JUNOS™ Software

JUNOScope Software User Guide

Release 9.5

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-029336-01, Revision 1

JUNOS™ Software JUNOScope Software User Guide
Release 9.5

Writing: Paka Sheryll Marion Sampson
Editing: Stella Hackell
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
13 April 2009—530–029336–01 Revision 1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

Table of Contents

Part 3 Modifying JUNOScope Software Settings

Part 7 Performing Inventory Management

Part 9 Device Operational Monitoring Tools

Part 10 Device Configuration Management Tools

Part 11 JUNOScope Window and Dialog Box Reference

Part 14 Integrating External Web Applications with JUNOScope

Part 15 Index

List of Figures

List of Tables

About This Guide

This preface provides the following guidelines for using the *JUNOS™ Software JUNOScope Software User Guide*:

JUNOS Documentation and Release Notes

For a list of related JUNOS documentation, see http://www.juniper.net/techpubs/software/junos/.

If the information in the latest *JUNOS Release Notes* differs from the information in the documentation, follow the *JUNOS Release Notes*.

To obtain the most current version of all Juniper Networks technical documentation, see the product documentation page on the Juniper Networks Web site at http://www.juniper.net/.

Table 1 on page xxxvii lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at http://www.juniper.net/books.

Table 1: Additional Books Available Through http://www.juniper.net/books

Book	Description
Interdomain Multicast Routing	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.

Table 1: Additional Books Available Through http://www.juniper.net/books *(continued)*

Book	Description
JUNOS Cookbook	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
MPLS-Enabled Applications	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.
OSPF and IS-IS: Choosing an IGP for Large-Scale Networks	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks.
Routing Policy and Protocols for Multivendor IP Networks	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.
The Complete IS-IS Protocol	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

Objectives

This guide provides a reference for you to install, set up, and use the JUNOScope software. The JUNOScope software is a Juniper Networks network management application that lets you configure and monitor Juniper Networks routers on your network.

NOTE: For additional information about the JUNOS software—either corrections to or information that might have been omitted from this guide—see the software release notes at http://www.juniper.net/.

Audience

This guide is designed for the JUNOScope software administrator and those who have access to manage Juniper Networks J-series, M-series, MX-series, or T-series routing platforms.

To use this guide, you should have good UNIX (Solaris) system administration skills, database administration skills (MySQL), an understanding of the JUNOS command-line

interface (CLI), and a knowledge of the JUNOScript application programming interface (API).

In addition, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

Supported Routing Platforms

For the features described in this manual, the JUNOS software currently supports the following routing platforms:

- J-series
- M-series
- MX-series
- T-series

Using the Indexes

This reference contains a standard index with topic entries.

Documentation Conventions

Table 2 on page xl defines notice icons used in this guide.

Table 2: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 3 on page xl defines the text and syntax conventions used in this guide.

Table 3: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic text like this	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric *metric*>;

Table 3: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast | multicast (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [*community-ids*]

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	■ In the Logical Interfaces box, select **All Interfaces**. ■ To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols > Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs])*

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html.

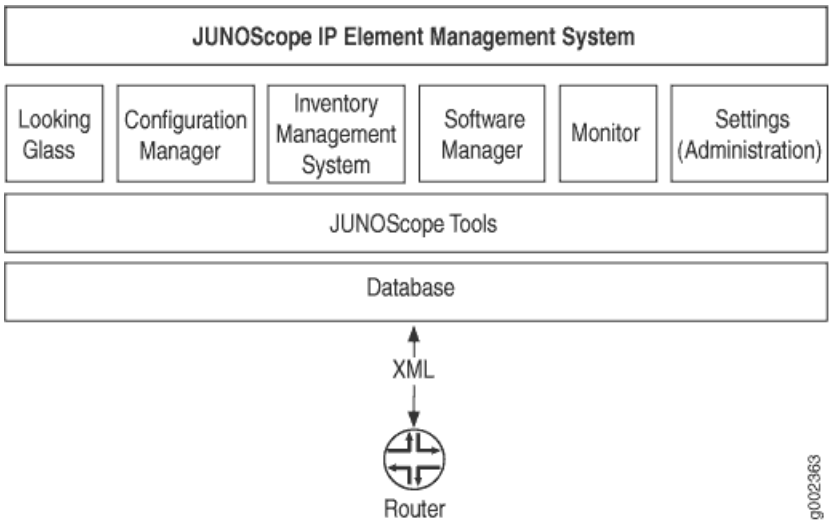
Part 1
JUNOScope Software Overview

Chapter 1

JUNOScope Software Overview

This chapter provides an overview of the JUNOScope software, an element management application that provides tools for managing IP services for configured devices on the network, such as the J-series, M-series, MX-series, and T-series routing platforms. (See Figure 1 on page 3.)

Figure 1: JUNOScope Software Element Management Tools



JUNOScope element management tools include:

- Looking Glass for viewing real-time operational, diagnostics, and troubleshooting information for a selected device.
- Configuration Manager for managing current and archived device configurations. The Web-based Configuration Browser lets you view the current device configuration. The Web-based Configuration Editor lets you edit the current device configuration. The repository tools let you archive and import device configurations, and store them in the JUNOScope CVS repository. Other repository tools let you manipulate the archived configuration and manage JUNOS-based scripts such as commit scripts, operation (op) scripts, and event scripts.
- Inventory Management System for scanning the inventory, such as software, license, and hardware, on selected devices on the network. The Inventory Management System also allows you to view predefined reports or generate

custom reports. The system also includes a demo database from which you can generate demo reports.

- Software Management for managing the download, installation, and deployment of software images in a network.
- Provisioning for configuring MPLS and GRE tunnels and provisioning pseudowires.
- Monitor for viewing and managing scheduled and pending operations, the final status of completed tasks, and all authentication activities and privileged operations performed by authorized users. The Monitoring tool lets you purge status and log records that are no longer needed.
- Settings (Administration) for modifying JUNOScope system settings that affect its operation.

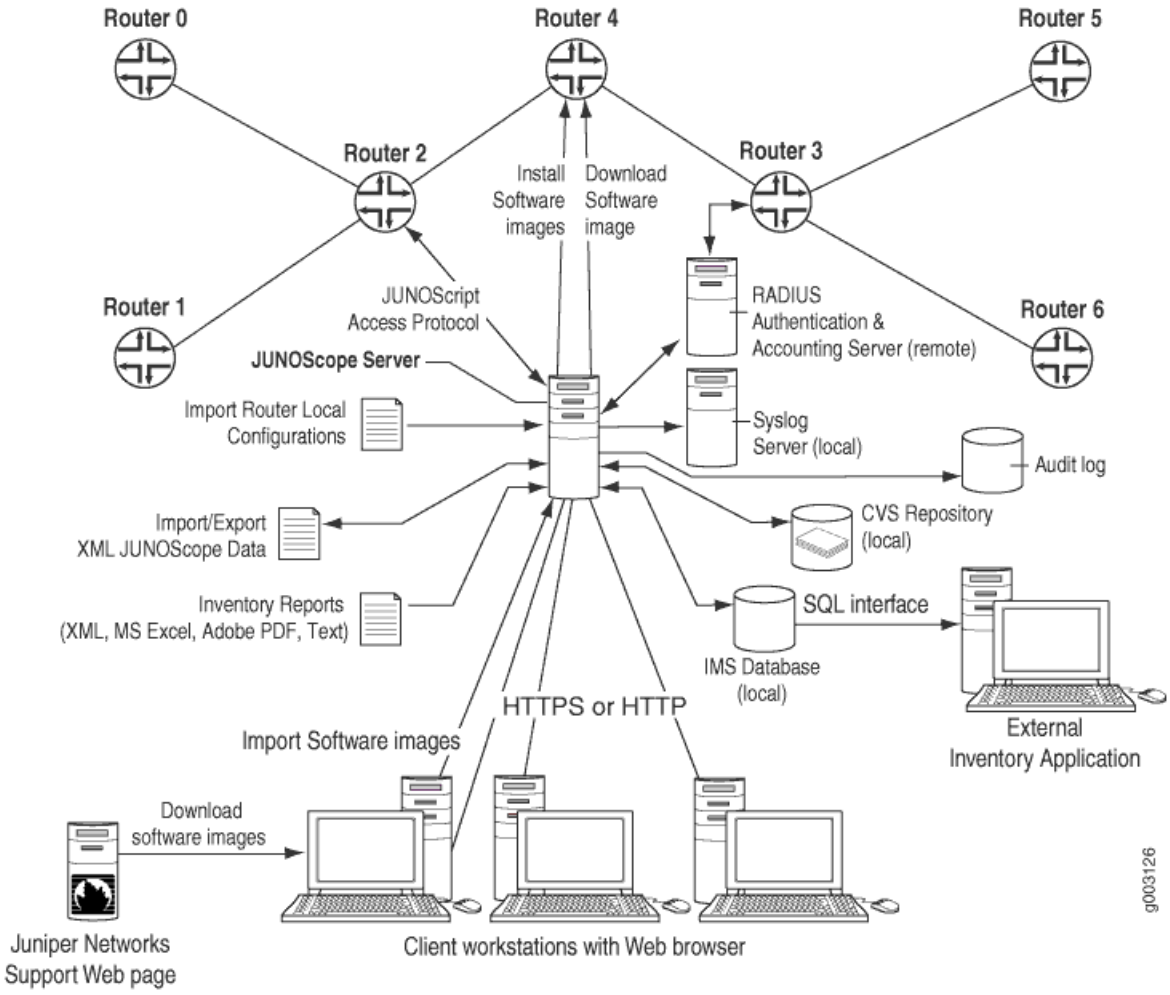
The following topics provide an overview of the JUNOScope software:

- JUNOScope Software Architecture on page 4
- Licensed JUNOScope Modules on page 6
- JUNOScope Software Features on page 7

JUNOScope Software Architecture

The JUNOScope software is a Web server application that runs on a UNIX workstation. You can connect to the JUNOScope software and log in from a client workstation running a Microsoft Internet Explorer 6 or Netscape Navigator 6 Web browser or later with JavaScript enabled. JUNOScope accepts Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) or Hypertext Transfer Protocol (HTTP) connections. (See Figure 2 on page 5.)

Figure 2: JUNOScope Software Architecture



The JUNOScope software includes a Structured Query Language (SQL) database for storing the data collection. The JUNOScope software is bundled with MySQL, a relational database management system (RDBMS) which provides an SQL interface for extracting Inventory Management System information to an external inventory application. The JUNOScope software also includes a Concurrent Versions System (CVS) repository for archiving revisions of configuration files.

The JUNOScope software is a client of the JUNOScript server that runs on the router. The JUNOScope software connects to the JUNOScript server, which allows connection to routers using JUNOScript-specific access protocols, such as secure sockets layer (SSL) (a protocol for sending encrypted text over a Transmission Control Protocol [TCP] connection), and clear-text. The JUNOScope software uses the JUNOScript application programming interface (API) to interact with the router, sending and receiving information in Extensible Markup Language (XML) for operations such as archiving, restoring, and browsing a configuration file, and obtaining router operational status information.

The JUNOScope software connects to Juniper Networks J-series, M-series, MX-series, and T-series routing platforms running the current JUNOS software release and including at least two previous releases. Starting Release 9.3, JUNOScope software also supports devices running BXOS software.

NOTE: JUNOScope features such as Looking Glass, transfer on commit, partial config audit, config editor, config view, deploy scripts, and disable scripts are not supported on BXOS devices.

The JUNOScope software provides security between the client and the server. MD5 RSA certification is available between the JUNOScope server and the client Web browser. All communication is encrypted between the client Web browser and the JUNOScope server. The JUNOScope software installation creates an X.509 digital certificate for the HTTPS server. The JUNOScope software administrator can use self-assigned certificates or have one assigned by a trusted certificate authority.

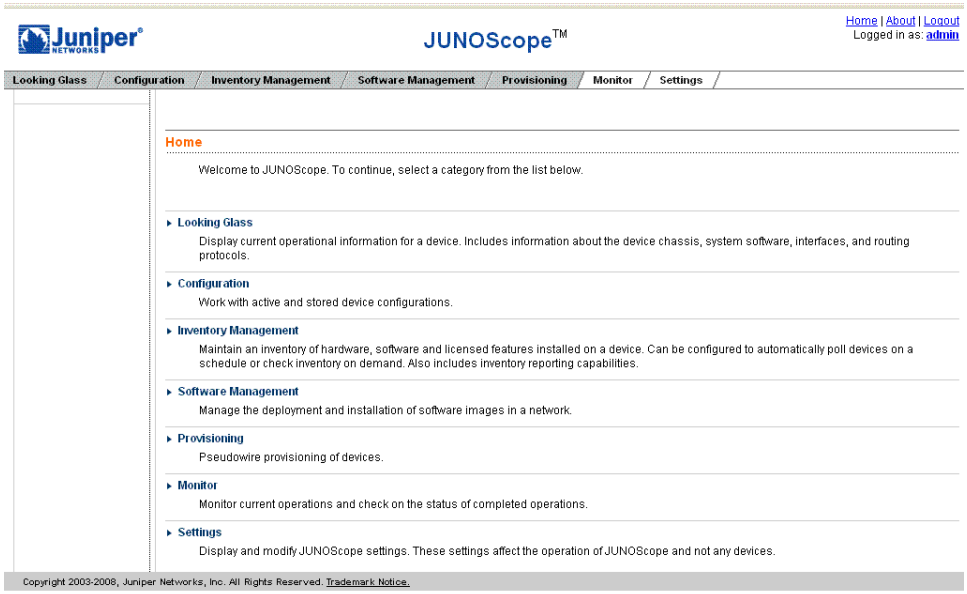
The JUNOScope software installer installs the JUNOScope software. The installer owns the installation and has privileges to upgrade and reconfigure.

The JUNOScope installation program creates an administrator account that allows the JUNOScope administrator to log in to the software and set up systems settings that control how the software operates. See “Settings” on page 14.

Licensed JUNOScope Modules

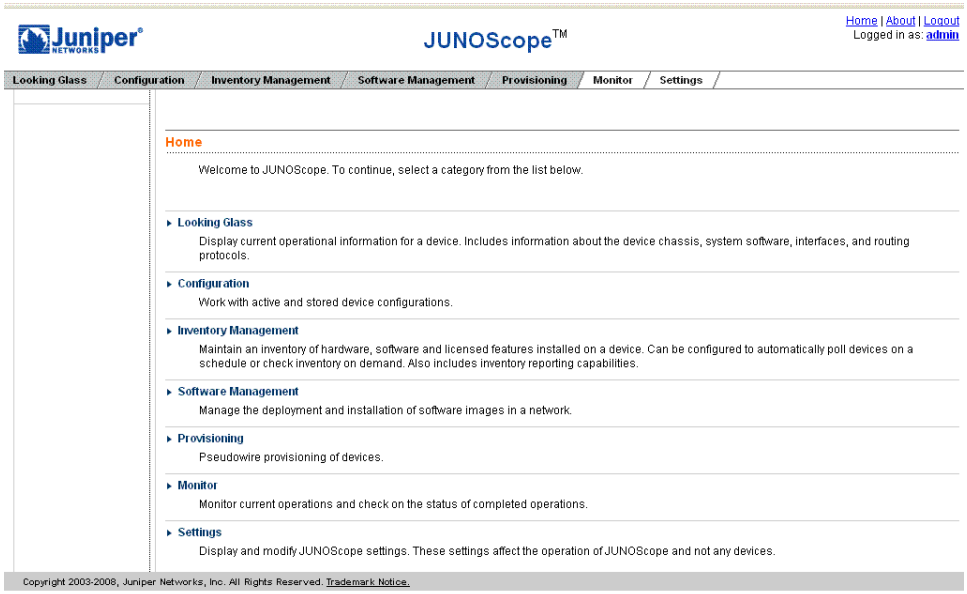
Some JUNOScope software modules, such as Looking Glass, Configuration Management, Inventory Management, Provisioning, and Software Management, are available only if they are licensed and if the software administrator has installed them. If a software module is not installed, it is disabled (unavailable) on the JUNOScope main window, and you cannot use it.

In the JUNOScope main window shown below, Looking Glass and Software Manager are neither licensed nor installed.



JUNOScope Software Features

The main window is displayed when you log in to the software using a Web browser on a client workstation. The main window includes the main command links to all of the various JUNOScope software modules. For more information about the parts of the JUNOScope main window, see Figure 17 on page 439.



The JUNOScope software provides the following main modules. They appear as main command menus and as tabs in the JUNOScope software user interface. Each main menu has a set of submenus that correspond to administrator or user tasks.

- Looking Glass on page 8
- Configuration Management on page 9
- Inventory Management on page 11
- Software Manager on page 13
- Provisioning on page 13
- Monitor on page 13
- Settings on page 14

Looking Glass

The Looking Glass module provides a graphical user interface (GUI) for querying and viewing device status and troubleshooting information from connected devices, including router chassis, system management, Adaptive Services (AS) Physical Interface Card (PIC), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Multiprotocol Label Switching (MPLS), and Resource Reservation Protocol (RSVP) status information. For more information about Looking Glass, see “Using Looking Glass” on page 417.

Configuration Management

The JUNOScope software configuration management module lets users manage device configurations that are currently running on connected devices and configurations that have been archived or imported in the JUNOScope CVS repository.

Current

The configuration management module lets you view and edit current device configurations using the Configuration Browser and the Configuration Editor.

Configuration Browser

(Configuration > Current > View) Provides a GUI for viewing the setup of the currently committed configuration that is running on a selected device. Use the Configuration Browser to view the configuration statement hierarchy in brief or detailed mode, including viewing statement inheritance. For more information, see "Using the Configuration Browser" on page 425.

Configuration Editor

(Configuration > Current > Edit) Provides a GUI for editing a configuration on a selected device. Use the Configuration Editor to modify the existing configuration. You can also use the Configuration Editor to commit the modified configuration, as well as discard any unwanted configuration changes. If a device has redundant Routing Engines, committed changes will be synchronized on both the master and backup. For more information, see "Using the Configuration Editor" on page 431.

Repository

The configuration management module lets you archive and import devices configurations into the JUNOScope CVS repository. The repository holds version of device configurations. Each device can have many different versions of a configuration in the repository. Once a device configuration version is stored in the JUNOScope repository, you can manipulate it, including tag, audit, compare, display, or restore.

Archive

(Configuration > Repository > Archive) Lets you download the active configuration file from a device or group of devices. The downloaded version of the configuration file is archived in the JUNOScope software CVS repository. You can save configuration archive operations and combine them with other operations, such as restore and inventory scan, to be run concurrently or sequentially in real time or at a scheduled interval. For more information, see "Archiving and Manipulating Device Configurations" on page 193.

Archive Tags

(Configuration > Repository > Archive Tags) Lets you associate tags with a configuration version so you can compare it with another version. The comparison

can be made with the active or current configuration or with a version from the JUNOScope CVS repository. For more information about tagging device configurations, see “Setting Up Archived Configuration Tags and Auditing Configurations and Partial Configurations” on page 209.

Audit Configurations

(Configuration > Repository > Audit Configurations) Lets you check for differences between device configuration versions in the JUNOScope CVS repository for one or more devices. For more information about auditing differences in device configurations, see “Setting Up Archived Configuration Tags and Auditing Configurations and Partial Configurations” on page 209.

Compare

(Configuration > Repository > Compare) Lets you compare the differences between the contents of two revisions of a configuration file that you select in JUNOScope. By default, the JUNOScope software compares the newer revision of a configuration file to an older one. You can also select to compare an older revision of a configuration file with a newer one. For more information, see “Comparing Configuration Files” on page 225.

Display

(Configuration > Repository > Display) Displays the contents of a configuration file revision that you select in JUNOScope. For more information, see “Displaying a Configuration File” on page 237.

Transfer on Commit

(Configuration > Repository > Transfer on Commit) Lets you configure devices to transfer its currently active configuration to JUNOScope each time a candidate configuration is committed. For more information, see “Configuring the JUNOScope Server for Transfer on Commit” on page 200.

Import

(Configuration > Repository > Import) Lets you import into JUNOScope a portion or all of a device configuration that you have saved in ASCII file format to a file on the local file system. The imported configuration is stored in the CVS repository. You can then compare, display, or restore the imported configuration. For more information about importing configuration files, see “Importing and Deleting Configuration Files” on page 229.

Restore

(Configuration > Repository > Restore) Uploads an archived configuration file to the device from which it was archived or uploads an imported configuration to a selected device. JUNOScope locks the device configuration and loads the new configuration on the device, overriding or merging (discarding) the old configuration. JUNOscope issues a commit confirmed command and a commit-configuration JUNOScript

XML tag command. If the target device has installed and configured dual Routing Engines, JUNOScope issues a commit synchronize command. JUNOScope then unlocks the configuration. If an error occurs, JUNOScope issues a rollback command, causing the configuration to revert to the last saved configuration.

You can save configuration restore operations and combine them with other operations, such as archive and inventory scan, to be run concurrently or sequentially in real time or at a scheduled interval.

For more information, see "Restoring a Configuration File" on page 241.

Delete

(Configuration > Repository > Delete) Lets you delete user imported configuration files from the JUNOScope CVS repository. For more information see "Importing and Deleting Configuration Files" on page 229.

Save

(Configuration > Repository > Save) Lets you save archived configurations to a local file system. For more information see "Archiving and Manipulating Device Configurations" on page 193.

Edit

(Configuration > Repository > Edit) Lets you edit an archived configuration file. For more information see "Archiving and Manipulating Device Configurations" on page 193.

Scripts

(Configuration > Repository > Scripts) Lets you Lets you manage JUNOS-based scripts. JUNOS-based scripts such as commit scripts, operation (op) scripts, and event scripts can be imported into the JUNOScope CVS repository from the local file system and deployed to a group of routers.You can also view, edit, compare, and disable these scripts. For more information see "Managing JUNOS Scripts" on page 249.

Inventory Management

The Inventory Management System module consists of two main features: Scan and Reports.

If the Inventory Management System software module is not licensed for use, the JUNOScope software administrator should select not to install it. If this software module is not installed, it is disabled (unavailable) in the JUNOScope main window.

An external inventory application can connect to the Inventory Management System database and extract inventory data, such as hardware, software, licensed features, and inventory scan events, from the database by way of a Structured Query Language (SQL) interface. A unique username and password must be configured during the

JUNOScope software installation to enable read-only access to the Inventory Management System database.

The Inventory Management System includes Demo reports generated from a demonstration database so you can learn how to use report features with having to actually scan device inventory on the production network.

Scan

The Scan feature scans the inventory of one or more selected devices for hardware, software feature licenses, and JUNOS software and its installed packages. The Inventory Management System scans devices in real time or as part of a scheduled operation. You can save inventory scan operations and combine them with other operations, such as archive and restore, to be run concurrently or sequentially in real time or at a scheduled interval.

For more information about scanning inventory items on devices, see “Scanning Inventory Data” on page 339.

Reports

Once device inventory has been scanned and stored in the JUNOScope database, you can generate various predefined or user-specified reports. You can manipulate inventory reports using tools to sort, query, and configure columns. You can save custom inventory reports, including user-specified definitions and controls. All JUNOScope users can view and share saved inventory reports. The Inventory Management System displays reports in a browser in HTML, and can also be exported in Extensible Markup Language (XML), comma-separated values (CSV) text, Adobe PDF, and Microsoft Excel formats. For more information, see “Using Inventory Reports” on page 345.

Repository

The Inventory Management System repository allows you to schedule custom inventory reports to run at a specified time without intervention and to view archived custom inventory reports that have been run.

- Schedule—The JUNOScope Inventory Management System now allows you to run custom inventory reports (such as event, hardware, software, and license) at a specified time without intervention. You can schedule custom inventory reports that you save to a filename. You can also save scheduled custom inventory report operations and combine them using Task Manager (Settings > Saved Operations) with other operations, such as archive, restore, inventory scan, install software image, and download software image.
- Repository—You can view scheduled report status using Monitor > Status. Scheduled reports are archived in the Inventory Management System repository for future viewing in Adobe PDF or Microsoft Excel format.

For more information about scheduling and viewing custom inventory reports, see “Scheduling Custom Inventory Reports and Viewing Archived Inventory Reports” on page 369.

Software Manager

Software Manager is a licensable module that controls the deployment and installation of JUNOS software images in a network. Administrators can use Software Manager as the central management point from which to import, download and install software images in a controlled and auditable manner. Used with other JUNOScope features, such as the Task Manager, Scheduler and Inventory Manager, Software Manager allows the administrator to better control how and when JUNOS software images are rolled out in a network. For more information about Software Manager, see "Using the Software Manager" on page 397.

Provisioning

Provisioning is a licensable module that enables you to provision MPLS and GRE tunnels as well as pseudowires for carrying legacy network traffic over MPLS and IP networks. To access Provisioning tab, you must have installed IP Backhaul manager license. Provisioning tab enables you to configure and provision MPLS and GRE tunnels, and to provision, filter, and test pseudowires. For more information about Provisioning, see "Provisioning Pseudowires" on page 281.

Monitor

The JUNOScope monitor operations component lets users perform the following tasks.

Operations

Display a schedule of pending operations that are configured. You can also delete operations. An operation appears in Manage Operations when you use the Configuration > Repository > Archive command and the Inventory Management > Scan command to set an archive schedule for a specified time and interval. An operation is not listed when you schedule an operation using the Now option. For more information, see "Managing Operations" on page 313.

Status

Display the status of all JUNOScope operations run on all devices, groups, or selected devices. You can apply a filter to see only specific operations, such as operations run at a specific time or with a particular status. The JUNOScope operations are listed by device or group name on which the operation occurs, operation status, operation start time, last update time, and any message about the operation. Operation status includes pending, connecting, writing, success, or error. For more information, see "Viewing and Maintaining Operation Status" on page 315.

Audit Log

Display the records of all JUNOScope user authentication activities and privileged operations that are stored in the database. Authentication activities include user logins, login failures, logouts, and session timeouts. Privileged operations are changes of information in the system or network, including configuration commits,

configuration archives, user account additions, user account deletions, password changes, device additions, device deletions, label association changes, and authentication information changes. User authentication activity and privileged operation audit records are also sent as system log messages to the system log server and to an optional RADIUS accounting server if one is configured.

Purge

Delete unwanted records from both the Status and Audit Log tables. The Status Log displays the records of all JUNOScope operations run on all devices, groups, or selected devices. The Audit Log table displays the records of all JUNOScope user authentication activities and privileged operations that are stored in the database. You can filter the records you don't want by specified criteria.

Settings

The JUNOScope system settings component lets the administrator set up the software to work with the following information.

Authentication Information

Specify the authentication information (login and password for accessing a device). The JUNOScope software administrator can chose to have sensitive data encrypted at export. For more information, see "Setting Up Authentication Information" on page 37.

Access Methods

Specify the access method (JUNOScript access protocol to connect to the JUNOScript server running on a device) configured on a device for remotely connecting to that device from the JUNOScope software. The JUNOScope software administrator can chose to have sensitive data encrypted at export. For more information, see "Setting Up Access Methods" on page 45.

Devices

Connect to and discover information about devices on the network. The JUNOScope software performs operations on devices, such as archive, display, compare, or restore. Additionally, the JUNOScope software scans devices for inventory information. You can associate a device with one or more text labels used to statically organize a group of devices for JUNOScope operations. For more information, see "Setting Up Devices" on page 57.

Groups

Group devices for performing immediate or scheduled operations using criteria, such as device name, model, hostname, comment, or label (see "Labels" on page 15). For more information, see "Setting Up Groups" on page 67.

Labels

Labels, in free text format, provide a way to statically associate a group of devices. A label must have a unique name, such as Edge; an optional category name, such as Router Type, so you can logically organize labels; and an optional comment to help you understand the label purpose. You can associate an existing label with one or more devices. You can use a label as a rule in the group criteria wizard for setting up groups of devices. For more information about setting up labels, see "Setting Up Labels" on page 83. For more information about associating a device with a label, see "Setting Up Devices" on page 57. For more information about using a label to create a group, see "Setting Up Groups" on page 67.

Schedules

Specify the time or interval when you want the JUNOScope software to perform operations on one or more devices, such as archive, display, or compare a device configuration, or scan device hardware, software, or licensed feature inventory. For more information, see "Setting Up Schedules" on page 89.

Users

Provides the following user authentication:

- Local Authentication—Set up local accounts and a template account so that local users and users with RADIUS accounts can log in to JUNOScope with the appropriate permissions. For more information, see "Setting Up User Local Authentication" on page 97.
- User Group Authorization—Create user groups of one or more JUNOScope users that have specified permissions and access to devices and device groups configured in the JUNOScope software. The administrator can associate devices and device groups to a user group. User group authentication provides four predefined user groups: administrator, read-write user, read-only user, and nobody. Every user group must be associated with one of permission level: superuser, read-write, read-only, and none. For more information about user group authorization, see "Setting Up User Group Authorizationand Viewing User Permissions" on page 105.
- Authentication Policy—Configure and enforce an authentication policy for each JUNOScope user. The JUNOScope administrator can edit the user authentication policy, including locking the account, specifying maximum login attempts, and setting an access window within which the failed login attempts occur. For more information about authentication policy, see "Editing a User Authentication Policy" on page 133.

RADIUS Configuration

Set up RADIUS server host information so that users with RADIUS accounts can log in to JUNOScope. The JUNOScope administrator can also specify the port to which all user authentication activity and privileged operation audit records are sent. For more information, see "Setting Up RADIUS Configuration" on page 141.

Import/Export All Data

Import or export required JUNOScope database data from or to another JUNOScope server.

Export All

The JUNOScope administrator can now export all JUNOScope data, with the following options for sensitive data:

- Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
- Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export authentication information to another system.
- Export sensitive data unencrypted—Sensitive data is not encrypted at export.

Import All

The JUNOScope administrator can import sensitive data by supplying a key if the data was exported using the " encrypt sensitive data and provide key at import time" method. Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers. The available import method options include ignore, merge, and override.

For more information, see "Importing and Exporting All Settings Data" on page 159.

Saved Operations (Task Manager)

You can save operations such as archive, restore, and inventory scan from devices on the network and reuse them to build compound operations. You can specify the order in which you want these compound operations to be executed. Reusing operations reduces production time and errors.

Use the Task Manager (Setting > Saved Operations) to create compound operations from archive, restore, or inventory operations that you save to reuse later. From Task Manager (the Saved Operations page), you can add compound operations, specify their execution order, run operations in real time or as part of an existing schedule, view simple operation settings. edit the order in which compound operations run (concurrently or sequentially), and delete operations.

Part 2
Installing JUNOScope Software

Chapter 2

Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software

This chapter describes how to install the JUNOScope software to run on a UNIX server in your network, how to connect to the software from a supported Web browser, and how to log in. It also describes how to reinstall, upgrade, and deinstall the software.

The user who installs the JUNOScope software on a Linux server as root must exist in \etc\passwd. This is a MySQL requirement. The JUNOScope installer must provide the JUNOScope software administrator username and password.

This chapter includes the following topics:

JUNOScope Software System Requirements

You can install the JUNOScope software on a UNIX Sun Solaris or Linux server. Ensure that the UNIX server on which you install the JUNOScope software meets the minimum system requirements. For a Sun Solaris server, see Table 4 on page 20. For a Linux server, see Table 5 on page 20.

Sun Solaris Server System Minimum Requirements

Before you install the JUNOScope software on a UNIX Sun Solaris server, ensure that the server meets the minimum system requirements shown in Table 4 on page 20.

Table 4: JUNOScope Minimum Sun Solaris Server System Requirements

System	Minimum Requirement
Operating system	Solaris 5.8 and above
Processor	UltraSPARC III or equivalent
Speed	1.3 GHz or faster
RAM	1 gigabyte (GB)
Free disk space	1 GB

Red Hat Linux Server System Minimum Requirements

Before you install the JUNOScope software on a UNIX Linux server, ensure that the server meets the minimum system requirements shown in Table 5 on page 20. (See also “Red Hat Enterprise Linux ES File Package Requirements” on page 21.)

Table 5: JUNOScope Minimum Linux Server System Requirements

System	Minimum Requirement
Hardware	Red Hat certified hardware platforms
Operating system	Red Hat Enterprise Linux ES version 3 and 4
Processor	Pentium 4 processor
Speed	2.8 GHz or faster
RAM	1 GB
Free disk space	1 GB

NOTE: To receive system log messages from the JUNOScope software, start syslogd in Red Hat Enterprise Linux with the -r option.

Red Hat Enterprise Linux ES File Package Requirements

If a minimal install of Red Hat Enterprise Linux ES is done on the server, the JUNOScope software administrator should ensure that the file packages shown in Table 6 on page 21 are installed for the JUNOScope software to run properly. Each package should be available in a full install of Red Hat Enterprise Linux ES.

Table 6: Red Hat Enterprise Linux ES File Package Requirements

Version	Required File Packages
Red Hat Enterprise Linux ES version 3 (Update 5)	krb5-libs-1.2.7-44.i386.rpm XFree86-libs-4.3.0-81.EL.i386.rpm
Red Hat Enterprise Linux ES version 3 (Update 6)	krb5-libs-1.2.7-47.i386.rpm XFree86-libs-4.3.0-97.EL.i386.rpm
Red Hat Enterprise Linux ES version 4 (Update 1)	compat-libcom_err-1.0-5.i386.rpm krb5-libs-1.3.4-12.i386.rpm xorg-x11-deprecated-libs-6.8.2-1.EL.13.6.i386.rpm xorg-x11-libs-6.8.2-1.EL.13.6.i386.rpm
Red Hat Enterprise Linux ES version 4 (Update 2)	compat-libcom_err-1.0-5.i386.rpm krb5-libs-1.3.4-17.i386.rpm xorg-x11-deprecated-libs-6.8.2-1.EL.13.6.i386.rpm xorg-x11-libs-6.8.2-1.EL.13.6.i386.rpm

To verify that the file package krb5-libs-1.3.4-17.i386.rpm is installed, use the following command:

hostname% **rpm –query –package krb5-lib-1.3.4-17.i386.rpm**

You can install each package individually using rpm, from the original Red Hat Enterprise Linux ES distribution.

To install the file package xorg-x11-libs-6.8.2-1.EL.13.6.i386.rpm, use the following command:

hostname% **rpm –install xorg-x11-libs-6.8.2-1.EL.13.6.i386.rpm**

JUNOScope Software Client Workstation Requirements

Ensure that the client workstation from which you connect to the JUNOScope software is running either Microsoft Internet Explorer 6 or Netscape Navigator 6 or later with JavaScript enabled.

RADIUS Server Requirements

Ensure that the Remote Authentication Dial-In User Service (RADIUS) server complies with RFC 2865.

Prerequisite Information

Before you install the JUNOScope software, you should know the following information:

- The user who installs the JUNOScope software on a Linux server as root must exist in \etc\passwd. This is a MySQL requirement.
- SQL database connection—The JUNOScope default installation uses a locally installed MySQL database for which the default Java Database Connectivity (JDBC) URL is appropriate. If you enter a URL that points to a JDBC database other than the one bundled with the product, it is not supported.
- Information for creating an X.509 digital certificate—The JUNOScope software installation creates an X.509 digital certificate for the HTTPS server. You must provide the following information:
  - Common server name; for example, nms.juniper.net.
  - Organization that runs the server; for example, Juniper Networks, Inc.
  - State or province where the server is located; for example, California.
  - Country where the server is located; for example, a two-letter code such as US.
- JUNOScope software installation directory—By default, the JUNOScope software is installed into the current working directory.
- Recommended Java Runtime patch cluster—The JUNOScope installation recommends the current patch cluster for the JUNOScope software for correct operation. For example, for a workstation running Solaris 5.8, the following patch cluster is required: J2SE_Solaris_8_Recommended Patch Cluster. The patch cluster is available from http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access. Installation must be performed by root. If your workstation does not have the required patch cluster, you can install it after the JUNOScope installation.

Installation Overview

This section provides an overview summary of what happens when you run the JUNOScope software installation program. The installation program does the following:

- Displays the JUNOScope Software License Agreement for you to accept. If you do not accept the agreement, the installation program will not continue.
- Informs you of and recommends the proper Java Runtime patch cluster that must be installed for the UNIX workstation operating system. If your workstation does not have the proper patch cluster, the JUNOScope software will not operate correctly. You can install the patch cluster as root after you install the JUNOScope software.
- Checks the JUNOScope software installation file data integrity and extracts the required files. If a data integrity problem is detected, the installation will not continue.
- Asks whether you want to protect user, group, or all data files.
- Prompts for the HTTPS port that the JUNOScope software Web server uses for its transactions. It is recommended that you use the HTTPS port for communication between the JUNOScope Web browsers and the JUNOScope server.
- Asks whether you want the JUNOScope software Web server to accept insecure HTTP requests and prompts for the HTTP port on which to listen.
- Asks whether you want the JUNOScope software Web server to resolve client addresses.
- Prompts for the JDBC URLs to access the JUNOScope database and the JUNOScope demo database.
- Prompts for the key used to encrypt and decrypt sensitive data.
- Prompts for the password for the JUNOScope software database superuser.
- Prompts for the JUNOScope software database username and password.
- Prompts for the database username and password for the SQL interface to the Inventory Management System.
- Asks whether you want to enable the SQL interface to the Inventory Management System.
- Prompts for the JUNOScope software administrator username and password.
- Confirms whether you want to enable JUNOScope debug logging.
- Prompts for a pipe or syslog logging server facility to indicate how the syslog daemon (syslogd) decides where to send JUNOScope software system log messages it receives. There are eight logging facilities commonly used for syslog, including local0 through local7. The default is local2.
- Generates an X.509 digital certificate to authenticate the JUNOScope HTTPS Web server.
- Confirms whether you want to continue the JUNOScope installation, go back and change existing installation settings, or quit.

- Extracts the database files and generates an X.509 digital certificate with the settings you indicated.
- Prompts you to select to install the JUNOScope software licensed features—such as Looking Glass, Configuration Manager (Configuration menu), or Inventory Management—that you have purchased and are authorized to use. Only the software features that you install will be enabled in the JUNOScope main window.
- Prepares the JUNOScope software database tables, then installs them.
- Initializes and checks the JUNOScope software database.
- Starts Tomcat, an application server from the Apache Software Foundation that executes Java servlets and renders Web pages.

Starting the JUNOScope Software Installation

This section describes how to start the JUNOScope software installation. Before installing the JUNOScope software, ensure that the workstation meets the system requirements (see "JUNOScope Software System Requirements" on page 20). You can download the JUNOScope software from the Juniper Networks Web site.

Downloading the JUNOScope Software from the Juniper Networks Software Web Page

To download the JUNOScope software, follow these steps:

1. Using a Web browser, go to the following location:

   http://www.juniper.net/support/csc/swdist-encr/swdist-jtk/

2. Log in to the Juniper Networks authentication system using your username and password supplied by a Juniper Networks representative. To download the software, you must have a service contract and an access account. If you do not have an access account, complete the registration form at the Juniper Networks Web site, https://www.juniper.net/registration/Register.jsp.
3. Download the JUNOScope software to your local UNIX host.
4. Start the JUNOScope installation program with the following command:

   hostname% *download-directory*/**jtk-install**-*X.XXX.X*-**sunos5-sparc.sh** *install-directory*

   or

   hostname% *download-directory*/**jtk-install**-*X.XXX.X*-**linux2-i386.sh** *install-directory*

   Replace *download-directory* with the directory into which you downloaded the JUNOScope software from the software download page.

   /jtk-install-*X.XXX.X*-**sunos5-sparc.sh** or **jtk-install**-*X.XXX.X*-**linux2-i386.sh** is the JUNOScope software file. Replace *X* with the software version to download (for example, 7.3R1.3).

Replace *install-directory* with the directory in which to install the JUNOScope software. If you do not specify an installation directory, the software is installed in the current directory.

For information about installing JUNOScope, see "Installing the JUNOScope Software" on page 25.

Installing the JUNOScope Software

To install the JUNOScope software, follow these steps:

1. To accept the JUNOScope Software License Agreement, type **Yes**. If you do not accept the terms of the agreement, you cannot install the JUNOScope software.

   The JUNOScope installation informs you that if problems are encountered with the Java Runtime, you must install or update the required patch cluster. The installation recommends the required patch cluster; for example for Solaris 5.8, J2SE_Solaris_8_Recommended Patch Cluster is required. Patch clusters are available from http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access. We recommend that you install the latest patch cluster before reporting problems with the Java Runtime.

   On a Linux server, the JUNOScope installation checks to ensure that the required linux packages are installed. If any of the packages (see "Red Hat Enterprise Linux ES File Package Requirements" on page 21) are missing the installation lists the missing packages and waits for you to press any key to continue with the JUNOScope installation. We recommend that you install all the linux packages for proper functioning of JUNOScope features.

2. To confirm whether you want to continue the JUNOScope installation or quit, type **C**.

   The JUNOScope installation checks the installation file data integrity, then extracts the installation files. This process takes a few minutes.

3. Specify how you want to protect JUNOScope data files. The available options for protecting data files associated with JUNOScope include:

   - user—Only the user installing JUNOScope can read.
   - group—Any user in the JUNOScope installer's group can read but not write.
   - all—Any JUNOScope user can read but not write.

4. Indicate the HTTPS port on which the JUNOScope Web server should listen for HTTPS requests. The default port is 8443.

NOTE: If you specify a port number less than 1024, the server must run as root.

It is recommended that you use the HTTPS port for communication between the JUNOScope Web browsers and the JUNOScope server.

---

5. Indicate the HTTP port on which to listen for HTTP requests. The default port is 8080.

NOTE: If you specify a port number less than 1024, the server must run as root.

---

6. Indicate the port on which the JUNOScope server should listen for control messages. The recommended port is 8005. The server listens on local port 8005 for control. Connections can only be made from the local host.
7. Indicate the HTTP port on which the JUNOScope report server should listen. The default is 8888.
8. Indicate the JDBC URLs for accessing the JUNOScope database. The default URL is jdbc:mysql://localhost/jtk.
9. Indicate the JDBC URLs for the demo database. The default URL is jdbc:mysql://localhost/demo.
10. Type the key used to encrypt and decrypt the import and export of sensitive data. This key can be up to 16 characters long. Retype the password to confirm it. The key is concealed and stored in the JUNOScope software.
11. Confirm whether you want the JUNOScope installation to install MySQL in *<install-directory>/*mysql. The default is yes. If MySQL is already installed on the workstation, indicate no to use that database.
12. (Prompted only if install is done as root.) Type the username of the person installing the JUNOScope software, not root. If the JUNOScope installation is run by root, MySQL will change its UID identifier to a less privileged user. Unless using privileged ports, the JUNOScope server is also run as this user.

NOTE:

A JUNOScope software password should meet the following restrictions:

- Allow the full range of ASCII characters (except control characters).
- Enforce a minimum of 6 characters.
- Require a change in the character set, including uppercase, lowercase, numeric, and punctuation.

---

13. (Prompted only if install is done as root.) Type the name of the group that owns the JUNOScope installation. The default is the primary group of the user you specified in Step 12.
14. Type the password for the database (internal) administrative user, then retype the password to confirm it. The password should contain numbers and/or punctuation.
15. Type the database user for JDBC access. The default is jtk. All access to the JUNOScope database is done as this user.

16. Type the password for the database user, then retype the password to confirm it. The password should contain numbers and/or punctuation.
17. Confirm whether you want to enable access to the Inventory Management System SQL interface. The default is no. If you select no, the database username and password (see Steps 18 and 19) will not be displayed because the SQL interface is not enabled.

WARNING: If you select no, the SQL interface cannot be accessed by any other application or host except JUNOScope clients. If you select yes, the MySQL database can be accessed by any application with Inventory Management System user credentials.

---

18. (If you enabled the Inventory Management System SQL interface) Type the username for the SQL interface to the Inventory Management System database. The default is ims.
19. (If you enabled the Inventory Management System SQL interface) Type a password for the SQL interface to the Inventory Management System, then retype the password to confirm it. The password should contain numbers and/or punctuation.
20. Type the JUNOScope administrative user account name. The default account name is admin. The JUNOScope installation creates this initial JUNOScope administrative user account so the administrator can use it to add other users.
21. Type the password for the JUNOScope administrator, then retype the password to confirm it. The password for the administrator should not match the username, and should not be a word that can be easily guessed.
22. Confirm whether you want to enable debug logging for technical support purposes. The default is no.
23. Type the idle session timeout in minutes. The default is 60 minutes.
24. Type the syslog facility or pipe where you want the syslog daemon (syslogd) to sent JUNOScope software system log messages it receives. The available eight logging facilities include local0 to local7. The default is local2.
25. Type the Java Virtual Machine (JVM) heap size in Mega Bytes. The default and minimum recommended JVM heap size is 675 MB. You need to enter at least the minimum recommended value of the JVM heap size to proceed with the installation. You can specify a higher JVM heap size value for better performance but it may affect the server startup process.
26. Provide the following information to generate an X.509 certificate for the JUNOScope HTTPS server (Web browsers will not accept a certificate that appears to belong to a different host):
    - The common name for the JUNOScope software server. For example, specify the Common Name field of an X.509 certificate. A wildcard entry such as *.juniper.net will work. The default name is the hostname.
    - The organization unit that runs the server (optional). For example, specify Network Management.

- The organization that runs the server. For example, specify Juniper Networks Inc.
- The locality name or location of this server (optional). For example, specify Sunnyvale.
- The state or province where the server is located. For example, specify California.
- The country code where this server is located. For example, type a two-letter code such as US or AU.

27. Enter the JUNOScope software serial number available in the Software Serial Number Certificate email, or printed on the JUNOScope CD label and then re-enter the serial number to confirm.
28. Select the JUNOScope software features that you are licensed to operate: Looking Glass, Configuration Manager (Configuration menu), Inventory Manager, Software Manager, or IP Backhaul Manager. If you do not have a license to install a feature, select no (the default). If you have a license to install a feature, select yes. Any feature that you select not to install will be disabled (unavailable) in the JUNOScope main window.
    - For more information about the Looking Glass feature, see "Using Looking Glass" on page 417.
    - For more information about the Configuration Manager features, see "Using the Configuration Browser" on page 425 and "Using the Configuration Editor" on page 431.
    - For more information about the Inventory Management feature, see "Using Inventory Reports" on page 345.
    - For more information about the Software Manager feature, see "Using the Software Manager" on page 397.
    - For more information about the IP Backhaul Manager feature, see "Provisioning Pseudowires" on page 281.
29. Confirm whether you want to continue the JUNOScope installation, start over, reset the selections to their default, or quit.

    The JUNOScope installation program extracts the database files and generates a certificate for the settings that you indicated. For example, CN = sunmaker.juniper.net, OU = Engineering, O = Juniper Networks Inc., S = California, C = US.

    The JUNOScope installation takes a few minutes to prepare and install the database tables. The installation then shuts down the database, then restarts and checks it.

    The installation starts Tomcat, an application server from the Apache Software Foundation that executes Java servlets and renders Web pages. When this is done, the JUNOScope installation is complete.

Reconfiguring the JUNOScope Software

You can change the following JUNOScope software installation settings without rerunning the installation program.

- The HTTPS and HTTP ports on which the JUNOScope Web server should listen
- The port on which the JUNOScope server listens for control messages
- The HTTP port on which the JUNOScope report server should listen
- The Java Database Connectivity (JDBC) URL for accessing the JUNOScope database
- Access to the Inventory Management System SQL interface
- Debug logging
- Idle session timeout
- Licensed software modules

You cannot change some settings such as passwords.

To change JUNOScope software settings, use the following command:

hostname% <*install-directory*>**/jtk/bin/jtk-setup.sh**

Reinstalling and Upgrading the JUNOScope Software

The process for reinstalling or upgrading the JUNOScope software is the same as for installing the software. To install the JUNOScope software, see "Installing the JUNOScope Software" on page 25.

To reinstall or upgrade the JUNOScope software, you must use the same user ID as the one used for the currently installed software.

Starting the JUNOScope Software Manually

The JUNOScope software is automatically started after you install or upgrade the JUNOScope software. If you stop the JUNOScope software, you can restart it using the following procedure.

To start the JUNOScope software after running the installation program, follow these steps:

1. Type the following command:

   hostname% <*install-directory*>**/jtk/rc.d/jtk start**

2. Connect to the JUNOScope software server and log in. For more information, see "Connecting to the JUNOScope Software from a Client Workstation and Logging In" on page 30.

If you reboot the UNIX workstation on which you installed the JUNOScope software, the JUNOScope software will not start automatically. For more information, see "Starting the JUNOScope Software Automatically at Boot Time" on page 30.

Starting the JUNOScope Software Automatically at Boot Time

To start the JUNOScope software and the database when the UNIX workstation boots, type the following command:

hostname% **ln -s** *<install-directory>***/jtk/rc.d/jtk/ /etc/rc2.d/S99jtk**

Connecting to the JUNOScope Software from a Client Workstation and Logging In

You can connect to the JUNOScope software Web server from a UNIX or PC client workstation running Microsoft Internet Explorer 6 or Netscape Navigator 6 or later.

The JUNOScope administrator can log in to JUNOScope with the administrative username and password specified during the installation process.

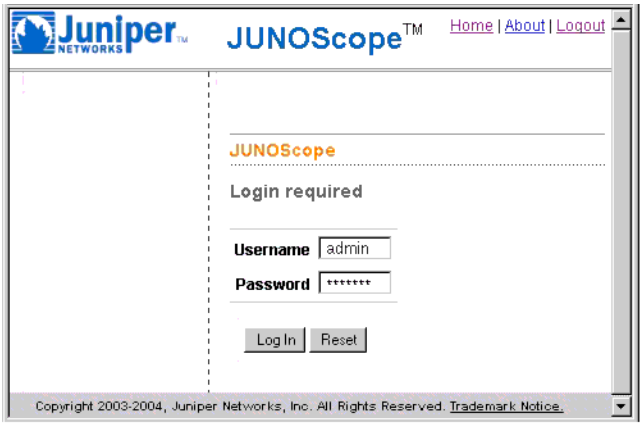
The default administrative username is admin. The administrator can add new users to log in and use the JUNOScope software. Each user must have a unique username and password. For more information about adding new users, see "Setting Up User Local Authentication" on page 97.

To connect to the JUNOScope software Web server and log in, follow these steps:

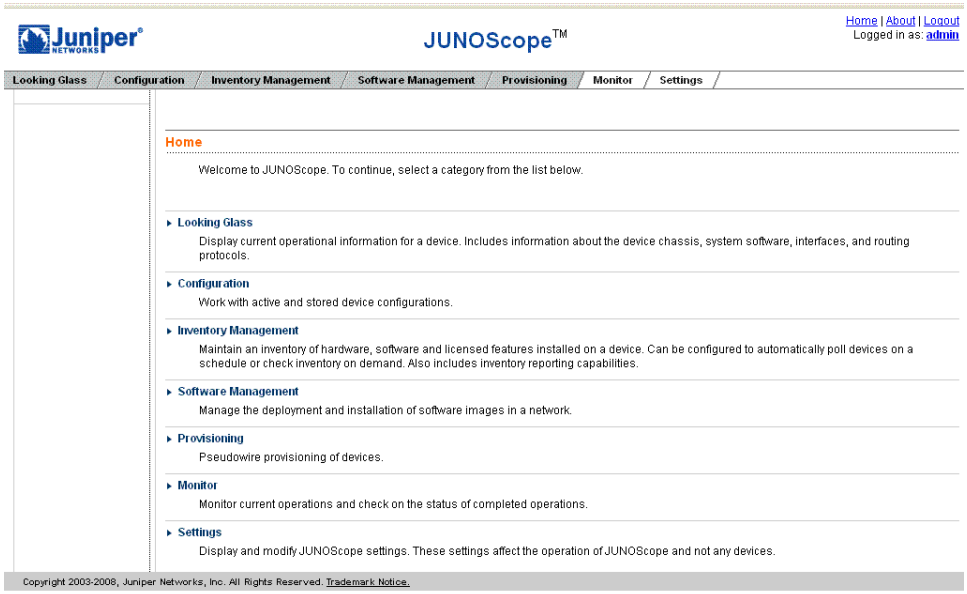
1. Start your Web browser.
2. Enter the following URL in your Web browser Address text box:

   https://*hostname***:***port-number***/jtk**

   Where *hostname* is the name of the UNIX workstation on which the JUNOScope software is installed, and *port-number* is the port on which the JUNOScope Web server listens for HTTPS requests. The default port is 8443. The JUNOScope Login dialog box appears.



3. In the Username text box, type the administrative username. The username is the JUNOScope software administrative username specified during installation.
4. In the Password text box, type the administrative user's password.
5. Click Log In. The JUNOScope main window appears.



For more detailed information about the JUNOScope main window, see "JUNOScope Main Window" on page 439.

Stopping the JUNOScope Software

To stop the JUNOScope software and the database, type the following command:

hostname% <*install-directory*>/**jtk/rc.d/jtk stop**

Shutting Down the JUNOScope Software

To automatically shut down the JUNOScope software during system shutdown, type the following commands:

hostname% **ln -s** <*install-directory*>/**jtk/rc.d/jtk /etc/rc2.d/K19jtk**
hostname% **ln -s** <*install-directory*>/**jtk/rc.d/jtk /etc/rc0.d/K19jtk**

Where to Go from Here

To set up the JUNOScope software for configuration and fault management operations, see the following sections:

- To specify the authentication information (login and password for accessing a router) configured on a router for remotely connecting to that router from the JUNOScope software, see “Setting Up Authentication Information” on page 37.
- To specify the access method (JUNOScript access protocol to connect to the JUNOScript server running on a router) configured on a router for remotely connecting to that router from the JUNOScope software, see “Setting Up Access Methods” on page 45.
- To specify the Juniper Networks routing platforms to which you want to connect the JUNOScope software, see “Setting Up Devices” on page 57.
- To specify router groups for configuration management operations, see “Setting Up Groups” on page 67.
- To add labels for dynamically organizing and categorizing groups of devices, see “Setting Up Labels” on page 83.
- To add schedules for archiving router configuration files, see “Setting Up Schedules” on page 89.
- To add user local authentication and RADIUS configuration settings, see “Setting Up User Local Authentication” on page 97.
- To configure user authentication on a RADIUS server and in the JUNOScope software so that users with a RADIUS account can log in to the JUNOScope software, see “Setting Up RADIUS Configuration” on page 141.
- To import all JUNOScope data from another server or to export all JUNOScope data to another server, see “Importing and Exporting All Settings Data” on page 159.

Chapter 3

Uninstalling the JUNOScope Software

This chapter describes how to stop and remove the JUNOScope software that is running on a UNIX server. Uninstall should either be performed as the UNIX user who first installed the JUNOScope software or as root.

Starting the JUNOScope Software Uninstall Process

To uninstall the JUNOScope software, follow these steps:

1. Stop the JUNOScope software and database by changing to the directory where you installed the JUNOScope software and typing the following command:

   hostname% *<install-directory>* /**jtk/rc.d/jtk stop**

2. Remove the JUNOScope software by typing the following command:

   hostname% **rm -rf** *<install-directory>*

NOTE: This command removes the JUNOScope *<install-directory>* , including all data.

Part 3
Modifying JUNOScope Software Settings

Chapter 4

Setting Up Authentication Information

This chapter describes how to set up the JUNOScope software to connect to routing platforms on your network for configuration operations.

You can specify the authentication information (login and password for accessing a router) configured on a router for remotely connecting to that router from the JUNOScope software. The JUNOScope software supports secure sockets layer (SSL) and clear-text access protocols. We recommend that you set up authentication information and access methods before you set up routers.

You can import authentication information from another JUNOScope server or export it as backup or for importing to another server.

You must have superuser permissions to set up authentication information.

This chapter includes the following topics:

Prerequisites for Authentication Information

You should know the authentication user account (login name and password) configured on the router for users to access that router. The user account information is configured on the router at the [edit system login] hierarchy level.

Understanding Authentication Information and Access Methods

If each router has the same username, password, and access protocol configured, you can set up one access method for all routers.

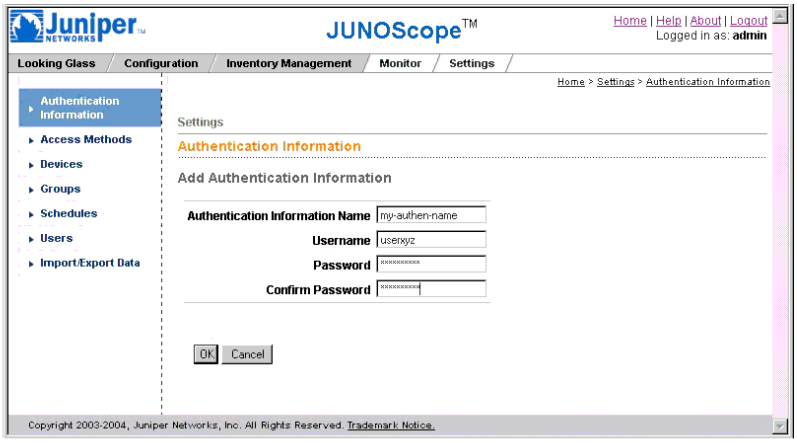
Different JUNOScope users can use the same authentication information to access a router if they all have the same permissions. If a user's permissions are different, you must create two different authentication information entries.

You can create two access methods using the same authentication information and different access protocols. Or you can create two access methods with the same selections but with a different access method name.

Adding Authentication Information

To add additional authentication information, follow these steps:

1. From the JUNOScope main window, click Settings > Authentication Information. The Authentication Information dialog box appears.
2. Click Add. The Add Authentication Information dialog box appears.

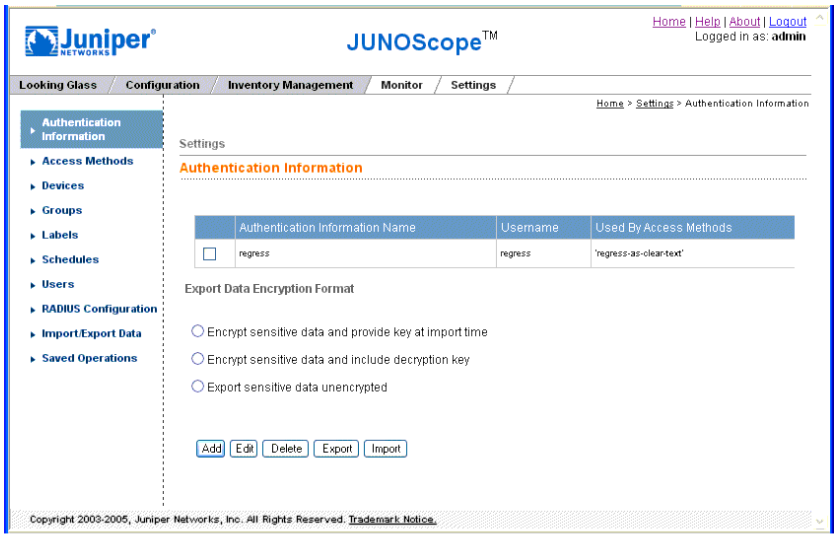


3. In the Authentication Information Name text box, type a name for the authentication information. This name will be listed in the Authentication Information drop-down list box in the Add Access Methods dialog box.
4. In the Username text box, type a user login name that is configured on the router. This must be the username of a valid user on the router.
5. In the Password text box, type a user password that is configured on the router. This must be the password of a valid user on the router.
6. In the Confirm Password text box, retype the user password to confirm it.
7. Click OK. The Authentication Information dialog box appears with the new authentication information listed.

Viewing Authentication Information

To view added authentication information, follow these steps:

1. From the JUNOScope main window, click Settings > Authentication Information. The Authentication Information dialog box appears.



The authentication information is listed alphabetically by Authentication Information Name. From the Authentication Information dialog box, you can add, edit, delete, export, or import authentication information. Select the check box for the authentication information item to edit or delete.

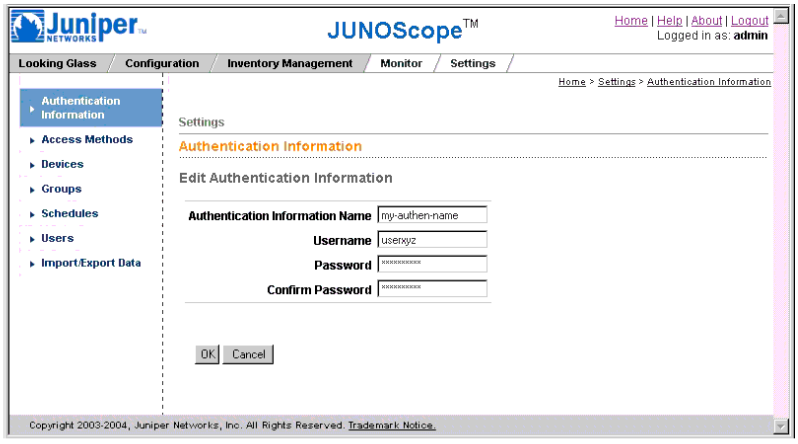
2. Select one of the following ways to export authentication information from the JUNOScope software:

- Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
- Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export authentication information to another system.
- Export sensitive data unencrypted—Sensitive data is not encrypted at export.

Editing Authentication Information

To edit existing authentication information that has changed on a router, follow these steps:

1. In the JUNOScope main window, click Settings > Authentication Information. The Authentication Information dialog box appears.
2. Select the check box for the authentication information that you want to edit.
3. Click Edit. The Edit Authentication Information dialog box appears.



4. Edit the appropriate authentication information.
5. Click OK. The edited authentication information is listed in the Authentication Information dialog box.

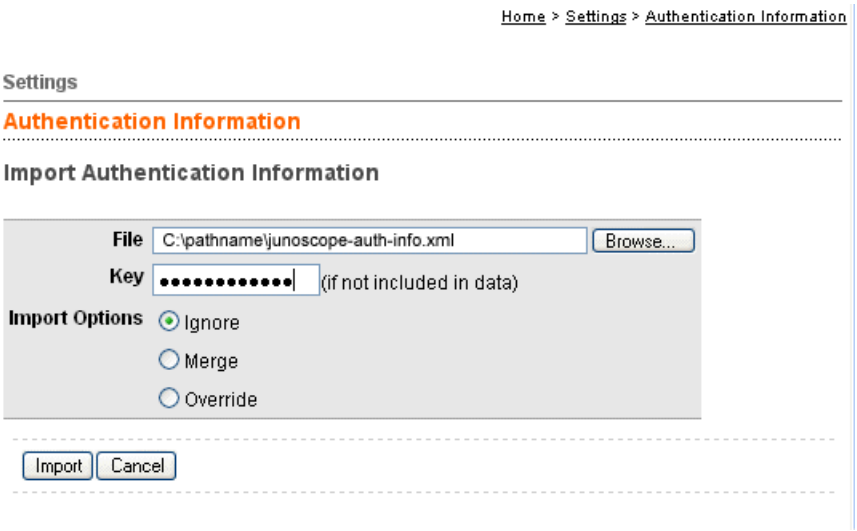
Importing Authentication Information

You can import authentication information from another JUNOScope server or by using the provided sample XML import file export-import-sample.xml, located on the JUNOScope server.

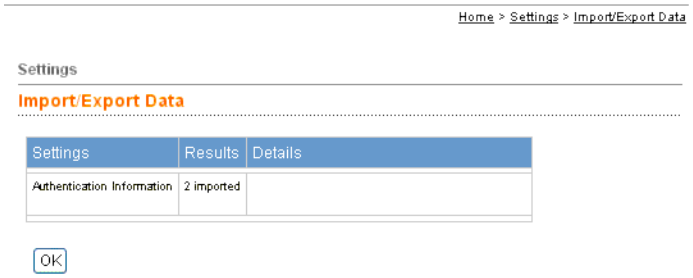
Importing authentication information is useful when you do not want to enter setup information manually.

To import authentication information, follow these steps:

1. In the JUNOScope main window, click Settings > Authentication Information. The Authentication Information dialog box appears.
2. Click Import. The Import Authentication Information dialog box appears.



3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default access.xml file exported from another JUNOScope server, or use the export-import-sample.xml file as a guide to generate a file to import.
4. Type the key to decrypt the sensitive authentication information data that you want to import. The key is required if you selected not to include it when the data was exported. This key can be up to 16 characters long and was created during the JUNOScope installation.
5. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.
6. Click Import. The Import status dialog box appears.



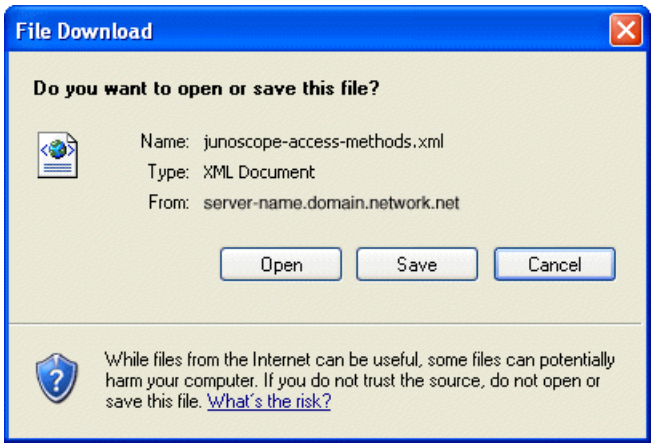
   The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.
7. Click OK. The imported data is listed in the Authentication Information dialog box.

Exporting Authentication Information

You can export authentication information that you want to back up or import to another JUNOScope server.

To export authentication information, follow these steps:

1. In the JUNOScope main window, click Settings > Authentication Information. The Authentication Information dialog box appears.
2. Click Export. The File Download dialog box appears.



3. Click Save to export the Authentication Information and save it to the local file system in a file named junoscope-access-methods.xml. Click Open to view the export file contents.

Deleting Authentication Information

NOTE: You cannot delete authentication information that is currently being used by an access method. You must first delete the access method, then delete the authentication information. You cannot delete an access method if it is currently being used by a device. You must first delete the device, then delete the access method.

To delete authentication information, follow these steps:

1. In the JUNOScope main window, click Settings > Authentication Information. The Authentication Information dialog box appears.
2. Select the check box for the authentication information that you want to delete.
3. Click Delete. The authentication information is deleted from the Authentication Information table.

Chapter 5

Setting Up Access Methods

This chapter describes how to set up the JUNOScope software to connect to routing platforms on your network for configuration operations.

You can specify the access method (JUNOScript or NETCONF access protocol to connect to the JUNOScript or NETCONF server running on a router) configured on a router for remotely connecting to that router from the JUNOScope software. The JUNOScope software supports secure sockets layer (SSL) and clear-text access protocols for JUNOScript, and Secure Shell (SSH) for NETCONF. We recommend that you set up access methods before you set up routers.

You can import access method information from another JUNOScope server or export it as backup or for importing to another server.

You must have superuser permissions to set up access methods.

This chapter includes the following topics:

Understanding the JUNOScript API

The JUNOScript application programming interface (API) is an Extensible Markup Language (XML) application that Juniper Networks routers use to exchange information with client applications. XML is a metalanguage for defining how to mark the organizational structures and individual items in a data set or document with tags that describe the function of the structures and items. The JUNOScript API defines tags for describing router components and configuration.

Client applications can configure or request information from a router by encoding the request with JUNOScript tags and sending it to the JUNOScript server on the router. (The JUNOScript server is a component of the management daemon [mgd process] running on the router and does not appear as a separate entry in process listings.) The JUNOScript server directs the request to the appropriate software modules within the router, encodes the response in JUNOScript tags or formatted ASCII as requested by the client application, and returns the result to the client application. For example, to request information about the status of a router's interfaces, a client application can send the JUNOScript <get-interface-information> tag element. The JUNOScript server gathers the information and returns it in the <interface-information> tag element. For more information about the JUNOScript server, see the *JUNOScript API Guide*.

Supported JUNOScript Access Protocols

The JUNOScope software uses SSL and clear-text JUNOScript access protocols (see Table 7 on page 46), which also specify the associated authentication mechanism.

The SSL protocol is preferred because it encrypts security information (such as a password) before transmitting it across the network. The clear-text protocol does not encrypt security information.

Table 7: Supported Access Protocols and Authentication Mechanisms

Access Protocol	Authentication Mechanism
clear-text, a JUNOScript-specific protocol for sending unencrypted text over a Transmission Control Protocol (TCP) connection	JUNOScript-specific
SSL, a JUNOScript-specific protocol for sending encrypted text over a TCP connection	JUNOScript-specific

Prerequisites for Establishing a JUNOScript Server Connection

To create a connection, both the JUNOScript server and the client application must be able to access the software for the access protocol used by the client application. The JUNOScript server can access the protocols listed in Table 7 on page 46 because the JUNOS software distribution includes them. On most operating systems, client applications can access the software for TCP (used by the JUNOScript-specific clear-text protocol) as part of the standard distribution. For information about obtaining SSL software, see http://www.openssl.org.

The following topics describe the prerequisites for establishing a connection with the JUNOScript server:

- Prerequisites for clear-text Connections on page 47
- Prerequisites for SSL Connections on page 47

When the prerequisites are satisfied, the client application connects to the JUNOScript server by opening a socket or other communications channel to the JUNOScript

server machine (router) and invoking one of the remote-connection routines appropriate for the programming language and access protocol that the application uses.

Prerequisites for clear-text Connections

If the client application uses the clear-text protocol to send unencrypted text directly over a TCP connection without using any additional protocol (such as SSL), you must activate the xnm-clear-text service on port 3221 on the JUNOScript server machine. To do this, follow these steps:

1. Enter command-line interface (CLI) configuration mode on the JUNOScript server machine and issue the following command:

   [edit]
   user@host# **set system services xnm-clear-text**

2. Commit the configuration:

   [edit]
   user@host# **commit**

Prerequisites for SSL Connections

The SSL protocol uses public-private key technology, which requires a paired private key and authentication certificate. To enable a client application to establish SSL connections, follow these steps:

1. Install the SSL client on the machine where the client application runs.

   Skip this step if the client application uses the JUNOScript Perl module described in " Write Perl Client Applications" in the *JUNOScript API Guide*. As part of the Perl module installation procedure, you install a prerequisites package that includes the necessary SSL software.

2. Use one of the following two methods to obtain an authentication certificate in privacy-enhanced mail (PEM) format:

   - Request a certificate from a Certificate Authority; these agencies usually charge a fee.
   - Issue the following openssl command to generate a self-signed certificate; for information about obtaining the openssl software, see http://www.openssl.org.

     The command writes the certificate and an unencrypted 1024-bit RSA private key to the *certificate-file*.pem file. The command appears here on two lines only for legibility:

     % **openssl req -x509 -nodes -newkey rsa:1024** \
     -keyout *certificate-file* **.pem -out** *certificate-file* **.pem**

3. Enter CLI configuration mode on the JUNOScript server and issue the following commands to import the certificate. In the first command, substitute the

certificate name for the *certificate-name* variable. In the second command, for the *URL-or-path* variable, substitute the name of the file that contains the paired certificate and private key, either as a URL or as a pathname on the local disk.

```
[edit]
user@host# edit security certificates local certificate-name
[edit security certificates local certificate-name ]
user@host# set load-key-file URL-or-path?
```

NOTE: The CLI expects the private key in the specified file (*URL-or-path*) to be unencrypted. If the key is encrypted, the CLI prompts for the passphrase associated with it, decrypts it, and stores the unencrypted version.

---

4. Issue the following commands to activate the xnm-ssl service, which listens on port 3220. In the last command, substitute the same value for the *certificate-name* variable as in Step 3.

```
[edit security certificates local certificate-name ]
user@host# top
[edit]
user@host# edit system services
[edit system services]
user@host# set xnm-ssl local-certificate certificate-name
```

5. Verify that 127.0.0.1 is one of the IP addresses configured for the loopback interface, lo0, on the JUNOScript server machine. The output from the show interfaces lo0 command must include an address statement similar to the following:

```
[edit system services]
user@host# top
[edit]
user@host# show interfaces lo0
unit 0 {
   family inet {
      address 127.0.0.1/32;
   }
}
```

If necessary, issue the following command to add the address at the [edit interfaces lo0 unit 0 family inet] hierarchy level:

```
[edit]
user@host# set interfaces lo0 unit 0 family inet address 127.0.0.1
```

6. Commit the configuration:

```
[edit]
user@host# commit
```

Understanding the NETCONF API

The NETCONF API (application programming interface) is an Extensible Markup Language (XML) application that client applications use to request and change configuration information devices that run operating systems that are compatible with NETCONF API. Applications use the API to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as show, set, and commit to perform those operations.

The NETCONF API is described in *RFC 4741, NETCONF Configuration Protocol*, available at http://www.ietf.org/rfc/rfc4741.txt.

Client applications request or change information on a routing platform by encoding the request with tag elements from the NETCONF API and sending it to the NETCONF server on the routing platform. (The NETCONF server is integrated into the JUNOS software and does not appear as a separate entry in process listings.) The NETCONF server directs the request to the appropriate software modules within the routing platform, encodes the response in NETCONF API XML tag elements, and returns the result to the client application. For example, to request information about the status of a routing platform's interfaces, a client application sends the <get-interface-information> tag element from the JUNOS XML API. The NETCONF server gathers the information from the interface process and returns it in the <interface-information> tag element.

For more information about NETCONF API, see the *JUNOS Software NETCONF API Guide*.

Prerequisites for Establishing a NETCONF Server Session

The NETCONF server communicates with client applications within the context of a NETCONF session. The server and client explicitly establish a connection and session before exchanging data, and close the session and connection when they are finished. Client applications access the NETCONF server using the SSH protocol and use the standard SSH authentication mechanism.

Before you establish a NETCONF server session, ensure that:

- The NETCONF server and client applications comply with *RFC 4742, Using the NETCONF Configuration Protocol over Secure Shell (SSH)*, available at http://www.ietf.org/rfc/rfc4742.txt.
- SSH Software is installed on the configuration management server.

You must enable NETCONF over SSH protocol on port 830 of the device running NETCONF server. To do this, enter the set system services netconf ssh command at the command line interface of the NETCONF server device.

```
[edit]
user@host# set system services netconf ssh
```

Understanding Authentication Information and Access Methods

Setting up an access method requires that you add authentication information first, then add access method information.

If each router has the same username, password, and access protocol configured, you can set up one access method for all routers.

Different JUNOScope users can use the same authentication information to access a router if they all have the same permissions. If a user's permissions are different, you must create two different authentication information entries.

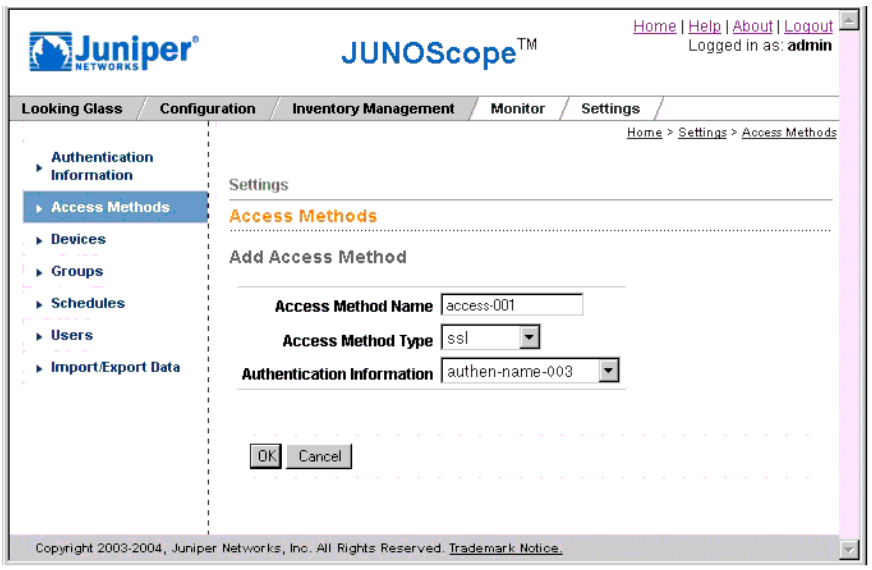
You can create two access methods using the same authentication information and different access protocols. Or you can create two access methods with the same selections but with a different access method name.

Adding an Access Method

You are not done setting up access methods without at least one authentication information entry. You can use the Add button to add a new entry, or edit or delete an existing entry.

To add an access method, follow these steps:

1. From the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Click Add. The Add Access Method dialog box appears.



3. In the Access Method Name text box, type a name for the remote router access method to use in the JUNOScope software. This is the access method name used in the Add Device dialog box. See "Adding a Device" on page 58.

4. In the Access Method Type drop-down list box, select a supported access protocol that is configured on the router:,JUNOScript over clear-text, JUNOScript over SSL, or NETCONF over SSH.

NOTE: The NETCONF over SSH option is available only if you have installed IP Backhaul Manager license.

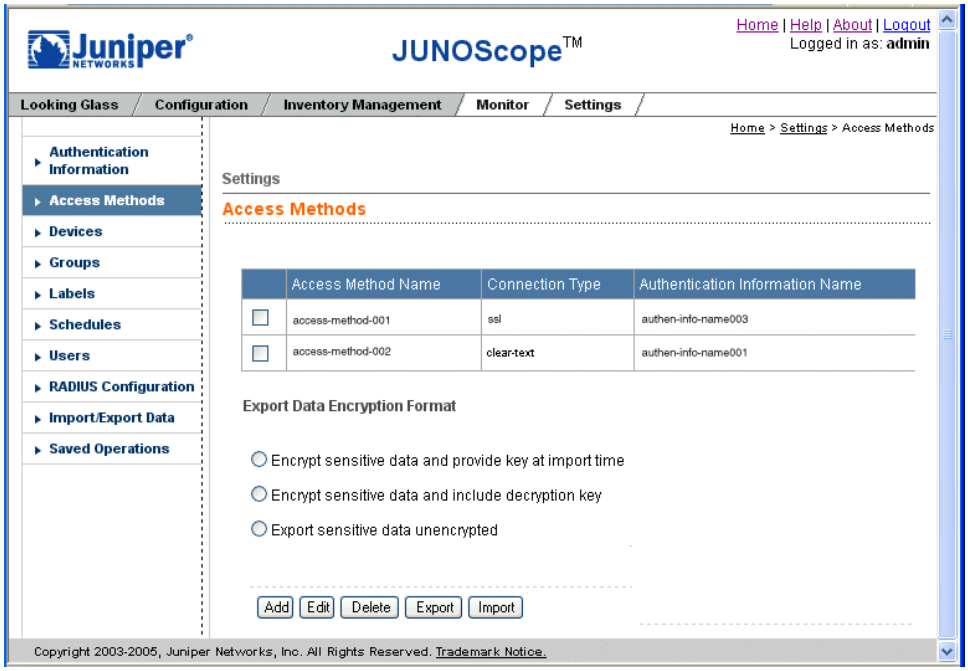
NOTE: You must choose the NETCONF over SSH option if you want to access BXOS devices. BXOS devices support only the NETCONF over SSH access method.

5. In the Authentication Information drop-down list box, select an authentication name. This is the same name that you created in the Add Authentication Information dialog box.
6. Click OK. The new access method is listed in the Access Methods dialog box.

Viewing Access Methods

To view added access methods, follow these steps:

1. From the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.



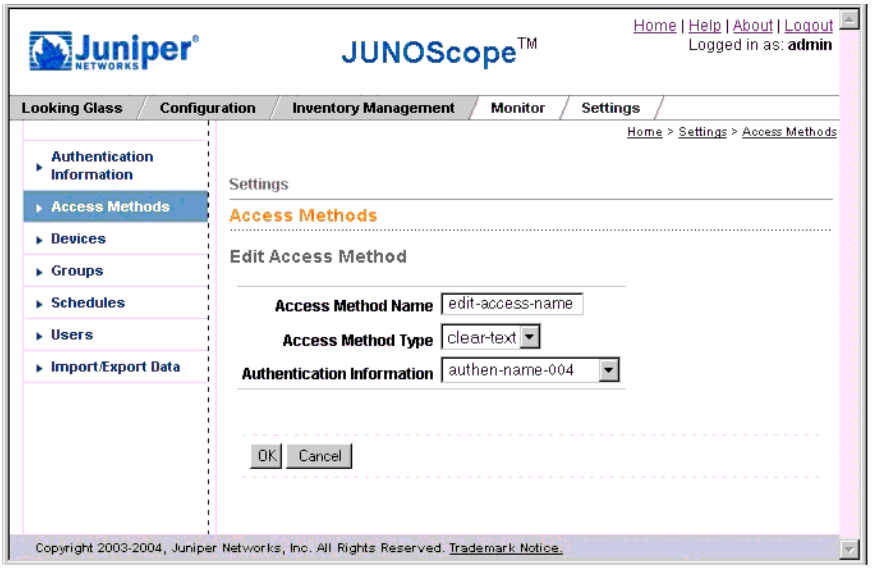
The access methods are listed alphabetically in the table by name, connection type, and authentication information name. The Access Methods dialog box, lets you add, edit, delete, export, or import data. Select the check box for the access method item to edit or delete.

