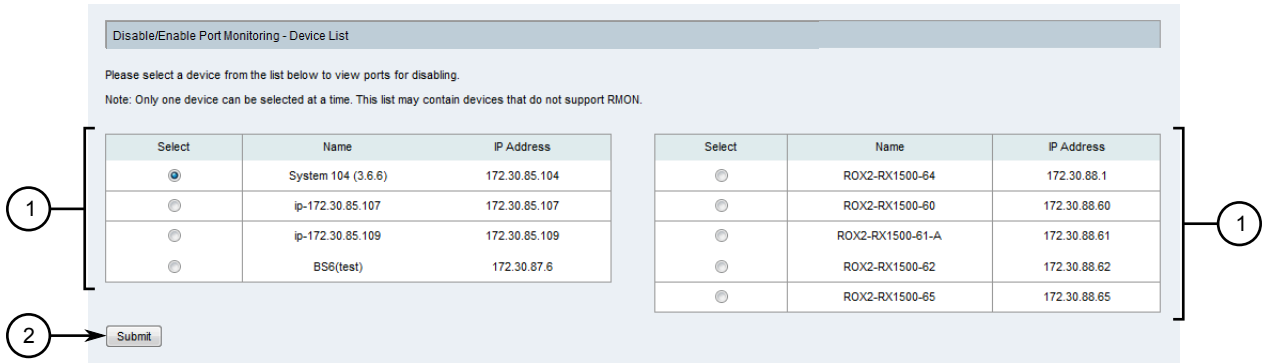


Figure 365: Disable/Enable Port Monitoring - Device List Form

1. Device Options **2.** Submit Button

2. Select the associated device from the list and then click **Submit**. The **Disable/Enable Port Monitoring - Ports List** form appears.

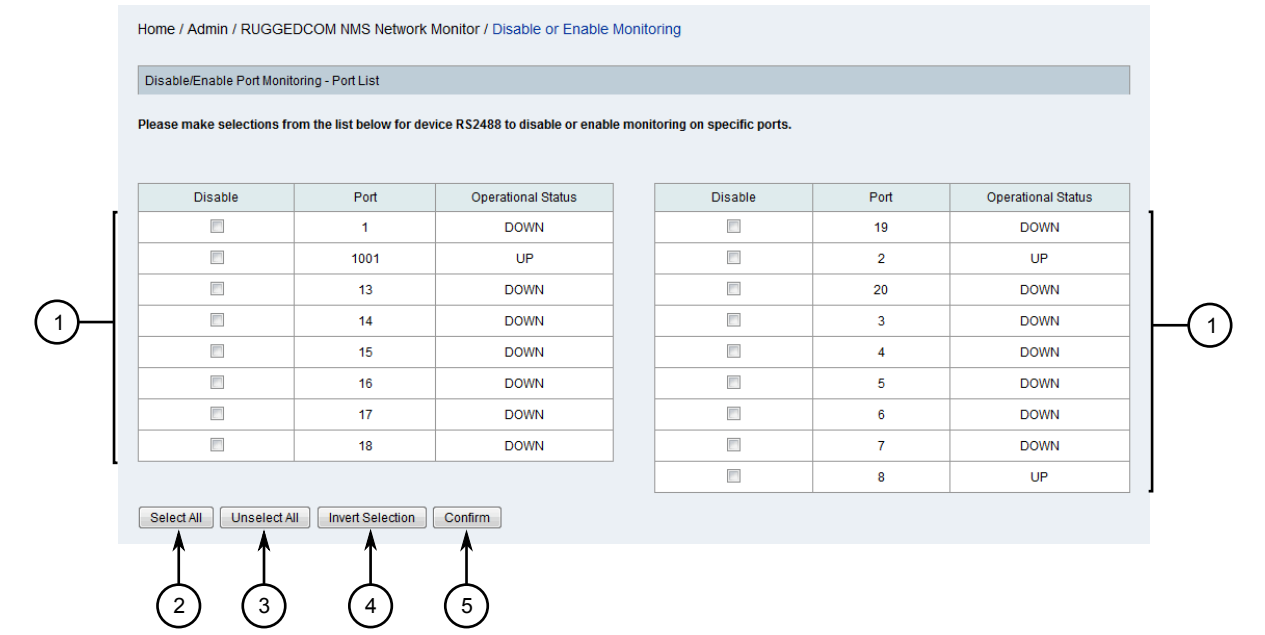


Figure 366: Disable/Enable Port Monitoring - Ports List Form

1. Port Check Boxes **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Confirm Button

3. Either individually or using the **Select All**, **Unselect All** or **Invert Selection** buttons, select or clear one or more ports. Selected ports will be blacklisted (excluded) from network monitoring, and unselected ports will be monitored.
4. Click **Confirm**. Monitoring is disabled only for all selected ports.

Section 6.9.3.6

Enabling or Disabling Monitoring for Specific Devices

To enable or disable network monitoring on a specific devices, do the following:

1. On the toolbar, click **Admin**, click **Manage Network Monitor**, and then click **Disable/Enable Monitoring on a Device**. The **Disable/Enable Device Monitoring - Device List** form appears.

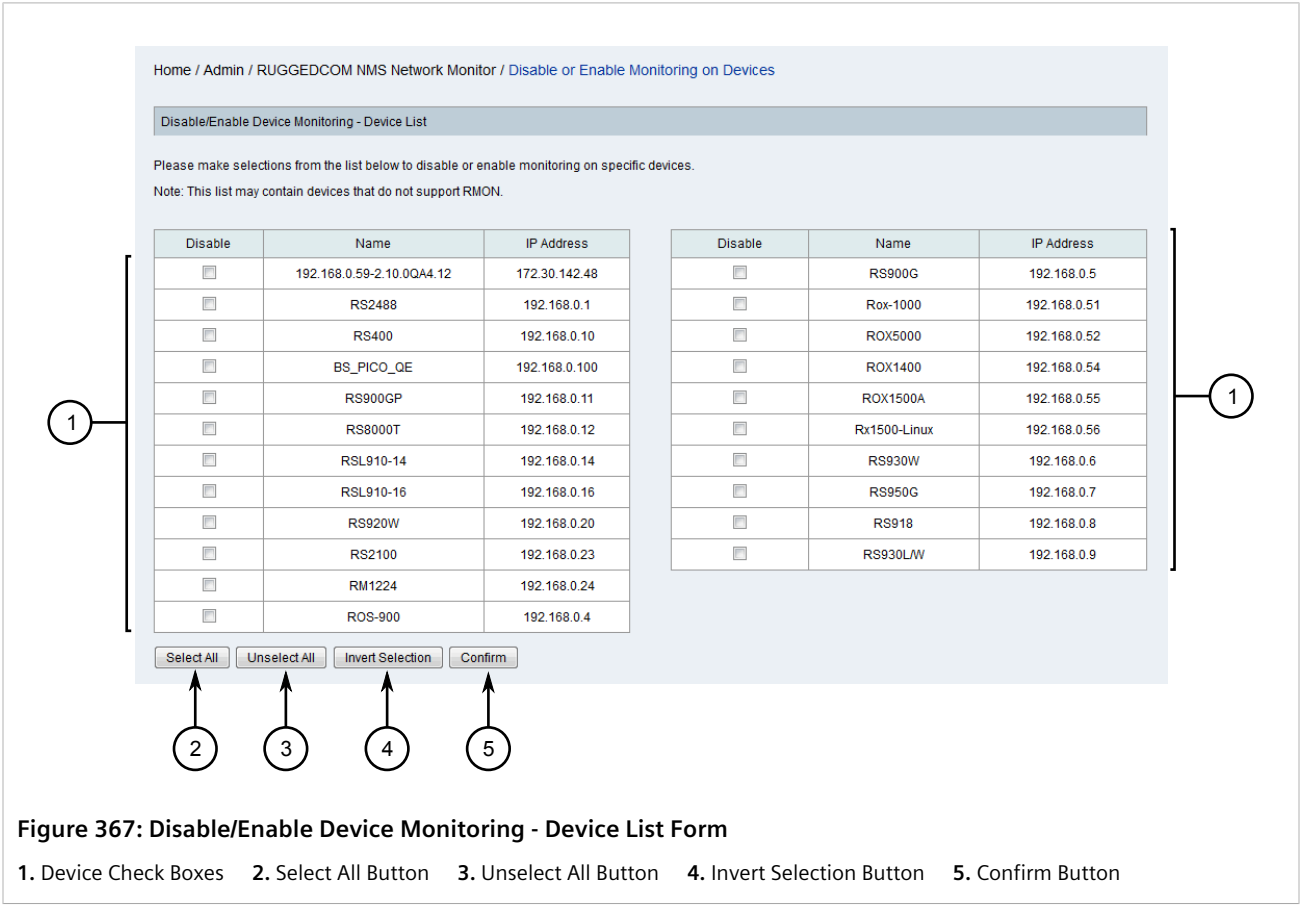


Figure 367: Disable/Enable Device Monitoring - Device List Form

1. Device Check Boxes **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Confirm Button

2. Either individually or using the **Select All**, **Unselect All** or **Invert Selection** buttons, select or clear one or more devices. Selected devices will be blacklisted (excluded) from network monitoring, and unselected devices will be monitored.
3. Click **Confirm**. Monitoring is enabled only for all selected devices.

Section 6.9.3.7
Viewing a List of Blacklisted Ports and Devices

To view a list of ports and devices that are blacklisted (excluded) from network monitoring, click **Admin** on the toolbar, click **Manage Network Monitor**, and then click **Show Devices and Ports in Blacklist** . The **Show Black List - Device List** form appears.

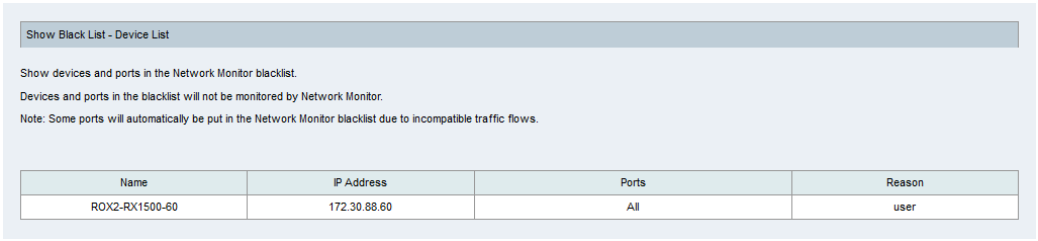


Figure 368: Show Black List - Device List Form

The table lists the devices and/or associated ports that have been blacklisted.

Column	Description
Name	The name of the device.
IP Address	The device's IP address.
Port	The ports that have been blacklisted. If all ports have been blacklisted, the device itself has been blacklisted.
Reason	The reason the device or ports have been blacklisted. This can either be by user choice or the device/port consistently exceeded the thresholds.

To restore network monitoring for a device/port, either enable network monitoring for the device/port (if it was previously disabled by a user) or stabilize the traffic flow through the device/port. For more information about enabling network monitoring for a device/port, refer to either Section 6.9.3.6, “Enabling or Disabling Monitoring for Specific Devices” or Section 6.9.3.5, “Enabling or Disabling Monitoring for Specific Ports” .

Section 6.9.3.8
Viewing a List of Top Contributors

To view a list of the top *contributors* for bandwidth use, number of InOctets received, number of InPkts received, number of InBroadcasts received, or number of InMulticasts received, do the following:

1. On the toolbar, click **Network Monitor** and then click the **Top Contributors** tab. The **Top Contributors** tab appears.

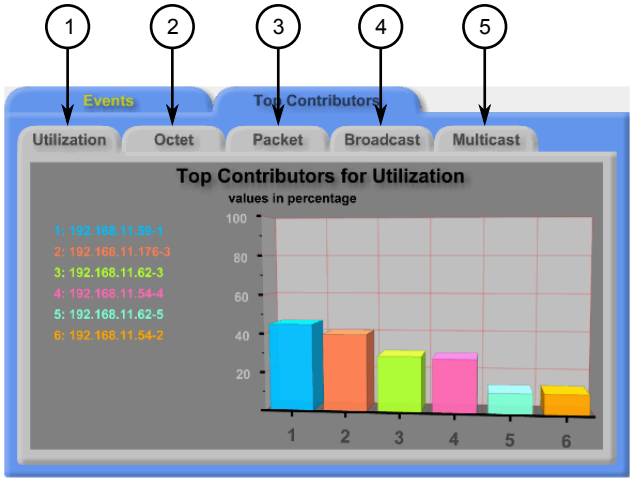


Figure 369: Network Status Screen

1. Utilization Tab **2.** InOctets Tab **3.** InPkts Tab **4.** InBroadcasts Tab **5.** InMulticasts Tab

2. Select one of the available tabs to view the devices/ports that rank highest in each category. By default, the top five contributors are listed, but this can increased/decreased as required. For information about changing the number of contributors listed, refer to Section 6.9.3.4, "Configuring Network Monitoring" .

Section 6.10

Managing ROX Devices

This section describes how to manage RUGGEDCOM ROX devices managed by RUGGEDCOM NMS.

NOTE
For information about how to download, upload, compare, save and delete configuration files for RUGGEDCOM ROX devices, refer to *Section 6.6, "Managing Archived Configuration Files"* .

CONTENTS

Section 6.10.1

Enabling/Disabling the Apache Web Server

RUGGEDCOM NMS uses the Apache Web server to issue updates to ROX-based devices. It is enabled by default.

To disable or re-enable the Apache Web server, do the following:

1. Log on to the RUGGEDCOM NMS server.
2. At the prompt, type the **su** and then press **Enter**.
3. Type the root password and then press **Enter**.
4. Enable or disable the service by typing:

   Disabling

   ```
   update-rc.d -f apache2 remove
   /etc/init.d/apache2 stop
   ```

   Enabling

   ```
   update-rc.d -f apache2 defaults
   /etc/init.d/apache2 start
   ```

Section 6.10.2

Downloading ROX Debug Information

Important information about a recent device crash or an existing alarm condition that requires user intervention can be downloaded from a RUGGEDCOM ROX device in the form of a debug log.

IMPORTANT!
Debug logs should be forwarded to Siemens Customer Support for analysis. The detailed information will allow Siemens to diagnose the cause of the abnormal operation or system fault that triggered the event.

To retrieve a debug log from RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Archived Configuration File Upload**. The **Configuration Upload** screen appears.

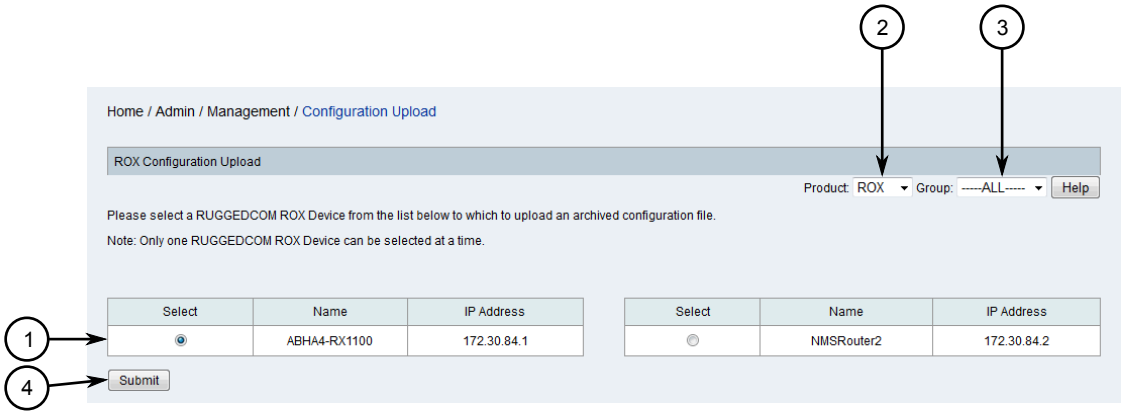


Figure 370: Configuration Upload Screen

1. Available Devices **2.** Product List **3.** Group List **4.** Submit Button

2. Use the **Product** and **Group** lists to filter the list of available devices.
3. Select a device and then click **Submit**. If previously archived configuration files are available for the chosen device, the **Configuration Upload** screen appears.

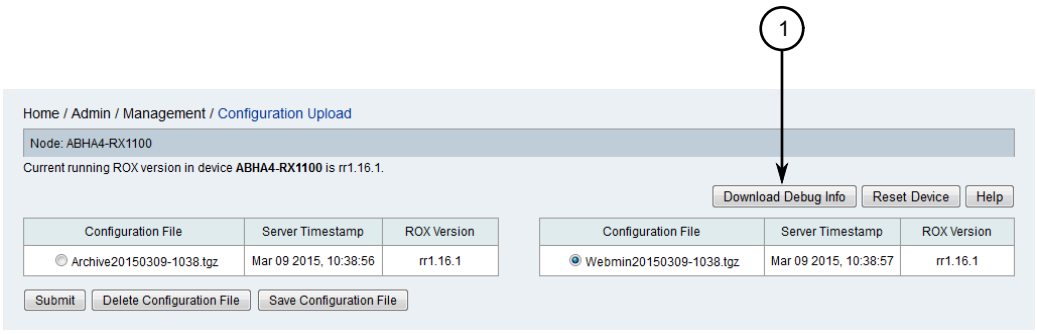


Figure 371: Configuration Upload Screen

1. Download Debug Info Button

4. Click **Download Debug Info**. A confirmation message appears.
5. Click **OK**. A dialog box appears.
6. Select where to save the file locally and then click **OK**.
7. Forward the debug log file to RUGGEDCOM NMS Customer Support for troubleshooting.

Section 6.10.3

Managing the Configuration of ROX Devices

RUGGEDCOM NMS makes updating multiple RUGGEDCOM NMS ROX devices simple and easy by using partial configuration files. Partial configuration files are generic and safe to apply to multiple routers, as they do not contain any unique identifying information, such as IP addresses.

Partial configuration files can be retrieved, archived, uploaded and applied to any ROX device.

A typical work flow for applying a partial configuration file is as follows:

1. Download a local copy of a partial configuration file from a ROX device.
2. [Optional] Extract the configuration file, modify it locally, and then compress it again as a tarball (*.tgz).
3. Upload the file to the RUGGEDCOM NMS server.
4. Upload the file to one or more ROX devices.

Alternatively, if a ROX device already has an ideal configuration, a partial configuration file can be downloaded from it and applied directly to other ROX devices managed by RUGGEDCOM NMS.

CONTENTS

- Section 6.10.3.6, “Applying a Partial Configuration File Directly to Other ROX Devices”

Section 6.10.3.1
Downloading a Partial Configuration File

To download a partial configuration file from a RUGGEDCOM ROX device, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX Management**, and then click **ROX Partial Configuration Download**. The **Configuration Download** screen appears.

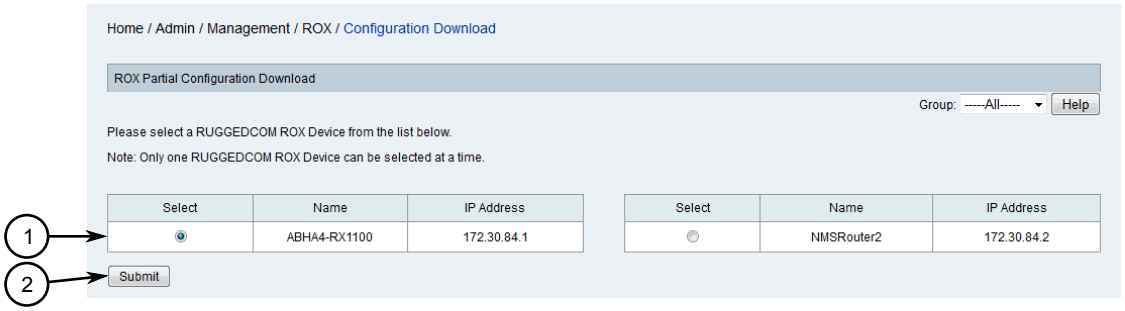


Figure 372: Configuration Download Screen

1. Available ROX Devices **2.** Submit Button

2. Select a device and then click **Submit**. The **Subsystem List** screen appears.

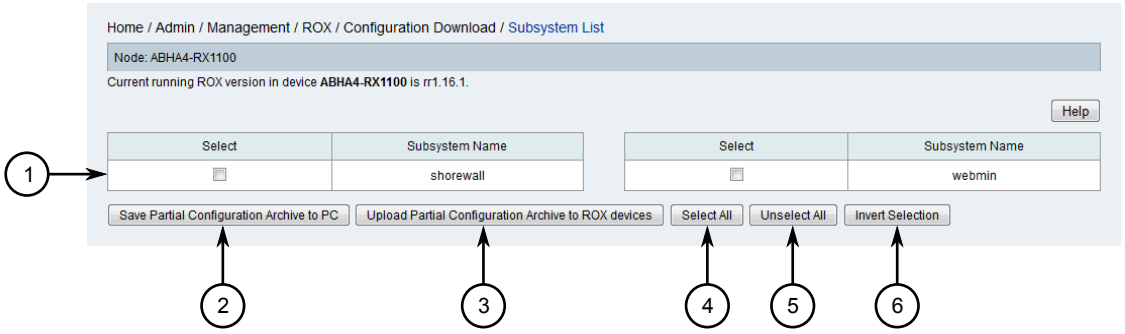


Figure 373: Configuration Download Screen

1. Available Sub-Systems **2.** Save Partial Configuration Archive to PC Button **3.** Upload Partial Configuration Archive to ROX Devices Button **4.** Select All Button **5.** Unselect All Button **6.** Invert Selection Button

3. Select one or more subsystems to generate the partial configuration from, and then click **Save Partial Configuration Archive to PC**. A confirmation dialog box appears.
4. Click **OK**. The file is compressed and saved with the filename `ArchivePart.tgz`.

Section 6.10.3.2
Uploading a Partial Configuration File to ROX Devices

To upload a partial configuration file from RUGGEDCOM NMS to one or more ROX devices, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX Management**, and then click **Bulk ROX Partial Configuration Upload**. The **Configuration Upload** screen appears.

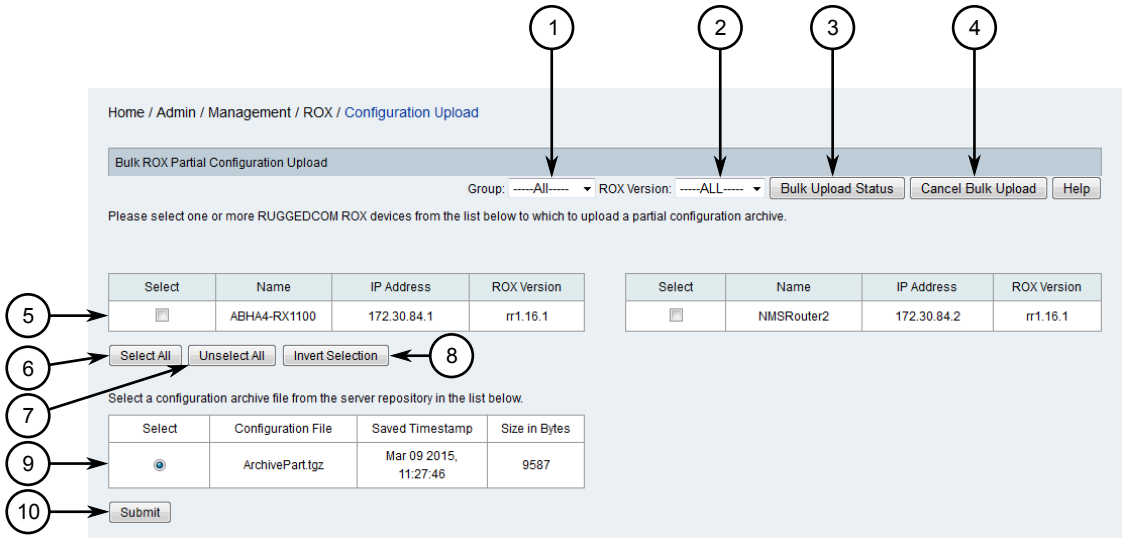


Figure 374: Configuration Upload Screen

1. Group List **2.** ROX Version List **3.** Bulk Upload Status Button **4.** Cancel Bulk Upload Button **5.** Available ROX Devices **6.** Select All Button **7.** Unselect All Button **8.** Invert Selection Button **9.** Available Partial Configuration Files **10.** Submit Button

2. Use the **Group** and **ROX Version** lists to filter the list of ROX available devices.
3. Select one or more devices to receive the partial configuration file.
4. Select a partial configuration file and then click **Submit**. The **List** screen appears listing all recent events, including a new event signaling the upload of the partial configuration file to the first target device. As the upload process continues in the background, a new event of the type *RNMSSingleUploadSuccess* is generated for each ROX device that is updated.