2. Select one of the following ways to export authentication information from the JUNOScope software:
   - Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
   - Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export access methods information to another system.
   - Export sensitive data unencrypted—Sensitive data is not encrypted at export.

Editing Access Method Information

To edit access method information, follow these steps:

1. In the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Select the check box for the access method that you want to edit.
3. Click Edit. The Edit Access Method dialog box appears.



4. Edit the access method name, access method type, or authentication information.
5. Click OK. The edited access method information is listed in the Access Methods dialog box.

Importing Access Methods

You can import access method or authentication information from another JUNOScope server or by using the provided sample XML import file export-import-sample.xml, located on the JUNOScope server.

Importing an access method or authentication information is useful when you do not want to enter setup information manually.

To import access methods, follow these steps:

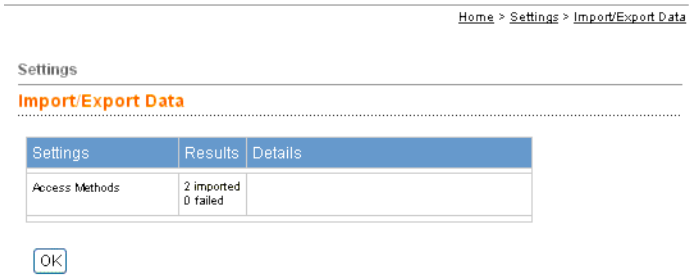
1. In the JUNOScope main window, click Settings > Access Methods. The Authentication Information or Access Methods dialog box appears.
2. Click Import. The Import Access Methods dialog box appears.

3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default access.xml file exported from another JUNOScope server, or use the export-import-sample.xml file as a guide to generate a file to import
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing

record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

5. Click Import. The Import status dialog box appears.



The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

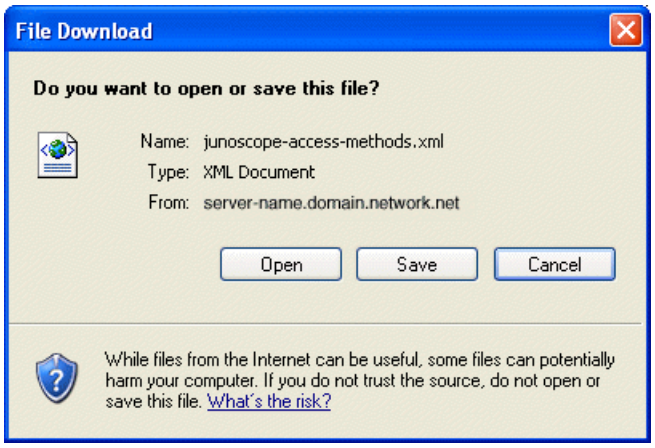
6. Click OK. The imported data is listed in the Access Methods dialog box.

Exporting Access Methods

You can export access methods that you want to back up or import to another JUNOScope server.

To export access methods, follow these steps:

1. In the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Click Export. The File Download dialog box appears.



3. Click Save to export the access methods data and save it to the local file system in a file named junoscope-access-methods.xml. Click Open to view the export file contents.

Deleting Access Methods

NOTE: You cannot delete authentication information that is currently being used by an access method. You must first delete the access method, then delete the authentication information. You cannot delete an access method if it is currently being used by a device. You must first delete the device, then delete the access method.

To delete an access method, follow these steps:

1. In the JUNOScope main window, click Settings > Access Methods. The Access Methods dialog box appears.
2. Select the check box for the access method that you want to delete.
3. Click Delete. The access method is deleted from the Access Methods table or the Authentication Information table.

Chapter 6

Setting Up Devices

This chapter describes how to add the routers or devices on which you want to run JUNOScope software configuration management and monitoring operations.

The JUNOScope software supports Juniper Networks routing platforms running the JUNOScript server and JUNOS software. In the JUNOScope software, each router must have a unique device name, Domain Name System (DNS) name or IP address, remote access method, model number, and an optional comment. We recommend that you set up access methods before you set up devices (see "Setting Up Access Methods" on page 45).

You can associate one or more existing labels to a device when you add, copy, or edit it. Labels, in free text format, provide a way to define static associations with a group of devices, such as 'Region: North', 'Customer: Important', and so on. You create labels using the Settings > Labels command. When you create labels, you can associate them with devices. Operations such as archive configuration and scan inventory can be performed on a large group of routers based on labels. For more information about setting up labels, see "Setting Up Labels" on page 83.

You can import device information from another JUNOScope server or export it as backup or for importing to another server.

You must have superuser permissions to set up devices.

The following topics describe how to manage devices using the JUNOScope software:

Prerequisites for Adding a Device

Before setting up devices, you should have the following information for each router you want the JUNOScope software to manage:

- The name of the router that you want to use for the JUNOScope software.
- The router DNS name or IP address. This can be an IP address (you can specify the loopback IP address) or DNS name (*router-name.domain-name*) that resolves to the address that the JUNOScope software uses to connect.
- The JUNOScript access protocol configured on the router (see "Supported JUNOScript Access Protocols" on page 46 and "Prerequisites for Establishing a JUNOScript Server Connection" on page 46).

Adding a Device

You must first add a router, as described in this procedure, before you can manage it.

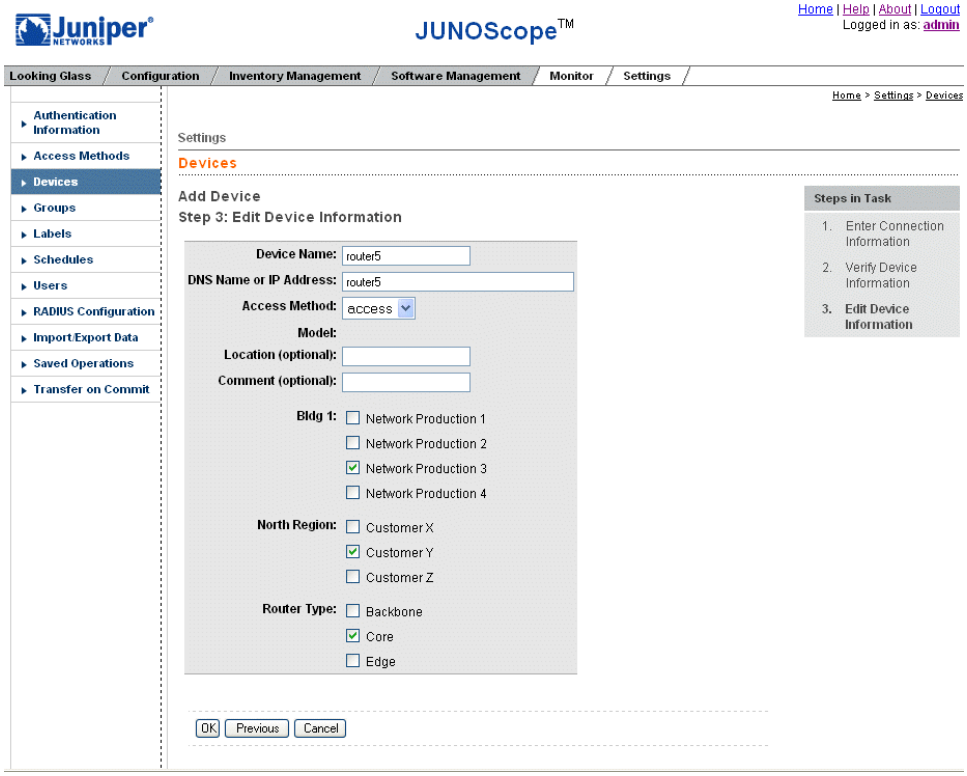
To add a device, follow these steps:

1. In the JUNOScope main window, click Settings > Devices. The Devices dialog box appears.
2. Click Add. The Add Device—Enter Connection Information dialog box appears.

3. Type a DNS name or IP address for the device.
4. In the Access Method drop-down list box, select an access method for connecting to the device.
5. Click Next.

   The JUNOScope software connects to the device, and the Add a Device—Verify Device Information dialog box appears displaying the device hostname, domain name, hardware model number, JUNOS software version and whether it is supported, and the number of Routing Engines installed on the device.

6. Click Next. The Add Device—Edit Device Information dialog box appears with the information about the device already filled in.



7. Verify that the device information is correct and add a descriptive comment and location of the device if required.

8. Click the label check box(es), if configured, at the bottom area of the dialog box to associate the device with an existing label. A label is used to statically group multiple devices so that JUNOScope operations, such as archive and inventory

scan can be performed on them. For information about setting up labels, see "Setting Up Labels" on page 83.

9. Click OK. The new device information is stored in the JUNOScope software database and is listed in the Devices dialog box.

Associating a Device with a Label

Use labels to statically organize devices into logical groups. You can associate a device with existing labels when you add, copy, or edit a device. For more information about creating labels, see "Setting Up Labels" on page 83.

To associate a device with a label, do the following:

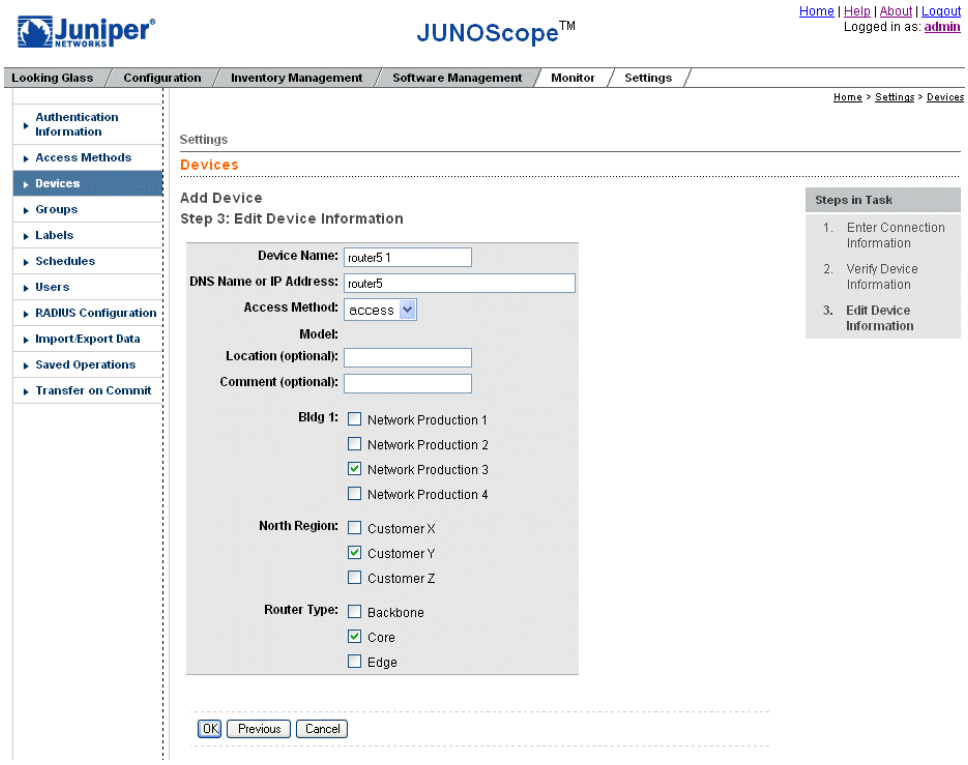
1. In the JUNOScope main window, click Settings > Devices. The Devices dialog box appears.
2. Add a new device, copy an existing device, or edit an existing device:
   - For more information about adding a device, see "Adding a Device" on page 58.
   - For more information about copying a device, see "Copying a Device" on page 60.
   - For more information about editing a device, see "Editing a Device" on page 62.
   - From the Add Device—Edit Device Information dialog box, Add Device—Edit Device Information dialog box, or the Devices—Edit Device dialog box, select one or more label boxes at the bottom of a dialog box.
3. Click OK to associate the added, copied, or edited device with the label(s).

Copying a Device

To copy a device that you have added, follow these steps:

1. In the JUNOScope main window, click Settings > Devices. The Devices dialog box appears.
2. Select the check box for the device you want to copy.
3. Click Copy. The Add Device—Edit Device Information dialog box appears. When you copy a device, a number is appended to the device name corresponding to the number of times you copied the device.

NOTE: You can copy a device up to nine times without renaming it. An error message appears when you copy it the tenth time.



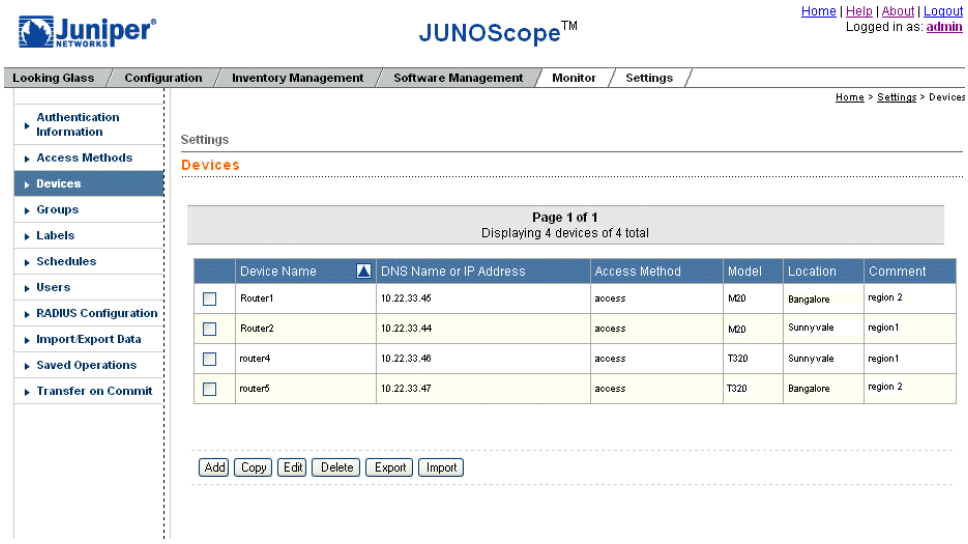
4. Edit the device information for the device.
5. Edit the label associated with the copied device by clicking the appropriate check boxes at the bottom area of the dialog box. Labels that are associated with the original device are also checked for the copied device.
6. Click OK. The device is stored in the JUNOScope software database and is listed in the Devices dialog box.

Viewing Devices

You can view at a glance the routers you configure and monitor using the JUNOScope software. The Devices dialog box is empty until you add a device.

To view devices, do the following:

1. in the JUNOScope main window, click Settings > Devices. The Devices dialog box appears with a list of routers added for management by the JUNOScope software.



Devices are listed by device name, DNS name or IP address, access method, model number, location, and comment.

You can sort the Devices table data by clicking column name. Clicking the column name toggles between ascending and descending sort order.

From the Devices dialog box, you can add, copy, edit, delete, export, or import devices.

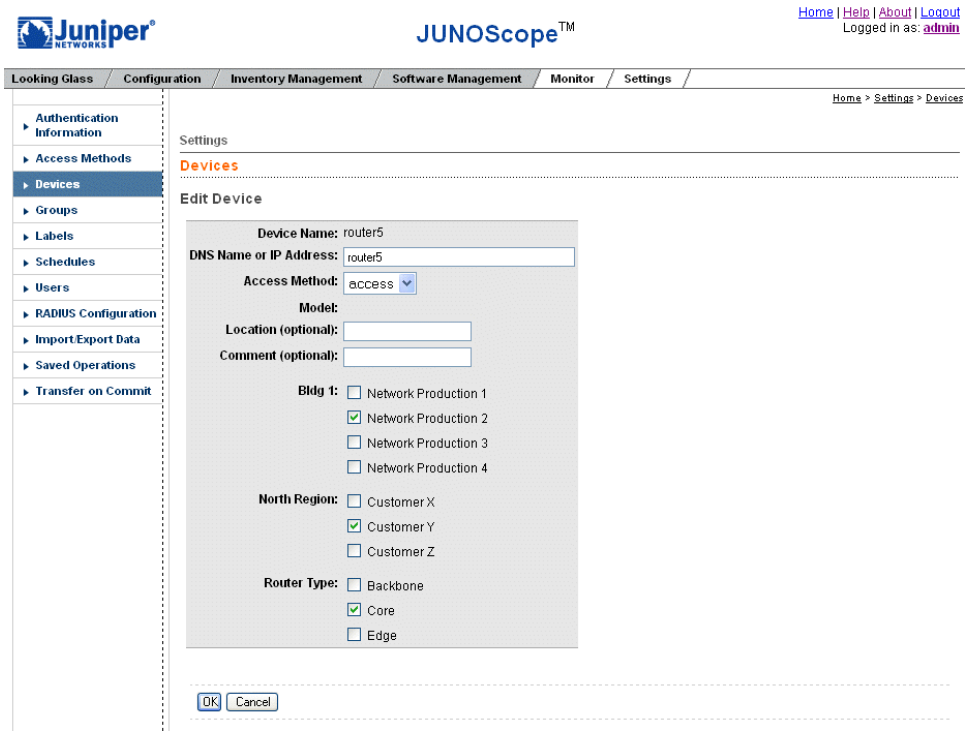
Editing a Device

When there are changes to devices on your network, you can edit router information.

To edit a device, follow these steps:

1. In the JUNOScope main window, click Settings > Devices. The Devices dialog box appears.
2. Select the check box for the device that you want to edit.

3. Click Edit. The Edit Device dialog box appears.



4. Edit the device information as needed.
5. Edit the labels associated with a device by clicking the appropriate check boxes at the bottom of the dialog box.
6. Click OK. The edited device information is stored in the JUNOScope software database and is displayed in the Devices dialog box.

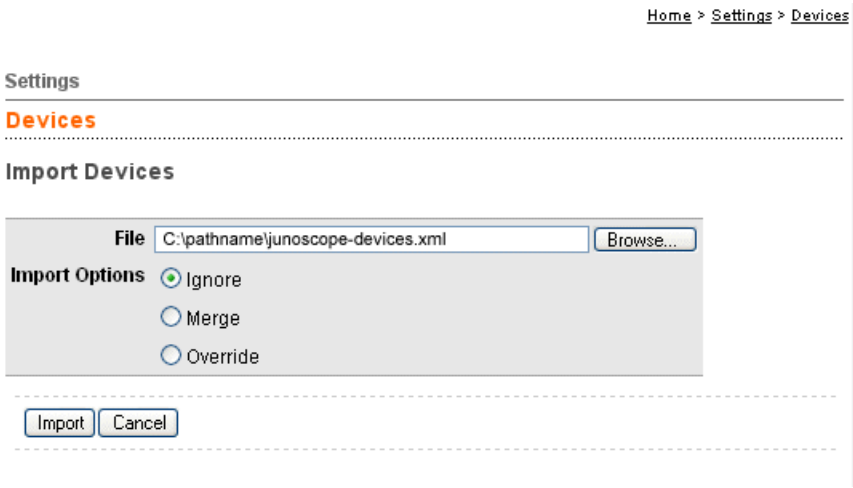
Importing Device Information

You can import device information from another JUNOScope server, or you can use the provided sample XML import file export-import-sample.xml as a guide.

Importing device information is useful when you do not want to enter setup information manually.

To import device information, follow these steps:

1. In the JUNOScope main window, click Settings > Devices. The Devices dialog box appears.
2. Click Import. The Import Devices dialog box appears.



3. In the File text box, either type the name of the XML file that you want to import or browse to it. For example, you can import the default devices.xml export file from another JUNOScope server or use the provided sample export-import-sample.xml XML file to generate a file to import.

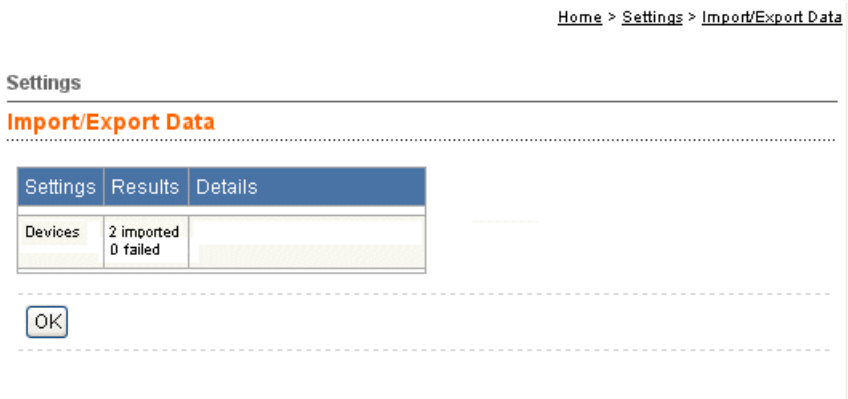
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:

   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

5. Click Import. The Import status dialog box appears.



The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

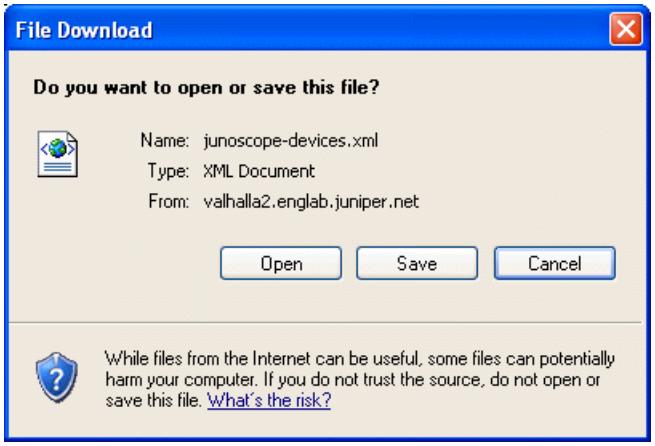
6. Click OK. The imported data is listed in the Devices dialog box.

Exporting Device Information

You can export device information that you want to back up or import to another JUNOScope server.

To export device information, follow these steps:

1. In the JUNOScope main window, click Settings > Devices. The Devices dialog box appears.
2. Click Export. The File Download dialog box appears.



3. Click Save to export the access methods data and save it to the local file system in a file named junoscope-devices.xml. Click Open to view the export XML file content.

NOTE: The junoscope- XML file prefix is not generated if you use the Microsoft Internet Explorer 6.0 Web browser to export JUNOScope setup data. You will only see the devices filename.

Deleting a Device

You can delete devices that no longer exist or need management from the JUNOScope software database.

NOTE: You cannot delete a device that is associated with an active operation schedule. To delete that device, you must click Manage Operations and delete the schedule associated with the device first, then delete the device using the following procedure.

When you delete a device, the corresponding label(s) with which the device is associated are also removed.

To delete a device, follow these steps:

1. In the JUNOScope main window, click Settings > Devices. The Devices dialog box appears.
2. Select the check box for the device that you want to delete.
3. Click Delete.

   The device is deleted from the JUNOScope database. Any operations scheduled for the deleted device will fail unless you delete the scheduled operation using "Managing Operations" on page 313.

Chapter 7

Setting Up Groups

This chapter describes how to define groups of routers (devices) on which you want to run JUNOScope operations. The JUNOScope software can perform operations on groups, such as archiving a configuration file from a group of devices or scanning the hardware, licensed features, and software packages installed.

You can associate devices with JUNOScope software operations. Groups are comprised of devices that are associated by some common factor, such as device name, model, hostname, comment, or label. A group is a separate entity that has no effect until you associate it with an operation, such as archive.

You can specify the rules for querying a group from the device information stored in the JUNOScope software database. You can define rules by combining a device attribute (device name, device hostname, model, comment, or label) with a positive (“does/is”) or negative (“not”) comparison operator and a value. After you have added the first rule, you can add other rules to the end of the list of rules, insert them after a given rule, or insert them before a given rule with either “and” or “or” joining the new rule. You can also delete existing rules from the list.

Device attributes (for example, name, model, as comparison) provide a way to dynamically associate a group of devices. Label comparisons provide a way to statically associate a group of devices.

We recommend that you set up devices before you set up groups so that there will be device information in the JUNOScope software database from which to select. For information about setting up devices for the JUNOScope software, see “Setting Up Devices” on page 57.

You must have superuser permission to set up groups.

The following topics describe how to manage groups:

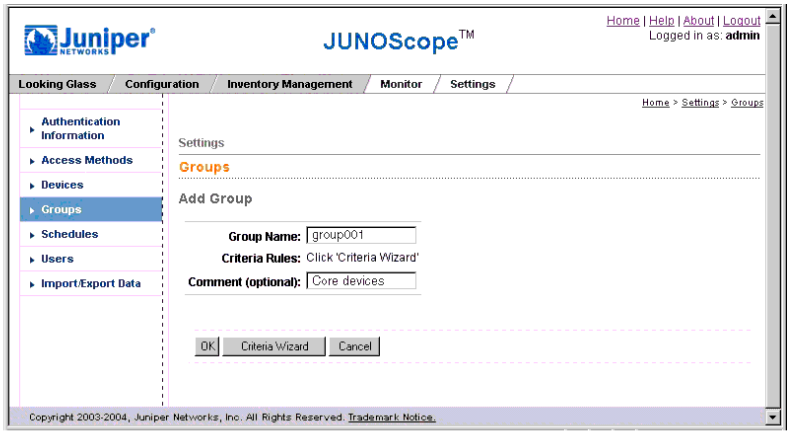
- Exporting Group Information on page 81
- Deleting a Group on page 82

Adding a Group

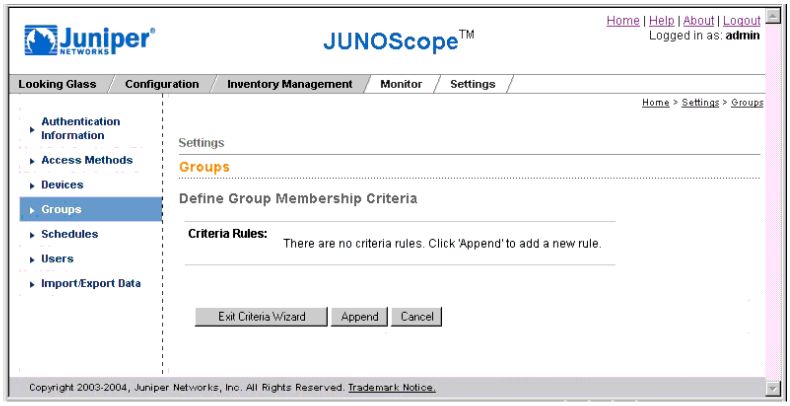
You can add a group of two or more devices for management.

To add a group, follow these steps:

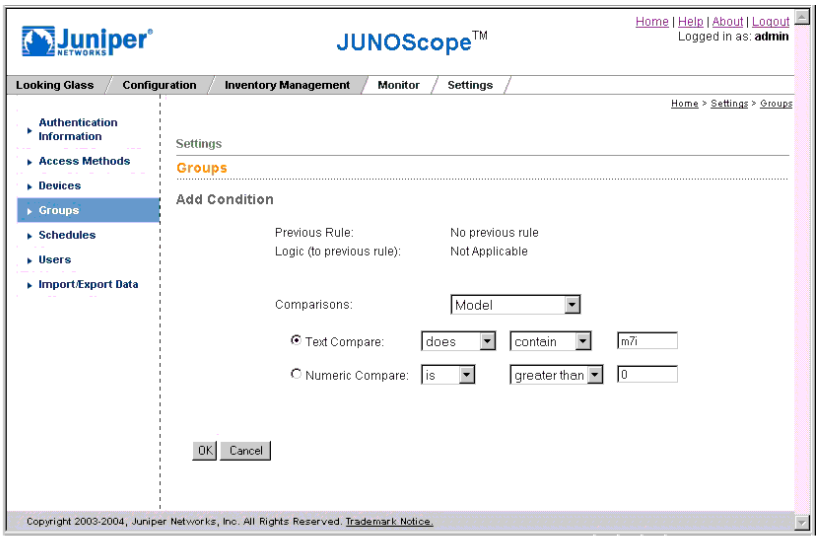
1. In the JUNOScope main window, click Settings > Groups. The Groups dialog box appears.
2. Click Add. The Add Group dialog box appears.



3. In the Group Name text box, type a name for the device group that you want to add. The group name can be as long as you want.
4. In the Comment text box, type an optional descriptive comment for the device group. The comment can be as long as you want.
5. Click Criteria Wizard to create a rule for querying device group members from the JUNOScope software database. The Define Group Membership Criteria dialog box appears.



6. Click Append to add a criteria rule. The Add Condition dialog box appears.



7. In the Comparisons drop-down list box, select the device information you want to compare. The available options include device name, device hostname, model, location, comment, and label. If you do not want to use a label as a comparison in a rule, skip to Step 9.

8. To use an existing label as a rule to statically organize a group of devices, do the following:

   a. Select the Has Label option in the Comparisons drop-down list box. The Add Condition dialog box appears listing the existing label and category names.

   b. Select the label category and label name in the description drop-down list box.

   c. Click OK.

9. Click either Text Compare or Numeric Compare, and do one of the following.

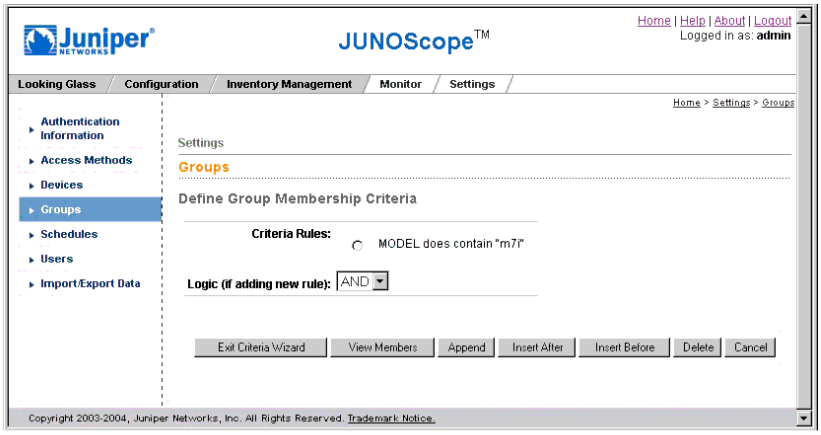
   a. For Text Compare, follow these steps:

      - From the first drop-down list box, select whether the comparison does or does not compare.
      - From the second drop-down list box, select whether the comparison contains, begins with, ends with, or equals.
      - In the text box, type the text that you want to compare.

   b. For Numeric Compare, follow these steps:

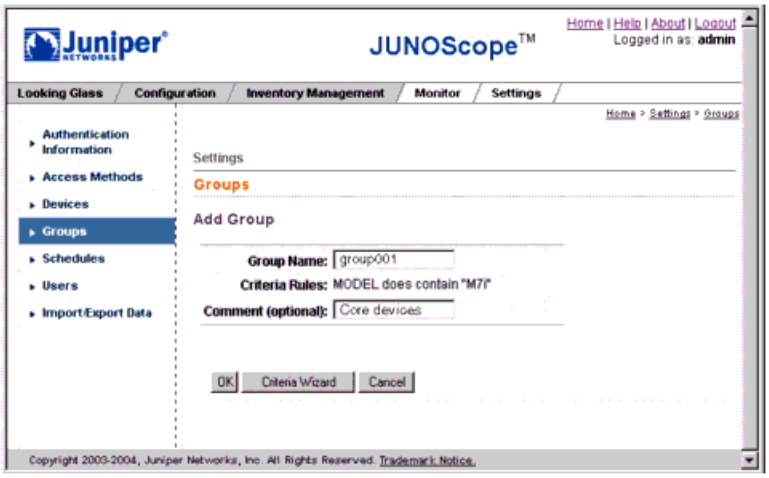
      - From the first drop-down list box, select whether the comparison is or is not a comparison.
      - From the second drop-down list box, select whether the comparison is greater than, less than, or equal to.
      - In the text box, type the value that you want to compare.

10. Click OK. The Define Group Membership Criteria dialog box appears, and the new criteria rule is displayed.

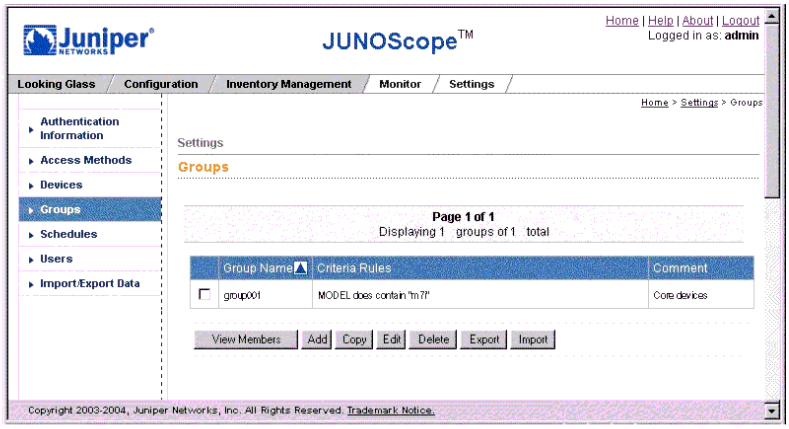


11. Click View Members to verify that the members (devices) you want are in the group you specified. The Group Members dialog box appears.

12. Click OK. The Define Group Membership Criteria dialog box reappears.
13. Click Exit Criteria Wizard. The Add Group dialog box appears, and the Criteria Rule you created is listed.



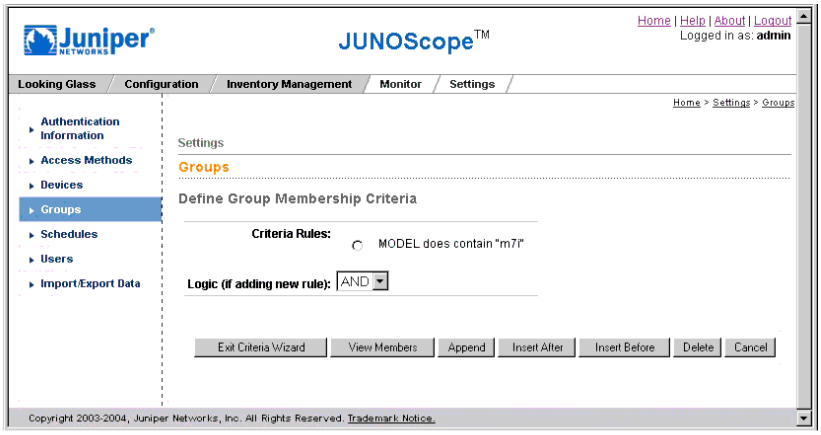
14. Click OK. The group is added to the JUNOScope software database and listed in the Groups dialog box.



Adding Multiple Criteria Rules with Logic

To add multiple criteria rules with logic, follow these steps:

1. Repeat Step 1 through Step 12 in “Adding a Group” on page 68.



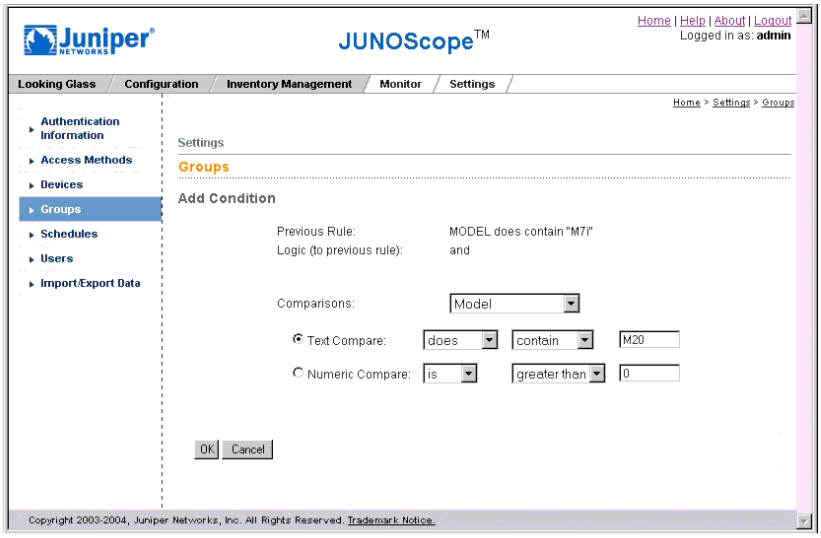
2. In the Define Group Membership Criteria dialog box, select the criteria logic that you want from the Logic (if adding new rule) drop-down list box; select either AND or OR.

3. Click Append.

   You can also click one of the following command buttons:

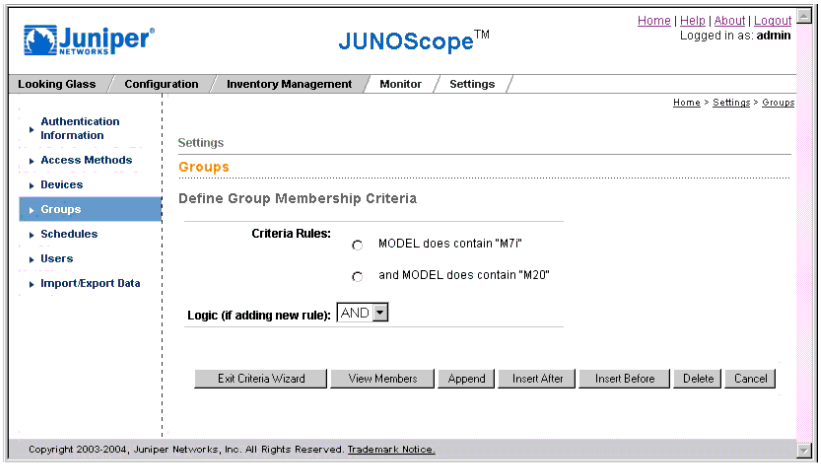
   - Insert After—Inserts the new rule after the criteria rule that you selected in Step 2.
   - Insert Before—Inserts the new rule before the criteria rule that you selected in Step 2.

   The Add Condition dialog box appears.

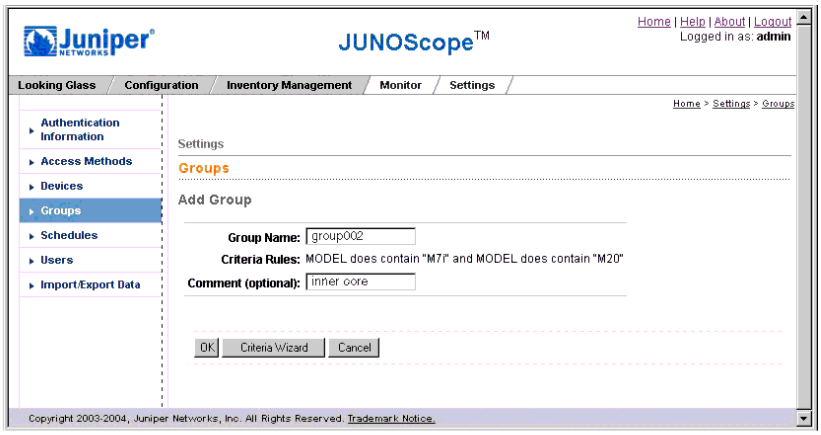


4. In the Comparisons drop-down list box, select the device information you want to compare. The available options include device name, device hostname, model, location, and comment.

5. Select either Text Compare or Numeric Compare, and do one of the following.
   a. For Text Compare, follow these steps:
      - From the first drop-down list box, select whether the comparison does or does not compare.
      - From the second drop-down list box, select whether the comparison contains, begins with, ends with, or equals.
      - In the text box, type the text that you want to compare.
   b. For Numeric Compare, follow these steps:
      - From the first drop-down list box, select whether the comparison is or is not a comparison.
      - From the second drop-down list box, select whether the comparison is greater than, less than, or equal to.
      - In the text box, type the value that you want to compare.
6. In the Add Condition dialog box, click OK. The Define Group Membership Criteria dialog box appears with the criteria rules displayed.

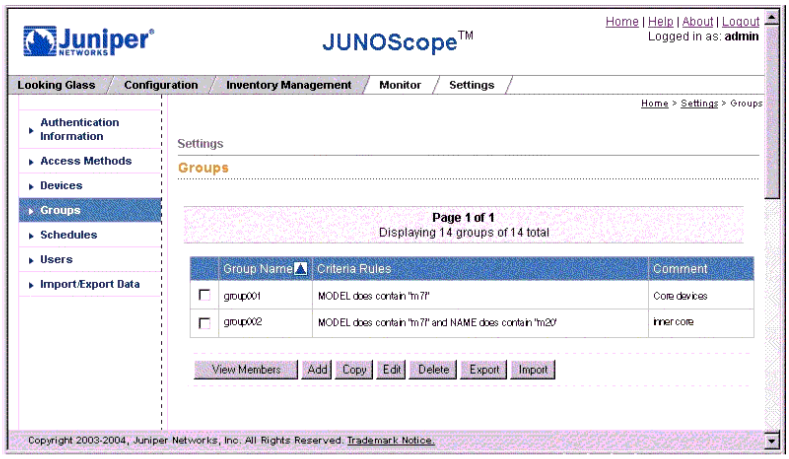


7. To add another rule, repeat Step 2 through Step 6.
8. In the Define Group Membership Criteria dialog box, click Exit Criteria Wizard. The Add Group dialog box appears.



9. In the Add Group dialog box, add a group name and an optional comment, then click OK.

   The group is added to the JUNOScope software database and the Groups dialog box.



Using a Label as a Group Rule Comparison

You can use a label as a comparison to create a group rule. You can select from existing label comparisons.

To use a label comparison to create a group rule, do the following:

1. From the JUNOScope main window, click Settings > Groups. The Group dialog box appears with the existing groups displayed.
2. Click Add, or select a group box and click Copy or Edit. The Add Group or Edit Group dialog box appears.
   - For information about adding a group, see “Adding a Group” on page 68.
   - For information about copying a group, see “Copying a Group” on page 75.

- For information about editing a group, see “Editing a Group” on page 76.

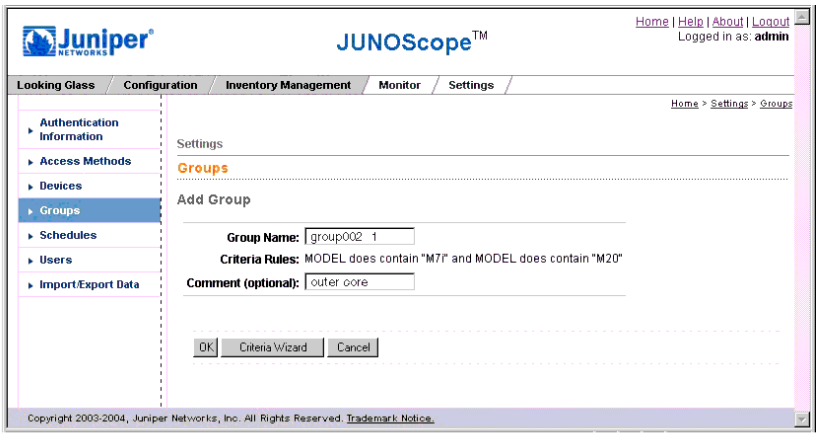
3. Click Criteria Wizard. The Define Group Membership Criteria dialog box appears.
4. Click Append. The Add Condition dialog box appears.
5. Select Has Label in the Comparisons drop-down list box. The Add Condition dialog box displays the available labels.
6. Select a label.
7. Click OK. The Define Group Membership Criteria dialog box appears from which you can exit the Criteria Wizard, view group members, add another rule condition, insert a condition, delete a rule condition, or cancel the operation.
   - For information about adding a group, see “Adding a Group” on page 68.
   - For information about copying a group, see “Copying a Group” on page 75.
   - For information about editing a group, see “Editing a Group” on page 76.

Copying a Group

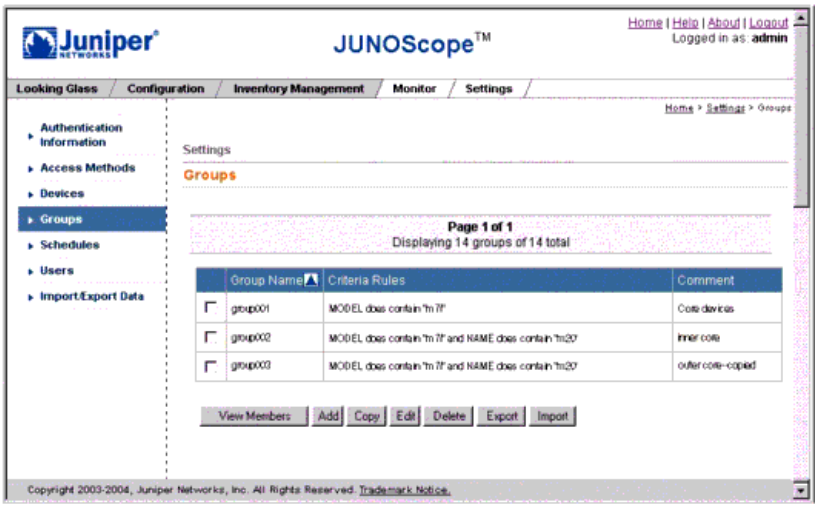
To copy a group that you have created, follow these steps:

1. In the JUNOScope main window, click Settings > Groups. The Groups dialog box appears with the added groups displayed.
2. Select the check box for the group you want to copy.
3. Click Copy.

   The Add Group dialog box appears. A 1 (the number one) appears after the group name (for example,*copied-group-name* 1).



4. You can edit the group name and the comment. You can also modify the group criteria by clicking Criteria Wizard. See “Adding a Group” on page 68.
5. Click OK. The copied group is added to the Groups dialog box.

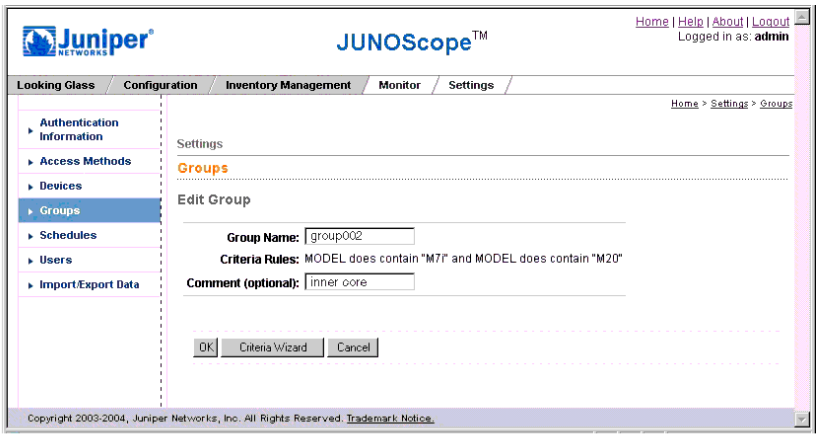


Editing a Group

You can edit the group information when you want to make changes to the group name, criteria rules, or comment.

To edit a group, follow these steps:

1. In the JUNOScope main window, click Settings > Groups. The Groups dialog box appears.
2. Select the check box for the group you want to edit.
3. Click Edit. The Edit Group dialog box appears.



4. You can edit the group name or the comment. The group name can be up to 20 characters in length. The comment can be as long as you want.

   You can also edit the criteria rule by clicking Criteria Wizard and following these steps:

a. Click Criteria Wizard. The Define Group Criteria dialog box appears.

b. If you are adding a new rule to the existing selection criteria, select a criteria rule option.

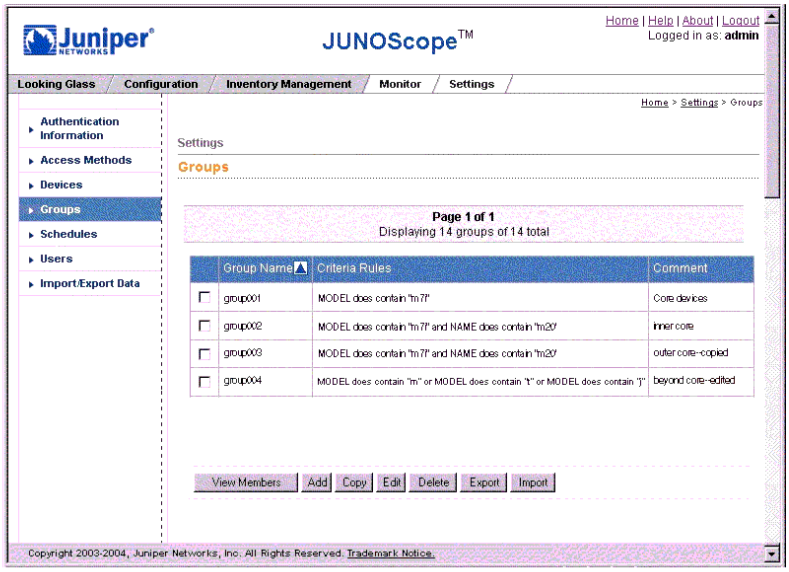
c. Select the Logic option that you want in the Logic drop-down list box; either AND or OR.

d. Click one of the following:

- Exit Criteria Wizard—Exits the criteria wizard without adding a new criteria rule.
- View Members—Displays the devices that are in the group.
- Append—Adds the new rule to end of the existing rule.
- Insert After—Inserts the new rule after the existing rule.
- Insert Before—Inserts the new rule before the existing rule.
- Delete—Deletes the selected rule.

e. Click Exit Criteria Wizard. The edited group information appears in the Edit a Group dialog box.

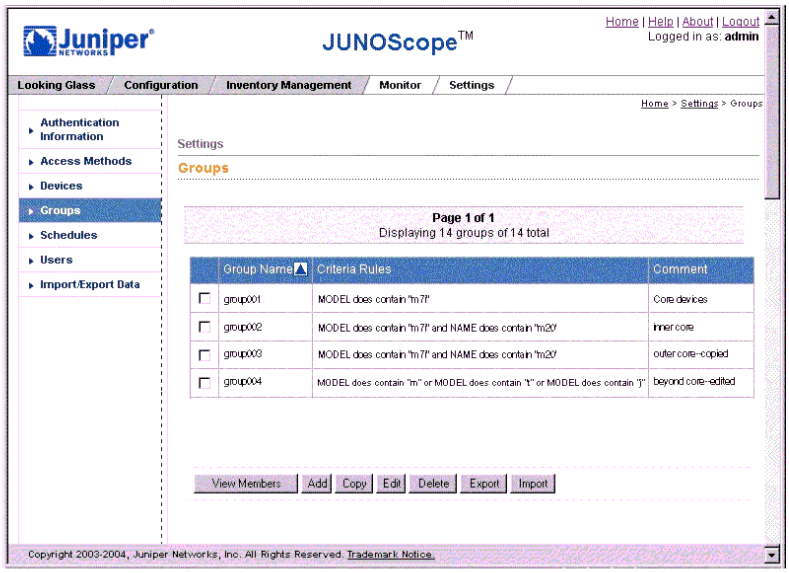
f. Click OK. The Groups dialog box appears with the edited group information. The group information is also updated in the JUNOScope software database.



Viewing Groups

You can view device groups that are available for management.

To view groups, in the JUNOScope main window, click Settings > Groups. The Groups dialog box appears with the groups listed in alphabetical, ascending order by group name, criteria rules, and comment.



Click a table column name to sort by that column. Clicking the column name toggles between ascending and descending sort order.

From the Groups dialog box, you can add a new group, view group members, edit an existing group, copy a group, or delete a group.

Viewing Group Members

You can view the devices or members that are included in a group.

To view group members, follow these steps:

1. In the JUNOscope main window, click Settings > Groups. The Groups dialog box appears with the added groups displayed.
2. In the Groups dialog box, select the check box for one or more groups for which you want to view members.
3. Click View Members. The Group Members dialog box appears.

The Group Members dialog box displays the names of all devices in the selected group(s).

4. Click OK.

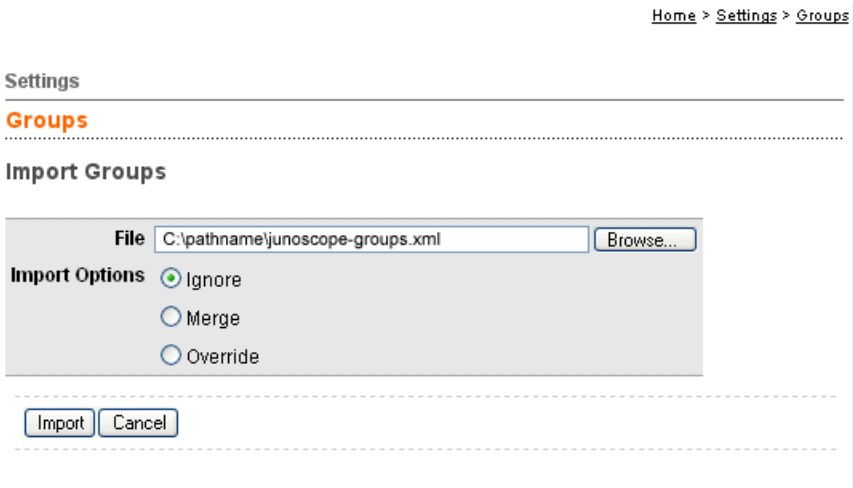
Importing Group Information

NOTE: You can only import a group that you have exported from another JUNOScope server. You cannot import a group using a modified export-import-sample.xml file. For more information about exporting group setup data, see "Exporting Group Information" on page 81.

Importing group information is useful when you do not want to enter setup information manually.

To import group information, follow these steps:

1. In the JUNOScope main window, click Settings > Groups. The Groups dialog box appears.
2. Click Import. The Import Groups dialog box appears.



3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default groups.xml file exported from another JUNOScope server.

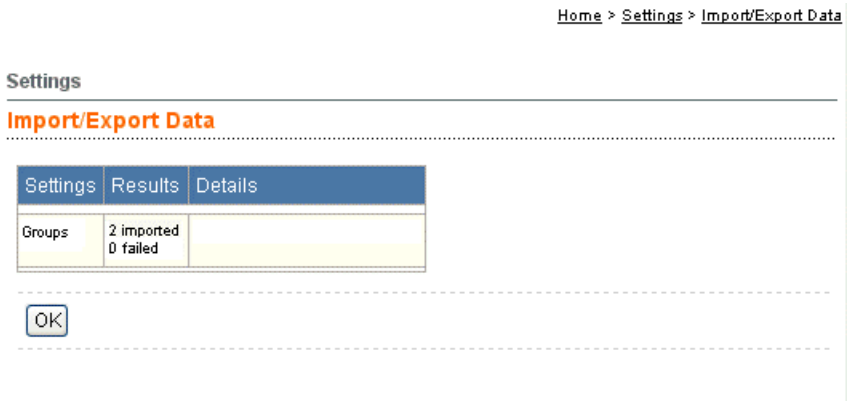
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:

   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

5. Click Import. The Import status dialog box appears.



The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

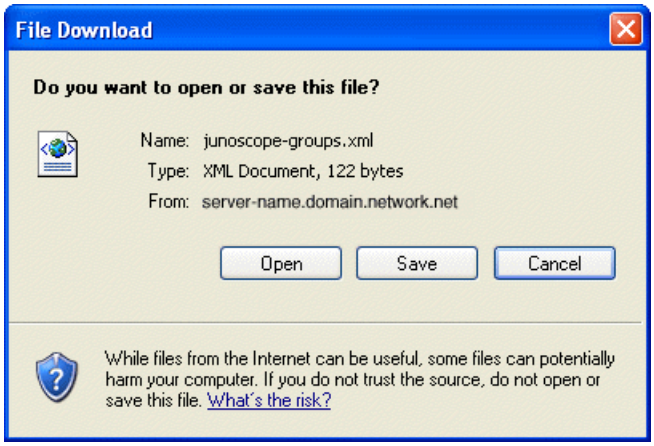
6. Click OK. The imported data is listed in the Groups dialog box.

Exporting Group Information

You can export group information that you want to save to the local file system or import to another JUNOScope server.

To export group information, follow these steps:

1. In the JUNOScope main window, click Settings > Groups. The Groups dialog box appears.
2. Click Export. The File Download dialog box appears.



3. In the File Download dialog box, click Save to export the file and save it to the local file system in a file named junoscope-groups.xml. Click Open to view the contents of the export XML file.
4. Click Export.

Deleting a Group

You can delete group information from the JUNOScope software database. When you delete a group, you are not deleting the devices. You only delete the information that groups the devices from the JUNOScope software database.

NOTE: You cannot delete a group that is used in a scheduled operation. You must first delete the operation scheduled for the group, then delete the group using the Settings > Groups command. See "Managing Operations" on page 313.

To delete a group, follow these steps:

1. In the JUNOScope main window, click Settings > Groups. The Groups dialog box appears.
2. Select one or more groups that you want to delete.
3. Click Delete.

   The group is deleted from the JUNOScope software database. Any scheduled operations associated with the group will fail unless you remove the operation. For more information, see "Managing Operations" on page 313.

Chapter 8

Setting Up Labels

This chapter describes how to create labels, or text names, that help you to statically organize a large group of devices on the network so that JUNOScope operations, such as archive configuration and scan inventory, can be performed on them.

A label consists of a unique name, a category used to logically organize labels, and a comment to describe the purpose of the label. For example, you could create the following labels—North, South, East, and West—in a category called Region.

You can associate an existing label with one or more devices. You can also use a label as a rule in the group criteria wizard for setting up groups of devices. For more information about associating a device with a label, see "Setting Up Devices" on page 57. For more information about using a label as a criterion for creating a group, see "Setting Up Groups" on page 67.

You can edit, copy, and delete labels. Additionally, you can import labels that have been saved to the local file system from another JUNOScope server and export them to the local file system.

You must have superuser permissions to set up labels.

The following topics describe how to set up labels using the JUNOScope software:

Adding a Label

To add a label, follow these steps:

1. Click Settings > Labels. The Labels dialog box appears. The Labels dialog box is empty until you add labels.
2. Click Add. The Add Label dialog box appears.

3. In the Name text box, type a label name.

   A label must have a unique name that does not match any existing label or group name used in the JUNOScope software. For example, you could use a network name, customer name, a specific service name, and so on. The label name can be up to 40 characters long.

4. In the Category text box, type a category for the label. The category is a name that you can use to group related labels. For example, you can specify the type of network, a customer location, or the type of device. The category name is 40 characters long.

5. In the Comment text box, type an optional comment. The comment should describe the purpose of the label.

6. Click OK. The label is listed in the Labels dialog box. For more information, see "Viewing Labels" on page 85.

Associating Devices with a Label

You can associate devices that have been added to the JUNOScope software with an existing label. Associating a label with a device lets you statically control JUNOScope operations that occur on multiple devices, such as archiving a device configuration or scanning device inventory.

To associate a label with a device, follow these steps:

1. Click Settings > Labels. The Labels dialog box appears.

2. Click Associate Devices in the Actions column for the label that you want to associate. The Associate Devices to Label dialog box appears.

3. Select one or more available devices that you want to associate with the selected label:

   - Use Shift + click to select several devices in a row in the Available Devices list box.
   - Use Ctrl + click to randomly select several devices in the Available Devices list box.
   - Click Add to add the selected available devices to the Selected Devices list box.
   - Click Add All to add all of the selected devices to the Selected Devices list box.
   - Click Remove to clear selected devices from the Selected Devices list box.
   - Click Remove All to clear all devices from the Selected Devices list box.

4. Click OK.

Editing a Label

You can edit a label name, category, or optional comment.

To edit a label, follow these steps:

1. Click Settings > Labels. The Labels dialog box appears.
2. Click Edit in the Actions column for the label you want to edit. The Edit Label dialog box appears.
3. Edit the label name, category, or comment.
4. Click OK.

Copying a Label

Copying a label provides a quick way of adding similar labels. You must however, edit the label name so that it is unique.

To copy a label, follow these steps:

1. Click Settings > Labels. the Labels dialog box appears.
2. Click Copy in the Actions column of the label you want to copy. The Copy Label dialog box appears.
3. Edit the label name so that it does not match any other label name. You can also edit the label category or comment.
4. Click OK.

Viewing Labels

You can view, at a glance, the labels that you have added.

To view existing labels, follow these steps:

1. Click Settings > Labels. The Labels dialog box appears.
2. You can sort the Name, Category, and Comment columns in ascending or descending order. Click a column to sort it in ascending order; click the column again to sort it in descending order.

Importing a Label

You can import labels that have been saved to the local file system from another JUNOScope server.

To import labels from a file on the local file system, follow these steps:

1. Click Settings > Labels. The Import Labels dialog box appears.
2. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and

the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

3. Click Import. The Import Results dialog box appears indicating the import status of the label.
4. Click OK. The imported data is listed in the Labels dialog box.

Exporting a Label

You can export all labels that you have added to a file on the local file system. The label information is exported in XML format. The resulting file is called export.

To export all label information, follow these steps:

1. Click Settings > Labels. The Labels dialog box appears.
2. Click Export. The File Download dialog box appears.
3. Click Save to export the labels data and save it to the local file system in a file named junoscope-labels.xml. Click Open to view the labels export file content.
4. Navigate to where you want to save the Label export file.
5. Click Save.

Deleting a Label

You can delete labels that you no longer need.

To delete a label, follow these steps:

1. Click Settings > Labels. The Labels dialog box appears.
2. Click Delete in the Actions column for the label that you want to delete.

   The label is deleted from the JUNOScope database provided no scheduled operation is using the label. If the label is being used by a scheduled operation, a message appears stating that the label is already in use. In that case, delete

the scheduled operation that includes the labels you want to delete (see “Deleting a Schedule” on page 96).

Chapter 9

Setting Up Schedules

This chapter describes how to set up schedules for running a configuration management operation, such as archive, restore, and inventory scan. You can specify the date, time, and interval when you want a JUNOScope software operation to occur.

A schedule is an independent entity that has no effect until you use it for an operation. When you set up a schedule, you are not doing anything operation related. You can use the same schedule for multiple operations.

When you want to see information about when an operation ran and when it is scheduled to run again, use the Manage > Operations command (see "Viewing Scheduled Operations" on page 313). The Operations page provides status information only for operations run using an existing schedule not for operations run using the Now schedule option.

You can import schedule information from another JUNOScope server or export it as backup or for importing to another server.

You must have superuser permission to set up a schedule.

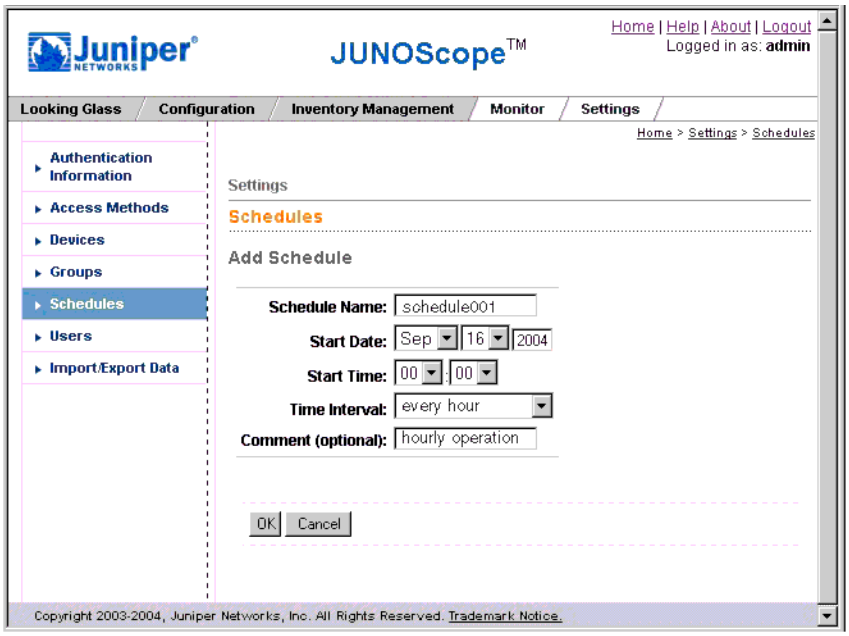
This chapter includes the following topics:

Adding a Schedule

As the JUNOScope software administrator, you can add a schedule for archiving a configuration file from an added router.

To add a schedule, follow these steps:

1. In the JUNOScope main window, click Settings > Schedules. The Schedules dialog box appears.
2. Click Add. The Add Schedule dialog box appears.



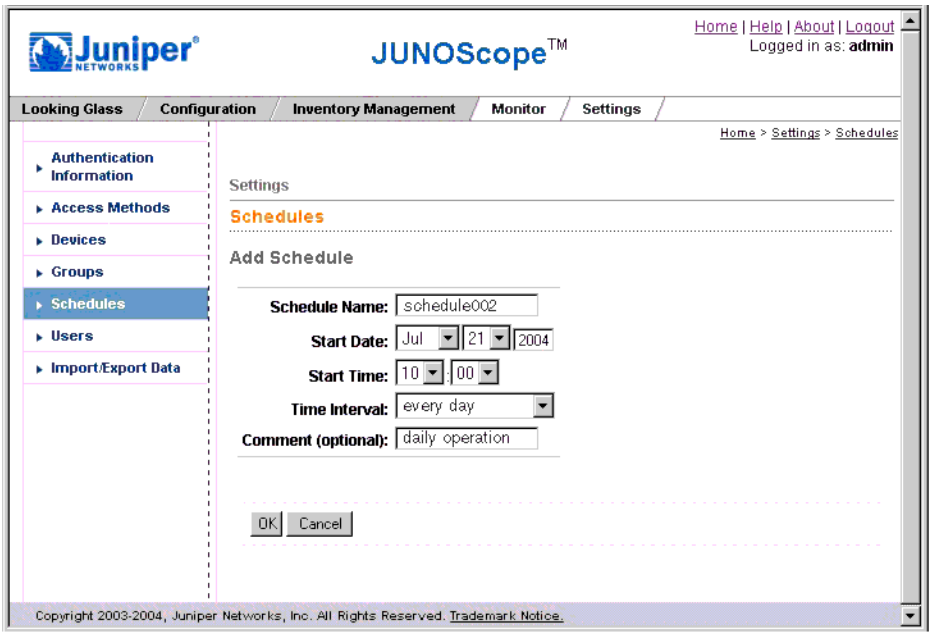
3. In the Schedule Name text box, type a name for the archive schedule that you want to add. The schedule name must be less than 20 characters long.
4. In the Start Date drop-down list boxes, select a schedule start date.
5. In the Start Time drop-down list boxes, select a schedule start time.
6. In the Time Interval drop-down list box, select the schedule time interval.
7. In the Comment text box, type an optional descriptive schedule comment.
8. Click OK.

   The schedule is saved in the JUNOScope software database and is listed in the Schedules dialog box.

Copying a Schedule

To copy a schedule that you have added, follow these steps:

1. In the JUNOScope main window, click Settings > Schedules. The Schedules dialog box appears.
2. Select the check box for the schedule you want to copy.
3. Click Copy. The Add Schedule dialog box appears.



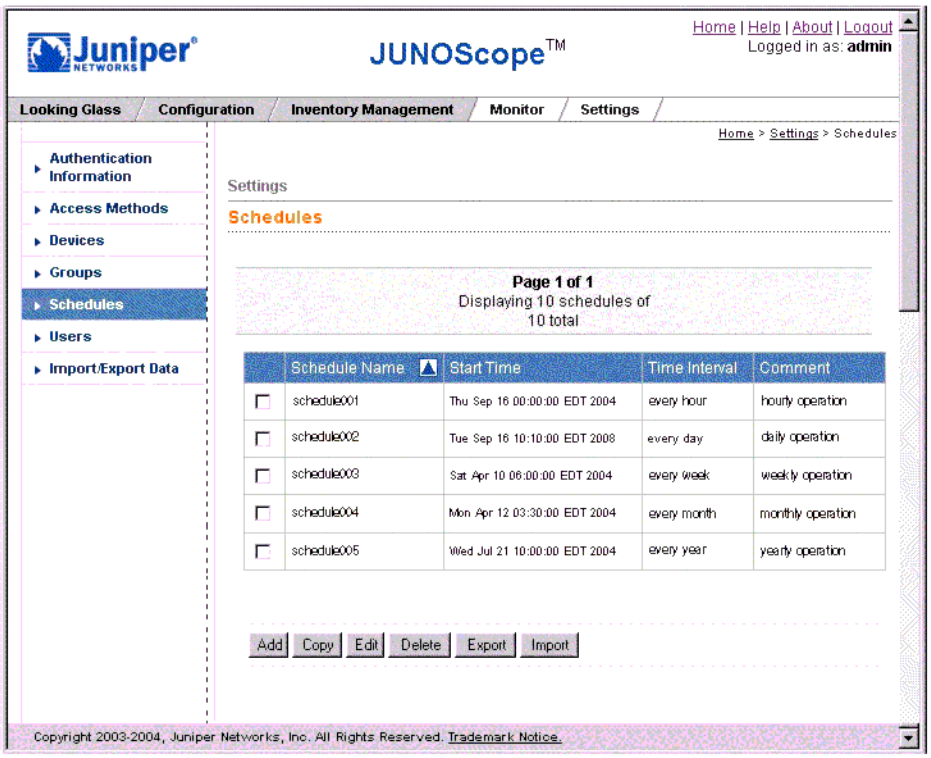
The copied schedule appears with a 1 (the number one) after its name.

4. Edit the copied schedule appropriately using the procedure “Editing a Schedule” on page 92.
5. Click OK. The copied schedule is listed in the Schedules dialog box.

Viewing Schedules

You can view all schedules that have been added for JUNOScope software management.

To view schedules, in the JUNOScope main window, click Settings > Schedules. The Schedules dialog box appears with the list of added schedules.



From the Schedules dialog box, you can add, edit, or delete one or more schedules.

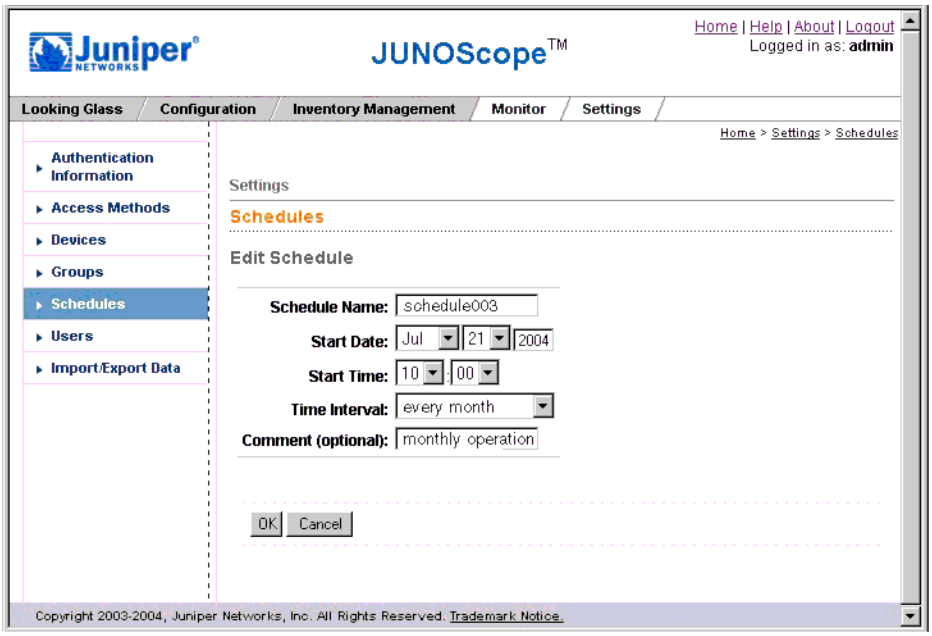
Click a table column name to sort by that column. Clicking the column name toggles between ascending and descending sort order.

Editing a Schedule

You can edit a schedule when you want an operation, such as archiving, to occur at a different time.

To edit a schedule, follow these steps:

1. In the JUNOScope main window, click Settings > Schedules. The Schedules dialog box appears.
2. Select the schedule that you want to edit.
3. Click Edit. The Edit Schedule dialog box appears.



4. Edit the schedule information as needed.
5. Click OK.

   The edited schedule information is stored in the JUNOScope software database and listed in the Schedules dialog box.

Importing Schedule Information

You can import device information from another JUNOScope server, or you can use the provided sample XML import file export-import-sample.xml as a guide.

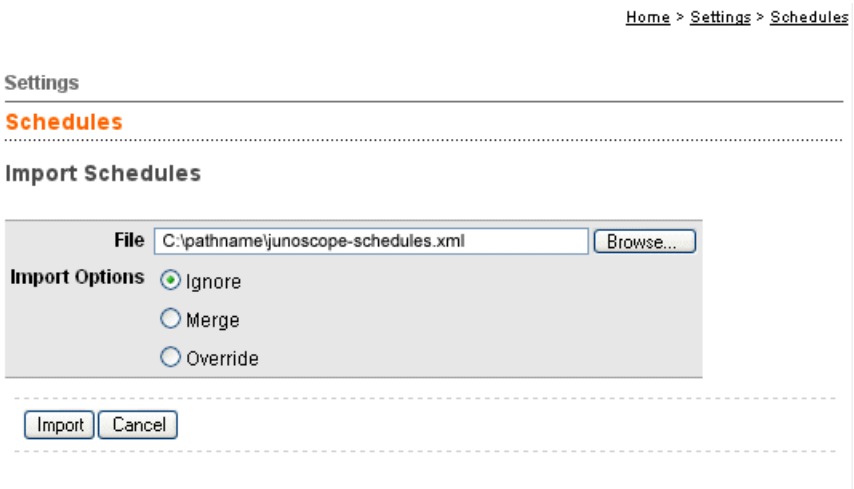
NOTE: Use only utc-milliseconds in the <start-time> element. This is the number of milliseconds since the epoch January 1, 1970. The <start-time> element text is ignored. The <period> element text can be every minute, every 5 minutes, every 15 minutes, every 30 minutes, every hour, every 6 hours, every 12 hours, every day, every 2 days, every week, every two weeks, every month, or every year.

Importing device information is useful when you do not want to enter setup information manually.

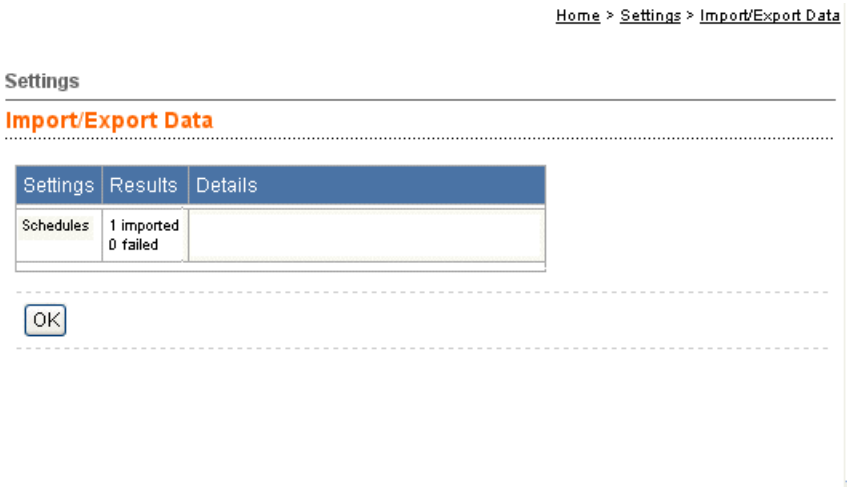
Importing access method or authentication information is useful when you want to use existing access method and authentication data that you have exported from another JUNOScope software server instead of adding that information manually.

To import schedules information, follow these steps:

1. In the JUNOScope main window, click Settings > Schedules. The Schedules dialog box appears.
2. Click Import. The Import Schedules dialog box appears.



3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default schedules.xml export file from another JUNOScope server or use the provided sample export-import-sample.xml XML file on the JUNOScope server to generate a file to import.
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.
5. Click Import. The Import status dialog box appears.



The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

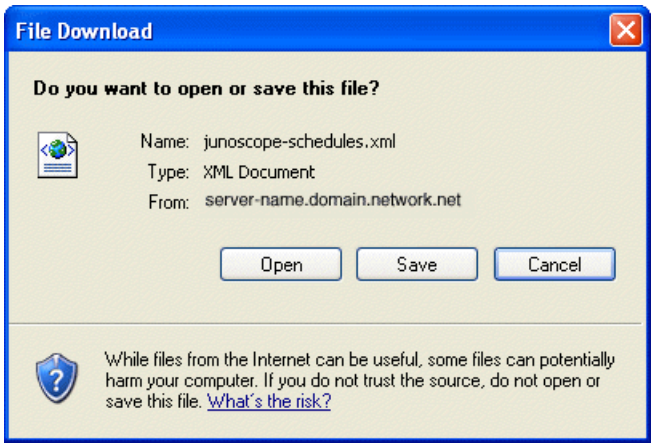
6. Click OK. The imported data is listed in the Groups dialog box.

Exporting Schedule Information

You can export schedule information that you want back up or import to another JUNOScope server.

To export schedule information, follow these steps:

1. In the JUNOScope main window, click Settings > Schedules. The Schedules dialog box appears.
2. Click Export. The File Download dialog box appears.



3. Click Save to export the schedule information to the local file system in a file named junoscope-schedules.xml. Click Open to view the contents of the schedule export file.

Deleting a Schedule

You can delete an operation schedule that you no longer want to occur.

NOTE: You cannot delete a schedule that is scheduled to be run. You must delete the operation first, then delete the schedule. See "Managing Operations" on page 313.

To delete a schedule, follow these steps:

1. In the JUNOScope main window, click Settings > Schedules. The Schedules dialog box appears.
2. Select the schedule(s) that you want to delete. You can delete one or more schedules at a time.
3. Click Delete. The schedule information is deleted from the Manage Schedules dialog box and from JUNOScope software database.

Chapter 10

Setting Up User Local Authentication

This chapter describes how to set up users to use the JUNOScope software to run configuration management operations and monitor Juniper Networks routing platforms.

You can add the users you want to log in to and use the JUNOScope software, and specify user groups with permissions to perform authorized JUNOScope software operations. You can add, change, and delete JUNOScope software user information when personnel changes occur.

You can import user information from another JUNOScope server or export it as backup or for importing to another server.

You must have superuser permission to set up users.

This chapter includes the following topics:

Predefined User Groups

There are four predefined user groups. The administrator can create other user groups, but each user group must be associated with one permission level. For information about JUNOScope software permission levels, see “Predefined User Groups” on page 107, “User Group Permission Levels” on page 108, and “Permissions and JUNOScope Feature Access Privileges” on page 108.

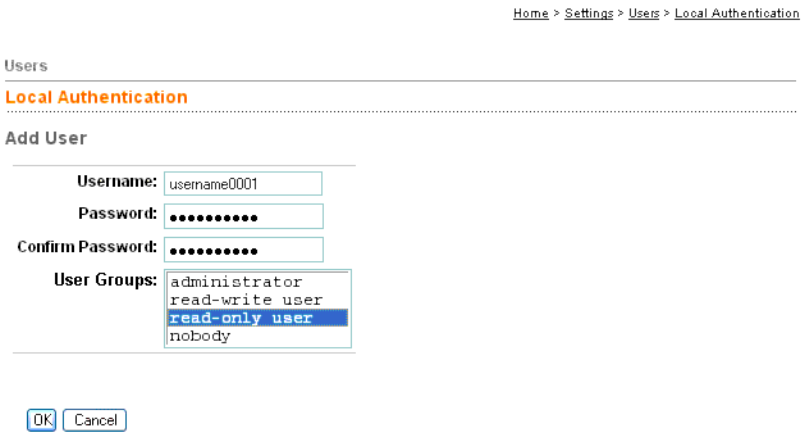
- Administrator—A user group that has full access to the JUNOScope software. (Settings menu) and read and write privileges to JUNOScope managed devices. The initially configured JUNOScope installer is always part of this user group. The administrator user group has read-write access to all devices.
- Read-write user—A user group that has read-write privileges to JUNOScope managed devices and operations. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having read-write permission is added to this user group.
- Read-only user—A user group that has only read privileges to JUNOScope managed devices and operations. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having read-only permission is added to this user group.
- Nobody—A user group that can only log in to the JUNOScope software. The nobody user group does not have access to any JUNOScope managed devices. No devices or device groups can be associated with this user group.

Adding a User

You can enable users to perform certain JUNOScope operations. Each user must have a username, password, and permissions.

To add a user, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Local Authentication. The Local Authentication dialog box appears.
2. Click Add. The Add User dialog box appears.



3. In the Username text box, type the name of the user you want to add. The username can be up to 20 characters long.
4. In the Password text box, type the user password. The user password should be between 6 and 128 characters long.

   A JUNOScope software password should meet the following restrictions:

   - Allow the full range of ASCII characters (except control characters).

- Enforce a minimum of 6 characters.
- Require a change in the character set, including uppercase, lowercase, numeric, and punctuation.

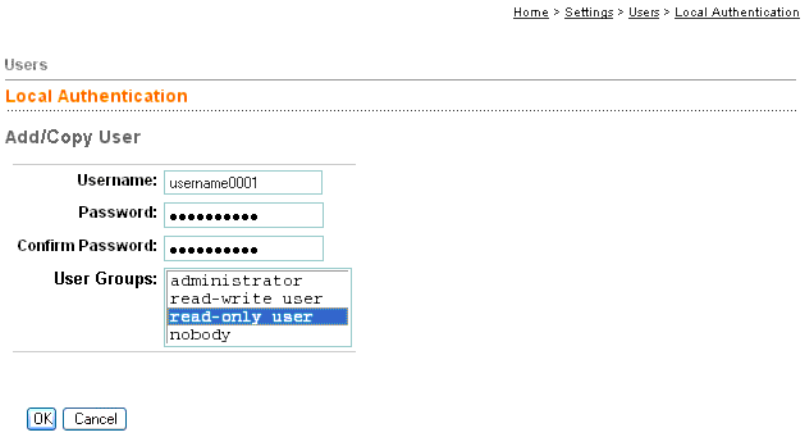
5. In the Confirm Password text box, retype the user password to confirm it.
6. In the User Groups drop-down list box, select one or more user groups for the user. Press Ctrl + click to select several user groups randomly. Press Shift + click to select several user groups in a row. For more information about user groups and permissions, see "Predefined User Groups" on page 97, "User Group Permission Levels" on page 108, and "Permissions and JUNOScope Feature Access Privileges" on page 108.
7. Click OK.

   The new user is added to the JUNOScope software database and listed in the Users dialog box by username, access privilege level, and toolbox access level.

Copying a User

To copy a user that you have added, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Local Authentication. The Local Authentication dialog box appears.
2. Select the check box for the user you want to copy.
3. Click Copy. The Add/Copy User dialog box appears.



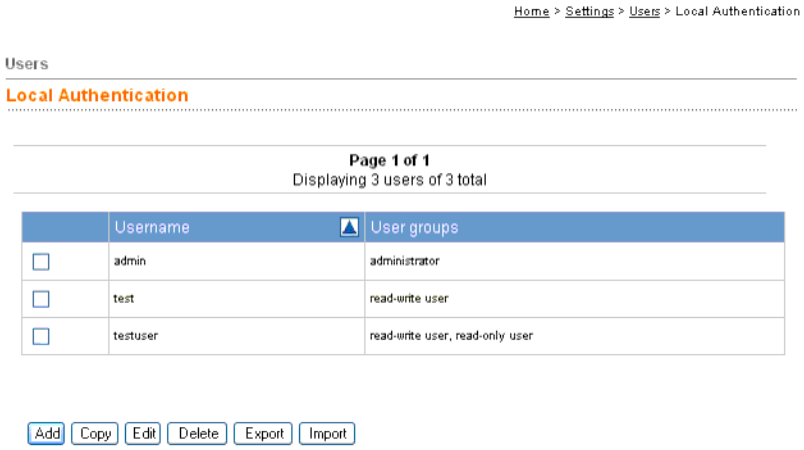
   The copied user appears with a 1 (the number one) after the name.

4. Edit the copied user information using the procedure "Editing User Information" on page 100.

Viewing Users

You can view a list of users and other administrators who have access privileges to use the JUNOScope software.

To view JUNOScope software users, in the JUNOScope main window, click Settings > Users > Local Authentication. The Local Authentication dialog box appears with a list of all added users by username and permissions.



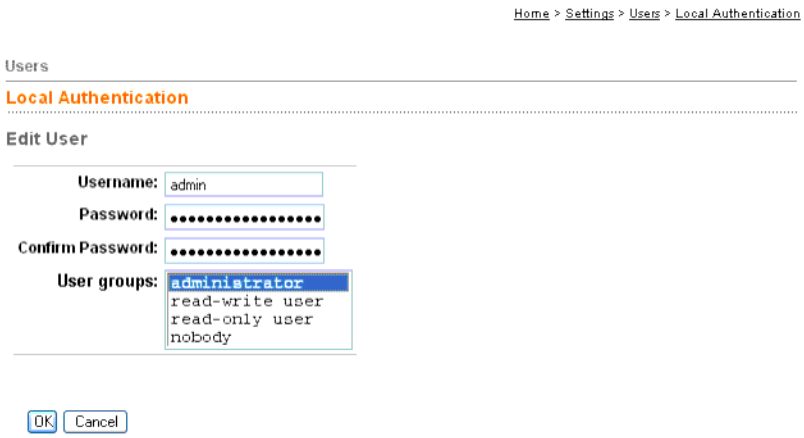
From the Local Authentication dialog box, you can add, edit, or delete JUNOScope software users. Click a table column name to sort by that column. Clicking the column name toggles between ascending and descending sort order.

Editing User Information

You can make changes to user information when personnel changes occur.

To edit user information, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Local Authentication. The Local Authentication dialog box appears.
2. Select the check box for the user that you want to edit.
3. Click Edit. The Edit User dialog box appears.



4. Edit the user information as needed:

   a. In the Username text box, type the name of the user you want. The username can be up to 20 characters long.

   b. In the Password text box, type the user password. The user password should be between 6 and 128 characters long.

      A JUNOScope software password should meet the following restrictions:

      - Allow the full range of ASCII characters (except control characters).
      - Enforce a minimum of 6 characters.
      - Require a change in the character set, including uppercase, lowercase, numeric, and punctuation.

   c. In the Confirm Password text box, retype the user password to confirm it.

5. In the User Groups drop-down list box, select the user groups for the user. Press Ctrl + click to randomly select several user groups. Press Shift + click to select several user groups in a row. For more information about user groups and permissions, see "Predefined User Groups" on page 107, "User Group Permission Levels" on page 108, and "Permissions and JUNOScope Feature Access Privileges" on page 108.

6. Click OK.

   The user information is changed in the JUNOScope software database. The changed username or permissions appear in the Users dialog box.

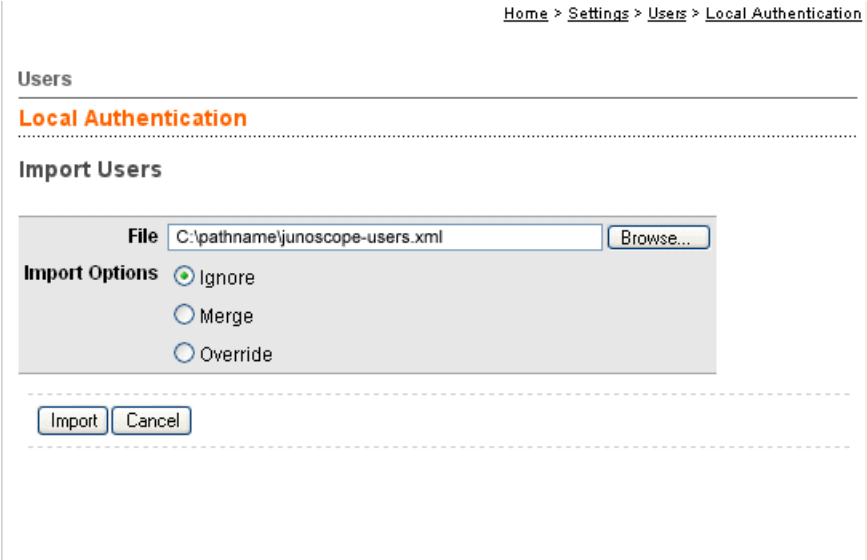
Importing User Information

You can import user information from another JUNOScope server, or you can use the provided sample XML import file export-import-sample.xml as a guide.

Importing user information is useful when you do not want to enter setup information manually.

To import user information, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Local Authentication. The Local Authentication dialog box appears.
2. Click Import. The Import Users dialog box appears.



3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default users.xml export file from another JUNOScope server or use the provided sample export-import-sample.xml XML file on the JUNOScope server to generate a file to import.
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

5. Click Import. The Import status dialog box appears.

The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

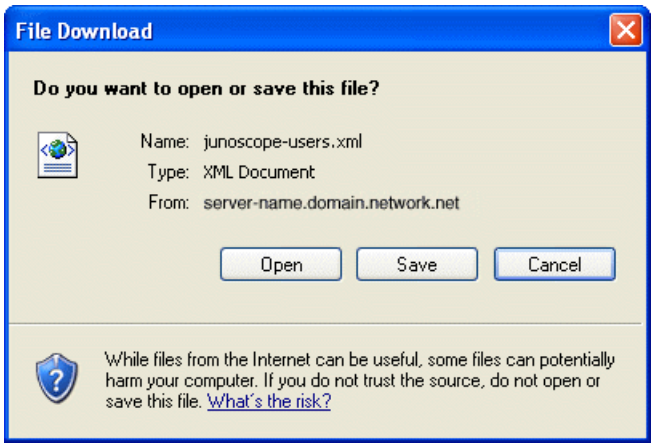
6. Click OK. The imported data is listed in the Users Local Authentication dialog box.

Exporting User Information

You can export user information that you want to save to the local file system or import to another JUNOScope server.

To export user information, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Local Authentication. The Local Authentication dialog box appears.
2. Click Export. The File Download dialog box appears.



3. Click Save to save the RADIUS authentication data and export it to the file system in a file named junoscope-radiusClients.xml. Click Open to view the contents of the export file.

Deleting a User

The JUNOScope software administrator can delete users who no longer need to perform JUNOScope operations.

To delete a user, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Local Authentication. The Local Authentication dialog box appears.
2. Select the check box for the user you want to delete.
3. Click Delete.

   The user is removed from the JUNOScope software database and the Users dialog box.

Chapter 11

Setting Up User Group Authorization and Viewing User Permissions

This chapter describes how to set up JUNOScope user group authorization for device access based on the user group association. The JUNOScope administrator can assign one or more users to belong to a user group.

There are two types of user groups: predefined and user-defined. After the JUNOScope software is installed, there are four predefined user groups, each associated with a permission level, and no user-defined user groups. The four pre-defined user groups are:

- Administrator
- Read-write user
- Read-only user
- Nobody

Each user group must have a permission level assigned to it. Four permission levels are available:

- Superuser
- Read-write
- Read-only
- None

The name and permission level assigned to the four predefined user groups are fixed, and cannot be changed or deleted.

If this group-based authorization feature is not used, the JUNOScope administrator does not have to create any new user-defined user groups. The administrator can simply treat three predefined user groups—for example, administrator, read-write user, and read-only user—as the three distinct permission levels of superuser, read-write, and read-only.

You can assign any name to user-defined user groups except for names that already exist, however, the permission level available is limited to read-only and read-write. In other words, the administrator cannot create a new user group with either superuser or none permission levels. The administrator and nobody user groups have unique authorization privileges across all devices.

The nobody user group and none permission level allow a user account to be created without access permission to any device, for example, a guest or demo account.

Each user must belong to at least one user group, but a user can belong to multiple user groups. A user assigned to multiple user groups will have the least restrictive permission. The order of permission restrictions, from least to the highest, is superuser, read-write, read-only, and none.

The administrator can assign a user group either read-only or read-write access permission to available devices and device groups that have been configured in the JUNOScope software. When a user group is assigned read-write access to devices or device groups, the users in the user group can do read-write operations on those devices and device groups, such as Configuration > Repository > Archive and Restore. When a user group is assigned read-only access to devices or device groups, the users in the user group can do read-only operations on those devices and device groups in the read-only operations, such as Monitor > Status and Configuration > Current > View. However, a user belonging to two user groups—one read-write and one read-only—has read-write access to devices and device groups in read-write user groups. Devices and device groups listed for read-only user groups are not available for write actions.

When devices are added to a device group, the device list includes only those devices to which the user has access permission. A user in a user group with access to a device group can operate on those members of the device group to which the user has access. For example, user group usergroup1 has read-write permission. usergroup1 has read-write access to devices device1, device2, and device3. usergroup1 also has read-write access to device group devgroup1. devgroup1 has device members device1, device2, device3, and device4. In this case, when user user1 belonging to usergroup1 tries to use devgroup1 in a read-write operation, such as Archive, devgroup1 will be expanded to member devices device1, device2, and device3.

NOTE: The device device4 will not be in the expanded list of members of devgroup1 in the archive operation.

If a user group has either superuser or read-write permission, it has read-write access to all devices associated with that user group. If the user group has read-only permission, it has read-only access to all devices associated with that user group. If a user group has no access, it can only log in to the JUNOScope software, but cannot access any devices.

The administrator user group has full permission to all devices on the network configured in the JUNOScope software. The administrator can create a network operations center (NOC) technician user group that has read-write permission to all devices configured in a network region. The administrator can also create a network operations center (NOC) operator user group that has read-only access to monitor all devices configured on the network.

You must belong to the administrator user group to set up user groups and edit associations among user groups, users, devices, or device groups.

Using Monitor > Operations, users can monitor scheduled operations of users belonging to the same user group, but can not view operations scheduled by users

belong to different user groups. Users belonging to the administrator user group can monitor operations scheduled by any user.

Using Settings > Saved Operations, users can use only those saved operations that have been created by users belonging to the same user group, but cannot use saved operations created by users belonging to different user groups. Users belonging to the administrator user group can use saved operations created by any user.

This chapter includes the following topics:

Predefined User Groups

There are four predefined user groups. The administrator can create other user groups, but each user group must be associated with one permission level.

- Administrator—A user group that has full access to the JUNOScope software. (Settings menu) and read and write privileges to JUNOScope managed devices. The initially configured JUNOScope installer and administrative user is always part of this user group. The administrator user group has read-write access to all devices. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having superuser permission level is added to this user group.
- Read-write user—A user group that has read-write privileges to JUNOScope managed devices and operations. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having read-write permission is added to this user group.
- Read-only user—A user group that has only read privileges to JUNOScope managed devices and operations. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having read-only permission is added to this user group.
- Nobody—A user group that can only log in to the JUNOScope software. The nobody user group does not have access to any JUNOScope managed devices. No devices or device groups can be associated with this user group.

User Group Permission Levels

There are four user group permission levels. The permission level of a user group determines what JUNOScope tasks or operations a user can perform and the level of device access.

- Superuser—Performs all JUNOScope management functions, manages user accounts, views and modifies JUNOScope settings, and has full access to devices
- Read-write—Has full access to devices with all functions available, but cannot set up JUNOScope settings.
- Read-only—Can view a device configuration, but cannot modify it, or perform any operation
- None—Is denied access to any devices and can only log in.

Permissions and JUNOScope Feature Access Privileges

Table 8 on page 108 describes the authorization that a user group needs to perform JUNOScope software tasks and access devices on the network that have been configured for element management.

Users with none permission can view the same JUNOScope operations as a user with read-only permission. The difference is that users with none permission cannot see or access any devices.

Table 8: JUNOScope User Group Permissions and Access Privileges

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Install, reinstall, upgrade, or downgrade JUNOScope software	X	—	—	—	The JUNOScope software installation is performed by the application installer.
Upgrade JUNOScope from a previous release	—	—	—	—	If the installer upgrades the JUNOScope software from an earlier version, existing users are assign to one of the three predefined user groups (administrator, read-write user, and read-only user), based on their existing permission level. In other words, users with superuser permission are put into the administrator user group; users with read-write permission are put to the read-write user group; and users with read-only permission are put into the read-only user group.
Looking Glass					

Table 8: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Query	X	X	X	X	Superuser, read-write, or read-only permission is required to access Looking Glass. Looking Glass reports require read-write or read-only permissions to a selected device. When a user, under a given user group, runs a query, the Device list is populated only with devices with read or read-write access.
Configuration Manager					
Configuration Browser	X	X	X	X	Superuser, read-write, or read-only permission is required for a user to browse a device configuration. Read-write or read-only permission is required for a user to browse a device configuration. The Device drop-down list box is populated only with devices with read-write or read-only access.
Configuration Editor	X	X	—	—	Superuser or read-write is required for a user to edit a device configuration. Read-write permission is required for a user to edit a device configuration. The Device drop-down list box is populated only with devices with read-write access.
Archive	X	X	—	—	Superuser or read-write permission is required for a user in a user group to archive a configuration in the JUNOScope repository. The Group and Select Device(s) drop-down list boxes are populated only with groups or devices with read-write access.
Archive Tag	X	X	—	—	Superuser or read-write permission is required to use Archive Tags. The Selected Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.
Archive Configurations	X	X	—	—	Superuser or read-write permission is required to use Audit Configurations. The Selected Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.

Table 8: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Import	X	X	—	—	Superuser or read-write permission is required for a user to import a configuration into the JUNOScope repository. Importing a configuration does not have any association with a device, therefore the user group requirement for import is read-write access for any device.
Compare	X	X	X	X	Superuser, read-write, or read-only permission is required for a user to compare configuration file versions in the JUNOScope repository. The Device drop-down list box is populated only with devices with read-write or read-only access.
Display	X	X	—	X	Superuser or read-write permission is required for a user to view a configuration file in the JUNOScope repository. The Device drop-down list box is populated only with devices with read-write or read-only access.
Restore	X	X	—	—	Superuser or read-write permission is required to restore a device configuration. The Device drop-down is populated only with devices with read-write access.
Inventory Management					
Scan	X	X	—	—	Superuser or read-write permission is required to scan a device for inventory. The Group and the Select Device(s) drop-down list box is populated only with groups or devices with read-write access.
Reports > Inventory	X	X	X	X	Superuser, read-write, ore read-only permission is required to view inventory reports. The Device drop-down list box in the Search and Advanced Query dialog boxes are limited to those devices with read or read-write access. In the Custom Report page, only those reports created by users in the same user group are visible. Read-only users cannot save or delete custom reports.
Reports > Demo	X	X	X	X	Superuser, read-write, ore read-only permission is required to view Demo reports. Read-only users cannot save or delete custom reports.
Repository > Schedule	X	X	—	—	Superuser or read-write permission is required.

Table 8: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Repository > View	X	X	—	—	Superuser or read-write permission is required.
Software Management					
Images	X	—	—	—	Device read-write access is required for users in a user group to perform operations, including image import, download, install, and delete.
Monitor					
Operations	X	X	X	X	Only those operations scheduled by users in the same user group are visible. Users in the Administrator user group can view all operations. Read-only users cannot delete operations.
Status	X	X	X	X	The Group and Selected Device drop-down list boxes are limited to those devices with read-only or read-write access. Even when All Devices is selected, a subset of the device operation status is shown, based on the user group. Users in the administrator user group can view all status.
Audit Log	X	—	—	—	Users in the administrator user group can only view Audit Log events.
Purge	X	—	—	—	Users in the administrator user group can purge Status records and Audit Log events.
Settings					
Authentication Information	X	—	—	—	Only users in the administrator user group can view this page.
Access Methods	X	—	—	—	Only users in the administrator user group can view this page.
Devices	X	—	—	—	Only users in the administrator user group can view this page.
Groups	X	—	—	—	Only users in the administrator user group can view this page.
Labels	X	—	—	—	Only users in the administrator user group can view this page.
Schedules	X	—	—	—	Only users in the administrator user group can view this page.

Table 8: JUNOScope User Group Permissions and Access Privileges *(continued)*

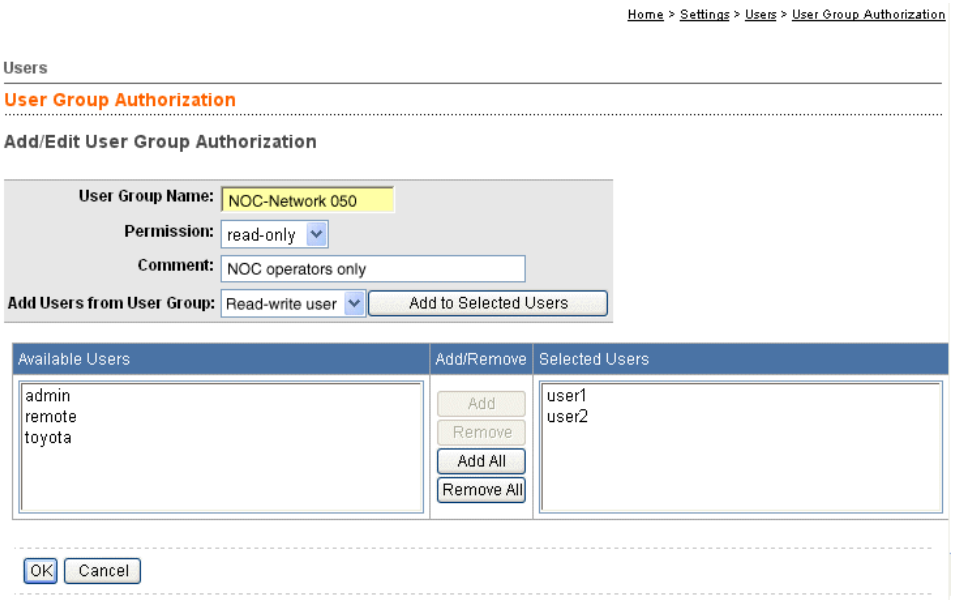
JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Users > Local Authentication	X	—	—	—	Only users in the administrator user group can view this page.
Users > User Group Authorization	X	—	—	—	Only users in the administrator user group can view this page.
User > Authentication Policy > Global Authentication	X	—	—	—	Only users in the administrator user group can view this page.
User > Authentication Policy > User Authentication Policy	X	—	—	—	Only users in the administrator user group can view this page.
RADIUS Configuration	X	—	—	—	Only users in the administrator user group can view this page.
Import/Export Data	X	—	—	—	Only users in the administrator user group can view this page.
Saved Operations	X	X	—	—	Only those operations saved by users in the same user group are visible in the Available Operations list box, in the Add Compound Operations dialog box.

Adding a User Group

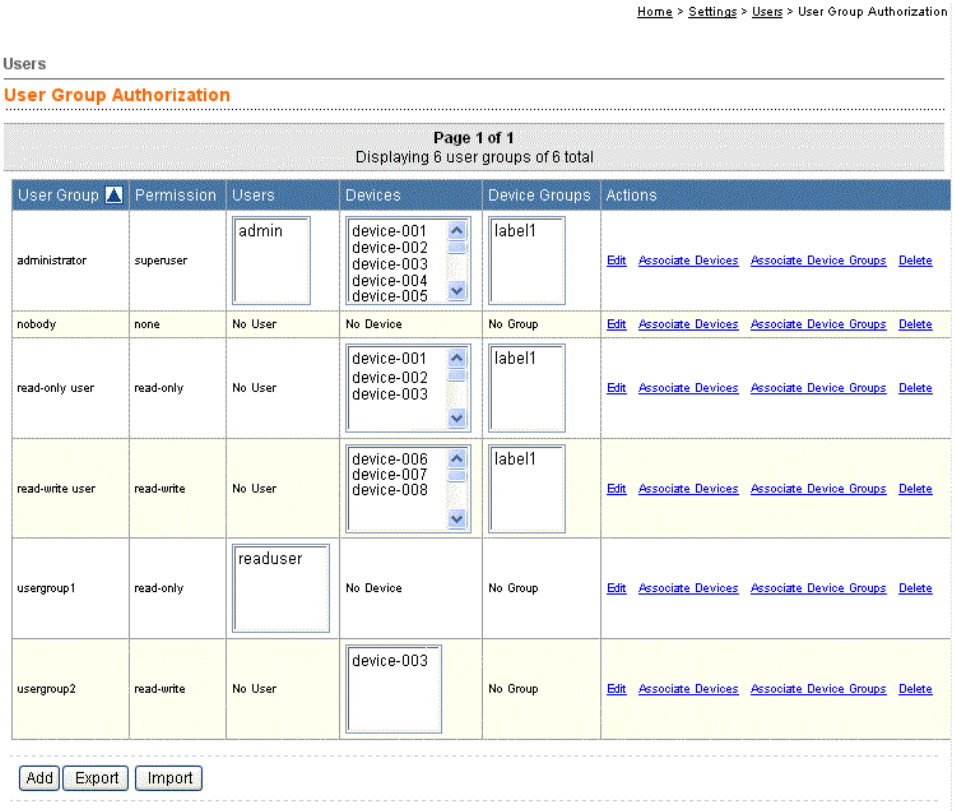
The JUNOScope administrator can add one or more users to a user group.

To add a user to a user group, follow these steps:

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.
2. Click Add. The Add/Edit User Group Authorization dialog box appears.



3. Type the name of the user group you want to add in the User Group Name text box.
4. Select the permission you want for the user group from the Permission drop-down list box.
5. Type an optional comment about the user group you want to add.
6. Select the user(s) you want to include in the user group. The users are created using the Settings > Local Authentication command. Select the user(s) you want in the Available Users list box, then click Add. Click Add All to include all listed users. The selected users appear in the Selected Users list box.
7. Click OK.
8. The new user group appears in the User Group Authorization dialog box.

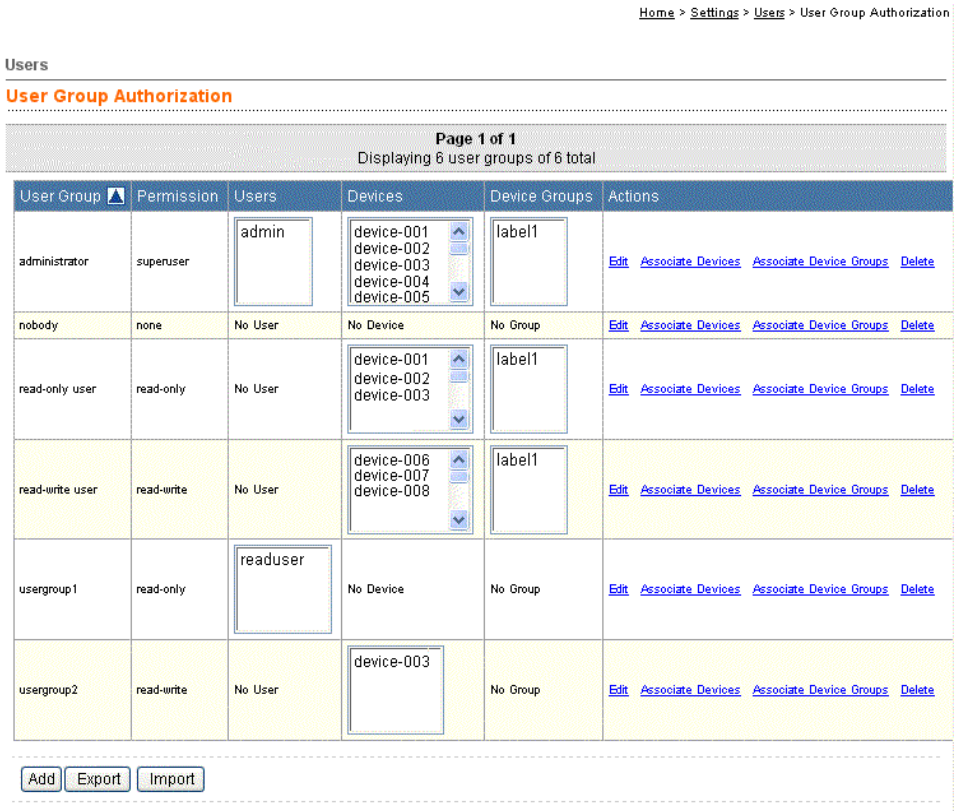


Viewing and Managing User Group Authorization Settings

Use the User Group Authorization dialog box to view and manage existing user group settings.

To view and manage user group authorization settings, follow this step:

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.



The User Group Authorization dialog box lets you view existing user groups and perform several operations, such as add, edit, associate devices, associate device groups, and delete user groups.

The user group authorization information is displayed in the dialog box in tabular format. The columns of information are as follows:

- The User Group column lists the names of the existing user groups in alphabetical order. Click the column header to sort the table alphabetically in ascending and descending order.
- The Permission column displays the user group access privilege name.
- The Users column list box displays the names of the users in the user group.
- The Devices column list box displays the names of the devices to which the user group has access.
- The Device Groups column list box displays all device groups the user group has access. A drop-down list box displays the names of multiple devices.
- The Actions column provides the following links for actions to manage user groups:

- Edit—Lets you edit user group settings using the Associate Users to a User Group (Edit User Group) dialog box. For more information about editing user group settings, see “Editing User Group Settings” on page 117.

- Associate Devices—Lets you add device access to user groups using the Associate Devices to a User Group (Add Device Access) dialog box. For more information about adding device access to user groups, see “Associating Devices to User Groups” on page 118.

- Associate Device Groups—Lets you add device group access to user groups using the Associate Device Groups to a User Groups (Add Device Group Access) dialog box. For more information about adding device group access to user groups, see “Associating Device Group Access to User Groups” on page 119.

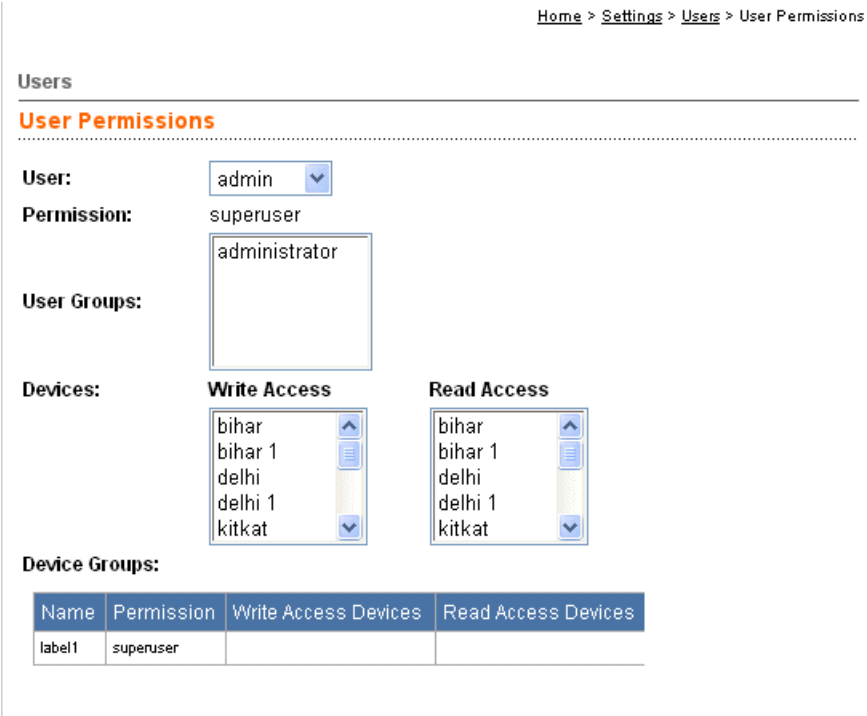
- Delete—Removes the user group from the JUNOScope database. For more information about deleting user groups, see “Deleting User Group Authorization” on page 122.

Viewing User Permissions

You can view user permissions for access to devices and device groups, if you have superuser permissions.

To view user permissions, follow these steps:

1. In the JUNOScope main window, click the Logged in as <username> link at the top right. The User Permissions dialog box pops up.



2. In the User drop-down list box, select the user whose permissions you want to view.

   The User Permissions dialog box displays the permission, user groups, devices, and device groups to which the user belongs and has access:

   - User drop-down list box/display field—For users belonging to the administrator user group, the field is a drop-down list box. For users in other user groups, the field is display only.
   - Permission display field—Displays the permission level assigned to the user. The permission level of a user determines what JUNOScope tasks or operations a user can perform and the level of device access. Four permission levels are available: superuser, read-write, read-only, and none. See "User Group Permission Levels" on page 108 for more information.
   - User Groups list box—Displays the user groups to which the user belongs. A user must be a part of at least one user group, and can be part of multiple user groups. This list box is not visible if you do not belong to the administrator user group.
   - Devices list boxes—Displays the devices to which the user has read-write or read-only access.
     - Write Access list box—Displays the devices to which the user has read-write access.
     - Read Access list box—Displays the devices to which the user has read-only access.
     - Device Groups table—Displays the device groups to which the user has access, the permission levels assigned to the user as part of a device group, and the access permissions the user has to devices as part of a device group:
       - Name column—Displays the names of the device groups to which the user group has access.
       - Permission column—Displays the permission level assigned to the user as part of the device group.
       - Write Access Devices column—Displays the devices to which the user has read-write access as part of the device group.
       - Read Access Devices column—Displays the devices to which the user has read-only access as part of the device group.

3. Click the Close link.

Editing User Group Settings

The JUNOScope administrator can change the following user group authorization settings when changes occur.

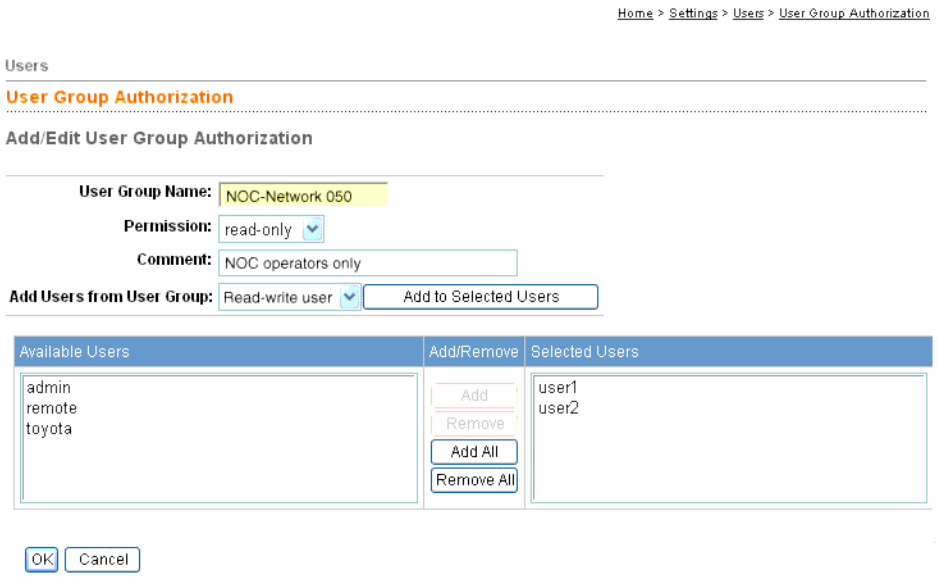
- User group name, if it is not a pre-existing user group.
- User group access permission.

- Users in the user group. You can select to add users from an existing user group.
- User group optional comment.

You cannot delete pre-existing user groups, which are administrator, read-write user, read-only user, and nobody.

To edit user group settings, follow these steps:

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.
2. Click the Edit action link for the user group you want to edit. The Add/Edit User Group Authorization dialog box appears.



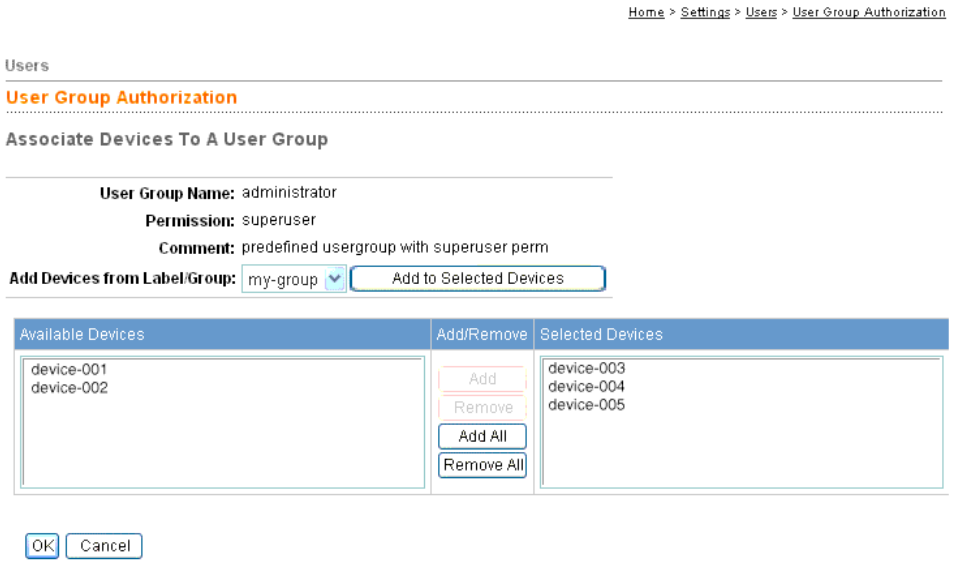
3. Change the user group settings that you want. You can modify the user group name, permission and optional comment. You can also change the selected users in the user group, including select users from an existing user group.
4. Click OK. The information appears in the Authorization (User Group Authorization) dialog box.

Associating Devices to User Groups

Once you create a user group, you can associate the devices to which you want that user group to have access. The existing devices available to associate are ones that you have already added using the Settings > Devices, Settings > Groups, and any labels used to statically organize large groups of devices that you have created using Setting > Labels.

To add device access to a user group, follow these steps:

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.
2. Click the Associate Devices action link. The Associate Devices to a User Group dialog box appears.



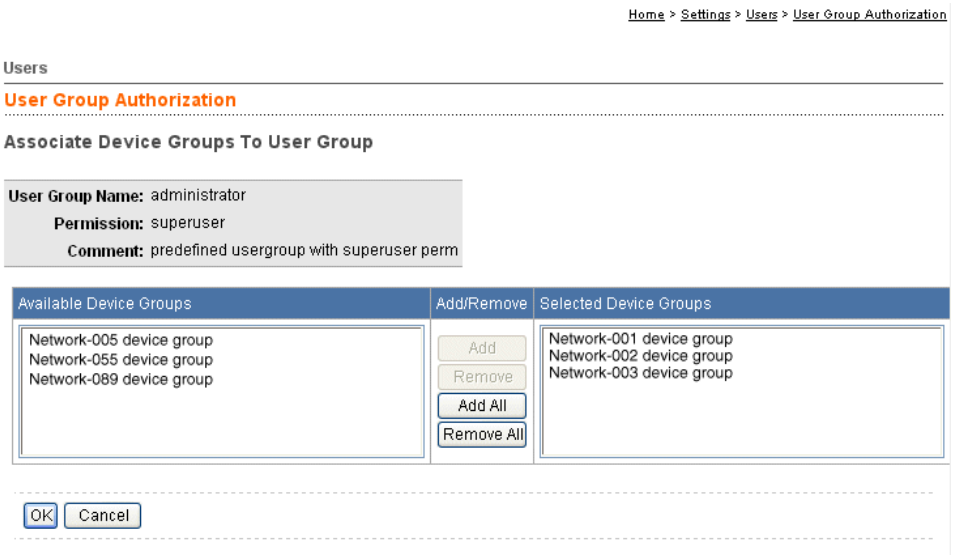
The dialog box displays the name, permission, and comment for the user group you selected.

3. To add devices to which the user group can have access do one of the following:
   - Click Add or Add All to add devices from the Available Devices list to the Selected Devices list. Click Remove or Remove All to move devices from the Selected devices list to the Available devices list.
   - To add devices from an existing label or group, select the existing Label or Group that you want from the Add Devices from Label/Group, then click Add to Selected Devices. For information about labels, see "Setting Up Labels" on page 83. For information about groups, see chapter "Setting Up Groups" on page 67.
4. Click OK. The user group now has access to the devices listed in the Selected Devices list box.

Associating Device Group Access to User Groups

To add device groups to which you want a user group to have access.

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.
2. Click the Associate Device Groups action link. The Associate Devices Groups to User Group dialog box appears.



The dialog box displays the name, permission, and comment for the user group you selected. Device group names are listed in the Available Device Groups list. If you haven't set up device groups, see "Setting Up Groups" on page 67.

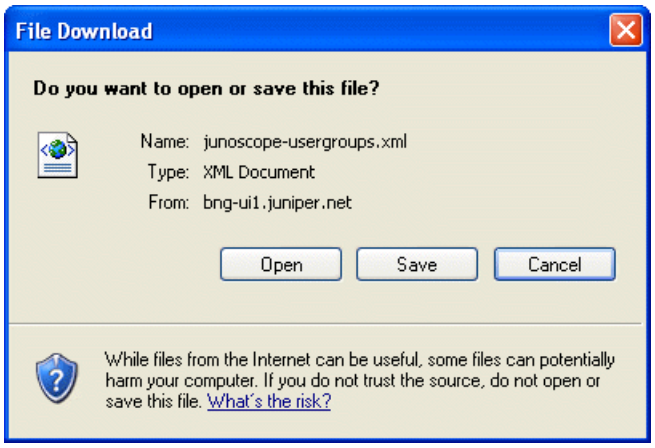
1. Select the device group(s) to which you want to add access for the user group, then click Add. Click Add All to add all listed devices.
2. Click OK. The user group now has access to the devices listed in the Selected Device Groups list box.

Exporting User Groups

You can export JUNOScope user group settings to an XML file on the local file system. You can use this file to import user group settings to another JUNOScope server.

To export user group settings, follow these steps:

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.
2. Click Export. The File Download dialog box appears.



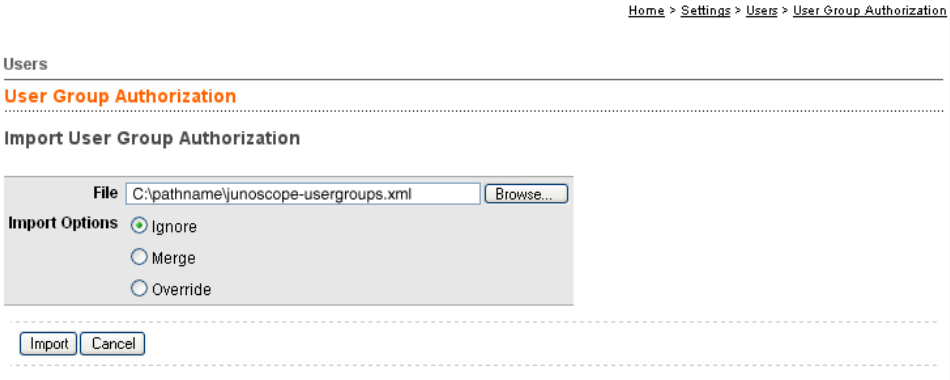
3. Do one of the following:
   - Click Save to save the user group data and export it to the file system in a file named junoscope-usergroups.xml. .
   - Click Open to view the contents of the export file.

Importing User Groups

You can import user group data into the JUNOScope server from a junoscope-usergroup.xml file that you have saved to the local file system.

To import user group authorization data, follow these steps:

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.
2. Click Import. The Import User Groups dialog box appears.

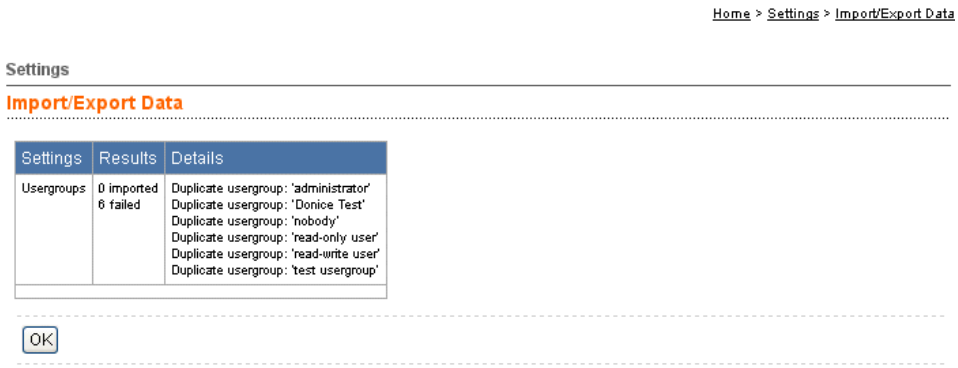


3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default junoscope-usergroups.xml export file from another JUNOScope server or use the provided sample export-import-sample.xml XML file on the JUNOScope server to generate a file to import.
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records

stored in the JUNOScope server and imported records. The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

5. Click Import. The Import status dialog box appears.

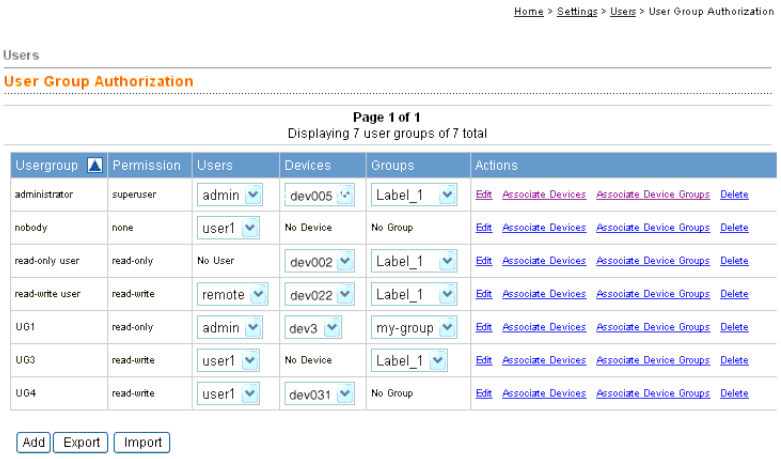


Deleting User Group Authorization

You can delete JUNOScope a user group from the Authorization (User Group Permissions) dialog box when you do not need them anymore. You cannot delete predefined user groups, such as administrator read-write user, read-only user, and nobody.

To delete user group authorization data, follow these steps:

1. In the JUNOScope main window, click Settings > Users > User Group Authorization. The User Group Authorization dialog box appears.



2. Click the Delete action link for the user group you want to delete.
3. Confirm that you want to delete the user group authorization record.

   The user group authorization record is removed from the User Group Authorization dialog box and from the JUNOScope database.

Chapter 12

Setting Up a Global Authentication Policy

This chapter describes how to setup and edit global authentication policies. The JUNOScope administrator can configure global authentication policies, across all users, that control access to the JUNOScope server from client machines. The global authentication policy is used for users for whom user authentication policy has not been configured. An administrator can configure a global authentication policy using maximum login attempts, access windows and an access control list. An administrator can create an access list which specifies which client machines should be denied or allowed access to the JUNOScope software.

This chapter includes the following topics:

Configuring a Global Authentication Policy

To configure global authentication policies, follow these steps:

1. From the JUNOScope main window, click Settings > Users > Authentication Policy > Global Authentication Policy. The Global Authentication Policy dialog box appears.

   The Global Authentication Policy dialog box displays the Maximum Login Attempts and the Access Window fields with zero as the default value, and the Access Control List Add button.

2. Enter the following information in the Global Authentication Policy dialog box:

   - Maximum Login Attempts—The maximum number of consecutive failure login attempts allowed within the access window for a user. If a user reaches the maximum number of login attempts, the user status automatically becomes locked. This field can have a value from 0 to 100. If the maximum login attempts is 0, the authentication policy for the user will not be active, the user account will be assumed to be unlocked, and the normal login mechanism will be applied. If a user account status is unlocked, the user can successfully log in to the JUNOScope software by providing a valid username and password. If the account status is locked, the user is denied access to the JUNOScope software, even if the user provides a valid username and password, and is shown the message " The user account is currently locked. Please contact the system administrator." For the JUNOScope administrator (the initially configured user), the user account is always unlocked.
   - Access Window—The access window for a user account starts when the first login failure occurs for the user account and runs until one of the following occurs:
     - A user successfully logs in. The access window is then reset.
     - A user tries unsuccessfully to log in for the maximum login attempts. The user account is then locked and the access window timer is reset.

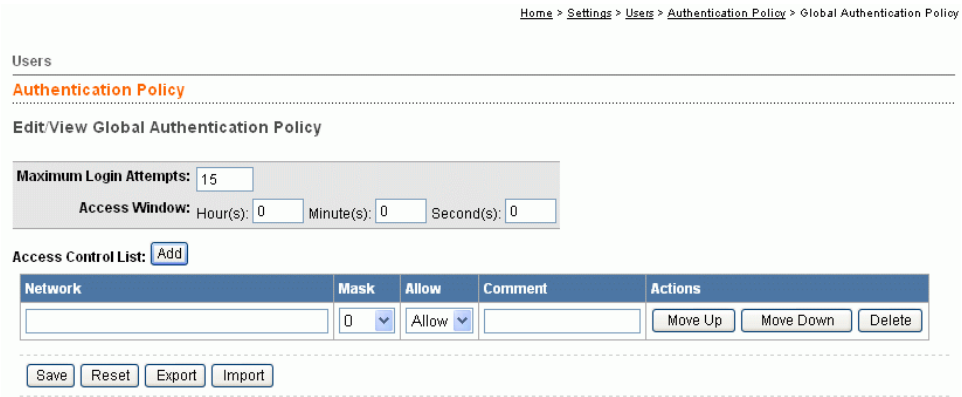
   The Access Window field can have a minimum value of 0 (for example, all the field minute(s), hour(s), second(s) having a value of 0) and a maximum value of 24 hours for example, the hour(s) field can have a maximum value of 24, while the minute(s) and second(s) fields have a value of 0). The default value is 0. However, individually, the hour(s) field can have a value from 0 to 24, the minute(s) field can have a value of from 0 to 59, and the second(s) field can have a value from 0 to 59. If the Access Window field is 0, the authentication policy

for the user account will not be active, and the normal login mechanism will always be applied.

The timer for the access window starts when an invalid login attempt is made on a user account. If a user account is not locked and no further invalid login attempt is tried for that account, the timer for the access window is automatically reset either after a time period equal to the access window or if the user successfully logs in to JUNOScope within the access window period.

If the authentication policy for a user account is set up with 3 maximum login attempts and a 1-hour access window, the clock for the access window starts at the first unsuccessful attempt when the user types an invalid password to login. If the user makes three unsuccessful attempts within 1 hour, then the user account will be LOCKED at the third unsuccessful attempt and will be redirected to the "The user account is currently locked. Please see the system administrator." message. Any further attempts by the user to log in using the username, even with a valid password, will be denied.

3. Click Add. A row with empty fields will be added to the access control list table.



4. Enter the following information in the access control list table row:

   - Network—The IP address of the client machines that should be allowed or denied access to the JUNOScope software. In the Network field you can specify a specific client address, in which case the user has to use the wild card as 32 (128 for IPv6), or the specific first valid client address, in which case you have to use the mask as the number of bits that should exactly match the given IP address.

   - Mask—The network mask of the client machines that should be allowed or denied access to the to the JUNOScope software. Specifies the number of bits of the client IP that should match with the given IP address.

   - Allow—The authentication action to be performed, whether to deny or allow access to the client machine if the IP address is matched.

   - Comment—The comment to identify access control list entry. You can provide a comment to identify each access control list entry or to provide a reason for allowing or denying access.

   - Actions—The Move Up and Move Down options used for ordering access control list entries. When a user logs in, the IP address of the machine from

which he has logged in is compared with the access list in sequence until a match is found. If a match is found then the action specified (allow/deny) is done, and the process does not continue further. However If no match is found the client is allowed access by default. Since order plays an important role in the access list, Move Up and Move Down options are provided to change the order of access control list entries. The Delete option is provided to delete an access control list entry.

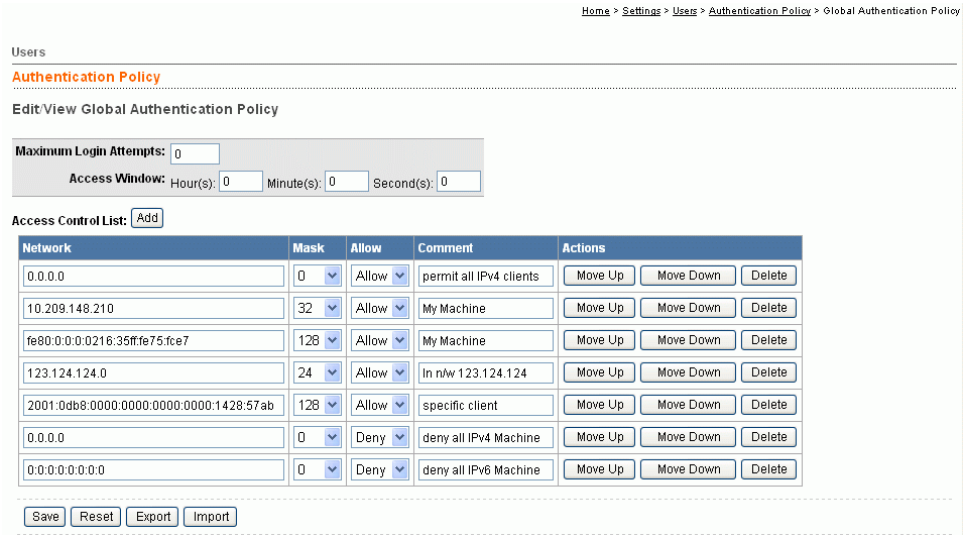
NOTE: Repeat Steps 3 and 4 to add more access control list entries to the access control list table.

5. Click Save to commit the changes to the database.
   Click Reset to clear all the values you have entered and restore the last saved values.

Editing a Global Authentication Policy

To edit global authentication policies, follow these steps:

1. From the JUNOScope main window, click Settings > Users > Authentication Policy > Global Authentication Policy. The Global Authentication Policy dialog box appears.



2. Edit the appropriate authentication policy information. See steps 2 and 4 in "Configuring a Global Authentication Policy" on page 125 for a description of the information.

3. Click Save to commit the changes to the database.
   Click Reset to clear all the values you have entered and restore the last saved values.

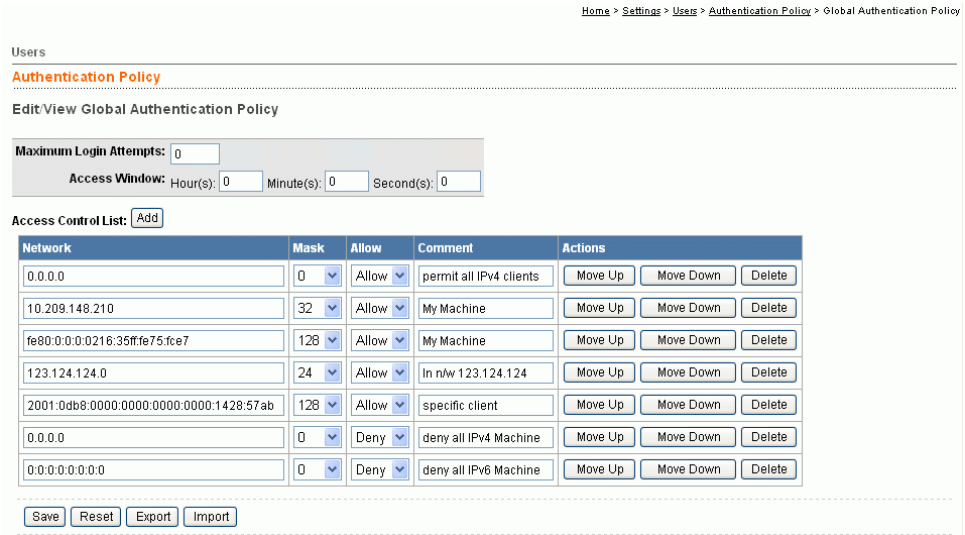
Importing Global Authentication Policy Information

You can import authentication information from another JUNOScope server or you can use the sample junoscope-globalPolicy.xml file as a guide.

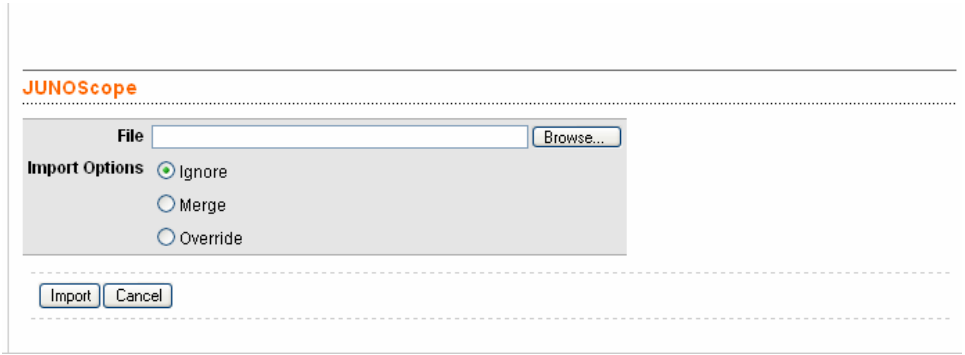
Importing device information is useful when you do not want to enter information manually.

To import authentication policy information, follow these steps:

1. From the JUNOScope main window, click Settings > Users > Authentication Policy > Global Authentication Policy. The Global Authentication Policy dialog box appears.



2. Click Import. The Import dialog box appears.



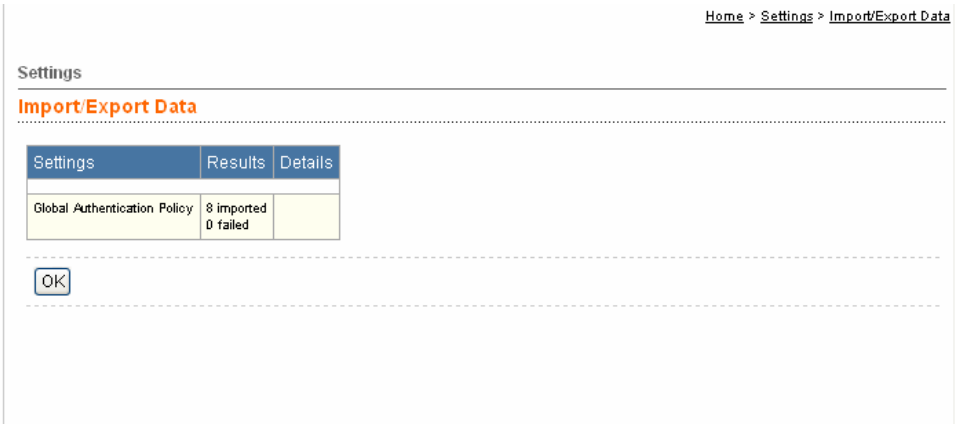
3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default schedules.xml export file from another JUNOScope server or use the provided samplejunoscope-globalPolicy.xml XML file on the JUNOScope server to generate a file to import.

4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:

   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are reset to the default values, then the imported data is updated in the database. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

NOTE: Access control lists are always deleted whichever the import method selected, as they are meaningful only as a chunk. Access control list data that is imported is added after validation of the data.

5. Click Import. The Import status dialog box appears.



   The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

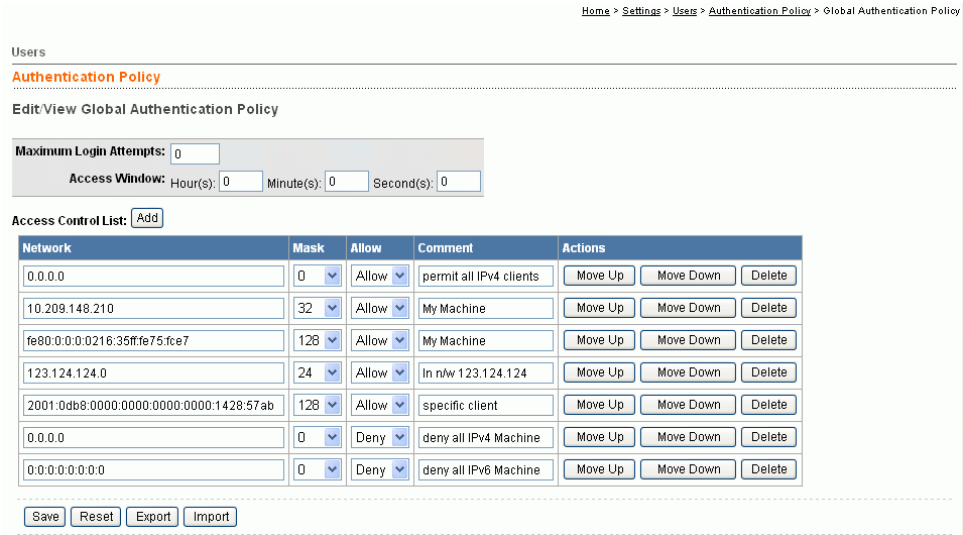
6. Click OK. The imported data is listed in the Global Authentication Policy dialog box.

Exporting Global Authentication Policy Information

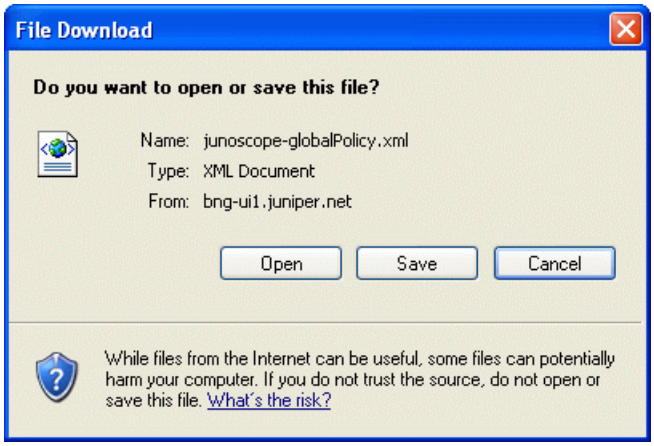
You can export global authentication policy information that you want to back up or import to another JUNOScope server.

To export global authentication policy information, follow these steps:

1. From the JUNOScope main window, click Settings > Users > Authentication Policy > Global Authentication Policy. The Global Authentication Policy dialog box appears.



2. Click Export. The File Download dialog box appears.



3. Click Save to export the global authentication policy information to the local file system in a file named junoscope-globalPolicy.xml. Click Open to view the contents of the export file.

Chapter 13

Editing a User Authentication Policy

This chapter describes how to view and edit a user's authentication policy. An authentication policy determines the user access policy to the JUNOscope software.

A default authentication policy is automatically generated for all users already configured in JUNOScope, all remote RADIUS users who have successfully logged in to JUNOScope, and when a new user is created.

The JUNOScope administrator can edit a user's authentication policy, which includes the following information:

- Maximum login attempts—The number of consecutive login failure attempts allowed.
- Access window—A maximum time interval for the failure attempts, depending on the authentication policy.
- User account status—Either LOCKED or UNLOCKED. If a user account is LOCKED, that user is denied access to the system even if a user provides a valid username and password. The user is denied access until the JUNOScope administrator changes the status to UNLOCKED.

You must have superuser permission to edit an authentication policy for a user.

This chapter includes the following topics:

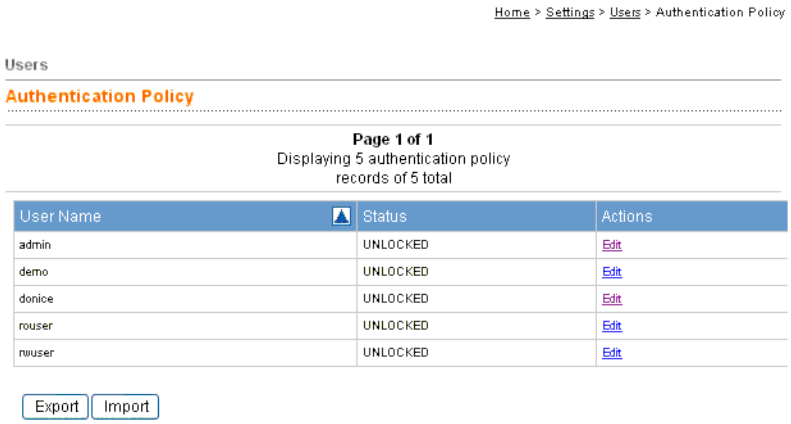
Viewing User Authentication Policies

A user authentication policy is automatically generated and displayed in the Authentication Policy table for:

- All users already configured in the JUNOScope software using Settings > Users > Local Authentication
- All remote RADIUS users who have successfully logged in the JUNOScope software
- All new users created using Settings > Users > Local Authentication

To view user authentication policies, do the following:

1. From the JUNOScope main window, click Settings > Users > Authentication Policy. The Authentication Policy dialog box appears.



By default, user login information is listed alphabetically by username in the Authentication Policy table in descending order. The username is the name a user uses to log in to the JUNOScope software.

The Authentication Policy table also lists the user account status, either UNLOCKED (the default) or LOCKED. The default is UNLOCKED. If the user account status is UNLOCKED, the user can successfully log in to the JUNOScope software by providing a valid username and password. If the user account status is LOCKED, the user is denied access to the JUNOScope software, even if the user provides a valid username and password, and is redirected to the "The user account is currently locked. Please contact system administrator." message. A user account remains locked until the JUNOScope administrator unlocks it.

When a client device is denied access the "Access denied. Please contact system administrator" message appears.

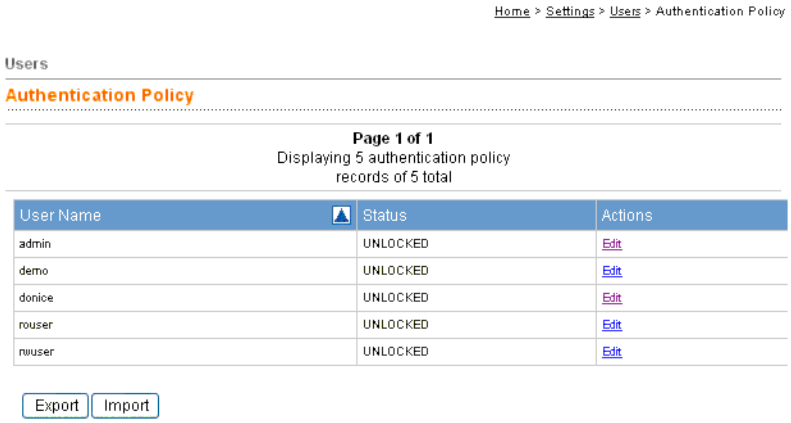
You can edit a user authentication policy by clicking the Edit link in the Actions column. See "Editing a User Authentication Policy" on page 134.

Editing a User Authentication Policy

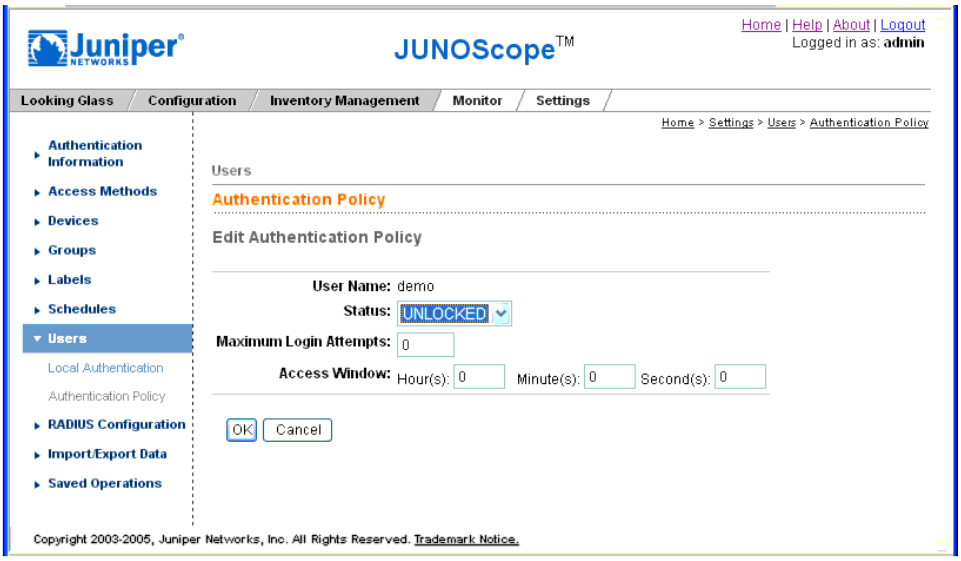
You can edit a user account authentication policy, which consists of the user status, maximum login attempts, and the access window time within which a user must successfully log in. You can also add new access control.

To edit a user authentication policy, follow these steps:

1. From the JUNOScope main window, click Setting > Users > Authentication Policy. The Authentication Policy dialog box appears.



2. In the Authentication Policy dialog box, click the Edit link in the Action column for the user authentication information you want to edit. The Edit Authentication Policy dialog box appears.



3. Edit the authentication policy settings that you want.

   In the Edit Authentication Policy dialog box, the User Name display field displays the name the user uses to log in to the JUNOScope software.

   You can modify the following information in the Edit Authentication Policy dialog box:

- Status—The user account status: either UNLOCKED (the default) or LOCKED. If a user account status is UNLOCKED, the user can successfully log in to the JUNOScope software by providing a valid username and password. If the account status is LOCKED, the user is denied access to the JUNOScope software, even if the user provides a valid username and password, and is redirected to the " The user account is currently locked. Please contact the system administrator." message.
- Maximum Login Attempts—The maximum number of consecutive failure login attempts allowed within the access window for a user. If a user reaches the maximum number of login attempts, the user status automatically becomes LOCKED. This field can have a value from 0 to 100. If the maximum login attempts is 0, the authentication policy for the user will not be active, the user account will be assumed to be UNLOCKED, and the normal login mechanism will be applied. For the JUNOScope administrator (the initially configured user), the user account is always UNLOCKED.
- Access Window—The access window for a user account starts when the first login failure occurs for the user account and runs until one of the following occurs:
  - A user successfully logs in. The access window is then reset.
  - A user tries unsuccessfully to log in for the maximum login attempts. The user account is then LOCKED and the access window is reset.

  The Access Window field can have a minimum value of 0 (for example, all the field minute(s), hour(s), second(s) having a value of 0) and a maximum value of 24 hours for example, the hour(s) field can have a maximum value of 24, while the minute(s) and second(s) fields have a value of 0). The default value is 0. However, individually, the hour(s) field can have a value from 0 to 24, the minute(s) field can have a value of from 0 to 59, and the second(s) field can have a value from 0 to 59. If the Access Window field is 0, the authentication policy for the user account will not be active, and the normal login mechanism will always be applied.

  The timer for the access window starts when an invalid login attempt is made on a user account. If a user account is not locked and no further invalid login attempt is tried for that account, the timer for the access window is automatically reset either after a time period equal to the access window or if the user successfully logs in to JUNOScope within the access window period.

  If the authentication policy for a user account is set up with 3 maximum login attempts and a 1-hour access window, the clock for the access window starts at the first unsuccessful attempt when the user types an invalid password to login. If the user makes three unsuccessful attempts within 1 hour, then the user account will be LOCKED at the third unsuccessful attempt and will be redirected to the " The user account is currently locked. Please see the system administrator." message. Any further attempts by the user to log in using the username, even with a valid password, will be denied.

4. Click OK.

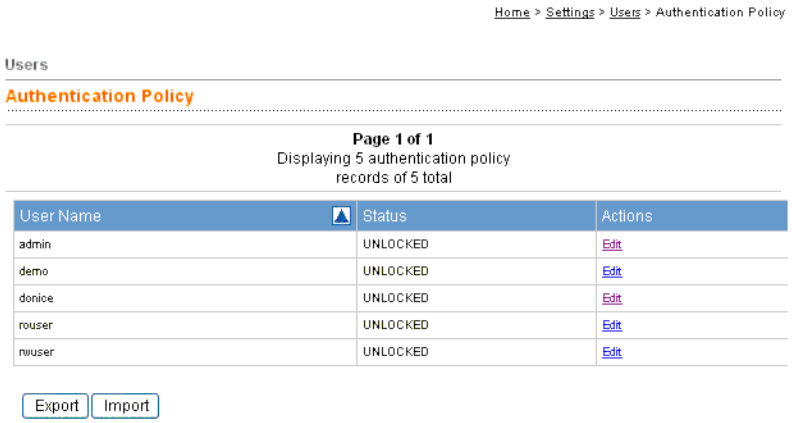
Importing Authentication Policy Information

You can import authentication information from another JUNOScope server or you can use the sample XML export-import-sample.xml file as a guide.

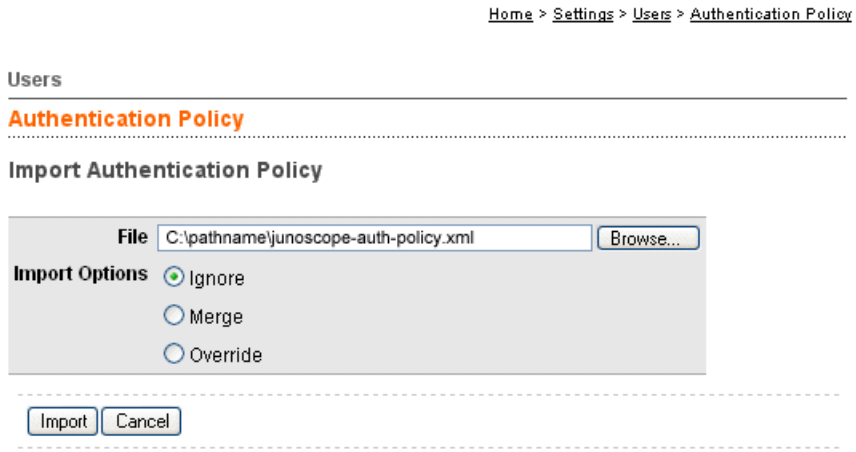
Importing device information is useful when you do not want to enter information manually.

To import authentication policy information, follow these steps:

1. In the JUNOScope main window, click Settings > Users > Authentication Policy. The Authentication Policy window appears.



2. Click Import. The Import dialog box appears.

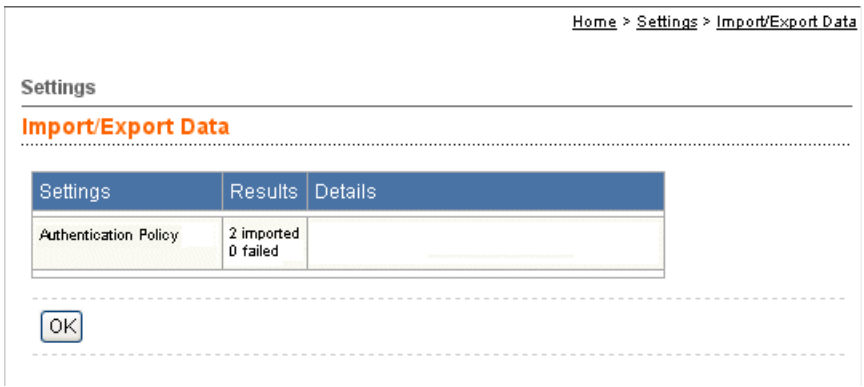


3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default schedules.xml export file from another JUNOScope server or use the provided sample export-import-sample.xml XML file on the JUNOScope server to generate a file to import.

4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:

   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

5. Click Import. The Import status dialog box appears.



   The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

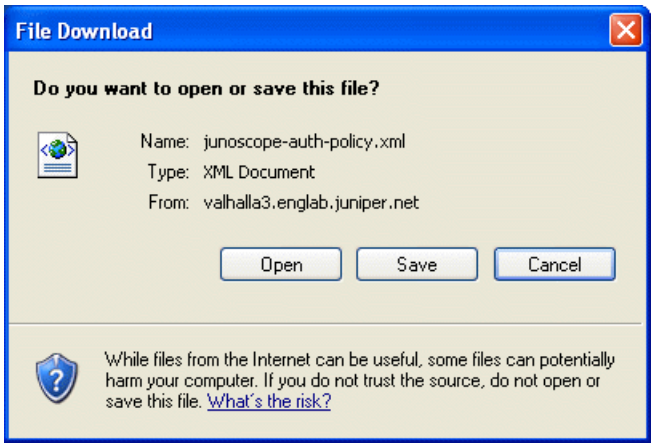
6. Click OK. The imported data is listed in the Authentication Policy dialog box.

Exporting Authentication Policy Information

You can export schedule information that you want back up or import to another JUNOScope server.

To export schedule information, follow these steps:

1. In the JUNOScope main window, click Settings > Users Authentication Policy. The Authentication Policy dialog box appears.
2. Click Export. The File Download dialog box appears.



3. Click Save to export the authentication policy information to the local file system in a file named junoscope-auth-policy.xml. Click Open to view the contents of the schedule export file.

Chapter 14

Setting Up RADIUS Configuration

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. This chapter describes how to configure user authentication on a RADIUS server and in the JUNOScope software so that users with a RADIUS account can log in to the JUNOScope software.

The RADIUS system administrator configures one or more RADIUS servers to share user account information with the JUNOScope software. The JUNOScope software administrator, with superuser permissions, adds the RADIUS server host information in JUNOScope. The JUNOScope administrator then creates one or more template accounts in JUNOScope so that RADIUS users get the appropriate permissions after they log in.

This chapter includes the following topics:

How RADIUS Configuration Works with JUNOScope

This section provides an overview of how JUNOScope RADIUS configuration works to enable remote users with RADIUS accounts to log in with appropriate permissions. The general sequence is as follows:

1. The RADIUS server administrator configures the RADIUS server(s) with Juniper Networks vendor-specific RADIUS attributes and user account records. (See “Configuring the RADIUS Server” on page 142.)
2. The RADIUS administrator ensures that all RADIUS servers are up and running.
3. The JUNOScope software administrator logs in to JUNOScope with superuser permissions, and adds the RADIUS server host information in JUNOScope. (See “Setting Up RADIUS Configuration in JUNOScope” on page 146.)

4. The JUNOScope administrator adds local and remote template accounts as needed in JUNOScope. (See "Configuring RADIUS Local and Remote Template Accounts in JUNOScope" on page 153.)
5. A user with a RADIUS account logs in to the JUNOScope software with username and password.
6. The JUNOScope software forwards a request to the RADIUS server to authenticate the user's login name.
7. If authentication succeeds, the RADIUS server returns the local username attribute to the JUNOScope software.
8. The template account (user) set up in JUNOScope determines the user group to which the RADIUS user belongs after log in.
9. The user logs in successfully with JUNOScope permissions derived from the least restrictive permission levels of all user groups to which the user belongs.

Configuring the RADIUS Server

The sections that follow describe how to modify specific RADIUS server configuration files with Juniper Networks vendor-specific attributes and user account information. All RADIUS servers should comply with RFC 2865.

- Configuring an AAA Merit RADIUS server on page 142
- Configuring an SBR Server on page 143
- Configuring a FreeRADIUS Server on page 145

For other RADIUS servers, modify the configuration files required for that server according to RFC 2138.

Configuring an AAA Merit RADIUS server

This section describes how to configure the clients, dictionary, users, and vendors configuration files on an authentication, authorization, and accounting (AAA) Merit RADIUS server. To do so, follow these steps:

1. Modify the RADIUS server 'client' configuration file as follows:

```
junoscope.server.name   secret        type=Juniper:nas
```

   Replace junoscope.server.name with the name of the JUNOscope software server to which you want users to log in. Replace secret with the shared secret between the RADIUS server and the client. The Network Access Server (NAS) type is Juniper.

2. Modify the RADIUS server 'dictionary' configuration file as follows:

```
# Juniper Extensions
Juniper.attr    Juniper-Local-User-Name        1       string (1, 0)
```

Where Juniper-Local-User-Name is a RADIUS vendor-specific attribute used by Juniper Networks.

3. Modify the RADIUS server 'users' configuration file used to maintain the permitted users list. For example, to add user 'edward' with password 'edward' and local user template 'fritz', change the 'users' configuration file as follows:

```
edward Password = "edward"
        Juniper:Juniper-Local-User-Name = "fritz"
```

The Juniper:Juniper-Local-User-Name is optional.