   All event information is recorded in the log file. For more information about the viewing the Configuration Management log file, refer to Section 6.1, "Viewing the Configuration Management Log" .

   Another method for tracking the upload process is to return to the **Configuration Upload** screen and click **Bulk Upload Status**. The **Bulk Upload/Operation Status** dialog box appears indicating the current status.

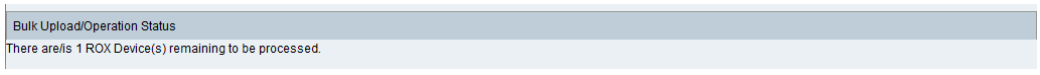


Figure 375: Bulk Upload/Operation Status Dialog Box

To cancel the upload process, do the following:

- Return to the **Configuration Upload** screen and click **Cancel Bulk Upload**. The **List** screen appears listing all recent events and, once the current upload is completed, a new event is generated indicating the process has been canceled.

Section 6.10.3.3

Uploading Partial Configuration Files to RUGGEDCOM NMS

Partial configuration files taken from a RUGGEDCOM ROX device must be uploaded to the RUGGEDCOM NMS server before they can be applied to other ROX devices.

To upload a partial configuration file to RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX Management**, and then click **ROX Generic Configuration Archive Management**. The **File Management** screen appears.

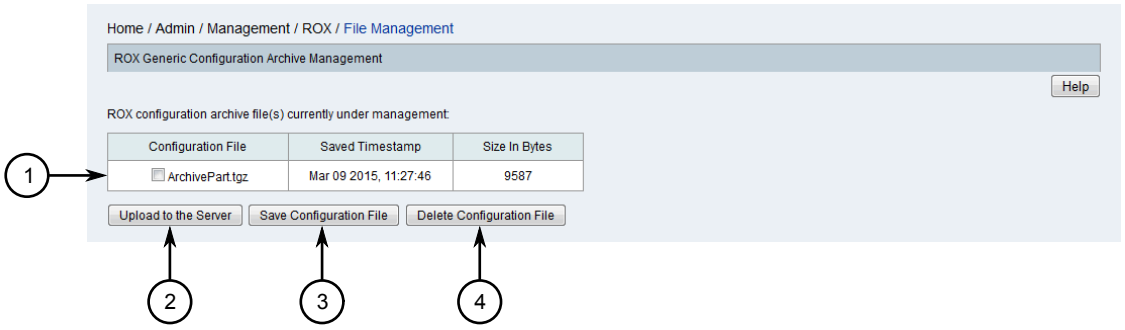


Figure 376: File Management Screen

1. Available Partial Configuration Files **2.** Upload to the Server Button **3.** Save Configuration File Button **4.** Delete Configuration File Button

2. Click **Upload to the Server**. The **Transfer a File to the Server** dialog box appears.

Figure 377: Transfer a File to the Server Dialog Box

1. Browse Button **2.** New File Name Box **3.** Submit Button

3. Click **Browser** and select the partial configuration file to upload.
4. Under **New File Name**, type the full name of the file as it should appear on the RUGGEDCOM NMS server, including the *.tgz extension. The file name can be entirely new or the same as the current file name.

5. Click **Submit**. A confirmation message appears.
6. Click **Continue**. The dialog box closes.
7. Refresh the **File Management** screen. The new partial configuration file appears.

Section 6.10.3.4
Save a Partial Configuration File from RUGGEDCOM NMS

To save a partial configuration file stored on the RUGGEDCOM NMS server, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX Management**, and then click **ROX Generic Configuration Archive Management**. The **File Management** screen appears.

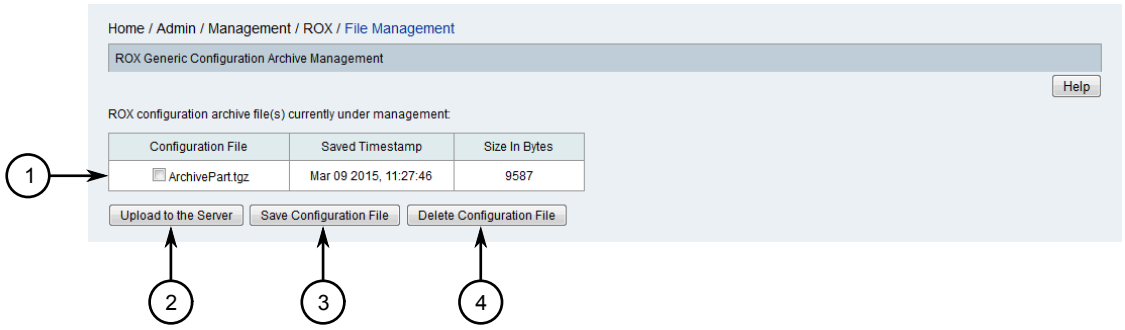


Figure 378: File Management Screen

1. Available Partial Configuration Files **2.** Upload to the Server Button **3.** Save Configuration File Button **4.** Delete Configuration File Button

2. Select a partial configuration file and then click **Save Configuration File**. A confirmation dialog box appears.
3. Click **OK**. The file is saved locally.

Section 6.10.3.5
Deleting a Partial Configuration File from RUGGEDCOM NMS

To delete a partial configuration file stored on the RUGGEDCOM NMS server, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX Management**, and then click **ROX Generic Configuration Archive Management**. The **File Management** screen appears.

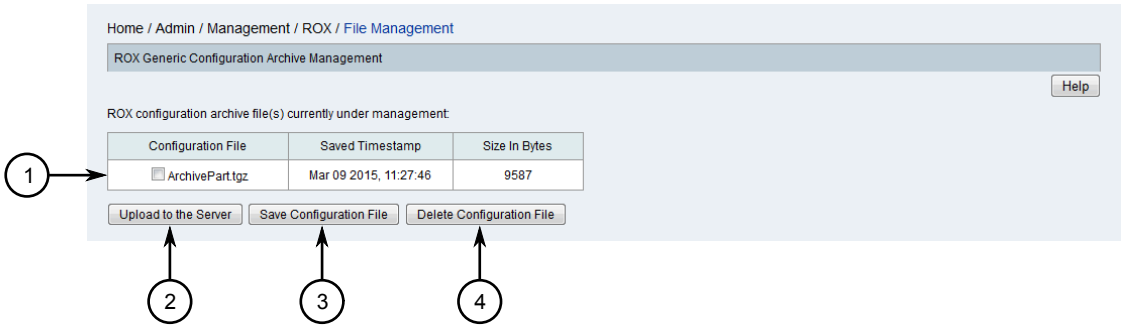


Figure 379: File Management Screen

1. Available Partial Configuration Files **2.** Upload to the Server Button **3.** Save Configuration File Button **4.** Delete Configuration File Button

2. Select a partial configuration file and then click **Delete Configuration File**. A confirmation dialog box appears.
3. Click **OK**. The file is deleted.

Section 6.10.3.6

Applying a Partial Configuration File Directly to Other ROX Devices

To download a partial configuration file from a RUGGEDCOM ROX device and apply it directly to other ROX devices without uploading it to the RUGGEDCOM NMS server, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX Management**, and then click **ROX Partial Configuration Management**. The **Configuration Download** screen appears.

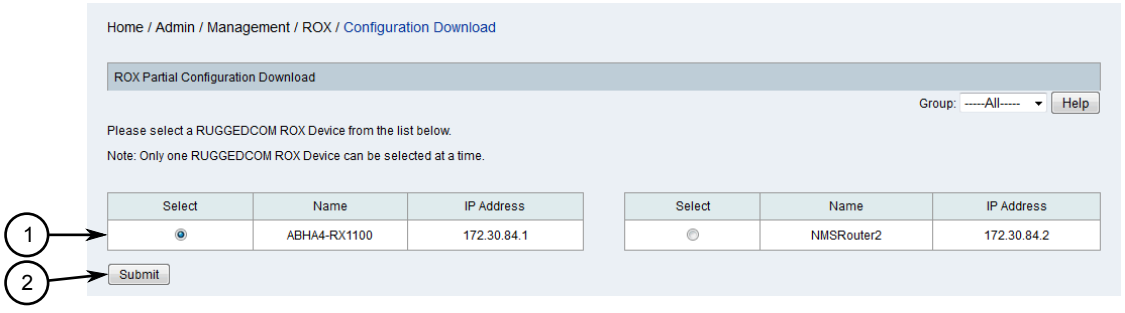


Figure 380: Configuration Download Screen

1. Available ROX Devices **2.** Submit Button

2. Select a device and then click **Submit**. The **Subsystem List** screen appears.

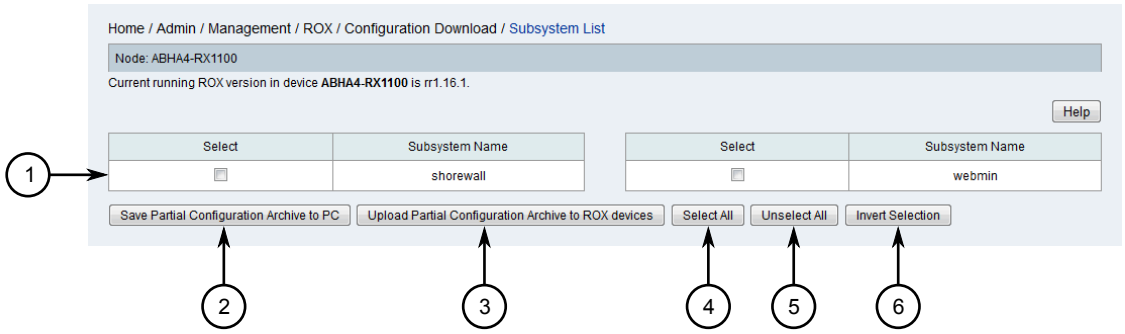


Figure 381: Configuration Download Screen

1. Available Sub-Systems **2.** Save Partial Configuration Archive to PC Button **3.** Upload Partial Configuration Archive to ROX Devices Button **4.** Select All Button **5.** Unselect All Button **6.** Invert Selection Button

3. Select one or more subsystems to generate the partial configuration from, and then click **Upload Partial Configuration Archive to ROX Devices**. A confirmation dialog box appears.
4. Click **OK**. The **Configuration Upload** screen appears.

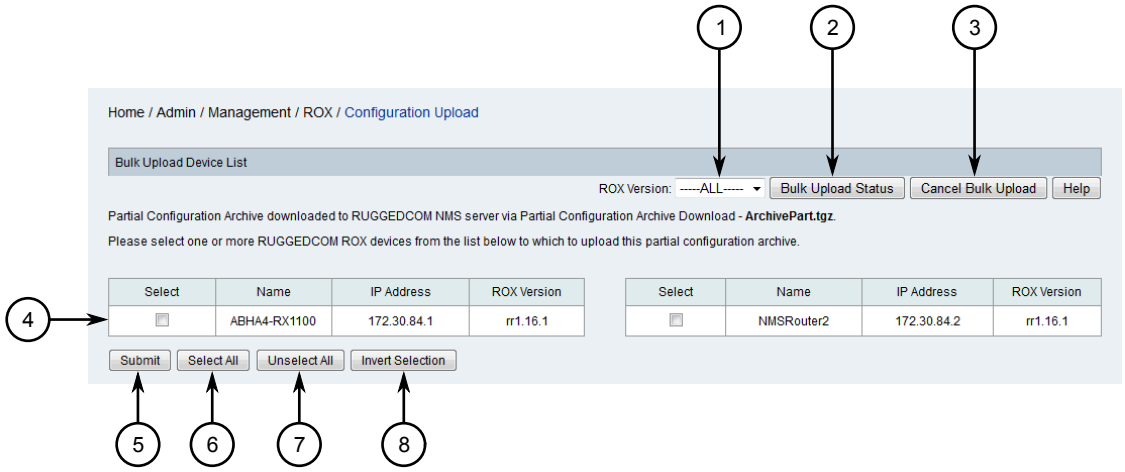


Figure 382: Configuration Upload Screen

1. ROX Version List **2.** Bulk Upload Status Button **3.** Cancel Bulk Upload Button **4.** Available ROX Devices **5.** Submit Button **6.** Select All Button **7.** Unselect All Button **8.** Invert Selection Button

5. Select one or more devices, and then click **Submit**. The **List** screen appears listing all recent events, including a new event signaling the upload of the partial configuration file to the first target device. As the upload process continues in the background, a new event of the type *RNMSSingleUploadSuccess* is generated for each ROX device that is updated.

   All event information is recorded in the log file. For more information about the viewing the Configuration Management log file, refer to Section 6.1, "Viewing the Configuration Management Log" .

   Another method for tracking the upload process is to return to the **Configuration Upload** screen and click **Bulk Upload Status**. The **Bulk Upload/Operation Status** dialog box appears indicating the current status.

Figure 383: Bulk Upload/Operation Status Dialog Box

To cancel the upload process, do the following:

- Return to the **Configuration Upload** screen and click **Cancel Bulk Upload**. The **List** screen appears listing all recent events and, once the current upload is completed, a new event is generated indicating the process has been canceled.

Section 6.10.4

Managing Firmware on ROX Devices

This section describes how to manage the firmware on RUGGEDCOM ROX devices managed by RUGGEDCOM NMS.

CONTENTS

Section 6.10.4.1

Adding a ROX Firmware Image to RUGGEDCOM NMS

Firmware images for RUGGEDCOM ROX devices must be copied directly to the RUGGEDCOM NMS server manually by the user.

To copy a RUGGEDCOM ROX firmware image to the RUGGEDCOM NMS server, do the following:

- On the RUGGEDCOM NMS server, copy the firmware image file to `/usr/share/opennms/ruggedcom/debian386/rr1/dists/rr1.`*`{version}`* , where *{version}* is the firmware version (e.g. rr1.16.0). If a folder matching the firmware version does not exist, create one.

Once a firmware image has been added, it will be appear in the RUGGEDCOM NMS Web interface during the upload process. For more information about uploading a firmware image to a ROX device, refer to Section 6.10.4.2, "Uploading Firmware Images to ROX Devices" .

Section 6.10.4.2

Uploading Firmware Images to ROX Devices

To upload a firmware image file to one or more RUGGEDCOM ROX devices managed by RUGGEDCOM NMS, do the following:

1. Make sure the IP address for the RUGGEDCOM NMS server is set in the configuration management daemon for the *`rox-srs-url`* parameter. For more information, refer to Section 4.6, "Configuring the Management Daemon" .
2. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Firmware Upgrade**. The **Firmware Upgrade** screen appears.

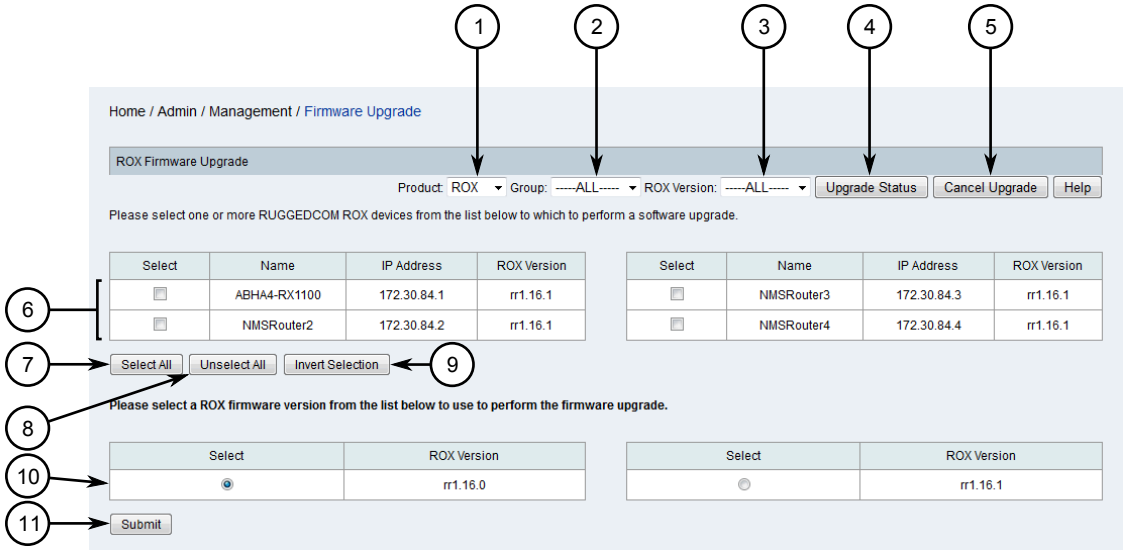


Figure 384: Firmware Upgrade Screen

1. Product List **2.** Group List **3.** ROX Version List **4.** Upgrade Status Button **5.** Cancel Upgrade Button **6.** Available ROX Devices **7.** Select All Button **8.** Unselect All Button **9.** Invert Selection Button **10.** Available Firmware Images **11.** Submit Button

3. Use the **Product** and **Group** lists to filter the list of ROX available devices.
4. Select one or more devices.

> **NOTE**
> *If the required firmware image is not listed, it must be added to the RUGGEDCOM NMS server. For more information, refer to* *Section 6.10.4.1, "Adding a ROX Firmware Image to RUGGEDCOM NMS"*.

5. Select a firmware image and then click **Submit**. A confirmation message appears.
6. Click **OK**. The **List** screen appears listing all recent events, including a new event signaling the upload of the firmware image to the first target device. As the upload process continues in the background, a new event of the type *RNMSSingleUploadSuccess* is generated for each ROX device that is updated.

   All event information is recorded in the log file. For more information about the viewing the Configuration Management log file, refer to Section 6.1, "Viewing the Configuration Management Log".

   Another method for tracking the upload process is to return to the **Firmware Upgrade** screen and click **Upload Status**. The **Bulk Upload/Operation Status** dialog box appears indicating the current status.

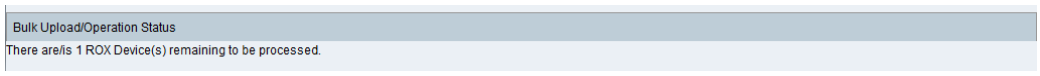


Figure 385: Bulk Upload/Operation Status Dialog Box

To cancel the upload process, do the following:

1. Return to the **Configuration Upload** screen and click **Cancel Upgrade**. A confirmation message appears.
2. Click **OK**. The upload process is stopped after the current upload has either completed or failed.

Section 6.11
Managing ROX II Devices

This section describes how to manage RUGGEDCOM ROX II devices managed by RUGGEDCOM NMS:

NOTE
For information about how to download, upload, compare, save and delete configuration files for RUGGEDCOM ROX II devices, refer to *Section 6.6, "Managing Archived Configuration Files"* .

CONTENTS

Section 6.11.1
Installing Feature Keys

To install one or more feature keys on a ROX II device managed by RUGGEDCOM NMS, do the following:

1. Add the feature key to the RUGGEDCOM NMS server under `/usr/share/opennms/ruggednms/featurekeys/{ip-address}` , where *{ip-address}* is the IP address for the device that uses the feature key. If a folder for the device/IP address is not available, create it.
2. Make sure the IP address for the RUGGEDCOM NMS server is set in the configuration management daemon for the ROX II feature key as follows:

   ```
   rox2-feature-keys-url= "http://{ip-address}/featurekeys"
   ```

   where *{ip-address}* is the IP address of the RUGGEDCOM NMS server.

   For more information, refer to Section 4.6, "Configuring the Management Daemon"

   .
3. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Feature Key Management**. The **Feature Key** screen appears.

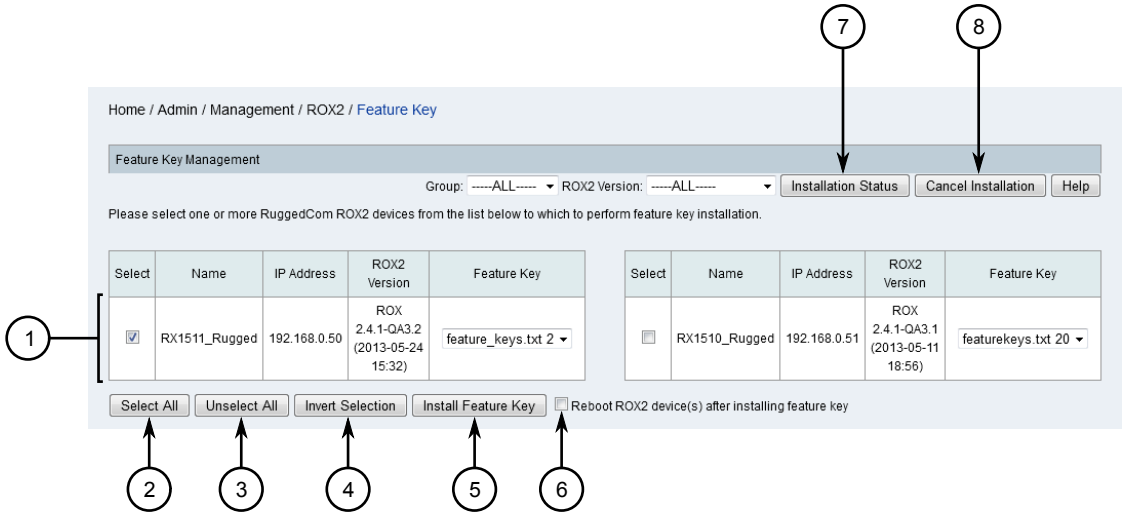


Figure 386: Feature Key Screen

1. Available Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection **5.** Install Feature Key Button **6.** Reboot ROX2 Device(s) After Installing Feature Key Check Box **7.** Installation Status Button **8.** Cancel Installation Button

NOTE
*The **Feature Key** column indicates which devices have feature keys installed.*

4. Select one or more devices and then choose which feature key to install.
5. [Optional] Select **Reboot ROX2 Device(s) After Installing Feature Key** to have each device reboot after the feature key has been installed.
6. Click **Install Feature Key**. A confirmation message appears.
7. Click **OK** to install the feature key(s). If multiple devices are selected, each device is updated sequentially.
8. Click **Installation Status** to view the current status of the installation process. Otherwise, details are recorded in the configuration management log file. For more information about viewing the configuration management log file, refer to Section 6.1, "Viewing the Configuration Management Log" .

Section 6.11.2
Downloading ROX II Debug Information

Important information about a recent device crash or an existing alarm condition that requires user intervention can be downloaded from a RUGGEDCOM ROX II device in the form of a debug log.

IMPORTANT!
Debug logs should be forwarded to Siemens Customer Support for analysis. The detailed information will allow Siemens to diagnose the cause of the abnormal operation or system fault that triggered the event.

To retrieve a debug log from RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Archived Configuration File Upload**. The **Configuration Upload** screen appears.

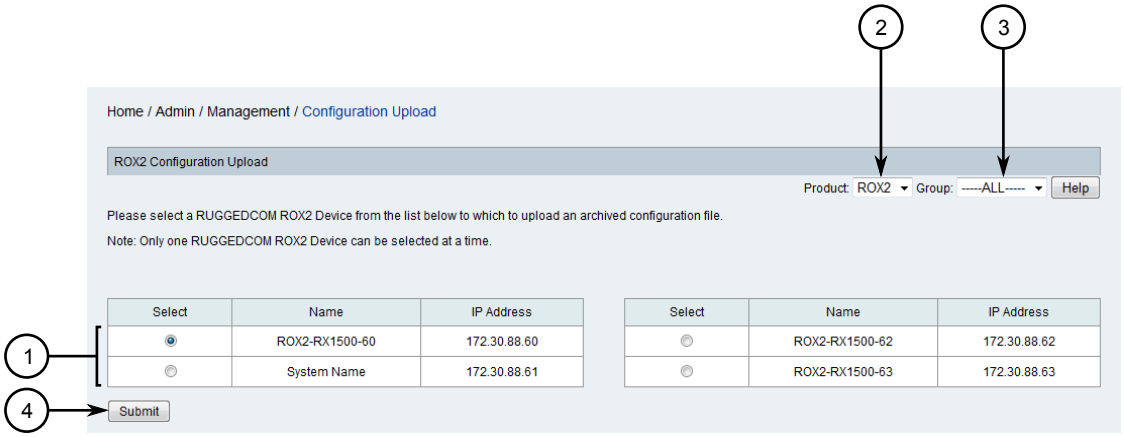


Figure 387: Configuration Upload Screen

1. Available Devices **2.** Product List **3.** Group List **4.** Submit Button

2. Use the **Product** and **Group** lists to filter the list of available devices.
3. Select a device and then click **Submit**. If previously archived configuration files are available for the chosen device, the **Configuration Upload** screen appears.

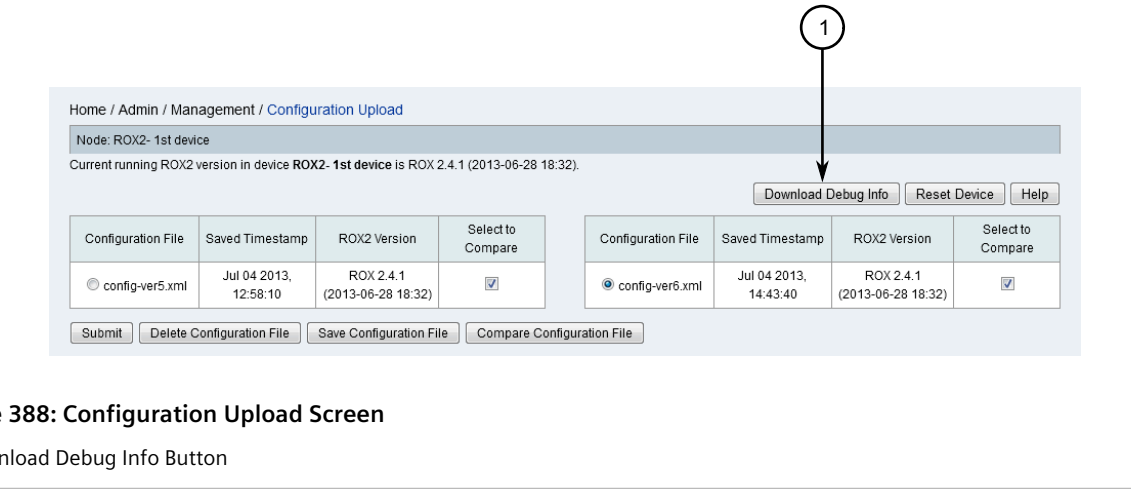


Figure 388: Configuration Upload Screen

1. Download Debug Info Button

4. Click **Download Debug Info**. A confirmation message appears.
5. Click **OK**. The **List** screen appears listing a new event that has been generated to mark the request for debug information from the device.
6. Monitor the header area for status messages. A status message will appear indicating whether or not the download was successful. If the download was not successful, contact the network administrator. Otherwise, proceed to the next step.
7. Log on to the RUGGEDCOM NMS server and locate the debug log (saved as a compressed *.zip file) under:

   `/usr/share/opennms/ruggednms/configMgtd/logs/ruggedComROX2Debug/{ip-address}/`

Where:

- *{ip-address}* is the IP address of the ROX II device.

8. Forward the debug log file to RUGGEDCOM NMS Customer Support for troubleshooting.

Section 6.11.3

Managing Firmware on ROX II Devices

This section describes how to manage the firmware on RUGGEDCOM ROX II devices managed by RUGGEDCOM NMS.

CONTENTS

Section 6.11.3.1

Adding a ROX II Firmware Image to RUGGEDCOM NMS

Firmware images for RUGGEDCOM ROX II devices must be copied directly to the RUGGEDCOM NMS server manually by the user.

NOTE
Bulk firmware upgrades are only available for ROX II devices using rr2.2.0+ firmware.

To copy a RUGGEDCOM ROX II firmware image to the RUGGEDCOM NMS server, do the following:

- On the RUGGEDCOM NMS server, copy the firmware image file to either `/usr/share/opennms/debian386/rr2/dists/rr2.2.{version}` or `/usr/share/opennms/{debianppc|debianarm}/rr2/dists/rr2.2.{version}` , where *{version}* is the firmware version (e.g. rr2.2.1). If a folder matching the firmware version does not exist, create one.

Once a firmware image has been added, it will be appear in the RUGGEDCOM NMS Web interface during the upload process. For more information about uploading a firmware image to a ROX II device, refer to Section 6.11.3.2, "Uploading Firmware Images to ROX II Devices" .

Section 6.11.3.2

Uploading Firmware Images to ROX II Devices

To upload a firmware image file to one or more RUGGEDCOM ROX II devices managed by RUGGEDCOM NMS, do the following:

1. Make sure the IP address for the RUGGEDCOM NMS server is set in the configuration management daemon for the *rox2-debianarm-firmware-url*, *rox2-debianppc-firmware-url* and *rox2-debian386-firmware-url* parameters. For more information, refer to Section 4.6, "Configuring the Management Daemon" .
2. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Firmware Upgrade**. The **Firmware Upgrade** screen appears.

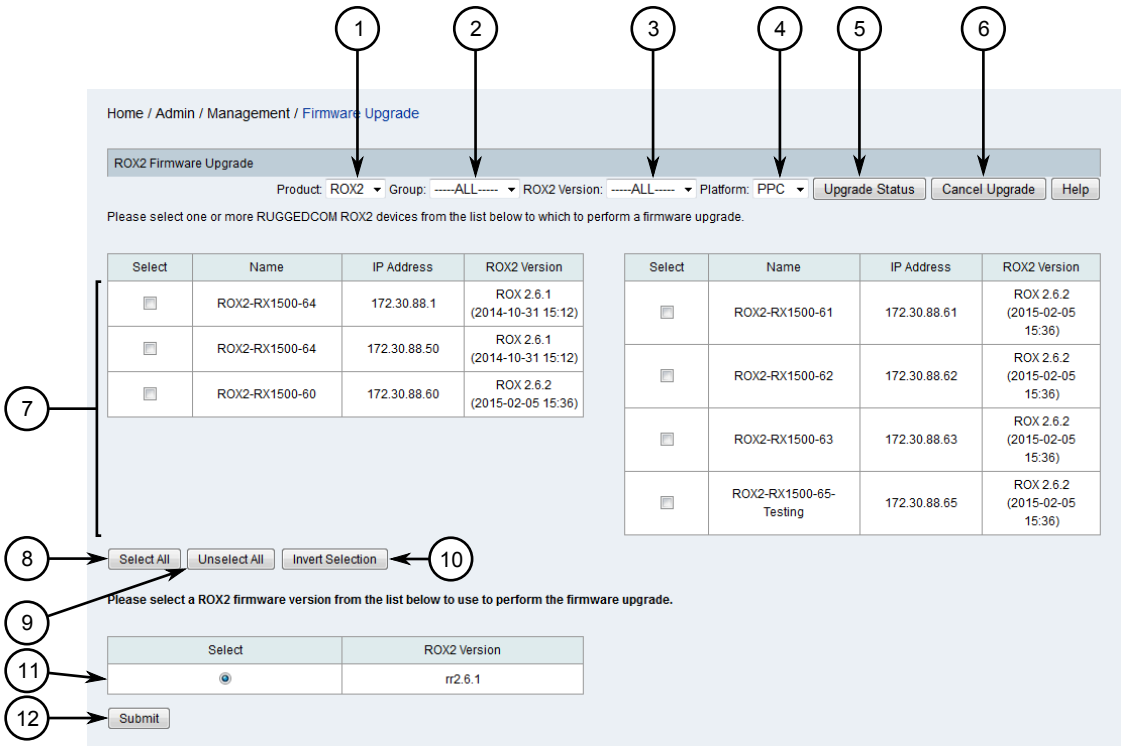


Figure 389: Firmware Upgrade Screen

1. Product List **2.** Group List **3.** ROX2 Version List **4.** Platform List **5.** Upgrade Status Button **6.** Cancel Upgrade Button **7.** Available ROX II Devices **8.** Select All Button **9.** Unselect All Button **10.** Invert Selection Button **11.** Available Firmware Images **12.** Submit Button

3. Use the **Product**, **Group**, **ROX2 Version** and **Platform** lists to filter the list of available ROX II devices.
4. Select one or more ROX II devices.

> **NOTE**
> *If the required firmware image is not listed, it must be added to the RUGGEDCOM NMS server. For more information, refer to* *Section 6.11.3.1, "Adding a ROX II Firmware Image to RUGGEDCOM NMS"* .

5. Select a firmware image and then click **Submit**. A confirmation message appears.
6. Click **OK**. The **List** screen appears listing all recent events, including a new event signaling the upload of the firmware image to the first target device. As the upload process continues in the background, a new event of the type *RNMSSingleUploadSuccess* is generated for each ROX II device that is updated.

   All event information is recorded in the log file. For more information about the viewing the Configuration Management log file, refer to Section 6.1, "Viewing the Configuration Management Log" .

   Another method for tracking the upload process is to return to the **Firmware Upgrade** screen and click **Upload Status**. The **Bulk Upload/Operation Status** dialog box appears indicating the current status.

Figure 390: Bulk Upload/Operation Status Dialog Box

To cancel the upload process, do the following:

1. Return to the **Configuration Upload** screen and click **Cancel Upgrade**. A confirmation message appears.
2. Click **OK**. The upload process is stopped after the current upload has either completed or failed.

Section 6.11.4

Managing Apps

RUGGEDCOM NMS supports the management of apps on ROX II devices. Apps can be installed, upgraded or removed for individual devices or for multiple devices in a single operation.

CONTENTS

Section 6.11.4.1

Adding Apps to RUGGEDCOM NMS

Apps for RUGGEDCOM ROX II devices must be copied directly to the RUGGEDCOM NMS server manually by the user.

NOTE
Currently, only RUGGEDCOM CROSSBOW and RUGGEDCOM ELAN apps are supported.

To copy a RUGGEDCOM ROX II app to the RUGGEDCOM NMS server, do the following:

- On the RUGGEDCOM NMS server, copy the firmware image file to `/usr/share/opennms/{debianppc|debianarm}/{crossbow or elan}/dists/{crossbow or elan}-{version}` , where *{version}* is the firmware version (e.g. 4.1.2). If a folder matching the app version does not exist, create one.

Once an app has been added, it will be appear in the RUGGEDCOM NMS Web interface during the installation/upgrade process. For more information about installing/upgrading an app to a ROX II device, refer to Section 6.11.4.2, "Installing/Upgrading Apps" .

Section 6.11.4.2

Installing/Upgrading Apps

To install or upgrade apps on one or more ROX II devices, do the following:

1. [Optional] If the app requires a feature key, make sure the necessary feature key is available on the RUGGEDCOM NMS server. Feature keys are stored under /usr/share/opennms/ruggednms/featurekeys/{ip-address} , where *{ip-address}* is the IP address for the device that uses the feature key.
2. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **App Management**. The **App** screen appears.

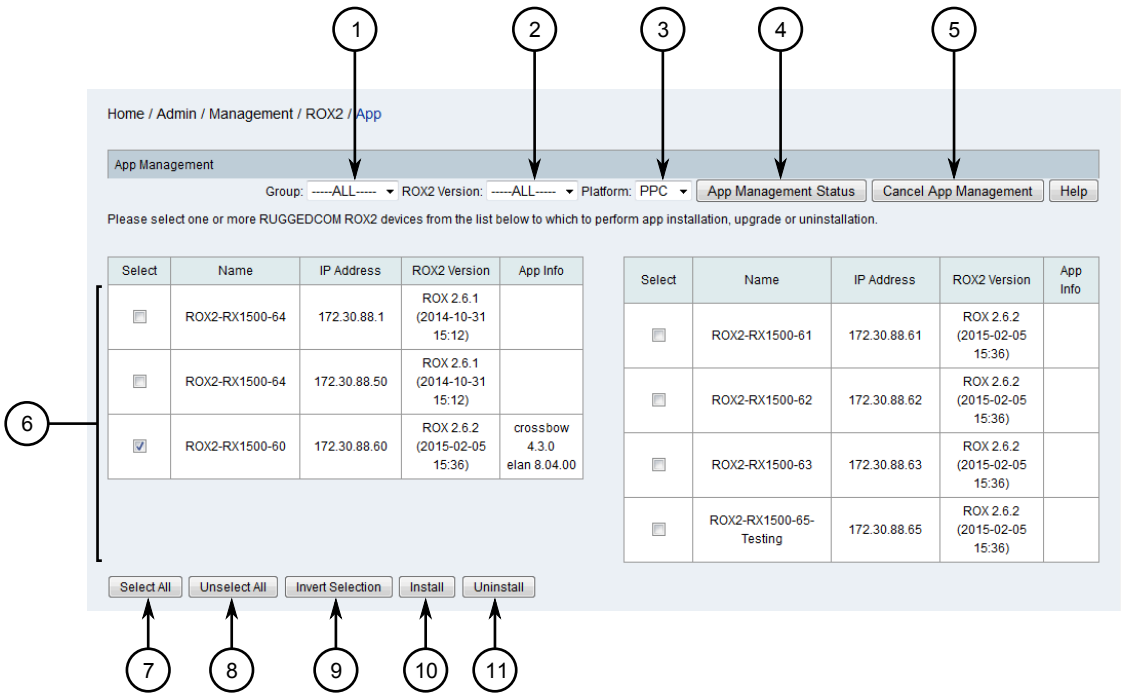


Figure 391: App Screen

1. Group List **2.** ROX2 Version List **3.** Platform List **4.** App Management Status Button **5.** Cancel App Management Button **6.** Available Devices **7.** Select All Button **8.** Unselect All Button **9.** Invert Selection **10.** Install Button **11.** Uninstall Button

3. Use the **Group**, **ROX2 Version** and **Platform** lists to filter the list of available devices.

NOTE
*The **App Info** column indicates which devices have apps installed.*

4. Select one or more devices and then click **Install**. The **Install** screen appears.

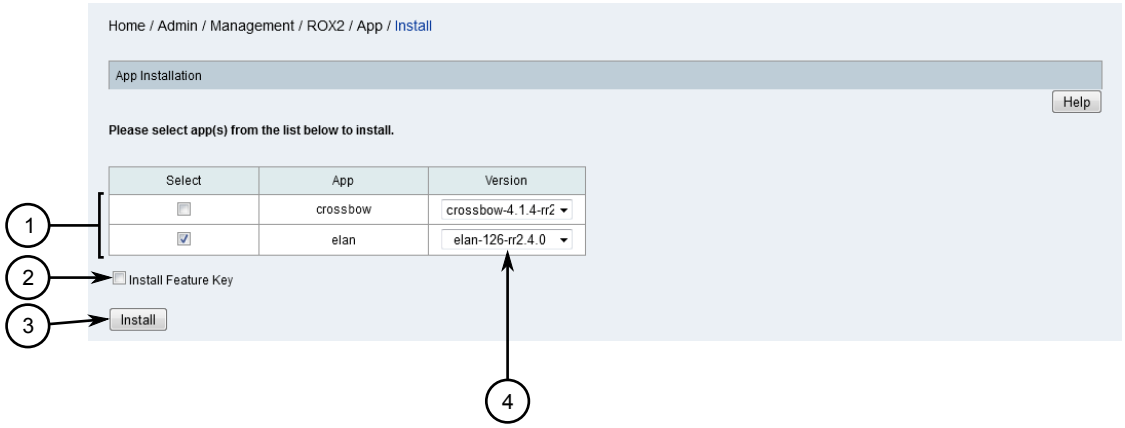


Figure 392: Install Screen

1. Available Apps **2.** Install Feature Key Check Box **3.** Install Button **4.** Version List

NOTE
If the required app is not listed, it must be added to the RUGGEDCOM NMS server. For more information, refer to *Section 6.11.4.1, "Adding Apps to RUGGEDCOM NMS"* .

5. Select one or more apps and then select which version to install from the **Version** column.
6. [Optional] Select **Install Feature Key** to install the feature key for each app at the same time. If RUGGEDCOM NMS finds more than one feature key stored on the RUGGEDCOM NMS server, it will send the one with the latest time stamp to the device.
7. Click **Install**. A confirmation message appears.
8. Click **OK** to install the app(s). For each app, RUGGEDCOM NMS verifies the operating system dependency. If an app is not compatible with the operating system installed on a device, a message appears. Otherwise, the app is installed/upgraded (along with feature keys, if select) and the device reboots. This process will continue in sequence until all selected apps are installed/upgraded on each selected device.
9. Click **App Management Status** to view the current status of the installation/upgrade process. Otherwise, details are recorded in the configuration management log file. For more information about viewing the configuration management log file, refer to Section 6.1, "Viewing the Configuration Management Log" .

Section 6.11.4.3
Removing an App

To remove an app from a ROX II device, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **App Management**. The **App** screen appears.

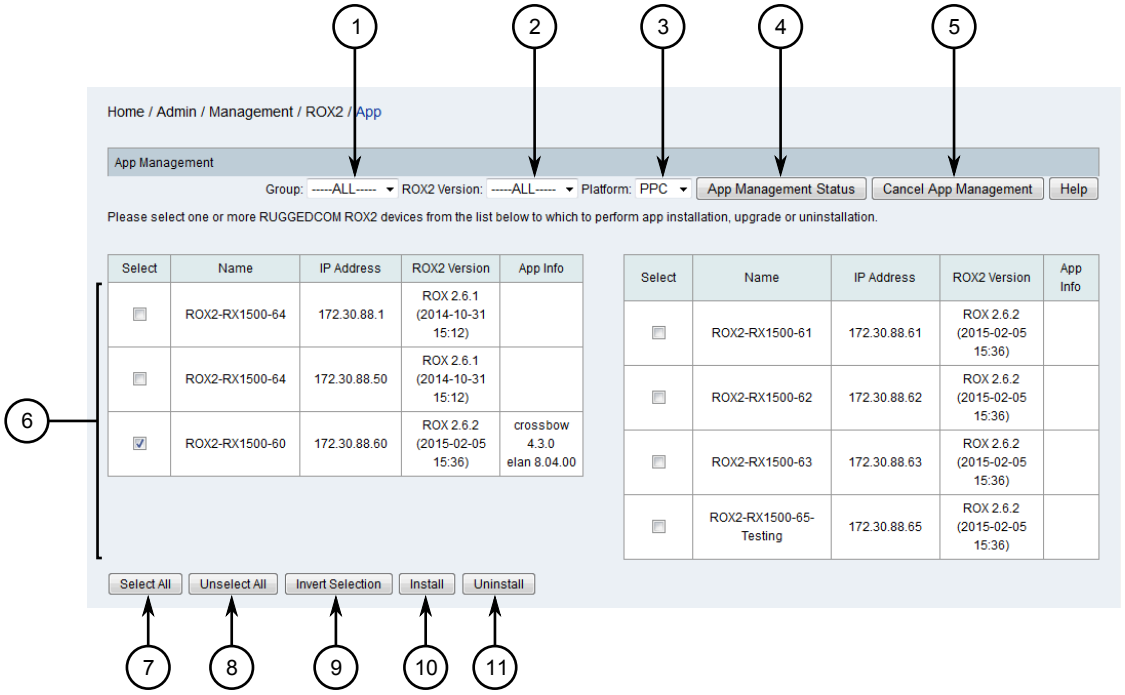


Figure 393: App Screen

1. Group List **2.** ROX2 Version List **3.** Platform List **4.** App Management Status Button **5.** Cancel App Management Button
6. Available Devices **7.** Select All Button **8.** Unselect All Button **9.** Invert Selection **10.** Install Button **11.** Uninstall Button

2. Use the **Group**, **ROX2 Version** and **Platform** lists to filter the list of available devices.

> **NOTE**
> *The **App Info** column indicates which devices have apps installed.*

3. Select the desired device and then click **Uninstall**. The **Uninstall** screen appears.

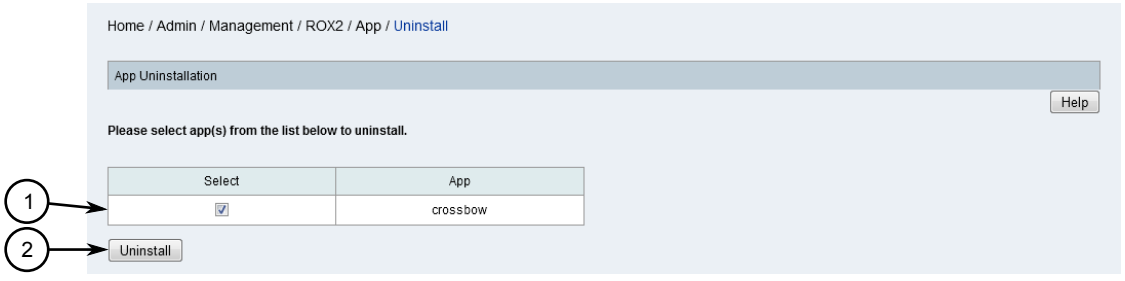


Figure 394: Uninstall Screen

1. Available Apps **2.** Uninstall Button

4. Select the desired app and then click **Uninstall**. A confirmation message appears.
5. Click **OK** to uninstall the app.

Section 6.11.5

Managing Firewalls

This section describes how to configure and manage firewalls for devices managed by RUGGEDCOM NMS that are running the ROX II operating system.

IMPORTANT!
For more information about how to configure a firewall on a ROX II device, refer to the RUGGEDCOM ROX II User Guide for the target ROX II device.

NOTE
Firewall configuration via RUGGEDCOM NMS is only available for ROX II devices running ROX v2.6.0 or higher.

CONTENTS

Section 6.11.5.1

Enabling/Disabling Firewalls for a Device

To enable/disable a firewall for a device managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Firewall Management**. A confirmation message appears.
2. Click **OK**. The **Firewall** screen appears.