4. Modify the RADIUS server 'vendors' configuration file as follows:

```
Juniper.attr Juniper.value 2636 Juniper
```

The Juniper Networks RADIUS Vendor ID attribute is 2636.

Configuring an SBR Server

This section describes how to configure a Steel-Belted RADIUS (SBR) server version 4.7 and other versions of the server.

- Configuring an SBR Server Version 4.7 on page 143
- Configuring Other SBR Server Versions on page 144

Configuring an SBR Server Version 4.7

To modify an SBR server version 4.7, follow these steps:

1. Start the Steel-Belted RADIUS Enterprise Edition Administrator program. The Steel-Belted Radius Administrator window appears.
2. Click the Servers option button.
3. Click either the Local option button (if the server is running locally) or the Remote option button, and specify the IP address of the remote server.
4. Click the Connect option button. A message is displayed in the Status field indicating that the server started and displaying information about the server.
5. Click the RAS Clients option button.
6. Click Add.
7. In the Client Name text box, type a unique client name for the JUNOScope server. You can also use the JUNOScope server DNS name as the client name.
8. Click OK.
9. Type the IP address of the JUNOScope server in the IP Address text field.
10. Select the Juniper M/T Series Make/Model value.
11. Click Edit Authentication Shared Secret, and type the shared RADIUS server secret.

12. Click Set.
13. To add new user accounts, modify the RADIUS server 'users' configuration. For example, to add a user 'edward' with password 'edward' and local user template 'fritz', follow these steps:
    a. Click the Users option button in the SBR Administration window.
    b. Click the Add option button, and type the RADIUS username edward.
    c. Click OK.
    d. Click the Set Password option button, and type the password edward.
    e. Make sure that the Allow PAP or CHAP option button is selected.
    f. Click OK.
    g. Click the Return List Attributes tab from the table.
    h. Click the Ins option button at the bottom of the table. The Add New Attribute window appears.
    i. Select the Juniper-Local-User-Name from the Attribute list, and type the corresponding local user template name fritz in the text field. The attribute is added to the Return List Attribute table.
14. Click Save to save the configuration.

Configuring Other SBR Server Versions

NOTE: If the RADIUS server you are configuring is other than SBR server version 4.7, perform the steps in this section before configuring the server as described in "Configuring an SBR Server Version 4.7" on page 143.

To configure an SBR server version other than 4.7 (if that version does not already support Juniper vendor-specific attributes) to make it capable of returning Juniper vendor-specific attributes in an "access-accept" packet, follow these steps:

1. Copy the custom dictionary text into the "radius/service/Juniper.dct" file:

```
##############################################################################
#
# This dictionary contains Juniper Vendor Specific Attributes
#
# (See README.DCT for more details on the format of this file)
##############################################################################

# Use the Radius specification attributes
#
@radius.dct
#
# Juniper specific parameters
#
MACRO Juniper-VSA(t,s) 26 [vid=2636 type1=%t% len1=+2 data=%s%]
ATTRIBUTE Juniper-Local-User-Name Juniper-VSA(1, string) r
ATTRIBUTE Juniper-Allow-Commands Juniper-VSA(2, string) r
ATTRIBUTE Juniper-Deny-Commands Juniper-VSA(3, string) r
ATTRIBUTE Juniper-Allow-Configuration Juniper-VSA(4, string) r
ATTRIBUTE Juniper-Deny-Configuration Juniper-VSA(5, string) r
##############################################################################

# Juniper.dct - Juniper Networks dictionary
##############################################################################
```

2. Copy the following text into the "radius/service/vendor.ini" file:

```
vendor-product = Juniper M/T Series
dictionary = Juniper
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```

3. Add the following line to the "radius/service/dictiona.dcm 'file:

```
@juniper.dct
```

4. Restart the RADIUS server to add the changes. A new Juniper RAS client model appears in the Steel-Belted Radius Administrator window. The Juniper vendor-specific attributes are available in the Return List Attributes list under a particular user.

Configuring a FreeRADIUS Server

To configure a FreeRADIUS server, follow these steps:

1. Modify the RADIUS server ‘clients.conf’ configuration file as follows:

```
client junoscope.server.IPAddress  {
 secret = junoscope
 shortname = junoscope.server.name
}
```

   Replace junoscope.server.IPAddress with the IP address of the JUNOscope software server to which you want users to log in. Replace junoscope with the shared secret between the RADIUS server and the client. Replace junoscope.server.name with the DNS name of the JUNOscope software server to which you want users to log in.

2. Modify the RADIUS server 'dictionary.juniper' configuration file as follows:

```
# Juniper Extensions
ATTRIBUTE    Juniper-Local-User-Name        1       string  Juniper
```

   Where Juniper-Local-User-Name is a RADIUS vendor-specific attribute used by Juniper Networks.

3. Modify the RADIUS server 'users' configuration file for maintaining the permitted users list. For example, to add user 'Edward' with password 'Edward' and local user template 'fritz', change the 'users' configuration file as follows:

```
Edward Auth-type:=Local, User-Password = "Edward"
Juniper-Local-User-Name = "fritz"
```

   The Juniper-Local-User-Name is optional.

4. Modify the RADIUS server 'dictionary.juniper' configuration file as follows:

```
VENDOR Juniper 2636
```

   The Juniper Networks RADIUS Vendor ID attribute is 2636.

Setting Up RADIUS Configuration in JUNOScope

For each RADIUS server with user accounts that should have access to JUNOScope, you must add that server host information in the JUNOScope software.

To set up RADIUS configuration in JUNOScope, see the following sections:

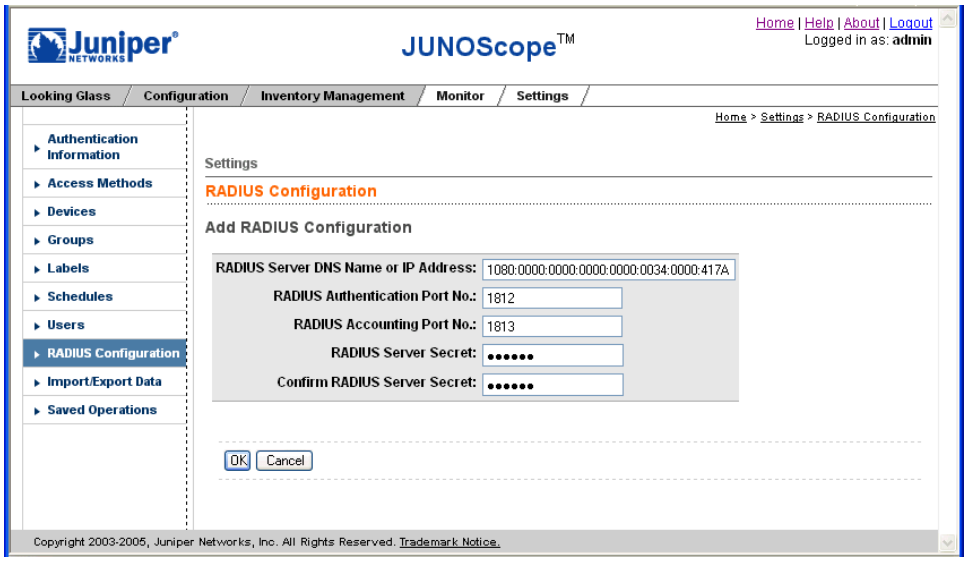
- Adding a RADIUS Configuration in JUNOScope on page 147
- Copying a RADIUS Configuration on page 148
- Editing a RADIUS Configuration on page 149
- Deleting a RADIUS Configuration on page 150

- Exporting RADIUS Configurations on page 150
- Importing RADIUS Configurations on page 151

Adding a RADIUS Configuration in JUNOScope

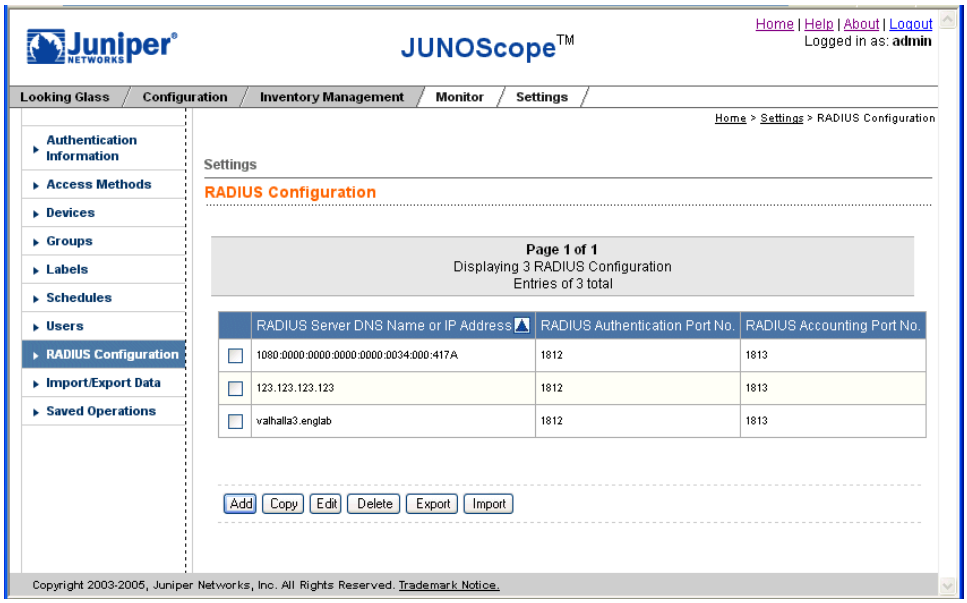
To add RADIUS server host information to JUNOScope, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. In JUNOScope, click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears. The message "No RADIUS configuration present" appears if you have not previously added a RADIUS configuration.
3. Click Add. The Add RADIUS Configuration dialog box appears.



4. Type the RADIUS server host DNS name or IP address in the text box. The name must be less than 40 characters.
5. Type the RADIUS server port number in the text box. The default port number is 1812. The port number value must be between 1 and 65,535.
6. Type the RADIUS accounting port number in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities that a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535.

   The RADIUS server port and the RADIUS accounting ports are optional, however, you must supply at least one of them.
7. Type the RADIUS server secret in the text box. The secret must be less than 40 characters.
8. Type the RADIUS server secret again to confirm it.
9. Click OK. The RADIUS configuration record is listed in the RADIUS Configuration dialog box by RADIUS server DNS name or IP address and RADIUS server port number.

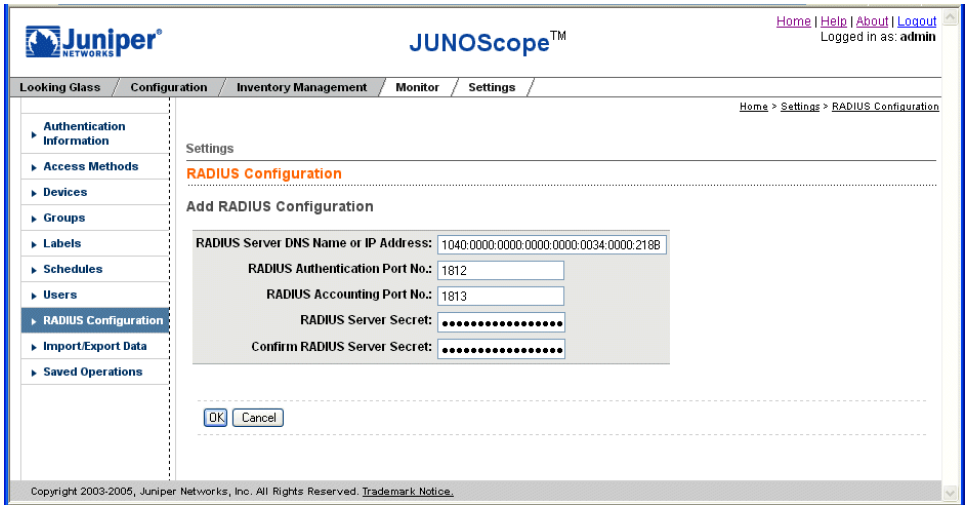


Copying a RADIUS Configuration

You can copy an existing RADIUS configuration record using the RADIUS Configuration Entry dialog box. To save the copied RADIUS configuration, you must change either the RADIUS server DNS name or the IP address and port number.

To copy a RADIUS configuration, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Select the RADIUS configuration record that you want to copy.
4. Click Copy. The Add RADIUS Configuration dialog box appears.



5. Type the RADIUS server host DNS name or IP address in the text box. The name must be less than 40 characters.
6. Type the RADIUS server port number in the text box. The default port number is 1812. The port number value must be between 1 and 65,535.
7. Type the RADIUS accounting port number in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities that a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535.

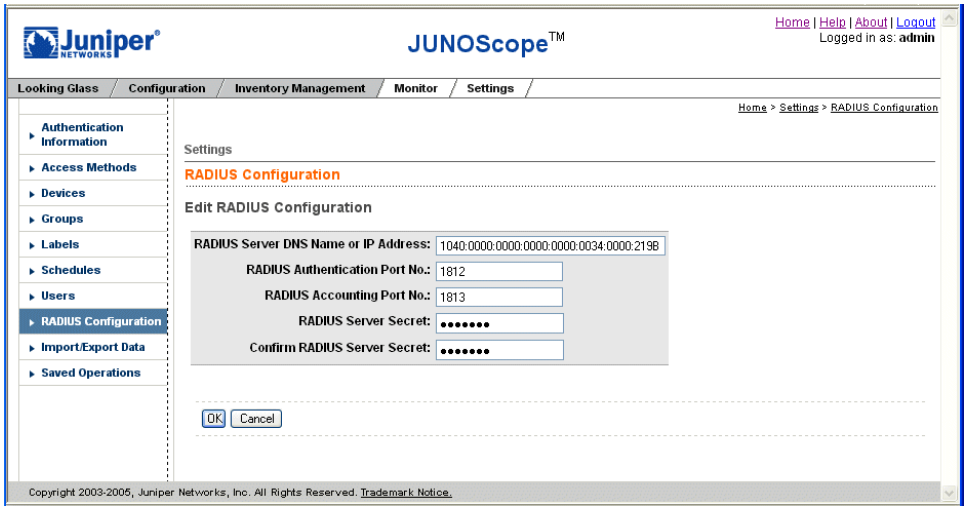
   The RADIUS server port and the RADIUS accounting ports are optional; however you must supply at least one of them.
8. Type the RADIUS server secret in the text box. The secret must be less than 40 characters.
9. Type the RADIUS server secret again to confirm it.
10. Click OK. The copied RADIUS configuration record is added in the RADIUS Configuration dialog box.

Editing a RADIUS Configuration

You can edit an existing RADIUS configuration record by changing the RADIUS server DNS name, IP address and port number, or RADIUS server secret.

To edit a RADIUS configuration, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Select the RADIUS configuration record that you want to edit.
4. Click Edit. The Edit RADIUS Configuration dialog box appears.



5. Type the RADIUS server host DNS name or IP address in the text box. The name must be less than 40 characters.

6. Type the RADIUS server port number in the text box. The default port number is 1812.
7. Type the RADIUS accounting port number in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities that a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535.

   The RADIUS server port and the RADIUS accounting ports are optional; however, you must supply at least one of them.
8. Type the RADIUS server secret in the text box. The secret must be less than 40 characters.
9. Type the RADIUS server secret again in the text box to confirm it.
10. Click OK. The edited RADIUS configuration record appears in the RADIUS Configuration Entry dialog box.

Deleting a RADIUS Configuration

To delete a RADIUS Configuration, follow these steps:

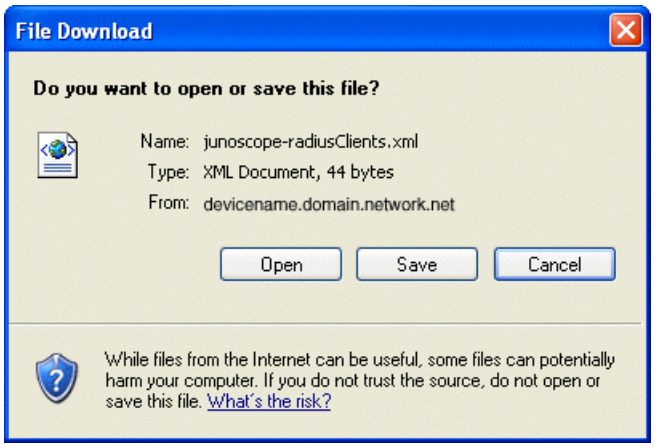
1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Select the RADIUS configuration record that you want to delete.
4. Click Delete. The RADIUS configuration record is deleted from the RADIUS Configuration dialog box and the JUNOScope database.

Exporting RADIUS Configurations

You can export RADIUS configuration information to the local file system or import to another JUNOScope server. You export all RADIUS configuration records to any XML file. The default filename is radiusClients .

To export RADIUS configuration records, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Click Export. The File Download dialog box appears.



4. Click Save to save the RADIUS configuration data and export it to the file system in a file named junoscope-radiusClients.xml. Click Open to view the contents of the export file.
5. Navigate in the local file system to where you want to save the RADIUS configuration records and click Save. The default RADIUS configuration entries export filename is radiusClients.
6. Click Open to view the export XML file content.

NOTE: The junoscope- XML file prefix is not generated if you use the Microsoft Internet Explorer 6.0 Web browser to export JUNOScope setup data. You will only see the radiusClients filename.

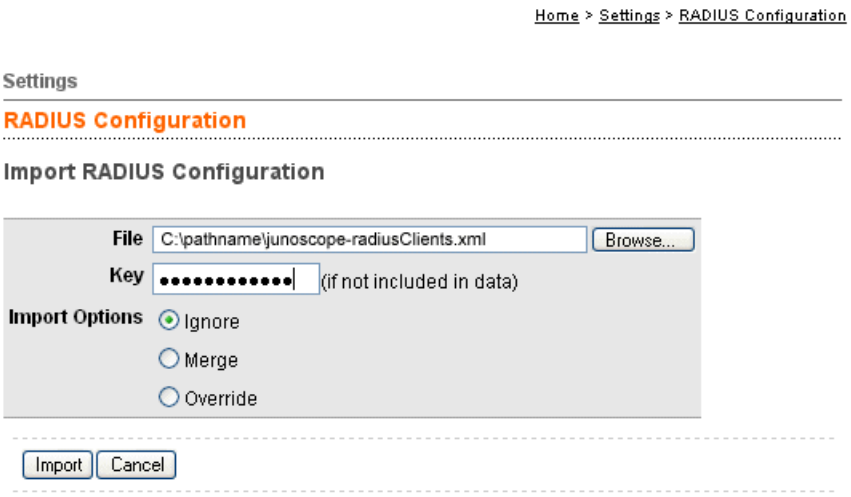
Importing RADIUS Configurations

You can import RADIUS configuration records from another JUNOScope server. You can import any valid XML file.

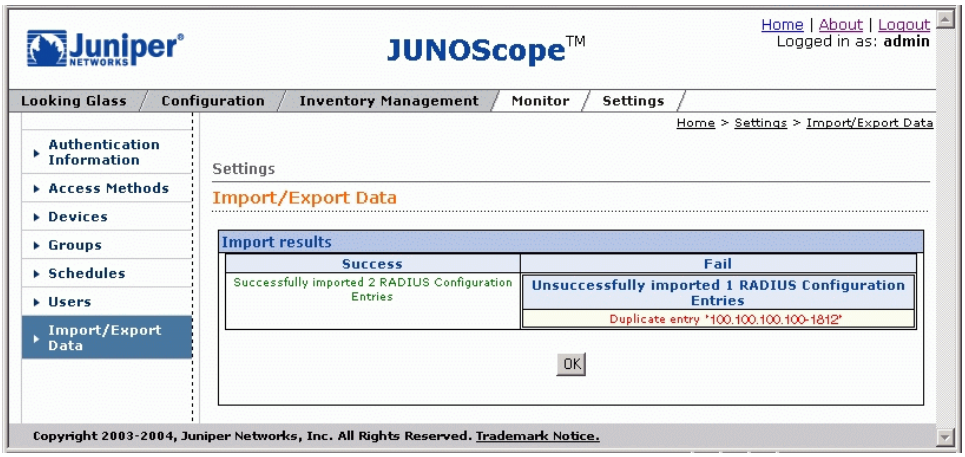
Importing RADIUS configuration information is useful when you do not want to add RADIUS configuration records manually.

To import RADIUS configuration records, follow these steps:

1. Log in to JUNOScope with superuser permissions.
2. Click Settings > RADIUS Configuration. The RADIUS Configuration dialog box appears.
3. Click Import. The Import RADIUS Configuration dialog box appears.

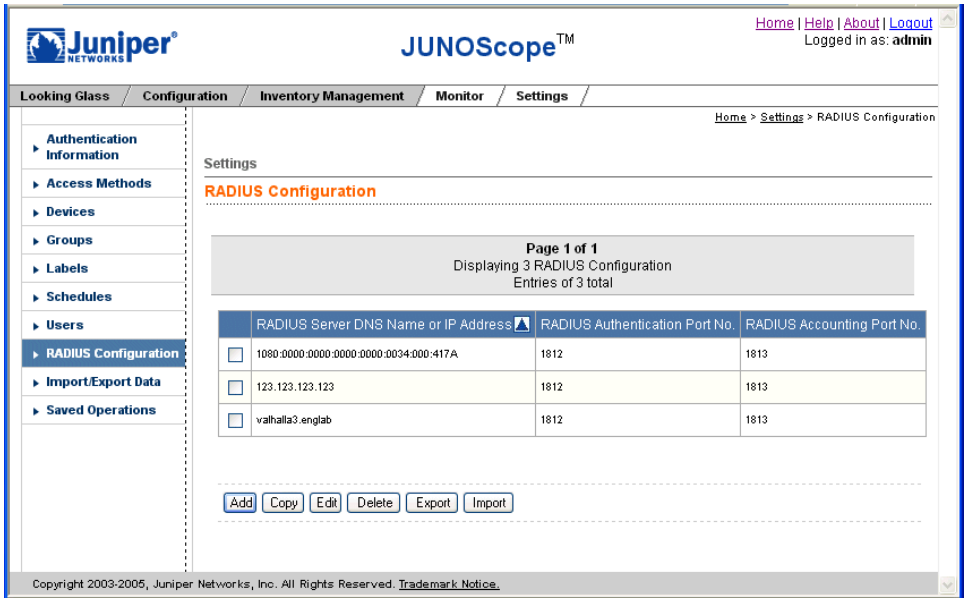


4. Click Browse and navigate to where the radiusClients RADIUS configuration file is located.
5. Type the key to decrypt the sensitive authentication information data that you want to import. The key is required if you selected not to include it when the data was exported. This key can be up to 16 characters long and was created during the JUNOScope installation.
6. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.
7. Double-click the radiusClients RADIUS configuration file.
8. The Import/Export Data dialog box appears confirming successful import of the RADIUS configuration records.



The Import/Export Data dialog box displays the RADIUS configuration records that have been successfully imported, how many records are duplicates, how many records did not import successfully, and any error descriptions.

9. Click OK. The imported RADIUS configuration records appear in the RADIUS Configuration dialog box.



Configuring RADIUS Local and Remote Template Accounts in JUNOScope

The JUNOScope software uses local password authentication. You set up a username, password, and permissions for each user allowed to log in to JUNOScope.

However, when you use RADIUS authentication, you must set up single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts.

A template account is a mapping between JUNOScope and the RADIUS server that allows RADIUS users to get the appropriate permissions. When a user with a RADIUS account logs in to JUNOScope, the software forwards the username and password to the RADIUS server for authentication. If authentication succeeds, the RADIUS server sends the Juniper-Local-User-Name attribute (if present for the user) to JUNOScope. Based on the received Juniper-Local-User-Name attribute and the configured template user accounts, JUNOScope determines the permissions for the user. The RADIUS account user gets the same permissions as the template user.

You set up template accounts the same way you create users in JUNOScope. To add a user in JUNOScope, see "Adding a User" on page 98. See also "RADIUS User Login Scenarios" on page 155.

Local Template Accounts

When you configure a local template and a user logs in, the JUNOScope software sends a request to the authentication server to authenticate the user's login name. When a user is authenticated, the RADIUS server returns the local username to JUNOScope. If a local username (for example, the Juniper-Local-User-Name attribute) is specified for that login name. the appropriate local template is selected. If no local template is returned by the RADIUS server or no corresponding local template exists in JUNOScope, JUNOScope will, by default, use the remote template (see "Remote Template Accounts" on page 154.)

Table 9 on page 154 shows the user account information that must exist on the RADIUS server and in the local template account or user set up in JUNOScope.

Table 9: Local Template Account

RADIUS Server User Account	JUNOScope Local Template Account
Username: "edward"	Username: fritz
Password: "edward"	Password: fritz
Juniper-Local-User-Name = "fritz"	Permissions: superuser

If a local user logs in to JUNOScope using username fritz and password fritz, the user will log in successfully with superuser permissions. However, if a RADIUS user "edward" logs in to JUNOScope successfully using username edward, that user gets the same permissions as fritz. In this case, user "edward" on successful login gets the superuser permissions. If you change the permission for fritz to read-write, user "edward", on successful login, will also get read-write permissions.

Remote Template Accounts

There can be only one remote template account in JUNOScope. You configure a remote template in JUNOScope by creating a user with username remote and a password with any secure name. (See "Adding a User" on page 98.)

In JUNOScope, a remote template is for a user with username 'remote' with a RADIUS account when either no Juniper-Local-User-Name attribute is specified for that user or the specified local user does not exist in JUNOScope (see Table 10 on page 155).

For example:

- The Juniper-Local-User-Name attribute is not specified for the user on the RADIUS server (see Table 12 on page 156)
- The Juniper-Local-User-Name attribute is specified, but the corresponding username is not present in JUNOScope.

Table 10: Remote Template Account

RADIUS Server User Account	JUNOScope Local Template Account
edward password = " edward"	Username: remote
Juniper-Local-User-Name attribute is not specified	Password: remote
	Permissions: superuser

Username "edward" will get the same permissions as the remote template (for example, the same permissions as user remote) if configured in JUNOScope.

If neither the local nor remote template is configured in JUNOScope (for example, for RADIUS user "edward", if both users fritz and remote do not exist in JUNOScope), the RADIUS user will not be able to log in.

For a user with an account in RADIUS to be able to successfully log in to JUNOScope, JUNOScope must have at least remote user template configured.

RADIUS User Login Scenarios

This section provides several scenarios that describe the user account and template account information that should be configured on the RADIUS server and in JUNOScope for a user to log in to JUNOScope with certain permissions.

All RADIUS servers should be up and running for RADIUS users to log in to JUNOScope successfully.

Scenario 1: Logging In to JUNOScope when a Remote Template Account Is Present

If a user account is present on the RADIUS server, the user should be able to log in to JUNOScope if either the Juniper-Local-User-Name attribute is not specified, or the username corresponding to the Juniper-Local-User-Name attribute does not exist in JUNOScope, but the username remote does (see Table 11 on page 156). See also "Remote Template Accounts" on page 154.

Table 11: RADIUS Server Setup, JUNOScope User Information, and Login Results

RADIUS Server Configuration	JUNOScope User Setup Information	Successful Login Results
bob password = 'bobpassword' Juniper-Local-User-Name is not specified	Username: remote Password: remote Permissions: read-only	Username: bob Password: bobpassword Permissions: read-only

Scenario 2: Logging In to JUNOScope when a Local Template Account Is Present

If a user account is present on the RADIUS server, the user should be able to log in if the Juniper-Local-User-Name attribute is specified and the corresponding local user is set up in JUNOScope (see Table 12 on page 156).

Table 12: RADIUS Server Setup, JUNOScope User Information, Login Results

RADIUS Server Configuration	JUNOScope User Setup Information	Successful Login Results
edward password = 'edward' Juniper-Local-User-Name = 'fritz'	Username: fritz Password: fritz Permissions: superuser	Username: fritz Password: fritz Permissions: superuser
	Username: remote Password: remote Permissions: read-only	Username: edward Password: edward Permissions: superuser
		Username: edward Password: edward Permissions: read-only (If you delete user fritz first)

Scenario 3: Logging In to JUNOScope when the Same User Account Is Present on the RADIUS Server and in JUNOScope

If the same username and password are present on the RADIUS server and in JUNOScope, the user can log in to JUNOScope using the username and password combination. After login, the user has the permissions that exist in JUNOScope (see Table 13 on page 157).

Table 13: RADIUS Server Setup, JUNOScope User Information, and Login Results

RADIUS Server Configuration	JUNOScope User Set Up Information	Successful Login Results
honda password = 'honda' Juniper-Local-User-Name = 'fritz'	Username: fritz Password: fritz Permissions: superuser	Username: fritz Password: fritz Permissions: superuser
	Username: honda Password: honda Permissions: read-only	Username: honda Password: honda Permissions: read-only
		Username: honda Password: honda Permissions: superuser (If you delete user honda first)

If the same username is present on the RADIUS server and in JUNOScope, but the passwords on the RADIUS server and in JUNOScope are different, the user can log in using the username and both passwords. After login, the user gets the same permissions as configured on the RADIUS server or locally in JUNOScope depending on whether the username and password combination exists on the RADIUS server or in JUNOScope (see Table 14 on page 157).

Table 14: RADIUS Server Setup, JUNOScope User Information, Login Results

RADIUS Server Configuration	JUNOScope User Setup Information	Successful Login Results
honda password = 'honda' Juniper-Local-User-Name = 'fritz'	Username: fritz Password: fritz Permissions: superuser	Username: honda Password: honda Permissions: superuser
	Username: honda Password: honda123 Permissions: read-only	Username: honda Password: honda123 Permissions: read-only

Chapter 15

Importing and Exporting All Settings Data

This chapter describes how to import and export all JUNOScope software settings data at once, including all dependancies, to and from the JUNOScope database in Extensible Markup Language (XML) file format on the local file system.

You must have superuser permissions to import or export all JUNOScope data.

For information about importing and exporting individual access methods, devices, groups, schedules, or user data, see the following chapters in this guide:

You must have superuser permission to import and export all setup data.

This chapter includes the following topics:

Importing All Settings Data

To import all JUNOScope settings data at once, follow these steps:

1. In the JUNOScope main window, click Settings > Import/Export Data. The Import/Export Data dialog box appears.

2. In the Import All Data area, type the XML filename or browse to the XML file you want to import.

   For example, you can import the default junoscope-all.xml XML file from another JUNOScope server or modify the sample export-import-sample.xml file on the JUNOScope server accordingly. The contents of the sample XML file are as follows:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <all-records xmlns:cinclude="http://apache.org/cocoon/include/1.0">
- <junoscope:users xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:user>
<junoscope:login>admin</junoscope:login>
<junoscope:password>@S@20954@D2A1C46FC4830C53@1B3568CD62D615C9</junoscope:passwo
rd>
<junoscope:user-role>superuser</junoscope:user-role>
</junoscope:user>
</junoscope:users>
- <junoscope:groups
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:group>
<junoscope:name>my-group</junoscope:name>
<junoscope:criteria>SELECT DISTINCT dev.name FROM devices dev WHERE (
dev.deleted_on = 0 ) AND ( ( dev.name LIKE '%delhi%' )
)</junoscope:criteria>
<junoscope:pretty>NAME does contain "delhi"</junoscope:pretty>
<junoscope:comment>my group</junoscope:comment>
</junoscope:group>
</junoscope:groups>
- <junoscope:labels
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:label>
<junoscope:name>my-label</junoscope:name>
<junoscope:category>core</junoscope:category>
<junoscope:comment />
</junoscope:label>
</junoscope:labels>
- <junoscope:devices
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:device>
<junoscope:name>munch</junoscope:name>
<junoscope:hostname>munch</junoscope:hostname>
<junoscope:priority>0</junoscope:priority>
<junoscope:model>J4300</junoscope:model>
<junoscope:comment />
<junoscope:default-access-method>my-access</junoscope:default-access-method>
<junoscope:device-label>my-label</junoscope:device-label>
</junoscope:device>
- <junoscope:device>
<junoscope:name>delhi</junoscope:name>
<junoscope:hostname>delhi</junoscope:hostname>
<junoscope:priority>0</junoscope:priority>
<junoscope:model>T320</junoscope:model>
<junoscope:comment />
<junoscope:default-access-method>my-access</junoscope:default-access-method>
<junoscope:device-label>my-label</junoscope:device-label>
</junoscope:device>
- <junoscope:device>
<junoscope:name>fivestar</junoscope:name>
<junoscope:hostname>fivestar</junoscope:hostname>
<junoscope:priority>0</junoscope:priority>
<junoscope:model>J6300</junoscope:model>
<junoscope:comment />
<junoscope:default-access-method>my-access</junoscope:default-access-method>
<junoscope:device-label>my-label</junoscope:device-label>
</junoscope:device>
</junoscope:devices>
- <junoscope:schedules
```

```
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:schedule>
<junoscope:name>my-sched</junoscope:name>
<junoscope:start-time utc-milliseconds="1138645800653">Tue Jan 31 00:00:00
 IST
2006</junoscope:start-time>
<junoscope:period>every minute</junoscope:period>
<junoscope:comment />
</junoscope:schedule>
</junoscope:schedules>
- <junoscope:access-methods
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
<junoscope:encryption-format>encrypted-and-key-included</junoscope:encryption-fo
rmat>
<junoscope:encryption-key>@S@9DAA03366CD26456EFBC333E44620CA9</junoscope:encrypt
ion-key>
- <junoscope:authentication-information>
<junoscope:name>my-auth</junoscope:name>
<junoscope:login>regress</junoscope:login>
<junoscope:password>@S@14095E0A0A8999C6F8C35FA5F797795C</junoscope:password>
</junoscope:authentication-information>
- <usergroup>
<name>NOC Operator</name>
<role>read-only</name>
<comment>NOC operator</comment>
</usergroup>
<?xml version="1.0" encoding="ISO-8859-1"?>
<junoscope:global-policy
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
<junoscope:maximum-login-attempts>0</junoscope:maximum-login-attempts>
<junoscope:access-window>23</junoscope:access-window>
<junoscope:access-policy>
<junoscope:ip-address>172.17.23.151</junoscope:ip-address>
<junoscope:mask>23</junoscope:mask>
<junoscope:allow>1</junoscope:allow>
<junoscope:comment>blocking my machine</junoscope:comment>
</junoscope:access-policy>
<junoscope:access-policy>
<junoscope:ip-address>2344:2344:2344:2344:2344:2344:2344:2344</junoscope:ip-address>
<junoscope:mask>72</junoscope:mask>
<junoscope:allow>1</junoscope:allow>
<junoscope:comment>ipv6Test</junoscope:comment>
</junoscope:access-policy>
<junoscope:access-policy>
<junoscope:ip-address>127.127.127.126</junoscope:ip-address>
<junoscope:mask>30</junoscope:mask>
<junoscope:allow>1</junoscope:allow>
<junoscope:comment>test</junoscope:comment>
</junoscope:access-policy>
<junoscope:access-policy>
<junoscope:ip-address>127.127.127.127</junoscope:ip-address>
<junoscope:mask>32</junoscope:mask>
<junoscope:allow>1</junoscope:allow>
<junoscope:comment>test</junoscope:comment>
</junoscope:access-policy>
</junoscope:global-policy>
- <junoscope:access-method>
<junoscope:name>my-access</junoscope:name>
<junoscope:type>clear-text</junoscope:type>
<junoscope:authentication>my-auth</junoscope:authentication>
</junoscope:access-method>
```

```
</junoscope:access-methods>
- <junoscope:radius-clients-config
xmlns:junoscope="http://xml.juniper.net/jtk/export/1.0">
- <junoscope:radius-server-entry>
<junoscope:server-name>10.209.148.102</junoscope:server-name>
<junoscope:port-no>1812</junoscope:port-no>
<junoscope:acct-port-no>1813</junoscope:acct-port-no>
<junoscope:shared-secret>@S@6DE028955F902AB28F435E9C314C38219490246BB894C586E582
6E93F712E90A3C9D8D53EE6AB4FE4B10FE0FAF25F636</junoscope:shared-secret>
</junoscope:radius-server-entry>
</junoscope:radius-clients-config>
</all-records>
```


3. Type the key to decrypt the sensitive data that you want to import if the key was not included when the data was exported.
4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records. The available import method options include:
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.
5. In the Import All Data area, click Import All Data. The Import/Export Data confirmation dialog box appears.

Home > Settings > Import/Export Data

Settings

Import/Export Data

Settings	Results	Details
Usergroups	7 imported 0 failed	
Users	5 imported 0 failed	
RADIUS Configuration	1 imported 0 failed	
Authentication Policy	6 imported 0 failed	
Labels	1 imported 0 failed	
Authentication Information	2 imported 0 failed	
Access Methods	1 imported 0 failed	
Devices	5 imported 0 failed	
Groups	1 imported 0 failed	
Schedules	0 imported 0 failed	
Saved Operations	1 imported 0 failed	
Global Authentication Policy	1 imported 0 failed	

OK

6. Click OK.

   All setup information in the database is saved with all dependencies to the local file system with the filename that you specified.

Exporting All Settings Data

You can export all JUNOScope settings data at once to an export XML file for importing later to another JUNOScope server.

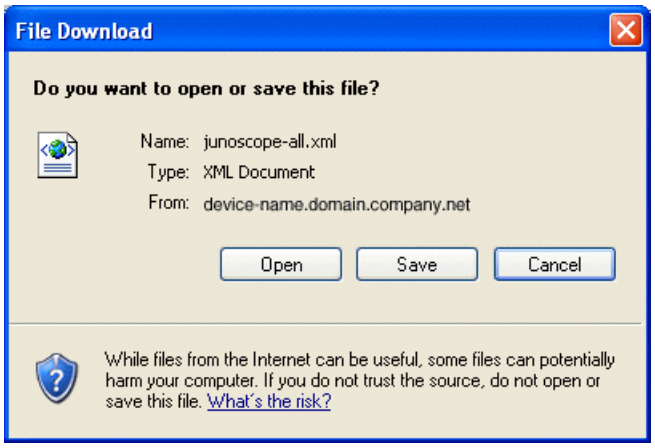
To export all setup data at once, follow these steps:

1. In the JUNOScope main window, click Settings > Import/Export Data. The Import/Export Data dialog box appears.

2. Select how you want sensitive data in authentication information exported from the JUNOScope software. Sensitive authentication information can be exported in one of the following ways:

   - Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
   - Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export all settings data to another system.
   - Export sensitive data unencrypted—Sensitive password data is not encrypted at export.

3. In the Export All Data area, click Export All Data. The File Download dialog box appears.



4. Click Save to export all of the setup data in the database to a default export XML file named junoscope-all.xml. Click Open to view the contents of the export XML file.

NOTE: The junoscope-all XML filename is not generated if you use the Microsoft Internet Explorer 6.0 Web browser to export JUNOScope setup data. You will see an export####### filename.

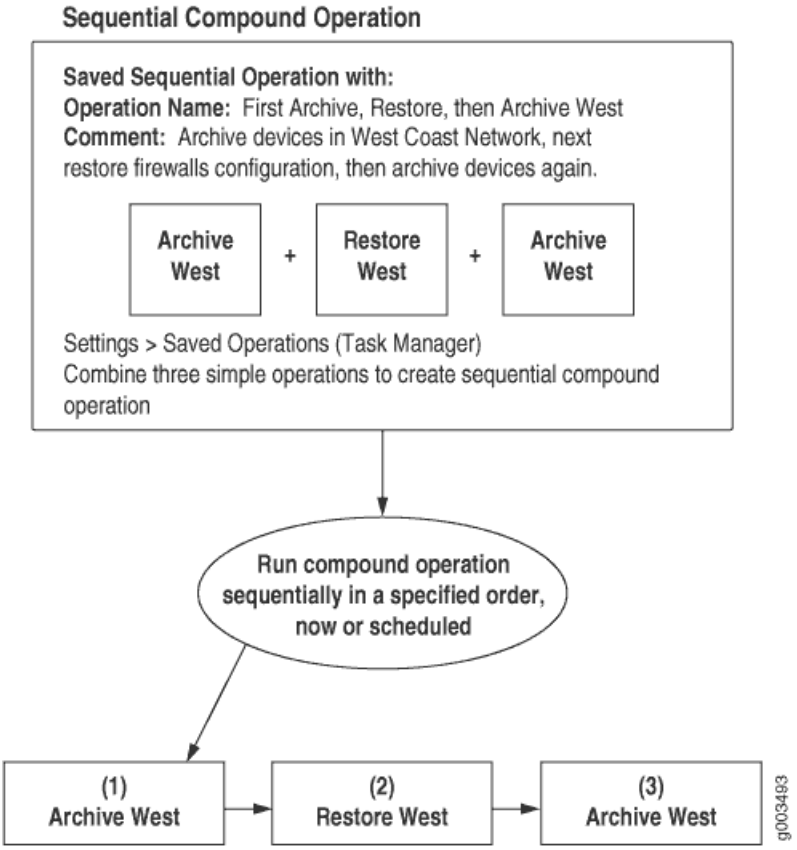
Chapter 16

Using Task Manager (Saved Operations)

Use Task Manager to create compound operations from any simple and compound operations that you have saved. A simple operation is an action applied to one or more devices; for example, archive router1. A compound operation is a combination of simple or compound actions applied to one or more devices; for example, archive all devices, restore-merge all routers, then archive all routers again.

You save simple archive (Settings > Archive), restore (Settings > Restore), and inventory scan (Inventory Management > Scan) operations by providing a unique name and an optional comment. Saved operations are listed in the Task Manager (Settings > Saved Operations). (See Figure 3 on page 167.)

Figure 3: Saved Operations



Devices on the network may share a large portion of their configuration with one another—they might have the same DNS, NTP, SNMP, system log, and RADIUS configuration; the same firewall filters; the same routing protocols, and the same routing policies. For this reason, you can take one configuration and import it into the JUNOScope software using Configuration > Repository > Import, then save that configuration with a unique name and a descriptive comment. Using Task Manager, you can then restore that configuration (upload it) to multiple devices. Saving operations from a device or group and reusing them reduces production time and errors.

With Task Manager, you can manipulate saved operations as follows:

- Create compound operations from simple operations and specify their execution order: concurrent or sequential. Concurrent compound operation tasks run on one or more devices in parallel or in no specified order; sequential compound operation tasks run on one or more devices in the order that you specify.
- Run operations in real time or as part of an existing schedule.
- Assign devices to a saved operation, and run it real time or as part of an existing schedule.
- View simple operation settings.
- Edit all compound operation settings.
- Delete operations.

You can immediately view the status of operations that have run in real time. You can view the status of these operations using an existing schedule (Monitor > Operations). You can also view the status of a selected operation (Monitor > Status).

To use Task Manager operations, you must have superuser or read-write permission.

This chapter includes the following topics:

Saving a Simple Operation

You can save simple operations, such as archive, restore, and inventory scan. A simple operation is a JUNOScope action applied to a device; for example, archive router1.

You save simple operations in the archive, restore, and inventory scan user interfaces by providing a unique name and an optional comment. Saved operations are listed in the Settings > Saved Operations dialog box of the Task Manager.

To save an archive, restore, or inventory scan operation, do one of the following:

- To save an archive operation, see "Saving an Archive Operation" on page 199
- To save a restore operation, see "Saving a Configuration Restore Operation" on page 245
- To save an inventory scan operation, see "Saving an Inventory Scan Operation" on page 342

Viewing Saved Operations

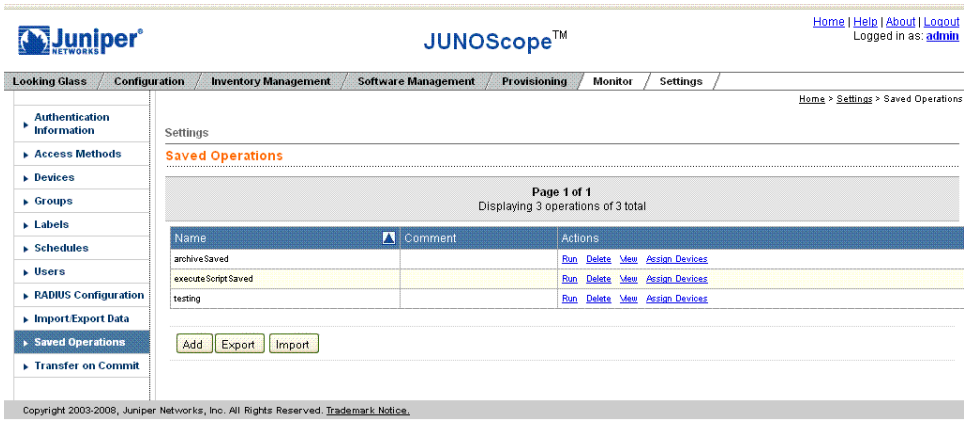
The Saved Operations dialog box lists simple operations (one action applied to a device) that you have saved from the archive, restore, or inventory scan user interfaces. This dialog box also lists compound operations (multiple actions applied to a device) that you can create using the Add button.

Use the Saved Operations dialog box to manage saved simple and compound operations at a glance. You can do the following:

- Sort all saved operations by Name or Comment by clicking the column header.
- Combine simple operations to create compound operations and specify the order in which they will run using the Add button and the Edit link. For more information, see "Adding a Concurrent Compound Operation" on page 170, "Adding a Sequential Compound Operation" on page 172, and "Editing Compound Operation Settings" on page 180.
- Run simple and compound operations using the Run link. For more information, see "Running a Saved Operation" on page 174.
- Delete operations using the Delete link. For more information, see "Deleting Saved Operations" on page 190.
- View simple operation settings using the View link. The View link is specific to simple operations only. For more information, see "Viewing Simple Operation Settings" on page 179.
- Edit compound operation execution order, sequencing, and other settings using the Edit link. For more information, see "Editing Compound Operation Settings" on page 180.

To view saved operations, do the following:

- From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.



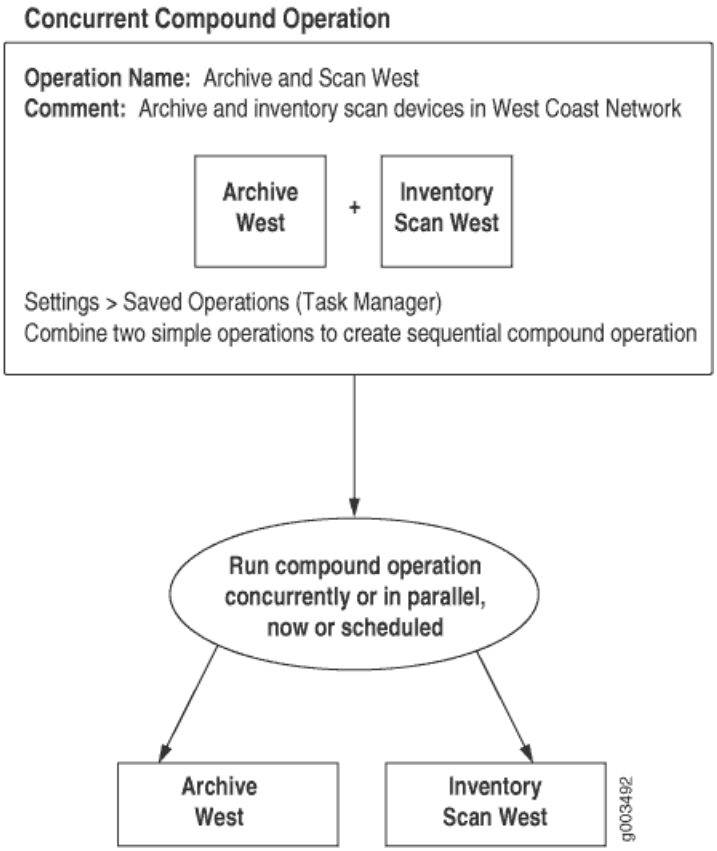
For more information about creating compound operations, see:

- Adding a Concurrent Compound Operation on page 170
- Adding a Sequential Compound Operation on page 172

Adding a Concurrent Compound Operation

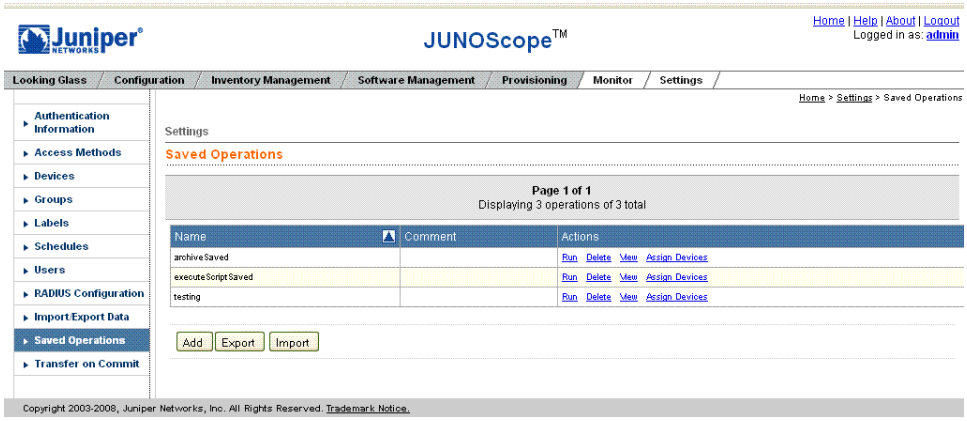
A concurrent compound operation is a combination of simple and compound actions, the execution order of which is not guaranteed. From the Saved Operations dialog box, you can combine simple and compound operations to run concurrently in real time or at a scheduled interval using the Add button and the Edit link. (See Figure 4 on page 171.)

Figure 4: Concurrent Compound Operation

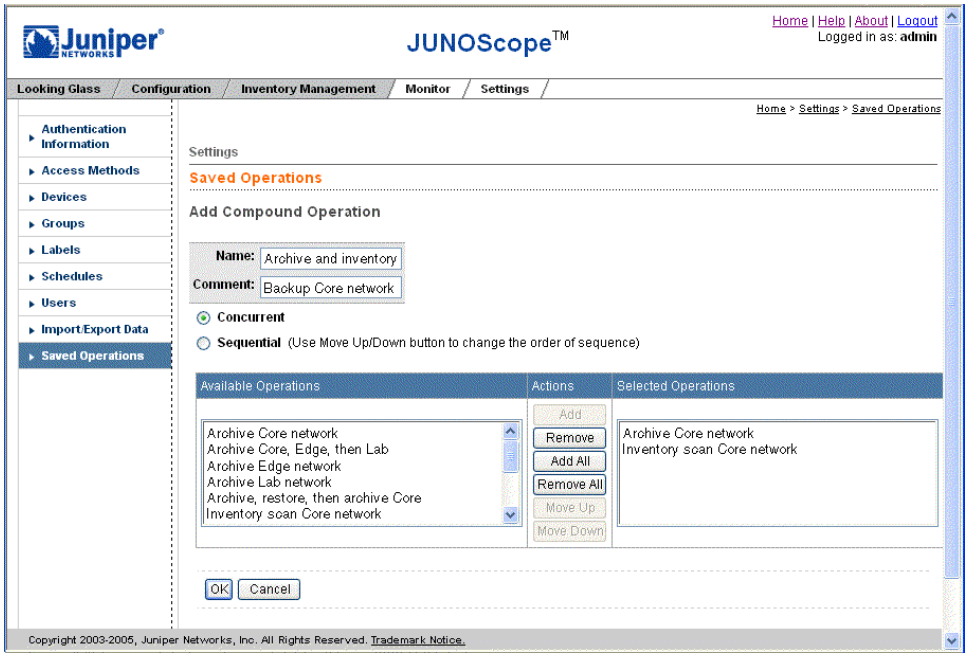


To add a concurrent compound operation, follow these steps:

1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.



2. Click Add. The Add Compound Operation dialog box appears.



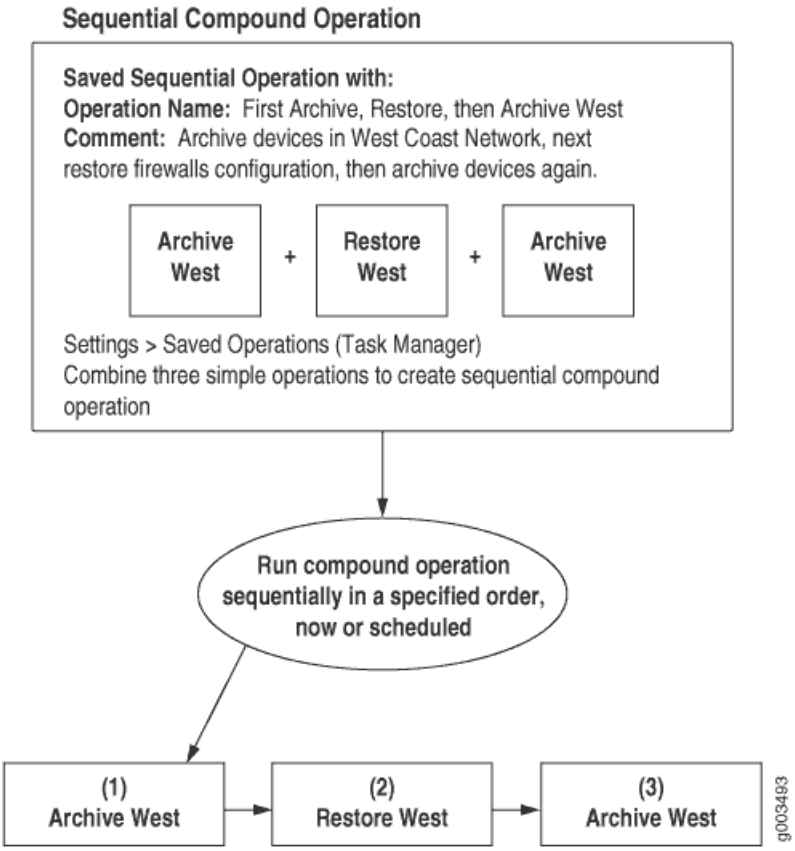
3. Type a unique name for the concurrent compound operation in the Name text box.
4. Type an optional comment describing the concurrent compound operation in the Comment text box.
5. Click the Concurrent option button.
6. Select the operations that you want to include in the concurrent compound operation from the Available Operations list box and click Add. The selected operations appear in the Selected Operations list box. The operations will be executed in parallel or no specified order.
7. Click OK.

   The compound operation name appears alphabetically in the Saved Operations dialog box. You can edit compound operations from the Saved Operations dialog box by clicking the Edit link. The Edit link is specific only to compound operations.

Adding a Sequential Compound Operation

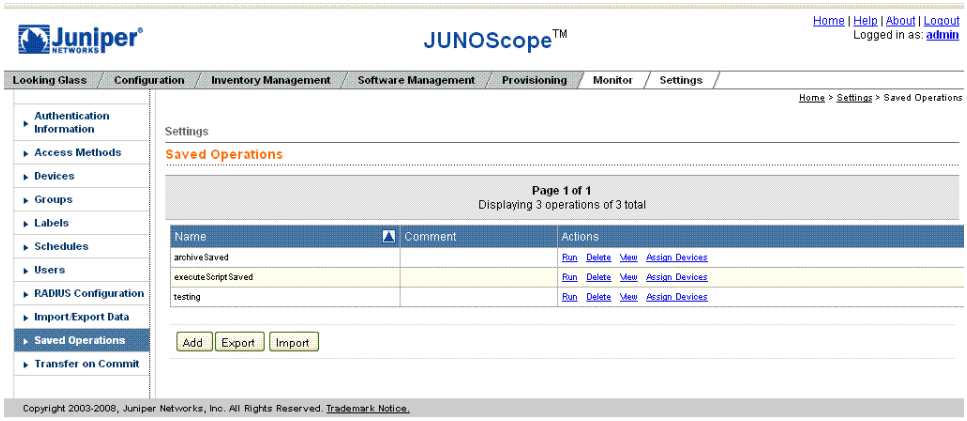
A sequential compound operation is a combination of simple or compound actions that you want to execute on one or more devices in a specific order or sequence. From the Saved Operations dialog box, you can combine simple or compound operations to create compound operations that run sequentially in real time, or at a scheduled interval using the Add button and the Edit link. (See Figure 5 on page 173.)

Figure 5: Sequential Compound Operation

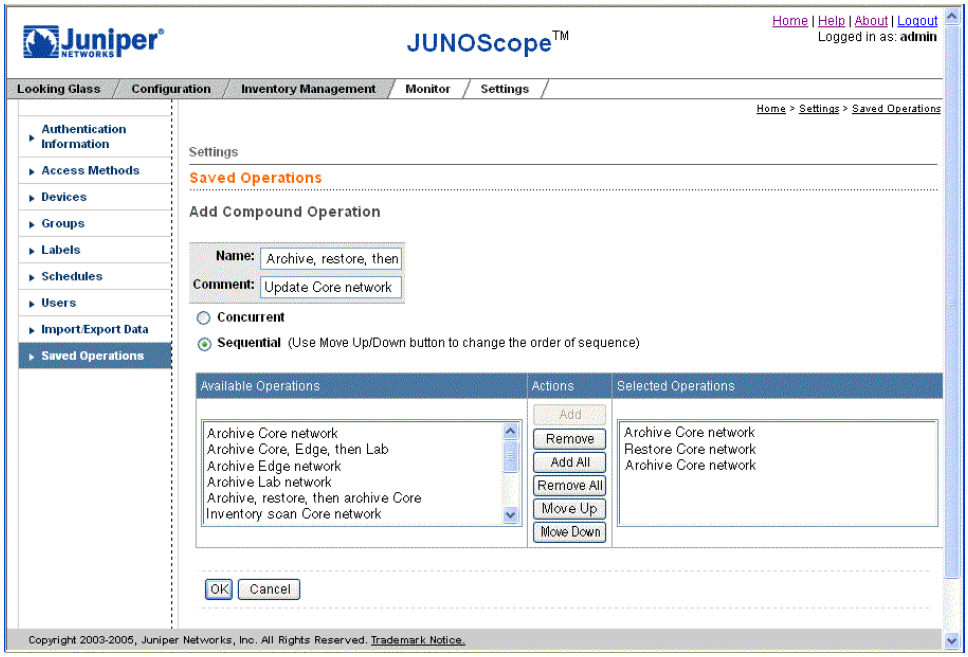


To add a sequential compound operation, follow these steps:

1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.



2. Click Add. The Add Compound Operation dialog box appears.



3. Type a name for the sequential compound operation in the Name text box.
4. Type an optional comment describing the sequential compound operation in the Comment text box.
5. Click the Sequential option button. The Move Up and Move Down action buttons are enabled.
6. Select the operations that you want to be in the sequential operation from the Available Operations list box, and click Add. The selected operations appear in the Selected Operations list box.
7. Use the Move Up and Move Down action buttons to change the order in which the operation will occur. These buttons are only available when you select the Sequential option. The operations will be executed in the order in which they appear in the list from top to bottom.
8. Click OK.

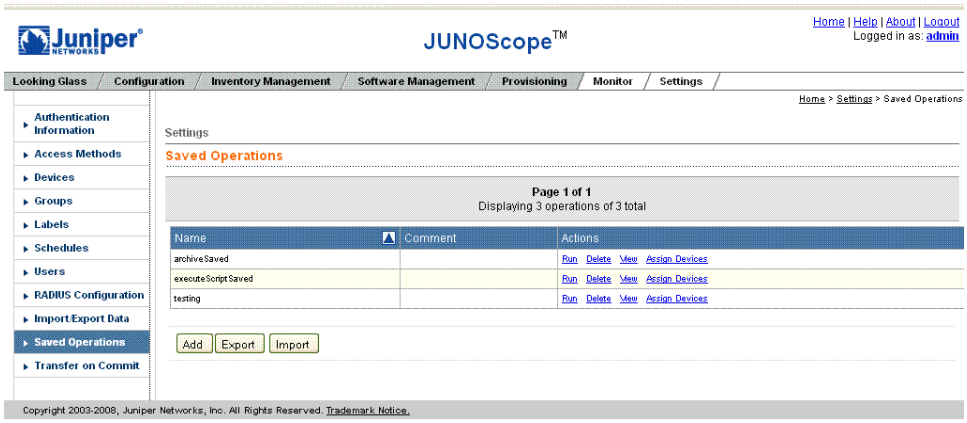
   The compound operation appears alphabetically in the Saved Operations list box. You can edit compound operations from the Saved Operations dialog box by clicking the Edit link. The Edit link is specific only to compound operations.

Running a Saved Operation

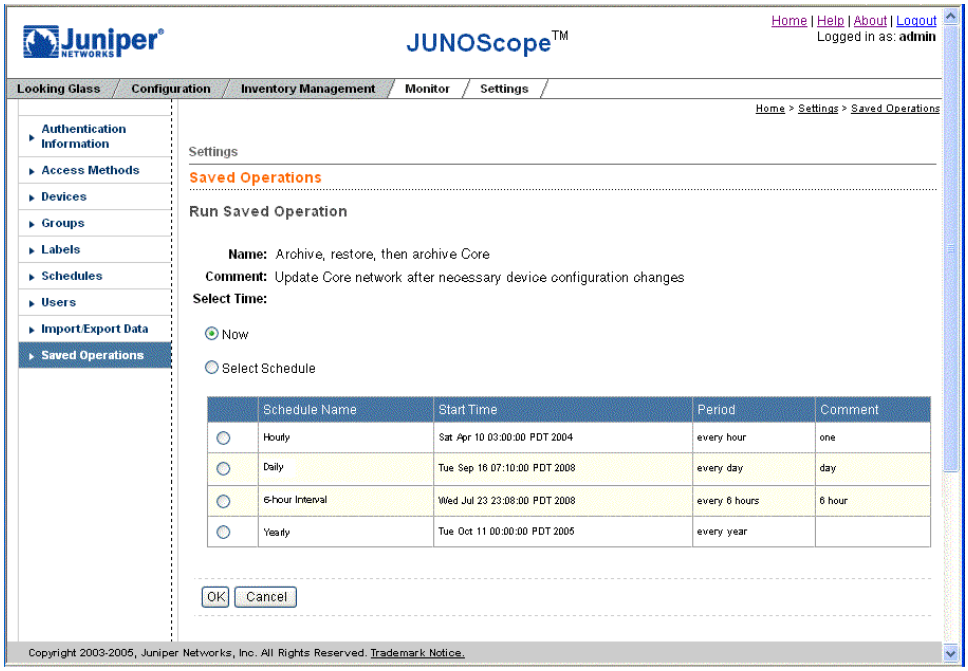
You can run saved operations in real time or at a scheduled interval. The execution of tasks in a concurrent compound operation is not guaranteed. The execution of tasks in a sequential compound operation is guaranteed in the order that you specify in the Add Compound Operation dialog box.

To run an operation that you have saved, follow these steps:

1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.



2. Click the Run link for the operation that you want to run. The Run Saved Operation dialog box appears.

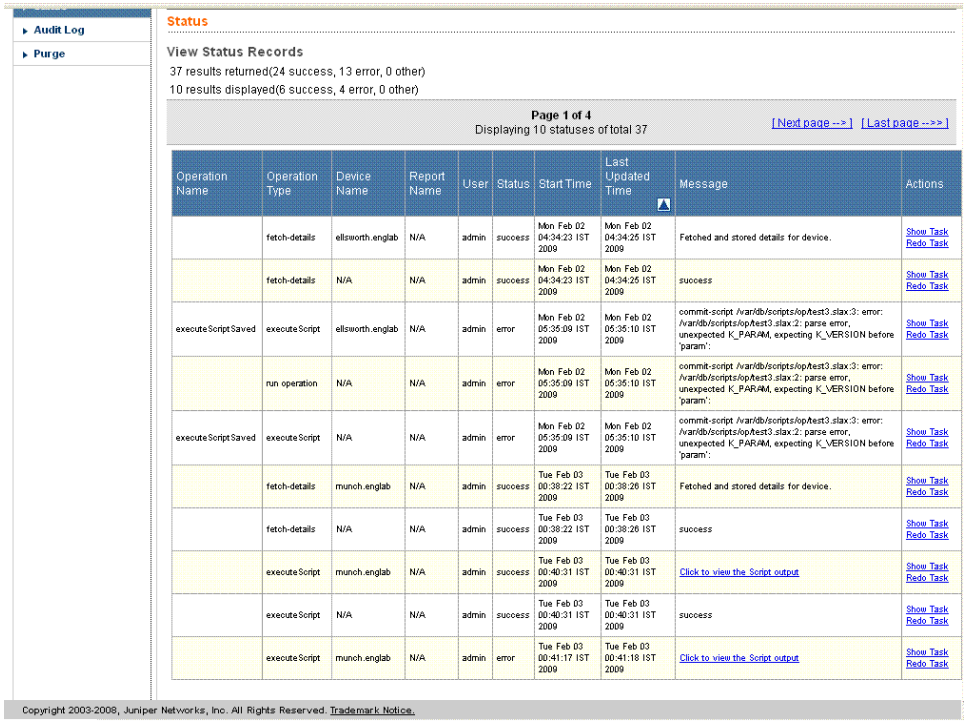


You can select to run the operation now or at a scheduled interval.

Running an Operation Now

To run an operation now or immediately, follow these steps:

1. In the Saved Operations dialog box, select the Run operation link for the operation that you want to run. The Run Saved Operation dialog box appears.
2. Click the Now option button and click OK to run the operation, immediately in real time. The View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

The View Status Records dialog box lets you view the status of each task that ran in a simple or compound operation. At a glance, you can see the operation name, operation type, the device name on which the operation ran, the user who ran the operation, operation status, start time, last updated time, and an operation status message.

The View Status Records dialog box refreshes every 10 seconds.

NOTE: If you run an operation using the Saved Operations wizard, you see one additional status record with an operation type of " run operation" to indicate the status of running the saved operation. This status record will not appear if you run an operation using the Archive, Restore, or Inventory Scan wizards.

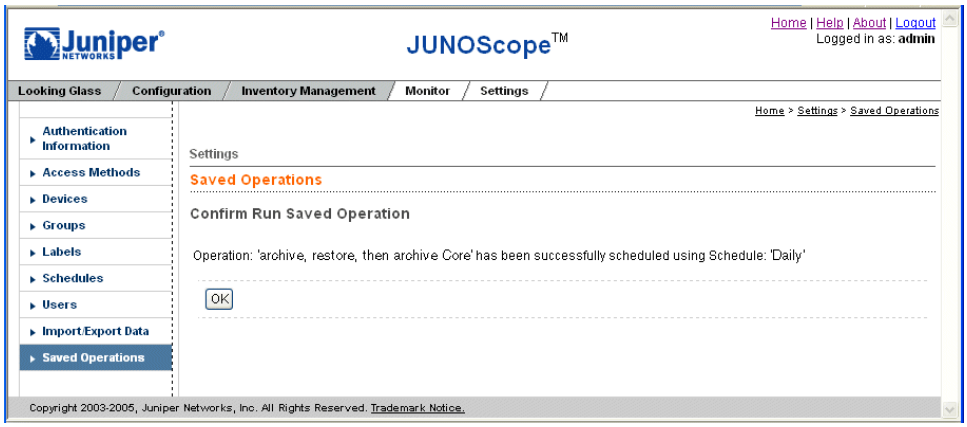
The status of a compound operation is successful when all tasks within it have run successfully.

Running a Scheduled Operation

To run a scheduled operation, do the following:

1. In the Run Saved Dialog Box, click the Select Schedule option button.
2. Select a schedule, and click OK.

   The Confirm Run Saved Operation dialog box appears.

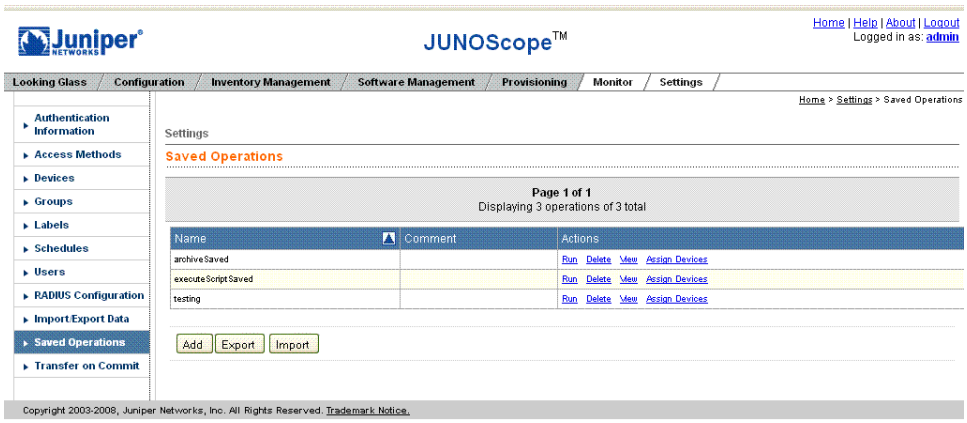


3. Confirm that the run settings for the operation are correct and click OK. The Saved Operations dialog box appears. The operation runs at the selected scheduled interval.

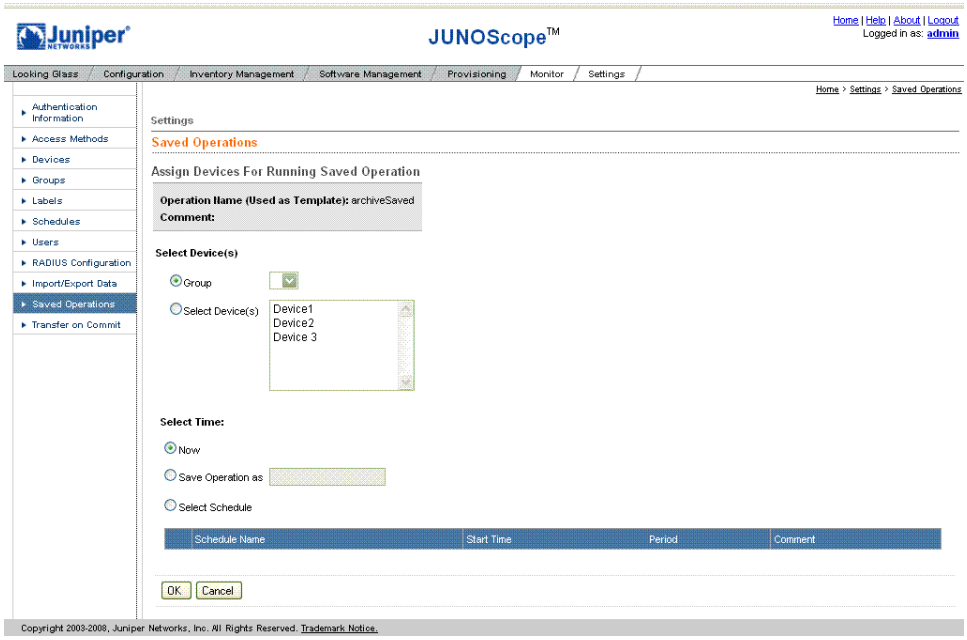
Assigning Devices to a Saved Operation

You can assign devices or a group to a saved operation. The saved operation is used as a template , but it will not run on the devices that were originally used in the saved operation. Instead, the saved operation will run on the new device or group which is specified by the user. A concurrent compound operation is created and the saved operation concurrently operates on each of these devices. If you assign a group to a saved operation, the group only expands once, and the saved operation runs on the devices belonging to that group.

1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.

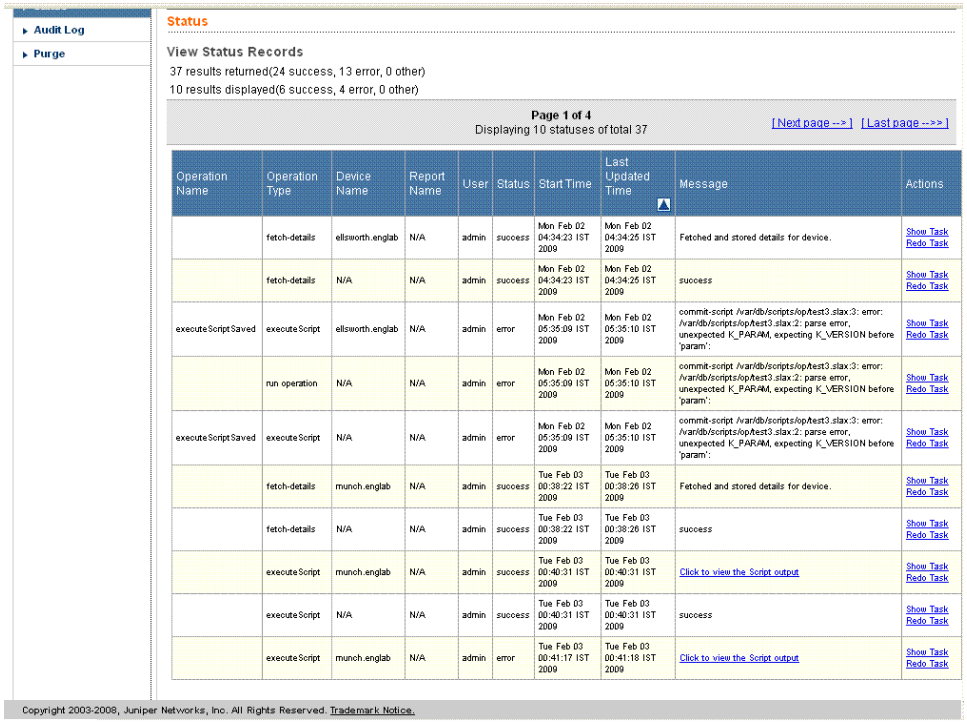


2. Click the Assign Devices link for the operation that you want to run. The Assign Devices for Running Saved Operation dialog box appears.



3. Select the Group or Select Device(s) option button.
4. Select the group or devices that you want from the Group or Select Device(s) list box. Shift + click to select multiple devices from the Select Device(s) drop-down list box.
5. Select when you want the software image download to occur by clicking the appropriate option button:
   - Now—(Default) Runs the operation immediately after you confirm it.
   - Save Operation as—Saves the current operation in the Settings > Saved Operations table so you can combine that operation with other operations or run that operation at a later time. Click the Save Operation as option button, then type an operation name in the text box. You cannot assign any more devices to these saved operations.
   - Select Schedule—Runs the operation at the scheduled time interval. Select the schedule that you want in the schedule table.
6. Click OK.
   - If you selected the Now option, the saved operation immediately runs on the devices or group that you assigned to the operation.
   - If you selected the Save Operation as option, the operation is saved and listed in the Settings > Saved Operations dialog box. You cannot assign any more devices to these saved operations therefore, only the Run, View, and Delete links are displayed on the Status—View Status Records dialog box.
   - If you selected the Select Schedule option and selected a schedule, the operation runs when the operation is scheduled to be run.

   When the operation run process is complete, the Status—View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

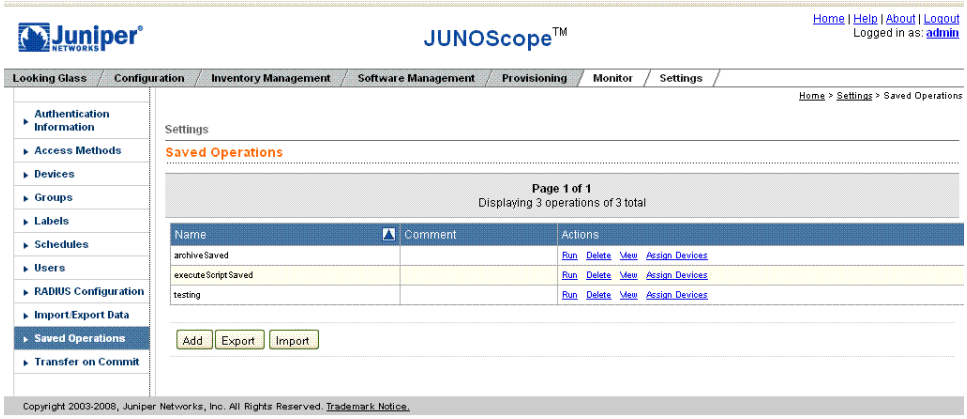
The Status—View Status Records dialog box lists the operation by operation name, operation type, report name, username, operation status, last updated time, and operation system log message. The operation status can be successful, failed, writing, pending, rebooting, connecting, or working.

Viewing Simple Operation Settings

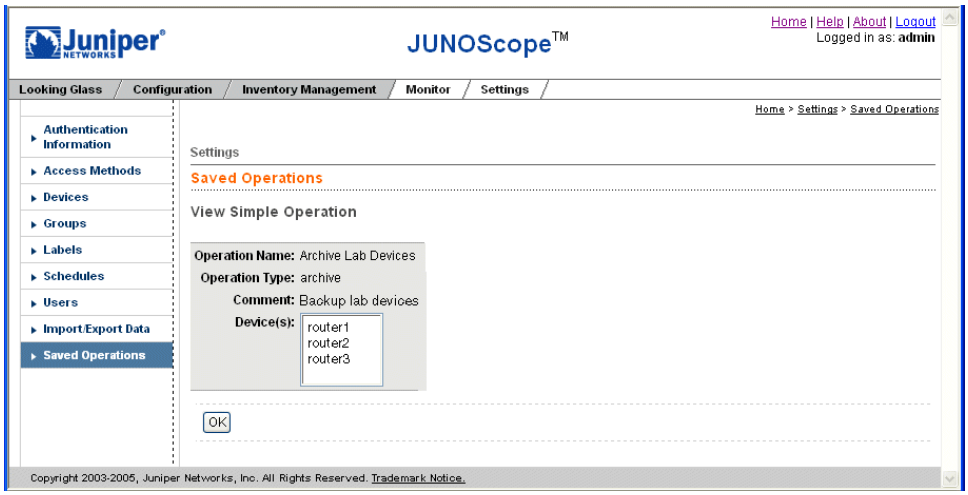
You can view the settings of a saved simple operation. For archive and inventory scan operations, the View Simple Operation dialog box displays the operation name, operation type, comment, and the devices on which the operation will execute. For restore operations, the View Simple Operation dialog box also displays, the archived configuration or the name of an imported configuration file, configuration revision level, configuration load action, and whether the Routing Engines are synchronized.

To view simple operation settings, follow these steps:

1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.



2. Click the View link for the saved operation that you want. The View Simple Operation dialog box appears.



3. Check that the operation settings are what you want, then click OK. You return to the Saved Operations dialog box.

Editing Compound Operation Settings

Editing compound operation settings gives you the flexibility of checking and changing the settings for compound operations made up of archive, restore, and inventory scan operations. Unlike simple operations, compound operations listed in the Saved Operations dialog box have an Edit link.

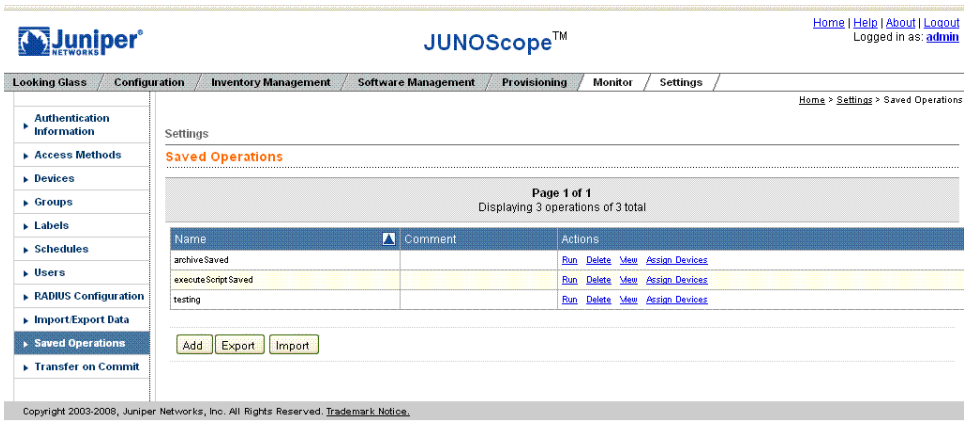
You can edit the following compound operation settings:

- Name.
- Optional comment.