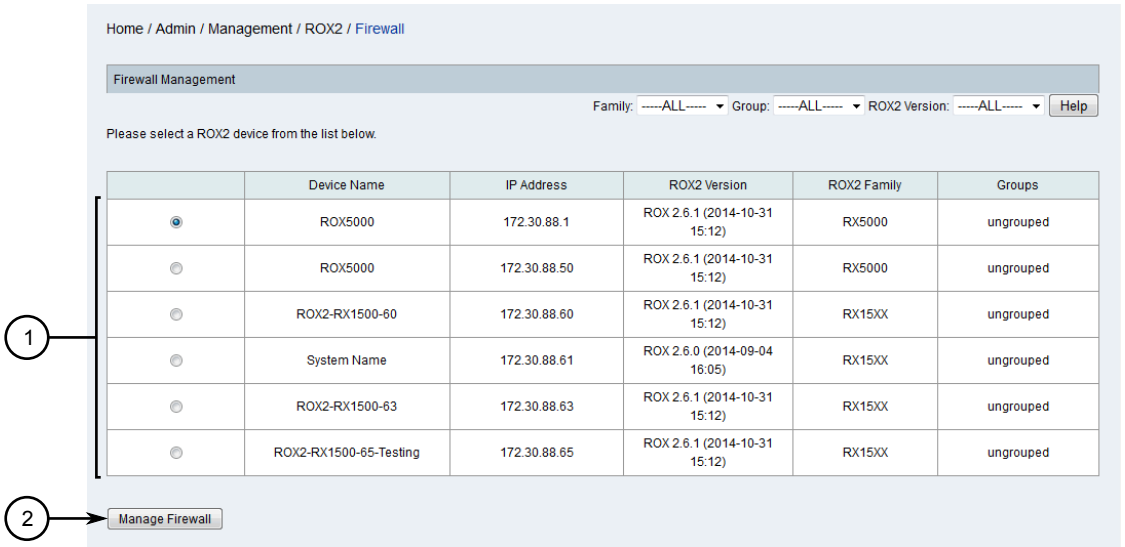


Figure 395: Firewall Screen

1. Available Devices **2.** Manage Firewall Button

3. Select a device and then click **Manage Firewall**. The **Profile** screen appears.

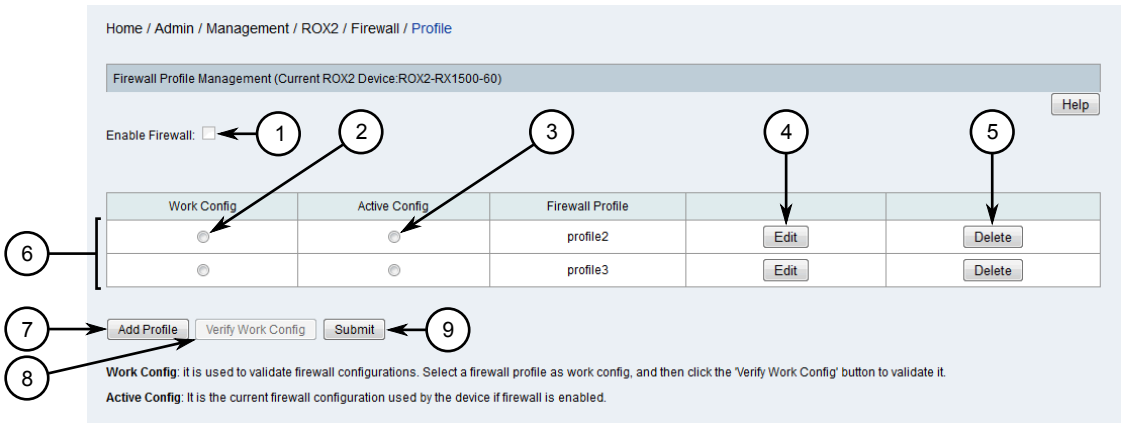


Figure 396: Firewall Screen

1. Enable Firewall Check Box **2.** Work Config Option **3.** Active Config Option **4.** Edit Button **5.** Delete Button **6.** Available Firewall Configurations **7.** Add Profile Button **8.** Verify Work Config Button **9.** Submit Button

4. Make sure one of the available firewall configurations is set to be the active configuration. For more information, refer to Section 6.11.5.2, "Activating a Firewall" .
5. Select **Enable Firewall** to enable the firewall for the selected device, or clear the check box to disable the firewall.
6. If a firewall configuration is not available, create one. For more information, refer to Section 6.11.5.3, "Adding a Firewall Configuration" .
7. Activate one of the available firewall configurations by clicking its option button under **Active Config**.

8. Click **Submit** to update the device configuration.

Section 6.11.5.2
Activating a Firewall

To activate a firewall for a ROX II device managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Firewall Management**. A confirmation message appears.
2. Click **OK**. The **Firewall** screen appears.

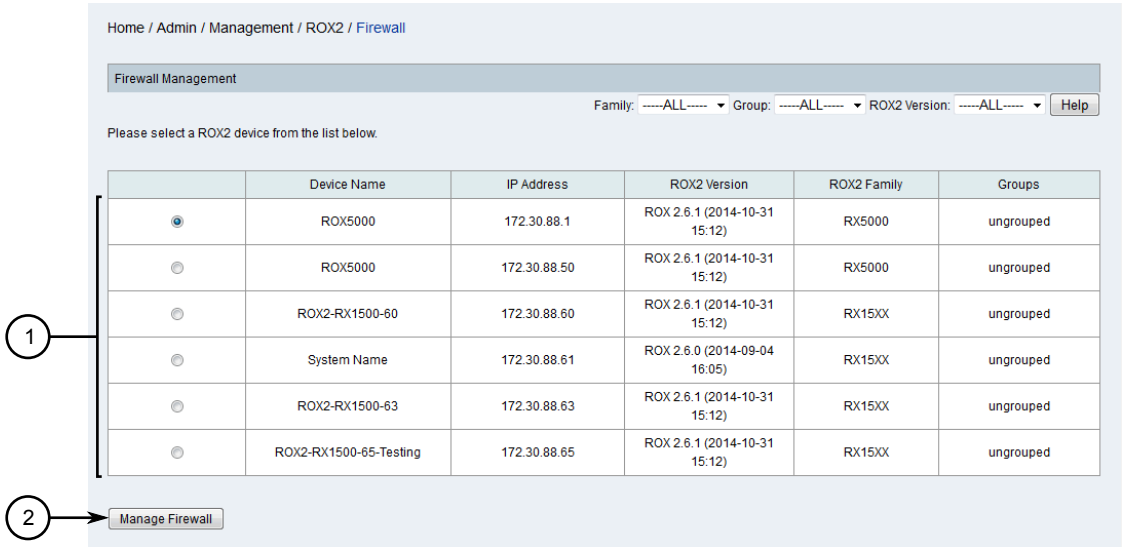


Figure 397: Firewall Screen

1. Available Devices **2.** Manage Firewall Button

3. Select a device and then click **Manage Firewall**. The **Profile** screen appears.

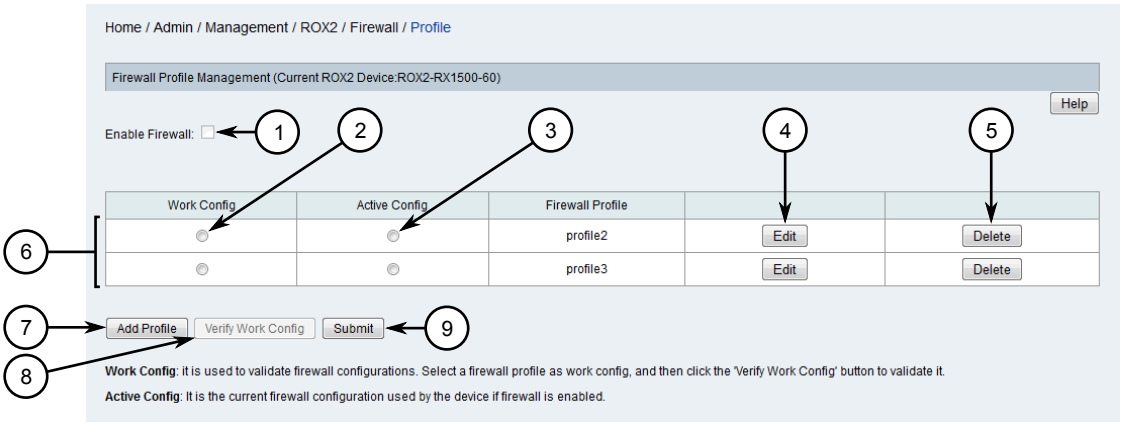


Figure 398: Firewall Screen

1. Enable Firewall Check Box **2.** Work Config Option **3.** Active Config Option **4.** Edit Button **5.** Delete Button **6.** Available Firewall Configurations **7.** Add Profile Button **8.** Verify Work Config Button **9.** Submit Button

4. If a firewall configuration is not available, create one. For more information, refer to Section 6.11.5.3, "Adding a Firewall Configuration" .
5. Activate one of the available firewall configurations by clicking its option button under **Active Config**.
6. Click **Submit** to update the device configuration.

Section 6.11.5.3
Adding a Firewall Configuration

To add a firewall configuration to a ROX II device managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Firewall Management**. A confirmation message appears.
2. Click **OK**. The **Firewall** screen appears.

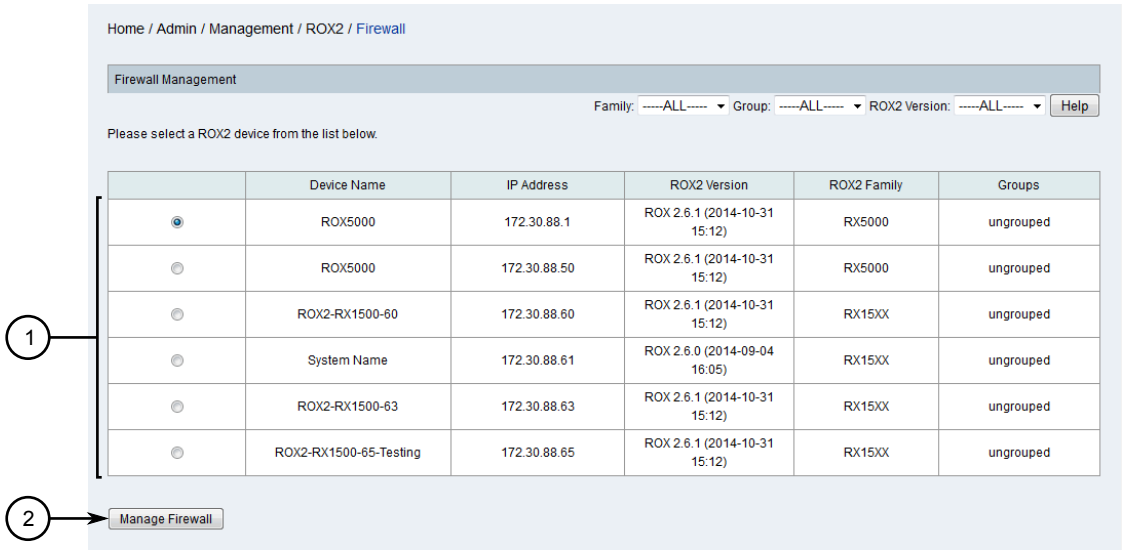


Figure 399: Firewall Screen

1. Available Devices **2.** Manage Firewall Button

3. Select a device and then click **Manage Firewall**. The **Profile** screen appears.

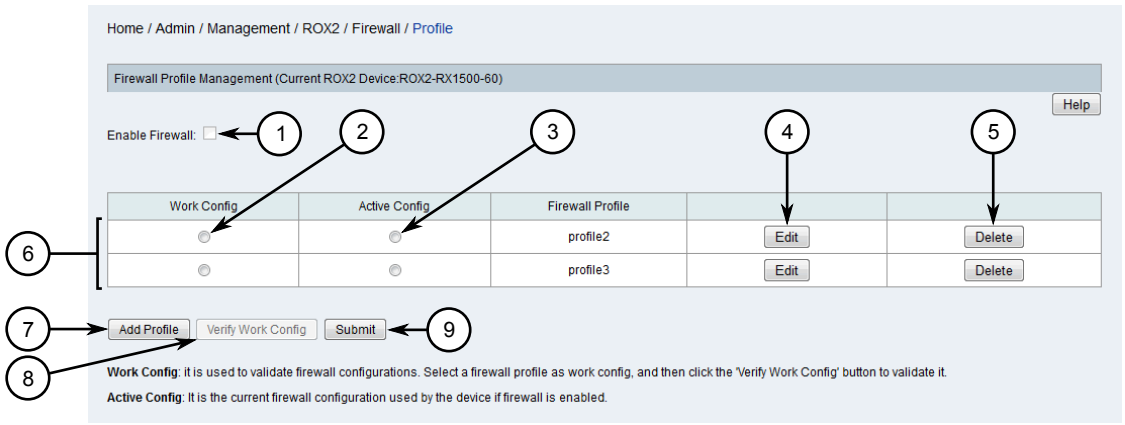


Figure 400: Profile Screen

1. Enable Firewall Check Box **2.** Work Config Option **3.** Active Config Option **4.** Edit Button **5.** Delete Button **6.** Available Firewall Configurations **7.** Add Profile Button **8.** Verify Work Config Button **9.** Submit Button

4. Click **Add Profile**. The **Adding a Profile** dialog box appears.

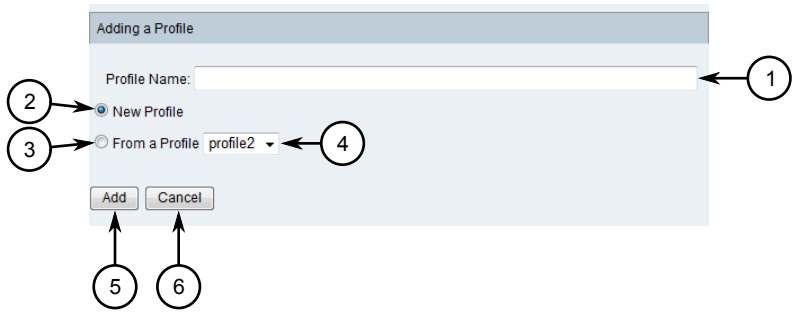


Figure 401: Adding a Profile Dialog Box

1. Profile Name Box **2.** New Profile Option **3.** From a Profile Option **4.** From a Profile List **5.** Add Button **6.** Cancel Button

5. Under **Profile Name**, type the name of the new firewall configuration.
6. Select either **New Profile** or **From a Profile**.
7. If **From a Profile** is selected, select a firewall configuration previously configured for the device. The new firewall configuration will inherit the values from the selected configuration.
8. Click **Add**. The **Configuration** screen appears.

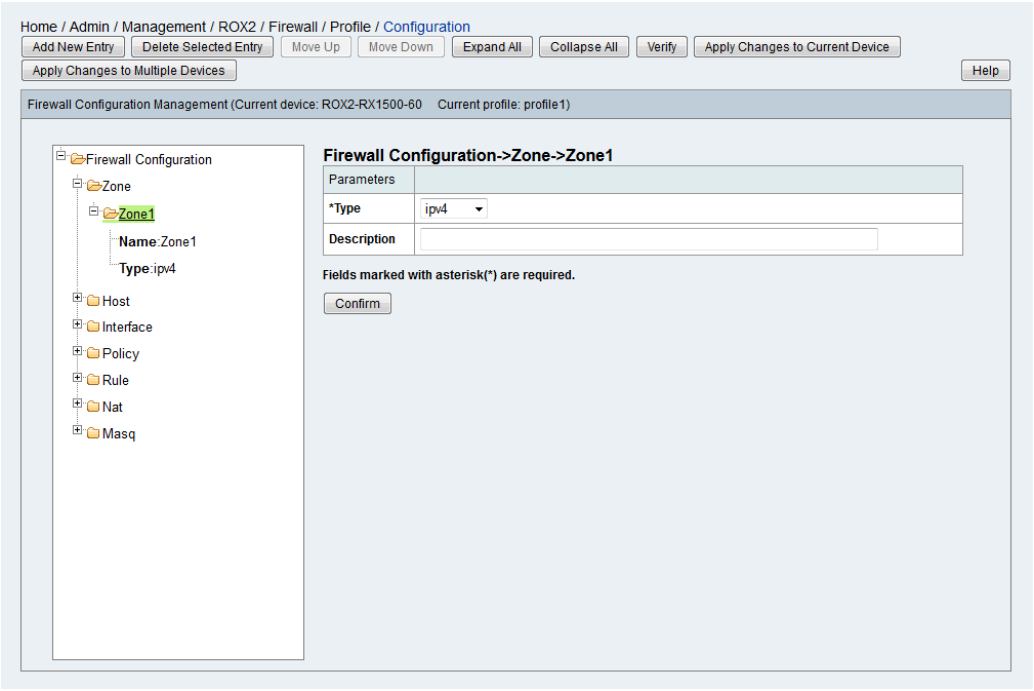


Figure 402: Configuration Screen

9. Configure the new firewall configuration. For more information, refer to Step 5 to Step 7 in Section 6.11.5.4, “Editing a Firewall Configuration” .

Section 6.11.5.4
Editing a Firewall Configuration

To edit an existing firewall configuration, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Firewall Management**. A confirmation message appears.
2. Click **OK**. The **Firewall** screen appears.

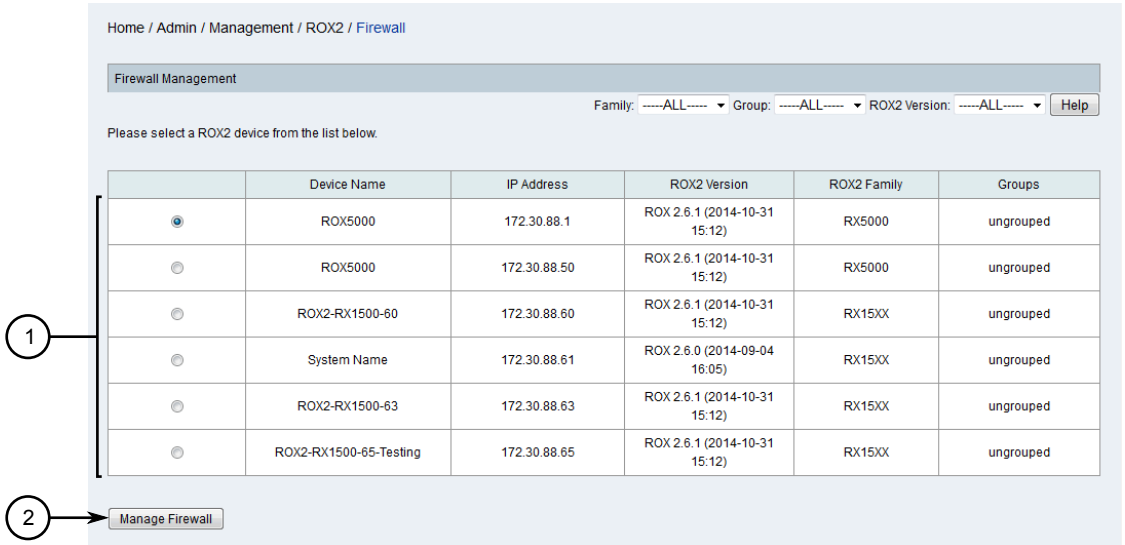


Figure 403: Firewall Screen

1. Available Devices **2.** Manage Firewall Button

3. Select a device and then click **Manage Firewall**. The **Profile** screen appears.

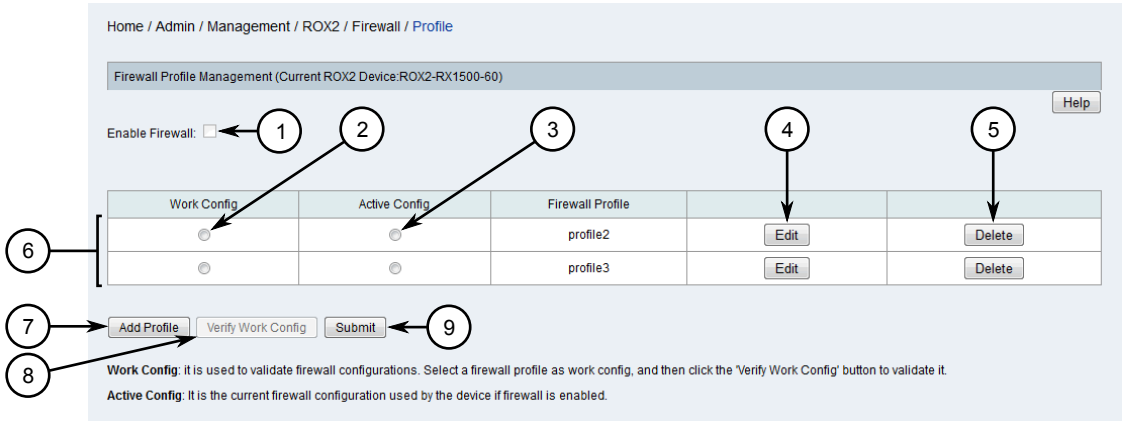


Figure 404: Profile Screen

1. Enable Firewall Check Box **2.** Work Config Option **3.** Active Config Option **4.** Edit Button **5.** Delete Button **6.** Available Firewall Configurations **7.** Add Profile Button **8.** Verify Work Config Button **9.** Submit Button

4. Click **Edit** for the desired firewall configuration. The **Configuration** screen appears.

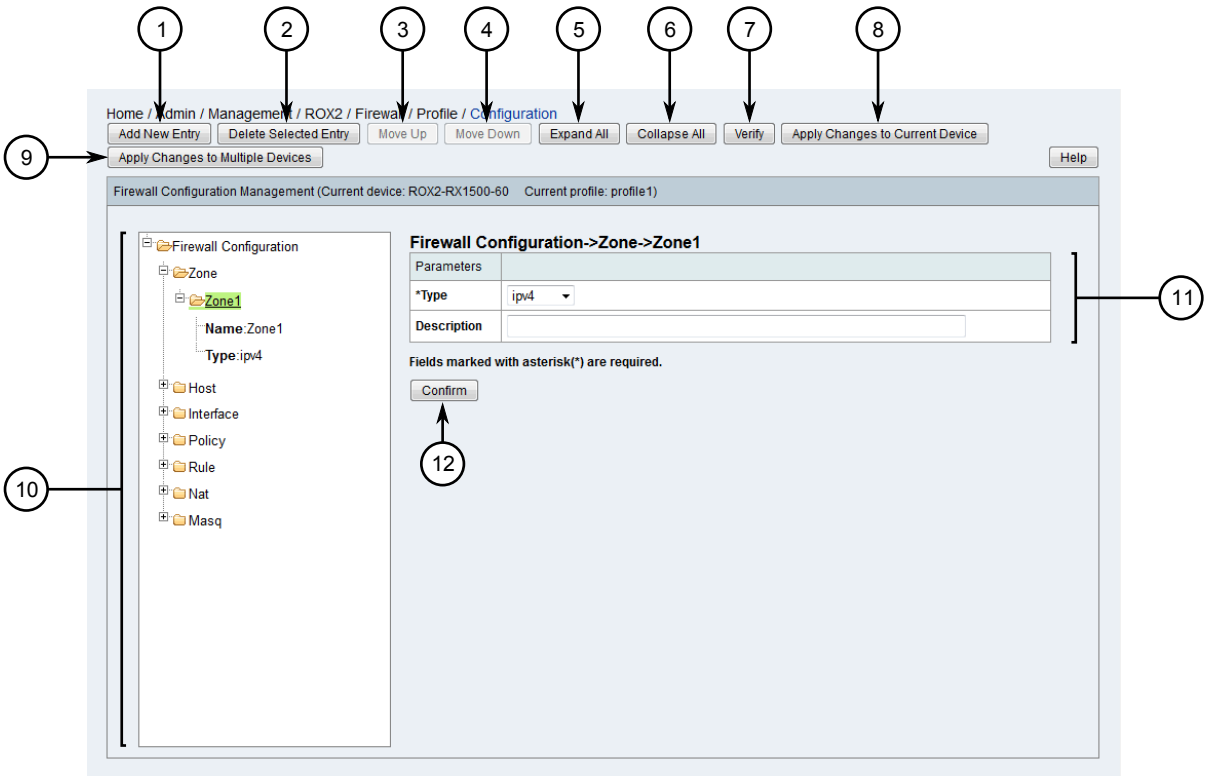


Figure 405: Configuration Screen

1. Add New Entry Button **2.** Delete Selected Entry Button **3.** Move Up Button **4.** Move Down Button **5.** Expand All Button **6.** Collapse All Button **7.** Verify Button **8.** Apply Changes to Current Device Button **9.** Apply Changes to Multiple Devices Button **10.** Tree Menu **11.** Entry Settings **12.** Confirm Button

5. Select the setting type from the tree menu and then click **Add New Entry**, or expand the setting type and select an existing entry. The required and optional parameters appear.

> **IMPORTANT!**
> *Each firewall configuration must include a zone called **fw** that is of the type **firewall**.*

6. Configure the following parameters as required:

Zone Settings

Parameter	Description
Name	A unique name for zone.
Type	**Synopsis:** ipv4, ipsec, firewall **Default:** ipv4 Zone types are firewall, IPv4 or IPSsec
Description	A description of the zone.

Host Settings

Parameter	Description
Name	A unique name for the host.
Zone	A pre-defined zone.
Interface	A pre-defined interface to which optional IPs and/or networks can be added.
Enable IPSec Zone	When selected, IPSec is enabled for the zone.
IP Address List	A comma-separated list of additional IP addresses and/or networks.
Description	A description of the host.

Interface Settings

Parameter	Description
Interface Name	A unique name for the interface.
Predefined Zone	A pre-defined zone.
Undefined Zone	An undefined zone. This is used on conjunction with the host definitions.
Broadcast IPv4 Address	An IPv4 address for a broadcast address.
Broadcast Auto-Detect	When selected, broadcast addresses are automatically detected.
Broadcast None	When selected, broadcasting is disabled.
ARP Filter Enable	When selected, the device responds only to ARP requests for configured IP addresses. This feature is permanently enabled system-wide since ROX v2.3.0. It is retained for pre-ROX v2.3.0 configurations.
Routeback Enable	Allows traffic on this interface to be routed back out that same interface.
TCP Flags Enable	When selected, illegal combinations of TCP flags are dropped and logged at the *info* level.
DHCP Enable	When selected, DHCP datagrams are allowed to enter and leave the interface.
NORFC1918 Enable	*Not currently implemented on ROX II devices.*
Route Filter Enable	When selected, route filtering is enabled.
Proxy ARP Enable	When selected, proxy ARP is enabled.
MAC List Enable	*Not currently implemented on ROX II devices.*
No Smurfs Enable	When selected, packets with a broadcast address as the source are dropped and logged at the *info* level.
Log Martians Enable	When selected, packets with impossible source addresses are logged.
Description	A description of the interface.

Policy Settings

Parameter	Description
Policy Name	A unique name for the policy.
Policy	**Synopsis:** { continue, reject, drop, accept } **Default:** reject The default action to take when establishing connections between different zones.
Source Zone	The source zone.
All Source Zone	The all source zone
Destination Zone	The destination zone
All Destination Zone	The all destination zone
Log Level	**Synopsis:** { emergency, alert, critical, error, warning, notice, info, debug, none } **Default:** none The level at which logging will take place. A value of `none` disables logging.
Description	A description of the policy.

Rule Settings

Parameter	Description
Rule Name	A unique name for the rule.
Predefined Source Zone	The pre-defined source zone.
Other Source Zone	A custom, comma-separated list of source zones.
All Source Zone	The all source zone
Predefined Destination Zone	The pre-defined destination zone.
Other Destination Zone	A custom, comma-separated list of destination zones.
All Destination Zone	The all destination zone.
Action	**Synopsis:** { dnat, dnat-, redirect, continue, reject, drop, accept } **Default:** reject The final action to take on incoming packets that match the rule.
Source Zone Hosts	A comma-separated list of host IPs for a predefined source zone.
Destination Zone Hosts	A comma-separated list of host IPs for a predefined destination zone. If required, include *:port* for dnat or redirect actions.
Protocol	The protocol to match for the rule.
Source Port	A single or comma-separated list of TCP/UDP port(s) the connection originated from.
Destination Port	A single or comma-separated list of TCP/UDP port(s) the connection is destined for.
Original Destination	The destination IP address in the connection request as it was received by the firewall.
Log Level	**Synopsis:** { emergency, alert, critical, error, warning, notice, info, debug, none }

Parameter	Description
	Default: none The level at which logging will take place. A value of `none` disables logging.
Description	A description of the rule.

Network Address Translation (NAT) Settings

Parameter	Description
Name	A unique name for the NAT entry.
External IP Address	The external IP Address for the chosen interface. The address must not be a DNS name. External IP addresses must be manually added to the interface.
Interface	The selected interface.
IP Alias Enable	When selected, an IP alias is created for the NAT entry.
Internal IP Address	The internal IP address. The address must not be a DNS name.
Limit Interface Enable	When selected, translation is only effective from the defined interface.
Local Enable	When selected, translation is only effective from the firewall system.
Description	A description of the NAT entry.

Masquerade and SNAT Settings

Parameter	Description
Masquerade Entry Name	A unique name for the masquerading configuration entry.
Outgoing Interface List	A comma-separated list of outgoing interfaces, typically the Internet-facing interface(s).
Outgoing Interface Specifics	A comma-separated list of outgoing interfaces, including specific IP destinations.
IP Alias Enable	When selected, an IP alias is created for the masquerading configuration entry.
Source Hosts	A subnet range or comma-separated list of host IP addresses.
SNAT Address	The source address. Providing an address enables SNAT (Source Network Address Translation).
Description	A description of the masquerading configuration entry.

7. Click **Confirm** to save the changes. RUGGEDCOM NMS verifies that all required parameters are defined.
8. [Optional] Delete unused entries by selecting them from the tree menu and then clicking **Delete Selected Entry**.
9. [Optional] Change the order in which entries are processed by selecting them from the tree menu and clicking either **Move Up** or **Move Down**.
10. [Optional] Click **Verify**. A dialog box appears displaying the status of a secondary validation process to determine if the new/updated configuration is compatible with the target device(s). If the validation fails, review the configuration and repeat Step 6 to Step 10 if necessary. Otherwise, click **Close** to close the dialog box.

IMPORTANT!
Only changes to zones, policies and rules can be applied to multiple devices at once. All other changes must be applied to devices individually.

11. Click **Apply Changes to Current Device** or **Apply Changes to Multiple Devices** to submit the changes.

Section 6.11.5.5
Verifying Changes to a Firewall Configuration

To verify changes made to a firewall configuration, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Firewall Management**. A confirmation message appears.
2. Click **OK**. The **Firewall** screen appears.

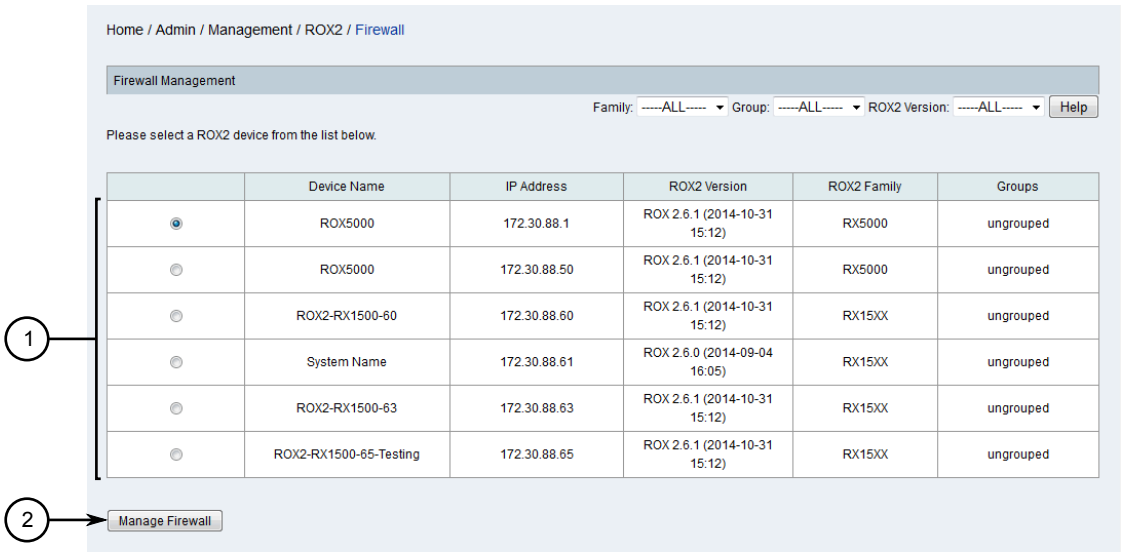


Figure 406: Firewall Screen

1. Available Devices **2.** Manage Firewall Button

3. Select a device and then click **Manage Firewall**. The **Profile** screen appears.

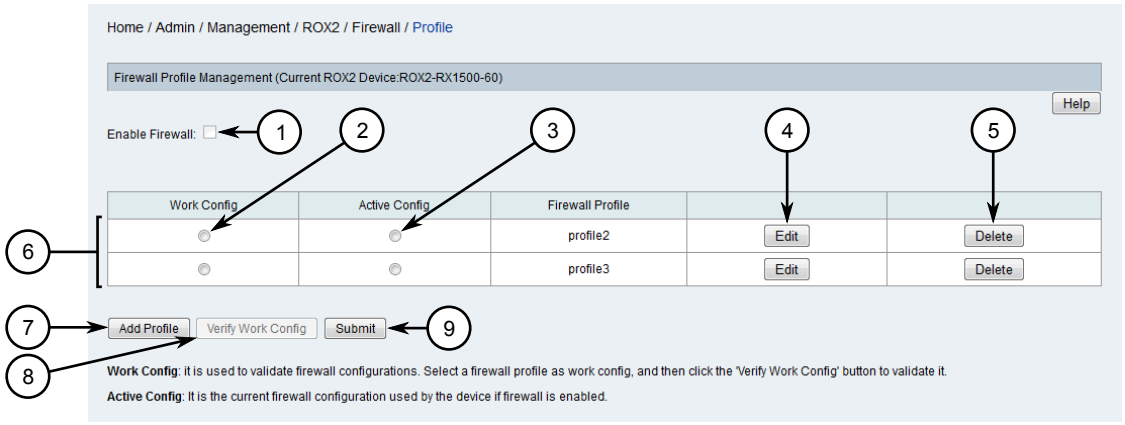


Figure 407: Profile Screen

1. Enable Firewall Check Box **2.** Work Config Option **3.** Active Config Option **4.** Edit Button **5.** Delete Button **6.** Available Firewall Configurations **7.** Add Profile Button **8.** Verify Work Config Button **9.** Submit Button

4. Click **Edit** for the desired firewall configuration. The **Configuration** screen appears.

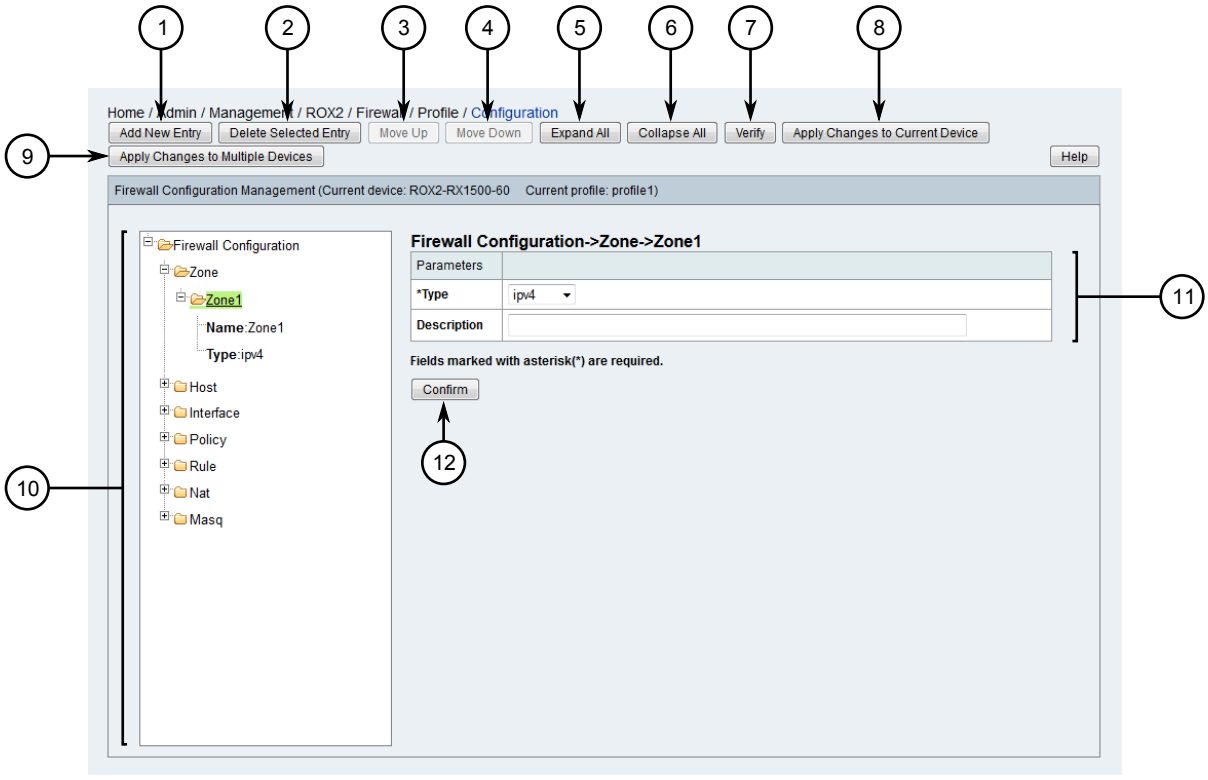


Figure 408: Configuration Screen

1. Add New Entry Button **2.** Delete Selected Entry Button **3.** Move Up Button **4.** Move Down Button **5.** Expand All Button **6.** Collapse All Button **7.** Verify Button **8.** Apply Changes to Current Device Button **9.** Apply Changes to Multiple Devices Button **10.** Tree Menu **11.** Entry Settings **12.** Confirm Button

5. Click **Verify**. A dialog box appears displaying the progress of the various validation steps. If successful, *Validation Passed* appears.

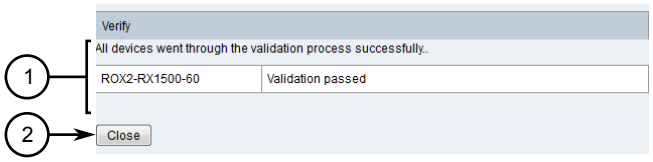


Figure 409: Verify Dialog Box

1. Verification Details **2.** Close Button

6. Click **Close**.
7. If the configuration did not pass validation, review and modify the configuration as required. For more information, refer to Section 6.11.5.4, "Editing a Firewall Configuration" .

Section 6.11.5.6

Verifying a Firewall Configuration Before Submitting it to a Device

To verify a firewall configuration before submitting it to a ROX II device, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Firewall Management**. A confirmation message appears.
2. Click **OK**. The **Firewall** screen appears.

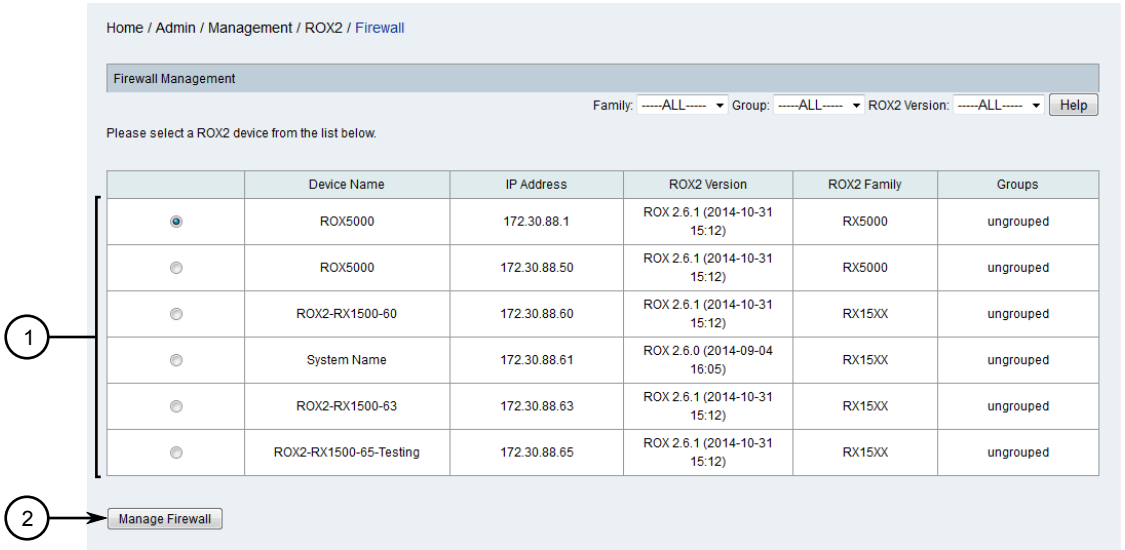


Figure 410: Firewall Screen

1. Available Devices **2.** Manage Firewall Button

3. Select a device and then click **Manage Firewall**. The **Profile** screen appears.

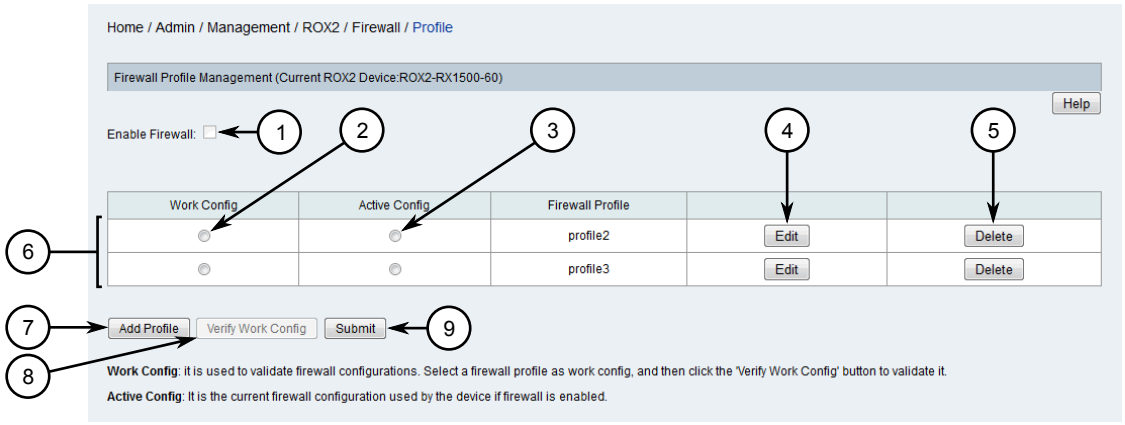


Figure 411: Profile Screen

1. Enable Firewall Check Box **2.** Work Config Option **3.** Active Config Option **4.** Edit Button **5.** Delete Button **6.** Available Firewall Configurations **7.** Add Profile Button **8.** Verify Work Config Button **9.** Submit Button

4. Make sure one of the available configurations is marked as the *working* configuration, and then click **Verify Work Config**. A dialog box appears displaying the progress of the various validation steps. If successful, *Validation Passed* appears.

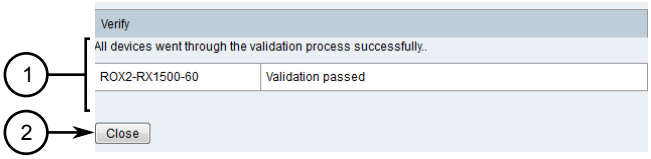


Figure 412: Verify Dialog Box

1. Verification Details **2.** Close Button

5. Click **Close**.
6. If the configuration did not pass validation, review and modify the configuration as required. For more information, refer to Section 6.11.5.4, "Editing a Firewall Configuration" .

Section 6.11.5.7
Deleting a Firewall

To delete a firewall configuration from a ROX II device managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **ROX2 Management**, and then click **Firewall Management**. A confirmation message appears.
2. Click **OK**. The **Firewall** screen appears.

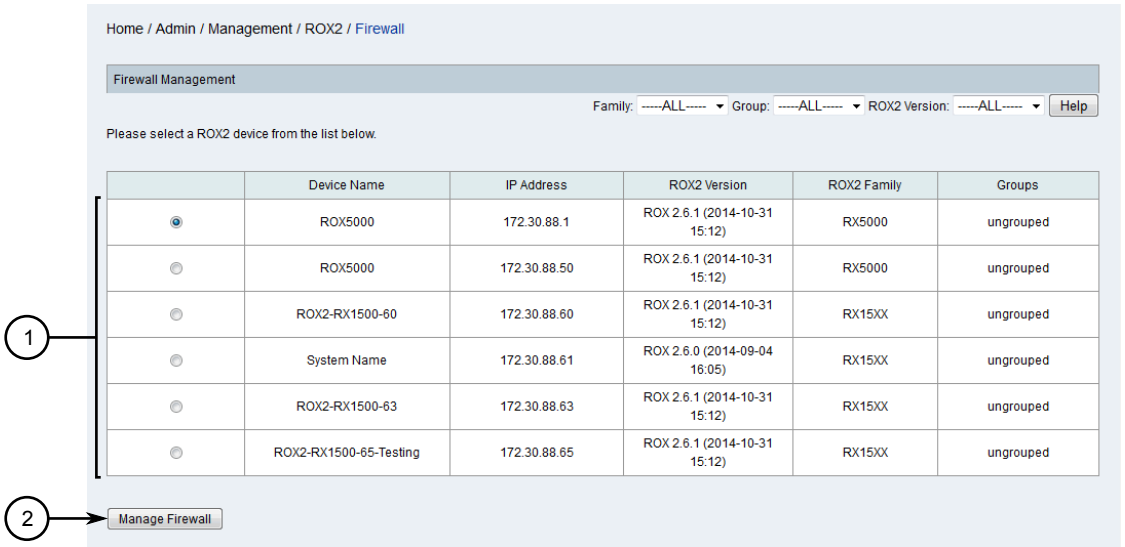


Figure 413: Firewall Screen

1. Available Devices **2.** Manage Firewall Button

3. Select a device and then click **Manage Firewall**. The **Profile** screen appears.

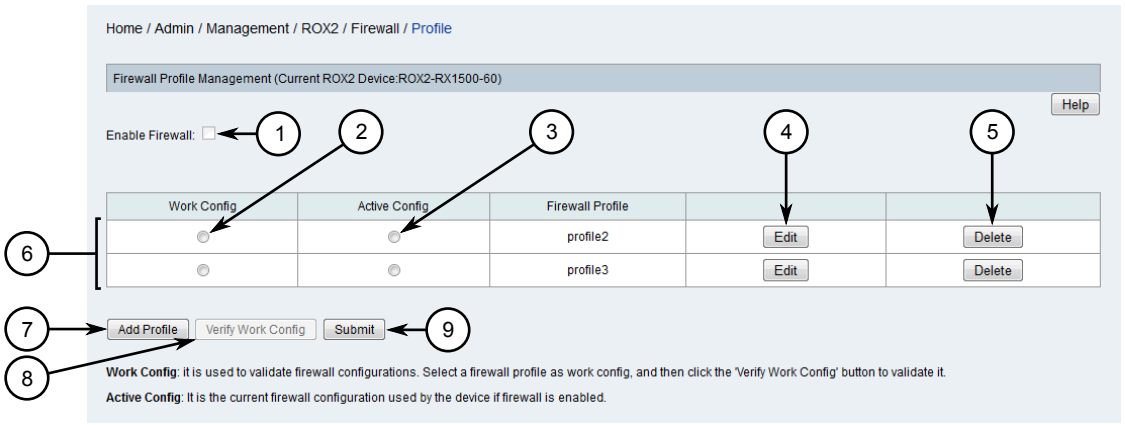


Figure 414: Firewall Screen

1. Enable Firewall Check Box **2.** Work Config Option **3.** Active Config Option **4.** Edit Button **5.** Delete Button **6.** Available Firewall Configurations **7.** Add Profile Button **8.** Verify Work Config Button **9.** Submit Button

4. Click **Delete Profile**. A confirmation message appears.
5. Click **OK** to delete the firewall configuration.

Section 6.12

Managing WIN Devices

The following sections describe how to manage RUGGEDCOM WIN devices (base stations and CPEs) managed by RUGGEDCOM NMS:

NOTE
For information about how to configure SNMP for one or more RUGGEDCOM WIN devices, refer to Section 6.12.3.1, "Configuring SNMP for WIN Base Stations" .