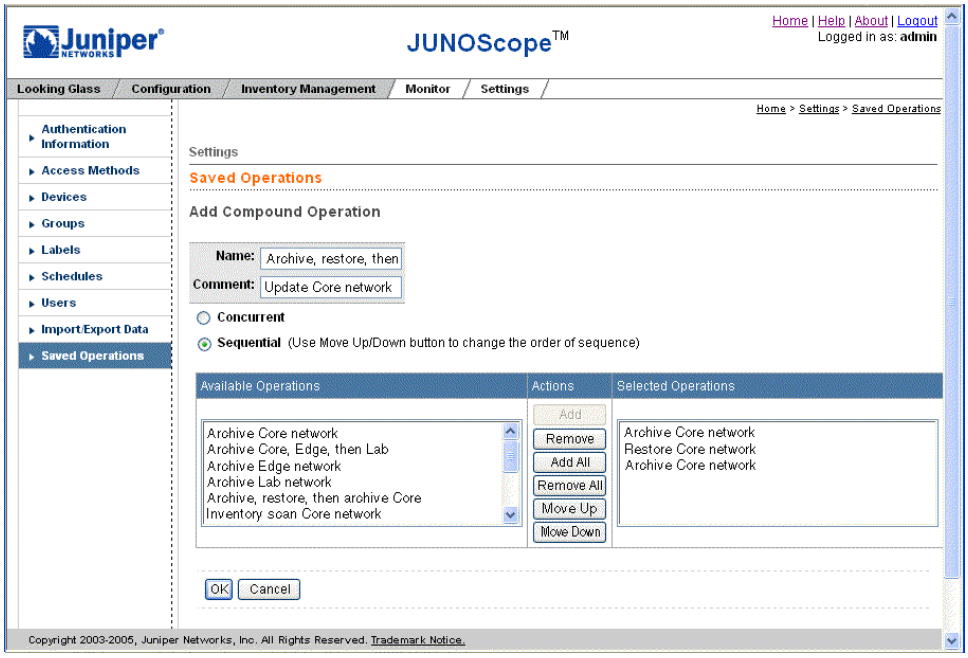
- Execution method—Concurrent or sequential. Concurrent compound operation tasks run on one or more devices at the same time; sequential compound operation tasks run on one or more devices in the order that you specify.
- For concurrent compound operations, you can edit the tasks that you want included. For sequential compound operations, you can edit the order in which you want tasks to occur.

To edit compound operation settings, follow these steps:

1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.



2. Click the Edit link for the saved operation that you want. The Edit Compound Operation dialog box appears.



3. Edit the settings in the Edit Compound Operations dialog box, then click OK. The Saved Operations dialog box appears.

Monitoring Run Operations

You can view the status of operations that have run in several ways:

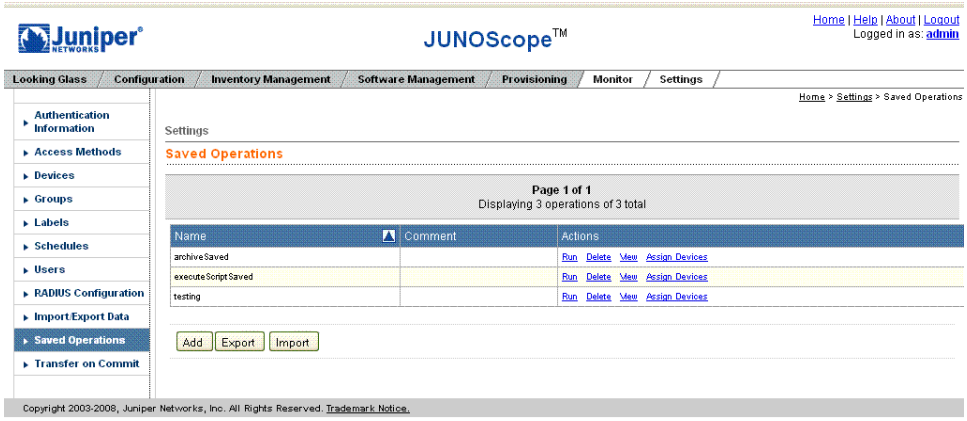
- Immediately after running an operation using the Now schedule option (see "Monitoring Operations Run in Real Time" on page 182)
- Using Monitor > Operations (see "Monitoring Operations Run Using a Schedule" on page 185)
- Using Monitor > Status (see "Monitoring Selected Operation Status" on page 185)

Monitoring Operations Run in Real Time

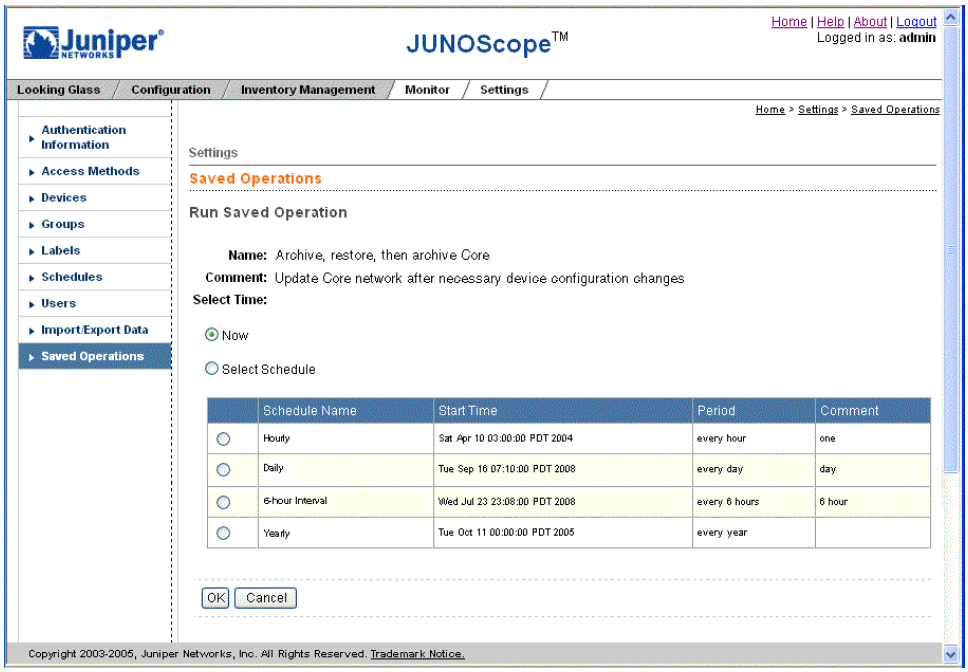
When you run an operation in real time using the Now schedule option, the View Status Records dialog box appears displaying the results of each task that was run.

To view the status of operations run in real time, follow these steps:

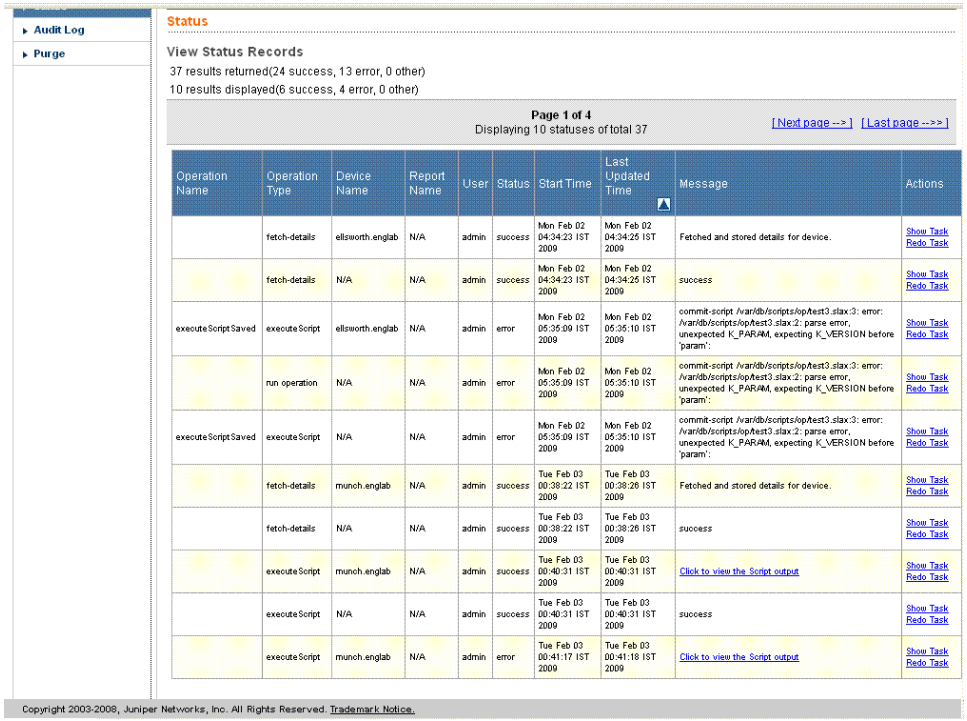
1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.

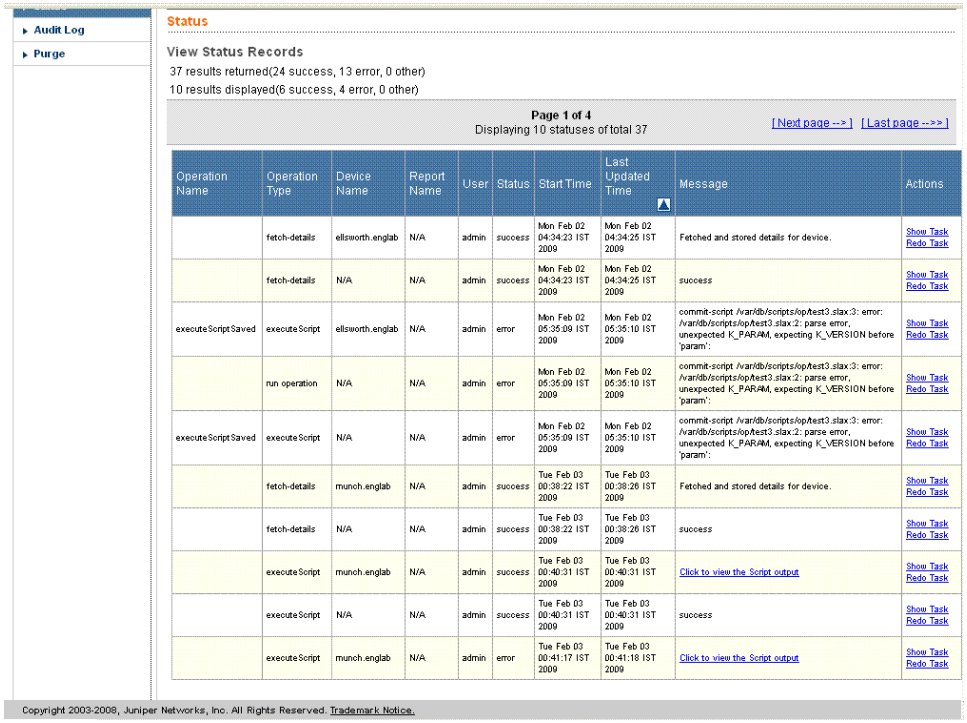


2. Click the Run link or the operation that you want to run. The Run Saved Operation dialog box appears.



3. Click the Now option button, and click OK to run the operation immediately in real time. The View Status Records dialog box appears.





Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

The View Status Records dialog box shows the status of each task that ran in a simple or compound operation. At a glance, you can see the operation name, operation type, the device name on which the operation ran, the user who ran the operation, operation status, start time, last updated time, and an operation status message.

The View Status Records dialog box refreshes every 10 seconds.

The status of a compound operation is successful when all tasks within it have run successfully.

Since a task can contain multiple Operations, in this step the operations in this task will be listed down. You can now select the operation you wish to redo and click on next.

JUNOScope displays two list boxes one with all the devices on which the operation was successful and the other list box will contain failed devices. You can select the devices on which you wish to redo the operation from either of the list boxes.

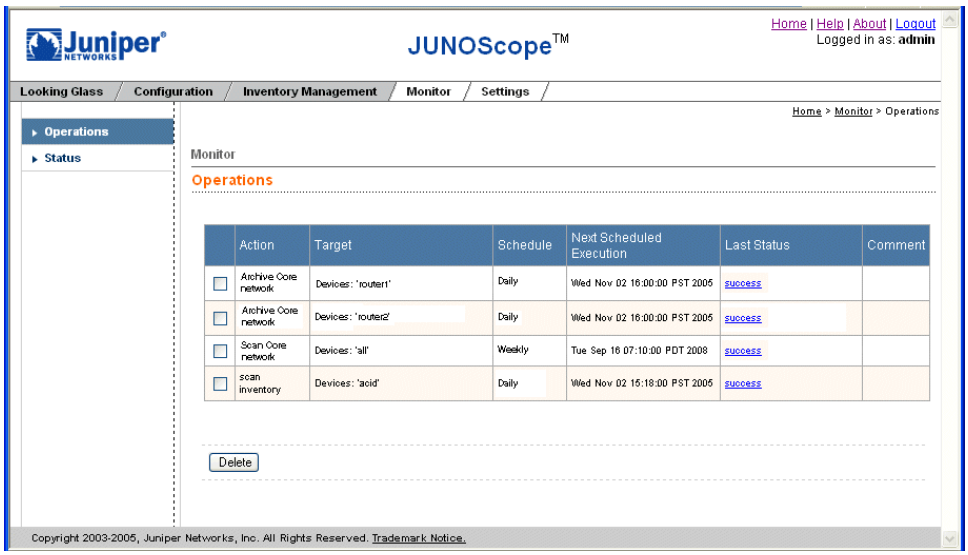
NOTE:

- The Redo Wizard always displays a device list even if during a task creation device group was selected.
- Only devices on which the operation failed (ERROR, ABORTED) or successful are listed. Devices on which the operation is in any other state is not be listed.
- Devices on which the Operation was executed but are deleted from JUNOScope will be excluded from the list boxes.

Monitoring Operations Run Using a Schedule

Use the Operations dialog box to view operations that have run using an existing schedule. An operation does not appear in the Operations dialog box if you ran it immediately using the Now option. For more detailed information about using the Operations dialog box, see “Managing Operations” on page 313.

To view the Operations dialog box, from the JUNOScope main window, click Monitor > Operations. The Monitor Operations dialog box appears.



The Operations dialog box lists all operations run using a schedule by operation type, target devices, execution schedule, when the operation is scheduled to run again, last run status, and an optional comment about the operation.

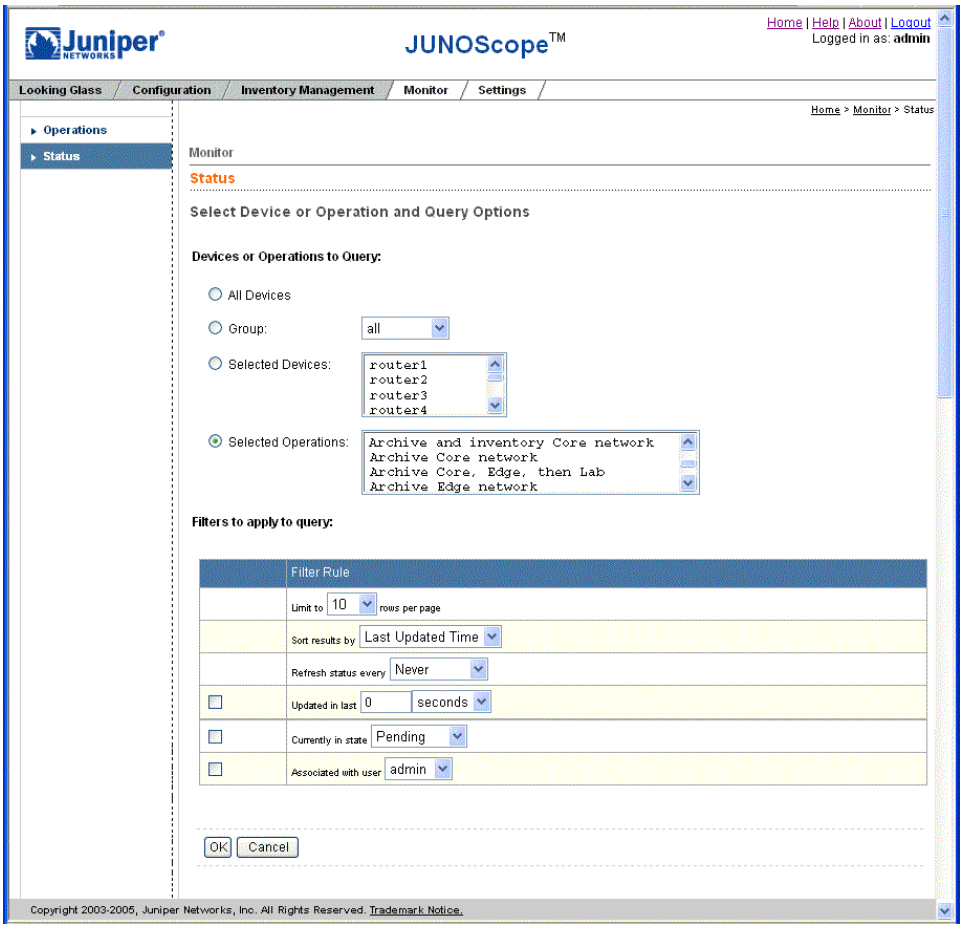
Click a link in the Last Status column for an operation to display the View Status Records dialog box (for more information, see “Monitoring Operations Run in Real Time” on page 182).

Monitoring Selected Operation Status

Use the Monitor Status dialog box to view the operation status of a saved operation that you select. For more detailed information about monitoring operation status, see “Viewing and Maintaining Operation Status” on page 315.

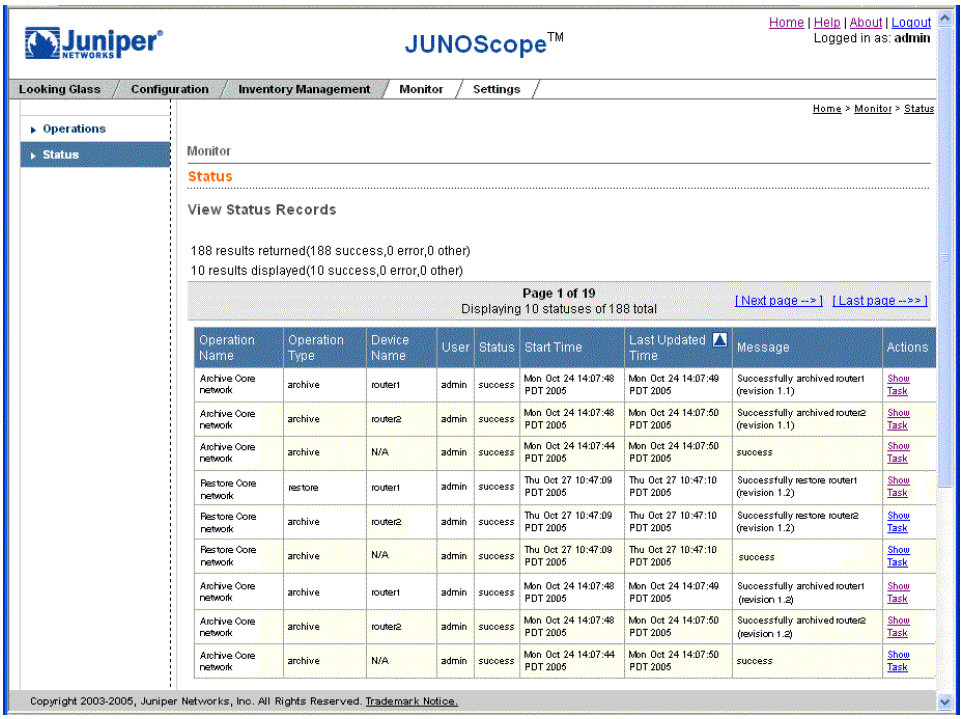
To view the status of a selected saved operation, follow these steps:

1. From the JUNOScope main window, click Operation > Status. The Status—Select Device or Operation and Query Options dialog box appears.



2. Click the Selected Operations option button, and select the saved operation for which you want to view status.

3. Click OK. The View Status Records dialog box appears displaying the operation status by operation name, operation type, device name, username, operation status, start time, last updated time, and a status message.



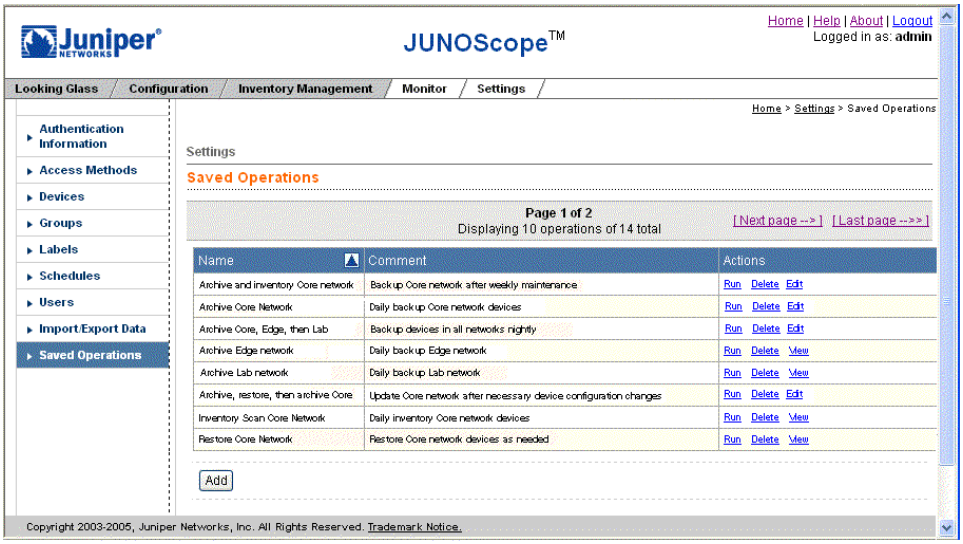
Click the Show Task link to display a page that displays the status records that are run as part of the task you selected. Click Back to status to return to the View Status Records dialog box.

Importing Saved Operations Information

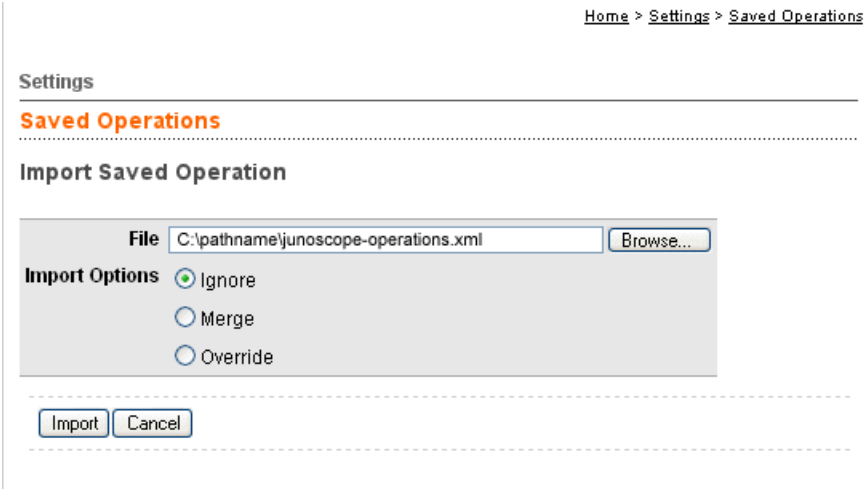
You can import device information from another JUNOScope server, or you can use the provided sample XML import file export-import-sample.xml as a guide. Importing saved operations information is useful when you do not want to enter that information manually.

To import schedules information, follow these steps:

1. In the JUNOScope main window, click Settings > Saved Operatins. The Saved Operations dialog box appears.



2. Click Import. The Import Schedules dialog box appears.



3. In the File text box, either browse to or type the name of the XML file that you want to import. For example, you can import the default schedules.xml export file from another JUNOScope server or use the provided sample export-import-sample.xml XML file on the JUNOScope server to generate a file to import.

NOTE: The junoscope- XML file prefix is not generated if you use the Microsoft Internet Explorer 6.0 Web browser to export JUNOScope setup data. You will only see the schedules filename.

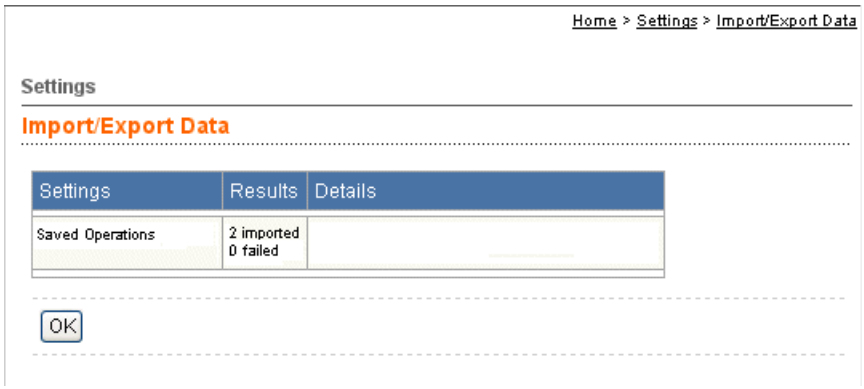
---

4. To support synchronizing JUNOScope settings imported from multiple servers, select an import method to be used if a conflict occurs between existing records

stored in the JUNOScope server and imported records. The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

5. Click Import. The Import status dialog box appears.



The dialog box indicates the number of records imported successfully and unsuccessfully. The Details column provides a description for records that fail import.

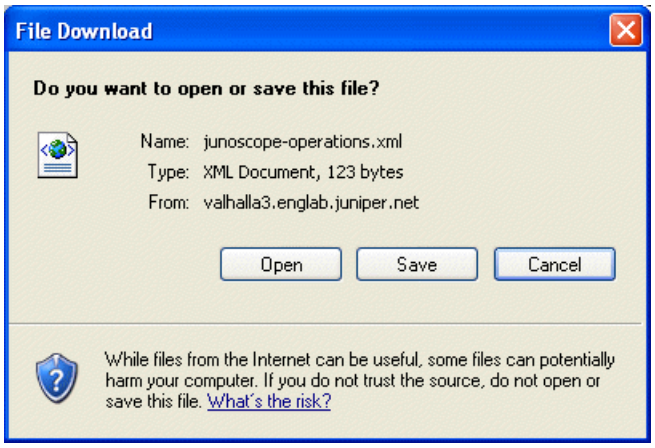
6. Click OK. The imported data is listed in the Saved Operations dialog box.

Exporting Saved Operations Information

You can export saved operations that you want back up or import to another JUNOScope server.

To export export saved operations information, follow these steps:

1. In the JUNOScope main window, click Settings > Saved Operations. The Saved Operaitons dialog box appears.
2. Click Export. The File Download dialog box appears.



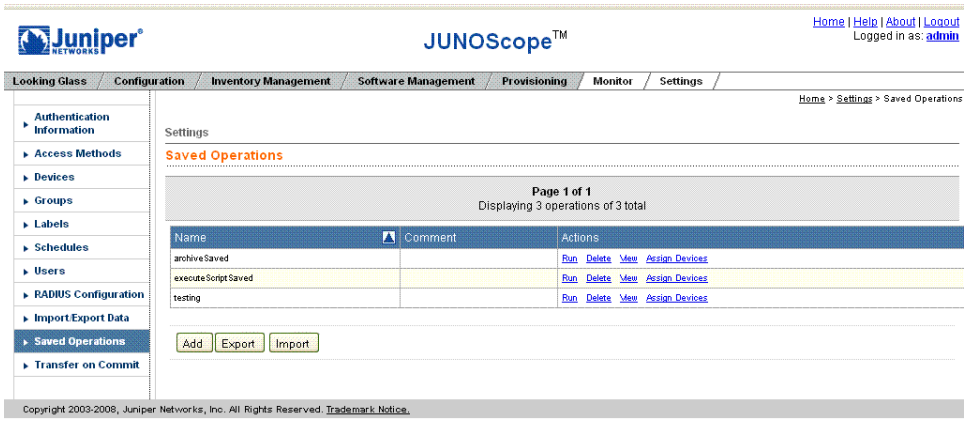
3. Click Save to save the saved operations information to the local filesystem.

Deleting Saved Operations

You can delete saved operations. However, you cannot delete a simple operation that is being used in a compound operation. Also, you cannot delete any simple or compound operation that is already scheduled to run. To delete an operation that is already scheduled to be run, use Monitor > Operations. For more information, see "Managing Operations" on page 313.

To delete an operation that you have saved, follow these steps:

1. From the JUNOScope main window, click Settings > Saved Operations. The Saved Operations dialog box appears.



2. Click the Delete link for the operation that you want.

Part 4
Performing Configuration Management

Chapter 17

Archiving and Manipulating Device Configurations

This chapter describes how to perform an archive operation that copies a configuration file from a router or a group of routers to the JUNOScope software and stores it in the Concurrent Versions System (CVS) repository, where all revisions of router configuration files are stored.

This chapter also describes how to edit archived configurations, save archived configurations to a local file system and save a configuration operation so that you can combine it with other operations, such as restore and inventory scan, to run on devices in your network that you specify,

Once archived, you can display a configuration, compare two revisions of a configuration, or restore a configuration.

This chapter also describes how to configure a JUNOS device to transfer its device configuration to the JUNOScope server when a commit succeeds.

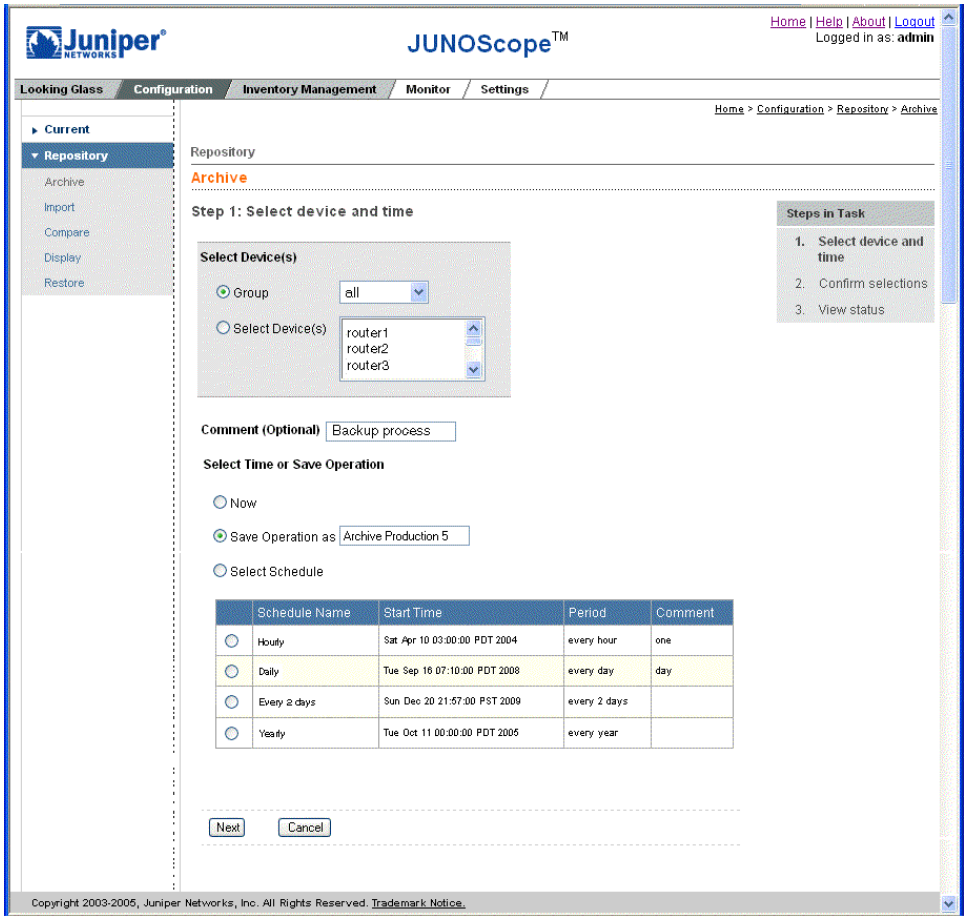
You must have superuser or read-write permission to archive a configuration file.

This chapter includes the following topics:

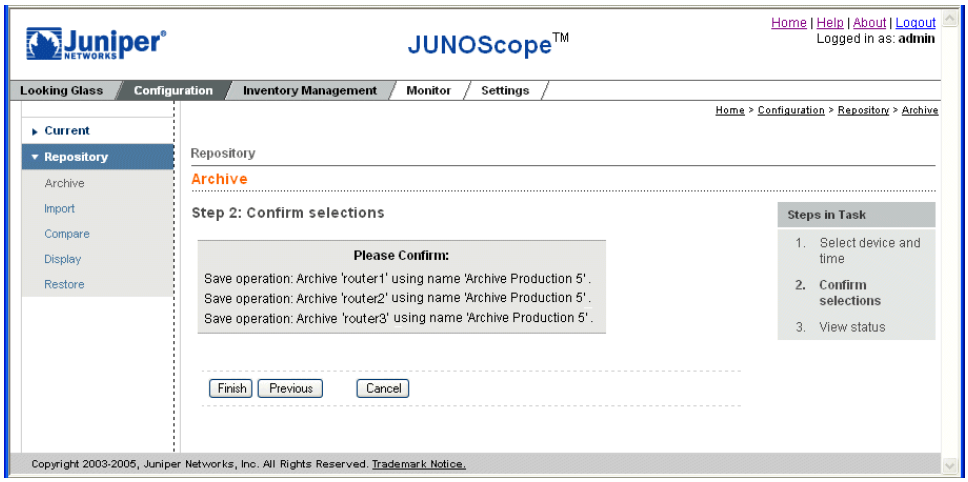
Archiving a Configuration File

To archive a configuration file, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Archive. The Archive—Select device and time dialog box appears.



2. Select the Group or Select Device(s) option button.
3. Select the group or devices that you want from the Group or Select Device(s) drop-down list box. Shift + click to select multiple devices from the Select Device(s) drop-down list box.
4. In the Comment text box, type an optional descriptive comment about the archive that you want to perform.
5. Select when you want the archive to occur by clicking the appropriate option button:
   - Now—(Default) Performs an archive immediately after you confirm it.
   - Select Schedule—Performs an archive at the scheduled time interval.
   - Select to save the archive operation to run at a later time. Click Save Operation as, then type an operation name in the text box.
6. Click Next. The Archive—Confirm selections dialog box appears. If you have selected a BXOS device or a group that contains BXOS devices, go to step 7, else go to step 8.



7. If you have selected a BXOS device or a group that contains BXOS devices, choose one of the following options from the Confirm Selections dialog box.

NOTE: BXOS configuration is archived in xml format.

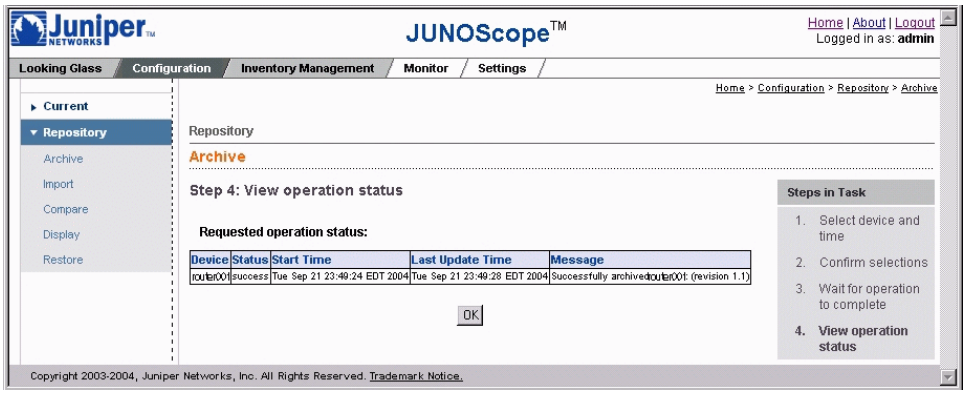
- Archive Startup Configuration—Choose this option if you want to archive the startup configuration on the BXOS device. By default, JUNOScope archives the startup configuration for BXOS devices.
- Archive Running Configuration—Choose this option if you want to archive the running configuration on the BXOS device.

NOTE: If you choose to archive a running configuration that is the same as the startup configuration archived on the JUNOScope server or vice versa, JUNOScope does not create a new version of the archived configuration when there is no difference between the archived configuration and the one submitted for archiving. The Comment field for the archived configuration indicates whether the archived configuration is a running configuration or startup configuration.

---

8. Confirm that the archive options that you selected are correct.
9. Click Finish to confirm the archive.
   - If you selected Now in Step 5, archiving occurs immediately and the Archive—Wait for operation to complete dialog box appears.
   - If you selected to save the archive operation, you return to the Configuration > Repository menu. To view the saved operation, click Settings > Saved Operations.
   - If you selected a schedule, archiving occurs when the operation is scheduled to be run.

     When the archive process is complete, the Archive—View operation status dialog box appears.



The Archive—View operation status dialog box lists the archive operation by device name, status, start time, last update time, and status message. The Archive operation status can be successful, failed, writing, pending, connecting, or working.

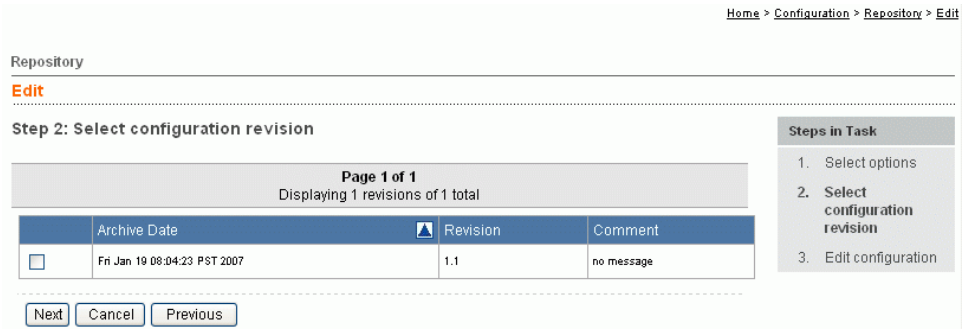
10. Click OK.

Editing Archived Configurations

To edit an archived configuration file, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Edit. The Select Options dialog box appears.

2. Select a configuration file from the Configuration File drop-down list box.
3. Select the corresponding device from the Device drop-down list box.
4. Click Next. The Select Configuration Revision dialog box appears.



5. Select the configuration revision you want to edit by selecting the check box in the corresponding row, then click Next. The Configuration Revision dialog box appears.

6. Edit the configuration, then click Save. The Save Result dialog box appears displaying whether the configuration file has been modified.

7. Click OK. The modified configuration file is added into the CVS repository as a new revision.

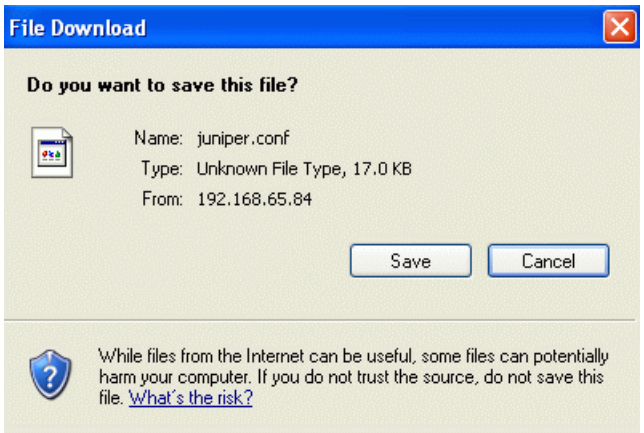
Saving Archived Configurations

To save an archived configuration file to a local machine, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Save. The Select Options dialog box appears.

2. Select a configuration file from the Configuration File drop-down list box.
3. Select the corresponding device from the Device drop-down list box.
4. Click Next. The Select Configuration Revision dialog box appears.

5. Select the configuration revision you want to save by selecting the check box in the corresponding row, then click Next. The File Download dialog box appears listing the archived configuration file, the file type, and the IP address of the router from which you are downloading the configuration file. Click Previous to go back to the Select Options dialog box.



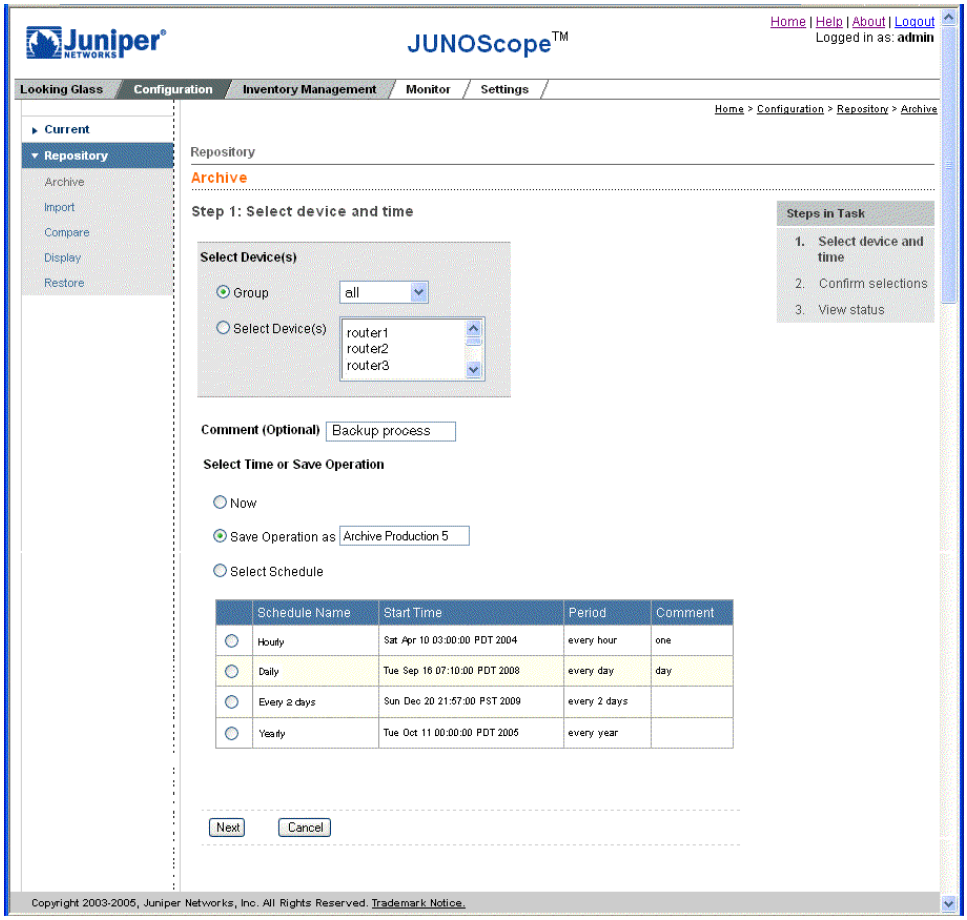
6. Click Save to save the configuration file to the local machine.

Saving an Archive Operation

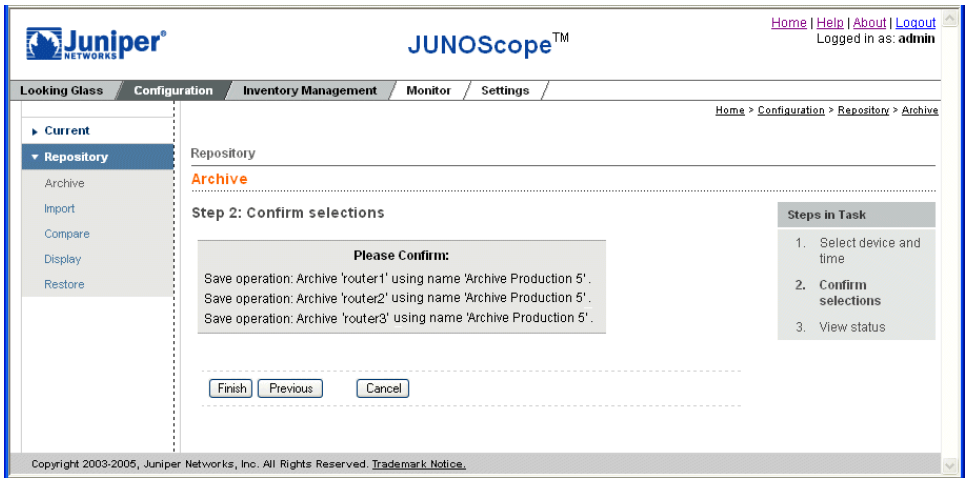
You can save an archive operation and combine it with other operations to run them concurrently or in sequence on specific devices.

To save an archive operation, follow these steps:

1. From the JUNOScope main window, click Configuration > Repository > Archive. The Archive—Select Device and Time dialog box appears.



2. Select the group or device(s) that you want to archive.
3. Type an optional comment about the archive operation.
4. Click the Save Operation as option button and type a name for the archive operation in the text box.
5. Click Next. The Archive Confirm Selections dialog box appears.



6. Confirm that the selections for the archive operation you want to save are correct.
7. Click Finish. The Configuration > Repository menu appears.

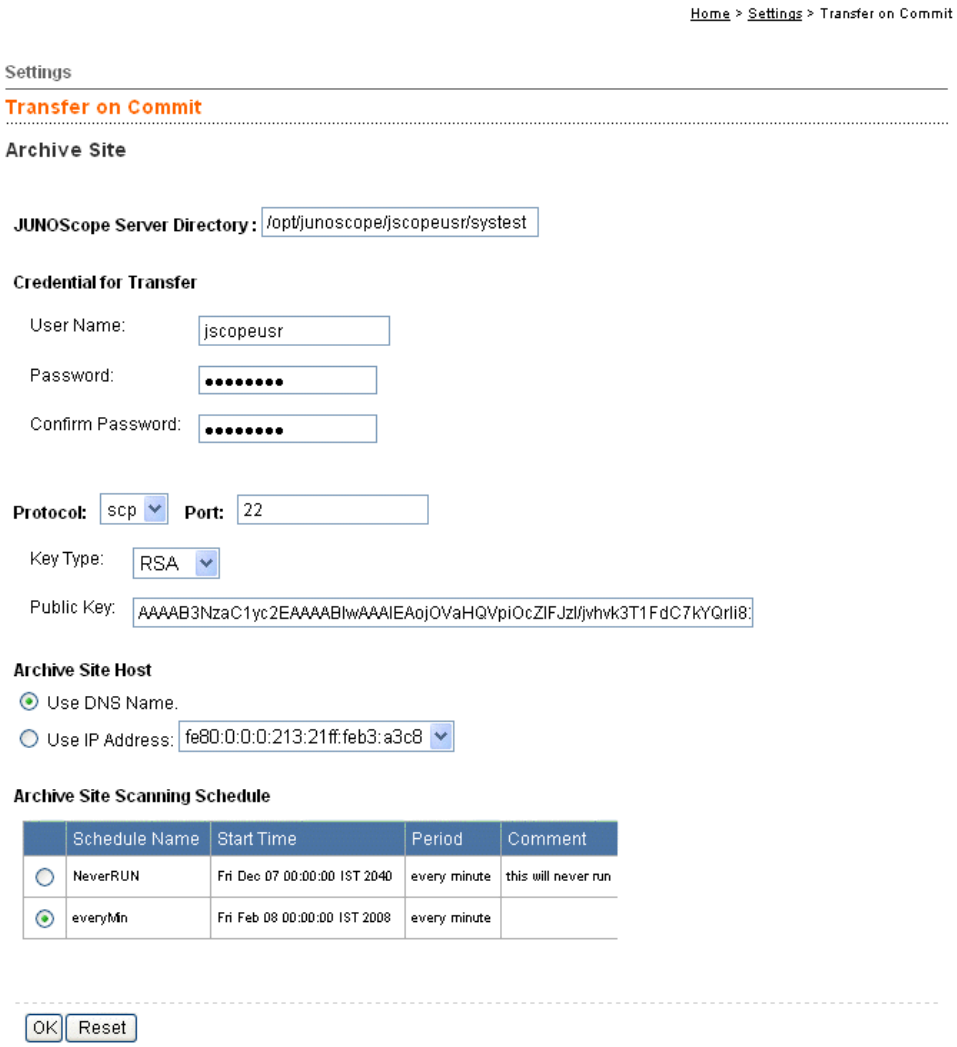
   To view the saved archive operation, click Settings > Saved Operations. To work with saved operations, see "Using Task Manager (Saved Operations)" on page 167.

Configuring the JUNOScope Server for Transfer on Commit

You can configure a JUNOS device to transfer its device configuration to the JUNOScope server when a commit operation succeeds. This feature ensures that the running configuration on the device is always archived in JUNOScope. You should configure the JUNOScope server for transfer-on-commit before configuring transfer-on-commit on devices. You must have superuser permissions to configure the JUNOScope server for transfer-on-commit.

To configure the JUNOScope server for transfer-on-commit, follow these steps:

1. In the JUNOScope main window, click Home > Settings > Transfer on Commit. The Archive Site dialog box appears.



2. Enter the directory to which the configuration will be transferred in the JUNOScope Server Directory text box.
3. Enter the credentials used by the device to connect to the server in the User Name and Password text boxes. This JUNOScope user and the JUNOScope administrator need read-write permission to the directory to which the configuration will be transferred.
4. Select the protocol used for connecting to the server from the Protocol drop-down list box. You can choose the scp or ftp protocol. To use the scp protocol, the ssh daemon must be running on the JUNOScope server.

5. Select the default ports for the protocol selected or enter a port to use for connecting to the server in the Port text box. The default ports are port 21 for ftp and port 22 for scp.
6. Select the key type and public key details required for connecting using the scp protocol.
7. Select whether to use the DNS name or IP address to connect to the JUNOScope server.
8. Schedule the archive site scanning operation.
9. Click OK to configure the archive site. Click Reset to discard your changes.

Configuring Devices to Transfer Committed Configurations

You can configure a JUNOS device to transfer its device configuration to the JUNOScope server when a commit operation succeeds. This feature ensures that the running configuration on the device is always archived in JUNOScope. You can enable or disable transfer-on-commit on selected devices after configuring the JUNOScope server for transfer-on-commit. You can also select a transferred configuration that could not be matched to any of the devices managed in JUNOScope, view the configuration file, select a device, and archive the unmatched transferred configuration into its device archive.

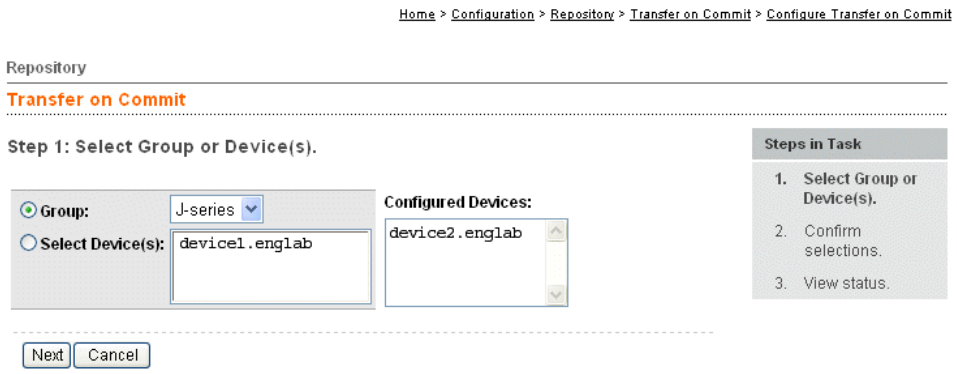
This section contains

Configuring Transfer on Commit

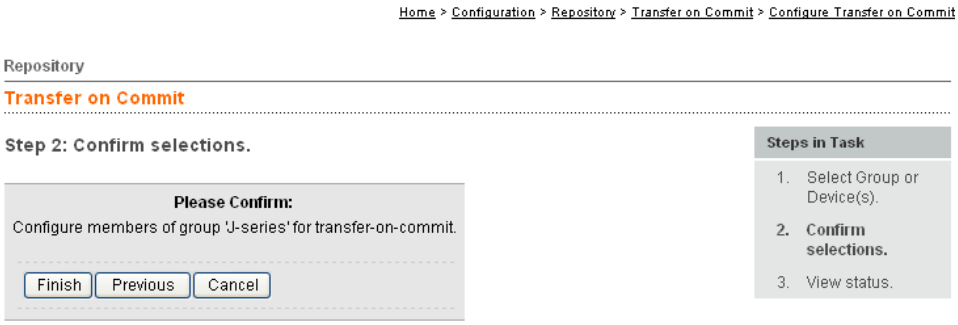
You can enable transfer-on-commit on selected devices. Configure your JUNOScope server for transfer-on-commit before enabling transfer-on commit on devices. You must have superuser or read-write permission to enable transfer-on-commit.

To configure transfer on commit on selected devices, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Transfer on Commit > Configure Transfer on Commit. The Select Group or Device(s) dialog box appears.



2. Select the group or device(s) on which you want to configure transfer-on-commit.
3. Click Next. The Confirm Selections dialog box appears.



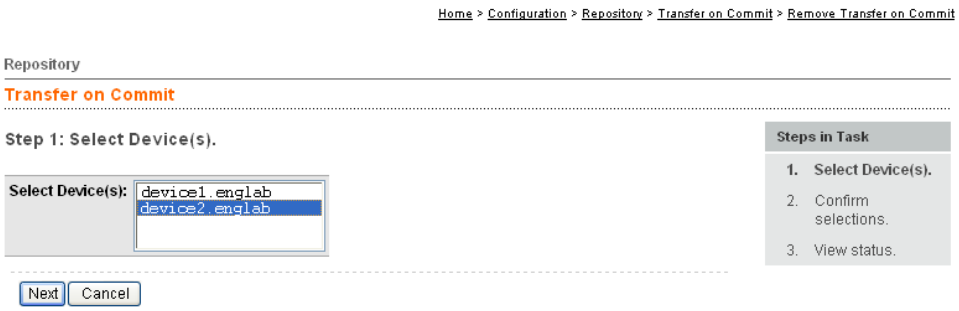
4. Confirm that the selections for performing the transfer-on-commit operation are correct and click Finish. The View Status Records dialog box shows the status of the transfer-on-commit operation.

Removing Transfer on Commit

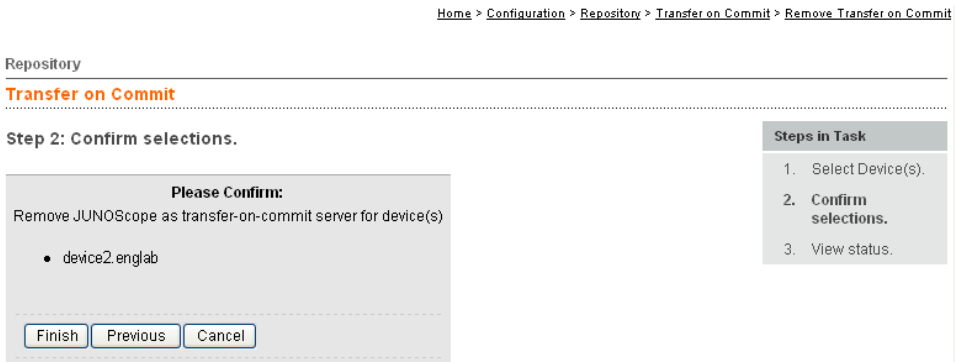
You can disable transfer-on-commit on selected devices. You must have superuser or read-write permission to disable transfer-on-commit.

To remove Transfer on Commit from selected devices, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Transfer on Commit > Remove Transfer on Commit. The Select Device(s) dialog box appears.



2. Select the device or devices on which you want to remove transfer-on-commit.
3. Click Next. The Confirm Selections dialog box appears.



4. Confirm that the selections for removing transfer-on-commit are correct and click Finish. The View Status Records dialog box shows the status of the transfer-on-commit operation.

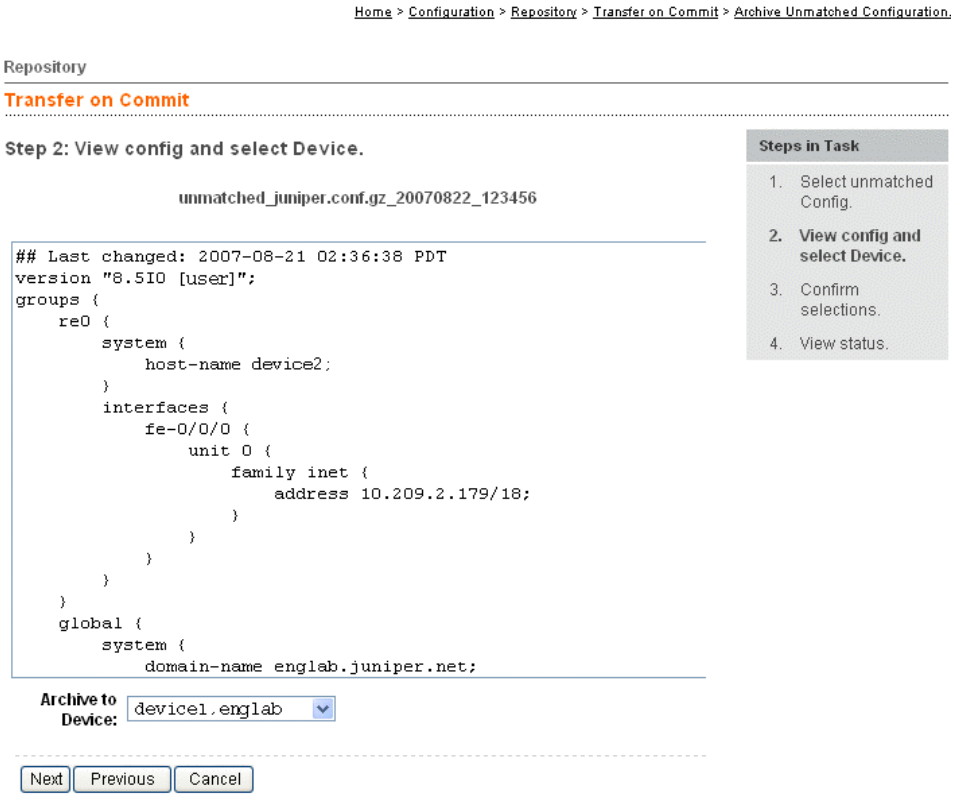
Archiving an Unmatched Configuration

JUNOScope associates a transferred configuration to a device based on the file name of the transferred configuration. If JUNOScope is not able to match the file name of the transferred configuration to any device, the configuration will be stored in the archive as an unmatched configuration. You can select a transferred configuration that could not be matched to any of the devices managed in JUNOScope, view the configuration file, select a device, and archive the unmatched transferred configuration into its device archive. You must have superuser or read-write permission to archive unmatched configurations.

To archive unmatched configurations, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Transfer on Commit > Archive Unmatched Configuration. The Select Unmatched Config dialog box appears.

2. Select the configuration you want to match from the Select Config drop-down list box and click Next. The View Config and Select Device dialog box appears.



3. Select the device to which you want to archive the unmatched configuration from the Archive to Device drop-down list box.

4. Click Next. The Confirm Selections dialog box appears.

5. Confirm that the selections for archiving unmatched configurations are correct and click Finish. The View Status dialog box shows the status of the archive operation.

Chapter 18

Setting Up Archived Configuration Tags and Auditing Configurations and Partial Configurations

This chapter describes how to set up a unique tag and associate the tag with archived device configuration revisions of one or more devices. It also describes how to check for differences between configuration revisions of selected devices or a group of devices, provided the device configuration exists in the repository. It also describes how to check for differences between a part of the running configuration file and a baseline partial configuration.

This chapter includes the following topics:

You must have superuser or read-write permission to set up and audit archived configuration tags.

Archiving Tags

This section describes how to add, edit, copy, delete, and associate tags with archived device configuration revisions of one or more devices. A tag serves as a unique identifier that you can use to label a particular revision of a device configuration file in the CVS repository. You can tag any CVS entry with a free text string (for example, golden, master, or template). The same tag can be associated with multiple device configurations, but not with multiple configuration revisions of the same device. If a tag already associated with a configuration revision of a device is added to another configuration revision of the same device, the tag will automatically be removed from the previous configuration revision.

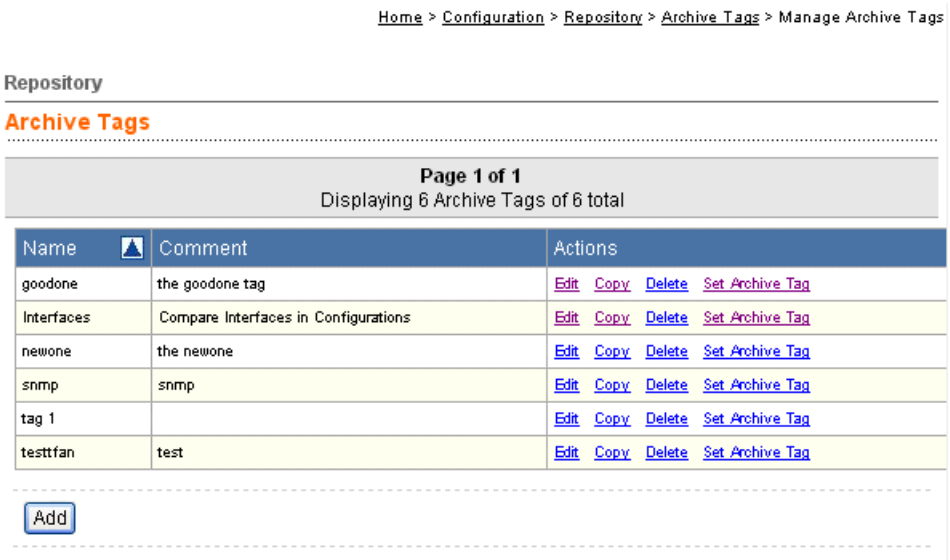
The JUNOScope administrator can select a device, view all configuration revisions for the selected device in the repository, then assign a tag to one of the configuration revisions of the selected device. The administrator can also select multiple devices and assign a tag to a configuration revision of each selected devices iteratively. Alternatively, the administrator can assign a tag to the Head Revision (latest revision) in the repository for all the selected devices. The administrator can compare any two configuration revisions of a device to determine which configuration revision to tag.

Adding an Archived Configuration Tag

The JUNOScope administrator can add unique text tags to label specific device configurations that have been archived in the JUNOScope CVS repository.

To add an archived configuration tag, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Archive Tags. The Archive Tags dialog box appears.



   Tags are listed in the Archive Configuration dialog box in alphabetical order by Name, Comment, and Actions. See Table 15 on page 212 for a description of the information. If you have not created any configuration archive tags, the dialog box will be empty.

2. Click Add. The Add Archive Tag dialog box appears.

3. In the Name text box, type a unique archive tag name.

   Follow these rules when adding an archive tag name or you will not be able to associate the tag with a device configuration:

   - Tag name length must be no more than 40 characters.
   - The first character of a tag name must be a letter.
   - The rest of the tag name characters can be alphanumeric characters.
   - The tag name can include a hyphen (-) or an underscore (_). Do not include a period (.).

     The archive tag names Head Revision and Running are reserved tag names that can be used for both source or target configuration files for comparison and auditing.

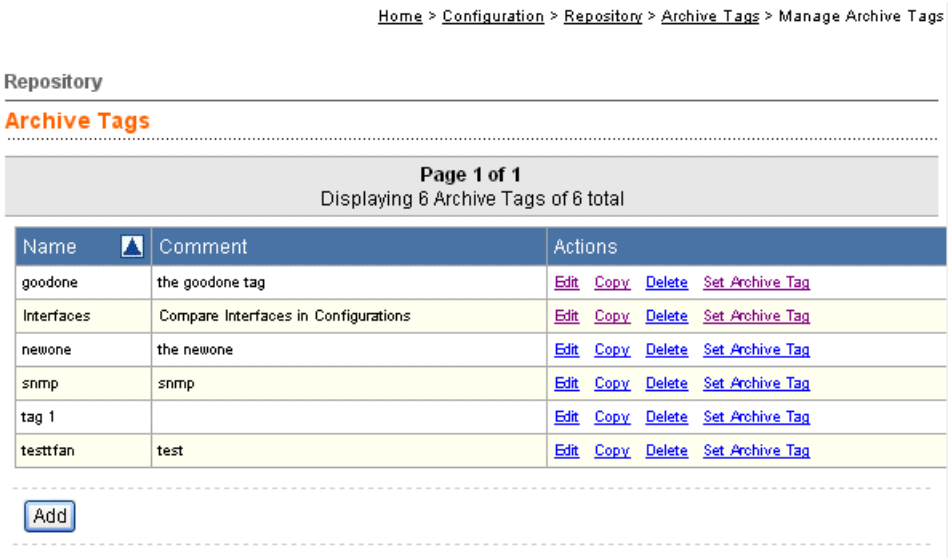
4. In the Comment text box, type an optional comment for the tag name.
5. Click OK. The new tag appears in the Archive Configuration dialog box.

Viewing Archived Configuration Tags

Use the Archive Configuration dialog box to set up and maintain configuration tag names. You can add, edit, copy, and delete tags. You can associate a tag with archived device configuration revisions of one or more devices and also untag archived device configuration revisions.

To view all archived configurations, follow this step:

1. In the JUNOScope main window, click Configuration > Repository > Archive Tags. The Archive Tags dialog box appears.



Tags are listed in the Archive Configuration dialog box in alphabetical order by Name, Comment, and Actions. See Table 15 on page 212 for a description of the information. If you have not created any configuration archive tags, the dialog box will be empty.

Table 15: Archive Configuration Dialog Box Labels

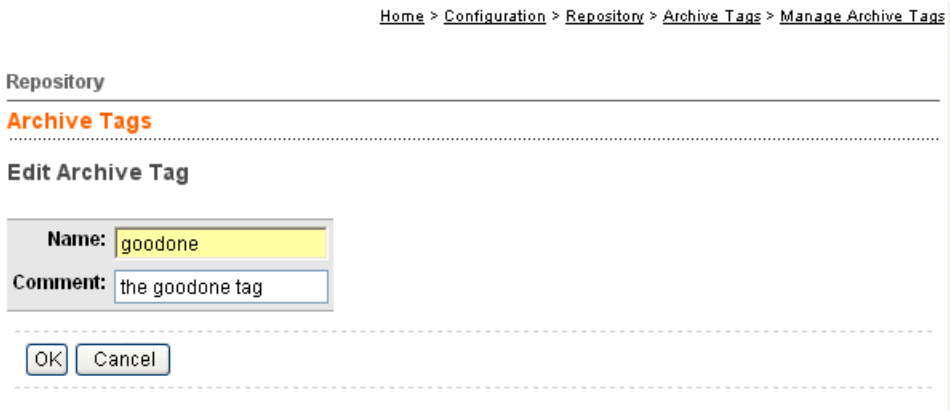
Column Name	Description
Name	Name of the archived configuration tag.
Comment	Comment entered while creating the archived configuration tag.
Actions	Actions that can be performed on an archived configuration tag. The possible actions are: ■ Edit—Edit or rename the selected tag. ■ Copy—Create a copy of the selected tag, including all associated device configurations. ■ Delete—Delete the selected tag. ■ Set Archive Tag—Associate the selected tag to a device or devices.

Editing Archived Configuration Tags

The JUNOScope administrator can edit an archived configuration tag name and comment.

To edit a tag name and comment, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Archive Tags. The Archive Tags dialog box appears.
2. Click the Edit action link for the tag that you want to edit. The Edit Archive Tags dialog box appears.



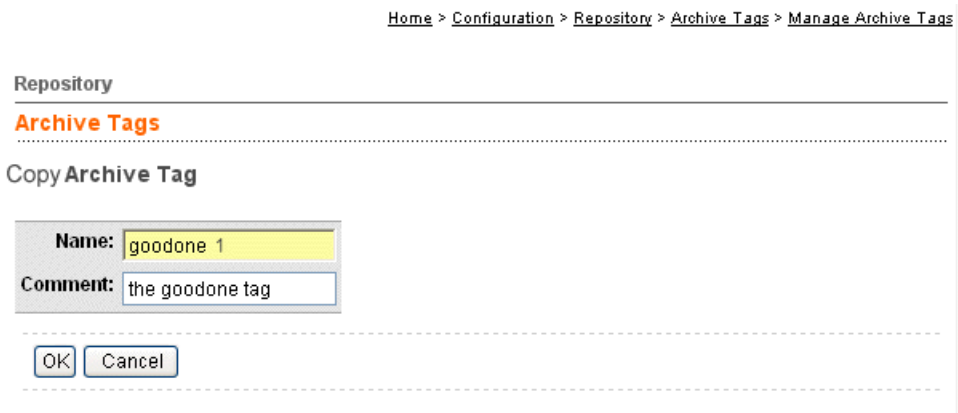
3. Modify the tag name and comment.
4. Click OK. The modified tag information appears in the Archive Tags dialog box.

Copying Archived Configuration Tags

You can copy the archive configuration tag name and comment.

To copy a tag name and comment, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Archive Tags. The Archive Tags dialog box appears.
2. Click the Copy action link for the tag that you want to copy. The Copy Archive Tags dialog box appears.



3. Modify the tag name or comment.
4. Click OK. The copied tag appears in the Archived Tags dialog box.

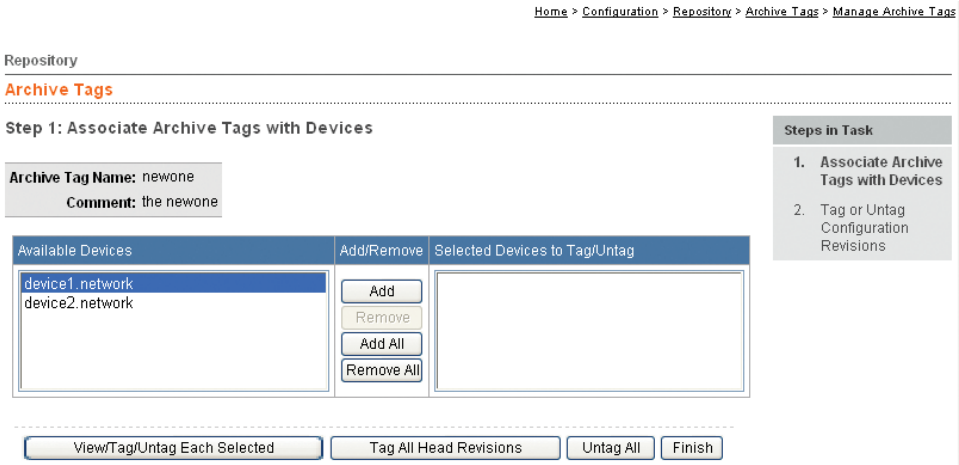
Associating Tags to Devices and Tagging Device Configuration Files

After a tag is created, the JUNOScope administrator must associate it with devices with archived configurations in the JUNOScope CVS repository. The administrator can select devices that have archived configurations to tag, view all the configurations of each selected device, then assign a tag or untag iteratively. The administrator can also assign a tag to the Head Revision (latest) in the repository for all devices selected.

NOTE: You cannot associate an archive tag to a device configuration unless the tag name meets the rules described in “Adding an Archived Configuration Tag” on page 210.

To associate and tag device configurations, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Archive Tags. The Archive Tags dialog box appears.
2. Click the Set Archive Tag action link for the tag that you want to associate with devices. The Associate Archive Tags with Devices dialog box appears.



3. Select a device or devices and move them into the Selected Devices to Tag/Untag list box using the buttons in the Add/Remove column.

4. Click one of the command buttons at the bottom of the dialog box to do the following:

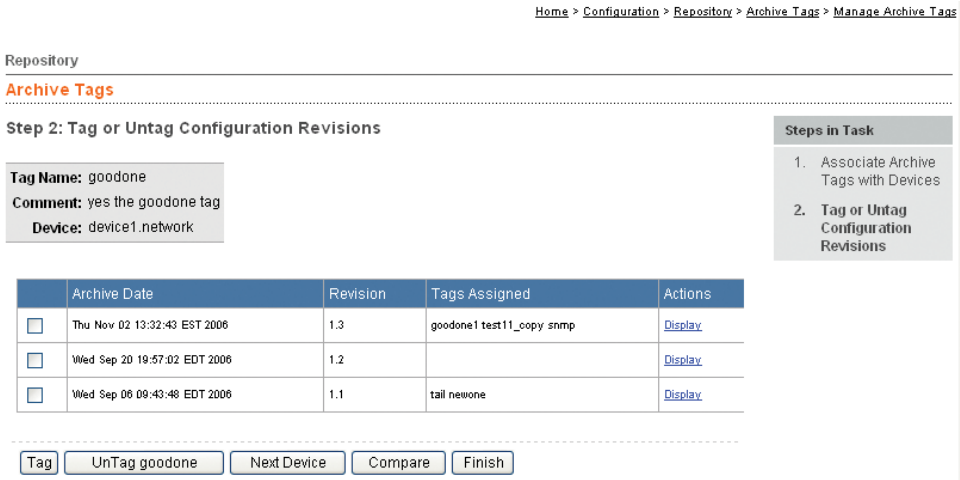
   - View/Tag/Untag Selected Devices—View all configuration revisions for each selected device in the Selected Devices to Tag/Untag list box, select a configuration revision and tag or untag configuration revisions for each device iteratively. Skip to step 5.

   - Tag All Head Revisions—Assign a tag to the head revision (latest) in the repository for all selected devices in the Selected Devices to Tag/Untag list box. If an existing tag is added to the head revision (latest) of a device, the tag is automatically removed from the old revision. If you click Tag All Head Revisions, the message Successfully tagged head revision of selected devices appears in the Associate Archive Tags with Devices dialog box after all the head revisions are tagged.

   - Untag All—Untag all the configuration revisions for all selected devices in the Selected Devices to Tag/Untag list box. If you click Untag All the message Successfully untagged selected devices appears after all the configuration revisions for the selected devices are untagged.

   - Finish—Save any changes made and return to the Archive Tags dialog box.

5. If you click View/Tag/Untag Selected Devices, the Tag or Untag configuration revisions dialog box appears.



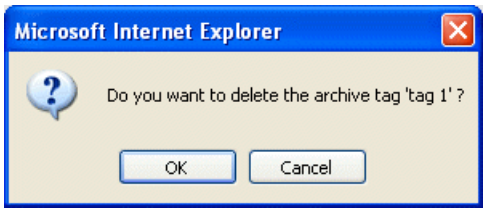
6. Select an archived configuration revision and click one of the command buttons at the bottom of the dialog box to do the following:
   - Tag—Apply the tag to the configuration revision selected.
   - UnTag Master—Remove the tag from the configuration revision selected if the tag has already been associated with the configuration revision.
   - Next Device—Display the Tag or Untag Configuration Revisions dialog box for the next device when you are tagging configuration revisions of multiple devices iteratively. You can tag configuration revisions of multiple devices iteratively using this command button.
   - Previous Device—Display the Tag or Untag Configuration Revisions dialog box for the previous device when you are tagging configuration revisions of multiple devices iteratively.
   - Compare—Compare two selected configuration revisions.
   - Finish—Save any changes made and return to the Associate Archive Tags with Devices dialog box.
7. Click Finish after you tag or untag configuration revisions to return to the Associate Archive Tags with Devices dialog box.

Deleting Archived Configuration Tags

The administrator can delete archived configuration tags that are no longer in use.

To delete an archived configuration tag, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Archive Tags. The Archive Tags dialog box appears.
2. Click the Delete action link for the tag that you want to associate. A confirmation dialog box appears.



3. Click OK. The tag is removed from the Archive Tags dialog box.

Auditing Configurations

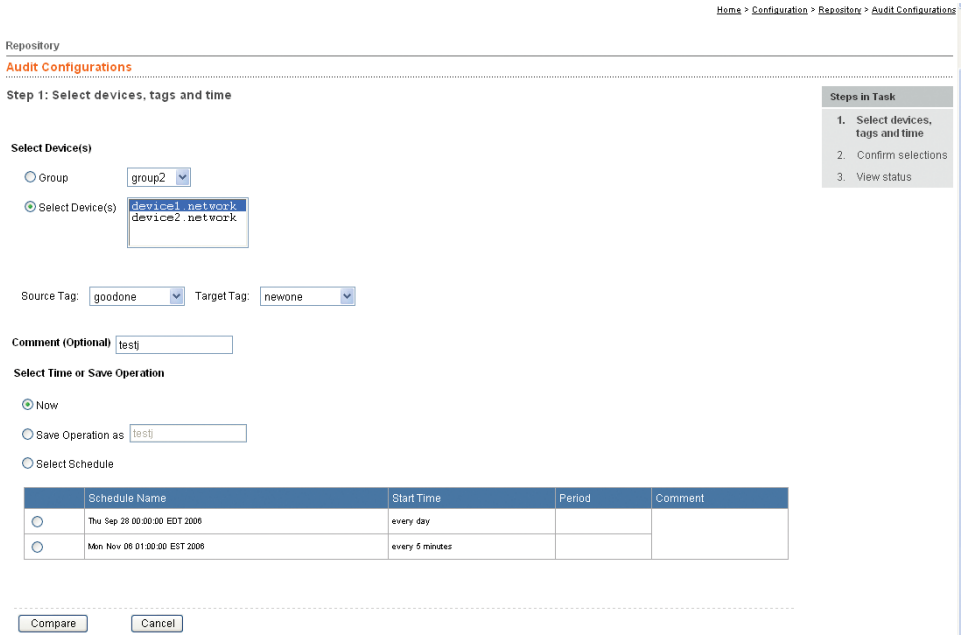
A JUNOScope administrator can perform configuration audits on one or more devices simultaneously, provided the device configuration exists in the repository. An administrator can maintain a master router configuration for each managed device and compare this record with the actual individual device configuration.

For any managed device, JUNOScope administrators can tag a configuration revision in its repository as a "master" (or any free-text description), then compare (or audit) it with another configuration revision. Comparisons can also be made with the “Running” and “Head Revision” configurations. "Running" is the current configuration which JUNOScope will obtain from the router. "Head Revision" is the most recent revision of a configuration file in the repository. If the "Running" option is selected, JUNOScope attempts to obtain the running configuration from the router, compare it with the latest revision in repository, and archive it as the "Head Revision" if they are different, before using it for comparison. If no difference is detected, the "Running " configuration is equivalent to the "Head Revision" configuration.

The source file and target files for audit are identified by different tag names. Once the audit configuration operation is complete the administrator can view any differences between the source and target configurations across all selected devices.

To audit configurations, follow these steps:

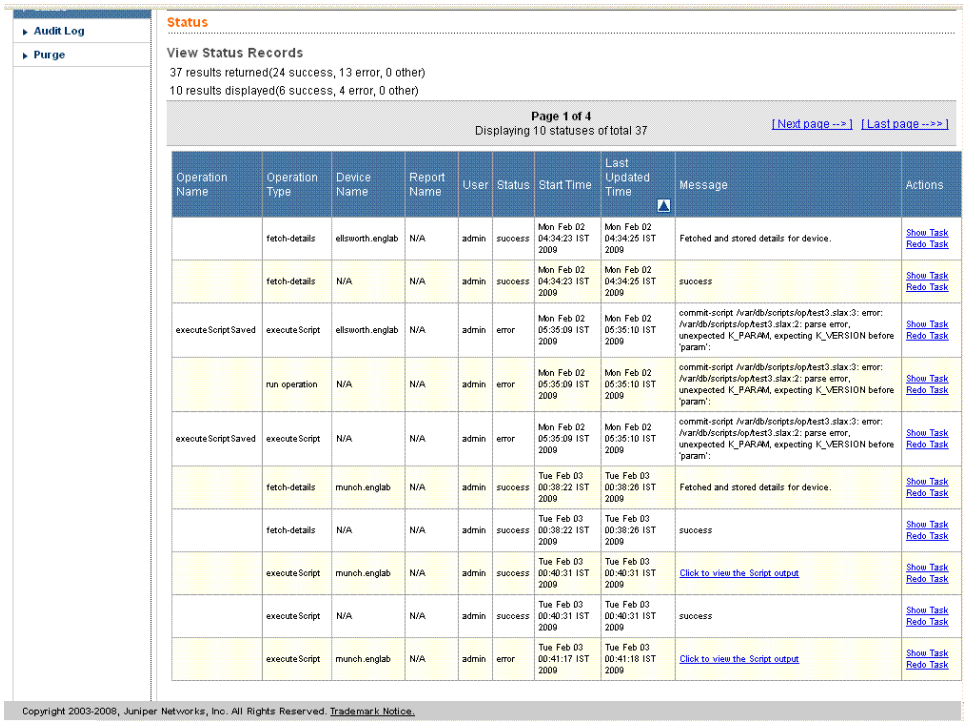
1. In the JUNOScope main window, click Configuration > Repository > Audit Configurations. The Select devices, tags, and time dialog box appears.