NOTE
For information about how to download, upload, compare, save and delete UV configuration files for RUGGEDCOM WIN devices, refer to Section 6.6, "Managing Archived Configuration Files" .

CONTENTS

Section 6.12.1

Configuring a Base Station

Available services and general information about one or more RUGGEDCOM WIN base stations can be configured via RUGGEDCOM NMS.

To configure one or more base stations managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

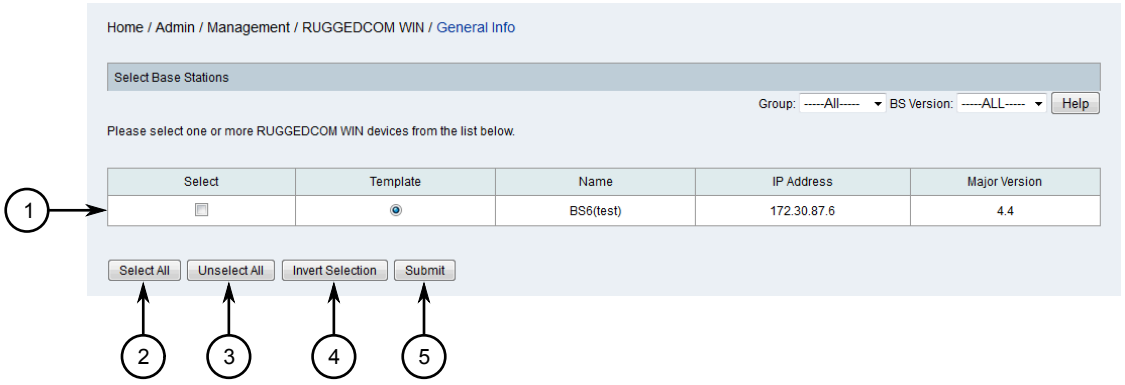


Figure 415: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Configure BS General Information** and **Frame Settings** tables appear.

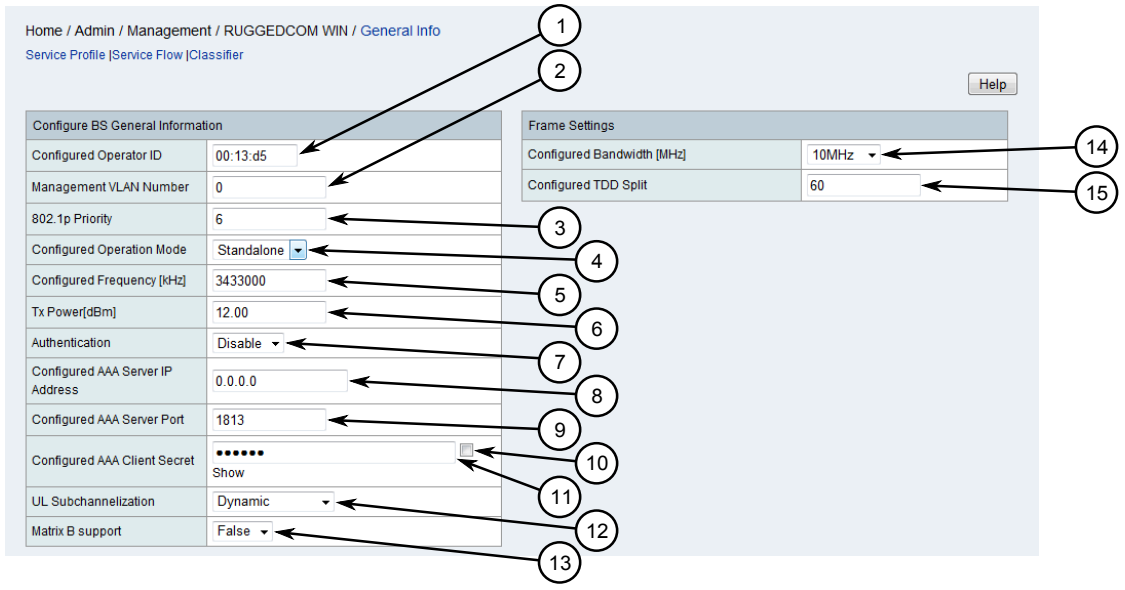


Figure 416: General Information and Frame Settings Tables

1. Configured Operator ID Box **2.** Management VLAN Number Box **3.** 802.1p Priority Box **4.** Configured Operation Mode List
5. Configured Frequency [kHz] Box **6.** Tx Power [dBm] Box **7.** Authentication List **8.** Configured AAA Server IP Address
9. Configured AAA Server Port **10.** Show Check Box **11.** Configured AAA Client Secret Box **12.** UL Subchannelization List
13. Matrix B Support List **14.** Configured Bandwidth [MHz] List **15.** Configured TDD Split Box

3. Under **Configure BS General Information**, configure the following parameters as required:

Parameter	Description
Configured Operator ID	The Network Access Provider identifier. Identifiers are unique to the operator and are managed by the IEEE (Institute of Electrical

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>and Electronics Engineers). For more information, refer to https://standards.ieee.org/develop/regauth/bopid .</td></tr>
<tr><td>Management VLAN Number</td><td>Synopsis: any numeric value
Default: 0
The identifier for the management VLAN.</td></tr>
<tr><td>802.1p Priority</td><td>Synopsis: 0 to 7
Default: 6
The 802.1p priority value for the management VLAN.</td></tr>
<tr><td>Configured Operation Mode</td><td>Synopsis: { Standalone, ASN-GW }
The base station operating mode. Options include:
<code>Standalone</code> – The base station installation topology does not include an ASN Gateway, and Quality of Service (QoS) functions are configure on the base station itself.
<code>ASN-GW</code> – The base station installation topology includes an ASN Gateway, and Quality of Service (QoS) functions are configured via the gateway.</td></tr>
<tr><td>Configured Frequency [kHz]</td><td>The base station radio frequency. For more information about the frequency range supported, refer to the RUGGEDCOM WIN Base Station User Guide for the target device.</td></tr>
<tr><td>Tx Power [dBm]</td><td>The base station transmission power setting. The value must be within the valid range determined by local regulations and within the capabilities of the device.
The supported power setting range for WIN base stations is as follows:<table><tr><th rowspan="2">Base Station Type</th><th rowspan="2">Band (GHz)</th><th colspan="2">Power Setting</th></tr><tr><th>Minimum</th><th>Maximum</th></tr><tr><td rowspan="3">Pico</td><td>2.3, 2.5, 3.3, 3.5, 3.65</td><td>12</td><td>27</td></tr><tr><td>4.9</td><td rowspan="2">9</td><td>24</td></tr><tr><td>5.8</td><td>21</td></tr><tr><td>Compact</td><td>—</td><td>21</td><td>36</td></tr></table></td></tr>
<tr><td>Authentication</td><td>Synopsis: { Disable, Enable }
Default: Disable
Enables or disables user authentication.</td></tr>
<tr><td>Configured AAA Server IP Address</td><td>The IP address for the AAA server. Not applicable in ASN-GW operation mode.</td></tr>
<tr><td>Configured AAA Server Port</td><td>The AAA server port number. Not applicable in ASN-GW operation mode.</td></tr>
<tr><td>Configured AAA Client Secret</td><td>The AAA server client secret. Click the Show check box to display the secret in plain text.</td></tr>
<tr><td>UL Subchannelization</td><td>Synopsis: { Dynamic, All Subchannels }
Default: Dynamic
Sets the minimum allocated up-link subchannels for automatic link adaptation.</td></tr>
<tr><td>Matrix B Support</td><td>Synopsis: { False, True }
Default: False</td></tr>
</table>

Parameter	Description
	Enables (true) or disables (false) support for MIMO Matrix B.

4. Under **Frame Settings**, configure the following parameters as required:

Parameter	Description
Configured Bandwidth [MHz]	**Synopsis:** { 3.5MHz, 5MHz, 7MHz, 10MHz } The base station bandwidth.
Configured TDD Split	**Synopsis:** 30 to 75 **Default:** 66 The frame TDD (Time Division Duplex) ratio. For recommended split values based on channel and cell range (extended or non-extended), refer to the *RUGGEDCOM WIN Base Station User Guide* for the target device.

5. Add, deactivate or delete service profiles as required. For more information, refer to Section 6.12.4, "Managing Base Station Service Profiles" .
6. Add, edit or delete service flows as required. For more information, refer to Section 6.12.5, "Managing Base Station Service Flows" .
7. Add, edit or delete classifiers as required. For more information, refer to Section 6.12.6, "Managing Base Station Classifiers" .
8. Click **Submit Changed Parameters** or **Submit all Parameters**.

Section 6.12.2
Managing Firmware on WIN Devices

This section describes how to manage the firmware on RUGGEDCOM WIN devices (base station and CPE) managed by RUGGEDCOM NMS.

CONTENTS

Section 6.12.2.1
Adding a WIN Firmware Image to RUGGEDCOM NMS

Firmware images for RUGGEDCOM WIN devices must be copied directly to the RUGGEDCOM NMS server manually by the user.

Bulk firmware upgrades are only available for WIN devices using rr2.2.0+ firmware.

To copy a RUGGEDCOM WIN firmware image to the RUGGEDCOM NMS server, do the following:

- On the RUGGEDCOM NMS server, copy the firmware image file to the appropriate folder:

  For Pico Base Station Devices (WIN7200 Series)

  - `/usr/share/opennms/ruggednms/configMgtd/ruggedMAX/firmware/BS{version}/Pico`

For Compact Base Station Devices (WIN7000 Series)

- `/usr/share/opennms/ruggednms/configMgtd/ruggedMAX/firmware/BS{version}/Compact`

For CPE Devices (WIN5000 Series)

- `/usr/share/opennms/ruggednms/configMgtd/ruggedMAX/firmware/CPE{version}`

Where *{version}* is the firmware version (e.g. BS4.1.4734.23). If a folder matching the firmware version does not exist, create one.

Once a firmware image has been added, it will be appear in the RUGGEDCOM NMS Web interface during the upload process. For more information about uploading a firmware image to a WIN device, refer to Section 6.12.2.2, "Uploading Firmware Images to WIN Devices" .

Section 6.12.2.2
Uploading Firmware Images to WIN Devices

To upload a firmware image file to one or more RUGGEDCOM WIN devices managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, and then click **Firmware Upgrade**. The **Firmware Upgrade** screen appears.

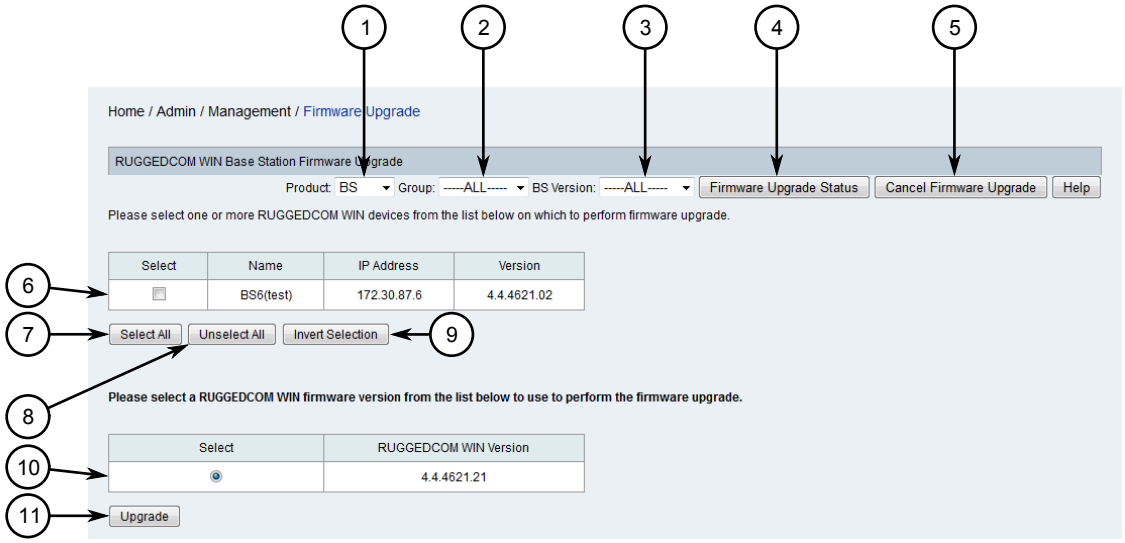


Figure 417: Firmware Upgrade Screen

1. Product List **2.** Group List **3.** BS Version or CPE Version List **4.** Upgrade Status Button **5.** Cancel Upgrade Button **6.** Available WIN Devices **7.** Select All Button **8.** Unselect All Button **9.** Invert Selection Button **10.** Available Firmware Images **11.** Upgrade Button

2. Use the **Product**, **Group** and **BS Version**/**CPE Version** lists to filter the list of WIN available devices.

IMPORTANT!
The maximum number of concurrent uploads to base station or CPE devices is defined by the configuration management daemon. Specifically, refer to the `bs-upgrade-thread-number` *and* `cpe-upgrade-thread-number` *parameters.*

If more devices are selected than the maximum allowed, the remaining devices will be processed in sequence as other devices finish uploading.

For more information about these parameters and the configuration management daemon, refer to *Section 4.6, "Configuring the Management Daemon"* .

3. Select one or more devices.

NOTE
If the required firmware image is not listed, it must be added to the RUGGEDCOM NMS server. For more information, refer to *Section 6.12.2.1, "Adding a WIN Firmware Image to RUGGEDCOM NMS "* .

4. Select a firmware image and then click **Submit**. A confirmation message appears.
5. Click **OK**. The **List** screen appears listing all recent events, including a new event signaling the upload of the firmware image to the first target device. As the upload process continues in the background, a new event of the type *RNMSSingleUploadSuccess* is generated for each WIN device that is updated.

   All event information is recorded in the log file. For more information about the viewing the Configuration Management log file, refer to Section 6.1, "Viewing the Configuration Management Log" .

   Another method for tracking the upload process is to return to the **Firmware Upgrade** screen and click **Upload Status**. The **Bulk Upload/Operation Status** dialog box appears indicating the current status.

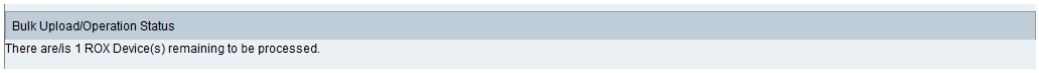


Figure 418: Bulk Upload/Operation Status Dialog Box

To cancel the upload process, do the following:

1. Return to the **Configuration Upload** screen and click **Cancel Upgrade**. A confirmation message appears.
2. Click **OK**. The upload process is stopped after the current upload has either completed or failed.

Section 6.12.3
Managing SNMP for WIN Base Stations

This section describes how to configure and manage SNMP settings for one or more RUGGEDCOM WIN base stations.

CONTENTS

Section 6.12.3.1
Configuring SNMP for WIN Base Stations

To configure SNMP for one or more RUGGEDCOM WIN base stations, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station SNMP Management**. The **SNMP** screen appears.

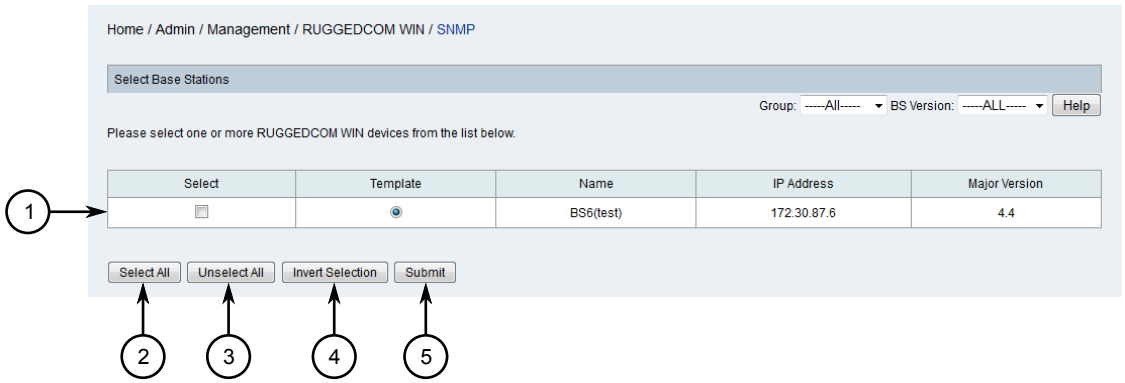


Figure 419: SNMP Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select the device designated as the template, as well as any other devices, then click **Submit**. The **SNMP** Screen appears.

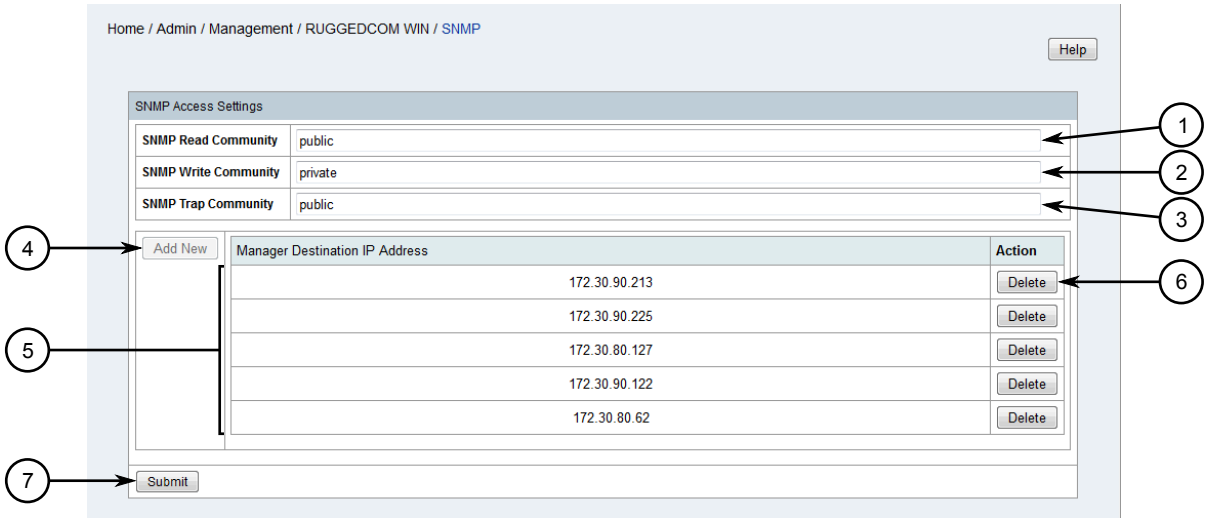


Figure 420: SNMP Screen

1. SNMP Read Community Box **2.** SNMP Write Community Box **3.** SNMP Trap Community Box **4.** Add New Button **5.** SNMP Trap Destinations **6.** Delete Button **7.** Submit Button

3. Configure the following parameters as required:

Parameter	Description
SNMP Read Community	**Default:** public The SNMP community name for read access. The name can be used as a password for secure information retrieval. The SNMP

Parameter	Description
	Read Community name must be different from the SNMP Write Community name.
SNMP Write Community	**Default:** private The SNMP community name for write access. The name can be used as a password for secure set commands. The SNMP Write Community name must be different from the SNMP Read Community name.
SNMP Trap Community	**Default:** public The SNMP community name to use when the SNMP service receives a request that does not contain the correct community name and does not match an accepted host name.

4. Add or delete SNMP trap destinations. For more information, refer to Section 6.12.3.2, "Adding an SNMP Trap Destination" or Section 6.12.3.3, "Deleting an SNMP Trap Destination" .
5. Click **Submit**. A confirmation message appears.
6. Click **OK** to apply the changes.

Section 6.12.3.2
Adding an SNMP Trap Destination

To add an SNMP trap destination, do the following:

NOTE
RUGGEDCOM WIN base stations support up to a maximum of five destinations.

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station SNMP Management**. The **SNMP** screen appears.

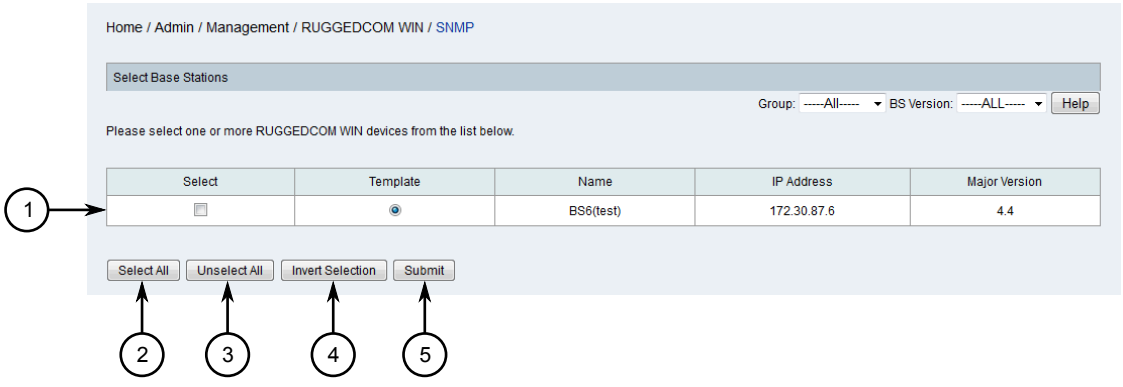


Figure 421: SNMP Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **SNMP** Screen appears.

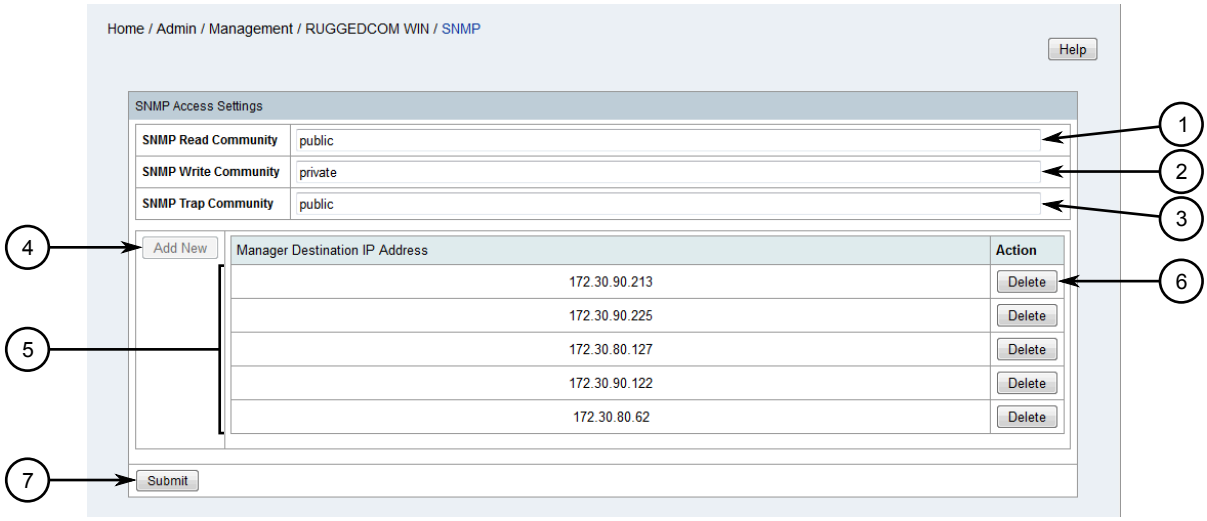


Figure 422: SNMP Screen

1. SNMP Read Community Box **2.** SNMP Write Community Box **3.** SNMP Trap Community Box **4.** Add New Button **5.** SNMP Trap Destinations **6.** Delete Button **7.** Submit Button

3. Click **Add New**. A dialog box appears.

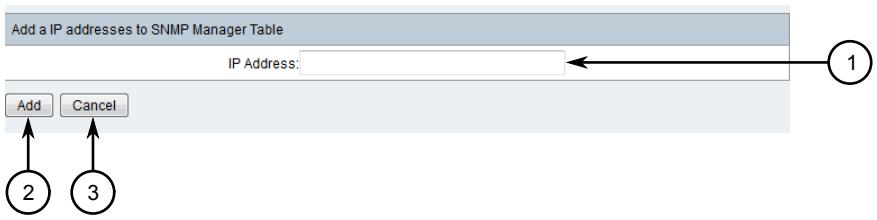


Figure 423: Dialog Box

1. IP Address Box **2.** Add Button **3.** Cancel Button

4. Under **IP Address**, type the IP address for a device that will be forwarded SNMP traps.
5. Click **Add**. The dialog box closes and the new destination is added.
6. Click **Submit**.