2. Select the Group or Select Device(s) option button.
3. Select the group or devices that you want from the Group or Select Device(s) list box. Shift + click to select multiple devices from the Select Device(s) drop-down list box.
4. Select the source tag and the target tag to be used for comparison, from the Source Tag and Target Tag list boxes.
5. In the Comment text box, type an optional descriptive comment about the audit that you want to perform.
6. Select when you want the audit to occur by clicking the appropriate option button:
   - Now—(Default) Performs an audit immediately after you confirm it.
   - Select Schedule—Performs an audit at the scheduled time interval.
   - Save Operation as—Select to save the audit operation to run at a later time. Click Save Operation as, then type an operation name in the text box.
7. Click Compare. The Confirm selections dialog box appears.

8. Confirm the selections you made are correct and click Finish to audit the configurations. Click Previous to return to the Select devices, tags and time dialog box and change your selection.

   - If you selected Now in Step 6, auditing occurs immediately and the View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

   - If you selected to save the archive operation, you return to the Configuration > Repository menu. To view the saved operation, click Settings > Saved Operations.

   - If you selected a schedule, archiving occurs when the operation is scheduled to be run.

The View Status Records dialog box lists the audit status by Operation name, Operation Type, Device Name, Report Name, User, Status, Start time, Last Updated Time and Message.

9. Click the Click to view differences link in the message column to compare the different configuration revisions.

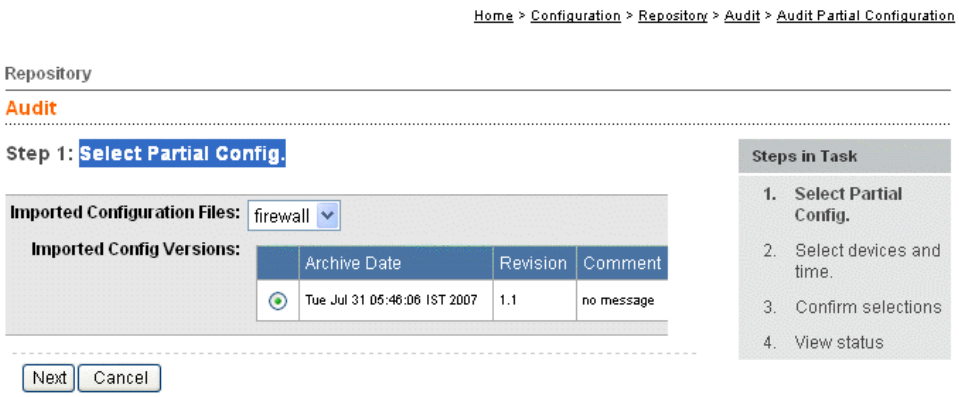
Auditing Partial Configurations

A JUNOScope user can audit a part of the configuration running on a router. A user can find differences between a part of the running configuration file and a baseline partial configuration.

NOTE: This feature is not supported on BXOS devices.

To audit partial configurations, follow these steps:

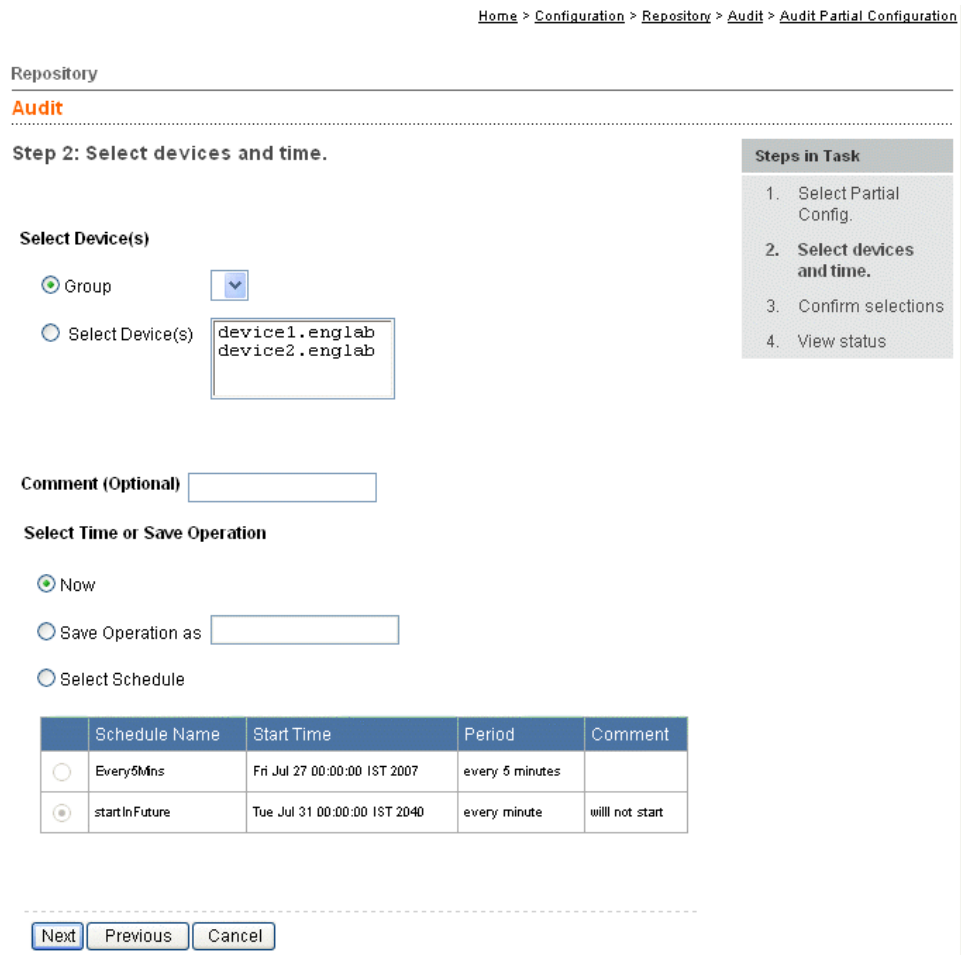
1. Click Configuration > Repository > Audit > Audit Partial Configurations. The Select Partial Configuration Dialog Box appears.



2. Select the imported configuration file (baseline partial configuration) that you want to compare with a running partial configuration from the Imported Configuration Files drop-down list box.

NOTE: The baseline partial configurations that are imported to the JUNOScope server must have their entire context.

3. Select the imported configuration file revision you want to compare with a running partial configuration by selecting the option button in the corresponding row in the Imported Config Versions table.
4. Click Next. The Select Devices and Time dialog box appears.



5. Select the Group or Select Device(s) option button.

NOTE: BXOS devices are not listed in the list of devices as auditing partial configuration is not supported on BXOS devices. However, you can choose a device group that contains BXOS devices among other devices. In such cases, JUNOScope carries out the partial configuration audit for devices other than the BXOS devices, and returns an Unsupported Operation message for the BXOS devices.

---

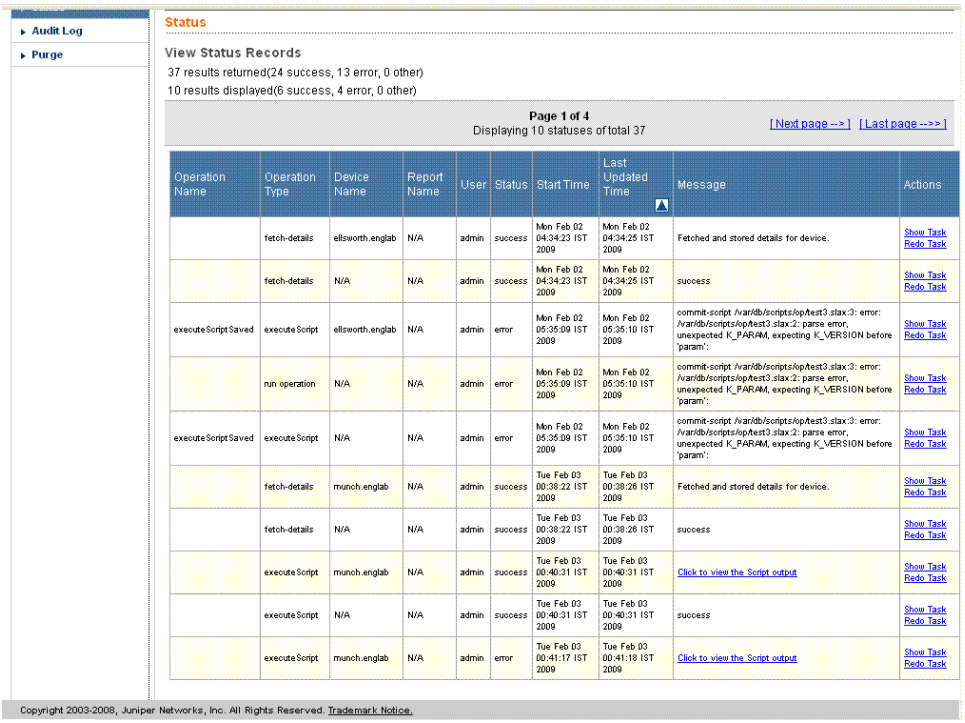
6. Select the group or devices that you want from the Group or Select Device(s) list box. Shift + click to select multiple devices from the Select Device(s) list.
7. In the Comment text box, type an optional descriptive comment about the audit that you want to perform.
8. Select the time you want the audit to occur by clicking the appropriate option button:
   - Now—(Default) Performs an audit immediately after you confirm it.
   - Save Operation as—Select to save the audit operation to run at a later time. Click Save Operation as, then type an operation name in the text box.

- Select Schedule—Performs an audit at the scheduled time interval. Click Select Schedule and select the option button for the schedule you want.

9. Click Next. The Confirm Selections dialog box appears.

10. Confirm that the selections you made are correct and click Finish to audit the configurations. Click Previous to return to the Select Devices and Time dialog box and change your selection.

- If you selected to perform the audit operation now, auditing occurs immediately and the View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:26 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

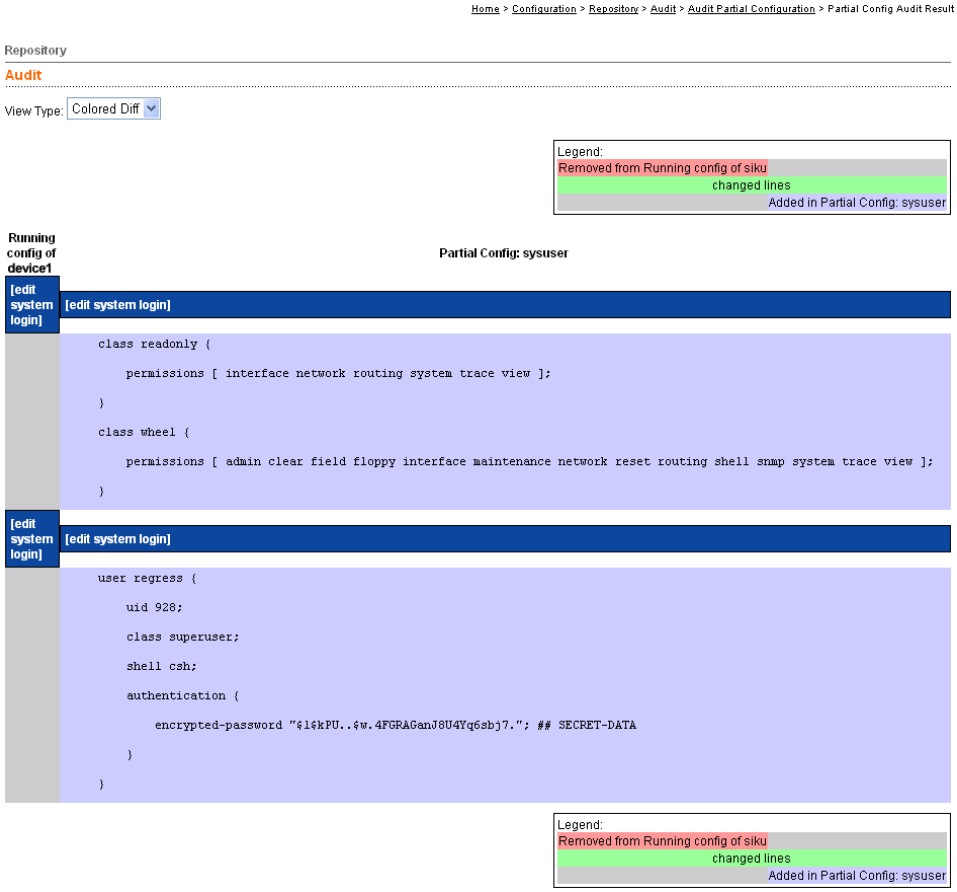
NOTE: If you have selected a device group that contains BXOS devices, JUNOScope displays an “Unsupported Operation” message for such devices.

- If you selected to save the audit operation, you return to the Configuration > Repository > Audit menu. To view the saved operation, click Settings > Saved Operations.
- If you selected a schedule, you return to the Configuration > Repository > Audit menu and auditing occurs when the operation is scheduled to be run.

11. Click the “Click to view the audit result” link in the Message column to view differences between a part of the running configuration file and a baseline partial configuration.
12. Select the compare output format—Colored Diff or Unidiff.

Colored Diff Compare Output Type

If you selected the Colored Diff compare output option to view differences between two configurations in color, the following compare output appears.

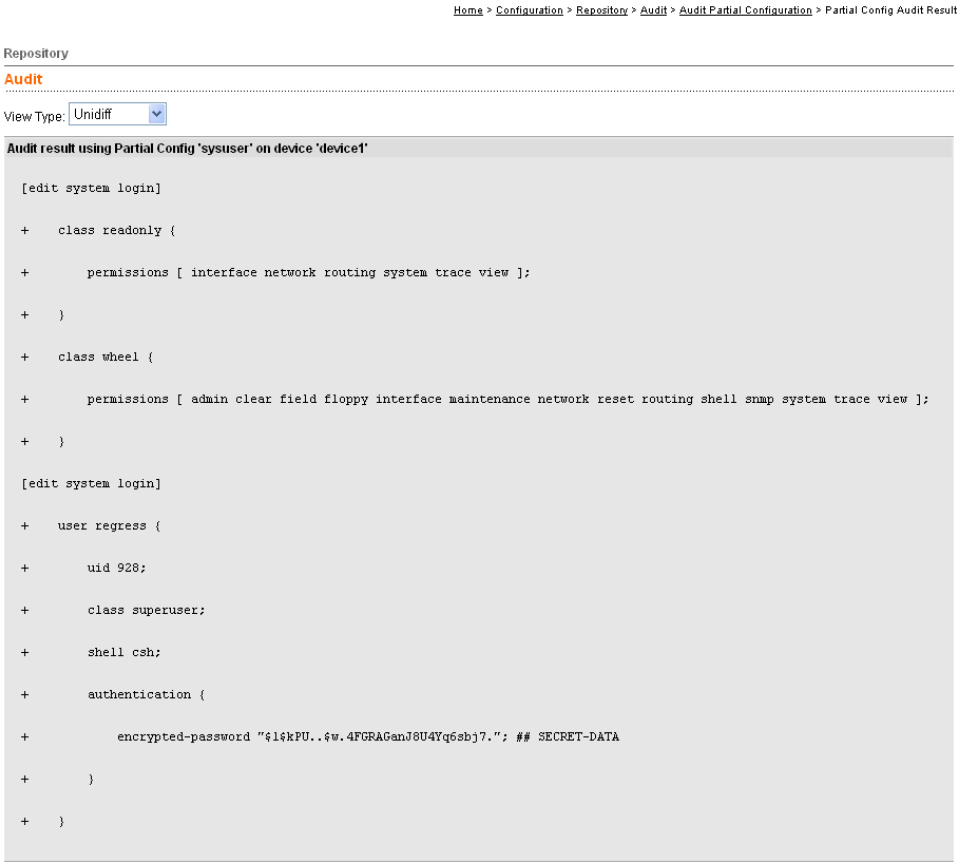


The Colored Diff highlights lines in the configuration file content that have been removed in the older version, or changed or added in the newer version.

You can change the compare output type by selecting Unidiff in the View Type drop-down list box.

UniDiff Compare Output Type

If you selected the Unidiff compare output option, the following compare output appears.



A minus sign (-) represents a difference in one revision of the configuration file; a plus sign (+) represents a difference in the other.

You can change the compare output type by selecting Colored Diff in the View Type drop-down list box.

Chapter 19

Comparing Configuration Files

This chapter describes how to compare the differences between two revisions of a configuration file stored in the JUNOScope Concurrent Versions System (CVS) repository. Configuration files are stored in CVS when you archive or import them from a router or a group of routers or when you import them from a text file on your local file system.

By default, the JUNOScope software compares the newer revision of a configuration file to the older revision. You can select to compare an older revision of a configuration file to a newer revision.

To compare configuration files, there must be at least two revisions of the files in the CVS repository. JUNOScope displays the differences of the configuration file revisions in color or by prefacing the changes with plus signs (+) or minus signs (-).

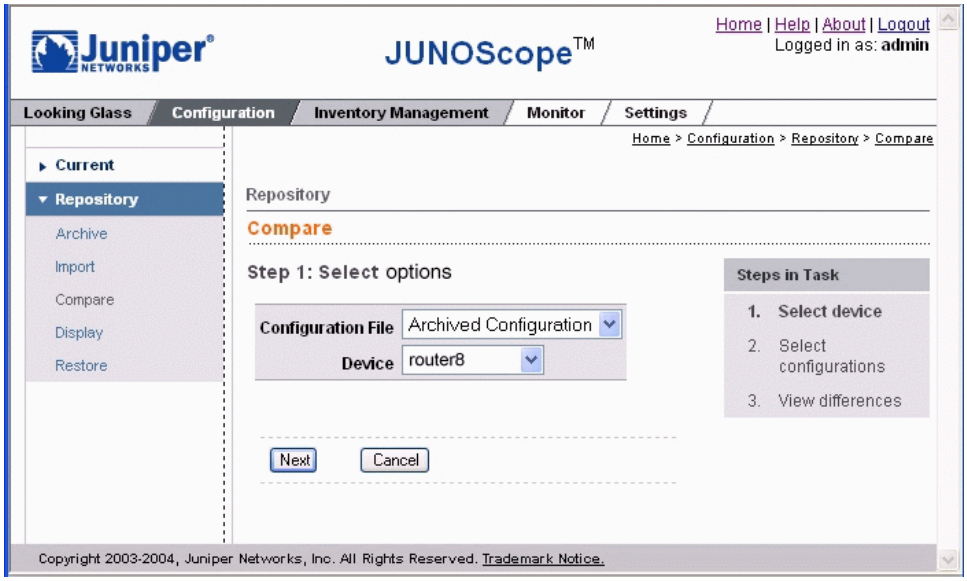
All JUNOScope users can compare configuration files.

■ Comparing Archives on page 225

Comparing Archives

To compare revisions of archived configuration files, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Compare. The Compare—Select Options dialog box appears.



2. Do one of the following:

   - To compare archived configurations, ensure that Archived Configuration is selected in the Configuration File drop-down list box, then go to Step 3.
   - To compare imported configuration files, select the filename of the file you want to load in the Configuration File drop-down list box, then skip to Step 4.

     The names of the imported configuration files are listed in the Configuration File drop-down list box. When you select an imported configuration file, the Device drop-down list box is disabled because the file is not associated with any device.

3. In the Device drop-down list box, select a device for which you want to compare two configuration files.

4. Click Next. The Compare—Select configurations dialog box appears with the available configuration files listed by the date on which they were stored in the CVS repository, and a revision level.

   Configuration file revisions are displayed in the Compare Archived Configurations dialog box when you have archived or imported a configuration file. There must be at least two configuration file revisions to compare. If no archived configuration revisions are displayed, you have not archived a configuration file yet.

   To archive a configuration file, see “Archiving and Manipulating Device Configurations” on page 193. To import a configuration file, see “Importing and Deleting Configuration Files” on page 229.

5. Select the check boxes for the two configuration file revisions to compare.

6. To compare the older file version to the new version, click the Swap revisions (Compare older revision to newer) check box.

By default, the JUNOScope software compares the newer revision of a configuration file to the older revision.

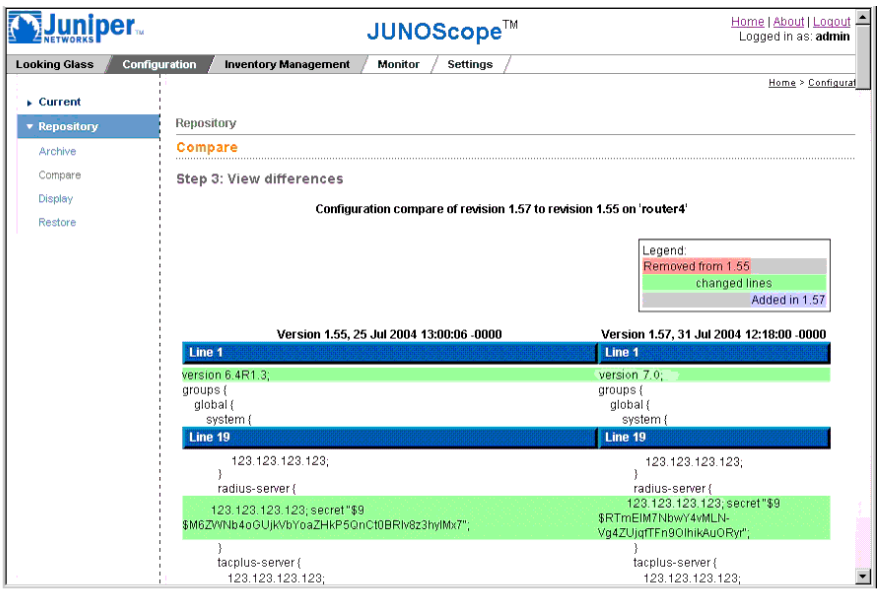
7. Select the compare output format—Colored Diff or Unidiff.

   For more information about Colored Diff, see “Colored Diff Compare Output Type” on page 227. For more information about Unidiff, see “Unidiff Output Compare Type” on page 228.

8. Click Finish. The configuration file difference(s) display in the View Differences dialog box.

Colored Diff Compare Output Type

If you selected the Colored Diff compare output option to view differences between two configurations in color, the following compare output appears.

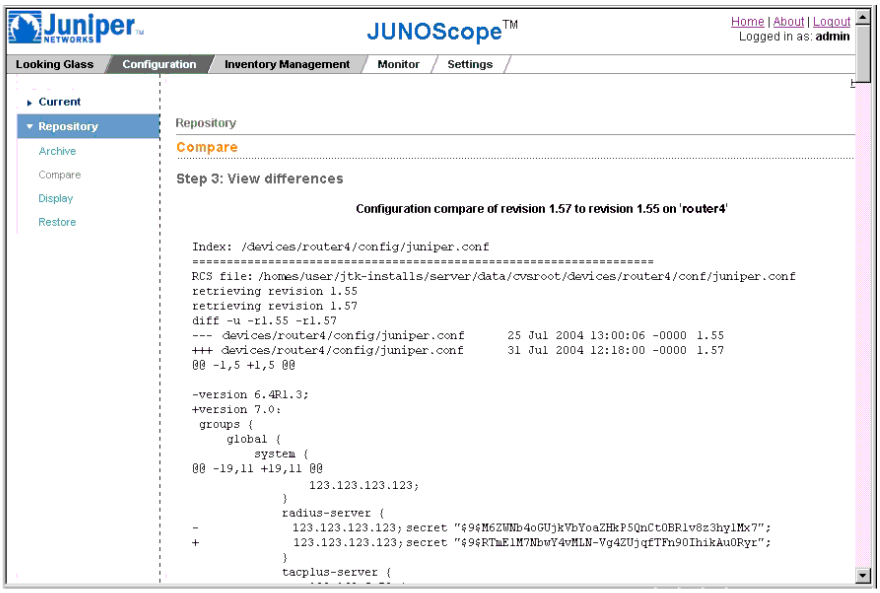


The Colored Diff highlights lines in the configuration file content that have been removed in the older version, or changed or added in the newer version.

You can change the compare output type by selecting Unidiff in the Compare Output Type drop-down list box.

Click OK to return to the Compare—Select Configurations dialog box.

Unidiff Output Compare Type



If you selected the Unidiff compare output option, the following compare output appears.

A minus sign (-) represents a difference in one revision of the configuration file; a plus sign (+) represents a difference in the other.

You can change the compare output type by selecting Colored Diff in the Compare Output Type drop-down list box.

Click OK to return to the Compare—Select Configurations dialog box.

Chapter 20

Importing and Deleting Configuration Files

This chapter describes how to import all or part of a configuration file into the JUNOScope software, where it is stored in the Concurrent Versions System (CVS) repository. Each time you import a configuration file with the same name, it is stored as a new version. This chapter also describes how to delete user-imported configuration files.

You can manually create a configuration file using a text editor. The configuration file contents must follow the configuration file guidelines described in the JUNOS software configuration guides. The configuration file can be in XML or text format.

You can modify a configuration file, then import it again.

You must have superuser or read-write permission to import or delete a configuration file and deploy a configuration to multiple devices.

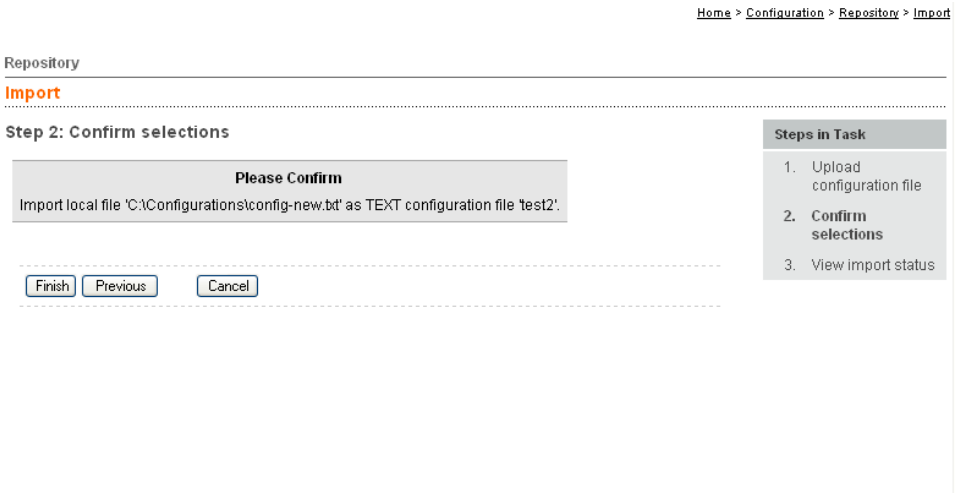
This chapter includes the following topics:

Importing a Configuration File

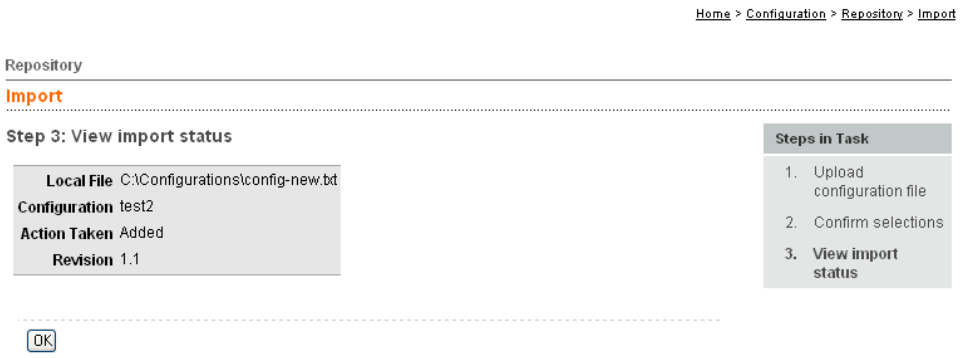
To import a configuration file, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Import. The Import—Upload configuration dialog box appears.

2. In the Local File text box, click Browse to navigate to the file on your file system that you want to import. You can import configuration files in ASCII text format or XML format.
3. In the Name in Repository text box, type the name that you want the file to have in the CVS repository.
4. Type an optional comment to identify the version of the imported configuration file.
5. Click Next. The Import—Confirmation Selections dialog box appears showing the file name, file type, and the comment that you specified.



6. Click Finish. The Import—View Import Status dialog box appears indicating that the configuration text file was imported into the JUNOScope software, versioned, then stored in the CVS repository.

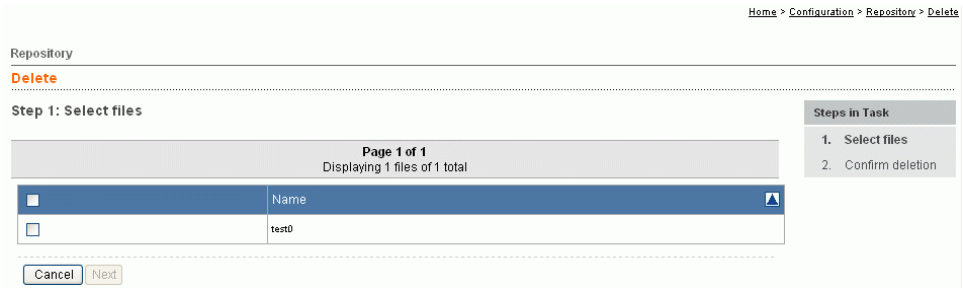


7. Click OK.

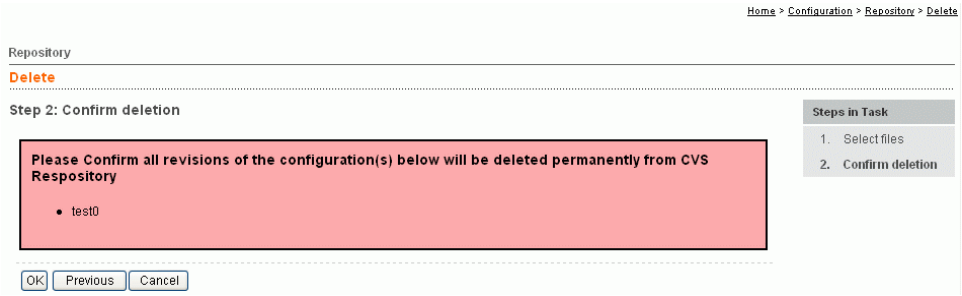
Deleting an Imported Configuration File

To delete an imported configuration file, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Delete. The Select Files dialog box appears.



2. Select the configuration file you want to delete by selecting the check box in the corresponding row.
3. Click Next. The Confirm Deletion dialog box appears.



4. Confirm the selections you made are correct, and click OK to delete the imported configuration file. Click Previous to go back to the Select Files dialog box without deleting the file.

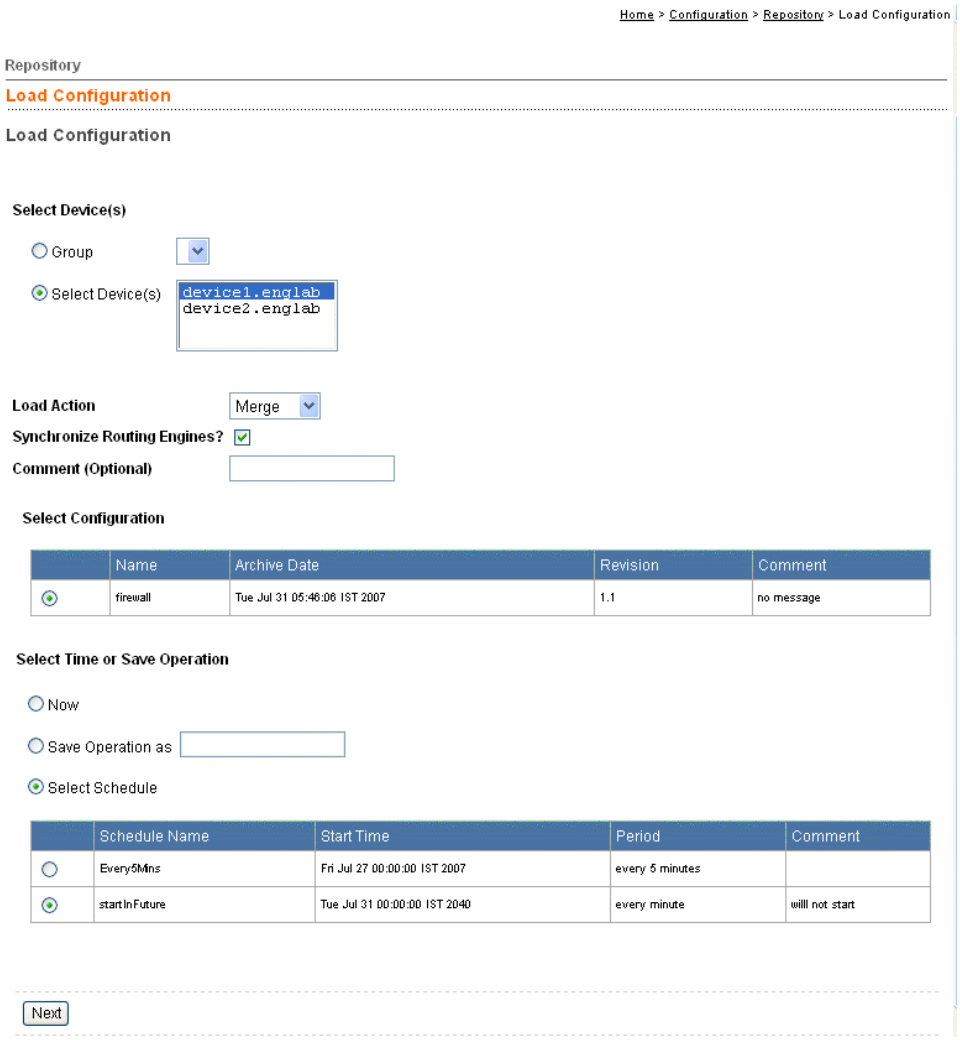
Loading Imported Configurations to Multiple Devices

You can deploy an imported configuration file to multiple routers and perform a simultaneous update of configurations on these devices.

NOTE: The Restore operation allows a JUNOScope user to restore an archived configuration file from the Concurrent Versions System (CVS) repository to the same router from which it was archived or load an imported configuration file to any router using the Restore operation. However the Restore operation supports only one device at a time unlike the Load Configuration feature.

To load an imported configuration to multiple routers, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Load Configuration. The Load Configuration dialog box appears.



2. Select the Group or Select Device(s) option button.
3. Select the group or devices that you want from the Group or Select Device(s) drop-down list box. Shift + click to select multiple devices from the Select Device(s) list.
4. Select whether you want to override, replace, or merge the current configuration on the devices.
   - Override—Discards the entire current configuration and loads the selected configuration.
   - Replace—Deletes a portion of the current configuration statement(s) and adds the selected configuration.

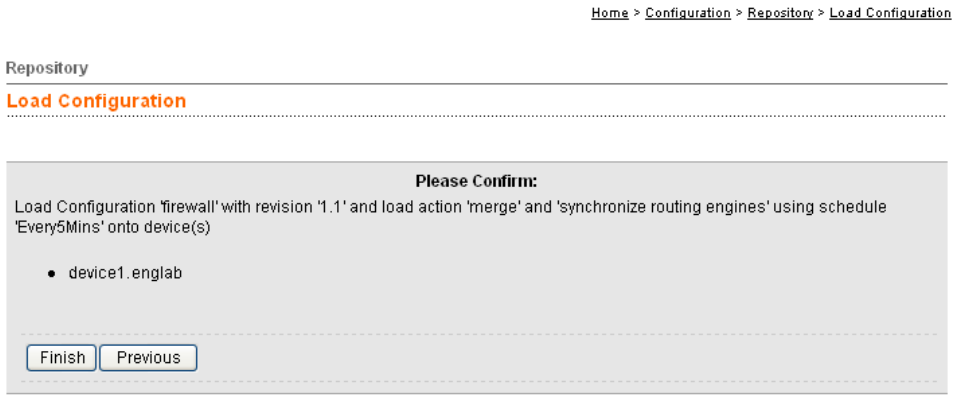
- Merge—(Default) Combines the selected configuration with the current configuration. If there are conflicting statements, the statements in the incoming configuration override those in the current configuration.

5. If the selected device is a JUNOS device that has two Routing Engines installed, click the Synchronize Routing Engines check box. This option, if checked, loads the configuration on both Routing Engines. .
6. In the Comment text box, type an optional descriptive comment about the bulk configuration update operation you want to perform.
7. Select the imported configuration file or partial configuration you want to load by selecting the check box in the corresponding row.

NOTE: If you have selected a BXOS device for loading the configuration, ensure that the configuration you want to load is in well-formed xml format. If the file is not in xml format or is structurally invalid, the load operation fails and returns an "unsupported operation" error.

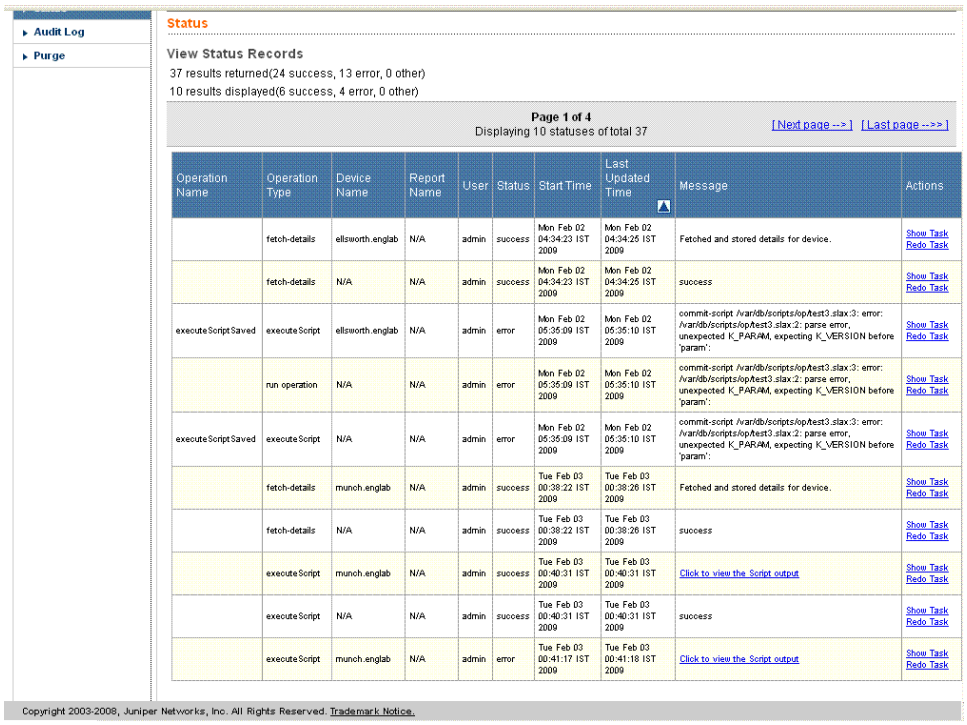
---

8. Select when you want to load the imported configuration file or partial configuration to the devices by clicking the appropriate option button:
   - Now—(Default) Loads the configuration immediately after you confirm it.
   - Select Schedule—Loads the configuration at the scheduled time interval. Click Select Schedule and select the option button for the schedule you want.
   - Save Operation as—Saves the load configuration operation to run at a later time. Click Save Operation as, then type an operation name in the text box.
9. Click Next. The Confirm Load Configuration dialog box appears.



10. If the selected device is a BXOS device, the Sync the Startup Configuration with Running check box is displayed. This option, when checked, synchronizes the running configuration with the startup configuration. If this option is not selected, only the running configuration is updated after the load operation. This option is displayed only when you have selected a BXOS device for loading configuration.
11. Click Finish to load the configuration to the devices. Click Previous to return to the Load Configuration dialog box.

- If you selected to upload the configuration now, then the View Status Records page shows the progress of the operation



Audit Log
Purge

Status

View Status Records

37 results returned(24 success, 13 error, 0 other)
10 results displayed(6 success, 4 error, 0 other)

Page 1 of 4
Displaying 10 statuses of total 37
[Next page -->] [Last page -->]

Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

Copyright 2003-2008, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.

- If you selected to save the upload configuration operation, you return to the Configuration > Repository > Load Configuration menu. To view the saved operation, click Settings > Saved Operations.

- If you selected a schedule, uploading occurs when the operation is scheduled to be run.

Chapter 21

Displaying a Configuration File

This chapter describes how to display the contents of a configuration file that has been stored in the JUNOScope Concurrent Versions System (CVS) repository. Configuration files are stored in CVS when you archive them from a router or a group of routers or when you import them from a text file on your local file system.

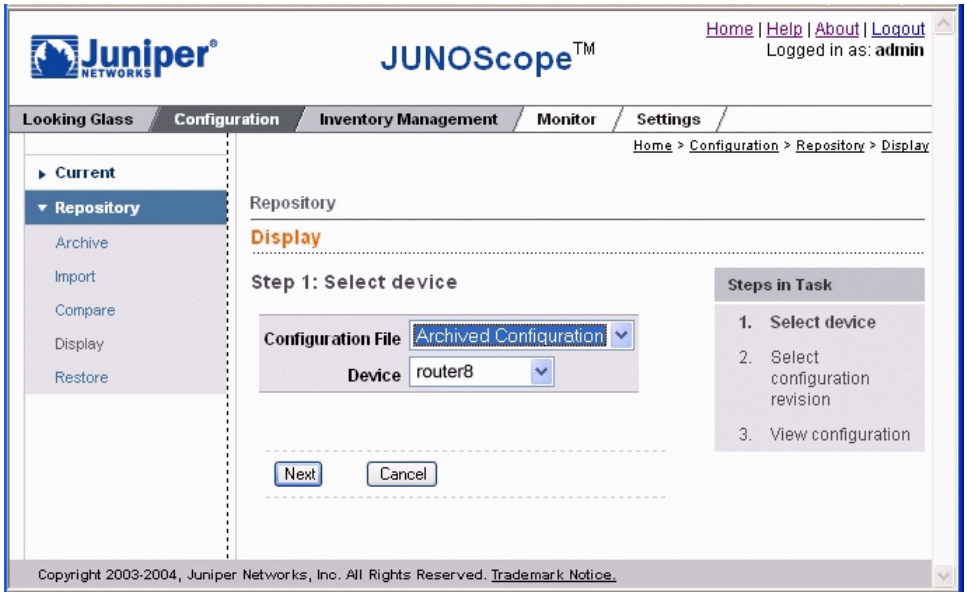
To display configuration file contents, you must have archived or imported at least one configuration. All JUNOScope users can display configuration files.

■ Displaying a Configuration on page 237

Displaying a Configuration

To display the contents of a configuration file, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Display. The Display—Select Options dialog box appears.



2. Do one of the following:

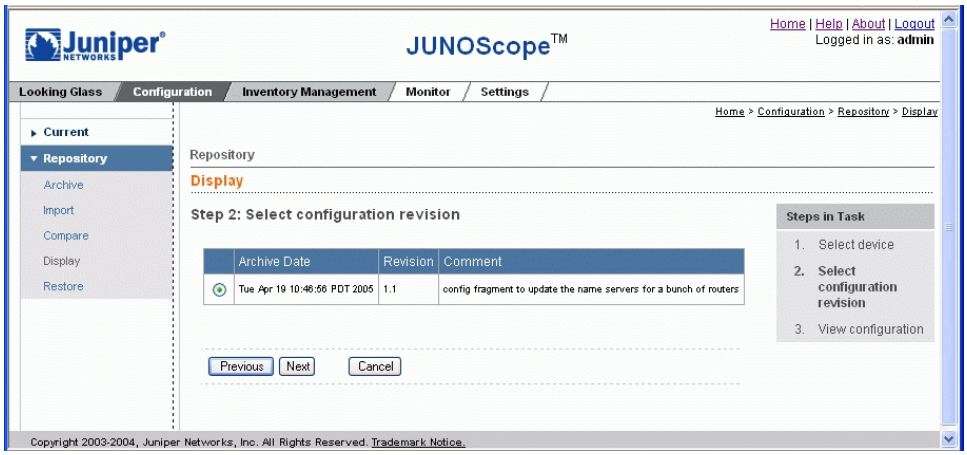
   ■ To display an archived configuration, ensure that Archived Configuration (the default selection) is selected in the Configuration File drop-down list box, then go to Step 3.

- To display an imported configuration file, select a filename in the Configuration File drop-down list box, then skip to Step 4. Configuration filenames only appear in the Configuration File drop-down list box when you have imported a configuration file. If you have not imported a configuration file, Archive Configuration only appears in the Configuration File drop-down list box.

  The Device drop-down list box is disabled when you select an imported configuration filename because an imported configuration is not associated with any device.

3. Select the device for which you want to display a configuration in the Device drop-down list box. Devices are displayed in the drop-down list box only when you have added them to the JUNOScope software. If no devices are displayed, you have not added a device yet. See "Setting Up Devices" on page 57.

4. Click Next. The Display—Select configuration revision dialog box appears with the available configuration file revisions listed by archive date, revision level, and comment.



5. Select the option button for the configuration file that you want to view.

   Configuration revisions are listed in the Select Configuration Revision dialog box only when you have archived or imported them. If you have not done so, the list is empty.

6. Click Next. The configuration file contents display in the Display—View Configuration dialog box.

7. Click Previous to return to the Select Configuration Revision dialog box.

Chapter 22

Restoring a Configuration File

This chapter describes how to restore an archived configuration file from the JUNOScope software Concurrent Versions System (CVS) repository to the same router from which you archived it. It also describes how to upload an imported a configuration file to any router. The configuration file is committed and overrides, replaces, or merges the active configuration file currently running on the router.

Configuration file versions are stored in the CVS repository when you archive or import them.

This chapter also describes how to save a restore operation so that you can combine it with other operations, such as archive and inventory scan, to run on specified devices in your network.

You must have superuser or read-write permission to restore a configuration file.

This chapter includes the following topics:

What Happens on the Router During a Restore Operation

The following steps describe what happens on the router when the JUNOScope software performs a restore and archive:

1. The user selects the configuration revision to restore.
2. JUNOScope connects to the JUNOScript server on the target router.
3. JUNOScope sends the following commands to the JUNOScript server to be performed on the router:
   a. Lock the router configuration.
   b. Load the new configuration on the router, overriding (discarding), replacing (deleting and adding), or merging (combining) the old configuration.
   c. Issue a commit confirmed command.

d. Issue a commit-configuration JUNOScript XML tag command. If the user specified it, JUNOScope issues a commit synchronize command.

e. Unlock the configuration.

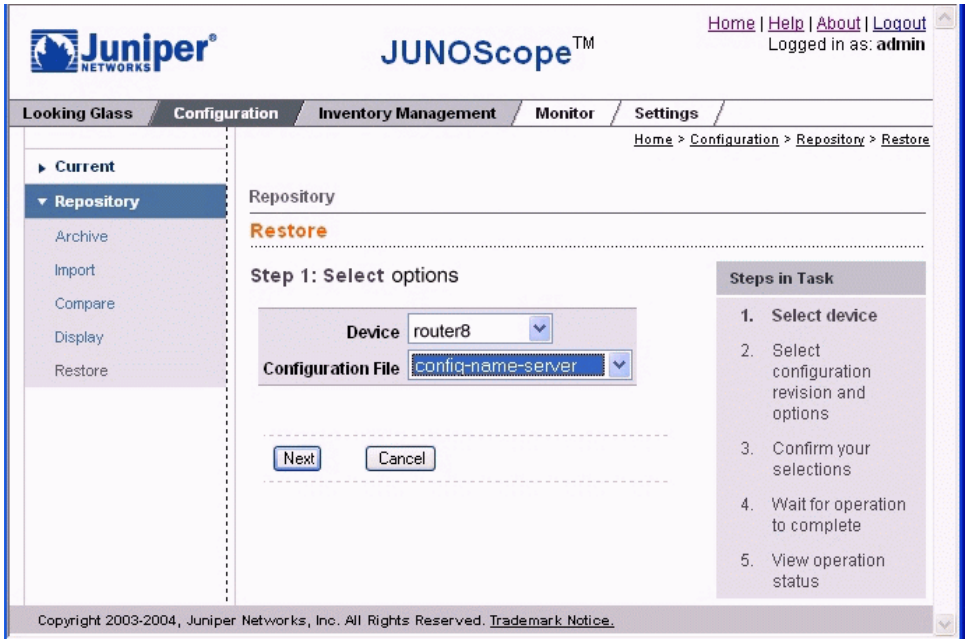
NOTE: If an error occurs, JUNOScope issues a rollback command, causing the configuration to revert to the last saved configuration.

4. JUNOScope updates the final status values for the restore operation.

Restoring a Configuration

To restore a configuration file, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Restore. The Restore—Select Options dialog box appears.



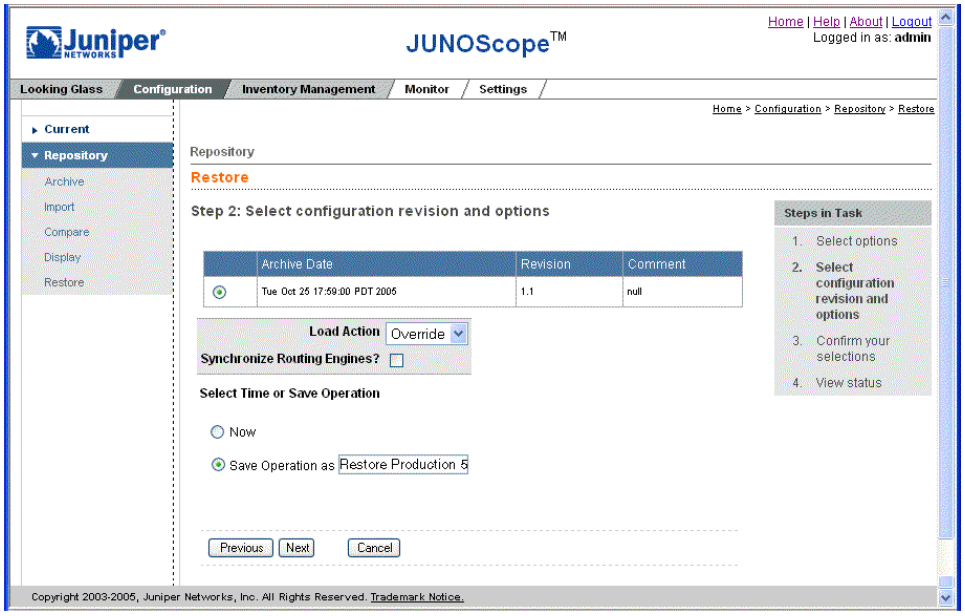
2. In the Device drop-down list box, select a device to which to restore a configuration file.

3. Do one of the following:

   - To restore an archived configuration, ensure that Archived Configuration (the default selection) is selected in the Configuration File drop-down list box.

   - To restore an imported configuration file, select a filename in the Configuration File drop-down list box. Configuration filenames only appear in the Configuration File drop-down list box when you have imported a configuration file. If you have not imported a configuration file, Archive Configuration only appears in the Configuration File drop-down list box.

4. Click Next. The Restore—Select configuration revision dialog box appears with the configurations stored in the JUNOScope CVS repository listed by archive date, revision, and comment.



5. Click the option button for the configuration file that you want to restore.

NOTE: If you have selected a BXOS device in Step 2, you must choose a configuration file that is in a well-formed XML format for restoring on the BXOS device. If the selected file is not in xml format or is structurally invalid, the restore operation fails and an “Unsupported Operation” message is returned.

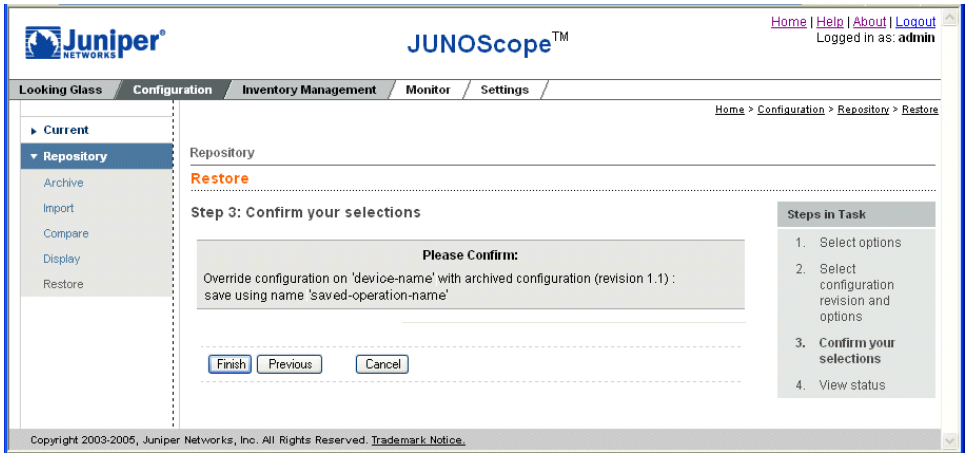
TIP: For BXOS archived configurations, the comment field indicates whether it is a startup configuration or a running configuration.

6. Select whether you want to override, replace, or merge (default) the current configuration on the device. The available options include:
   - Override—Discards all of the current configuration and loads the selected configuration.
   - Replace—Deletes the current configuration statement(s) and adds the selected configuration.
   - Merge—(Default) Combines the selected configuration statement(s) with the current configuration. If there are conflicting statements, the statements in the incoming configuration override those in the current configuration.
7. Do one of the following:
   - If the selected device is a JUNOS device that has two Routing Engines installed, click the Synchronize Routing Engines check box. This option, if

checked, restores the configuration on both Routing Engines. This option is not displayed when you have selected a device other than a JUNOS device.

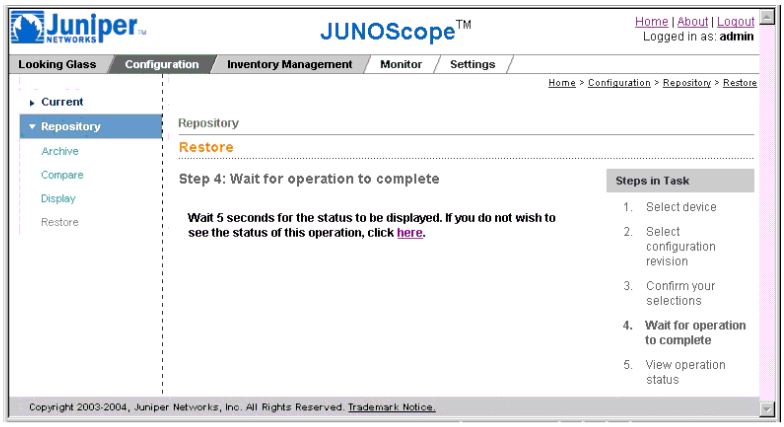
- If the selected device is a BXOS device, click the Sync the Startup Configuration with Running check box. This option, when checked, synchronizes the running configuration with the startup configuration. If this option is not selected, only the running configuration is updated after the restore operation. This option is displayed only when you have selected a BXOS device for restoring configuration.

8. Select when you want the restore operation to occur.
   - Click the Now option button to perform the restore operation immediately.
   - Click the Save Operation as option button to save the restore operation so that you can combine it with other operations to be run concurrently or in sequence. Type a name for the restore operation in the text box.
9. Click Next. The Restore—Confirm your selections dialog box appears.



10. Click Finish to confirm the restore operation.

    If you selected to save the restore operation, the Configuration > Repository menu appears. To view the saved restore operation, click Settings > Saved Operations.
11. The Restore—Wait for operation to complete dialog box appears; wait for the Restore operation to complete.



After a few seconds, the Restore—View operation status dialog box appears.

The Requested Operation Status dialog box lists the restore operation results by device, status, start time, last update time, and status message.

12. Click OK.

Saving a Configuration Restore Operation

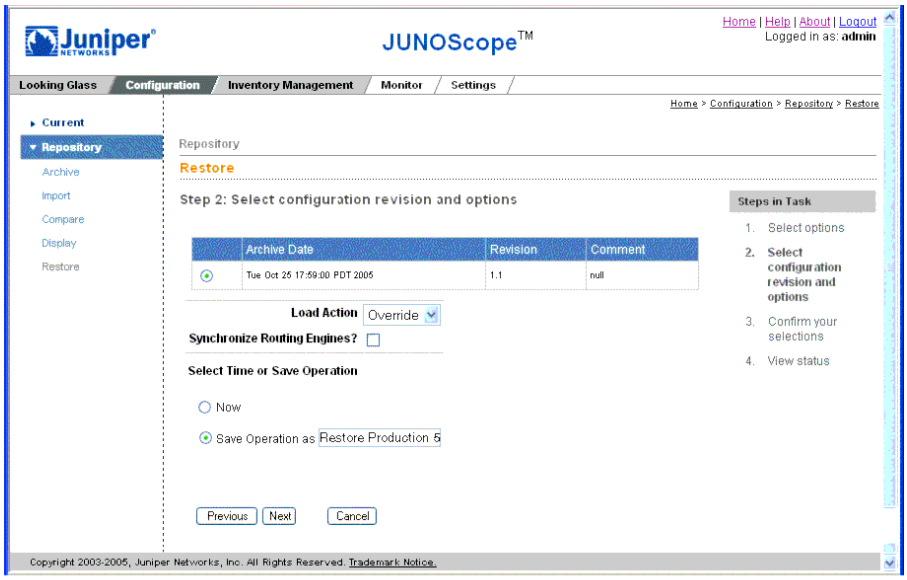
You can save restore operations and combine them with other saved operations to be run concurrently or sequentially on specific devices either immediately or at a specified time or interval.

To save a restore operation, follow these steps:

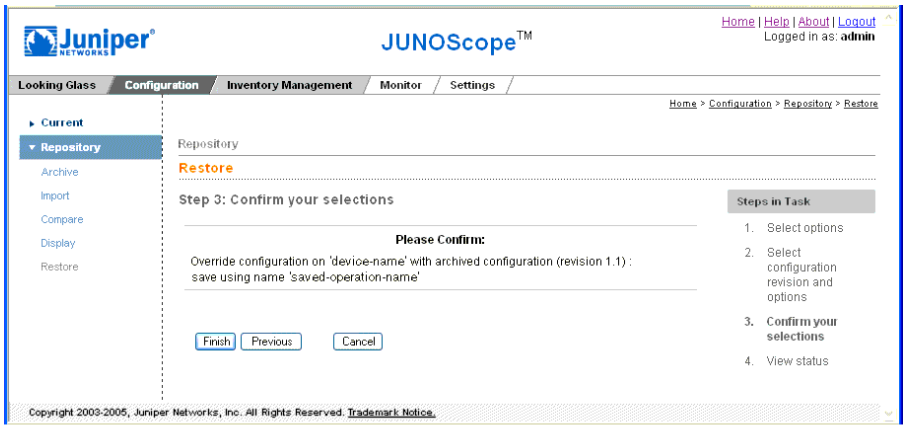
1. From the JUNOScope main window, click Configuration > Repository > Restore. The Restore—Select Options dialog box appears.

2. Select the configuration file or device that you want to restore to one or more devices.

3. Click Next. The Restore—Select Device and Time dialog box appears.



4. Select the archive revision that you want to restore.
5. Select the Restore load action that you want.
   - Override—Discards all of the current configuration and loads the selected configuration.
   - Replace—Deletes the current configuration statement(s) and adds the selected configuration.
   - Merge—(Default) Combines the selected configuration statement(s) with the current configuration. If there are conflicting statements, the statements in the incoming configuration override those in the current configuration.
6. If the device has redundant Routing Engines, select whether to synchronize them.
7. Click the Save Operation as option button and type a unique name in the Save Operation text box.
8. Click Next. The Restore—Confirm Your Selections dialog box appears.



9. Confirm that the restore selections that you want to save are correct, then click Finish.

   You return to the Configuration > Repository menu. To view a saved restore operation, click Settings > Saved Operations. To work with saved operations, see “Using Task Manager (Saved Operations)” on page 167.

Chapter 23

Managing JUNOS Scripts

This chapter describes how JUNOS-based scripts such as commit scripts, operation (op) scripts, and event scripts can be imported into the JUNOScope CVS repository from the local file system and deployed to a group of routers. Commit scripts are used to enforce custom configuration rules, while op scripts are used to automate network troubleshooting and network management. Event scripts are op scripts invoked in response to event notifications such as system log messages and Simple Network Management Protocol (SNMP) traps received by the event process. For more information see the JUNOS Configuration and Diagnostic Automation Guide. This chapter also describes how users can view, edit, compare, and disable these scripts.

This chapter includes the following topics:

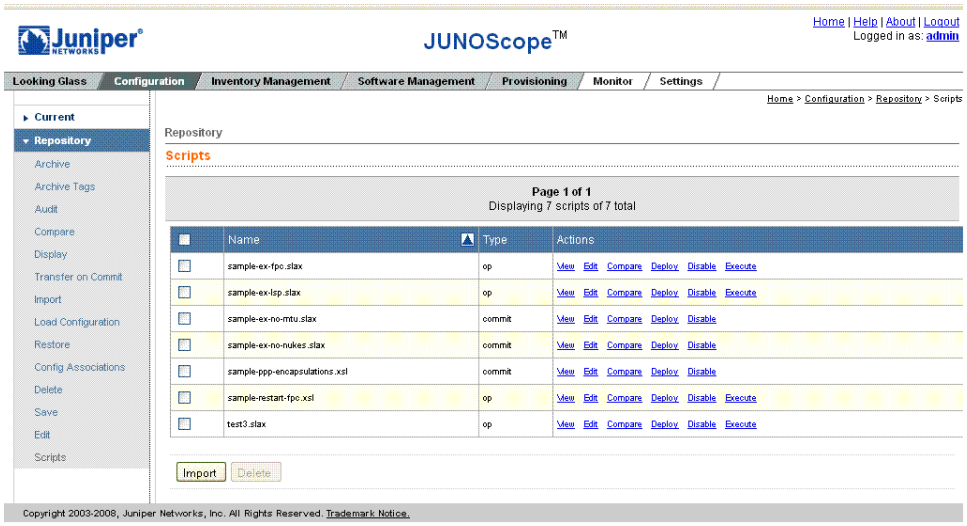
You must have superuser permission to manage JUNOS scripts.

Importing JUNOS Scripts

This section describes how you can import JUNOS-based scripts such as commit scripts, op scripts, and event scripts into the JUNOScope CVS repository from the local file system.

To import a JUNOS script into the JUNOScope CVS repository, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



All JUNOS-based scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on scripts.

2. Click Import. The Import dialog box appears.

3. Browse to the location on your local machine where you have stored the JUNOS script to be imported.

4. Enter the MD5 checksum value in the MD5 Checksum For Verification (Optional) field. The checksum can be obtained from http://www.juniper.net/customers/support/ when you download the script. This checksum value is compared with the checksum stored in JUNOScope to verify that the downloaded script is intact. This field is optional.

5. Select the script type from the Script Type drop-down list box.

There are three script types:

- Commit—A commit script enforces custom configuration rules. Each time a new candidate configuration is committed, the script inspects the configuration. If a configuration violates your custom rules, the script corrects the problem.
- Op—An op script automates network troubleshooting and network management. It can perform any function available through the remote procedure calls (RPCs) supported by two APIs: the JUNOS extensible markup language (XML) API and the JUNOScript API.
- Event—Event scripts are op scripts invoked in response to event notifications such as system log messages and SNMP traps received by the event process.

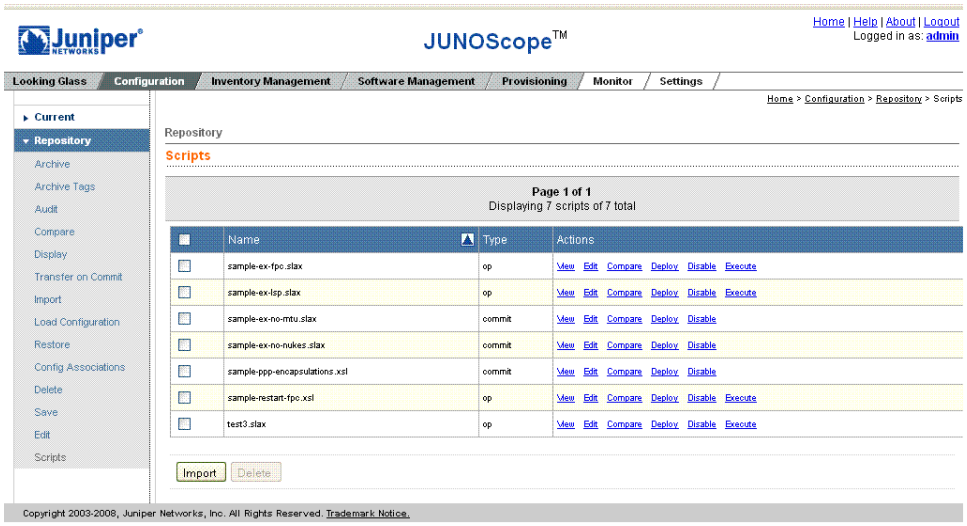
6. In the Comment text box, type an optional comment for the script.
7. Click Import. The Import Result dialog box appears.

8. Click OK. The new JUNOS script appears in the Scripts dialog box.

Viewing JUNOS Scripts

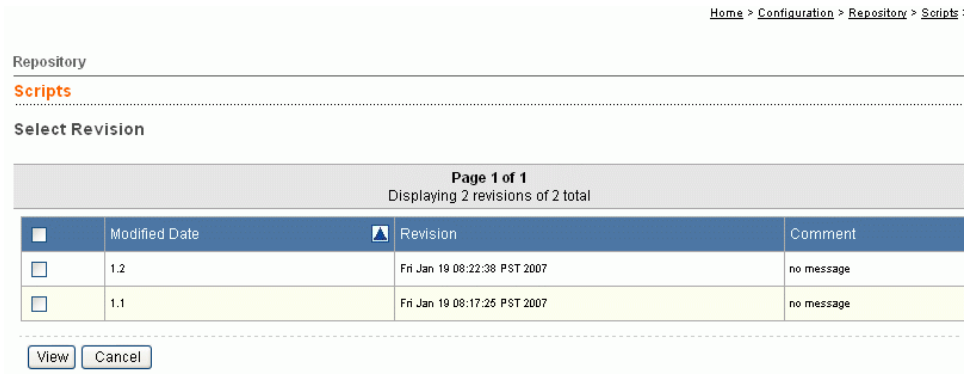
To view JUNOS scripts, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



All JUNOS scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on JUNOS scripts.

2. Select the JUNOS script you want to view by clicking View in the Action column in the corresponding row. The Select Revision dialog box appears.



The Select Revision dialog box lists the revisions of this script in the JUNOScope CVS repository.

3. Select the revision you want to view by selecting the check box in the corresponding row, then click View. The View dialog box appears.

Home > Configuration > Repository > Scripts

Repository

Scripts

View

re-drop.xsl revision 1.1

```
<?xml version="1.0" standalone="yes"?>
<!--
- $Id: re-drop.xsl,v 1.1 2007/01/19 16:20:36 tfan Exp $
-
- Copyright (c) 2004, Juniper Networks, Inc.
- All rights reserved.
-
-->
<xsl:stylesheet version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:junos="http://xml.juniper.net/junos/*/junos"
  xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
  xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">

  <xsl:import href="../import/junos.xsl"/>

  <xsl:template match="configuration">
    <transient-change>
      <interfaces>
        <interface>
          <name>fxp0</name>
          <unit>
            <name>0</name>
            <family>
              <iso/>
            </family>
          </unit>
        </interface>
      </interfaces>
    </transient-change>
  </xsl:template>

</xsl:stylesheet>
```

Previous OK

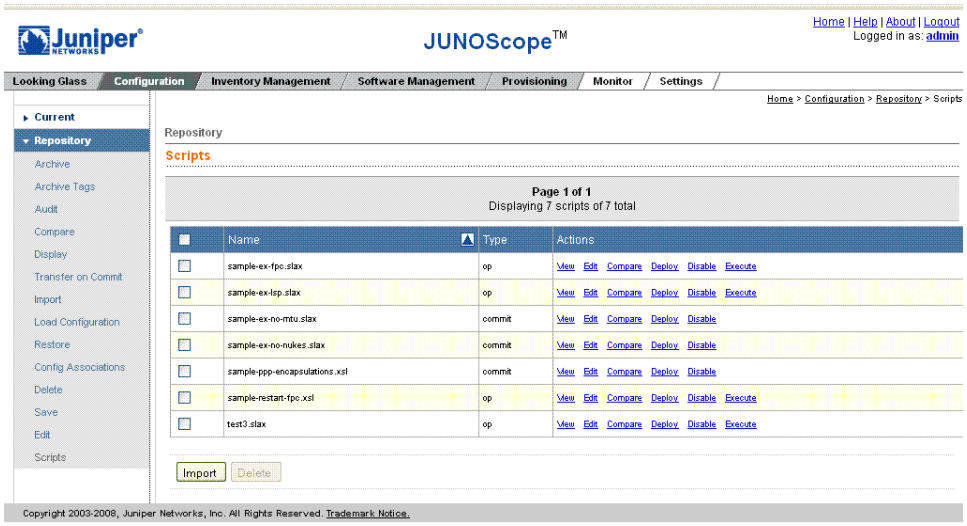
The script is displayed in the View Scripts dialog box.

4. Click Previous to return to the Select Revision dialog box to select another revision to view. Click OK to return to the Scripts dialog box.

Editing JUNOS Scripts

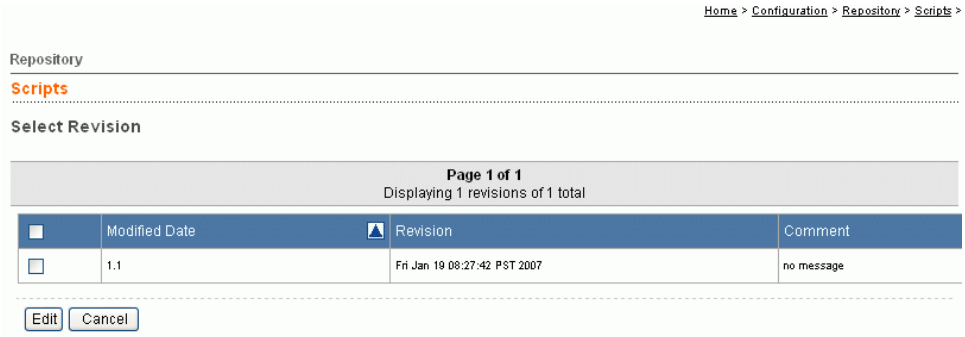
To edit JUNOS scripts, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



All JUNOS scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on JUNOS scripts.

2. Select the script you want to edit by clicking Edit in the Action column in the corresponding row. The Select Revision dialog box appears.



The Select Revision dialog box lists the revisions of this script in the JUNOScope CVS repository.

3. Select the revision you want to edit by selecting the check box in the corresponding row, then click Edit. The Edit dialog box appears.

The script is displayed in the Edit dialog box.

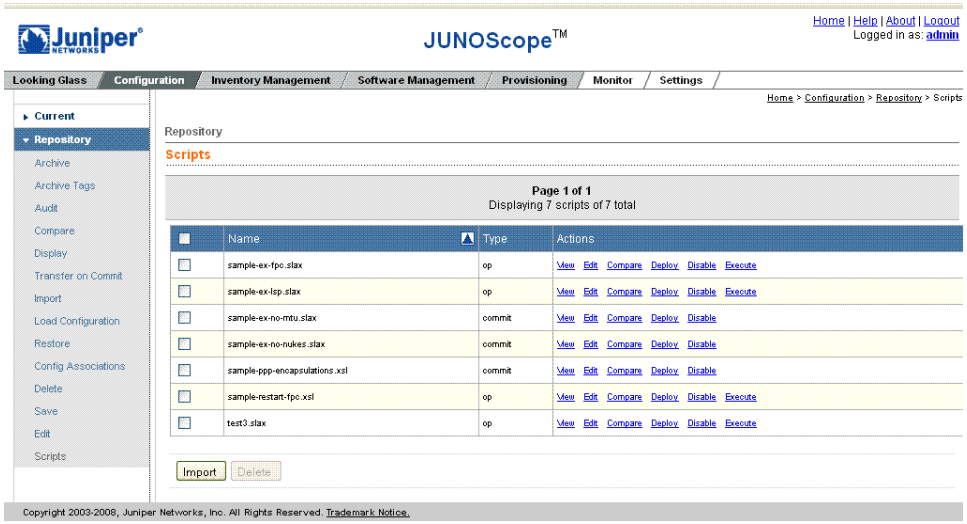
4. Modify the script as required in the Edit dialog box and click Save. The Save Result dialog box appears displaying whether the script has been modified.

5. Click OK. The modified script is added into the CVS repository as a new revision.

Comparing JUNOS Scripts

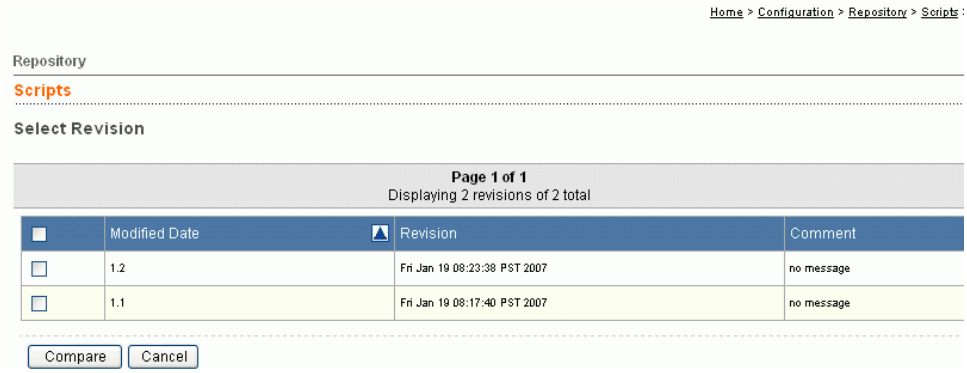
To compare JUNOS scripts in the JUNOScope CVS repository, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



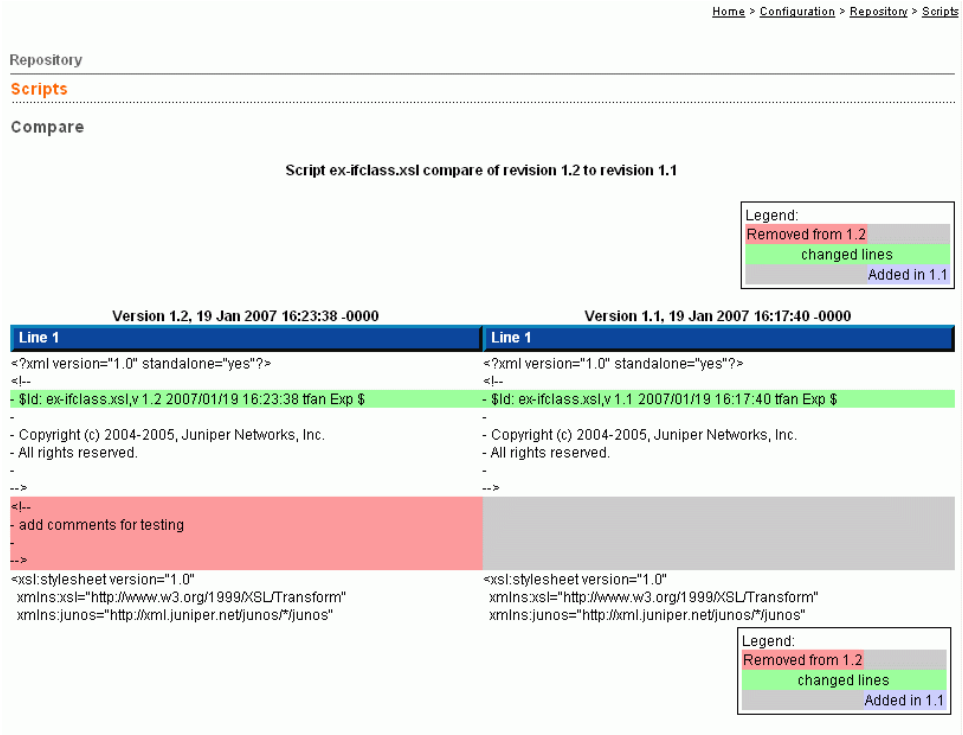
All JUNOS scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on scripts.

2. Select the scripts you want to compare by clicking Compare in the Action column in the corresponding row. The Select Revision dialog box appears.



The Select Revision dialog box lists the revisions of this script in the JUNOScope CVS repository.

3. Select the revisions you want to compare by selecting the check boxes in the corresponding rows, then click Compare. The Compare dialog box appears.

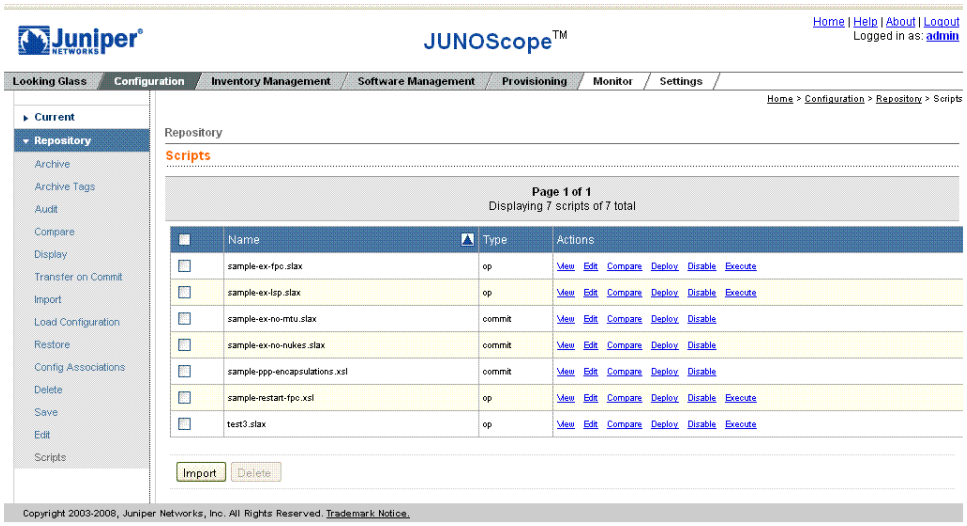


The two revisions that you selected to compare appear in the Compare display box. The latest revision appears on the left; the older revision on the right. The differences between the two configurations are highlighted. See the Legend for an explanation of the highlighting.

Deploying JUNOS Scripts

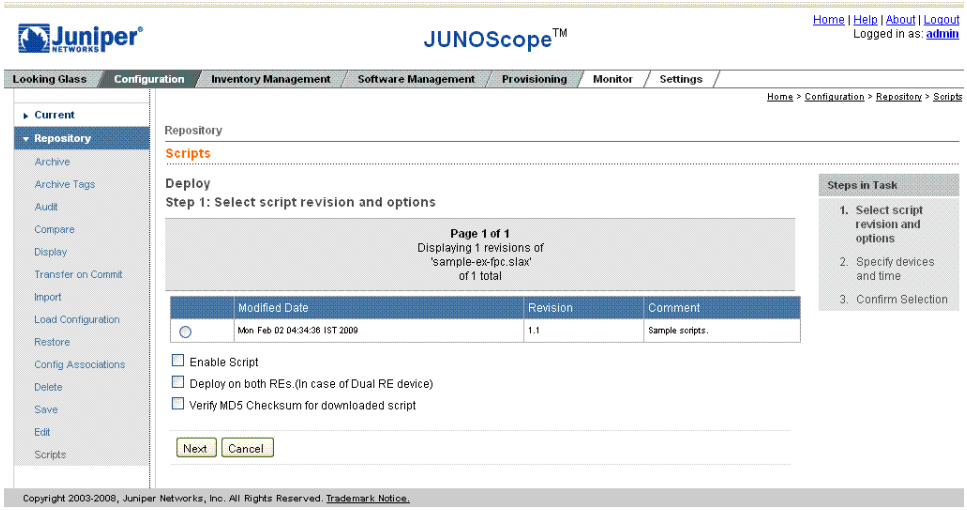
To deploy a JUNOS script in the JUNOScope CVS repository to a router or group of routers, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



All JUNOS scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on scripts.