Section 6.12.3.3

Deleting an SNMP Trap Destination

To delete an SNMP trap destination, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station SNMP Management**. The **SNMP** screen appears.

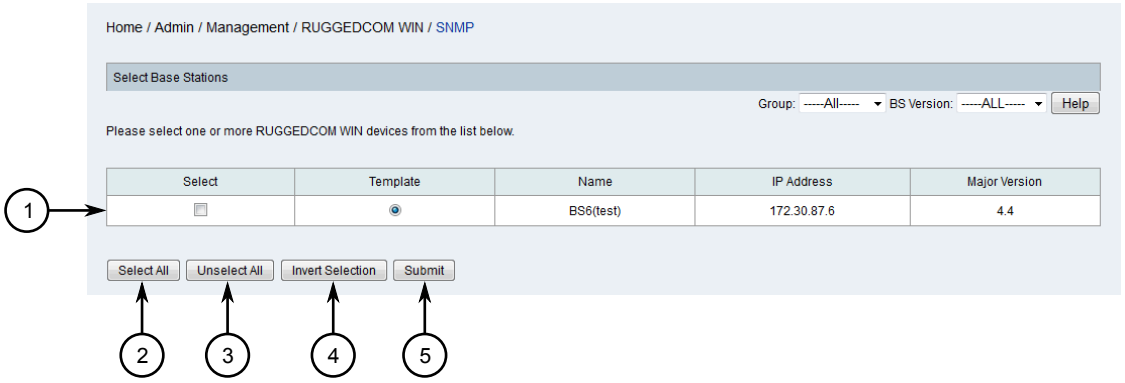


Figure 424: SNMP Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **SNMP** Screen appears.

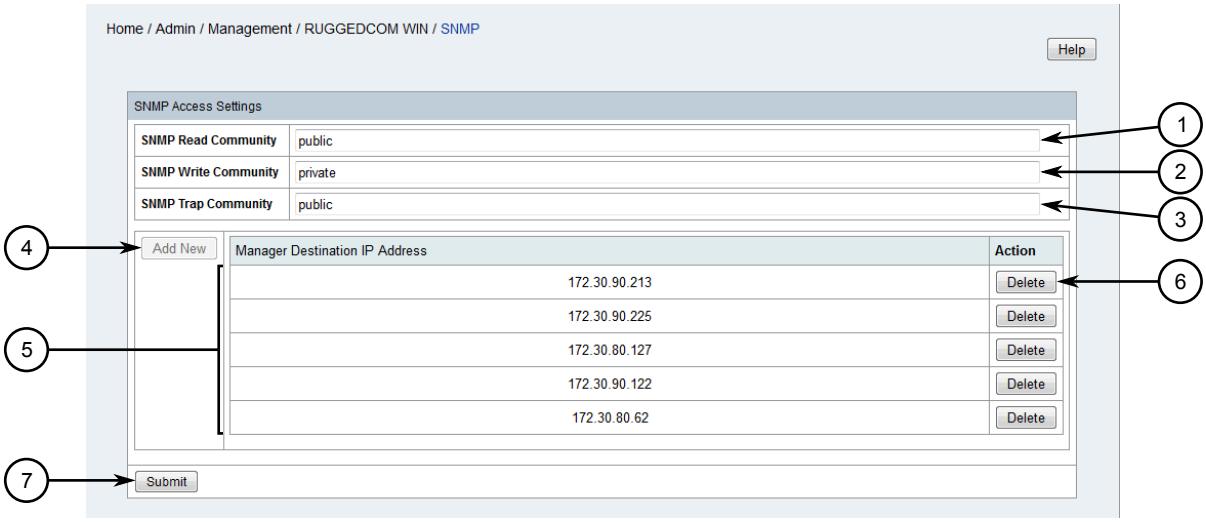


Figure 425: SNMP Screen

1. SNMP Read Community Box **2.** SNMP Write Community Box **3.** SNMP Trap Community Box **4.** Add New Button **5.** SNMP Trap Destinations **6.** Delete Button **7.** Submit Button

3. Click **Delete** next to the chosen destination. A confirmation message appears.
4. Click **OK**.
5. Click **Submit**.

Section 6.12.4

Managing Base Station Service Profiles

This section describes how to configure and manage service profiles for base stations managed by RUGGEDCOM NMS.

CONTENTS

Section 6.12.4.1

Viewing a List of Service Profiles

To view a list of service profiles configured for a specific RUGGEDCOM base station managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

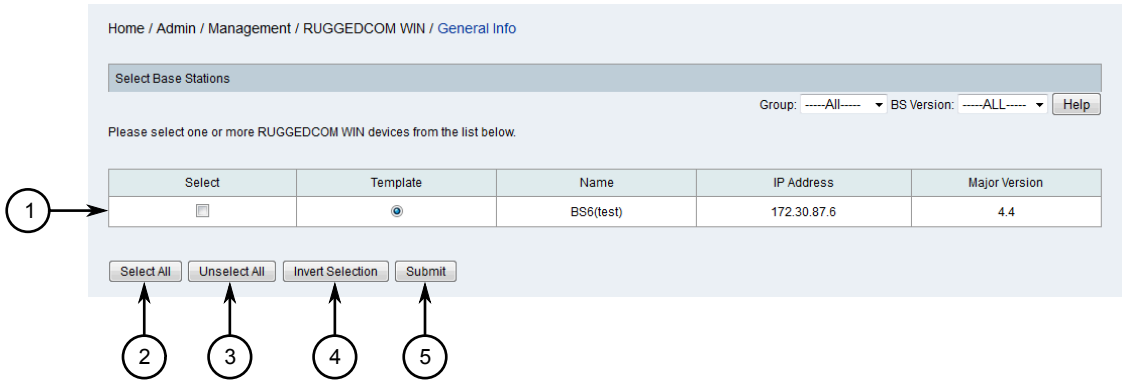


Figure 426: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Service Profiles** table appears, listing the available service profiles and their status.

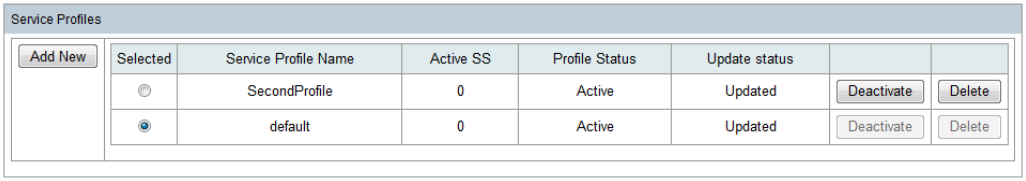


Figure 427: Service Profiles Table

Section 6.12.4.2
Adding a Service Profile

To add a service profile to a specific RUGGEDCOM WIN base station, do the following:

IMPORTANT!
Up to 32 service profiles can be configured per base station.

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

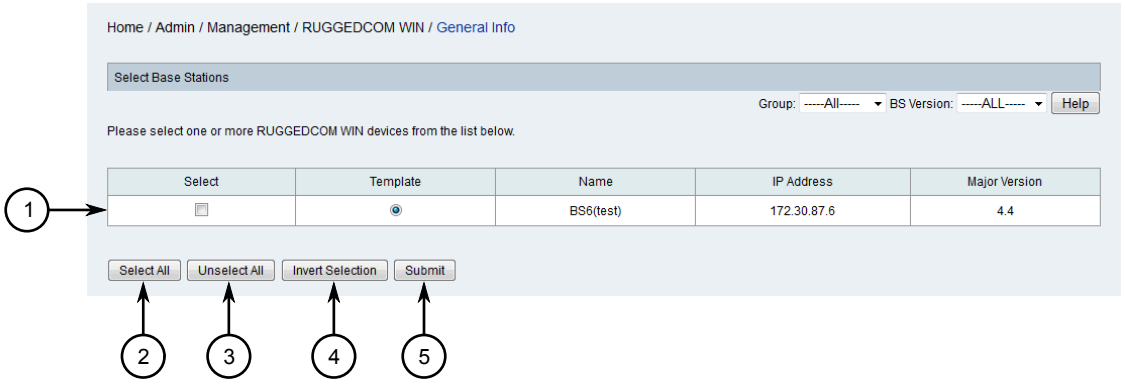


Figure 428: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Service Profiles** table appears.

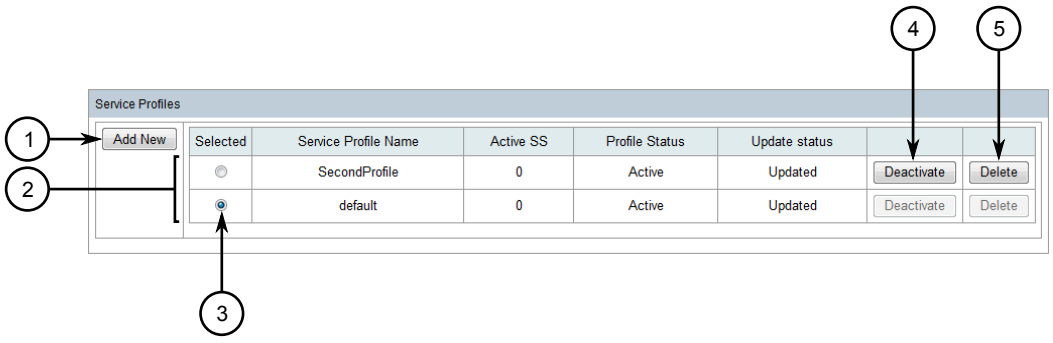


Figure 429: Service Profiles Table

1. Add New Button **2.** Available Service Profiles **3.** Selected Service Profile **4.** Deactivate Button **5.** Delete Button

3. Click **Add New**. A dialog box appears.

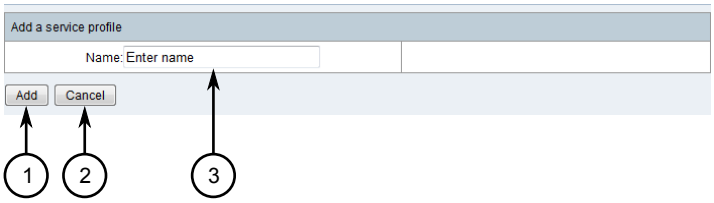


Figure 430: Dialog Box

1. Add Button **2.** Cancel Button **3.** Name Box

4. Under **Name**, type the name of the new service profile, then click **Add**. The dialog box closes and the new service profile is added to the table as the selected profile.

Section 6.12.4.3

Deactivating/Deleting a Service Profile

To deactivate or delete a service profile configured for a specific RUGGEDCOM WIN base station managed by RUGGEDCOM NMS, do the following:

NOTE
*The **default** service profile cannot be deactivated or deleted.*

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

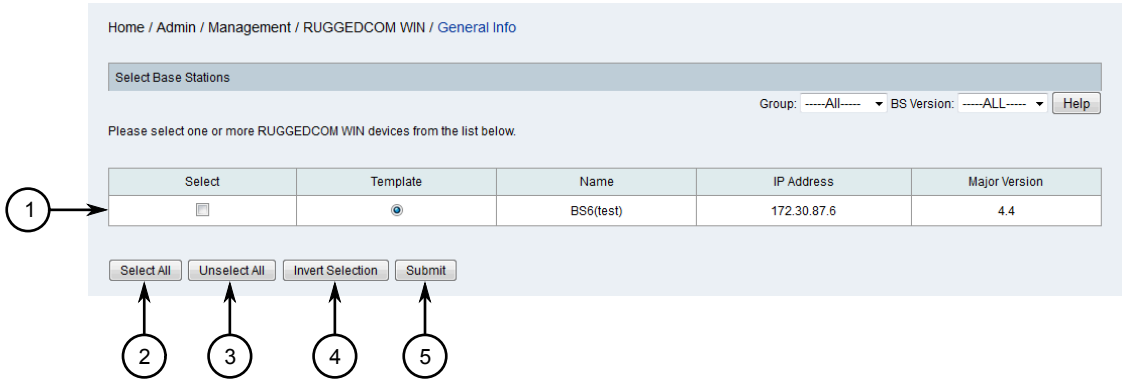


Figure 431: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Service Profiles** table appears.

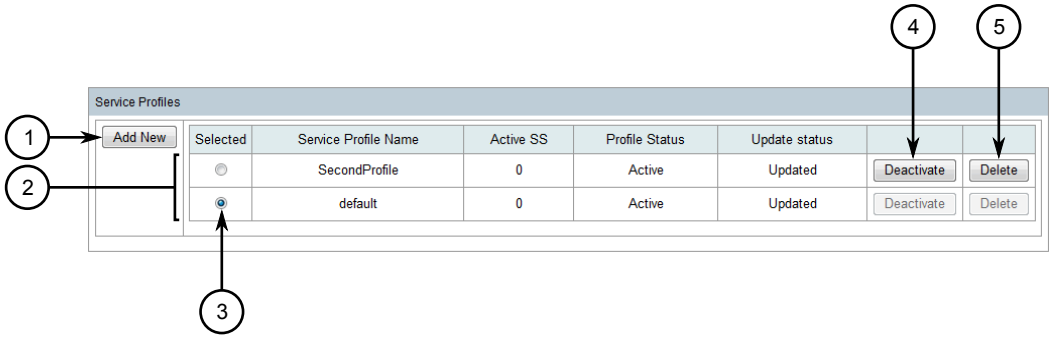


Figure 432: Service Profiles Table

1. Add New Button **2.** Available Service Profiles **3.** Selected Service Profile **4.** Deactivate Button **5.** Delete Button

3. Click either **Deactivate** or **Delete** next to the chosen service profile. A confirmation message appears.
4. Click **OK** to deactivate or delete the service profile.

Section 6.12.5

Managing Base Station Service Flows

This section describes how to configure and manage service flows for base stations managed by RUGGEDCOM NMS.

CONTENTS

Section 6.12.5.1

Viewing a List of Service Flows

To view a list of service flows configured for a specific RUGGEDCOM base station managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

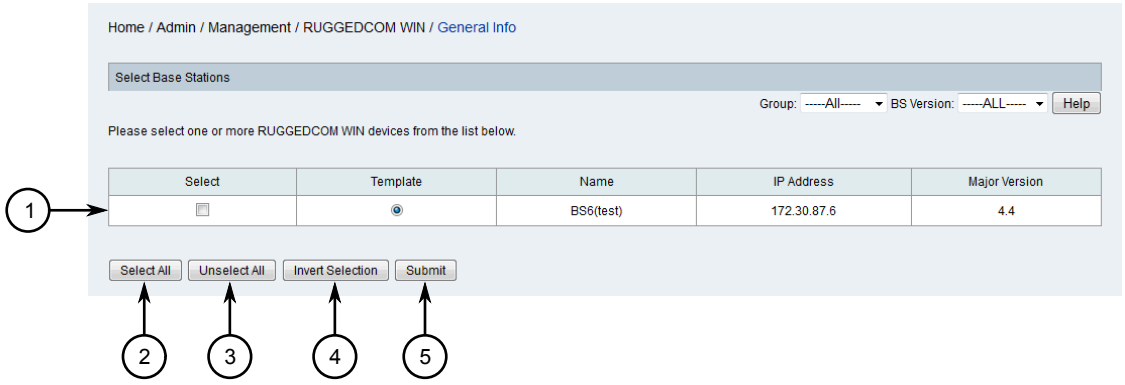


Figure 433: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Service Flow** table appears, listing the available service flows and their individual configuration.

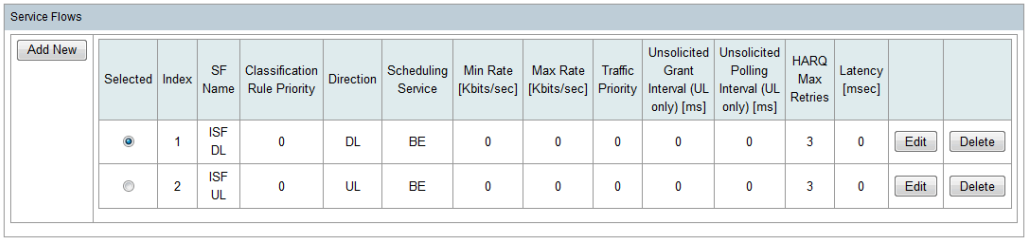


Figure 434: Service Flow Table

Section 6.12.5.2

Adding a Service Flow

To add a service flow to a specific RUGGEDCOM WIN base station, do the following:

NOTE
Up to 30 service flows can be configured per base station.

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

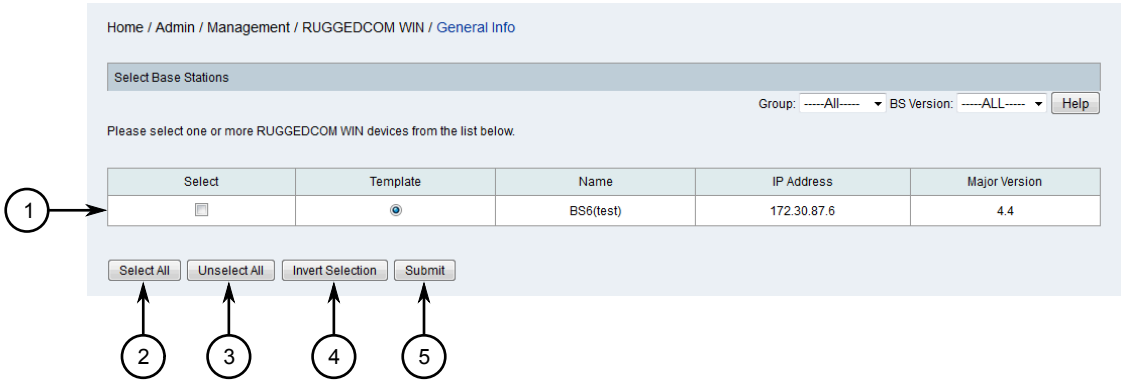


Figure 435: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Service Flows** table appears.

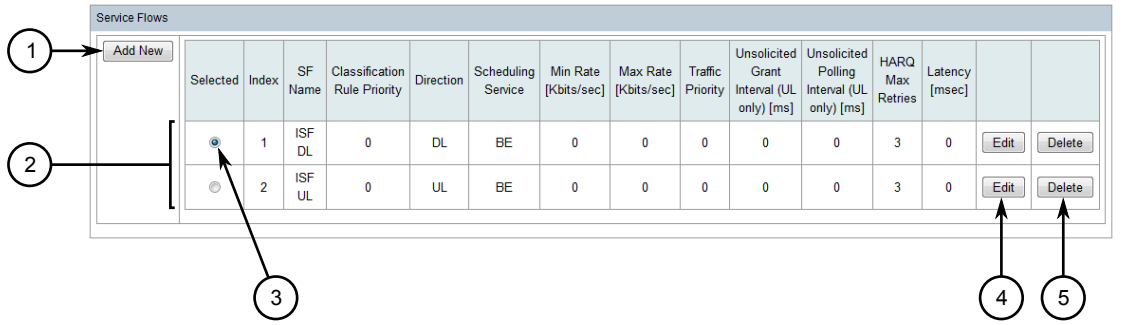


Figure 436: Service Flows Table

1. Add New Button **2.** Available Service Flows **3.** Selected Service Flow **4.** Edit Button **5.** Delete Button

3. Click **Add New**. A dialog box appears.

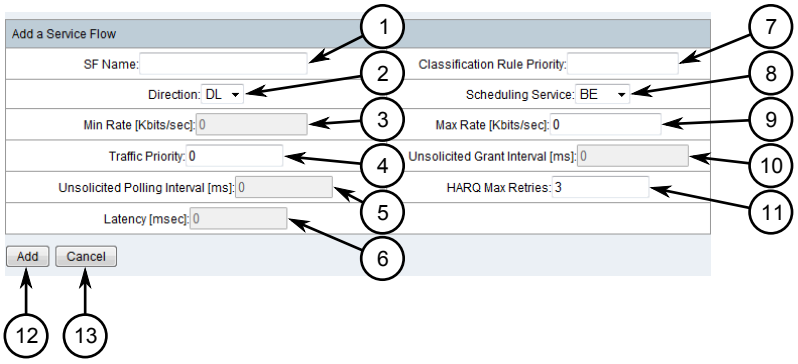


Figure 437: Dialog Box

1. SF Name Box **2.** Direction List **3.** Min Rate Box **4.** Traffic Priority Box **5.** Unsolicited Polling Interval Box **6.** Classification Rule Priority Box **7.** Scheduling Service List **8.** Max Rate Box **9.** Unsolicited Grant Interval Box **10.** HARQ Max Retries Box **11.** Latency Box **12.** Add Button **13.** Cancel Button

4. Configure the following parameters as required:

Parameter	Description
SF Name	The name of the service flow. It is recommended to include the service flow direction (e.g. UL or DL).
Classification Rule Priority	**Synopsis:** 0 to 255 Determines how the service flow data is classified. The same priority can be assigned to an uplink and to a downlink service flow, but the priority must be unique for each. There cannot be two service flows in the same direction with the same rule priority.
Direction	**Synopsis:** { DL, UL } The direction to which the service flow is assigned. Options include: • `DL` – Downlink • `UL` – Uplink
Scheduling Service	The scheduling service. Options include: • `UGS` – Unsolicited Grant Services. Used for Voice over IP (VoIP) without silence suppression. • `RT` – Real-Time polling service. Used for streaming audio and video (MPEG encoded). • `eRT` – Extended-Real-Time polling service. Used for Voice over IP (VoIP) without silence suppression. • `nRT` – Non-Real-Time polling service. Used for file transfers via FTP (File Transfer Protocol). • `BE` – Best Effort service. Used for Web browsing and data transfer.
Min Rate	The minimum bandwidth rate in bits/second (bps) for the service flow.
Max Rate	The maximum bandwidth rate in bits/second (bps) for the service flow.
Traffic Priority	The priority of the service flow over others.

Parameter	Description
Unsolicited Grant Interval	The interval in milliseconds (ms) between successive grant opportunities for the flow of uplink traffic. For RT (Real-Time) and nRT (Non-Real Time) polling only.
Unsolicited Polling Interval	The interval in milliseconds (ms) between successive polling grant opportunities for the flow of uplink traffic. For UGS (Unsolicited Grant Service) and eRT (Extended Real Time) polling only.
HARQ Max Retries	The maximum number of Hybrid Automatic Repeat Request (HARQ) attempts.
Latency	The maximum latency in milliseconds (ms) allowed starting at the arrival of a packet and until its successful transmission to its destination.