2. Select the script you want to deploy, then click the Deploy link in the Actions column in the corresponding row. The Select Script Revision and Options dialog box appears.

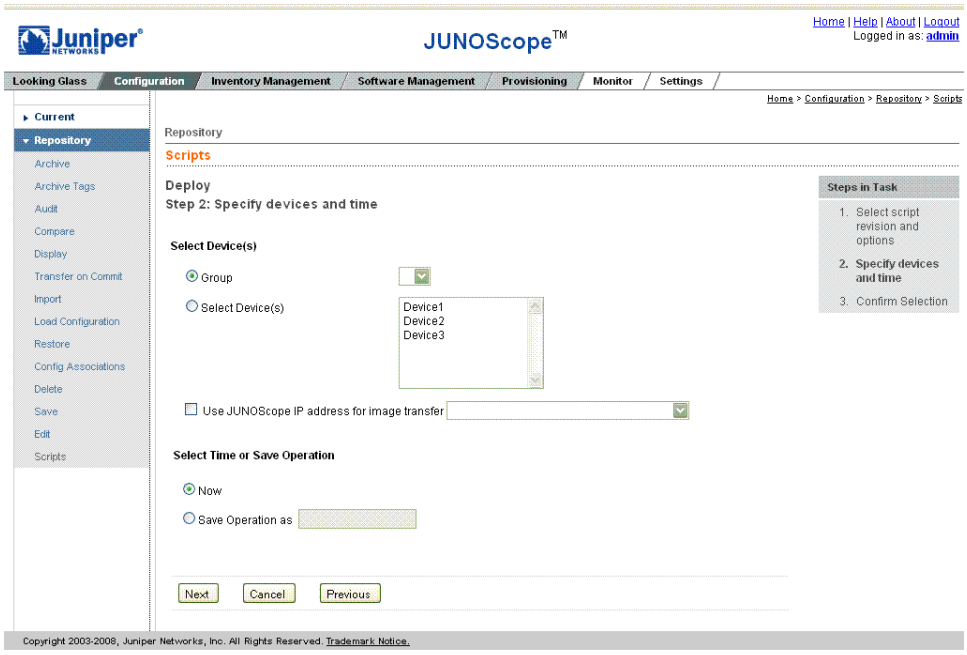


3. Select the script revision that you want to deploy.
4. Select the Enable Script check box to activate the script you are deploying.
5. Select the Deploy on Both REs (in case of dual RE) check box to deploy the script on both the routing engines. In case of dual routing engines, enabling this option will allow you to deploy the script on both the routing engine systems (i.e. master routing engine and backup routing engine). By default, the script is only deployed

to the current routing engine. The script is deployed to the other RE by performing a commit synchronize operation on the RE that you are connected to.

NOTE: The Deploy on both REs. (In case of Dual RE device) option is ignored for single RE systems.

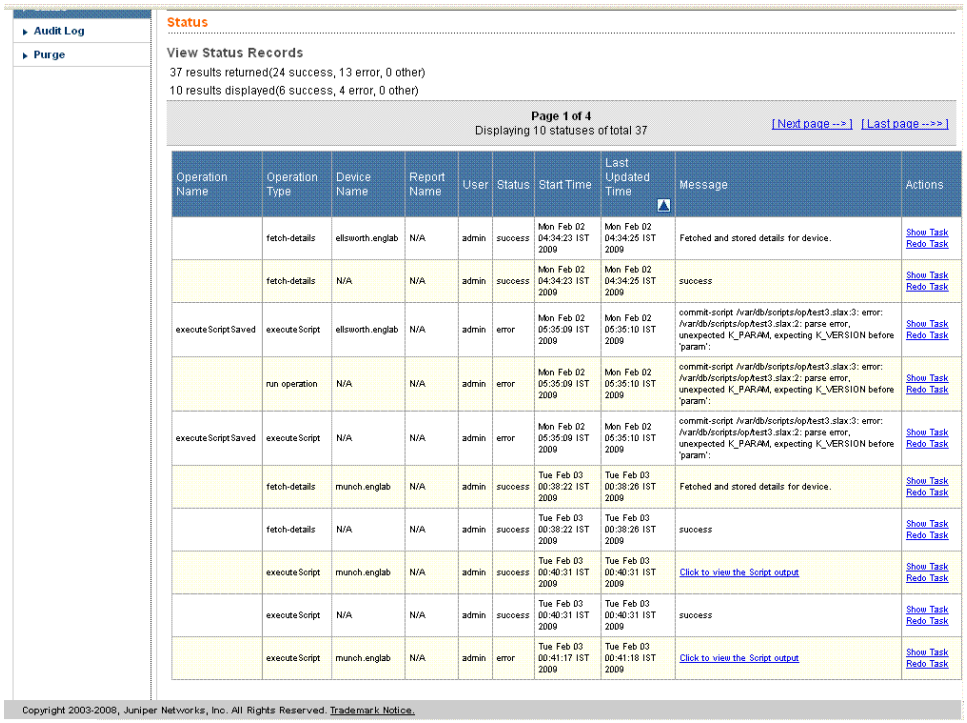
6. Select the Verify MD5 Checksum for downloaded script check box if you want to ensure that the downloaded script is intact. If you select this option, the MD5 checksum of the downloaded script is compared with the checksum stored in JUNOScope. If they do not match, the operation fails and the error message "MD5 checksum of downloaded script does not match the script in JUNOScope" appears in the JUNOScope status (Monitor > Status > View Status Record).
7. Click Next. The Specify Devices and Time dialog box appears.



8. Select the device or group of devices to which you want to deploy the script, from the Group or Select Devices list box. Shift-click to select multiple devices from the Select Device(s) drop-down list box.
9. Select when you want to deploy the script:
   - Now—(Default) Performs the deploy operation immediately after you confirm it.
   - Save Operation as—Select to save the deploy operation to run at a later time. Click Save Operation as, then type an operation name in the text box.
   - Click Next. The Confirm Selection dialog box appears.

10. Confirm that the selections you made are correct and click Finish to deploy the script to the router or group of routers. Click Previous to return to Specify Devices and Time dialog box.

    - If you selected Now in Step 7, deploy occurs immediately and the View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

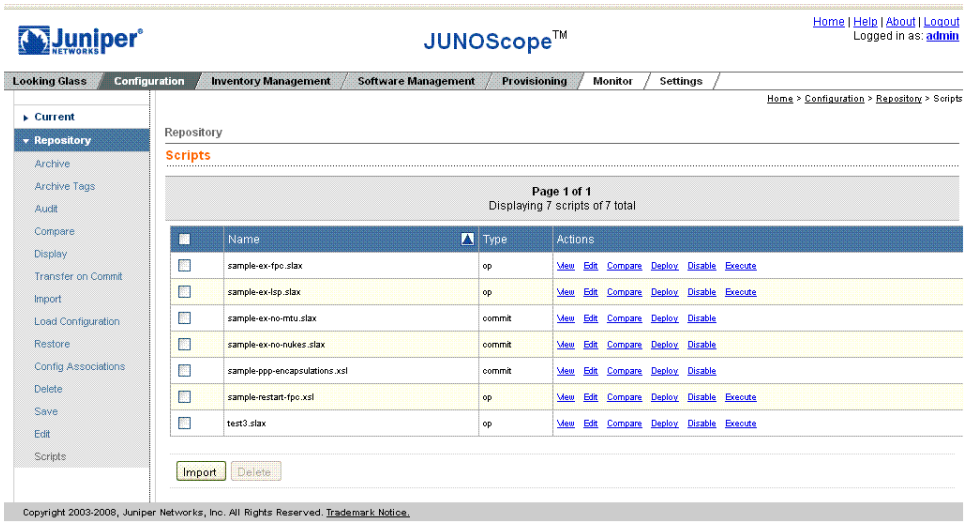
The View Status Records dialog box lists the deploy status by Operation name, Operation Type, Device Name, Report Name, User, Status, Start time, Last Updated Time, and Message.

- If you selected Save Operation as, to save the deploy operation, you return to the Configuration > Repository > Scripts menu. To view the saved operation, click Settings > Saved Operations.

Disabling JUNOS Scripts

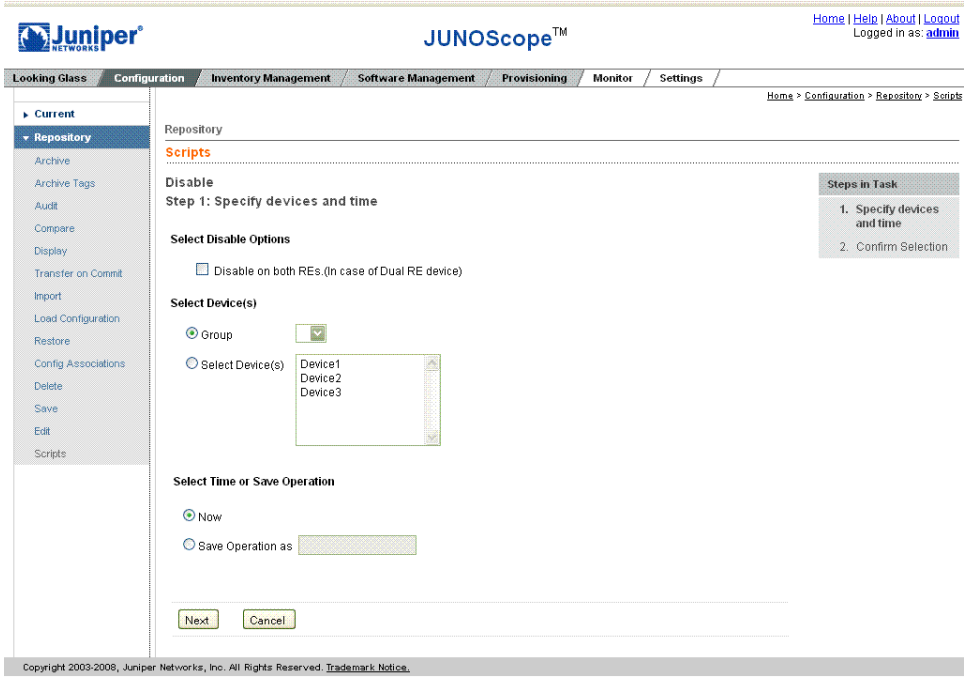
NOTE: You can disable commit scripts and op scripts using this feature, however you will have to manually enable or disable event scripts on the router.

1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



   All JUNOS scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on scripts.

2. Select the script you want to disable by clicking Disable in the Action column in the corresponding row. The Specify Devices and Time dialog box appears.



3. Select the Disable on both REs. (In case of Dual RE device) option if you want to disable the script on both routing engines. In case of dual RE devices, selecting this option will allow you to disable the script on both the routing engine systems (i.e. master routing engine and backup routing engine).

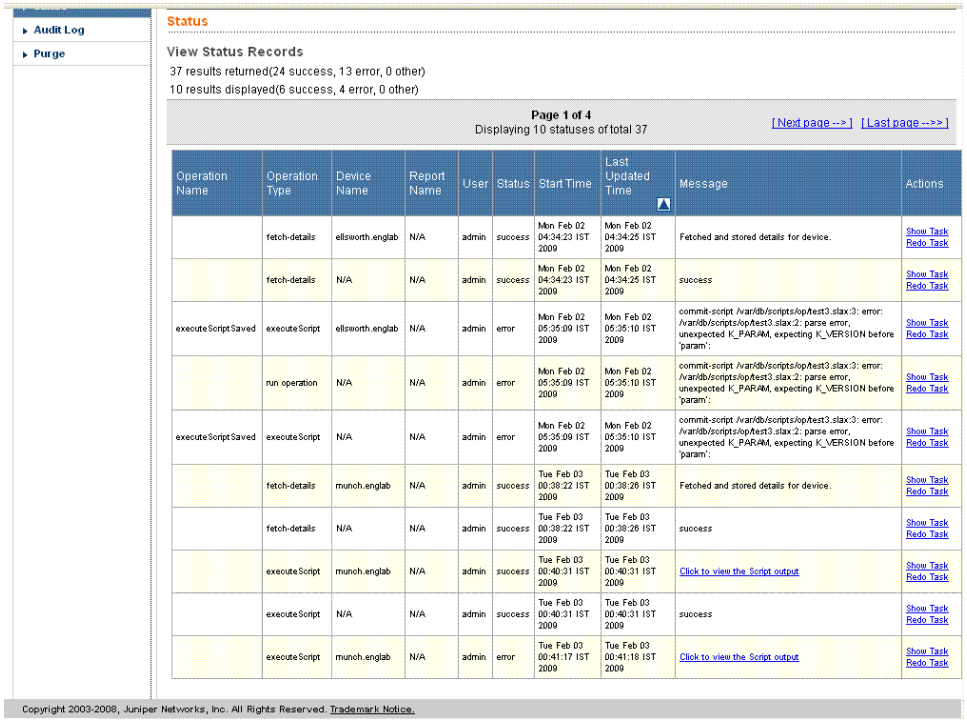
NOTE: The Disable on both REs. (In case of Dual RE device) option is ignored for single RE systems.

---

4. Select the device or group of devices on which you want to disable the script from the Group or Select Devices list box. Shift-click to select multiple devices from the Select Device(s) drop-down list box.
5. Select at what time you want to disable the script:
   - Now—(Default) Performs the disable operation immediately after you confirm it.
   - Save Operation as—Select to save the disable operation to run at a later time. Click Save Operation as, then type an operation name in the text box.
6. Click Next. The Confirm Selection dialog box appears.

7. Confirm that the selections you made are correct and click Finish to disable the script on the selected router or group of routers. Click Previous to return to Specify Devices and Time dialog box without disabling the script.

   - If you selected Now in Step 4, disable occurs immediately and the View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

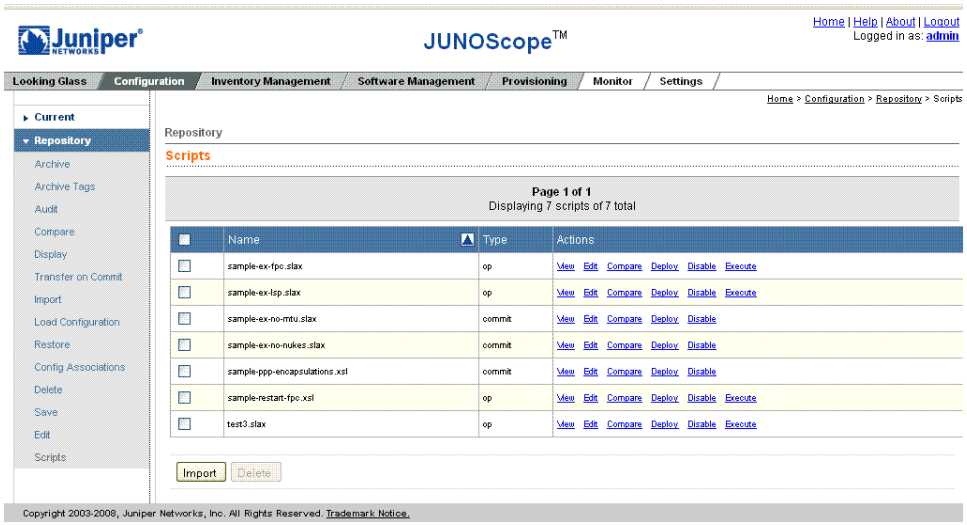
The View Status Records dialog box lists the disable status by Operation name, Operation Type, Device Name, Report Name, User, Status, Start time, Last Updated Time and Message.

- If you selected Save Operation as to save the disable operation, you return to the Configuration > Repository > Scripts menu. To view the saved operation, click Settings > Saved Operations.

Deleting JUNOS Scripts

To delete JUNOS scripts from the JUNOScope CVS repository, follow these steps:

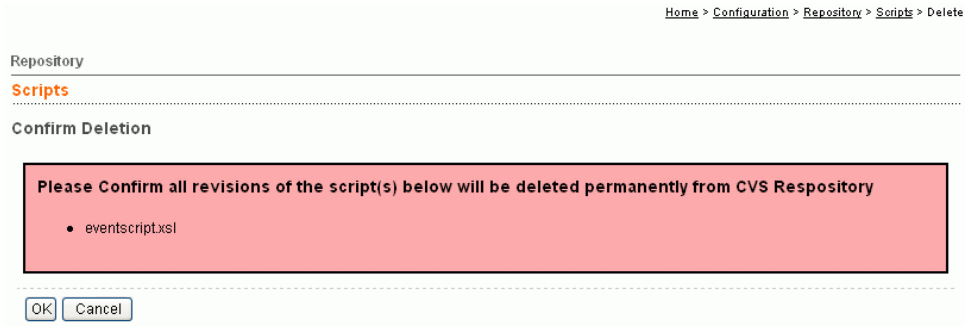
1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



   All JUNOS scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on scripts.

2. Select the check boxes in the corresponding rows to select the scripts you want to delete. Select the check box in the column header row to delete all the scripts in the JUNOScope CVS repository.

3. Click Delete. The Confirm Deletion dialog box appears.

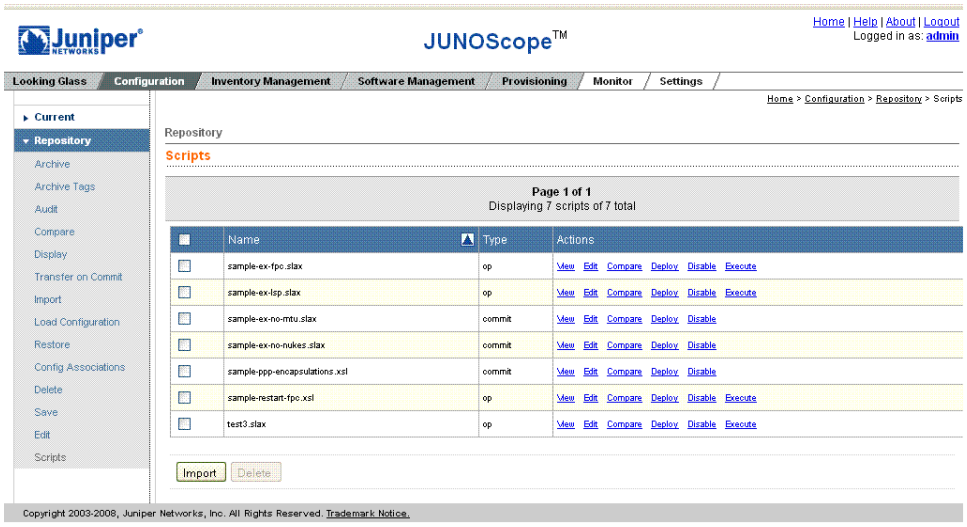


4. Click OK to confirm deletion of the script or scripts you selected. The Script dialog box appears without the deleted scripts.

Executing JUNOS Scripts

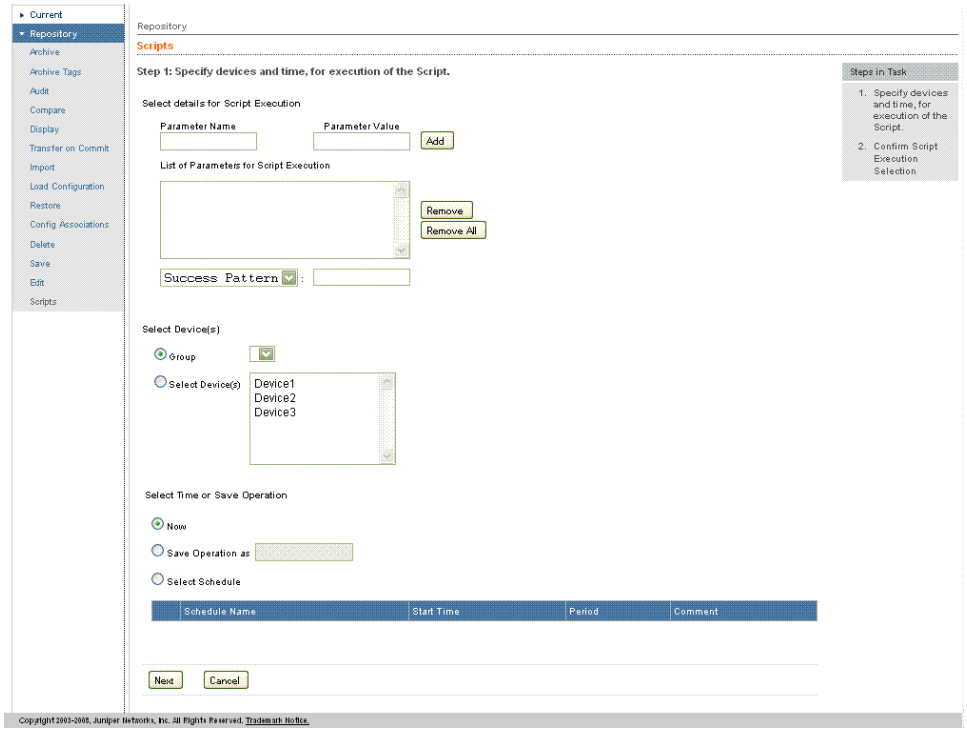
To execute an operation script, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Scripts. The Scripts dialog box appears.



   All scripts saved in the JUNOScope CVS repository are listed in the Scripts dialog box alphabetically by name. The dialog box displays the script filename, type, and the actions you can perform on scripts.

2. Click the Execute link of the script that you want to execute. The Select Script Revision and Options dialog box appears.



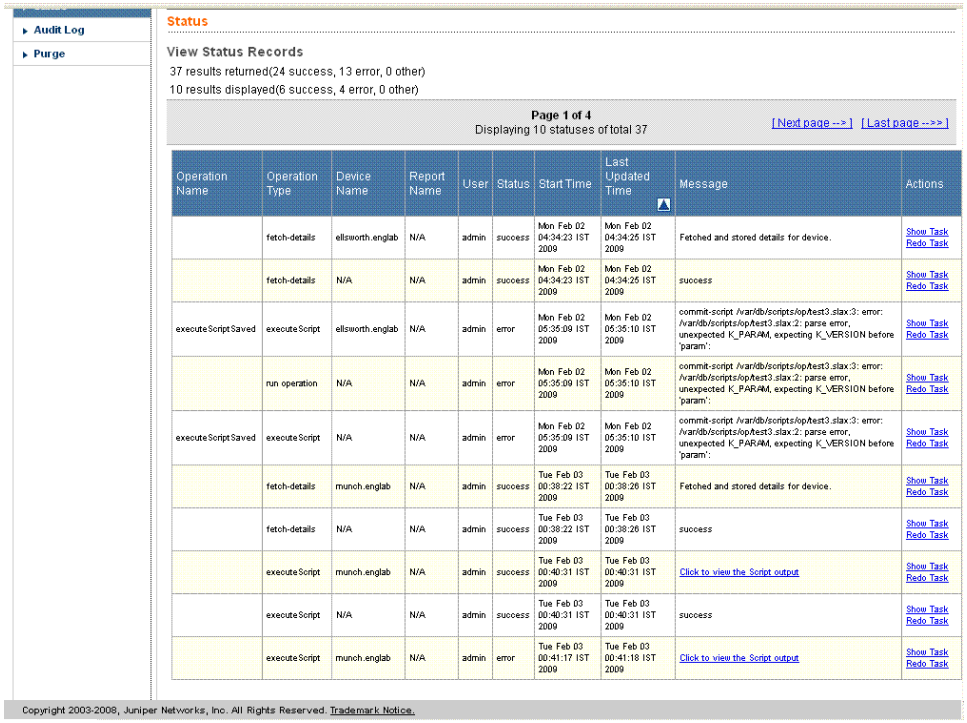
3. Select the script revision that you want to execute.
4. Specify the parameters for the script execution by providing the parameter name and value and clicking Add. The parameters are displayed in List of Parameters for script execution. You can delete a parameter by selecting the parameter and clicking Remove.
5. Select the pattern type (success or failure) from the list and enter a pattern value in the field. After the script executes successfully, JUNOScope searches for this value in the output of the script execution and displays the status message in the Status page (Monitor > Status > View Status Records).
   - Success pattern — If you select this option from the list, JUNOScope displays a “success” message in the Status page if the value is found in the output of the script execution and a “failure” message if the value is not found in the output.
   - Failure pattern — If you select this option from the list, JUNOScope displays a “failure” message in the Status page if the value is found in the output of the script execution and a “success” message if the value is not found in the output.
6. Select the device or group of devices on which you want to execute the script, from the Group or Select Devices list box. Shift-click to select multiple devices from the Select Device(s) drop-down list box.
7. Select when you want to execute the script:
   - Now— (Default) Performs the execute operation immediately after you confirm it.

- Save Operation as—Select to save the script execution operation and run it at a later time. Click Save Operation as, then type an operation name in the text box.
- Select Schedule—Performs the script execution operation at the scheduled time interval. Select the schedule that you want in the schedule table.

8. Click Next. The Confirm Selection dialog box appears.

9. Confirm that the selections you made are correct and click Finish to execute the script. Click Previous to return to Specify Devices and Time dialog box.
   - If you selected Now in Step 7, the execute operation occurs immediately and the View Status Records dialog box appears.

     The View Status Records dialog box lists the execute operation status by Operation name, Operation Type, Device Name, Report Name, User, Status, Start time, Last Updated Time, and Message.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

- If you selected **Save Operation as**, to save the execute operation, you return to the Configuration > Repository > Scripts menu. To view the saved operation, click Settings > Saved Operations.
- If you selected the **Select Schedule** option and selected a schedule, the script is executed when the operation is scheduled to be run.

The status page (Monitor > Status > View Status Record) will change. The executed operation script will have a new link **View Output** displayed under the Action column. Click **View Output** to view the results of the operation script execution.

Chapter 24

Managing Configuration File Associations

JUNOScope can be configured to act as an automatic configuration server (ACS). This means that JUNOScope can supply configuration files to several devices simultaneously. JUNOScope enables you to associate configuration files to a set of criteria that you specify. These criteria can be a set of conditions for parameters such as hostname, model, OS version and serial number with values that you specify; a pre-configured group of devices; or a combination of both. JUNOScope can simultaneously serve up to 200 devices.

You can import configuration files into JUNOScope from an external source using the Import feature (See "Importing and Deleting Configuration Files" on page 229) and can store the imported configuration files in the server.

When a device requests for a configuration file, the server compares the device attributes with the criteria and returns the URL of the first configuration file whose associated criteria match the device attributes. The device uses this URL to download the associated configuration file. If no configuration file is found, JUNOScope returns an HTTP 404 error to the device.

This chapter describes how JUNOScope supplies configuration files to devices. It also describes how you can create new configuration file associations, change the order of the configuration associations, and delete configuration file associations.

NOTE:

In order to use JUNOScope as an ACS, you must have:

- Superuser, or read-write permissions.
- Installed IP Backhaul Manager license.

This chapter includes the following topics:

How Configuration Association Works

JUNOScope enables you to import configuration files using the Import feature and store the imported files in the server. You can associate an imported configuration file with a set of criteria. JUNOScope returns a configuration file to a device if the attributes of the requesting device match its associated criteria.

1. First, the device sends a request to the JUNOScope server. This request is in the form of a URL which contains device details such a hostname, model, OS version, and serial number. The URL that the device uses to send a request to the configuration server has this format:

   http://< *ACS server* >:< *port* >/jtk/download/config/getURL?*hostname=?& osVersion=?&model=?&serialNumber=?*

   Where ACS server is the ip address or hostname of the JUNOScope server.

   For example, the URL that the device uses to send a request with values asd for hostname, asdf for OS Version, sdf for model, and sdfg for serial number is as follows:

   http://junoscope-server/ jtk/ download/ config/ getURL?hostname=asdf& osVersion=asdf& model=sdf& serialNumber=sdfg

2. When JUNOScope receives the request, it compares the device attributes with the criteria of the configuration associations on the server. JUNOScope starts comparing the device attributes with the criteria of the first configuration association in the list. The comparison is done till a match is found or till it reaches the end of the list.

3. If the device attributes match the criteria in a configuration association, JUNOScope constructs a URL which contains the configuration file and returns the URL to the device.

   If no match is found, and the default option is set (See Table 18 on page 273), JUNOScope returns the URL of the default configuration file.

   The URL which JUNOScope returns to the device has this format:

   http://< *ACS server* >:< *port* >/jtk/download/config/getConfig?configName=< *ConfigPath* >configVersion=< *ConfigRevision* >

   For example, the URL which JUNOScope returns to the device with values user-supplied/ archivedHCL for configName, and 1.1 for configVersion is as follows:

   http://junoscope-server/ jtk/ download/ config/ getConfig? configName=user-supplied/ archivedHCL& configVersion=1.1

   If no match is found, and the default option is not set, JUNOScope returns an HTTP 404 error to the device.

4. The device uses this URL to download the configuration file.

Displaying the List of Configuration Associations

To view the list of configuration file associations, in the JUNOScope main window, click Configuration > Repository > Config Associations. The List of Configuration Associations page displays the list of configuration file associations. The page also provides you with the buttons to Delete, Add, Reorder, Import and Export configuration associations.

Figure 6: List of Configuration Associations page

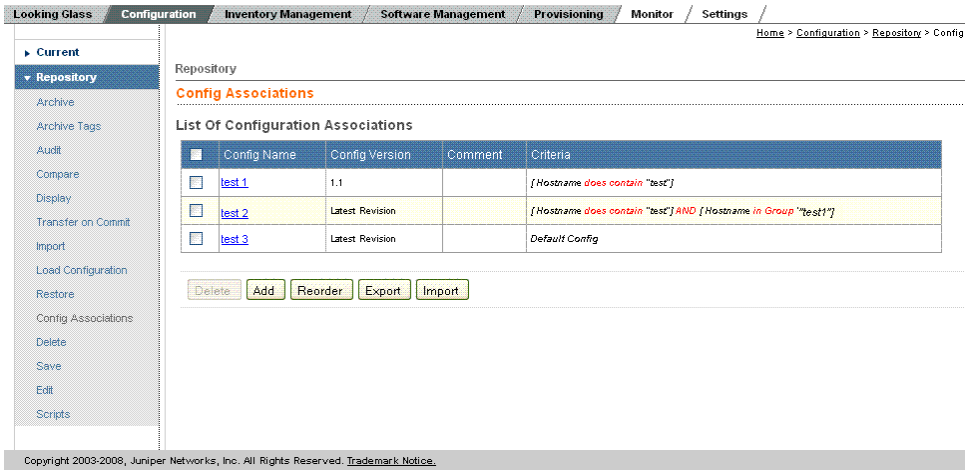


Table 16 on page 271 lists out the different labels and buttons, and their descriptions.

Table 16: List of Labels on the List of Configuration Associations Page

Label	Description
Config Name	The name of the configuration file used in the association. Click the Config Name of the configuration association to take you to the Edit Configuration Association page where you can edit that configuration file association.
Config Version	The version of the configuration file.
Comment	A brief description of the configuration.
Criteria	The set of rules that the device attributes must match in order for the configuration file to be returned to the requesting device.

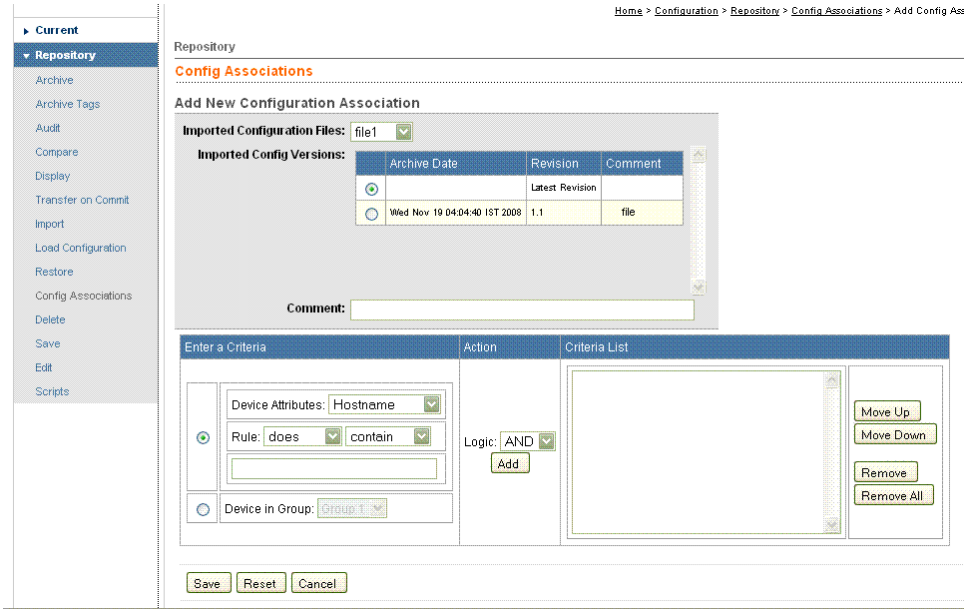
Table 17: List of buttons on the List of Configuration Associations Page

Buttons	Description
Delete	Deletes the selected configuration file associations.
Add	Displays the Add New Configuration Association page where you can create a new configuration file association.
Reorder	Displays the Reorder Configuration Associations page where you can change the order of the configuration associations in the list.
Import	Displays the Import Config Associations page where you can import configuration associations from an external source.
Export	Exports the selected configuration file associations.

Creating and Editing a Configuration File Association

You can create a new configuration file association to the list of configuration associations. You can also edit an existing configuration file association.

Figure 7: Add New Configuration Association page



To add or edit a configuration file association, follow these steps:

1. In the JUNOScope main window, click Home > Configuration > Repository > Config Associations > Add Config Association. The Add New Configuration Association page appears. This page enables you to create a new configuration file association.

   To edit an existing configuration file association, click the Config Name of the configuration association in the list of configuration associations. This takes you to the Edit Configuration Association page where you can edit that configuration file association.

2. Select a configuration file from the Imported Configuration Files list. This list contains all the configuration files that were imported into JUNOScope.

3. Select the revision of the configuration file that JUNOScope returns to the device, from the Imported Config Versions table. This is the version of the configuration file that is returned to the device if the device attributes match the criteria of that configuration association. This table lists the Revision number as well as the date when the configuration file was last revised. The content in this table changes when a different configuration file is selected.

   If you select the Latest Revision option, JUNOScope always returns the last revised version of the configuration file that is, the dynamic latest. This option is selected by default.

   If you select a particular version number, JUNOScope always returns that version of the configuration file even if there are newer versions of that configuration file available.

4. In the Comment text box, type an optional descriptive comment about the configuration file association.

5. In the Enter a Criteria list, specify a rule by doing one of the following actions:

Table 18: Options in the Enter a Criteria List

Label	Description
Default	Select this option if you want JUNOScope to return a default configuration file if none of the device attributes match any of the criteria in the configuration associations. You cannot associate criteria to a configuration file that has been designated as the default configuration association.

Table 18: Options in the Enter a Criteria List *(continued)*

Label	Description
Device Attributes	Select this option to specify a set of rules that the returned configuration file must match to. To specify a rule, follow these steps: a. Select the parameter from the Device Attribute list. The options are Hostname, Model, OS Version, and Serial Number. b. Set a rule for the parameter by selecting a combination of the options from the two lists. The options for the first list are does, and does not. The options for the second list are contain, begin with, end with, and equal. This sets the condition for the selected parameter. c. Specify a value that the device attribute must match in order to satisfy the criteria.
Device in Group	Select this option if you want JUNOScope to return the associated configuration file if the requesting device belongs to a certain group. You can select the group from the list. (To set up a label or a group, see“Setting Up Labels” on page 83 and “Setting Up Groups” on page 67) The hostname is used to check if the device belongs to the selected group of devices.

6. In the Action list, select one of the two options in the Logic list and click Add to add the rule to the Criteria list.
   - Select AND if you want the device to match both the rules that are combined by AND. This is the default selection.
   - Select OR if you want the device to match one of the rules that are combined by OR.
7. You can move the rules in the Criteria list by selecting the rule you want to move and clicking one of these buttons:
   - Move Up — Moves the selected rule to one row above its current position.
   - Move Down — Moves the selected rule to one row below its current position.

   You can also remove rules from the Criteria list by selecting the rule and clicking Remove. Click Remove All to remove all the rules from the Criteria list.
8. Click Save to save the configuration file association. After saving the configuration association, the Config Associations page, which contains the list of configuration file associations is displayed

   The new configuration association gets added to the end of the list of configuration associations.

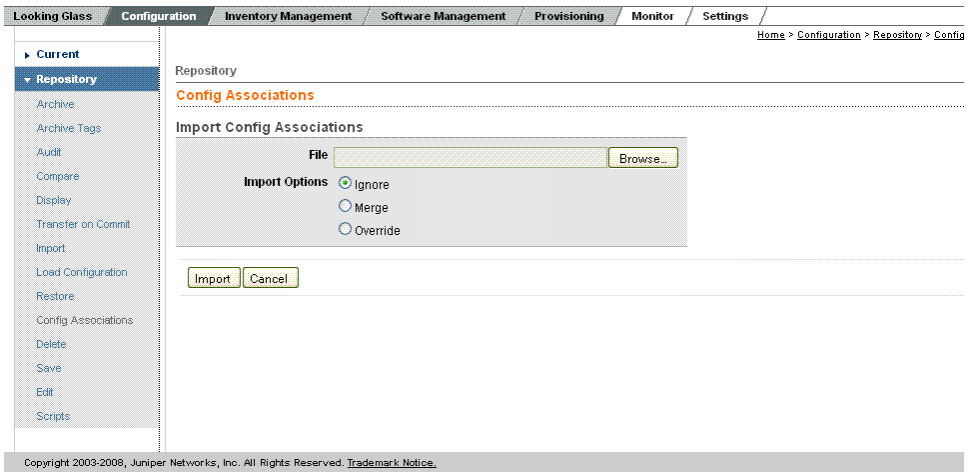
   Click Reset to restore all the field values to their default value. If you are editing a configuration association, then the field values change back to the last saved values of that configuration association.

Click Cancel to go back to the Config Associations page which contains the list of configuration file associations.

Importing a Configuration File Association

You can import configuration associations from an external source into JUNOScope using the Import Configuration Association feature.

Figure 8: Import Config Associations page



To import configuration associations into JUNOScope, follow these steps.

1. In the JUNOScope main window, click Configuration > Repository > Config Associations > Import. The Import Config Associations page is displayed. Click Browse... to open a dialog box from where you can select the XML file that contains the details of the configuration association that you want to import.
2. Select the Override option to solve issues that may arise when you try to import a configuration association that already exists in the server. The Override option removes all the existing records of the configuration association which you are trying to import.
3. Click Import to import the configuration association into JUNOScope.

   Click Cancel to return to the List of Configuration Associations page.

Changing the Order of the Configuration File Associations

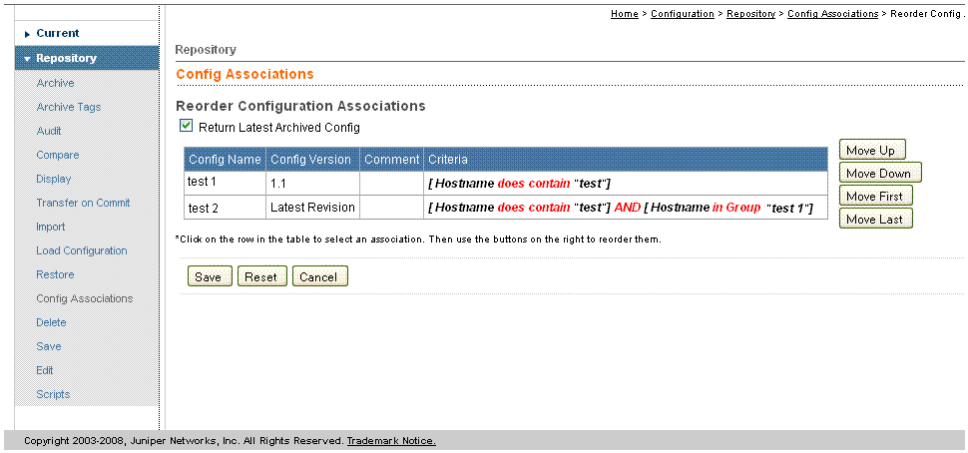
When JUNOScope receives a request from a device, it starts comparing the device attributes with the criteria from the first configuration association in the list to the last configuration association, that is, the comparison is done from top to bottom. By reordering the list of configuration file associations, you can change the order in which the criteria are checked.

NOTE: The default configuration association is not displayed in the Reorder Config Associations page. The default configuration association is always the last configuration association listed in the server and this position cannot be changed. This is because JUNOScope returns the default configuration file only if the device attributes does not match the criteria specified in any of the configuration associations. Because the comparison is done from top to bottom, the default configuration file is always last on the list.

To change the order of the configuration file associations, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Config Associations > Reorder Config Associations. The Reorder Config Associations page is displayed. This page contains the list of the configuration associations and enables you to change the order of the configuration file associations.

Figure 9: Reorder Config Associations page



2. Click the row to select the configuration association you want to move. The selected association will be highlighted in grey. The entire row gets highlighted in blue whenever you move the mouse over any part of the row.
3. To move the selected row, click one of these buttons:
   - Move Up — Moves the selected row to one row above its current position.
   - Move Down — Moves the selected row to one row below its current position.
   - Move First — Moves the selected row to the top of the list of configuration associations.
   - Move Last — Moves the selected row to the bottom of the list of configuration associations.
4. Click Save to save the order of the configuration associations. After saving the order, the List of Configuration Associations page is displayed.

   Click Reset to restore the original order of configuration associations.

Click Cancel to go back to the List of Configuration Associations page without saving the changes to the order of configuration associations.

NOTE: You can archive configurations for a device in JUNOScope using the Archive feature. (See "Archiving and Manipulating Device Configurations" on page 193) Every modification to the configuration file is saved as a new version and is archived in the server.

Select the Return Latest Archived Config checkbox if you want JUNOScope to return the latest configuration file that was archived in the server for that device. This option is selected by default. When the device sends a request, JUNOScope returns the latest configuration file that is archived in the server for that device. If JUNOScope doesn't have a configuration file archived for that device, then it starts comparing the device attributes with the criteria.

If the Return Latest Archived Config checkbox is not selected, JUNOScope will directly start its comparison of the device attributes with the criteria in the configuration associations.

Deleting a Configuration File Association

You can delete configuration file associations from the list of configuration associations.

To delete one or more configuration file associations from the list, follow these steps:

1. In the JUNOScope main window, click Configuration > Repository > Config Associations. The Config Associations page is displayed with the list of configuration file associations.
2. Select the configuration associations you want to delete by checking the box next to the configuration file association name.
3. Click Delete to delete the configuration file associations.

Part 5
Configuring Pseudowires

Chapter 25

Provisioning Pseudowires

Pseudowire is the emulation of native services (such as TDM and ATM) over packet-switched services (such as IP and MPLS) networks. When you configure a pseudowire, the packets travel over a PSN tunnel, which is either a Multiprotocol Label Switching (MPLS) or a generic routing encapsulation (GRE) tunnel.

Before you can provision pseudowires, you must:

- Install IPBackhaul Manager license.
- Configure IP address for Io0.0 Interface of the device
- Configure NETCONF over SSH access methods
- Configure MPLS or GRE tunnels.

This chapter gives an overview of the Provisioning tab, and explains the configurations required of provisioning pseudowires.

This chapter includes the following topics:

The Provisioning Tab

NOTE: To access the Provisioning tab, you must have a valid IP Backhaul Manager license. The Provisioning tab appears disabled if you do not have a valid IP Blackhaul Manager license installed.

The Provisioning tab contains the following options:

- MPLS/GRE Tunnels—Enables you to configure LSP paths and protocols, and to provision MPLS/GRE tunnel. For more information about the MPLS/GRE Tunnels options, see “Configuring MPLS and GRE Tunnels” on page 282.
- Pseudowires—Enables you to add, export, import, or delete pseudowires templates, provision pseudowires, and filter pseudowires. For more information about the Pseudowires, see “Provisioning Pseudowires” on page 298.

Configuring MPLS and GRE Tunnels

The MPLS/GRE Tunnels option on the Provisioning tab of JUNOScope enables you to configure the MPLS/GRE tunnels for pseudowire provisioning.

Configuring MPLS/GRE Tunnels involves three tasks:

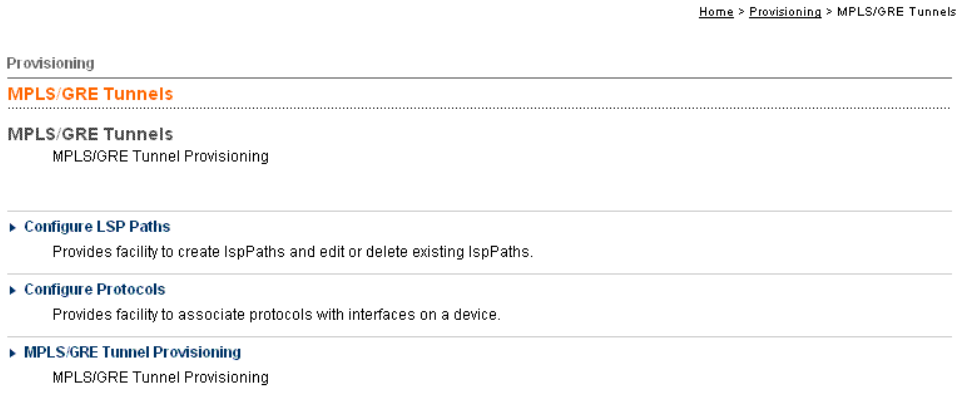
1. Configuring LSP Paths (optional). See “Configuring LSP Paths” on page 282.
2. Configuring Protocols. See “Configuring Protocols” on page 286.
3. Provisioning MPLS/GRE Tunnels. See “Provisioning MPLS and GRE Tunnels” on page 292.

Configuring LSP Paths

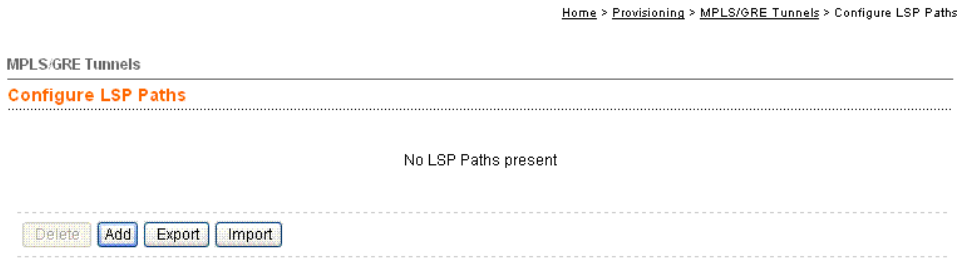
LSP paths consist of ordered set of nodes through which MPLS packets travel. You can specify the LSP paths for RSVP tunnel if you want to use static LSP paths. .

To add LSP Paths, follow these steps:

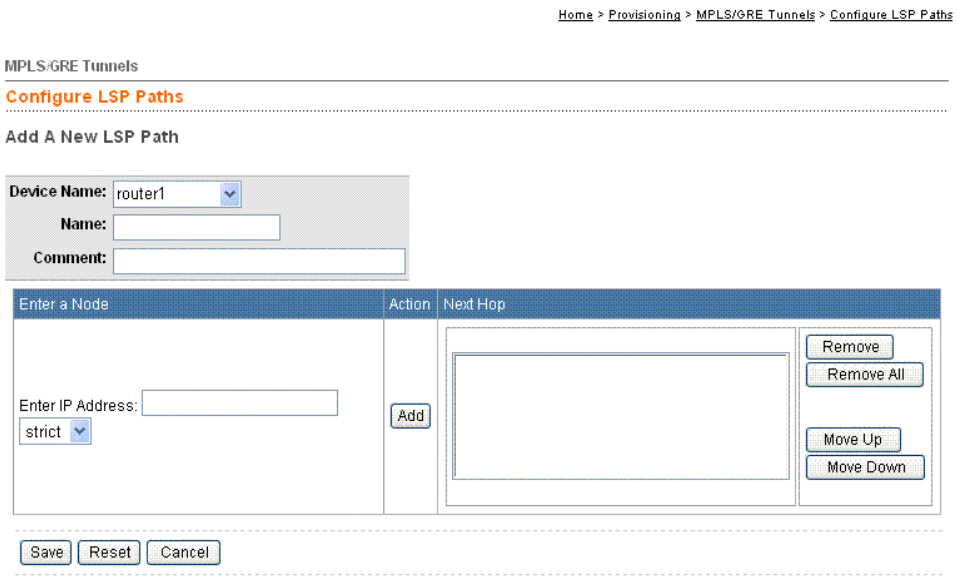
1. In the JUNOScope main window, click Provisioning > MPLS/GRE Tunnels. The MPLS/GRE Tunnels dialog box appears.



2. Click Configure LSP Paths. The Configure LSP Paths dialog box appears.



3. Click Add to add a new path. ,The Configure LSP Paths Add A New LSP Path dialog appears.



4. From the Device Name drop-down, select the name of the device to which the LSP Path will be applied.
5. In the Name text box, enter a name for the LSP Path. This field is manadatory., .
6. In the Comment text box, enter a description for the LSP Path. This field is optional..
7. In the Enter IP Address text box, enter the IP address of the next hop node, and choose one of the following status from the drop-down list adjacent to the Enter IP Address text box:
   - Strict—Indicates that the next hop must be adjacent.
   - Loose—Indicate that the next hop is not necessarily adjacent.
8. Click Add to add the new node to the Path.
9. Repeat Steps 6 through 8 to add multiple nodes.
10. Use the Move Up and Move Down buttons to specify the sequence of nodes in the path.
11. To remove a node from the Path, select a node and click Remove. You can click Remove All to remove all the nodes that you have added.
12. Click Save to save the path information

NOTE: When you click Save, the path is saved only in the JUNOScope database. The configuration for the path will be pushed to device only during Provisioning of MPLS/GRE tunnels

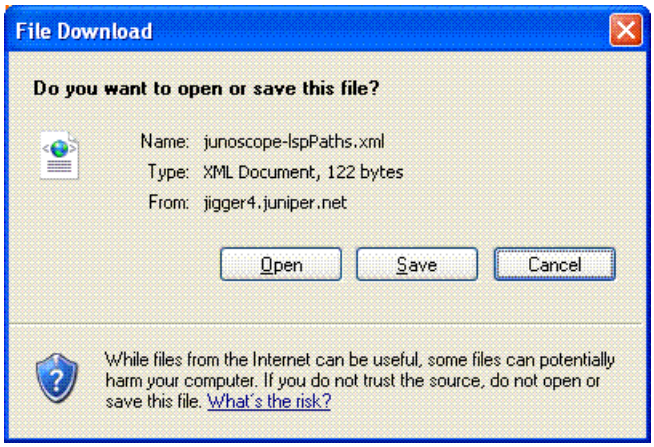
13. Click Reset to go back to the last saved configuration for the path.

Exporting LSP Paths

You can export LSP path information to xml format.

To export information about the LSP Paths configured on your device, follow these steps

1. Click Export from the Configure LSP Paths dialog box.. The Save File dialog box appears. JUNOScope creates an xml file that contains information about all the paths configured on the server.



2. Save the xml file to a location of your choice.

Importing LSP Paths

You can import LSP Paths which you have earlier exported and saved.

To import an LSP Path, follow these steps:

1. Click Import in the Configure LSP Paths dialog box. The Import LSP Paths dialog box appears.

2. Click Browse. The Choose File dialog box appears.
3. Navigate to the location of the file that you want to import and choose the file to be imported.
4. Select one of the following option buttons:
   - Ignore—(Default) If there are conflicting Path names in the imported record and an existing record on the JUNOScope server, the existing record on the JUNOScope server takes precedence over the imported record. The imported record is ignored and the existing record is retained without any change. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If the same Path name is present in the existing record on the JUNOScope server and in the imported record, the imported record is merged with the existing record and the path information is augmented as necessary. In such cases, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All imported records are inserted after deleting the existing records on the JUNOSCope server. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes to continue. If you want to retain the existing records on the JUNOScope server, select. No.
5. Click Import.

Deleting LSP Paths

To delete LSP paths from the JUNOScope server, follow these steps:

- In the JUNOScope main window, click Provisioning > MPLS/GRE Tunnels. The MPLS/GRE Tunnels dialog box appears.
- Click Configure LSP Paths. The Configure LSP Paths dialog box appears.

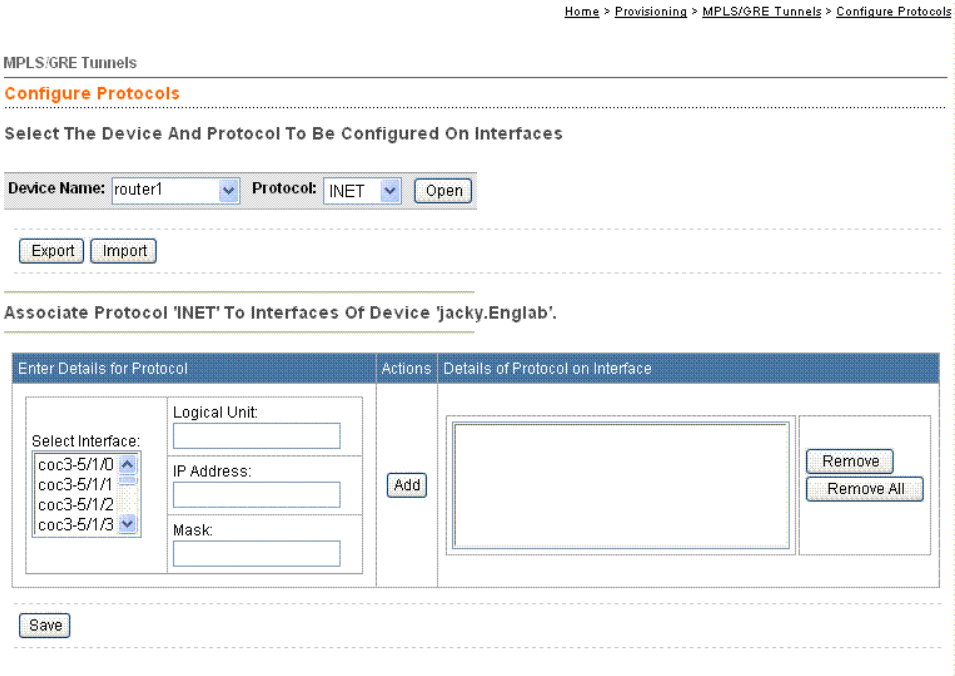
- Check the check box corresponding to the LSP Paths that you want to delete.
- Click Delete.

Configuring Protocols

You can specify the protocols to be configured on each interface.

To configure a protocol, follow these steps:

1. Click Configure Protocols under MPLS/GRE Tunnels. The Configure Protocols dialog box appears.



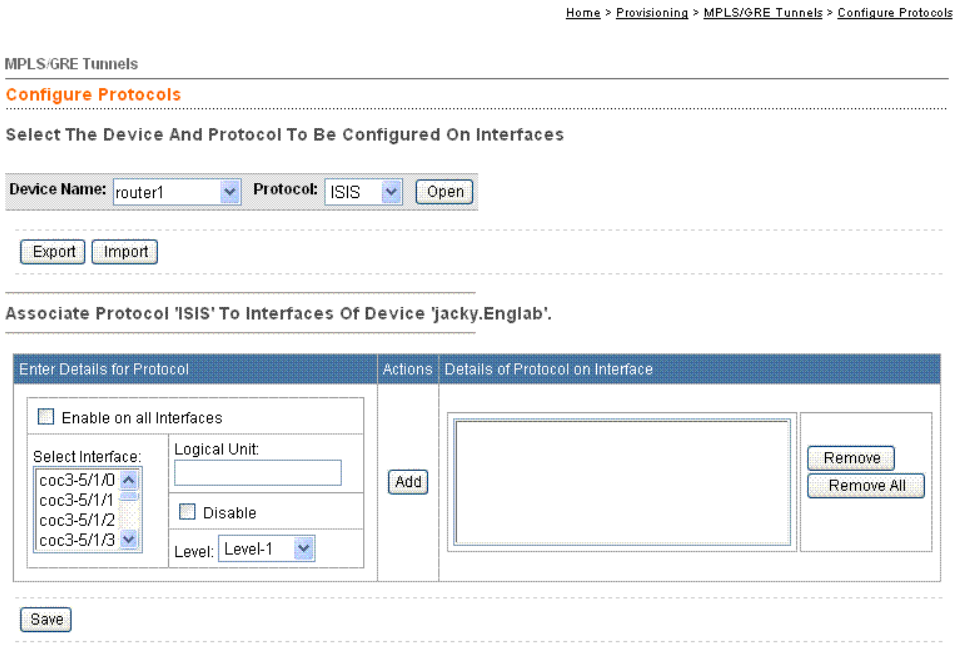
2. From the Device Name drop-down, select the name of the device on which you want to configure the protocols.
3. From the Protocols drop-down, select one of the following: ISIS, MPLS, LDP, RSVP, OSPF, INET.
4. Click Open. Depending on the protocol selected, parameters specific to the protocol appear. The parameters for specific interfaces are described in the following sections.

NOTE: For all protocols except INET, you can select the Enable on all Interfaces check box. For protocol-specific parameters, see the following sections.

5. Click Save to save the interfaces to be used during MPLS/GRE Tunnel Provisioning.

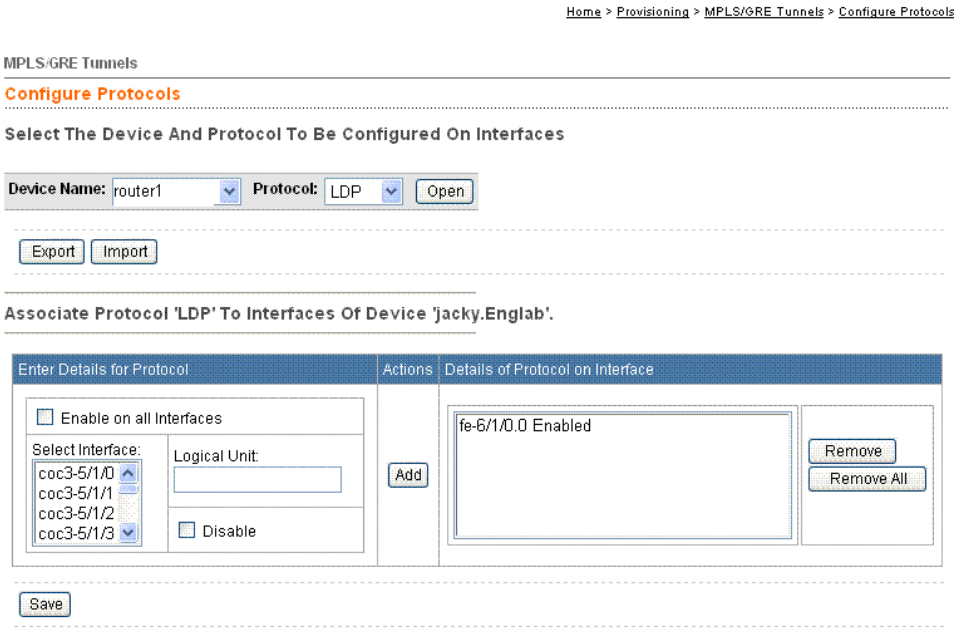
NOTE: When you click Save, the protocol information is saved to the JUNOScope database. Actual configuration will be pushed to device only during provisioning of MPLS/GRE tunnels.

For IS-IS



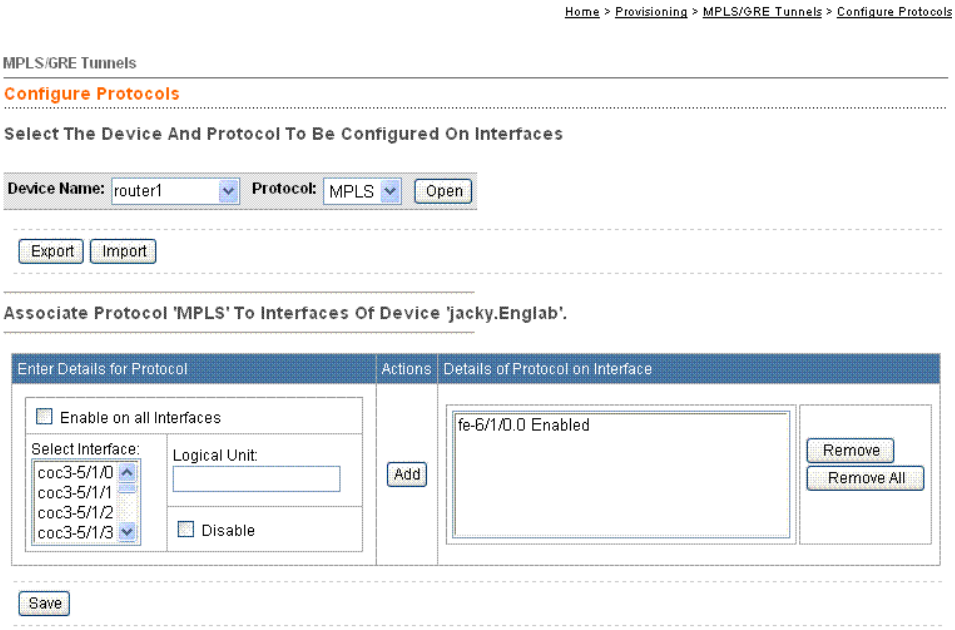
1. Select the interface(s).
2. Specify the Logical Unit.
3. Click Disable if you want to disable IS-IS on the selected interface.
4. Select the Level from the drop-down.
5. Click Add.
6. To remove an interface from the configuration, select an interface and click Remove. You can click Remove All to remove all the interfaces on which the protocol is configured.

For LDP



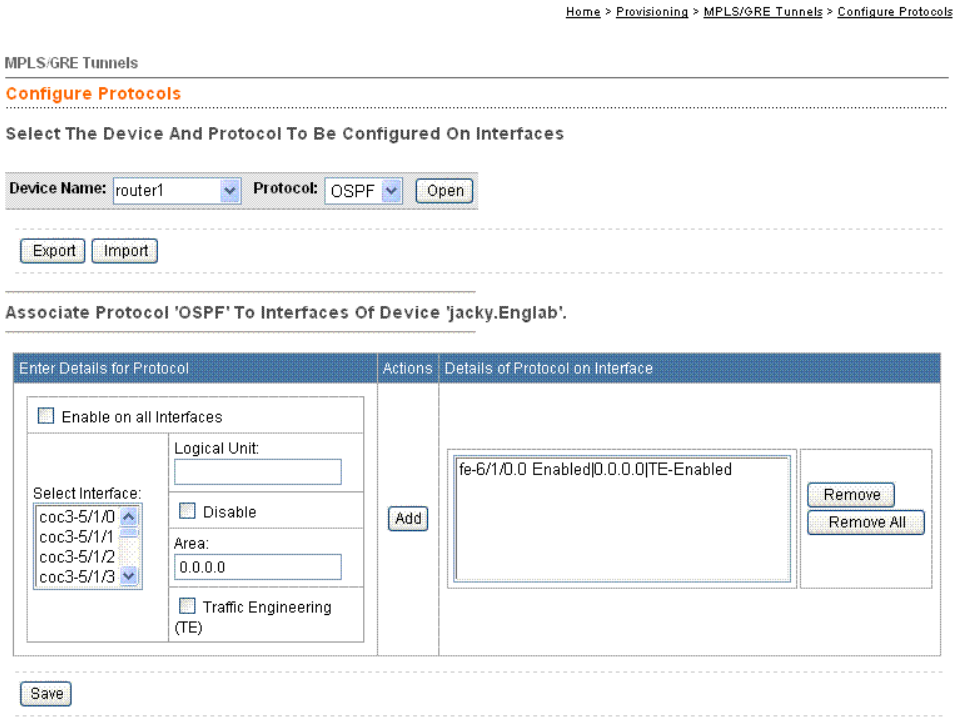
1. Select the interface from the list of interfaces.
2. Specify the Logical Unit.
3. Check Disable check box if you want to disable LDP on the selected interface.
4. Click Add.
5. To remove an interface from the configuration, select an interface and click Remove. You can click Remove All to remove all the interfaces on which the protocol is configured.

For MPLS



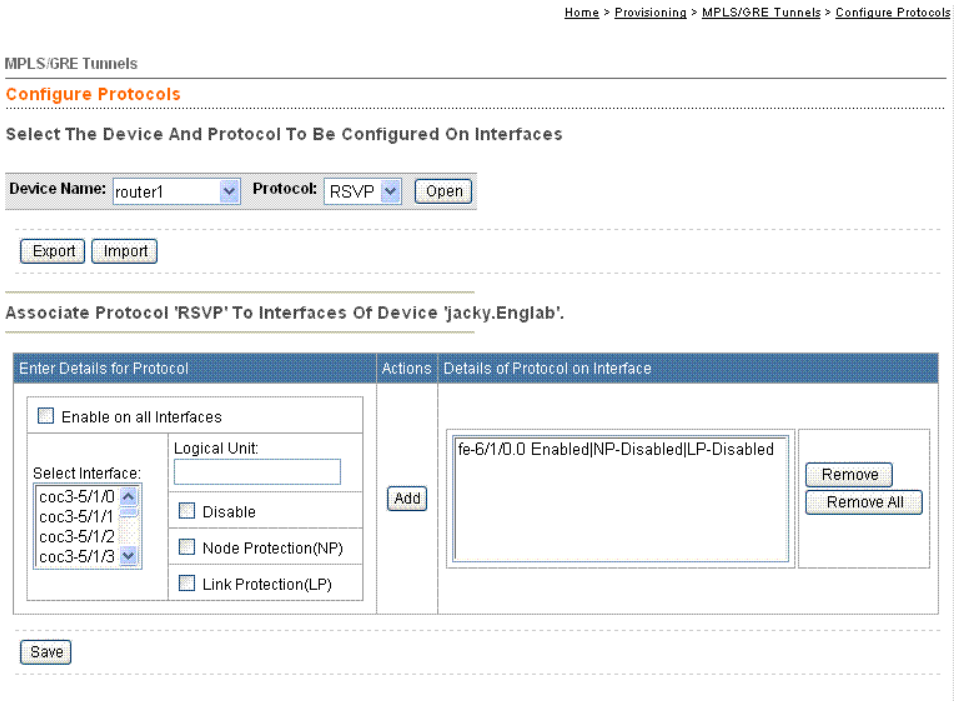
1. Select the interface(s).
2. Specify the Logical Unit.
3. Check Disable check box to disable MPLS on the selected interface.
4. Click Add.
5. To remove an interface from the configuration, select an interface and click Remove. You can click Remove All to remove all the interfaces on which the protocol is configured.

For OSPF



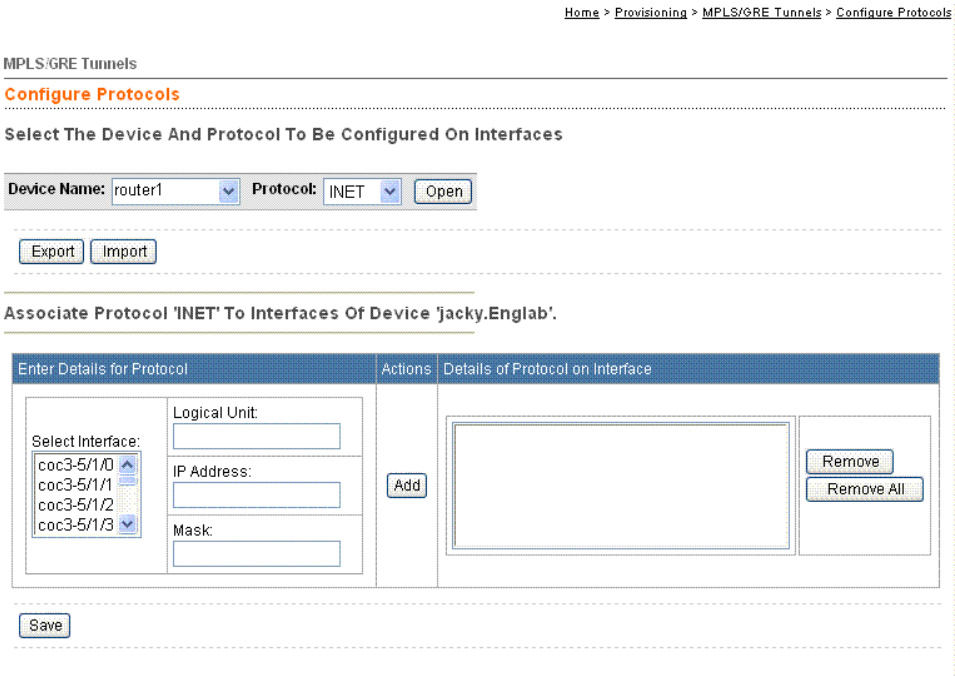
1. Select the interface(s).
2. Specify the Logical Unit. You can select the Disable check box.
3. Specify the Area.
4. Select the Traffic Engineering (TE) check box to enable MPLS TE on the interface.
5. Click Add.
6. To remove an interface from the configuration, select an interface and click Remove. You can click Remove All to remove all the interfaces on which the protocol is configured.

For RSVP



1. Select the interface from the list of interfaces.
2. Specify the Logical Unit. You can select the Disable check box.
3. Check Disable check box if you want to disable RSVP on the selected interface.
4. Click Add.
5. To remove an interface from the configuration, select an interface and click Remove. You can click Remove All to remove all the interfaces on which the protocol is configured.

For INET



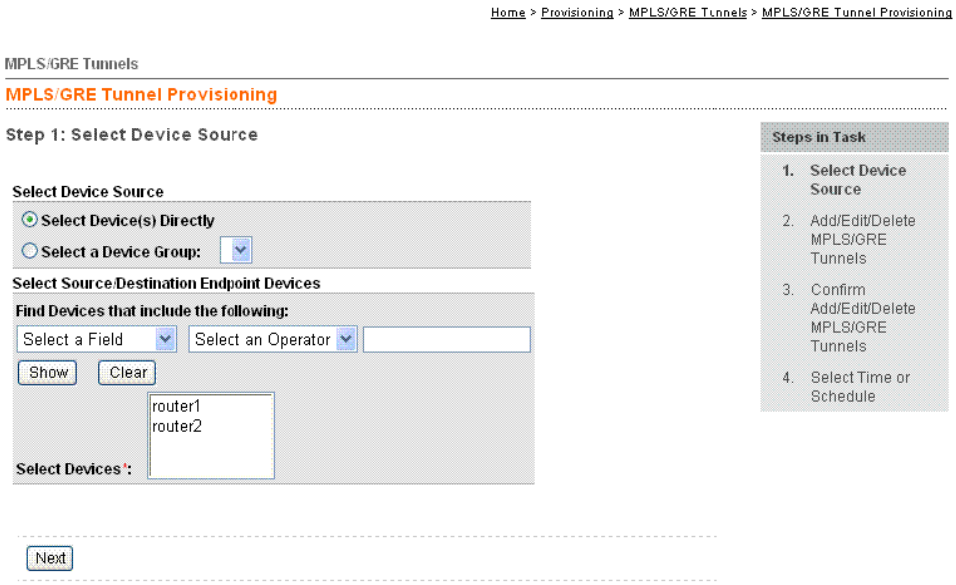
1. Select the interface(s).
2. Specify the Logical Unit.
3. Check the Disable check box if you want to disable INET on the selected interface.
4. Specify the IP Address and Numeric Subnet Mask (0–32).
5. Click Add.
6. To remove an interface from the configuration, select an interface and click Remove. You can click Remove All to remove all the interfaces on which the protocol is configured.

Provisioning MPLS and GRE Tunnels

JUNOScope supports the following types of tunnels: MPLS RSVP tunnel; MPLS LDP tunnel; and GRE tunnel The MPLS/GRE Tunnel Provisioning proceeds in four steps as described in the following sections.

Step1: Select the source and destination devices.

In this step you choose the device source and destination endpoint devices.



You can select device source by selecting either a group or by selecting devices directly You can choose one of the device groups from a list of device groups already created.

Device groups can be created by grouping devices dynamically based on one of the following filtering criteria: location, name, model, or hostname. Alternatively, devices can be grouped using static labels. When you have selected a device group, all the devices in that group are listed in the Select Devices list.

You can also directly select devices that are already added to JUNOScope from the Select Devices list

To select a device source

1. Select an option button to specify whether you wish to Select Devices Directly or Select a Device Group.
2. If you choose to select devices directly, you can search for devices on the following criteria under Find a device that includes the following:
   - From the Select a Field drop-down list, select one of the following options: Device Name, Device Hostname, Model, Location, and Comment.
   - From the Select an Operator drop-down list, select one of the following options: Contains, Does not Contain, Starts With, Ends with, and Equals.
   - Enter a string and click View to display a list of devices that meet the criteria specified in the preceding steps.

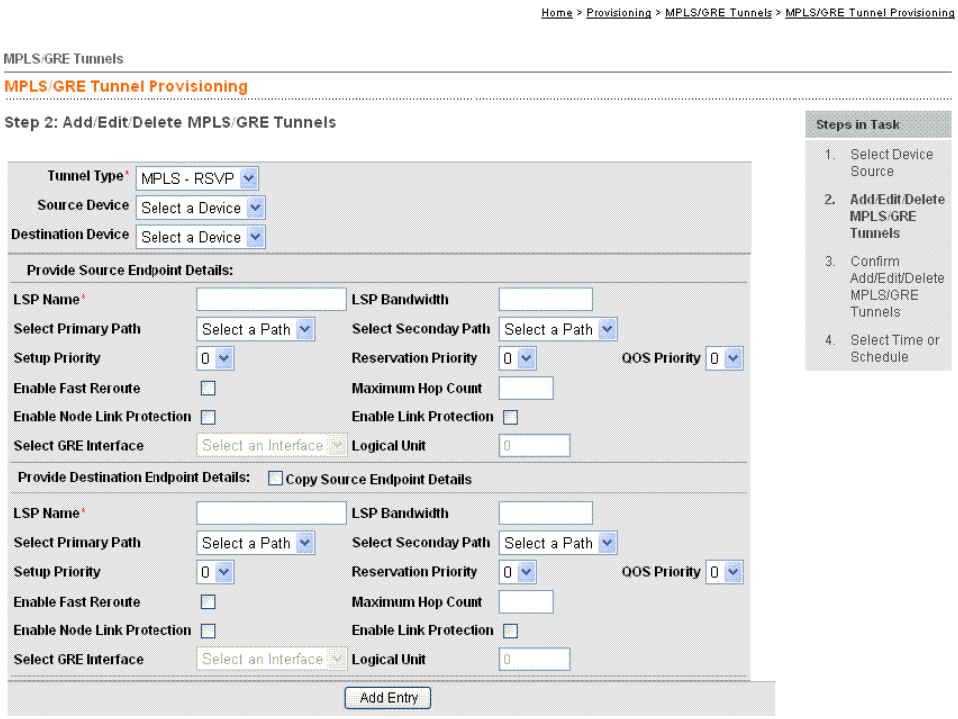
   For example, to list devices that have device names starting with J, select Device Name from the Select Field drop-down list, Starts With from the Select an

Operator drop-down list, enter J in the text box, and click View. All devices that have device names starting with J will be listed in the Select Devices list.

3. Select at least two Devices and click Next.

Step 2: Add/Edit/Delete Tunnel

In this step, you can provide details about the tunnel.



Three types of tunnel are supported. These are: MPLS-RSVP, MPLS-LDP, GRE

To Add/Edit/Delete Tunnel:

1. From the Tunnel Type drop-down, select a tunnel type. The available values are: MPLS-RSVP, MPLS-LDP, and GRE.
2. From the Source Device and Destination Device drop-down lists, select the source and device names.
3. Under Provide Source Endpoint Details:
   1. Specify an LSP Name and LSP Bandwidth.

NOTE: LSP Name is mandatory for MPLS-RSVP tunnel type.

   2. If you want the LSP Name specified in the preceding step to use a static LSP path, select an LSP Path to be used as the Primary path for the LSP Name

entered. This field is required only if Tunnel type selected is MPLS-RSVP. For MPLS-LDP and GRE tunnel types, this field is disabled.

3. If you want the LSP Name specified in step 1 to use a static LSP path, ,select an LSP Path to be used as the Secondary path for the LSP Name entered. This should be different from the Primary LSP Path.

   This field is required only if Tunnel type selected is MPLS-RSVP. For MPLS-LDP and GRE tunnel types, this field is disabled.

NOTE: LSP Primary Path and LSP Secondary Path cannot be the same.

---

4. From the respective drop-down list, select the Setup Priority, Reservation Priority, and the QoS Priority. These fields are available only when the selected tunnel type is MPLS-RSVP. For MPLS-LDP and GRE, tunnel types, these drop-down lists appear disabled.
5. Check the Enable Fast Reroute check box to enable fast reroute.

   This field is used only if Tunnel type selected is MPLS-RSVP Otherwise, this field appears disabled.
6. Specify the Reroute Bandwidth, which is the bandwidth reserved for reroute

   This field is enabled only if Tunnel Type is MPLS-RSVP and the Enable Fast Reroute check box is checked. Otherwise this field is disabled.
7. Specify the Hop Limit, which is the maximum number of hops.

   This field is enabled only if the tunnel type is MPLS-RSVP and Enable Fast Reroute check box is selected. Otherwise this field is disabled.
8. Select the corresponding check boxes, if you wish to, Enable Node Link Protection and Enable Link Protection. These check boxes are available only if the tunnel type is MPLS-RSVP. Otherwise, these are disabled.
9. Select the GRE Interface, if the tunnel type is GRE, from the drop-down.
10. Specify the Logical Unit for tunnel interface or software tunnel interface.

    This field is required only when tunnel type selected is GRE. For MPLS-RSVP and MPLS-LDP this field is disabled.

4. Repeat step 3 and all the substeps for the Device End Point, under Provide Destination Endpoint Details. Alternatively, click the Copy Source Endpoint Details to use the same settings as the source end point for the destination end point.
5. Click Add Entry to add a record in the list area. For newly created records, the state is shown as New whereas for edited records the state is shown as Modified,
6. Do one of the following:

- Click Add—To add a new record.
- Select an existing record and click Edit—To edit an existing record.
- Select an existing record and click Copy—To copy an existing record.
- Select an existing record and click Delete—To delete an existing record.
- Select an existing record and click Force Deploy—To modify a record even though no changes have been made. You can use this option to to push the configuration details to the devices, without making modifications to it, if you are editing the configuration

7. Click Next to go to Step 3 of the wizard or click Previous to go to Step 1 of the wizard.

The tabular area at the bottom of the window displays all the tunnels between devices that are selected in Step 1 of the wizard.

The following information is presented in the table:

- State

  State reflects the state of the record, namely:

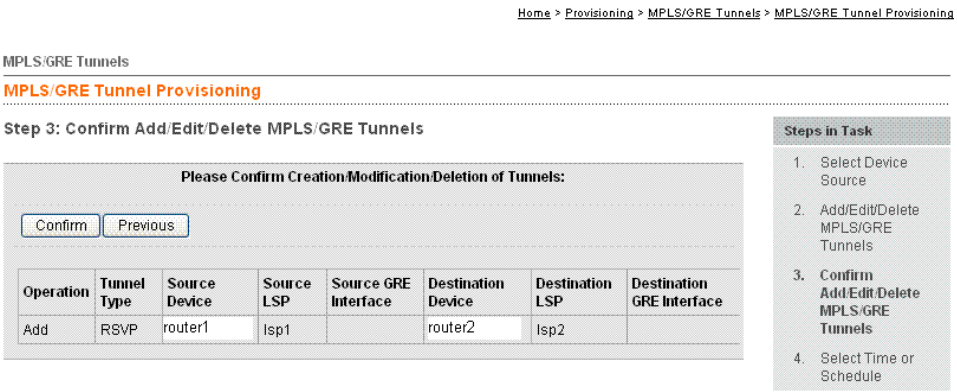
  - New: If a record is newly added.
  - Modified: If a record is modified.
  - Unchanged: If a record is not modified.