5. Click **Add**. The dialog box closes and the new service flow is added to the table as the selected service flow.
6. [Optional] Configure one or more classifiers to determine the traffic to which the service flow is applied. For more information, refer to Section 6.12.6.2, "Adding a Classifier" .

Section 6.12.5.3
Deleting a Service Flow

To delete a service flow configured for a specific RUGGEDCOM WIN base station managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

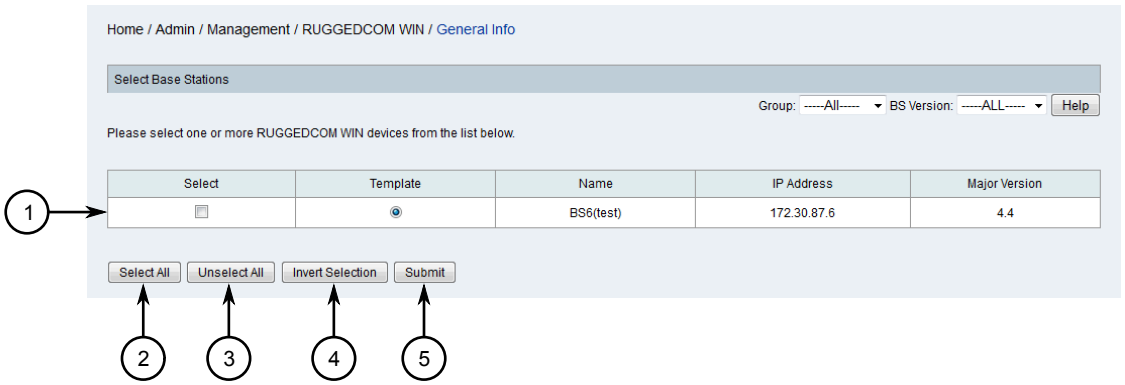


Figure 438: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Service Flow** table appears.

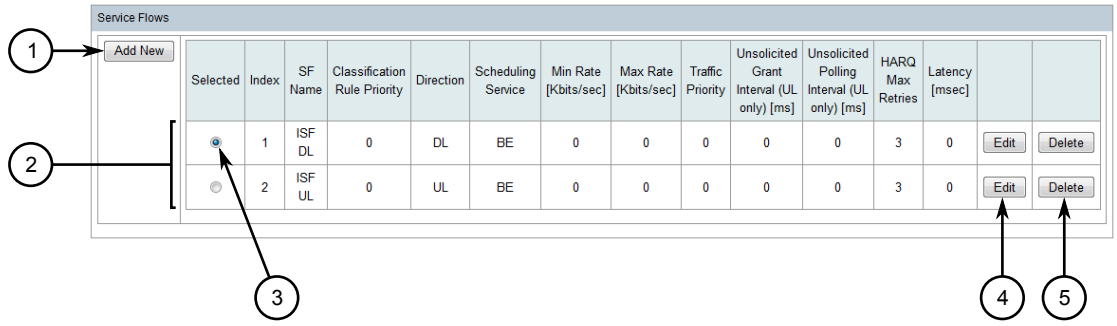


Figure 439: Service Flow Table

1. Add New Button **2.** Available Service Flows **3.** Selected Service Flow **4.** Edit Button **5.** Delete Button

3. Click **Delete** next to the chosen service flow. A confirmation message appears.
4. Click **OK** to delete the service flow.

Section 6.12.6

Managing Base Station Classifiers

Classifiers determine the traffic to which service flows are applied. Traffic can be defined according to the traffic source, traffic type, or combination of traffic source and type. For example, traffic can be defined by DSCP range, port range, IP address source or destination, and other parameters. The base station performs a logical OR when considering traffic types.

CONTENTS

Section 6.12.6.1

Viewing a List of Classifiers

To view a list of classifiers configured for a specific RUGGEDCOM base station managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

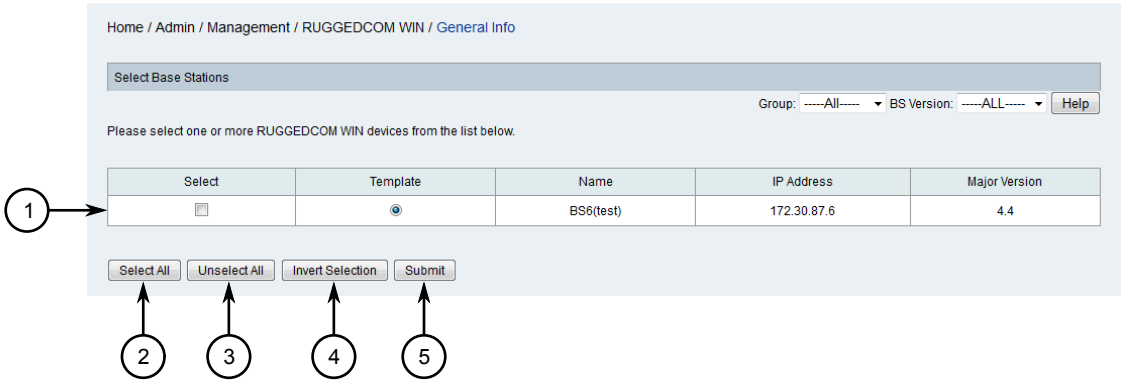


Figure 440: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Classifiers** table appears, listing the available classifiers and their types.

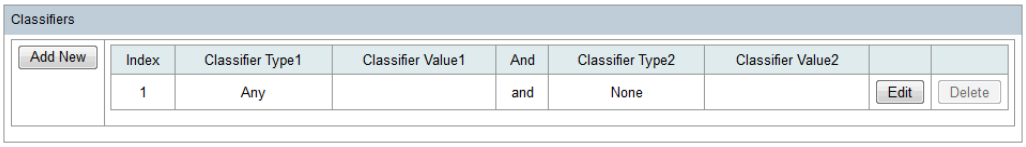


Figure 441: Classifier Table

Section 6.12.6.2
Adding a Classifier

To add a classifier to a specific RUGGEDCOM WIN base station, do the following:

NOTE
Up to 4 classifiers can be configured per base station.

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

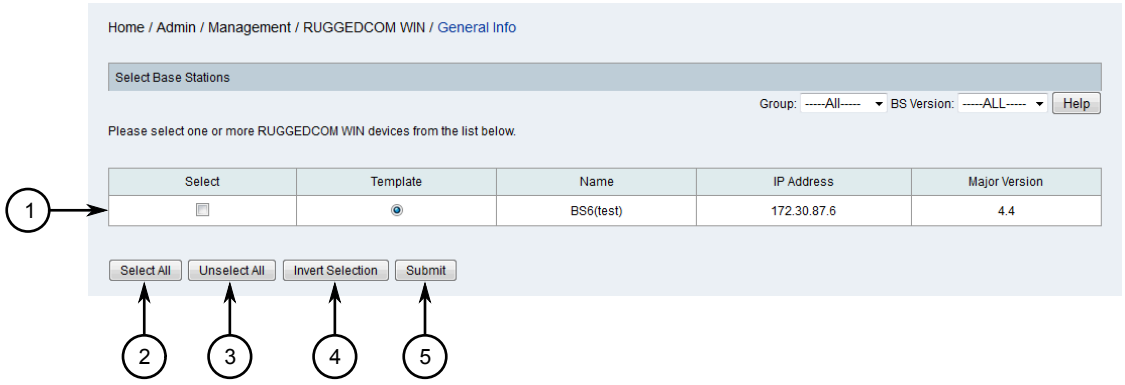


Figure 442: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Classifiers** table appears.

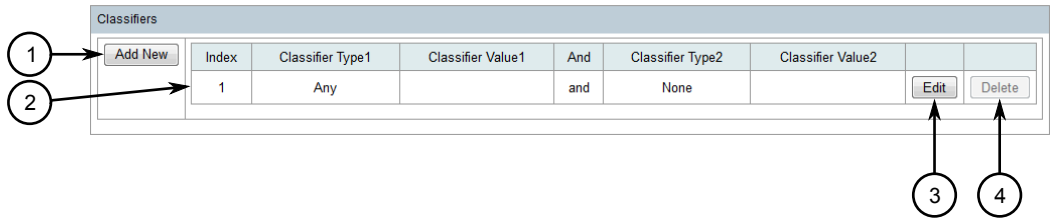


Figure 443: Classifiers Table

1. Add New Button **2.** Available Classifiers **3.** Edit Button **4.** Delete Button

3. Click **Add New**. A dialog box appears.

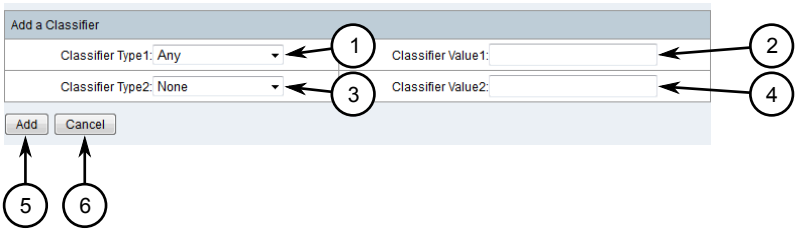


Figure 444: Dialog Box

1. Classifier Type1 List **2.** Classifier Value1 Box **3.** Classifier Type2 List **4.** Classifier Value2 Box **5.** Add Button **6.** Cancel Button

4. Configure up to two classifier types and their values. Options include:
   - `Any` – Any classifier type and value.
   - `None` – No classifier type or value.

- `MAC src` – A source MAC address with an optional subnet mask (e.g. 11:22:33:44:55:66/48). The default mask is *48*.
- `MAC dest` – A destination MAC address with an optional subnet mask (e.g. 11:22:33:44:55:66/48). The default mask is *48*.
- `IP src` – A source IP address with an optional subnet mask (e.g. 192.168.1.1/32). The default mask is *32*.
- `IP dest` – A destination IP address with an optional subnet mask (e.g. 192.168.1.1/32). The default mask is *32*.
- `Port src` – A source port or port range (e.g. 1230-1250).
- `Port dest` – A destination port or port range (e.g. 1230-1250).
- `DSCP` – A DSCP (Differentiated Services Code Point) range mask in the form of *toslow:toshigh:tosmask* (e.g. 13:57:63). The DSCP is the first six bits of the TOS (Type of Service) byte of the IP packet header.
- `IP protocol` – The value of the IP header field determining the upper layer protocol, such as TCP, UDP and others. Accepted values are between 0 and 255. A value of 6 represents TCP.

5. Click **Add**. The dialog box closes and the new classifier is added to the table.

Section 6.12.6.3

Deleting a Classifier

To delete a classifier configured for a specific RUGGEDCOM WIN base station managed by RUGGEDCOM NMS, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, click **RUGGEDCOM WIN BS Configuration Management**, and then click **Configure Base Station General Information**. The **General Info** screen appears.

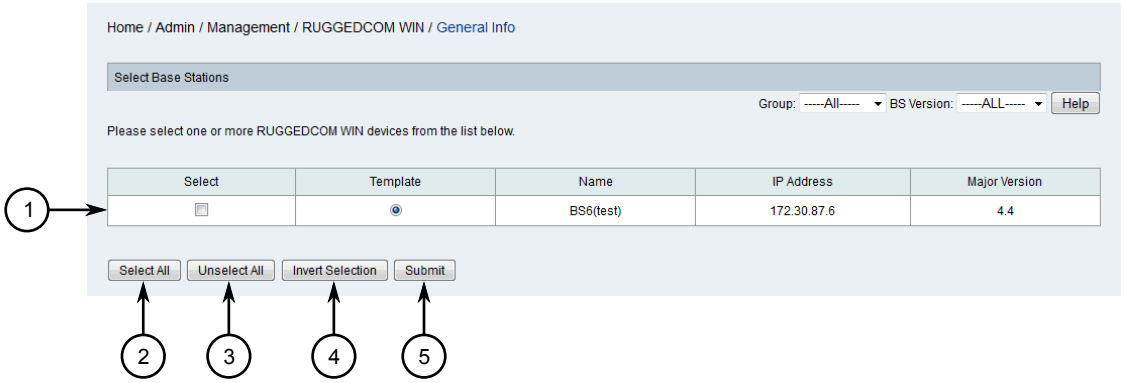


Figure 445: General Info Screen

1. Available Base Station Devices **2.** Select All Button **3.** Unselect All Button **4.** Invert Selection Button **5.** Submit Button

2. Select one or more devices and then click **Submit**. The **Classifiers** table appears.

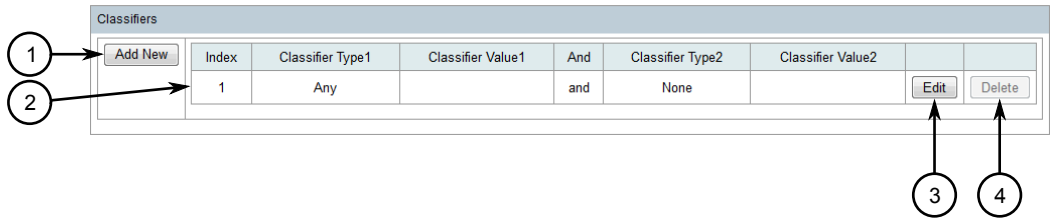


Figure 446: Classifiers Table

1. Add New Button **2.** Available Classifiers **3.** Edit Button **4.** Delete Button

3. Click **Delete** next to the chosen classifier. A confirmation message appears.
4. Click **OK** to delete the classifier.

Section 6.12.7

Setting the Active Partition

Each RUGGEDCOM WIN base station device supports two partitions that house a version of the operating system firmware. The partition containing the active software image is considered the Primary partition, with the Secondary partition housing an older or newer version of the software.

To set the current partition as the active partition or switch to the software image in the other partition, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, and then click **RUGGEDCOM WIN Base Station Software Control**. The **Software Control** screen appears.

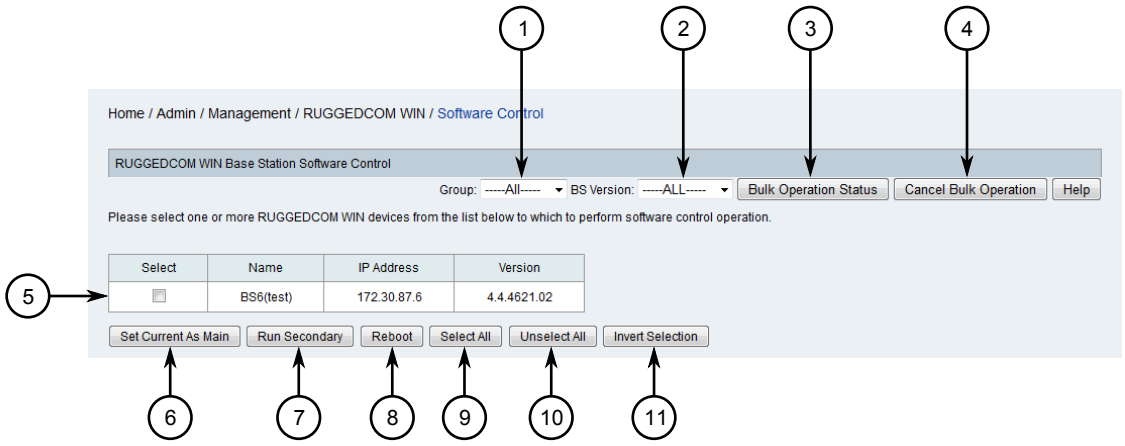


Figure 447: Software Control Screen

1. Bulk Operation Status Button **2.** Cancel Bulk Operation Button **3.** Available Base Station Devices **4.** Set Current As Main Button **5.** Run Secondary Button **6.** Reboot Button **7.** Select All Button **8.** Unselect All Button **9.** Invert Selection Button

2. Select one or more base station devices and then either:

- Click **Set Current As Main** followed by **Reboot** to set the software image currently running on each device as the main or primary image.
- Click **Run Secondary** to reboot the device(s) and load the secondary or backup software image.

The current, real-time status of the operation is displayed in the status bar. For more detailed information, click **Bulk Operation Status**. A dialog box appears displaying the detailed status of the operation for each selected device.

3. [Optional] To cancel the operation, click **Cancel Bulk Operation**.

Section 6.12.8
Managing Files on WIN Base Station Devices

RUGGEDCOM NMS can control the following file types on any RUGGEDCOM WIN base station device it manages:

File Type	Description
SW Package	The base station software package, which includes all software images and configuration files.
CDC	The CDC (Common Default Configuration) configuration file, which contains configuration items common to all RUGGEDCOM WIN base station devices.
UV	The UV (Unique Values) configuration file, containing configuration items specific to individual RUGGEDCOM WIN base station devices.

CONTENTS

Section 6.12.8.1
Copying a File

To copy a file from the primary partition to the secondary partition, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, and then click **RUGGEDCOM WIN Base Station File Control**. The **File Control** screen appears.

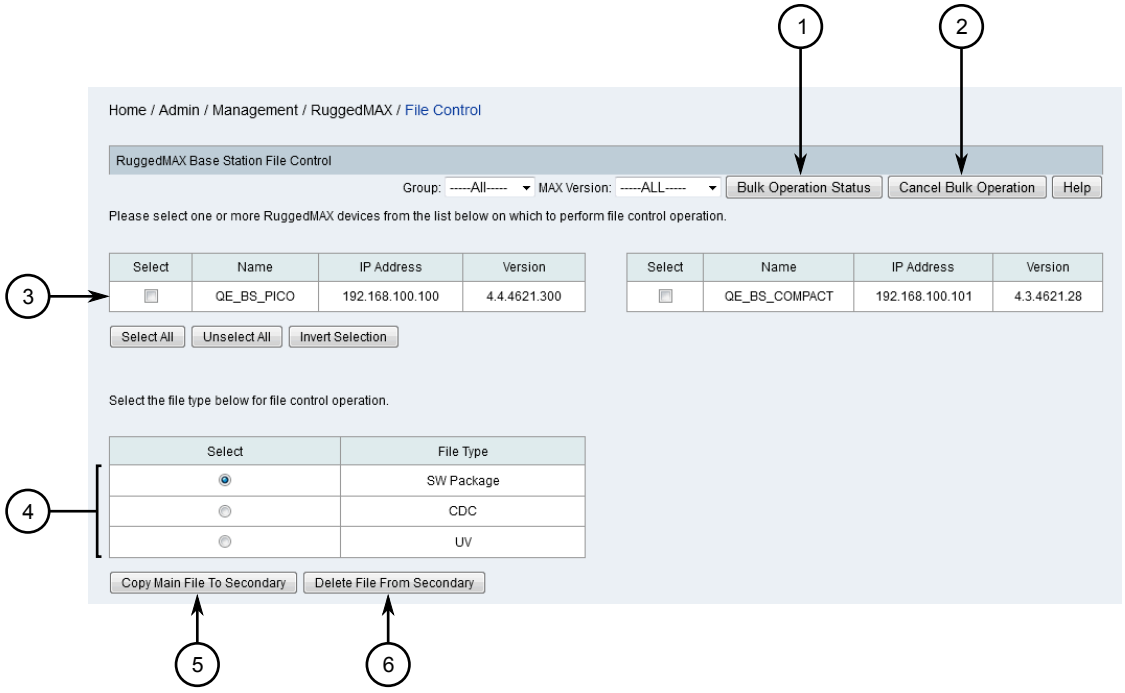


Figure 448: File Control Screen

1. Bulk Operation Status Button **2.** Cancel Bulk Operation Button **3.** Available Base Station Devices **4.** File Type Options **5.** Copy Main File to Secondary Button **6.** Delete File From Secondary Button

2. If a file of the same type already exists on the secondary partition, delete it. For more information, refer to Section 6.12.8.2, "Delete a File" .
3. Select on or more base station devices.
4. Select the file type. For more information about the available files types, refer to Section 6.12.8, "Managing Files on WIN Base Station Devices" .
5. Click **Copy Main File to Secondary**. RUGGEDCOM NMS begins moving the selected file type from the primary partition to the secondary partition for the selected device(s).

   The current, real-time status of the operation is displayed in the status bar. For more detailed information, click **Bulk Operation Status**. A dialog box appears displaying the detailed status of the operation for each selected device.
6. [Optional] To cancel the operation, click **Cancel Bulk Operation**.

Section 6.12.8.2
Delete a File

To delete a file from the secondary partition, do the following:

1. On the menu bar, click **Admin**, click **RUGGEDCOM NMS Configuration Management**, click **RUGGEDCOM WIN Base Station Management**, and then click **RUGGEDCOM WIN Base Station File Control**. The **File Control** screen appears.

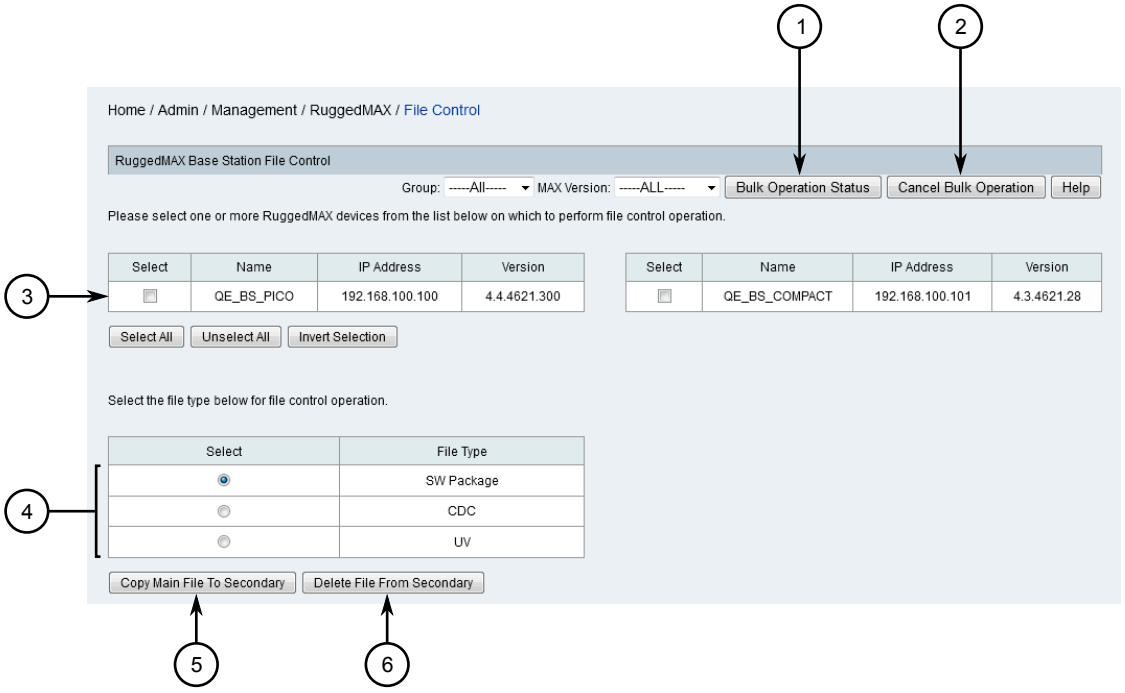


Figure 449: File Control Screen

1. Bulk Operation Status Button **2.** Cancel Bulk Operation Button **3.** Available Base Station Devices **4.** File Type Options **5.** Copy Main File to Secondary Button **6.** Delete File From Secondary Button

2. Select on or more base station devices.
3. Select the file type. For more information about the available files types, refer to Section 6.12.8, “Managing Files on WIN Base Station Devices” .
4. Click **Delete File From Secondary**. RUGGEDCOM NMS begins deleting the selected file type from the secondary partition on the selected device(s).

   The current, real-time status of the operation is displayed in the status bar. For more detailed information, click **Bulk Operation Status**. A dialog box appears displaying the detailed status of the operation for each selected device.
5. [Optional] To cancel the operation, click **Cancel Bulk Operation**.