NOTE: If multiple users are simultaneously accessing this wizard, each user will have different working records and changes in records will be stored at session level.

- Tunnel Type
- Source Device
- Source LSP
- Source GRE Interface
- Destination Device
- Destination LSP
- Destination GRE Interface

Step 3: Confirm Tunnel selections

In this step you confirm the creation, deletion, or modification of the Tunnel Parameters that you selected in Step 2.

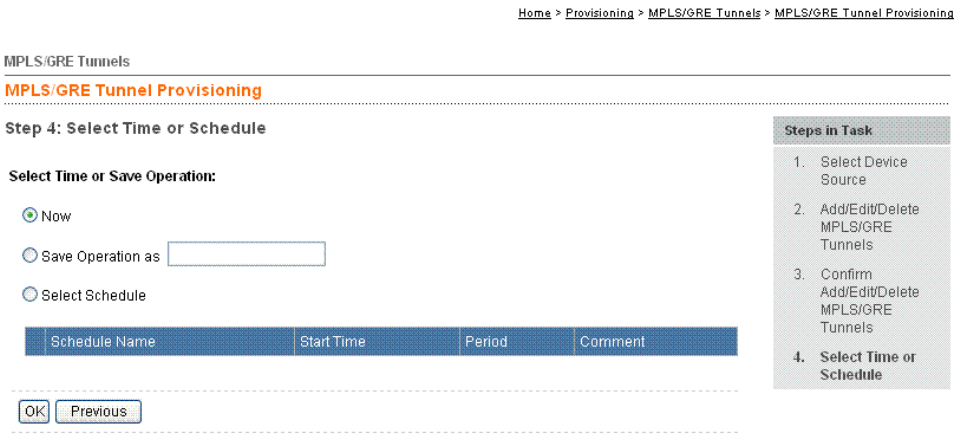


To confirm Tunnel selections:

1. Click Confirm to go to Step 4 of the wizard (Provision Tunnels).
2. Click Previous to go to Step 2 of the wizard (Add/Edit/Delete Tunnels).

Step 4: Provision MPLS/GRE Tunnels

In this step configurations are generated for MPLS/GRE tunnels created in step 3 and are pushed to devices.



To provision MPLS/GRE Tunnels:

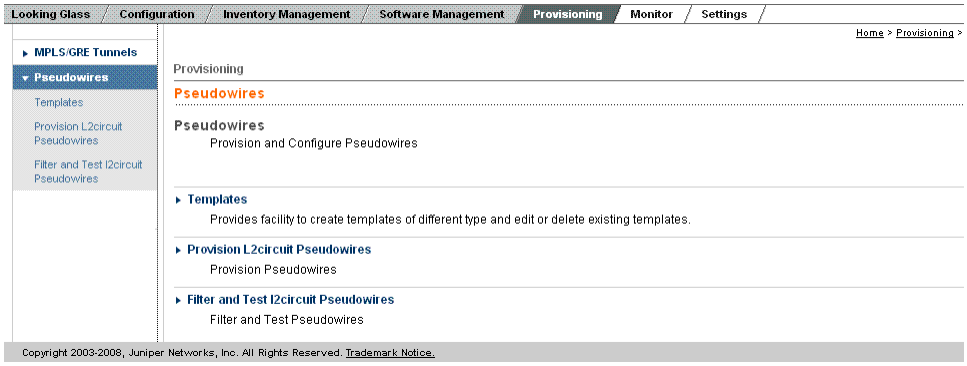
1. Select the Now radio button to push the configuration to the devices immediately.
2. Select the save Operation As button radio button and provide a name for the operation: the configuration can be saved as a named operation.
3. Select the Schedule radio button to select a schedule. The configurations will be pushed at the scheduled time.

NOTE: The schedule can be chosen from those defined in Settings. See Settings

Provisioning Pseudowires

A pseudowire is a circuit defined by two end point devices on which legacy traffic can be transported over IP/MPLS network. Pseudowire provisioning is the process of creating, modifying or deleting pseudowires between end points and pushing the configurations corresponding to the pseudowire to the devices. JUNOScope supports provisioning of LDP-based Layer 2 Circuit pseudowires only.

Figure 10: Provisioning Pseudowires Page



Pseudowire provisioning involves the following steps:

1. Creating templates for pseudowires
2. Selecting Device Source and Source/Destination Endpoint devices
3. Creating, modifying, or deleting links (pseudowires) between end points
4. Confirming Selections
5. Generating configuration for pseudowires generated in step 2 and provision pseudowires by pushing configurations generated in step3 to boxes
6. Filtering, viewing, and testing pseudowires

Pseudowire Template Wizard

The pseudowire template wizard enables users to create, edit, or delete pseudowire templates for:

1. ATM

NOTE: ATM pseudowires supported on JUNOS devices are for ATM-II PICs.

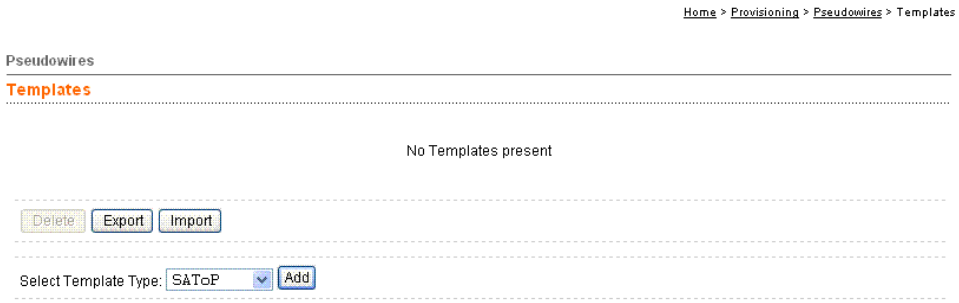
2. Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)

3. Ethernet

A template is a set of parameters needed for provisioning pseudowires. .

Pseudowire Templates List

When you click Pseudowire Templates, the template list appears.



From the Pseudowires Templates window, you can:

1. Add a new template. See “Adding and Editing Pseudowire Templates” on page 299.
2. Delete an existing template.
3. Edit a an existing template.
4. Export or import templates.

Adding and Editing Pseudowire Templates

To add or edit a pseudowire template

1. From Pseudowires, click Templates.
2. Select a pseudowire type and click Add.
3. Edit the parameters listed in Table 19 on page 299.
4. Click Save.

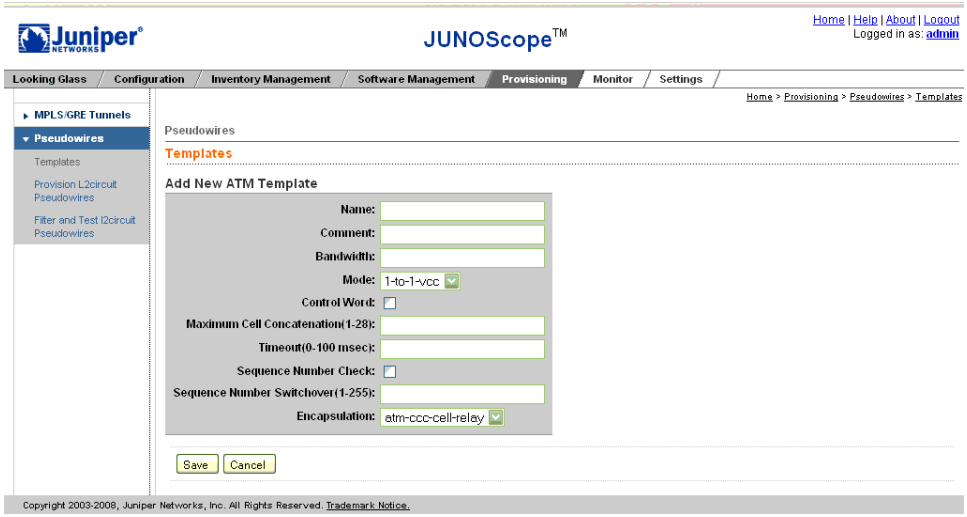
Table 19: Pseudowire Template Parameters

Parameter	Description
Common Parameters	
Name	A unique label for the Pseudowire Template
Type	Type of Pseudowires. The following three types are supported: TDM (SAToP), ATM, and Ethernet
Comment	

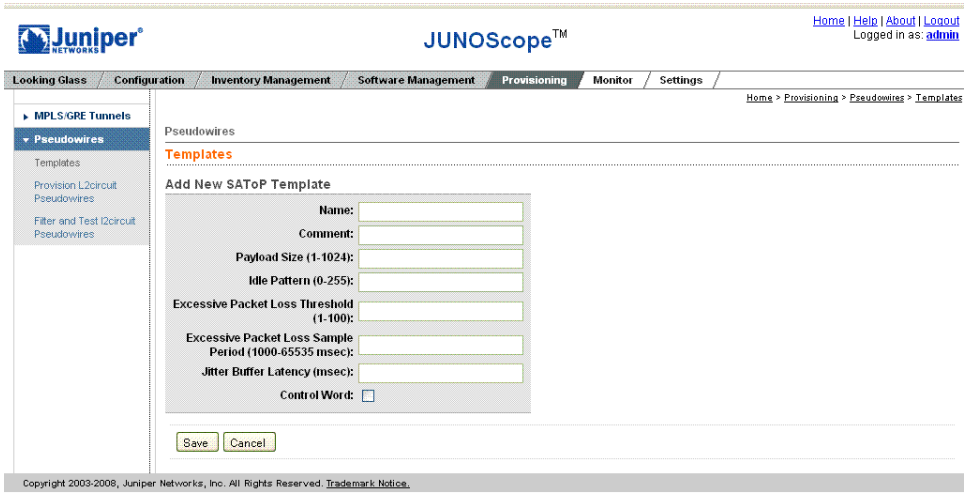
Table 19: Pseudowire Template Parameters *(continued)*

Parameter	Description
Control Word check box	Add a control word to the layer 2 encapsulation for the pseudowire
Parameters for ATM and Ethernet	
Encapsulation	Available values for ATM are atm-ccc-cell-relay and atm-ccc-vc-mux Available values for Ethernet are ethernet-ccc, vlan-ccc, and extended-vlan-ccc
Bandwidth	Bandwidth available for the pseudowire
Parameters for SAToP	
Payload size	Allowed range is 1 to 1024
Idle pattern	Allowed range is 0 to 255
Excessive packet loss threshold	Allowed range is 1 to 100
Excessive packet loss sample period	Allowed range is 1000 to 65535 milliseconds.
Jitter buffer latency	Specified in milliseconds.
Parameters for ATM	
Mode	Allowed options are 1–to-1–vcc, n–to-1-vcc, 1–to-1–vpc, n-to-1-vpc, aal5–pdu and aal5–sdu
Maximum Cell Concatenation	The maximum number of ATM cells that can be concatenated before the packet switched network (PSN) packet is sent out.
Timeout	The maximum time that the device should wait for the specified number of ATM cells to arrive for concatenation. If the specified number of ATM cells have not arrived in the specified time period, the device concatenates the ATM cells that have arrived and sends out the PSN packet.
Sequence Number Check	Allowed values are enable and disable
Sequence Number Switchover	Allowed values are enable and disable

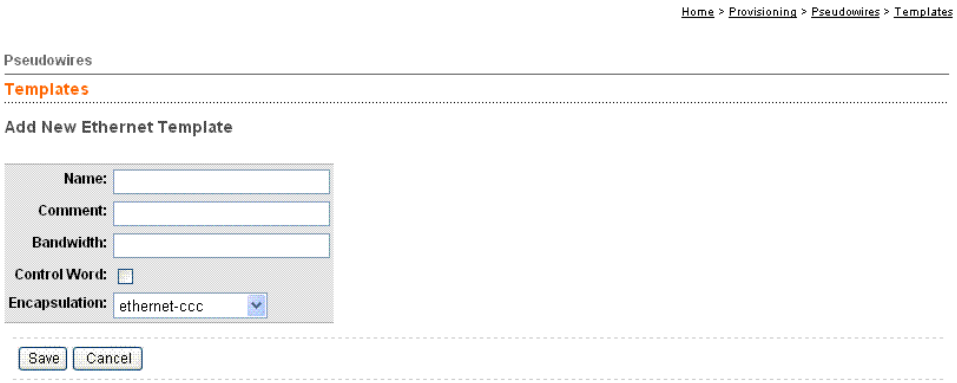
ATM Pseudowire Template



TDM (SAToP) Pseudowire Template



Ethernet Pseudowire Template

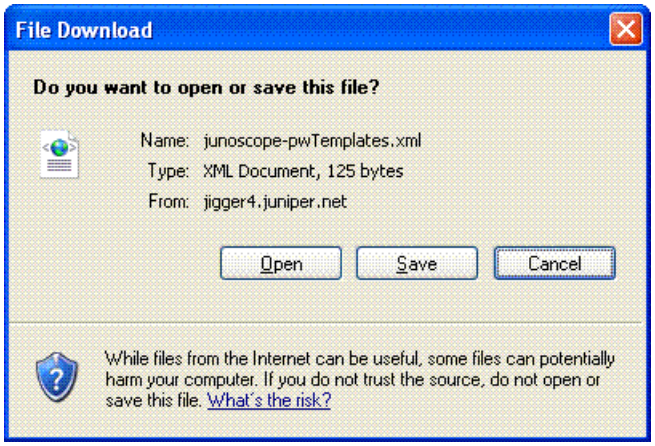


Exporting Pseudowire Templates

You can export pseudowire templates in xml format.

To export Pseudowire Templates

1. Click Export. The Save File dialog box appears. All the pseudowire templates are exported into an xml file.



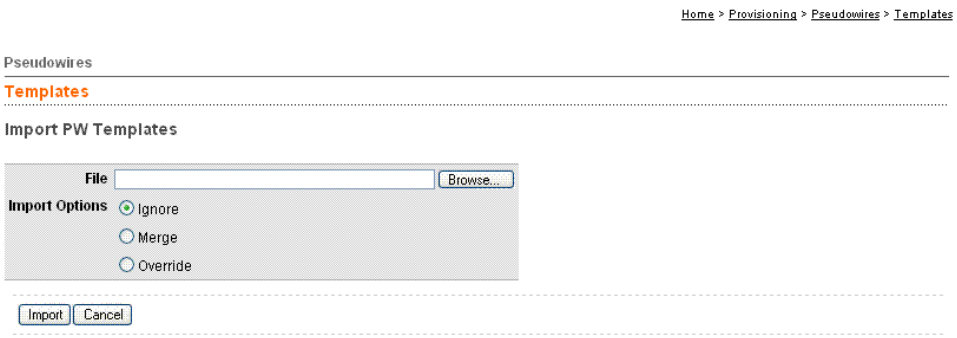
2. Click Save. The Save File dialog box appears. Save the file to a location of your choice.

Importing Pseudowire Templates

You can import a pseudowire template that you have earlier exported and saved.

To import Pseudowire Templates

1. Click Import in the Pseudowire Templates dialog box. The Import PW Templates dialog box appears.



2. Click Browse… and select the file you wish to import.
3. Select one of the option buttons: Ignore; Merge; Override
   - Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
   - Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
   - Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.
4. Click Import.

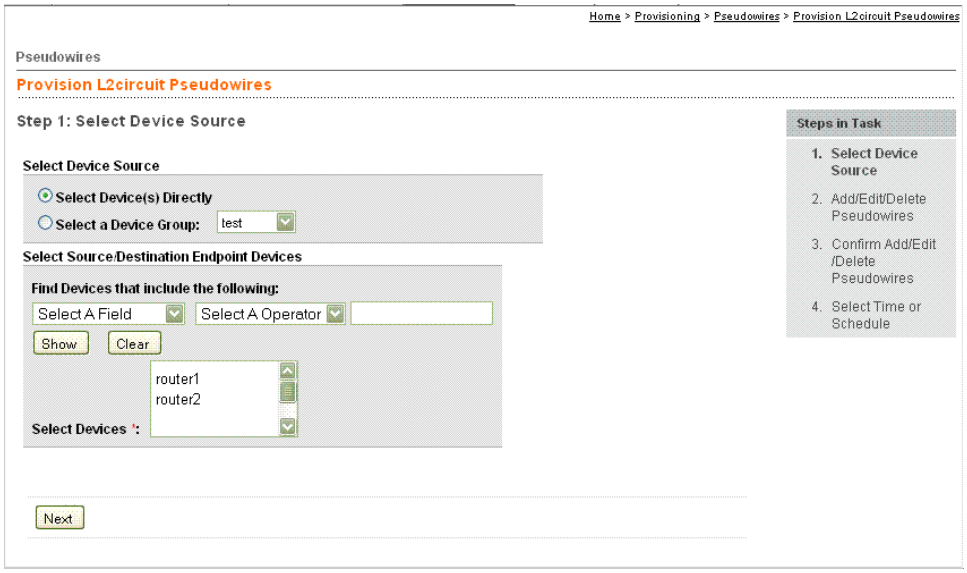
Provisioning Pseudowires

Pseudowire provisioning is the process of creating, modifying, or deleting pseudowires between end points and pushing the configurations corresponding to the pseudowire to the devices.

The pseudowire L2circuit provisioning wizard has four steps.

Step 1: Select the source and destination devices

In this step you choose the devices for source and destination of pseudowire.



You can select one of the device groups from a list of device groups already created by selecting the radio button "Select device groups". Alternatively, you can create device groups by grouping devices dynamically based on one of the following filtering criteria: location, name, hostname, or model

You can also directly select devices that are already added to JUNOScope by selecting the Select Devices Directly radio button. In this case, all devices that are added to JUNOScope are listed in the Select Devices list so that you can choose the devices from the list.

To select source and destination devices:

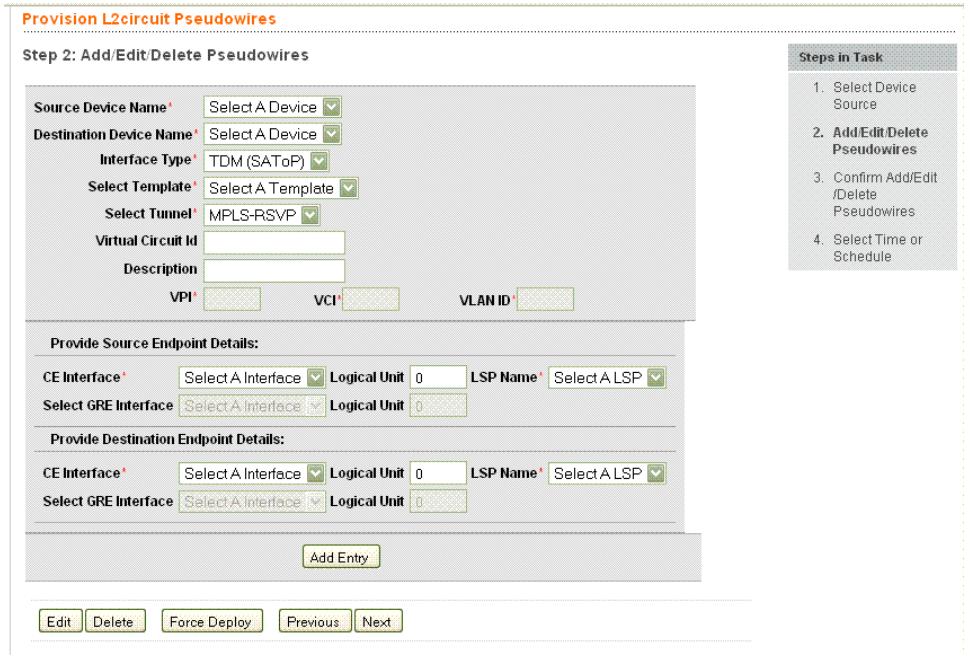
1. Select an option button to specify whether you wish to Select Devices Directly or Select a Device Group.
2. If you choose to select devices directly, you can either select the devices from the Select Devices list or filter the list of devices to generate a subset of devices based on the criterion of your choice. To filter the list of devices:
    1. From the Select a Field drop-down list, select one of the following options: Device Name, Device Hostname, Model, Location, and Comment.
    2. From the Select an Operator drop-down list, select one of the following options: Contains, Does not contain, Starts With, Ends With, and Equals.
    3. Enter a string and click View to display a list of devices that meet the criteria specified in the preceding steps.

    For example, to list devices that have device names starting with J, select Device Name from the Select Field drop-down list, Starts With from the Select an Operator drop-down list, enter J in the text box, and click View. All devices that have device names starting with J will be listed in the Select Devices list.

3. Click Next to go to Step 2 of the wizard.

Step2 Add/Edit/Delete Pseudowire

In this step you can create, modify, delete, or view pseudowires.



Pseudowires already provisioned or newly created for provisioning for the devices that are selected in step 2 of the wizard are shown at the bottom of wizard.

- You can select a pseudowire from the list and click Edit to modify the details. You can select a pseudowire from the list and click Delete to delete it.
- You can select a pseudowire from the list and click Force Deploy to redeploy the pseudowire configuration on devices without making any modifications to the pseudowire configuration

To add or modify a pseudowire:

1. Select the Source Device Name and Destination Device Name from the respective drop-downs.
2. Select and Interface Type. The options are: TDM (SAToP), ATM, and Ethernet
3. Select a Template and Select a Tunnel from the respective drop-downs. The templates in the drop-down depend on the interface type selected.
4. Specify the Virtual Circuit ID and provide a Description. The description is optional.

   If the Virtual Circuit ID is not specified, a Virtual Circuit ID is automatically generated for the pseudowire.

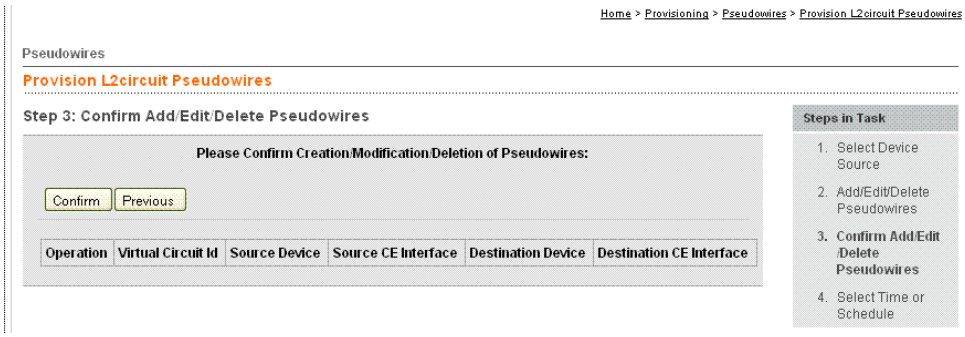
5. If the template type is ATM II, specify the VCI and VPI . These will be the same for both endpoints. If the interface type is not ATM, then these fields are disabled.
6. If the interface type is Ethernet, specify the VLAN ID. VLAN ID is the same for both endpoints. If the interface type is not Ethernet, then this field is disabled.
7. For the Source Endpoint and Destination Endpoint, specify the following:
    1. Device Name
    2. CE Interface: CE-facing interface. The drop-down lists the interfaces available for the endpoints specified.
    3. LSP Name: The drop-down list displays all LSPs configured on the endpoint devices that you have specified. LSP Name is mandatory if the selected end point is a BXOS device. LSP Name is optional if the end point is a JUNOS device.
    4. Logical Unit (number): The default value is 0. If you do not specify this, the system automatically assigns a unique logical unit based on the pseudowires that were already provisioned.
    5. If the pseudowire is to be provisioned over a GRE tunnel, select a GRE Interface and a Logical Unit for the interface.
8. Click Add Entry. The pseudowire is listed at the bottom of the wizard.

The table at the bottom of the wizard displays:

- State: State can be one of the following:
    - New: If the pseudowire is new.
    - Modified: If an exiting pseudowire is modified.
    - Unchanged: If an existing pseudowire is unchanged.
- Source Device Name
- Source CE Interface
- Destination Device Name
- Destination CE Interface
- Virtual Circuit ID

Step 3: Confirm Add/Edit/Delete Pseudowire selections

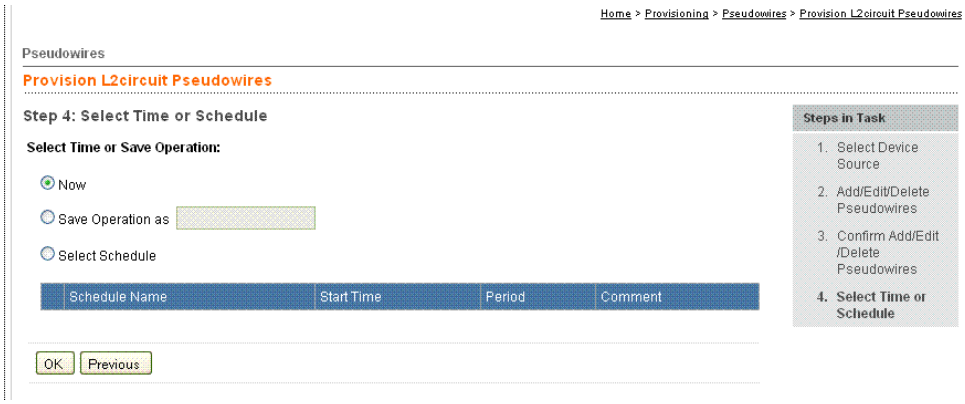
In this wizard you can Confirm the addition, modification, or deletion of the pseudowire; or go back to the Previous step.



Click Confirm to go to Step 4 of the wizard

Step 4: Provision Pseudowires

In this step configurations are generated for pseudowires created in step 3 and are pushed to the devices.



Configurations can be pushed either immediately or can be scheduled for a late time. Alternatively, pushing the configuration can be saved as a named operation.

To provision the pseudowires configured to the devices

1. Select the Now radio button to push the configuration to the devices immediately.
2. Select the save Operation As button radio button and provide a name for the operation. The configuration can be saved as a named operation.
3. Select the Schedule radio button to select a schedule. The configurations will be pushed at the scheduled time.

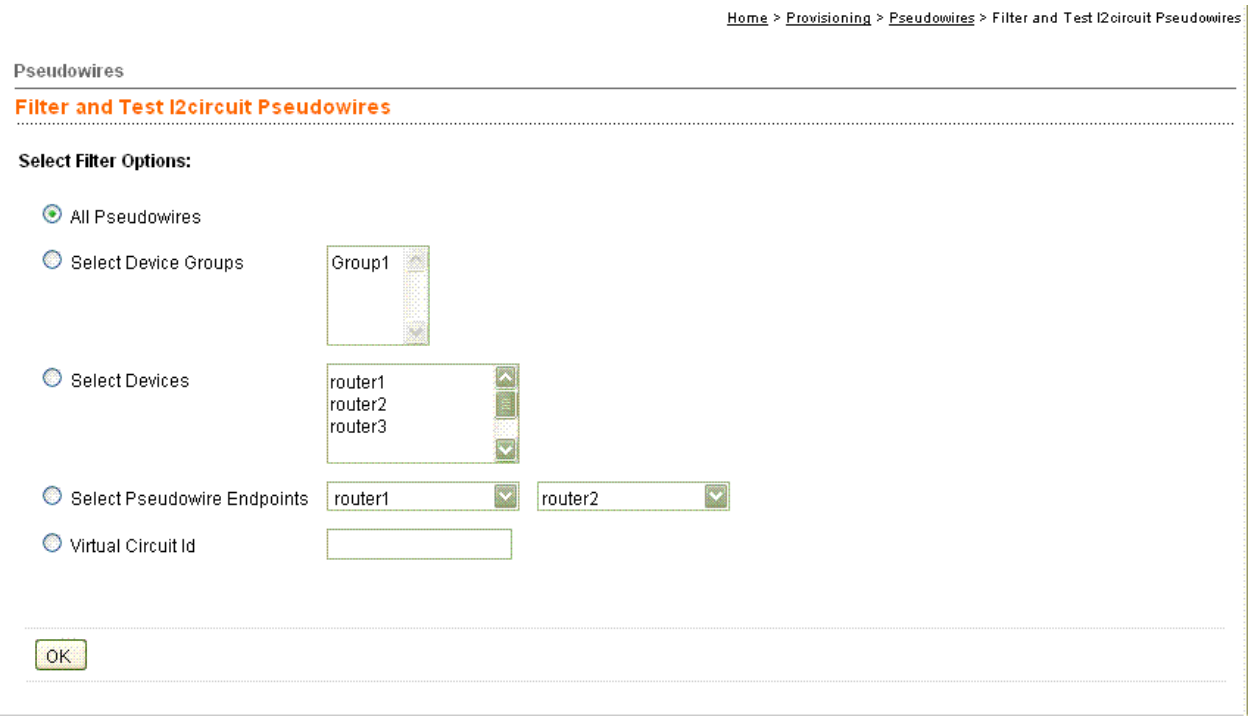
NOTE: The schedule can be chosen from those defined in Settings.

Filtering and Testing Pseudowires

You can use filtering criteria to monitor pseudowires that are already provisioned. Users with read-only, read-write and superuser privileges have access to the filtering wizard.

To filter and test pseudowires

1. Click Filter and Test l2circuit Pseudowires.
2. Select one of the option buttons under Select Filter Options. The following filtering criteria are supported:



- All Pseudowires: Select this option button to view all the pseudowires provisioned by JUNOScope.
- Select Device Group(s): Select this option button and select one or multiple device groups to view all the pseudowires that are provisioned on devices in the selected groups.
- Select Devices: Select this option button and select devices from the list box to view pseudowires provisioned on those devices.
- Select Pseudowire Endpoints: Select this option button and select, from the drop-downs the device names for endpoints to view pseudowires provisioned between these endpoints.
- Select Virtual Circuit ID: Select this option and specify a virtual circuit id to view all the pseudowires having the Virtual Circuit ID.

3. Click OK. The pseudowires are filtered according to the criteria you specified and displayed in a list.

Home > Provisioning > Pseudowires > Filter and Test l2circuit Pseudowires

Pseudowires

Filter and Test l2circuit Pseudowires

2 results returned

Page 1 of 1
Displaying 2 pseudowires of 2 total

View Test

Select	Source Device Name	Source Interface	Destination Device Name	Destination Interface	Virtual Circuit Id
	sim1	fe-1/1/0.0	sim2	fe-1/2/0.0	1
	sim1	fe-0/0/0.0	sim2	fe-0/0/1.0	5

4. Click View after selecting a pseudowire to display the details of the pseudowire.
5. Click Test to send show l2circuit connections command to each end point of the pseudowire, and to show the results.

Home > Provisioning > Pseudowires > Filter and Test l2circuit Pseudowires

Pseudowires

Filter and Test l2circuit Pseudowires

Pseudowire Test Results:

Previous

Source Device	Destination Device	Virtual Circuit Id	Status	Message
		0	NS	Device: 'null' not found in JUNOScope database
		0	NS	Device: 'null' not found in JUNOScope database

Part 6
Monitoring Operation Status

Chapter 26

Managing Operations

This chapter describes how to view the operations that have run using an existing schedule and to verify the next time they will run.

An operation appears in Monitor Operations when you run it using an existing schedule that you create using Settings > Schedule. An operation does not appear in Monitor Operations when you schedule an operation using the Now option.

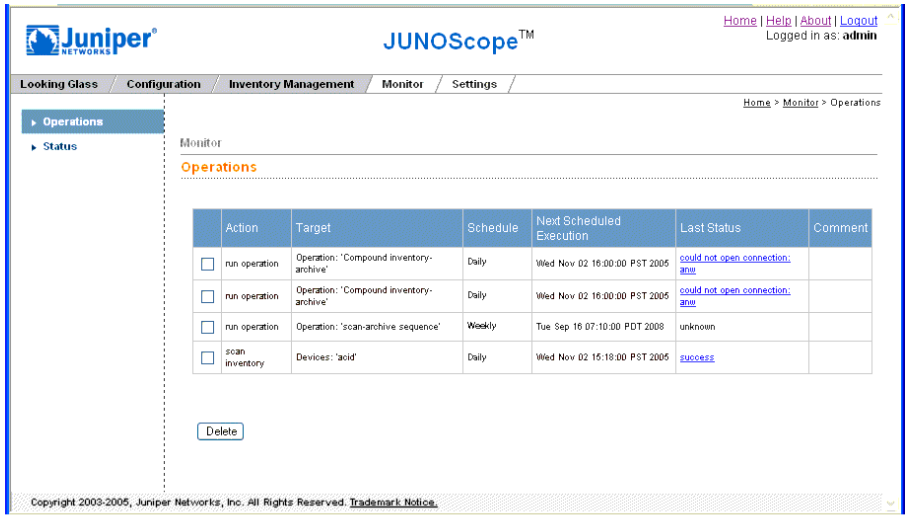
All JUNOScope software users can view scheduled operations. Users with read-only privileges cannot delete operations.

This chapter includes the following topics:

Viewing Scheduled Operations

To view scheduled operations that have run and the next time they will run, do the following:

- In the JUNOScope main window, click Monitor > Operations. The Operations dialog box appears.



The Operations dialog box lists operations that are scheduled to be run by action name (a compound operation is labeled **run operation**), target device on which the operation ran (a compound operation name is displayed in this column), schedule name, when the operation is next scheduled to run, the last status, and an operation comment. If you click a link in the Last Status column, the Monitor > Status dialog box appears displaying the status of the operation.

If no scheduled operations appear in the Monitor—Operations dialog box, you have not created a schedule. For more information about creating a schedule, see "Setting Up Schedules" on page 89.

Deleting a Scheduled Operation

You can delete a scheduled operation if it is not being used by an existing schedule. If an operation is being used in an existing schedule, you must first delete that schedule from Manage Operations.

To delete a scheduled operation, follow these steps:

1. In the JUNOScope main window, click Monitor > Operations. The Operations dialog box appears with a list of scheduled operations.
2. Select the check box for the scheduled operation that you want to delete.
3. Click Delete.

   The scheduled operation is removed from the JUNOScope software database and will not run.

Chapter 27

Viewing and Maintaining Operation Status

This chapter describes how to view the final status of configuration management operations that have run on a selected router or group of routers. It also describes how to purge the status table, after operation status records accumulate over a period of time, to reclaim disk space on the JUNOScope server. Use the View Status Records dialog box to view the status of all archive, restore, and inventory scan operations running on all devices, groups, and selected devices.

You can view the final status of operations run on specific devices, groups, or selected saved operations. You can view specific operation status by applying filters, such as operations updated in the last selected amount of time, currently in a selected state, or associated with a selected username. Operation status results are listed by device or group name on which the operation occurs, operation name, username, operation status, operation start time, last update time, and any message about the operation. Operation status includes pending, connecting, writing, success, or error.

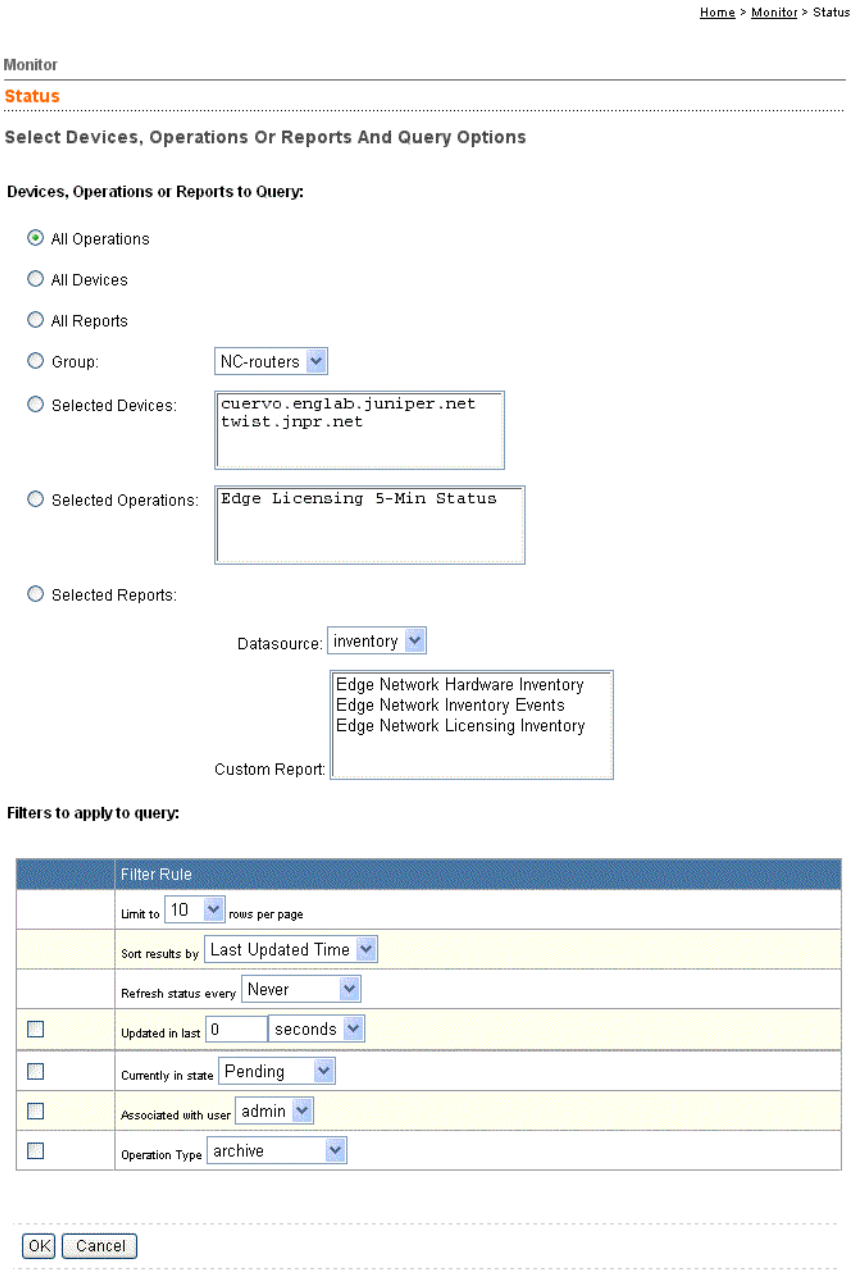
All JUNOScope software users can view operation status.

This chapter includes the following topics:

Viewing Status

To view operation status, follow these steps:

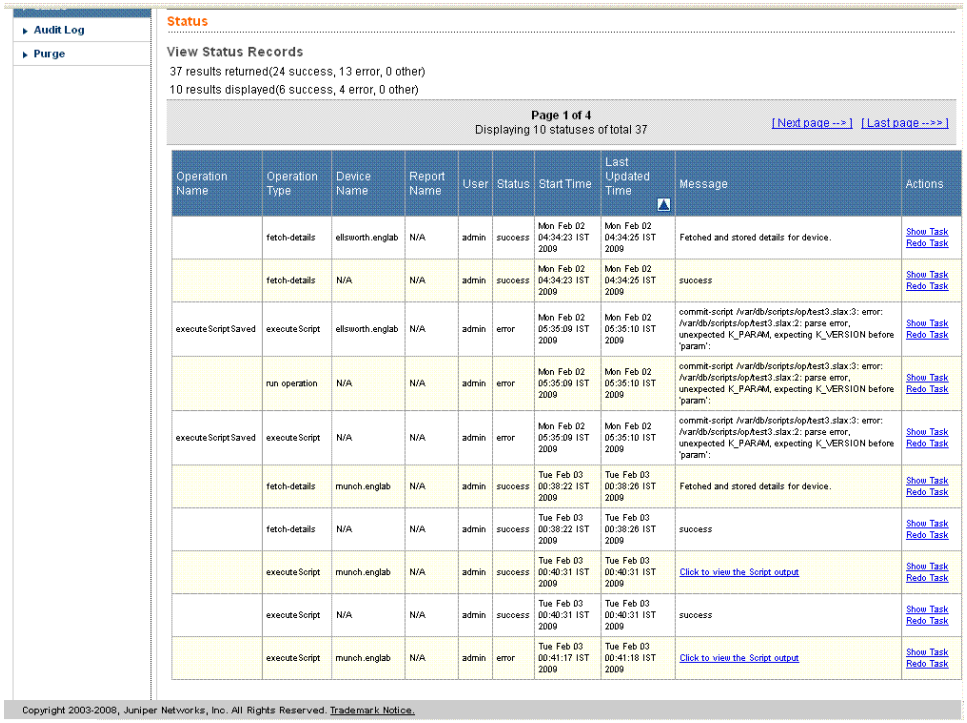
1. In the JUNOScope main window, click Monitor > Status. The Select Device and Query Options dialog box appears.



2. Select the operations to query.
3. Select the Groups or Devices to query.
4. Select the data source and the custom inventory reports to query.
5. Select from the following Filters to query reports to view.

- Limit to <#> rows per page drop-down list box—Filters the operation status by the number of rows to display per page: 10, 25, 50, or 100. The default is 10 rows.
- Sort results by <*column name*> drop-down list box—Sorts the results by the last modified time, operation name, operation type, device name, username, status, start time, or message. The default is to sort by the last modified time.
- Refresh status every <*selected time*> drop-down list box—Updates the operation status at an interval that you specify: Never, 10 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, 15 minutes, 30 minutes, or 1 hour. The default is Never.
- Updated in last <*time period*> check box, text box, and drop-down list box—Filters the operation status results by the last time period that you specify. The default is 0 seconds. Select the check box to enable this filter rule. Type a time value in the time period text box. Click the down arrow to view the available time periods: seconds, minutes, hours, and days.
- Currently in *state* check box and drop-down list box—Filters the operation status by those that are currently in a particular state: pending, connecting, working, writing, success, and error. The default is pending. Select the check box to enable this filter rule.
- Associated with user drop-down list box—Displays the operation status results that are associated with a selected username. The usernames that appear in the list box are the users that have been added using Settings > Users. Select the check box to enable this filter rule.
- Operation type drop-down list box—Displays the current JUNOScope operations that you can save, such as archive, restore, report, scan inventory, install, and download. The default is archive. Select the check box to enable this filter rule.

6. Click OK. The View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

The dialog box displays the status of all final operations listed by operation name, operation type, device name, report name, username, final operation status, operation start time, last updated status time, status message, and a link that lets you view the status of actions in the operation. Click Next Page to view additional operation status information. See Table 20 on page 318 for a description of the information.

Sort the table information by clicking on a column header. Click on a column heading to sort the table information in ascending or descending sort order.

Table 20: Monitor Status Table Column Descriptions

Column	Description
Operation Name	Saved operation name. The name that you give an operation when you save it to run at a later time using Settings > Saved Operations.
Operation Type	The type of JUNOScope operation that was run. Some operations, such as software image install, have multiple actions. You can view all actions in an operation by clicking the Show Task link.
Device Name	Name of the device on which an operation was run.
Report Name	Name of the custom report that was scheduled and run.
User	Username of the user who ran an operation.

Table 20: Monitor Status Table Column Descriptions *(continued)*

Column	Description
Status	The status of the operation that ran. The status can be pending, connecting, writing, rebooting, success, or error. The Message column describes the operation status.
Start Time	The time the operation ran.
Last Updated Time	The time the operation status was polled and refreshed.

7. Click OK.

Redoing a Task

You can now select a task and redo it. To redo a task, follow these steps:

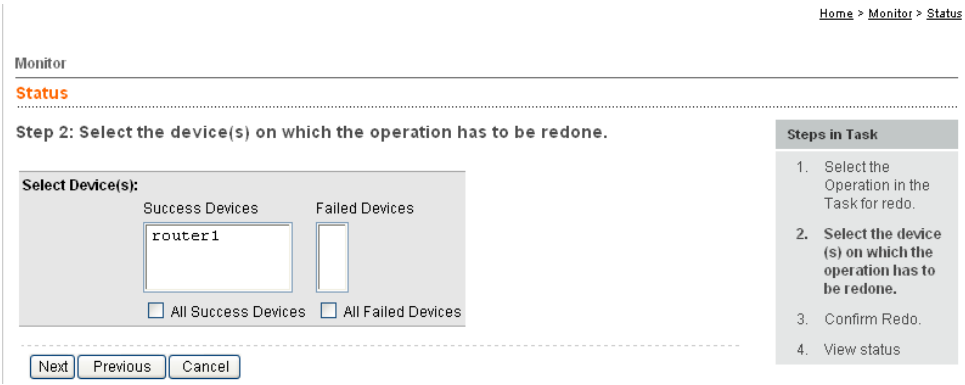
1. Click the Redo Task button in the View Status Records dialog box that appears after you perform an operation

   or

   Click Monitor > Status. Apply query options and filters in the Select Device and Query Options dialog box and click OK. Click the Redo task hyperlink in the Actions column of the View Status Records dialog box.

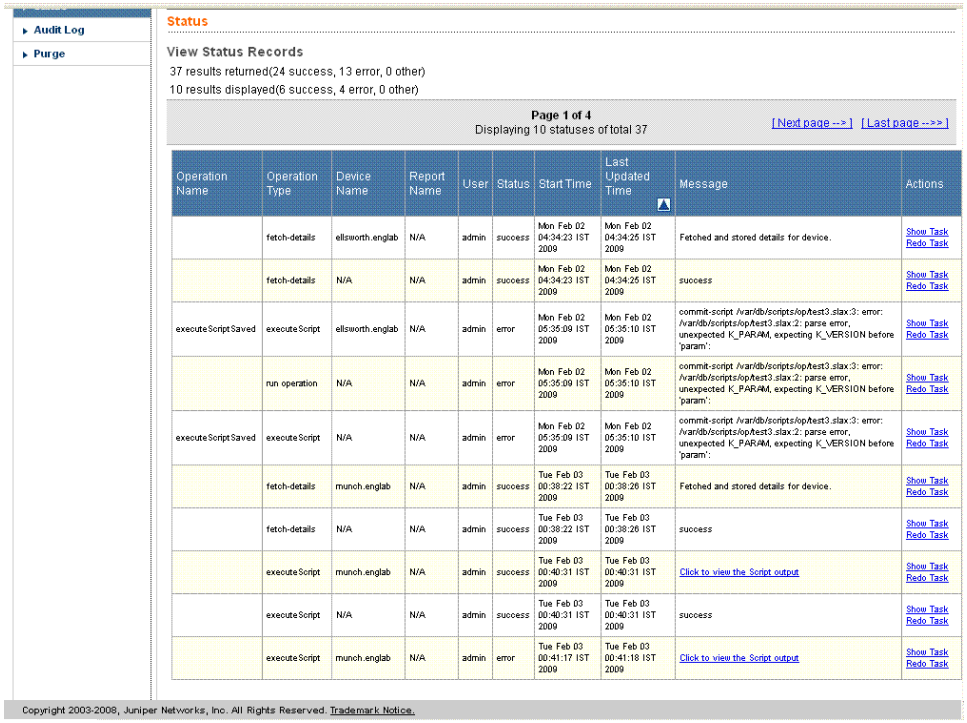
   The Select the Operation in the Task for Redo dialog box appears.

2. Select the operation you want to redo from the Select Operation drop-down list box and click Next. The Select the Device(s) on which the Operation has to be Redone dialog box appears.



3. Select the device or devices on which the operation has to be redone from the Success Devices list box, which lists all the devices on which the operation was successful, and the Failed Devices list box, which lists all the devices on which the operation failed. Select the All Success Devices check box to select all devices on which the operation was successful and the All Failed devices check box to select all devices on which the operation failed. Click Next. The Confirm Redo dialog box appears.

4. Confirm the selections you made and click Finish. The View Status Records dialog box displays the status of the operation.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

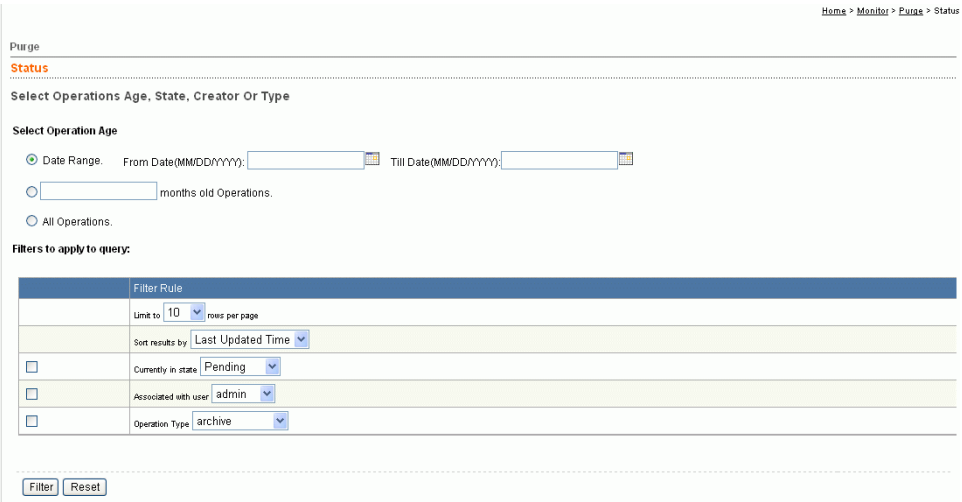
Purging the Status Table

Most JUNOScope operations add multiple status records to the Status table. As more operations are performed, this table grows in size and consumes disk space on the JUNOScope software server. The data in the Status table is useful only to administrators. From time to time, you must remove records that are no longer used in this table, and reclaim disk space if you are an administrator. You can purge all or selected status log records after filtering using the filter options provided in the Purge GUI.

You can filter Status Records, select the records to be purged and delete them.

To purge the Status table, follow these steps:

1. From the JUNOScope main window, click Monitor > Purge > Status. The Status Records Filter options dialog box appears.



2. Select the records you want to purge. You can choose to select all, records within a specified date range, or records that are a specified number of months old:

   - Date Range: From Date (MM/DD/YYYY)/To Date (MM/DD/YYYY) option text boxes—Type the date range within which to delete status records. Click the calendar icon view a calendar from which you can select a date and get the local time. Click Local Time to view the current time. Click OK in to insert the date that you selected.

   - Months old operations option text box—Type the number months to go back and retrieve status records to purge.

   - All Operations option button—Selects all status records to purge.

   - Select from the following filter rules.

   - Limit to number of rows per page drop-down list box—Filters the operation status by the number of rows to display per page: 10, 25, 50, or 100. The default is 10 rows.

   - Sort results by *column name* drop-down list box—Sorts the results by the last updated time, operation name, operation type, device name, username, status, start time, or message. The default is to sort by the last updated time.

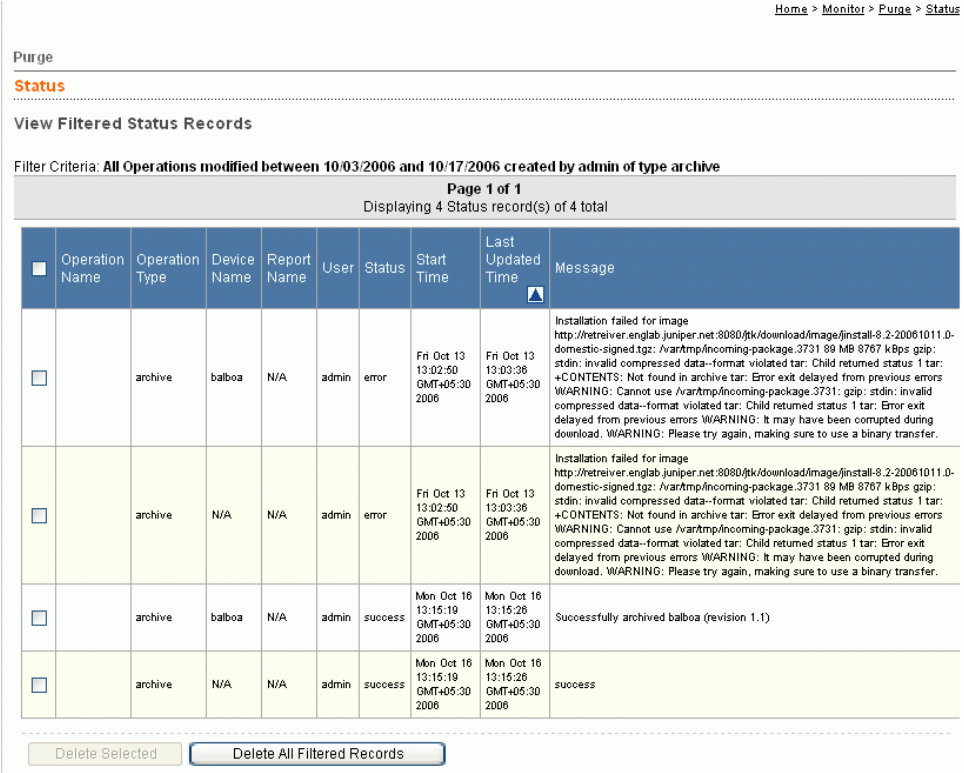
   - Currently in *state* check box and drop-down list box—Filters the operation status by those that are currently in a particular state: pending, connecting, working, writing, warning, success, and error. The default is pending. Select the check box to enable this filter rule.

   - Associated with user drop-down list box—Displays the operation status results that are associated with a selected username. The usernames that

appear in the list box are the users that have been added using Settings > Users. Select the check box to enable this filter rule.

- Operation type drop-down list box—Displays the current JUNOScope operations that you can save, such as archive, restore, report, scan inventory, install, and download. The default is archive. Select the check box to enable this filter rule.

3. Click Filter to proceed with the purge operation. The View Filtered Status Records dialog box appears. Click Reset to clear all the values you have selected and return to the default values.



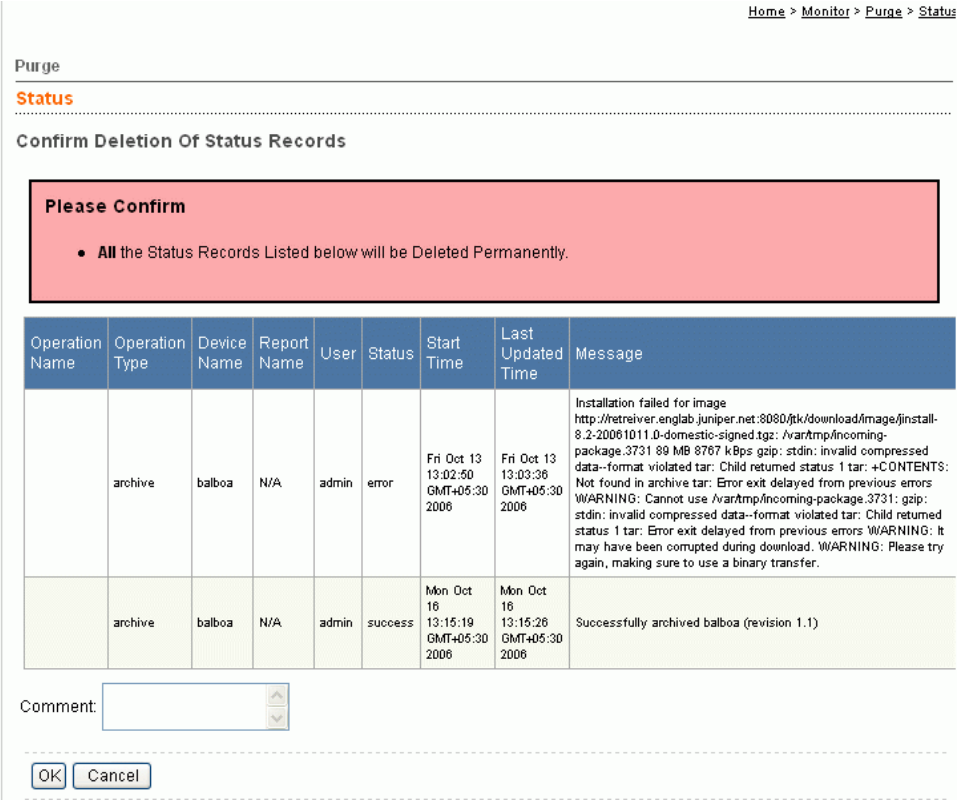
Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message
	archive	balboa	N/A	admin	error	Fri Oct 13 13:02:50 GMT+05:30 2006	Fri Oct 13 13:03:36 GMT+05:30 2006	Installation failed for image http://retreiver.englab.juniper.net:8080/jtk/download/image/jinstall-8.2-20061011.0-domestic-signed.tgz: /var/tmp/incoming-package.3731 89 MB 8767 kBps gzip: stdin: invalid compressed data--format violated tar: Child returned status 1 tar: +CONTENTS: Not found in archive tar: Error exit delayed from previous errors WARNING: Cannot use /var/tmp/incoming-package.3731: gzip: stdin: invalid compressed data--format violated tar: Child returned status 1 tar: Error exit delayed from previous errors WARNING: It may have been corrupted during download. WARNING: Please try again, making sure to use a binary transfer.
	archive	N/A	N/A	admin	error	Fri Oct 13 13:02:50 GMT+05:30 2006	Fri Oct 13 13:03:36 GMT+05:30 2006	Installation failed for image http://retreiver.englab.juniper.net:8080/jtk/download/image/jinstall-8.2-20061011.0-domestic-signed.tgz: /var/tmp/incoming-package.3731 89 MB 8767 kBps gzip: stdin: invalid compressed data--format violated tar: Child returned status 1 tar: +CONTENTS: Not found in archive tar: Error exit delayed from previous errors WARNING: Cannot use /var/tmp/incoming-package.3731: gzip: stdin: invalid compressed data--format violated tar: Child returned status 1 tar: Error exit delayed from previous errors WARNING: It may have been corrupted during download. WARNING: Please try again, making sure to use a binary transfer.
	archive	balboa	N/A	admin	success	Mon Oct 16 13:15:19 GMT+05:30 2006	Mon Oct 16 13:15:26 GMT+05:30 2006	Successfully archived balboa (revision 1.1)
	archive	N/A	N/A	admin	success	Mon Oct 16 13:15:19 GMT+05:30 2006	Mon Oct 16 13:15:26 GMT+05:30 2006	success

The dialog box displays the filter criteria and the list of the filtered status records listed by operation name, operation type, device name, report name, username, final operation status, operation start time, last updated status time, and status message. See Table 20 on page 318 for a description of the information. The records are initially sorted by last updated time in descending order, with the most recent events at the top of the list. Click on a column heading to sort the table information in ascending or descending sort order. Select the check boxes in the corresponding rows to select a filtered record. Select the check box in the column header row to select all filtered records in the dialog box.

4. Do one of the following:

- Select the records you want to delete and click Delete Selected to purge the selected records.

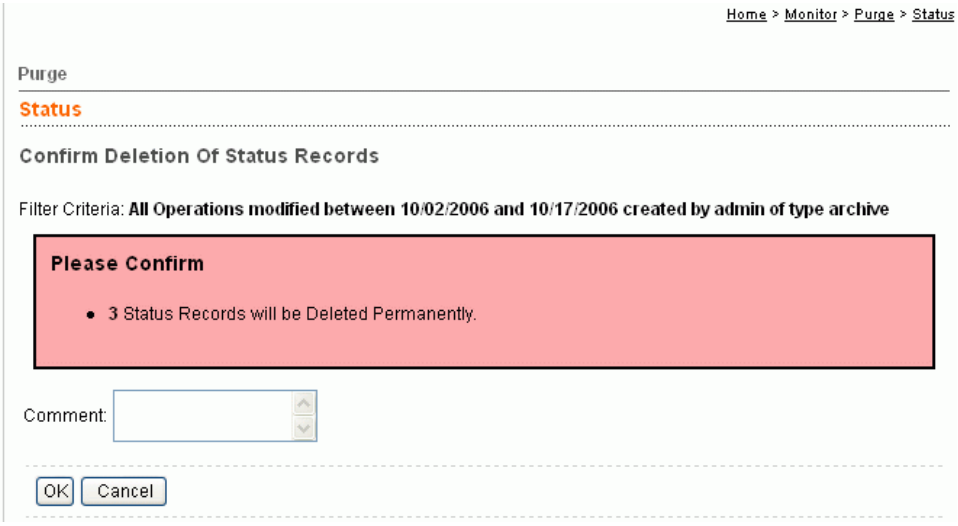
If you click Delete Selected, the Confirm Purge Status Records dialog box appears listing the records you selected for deletion. Enter the reason for deleting status records in the Comment field.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message
	archive	balboa	N/A	admin	error	Fri Oct 13 13:02:50 GMT+05:30 2006	Fri Oct 13 13:03:36 GMT+05:30 2006	Installation failed for image http://retreiver.englab.juniper.net:8080/jtk/download/image/jinstall-8.2-20061011.0-domestic-signed.tgz: /var/tmp/incoming-package.3731 89 MB 8767 kBps gzip: stdin: invalid compressed data--format violated tar: Child returned status 1 tar: +CONTENTS: Not found in archive tar: Error exit delayed from previous errors WARNING: Cannot use /var/tmp/incoming-package.3731: gzip: stdin: invalid compressed data--format violated tar: Child returned status 1 tar: Error exit delayed from previous errors WARNING: It may have been corrupted during download. WARNING: Please try again, making sure to use a binary transfer.
	archive	balboa	N/A	admin	success	Mon Oct 16 13:15:19 GMT+05:30 2006	Mon Oct 16 13:15:26 GMT+05:30 2006	Successfully archived balboa (revision 1.1)

- Click Delete All Filtered Records to delete all filtered records.

  If you click Delete All Filtered Records, the Confirm Purge All Status Records dialog box appears with the filter criteria and the number of records that will be deleted permanently. Enter the reason for deleting the status records in the Comment field.



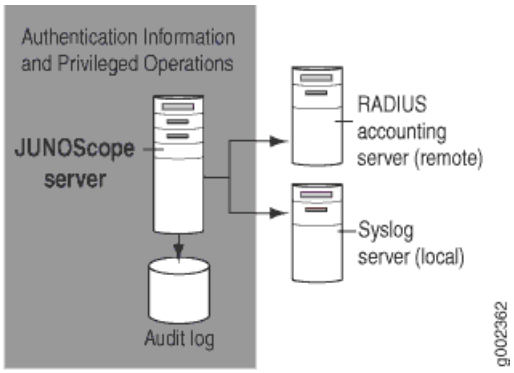
5. Click OK in the Confirm Purge All Status Records dialog box to confirm purge of status records. The Status Records are removed from the Status table in the JUNOScope database. Click Cancel to go back to the View Filtered Status Records dialog box.

Chapter 28

Monitoring and Maintaining the Audit Log

This chapter describes how to monitor authentication activity and privileged operation events in the audit log. JUNOScope auditable events are stored in the JUNOScope database and are subsequently sent to the system log server and an optional RADIUS accounting server if one is configured (see Figure 11 on page 327). This chapter also describes how to purge the audit log table, after audit log records accumulate over a period of time, to reclaim disk space on the JUNOScope server.

Figure 11: JUNOScope Security-Enhanced Sensitive Data Logging



Authentication activity events include the following:

- User logs in
- Login attempt failures because of an invalid username and/or password
- User logs out
- User session times out

Privileged operation events are user actions that change information in the JUNOScope system or in the network. Privileged events include the following:

- Configuration is committed on a device from the Configuration Editor
- Configuration is archived from a device
- Configuration is restored to a device
- User account is created
- User account is deleted

- User password is changed
- Device is added
- Device is deleted
- Label association is changed
- Access method is changed
- Authentication information is changed

Each audit record includes the date and time, event category, event type, username, and client IP address.

In addition to the internal audit log, audit events are also forwarded to the local syslog server and the configured RADIUS server (if any) as RADIUS accounting messages.

You must have superuser permission to view the audit log.

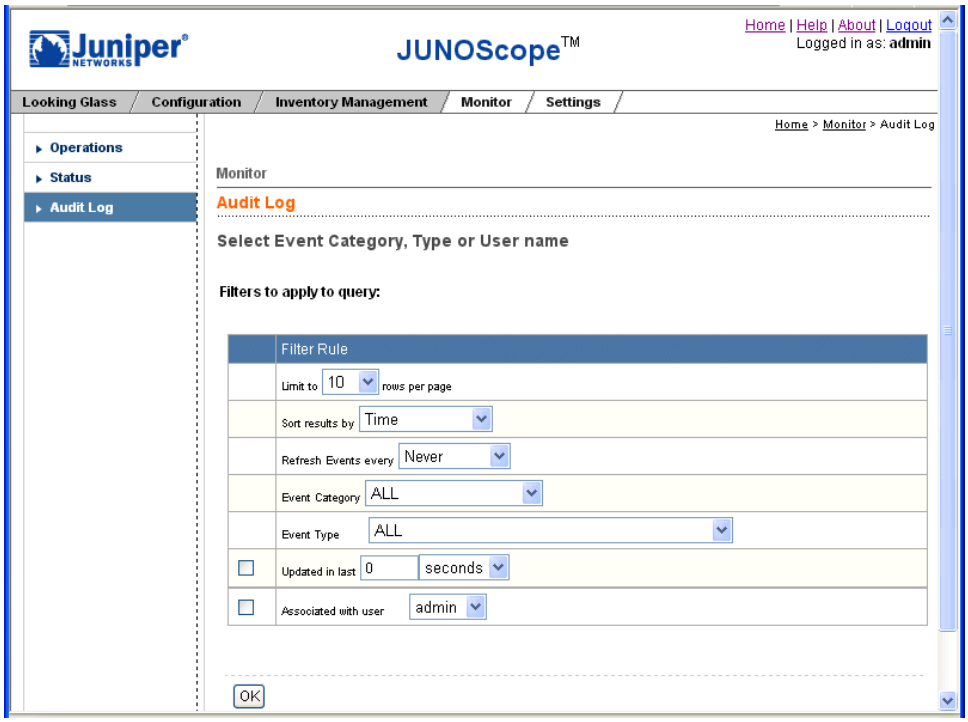
This chapter includes the following topic:

Displaying the Audit Log

The audit log displays JUNOScope authentication and privileged operation events by date and time, event category, event type, username, and client IP address. You can select filters to specify which records you want to see.

To display the Audit Log, follow these steps:

1. From the JUNOScope main window, click Monitor > Audit Log. The Audit Log Filters dialog box appears.



2. Select a filter rule to select the audit log records that you want to view:

   - Limit to *number* of rows per page drop-down list box—Select how many record rows you want to display per audit log page: 10, 25, 50, or 100. The default is 10.

   - Sort results by *column-name* drop-down list box—Select the column of data by which the audit log records will be sorted in the table: Time, Username, Client address, Event type, or Message. The default is Time.

   - Refresh Events every *interval* drop-down list box—Select when the audit log data will be updated in the table: from Never up to 1 hour. The default is Never.

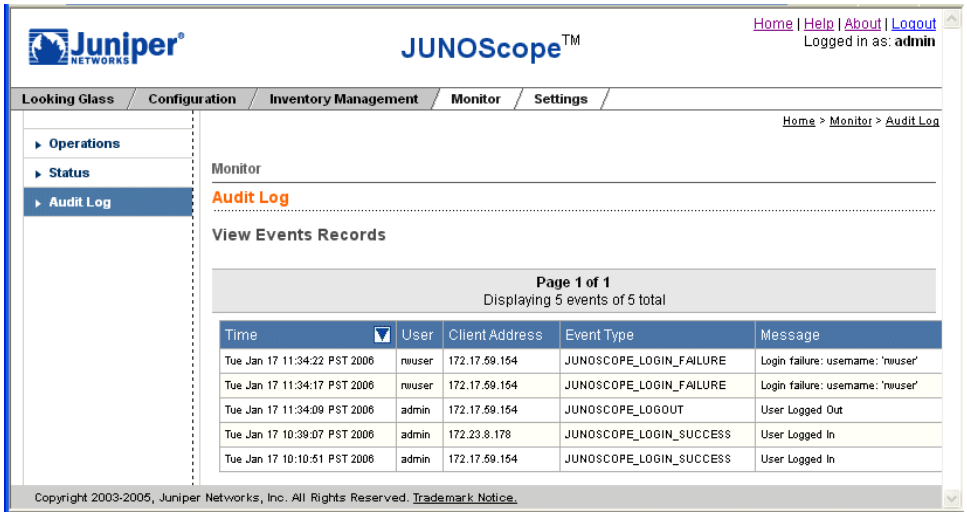
   - Event Category drop-down list box—Select the events category to display: All, Authentication, or Privileged Operations. Authentication activities include user login success, failure, logout, and session timeout. Privileged operations are changes of information in the system or in the network, such as restoring a configuration to a device or changing a user password. The default is All.

   - Event Type drop-down list box—This list box is dynamically populated based on the event category that you selected. For example, if you select the authentication event category, all authentication event message types appear in this drop-down list box.

   - Updated in last time period check box, text box, and drop-down list box—Select the audit log records that have been updated in the last specified length of time. You can select n seconds, minutes, hours, or days, where *n* represents the time you specify. The default is 0 seconds.

   - Associated with user drop-down list box—Select records that are associated with a specified username.

3. Click OK. The Audit Log dialog box appears.



Each audit record includes the date and time, event category, event type, username, and client IP address. The records are initially sorted by time in descending order so that the most recent events are at the top of the list. See Table 21 on page 330.

Table 21: Audit Log Columns

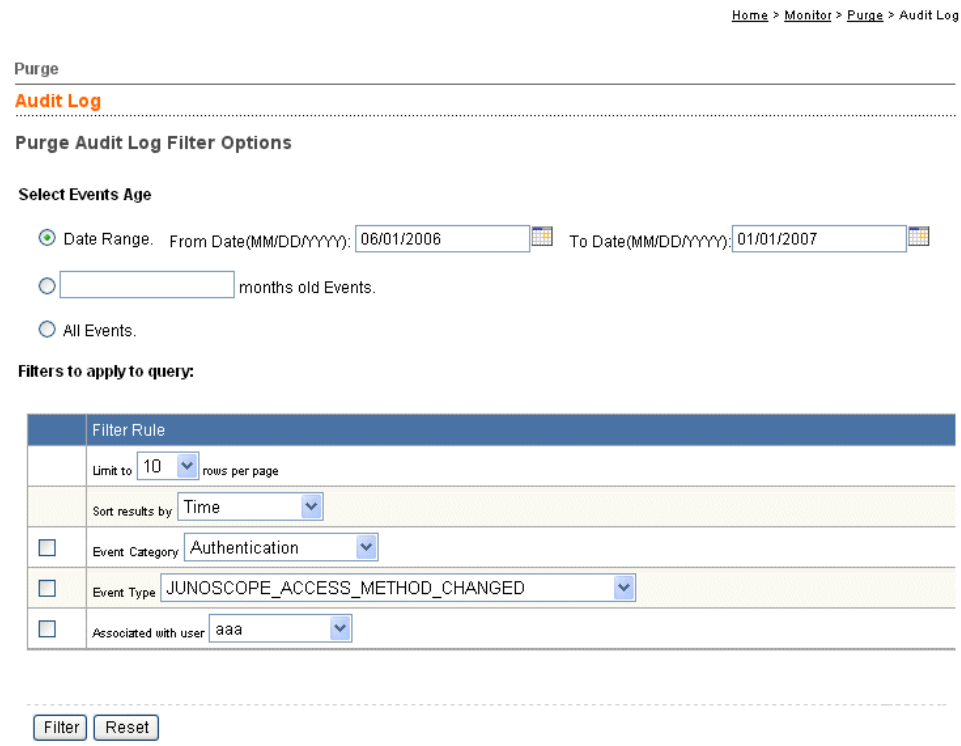
Column Name	Description
Time	The date and time that the event was logged. The format for date and time is *dow mon dd hh:mm:ss zzz yyyy*. Where: ■ *dow* is the day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat). ■ *mon* is the month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec). ■ *dd* is the day of the month (01 through 31), as two decimal digits. ■ *hh* is the hour of the day (00 through 23), as two decimal digits. ■ *mm* is the minute within the hour (00 through 59), as two decimal digits. ■ *ss* is the second within the minute (00 through 61), as two decimal digits. ■ *zzz* is the time zone (and may reflect Daylight Saving Time). If time zone information is not available, then *zzz* is empty; that is, it consists of no characters at all. ■ *yyyy* is the year, as four decimal digits.
User	The name of the user who performed that action that was logged. The default user is admin.
Client Address	The IP address of the client from which the action occurred.
Event Type	The title of the system log message that is logged.
Message	The description of the system log message that is logged.

Purging the Audit Log Table

Most Junoscope operations add multiple audit log records in the Audit Log table. As more and more operations are performed, this table grows in size and consumes disk space on the JUNOScope software server. The data in the Audit Log table is useful only to administrators. From time to time, you must remove records that are no longer used in the Audit Log table, and reclaim disk space if you are an administrator. You can purge all or selected audit log records, after filtering audit log records, using the filter options provided in the Purge GUI.

To purge the Audit Log table, follow these steps:

1. From the JUNOScope main window, click Monitor > Purge > Audit Log. The Audit Log Records Filter options dialog box appears.



2. In the Select Events Age area, specify the events you want to purge. You can choose to select all events, events within a specified date range, or events that are a specified number of months old.

3. Select from the following filter rules:

   - Limit to *number* of rows per page drop-down list box—Select how many record rows you want to display per audit log page: 10, 25, 50, or 100. The default is 10.

   - Sort results by *column-name* drop-down list box—Select the column of data by which the audit log records will be sorted in the table: Time, Username, Client address, Event type, or Message. The default is Time.

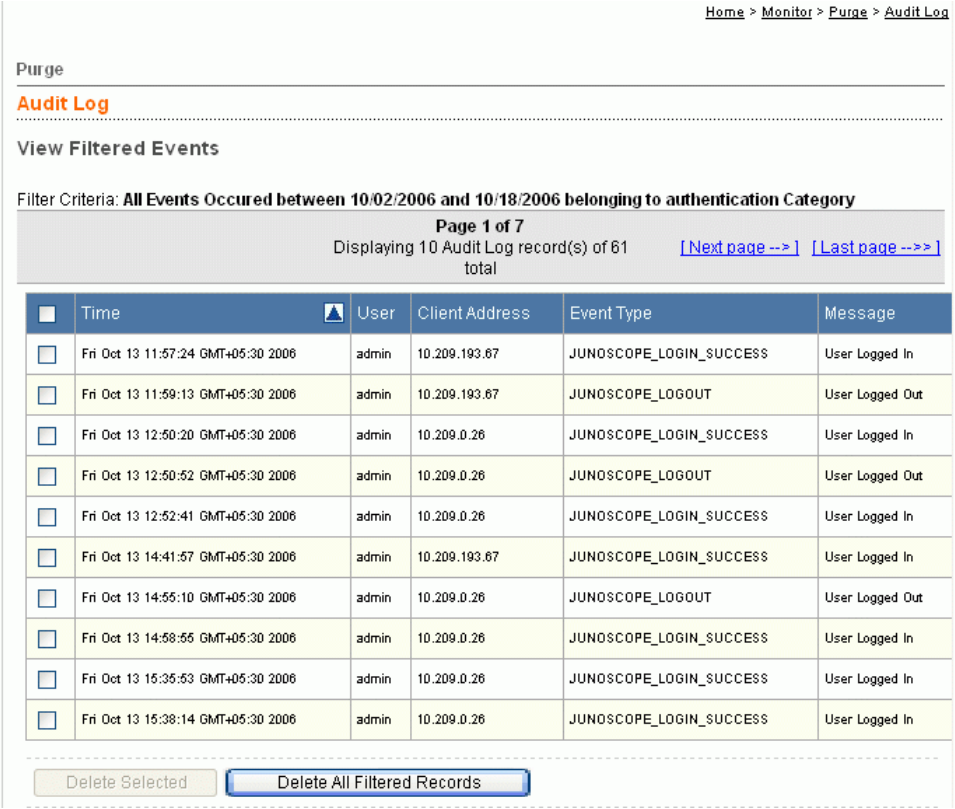
   - Event Category drop-down list box—Select the event category to display: Authentication, or Privileged Operations. Authentication activities include user login success, failure, logout, and session timeout. Privileged operations are changes of information in the system or in the network, such as restoring a configuration to a device or changing a user password. The default is Authentication.

   - Event Type drop-down list box—This list box is dynamically populated based on the event category that you selected. For example, if you select the

Authentication event category, all authentication event message types appear in this drop-down list box.

- Associated with user drop-down list box—Select records that are associated with a specified username.

4. Click Filter to proceed with the purge operation. The View Filtered Events dialog box appears. Click Reset to clear all the values you selected and return to the default values.



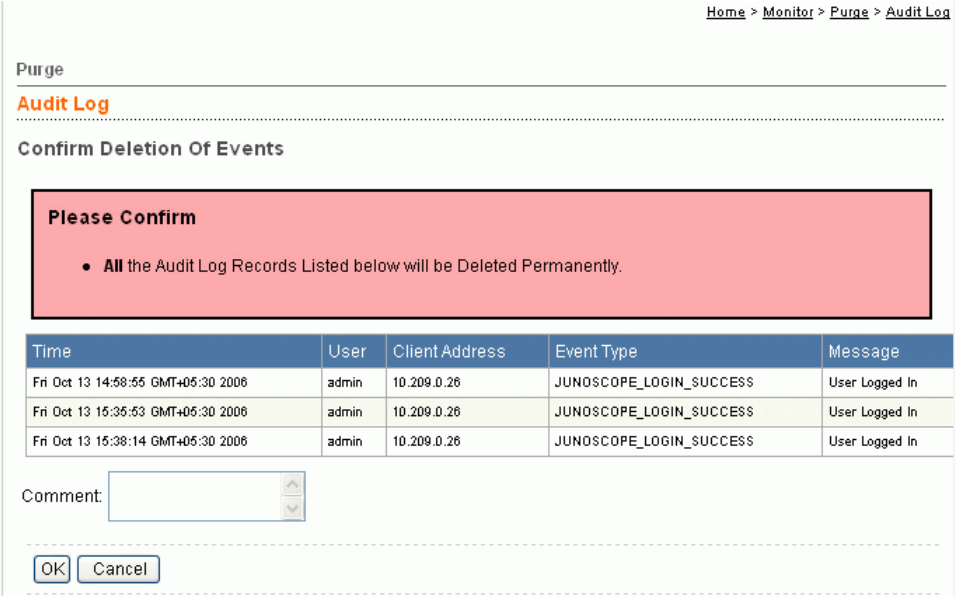
Time	User	Client Address	Event Type	Message
Fri Oct 13 11:57:24 GMT+05:30 2006	admin	10.209.193.67	JUNOSCOPE_LOGIN_SUCCESS	User Logged In
Fri Oct 13 11:59:13 GMT+05:30 2006	admin	10.209.193.67	JUNOSCOPE_LOGOUT	User Logged Out
Fri Oct 13 12:50:20 GMT+05:30 2006	admin	10.209.0.26	JUNOSCOPE_LOGIN_SUCCESS	User Logged In
Fri Oct 13 12:50:52 GMT+05:30 2006	admin	10.209.0.26	JUNOSCOPE_LOGOUT	User Logged Out
Fri Oct 13 12:52:41 GMT+05:30 2006	admin	10.209.0.26	JUNOSCOPE_LOGIN_SUCCESS	User Logged In
Fri Oct 13 14:41:57 GMT+05:30 2006	admin	10.209.193.67	JUNOSCOPE_LOGIN_SUCCESS	User Logged In
Fri Oct 13 14:55:10 GMT+05:30 2006	admin	10.209.0.26	JUNOSCOPE_LOGOUT	User Logged Out
Fri Oct 13 14:58:55 GMT+05:30 2006	admin	10.209.0.26	JUNOSCOPE_LOGIN_SUCCESS	User Logged In
Fri Oct 13 15:35:53 GMT+05:30 2006	admin	10.209.0.26	JUNOSCOPE_LOGIN_SUCCESS	User Logged In
Fri Oct 13 15:38:14 GMT+05:30 2006	admin	10.209.0.26	JUNOSCOPE_LOGIN_SUCCESS	User Logged In

The View Filtered Events dialog box displays the filter criteria and the list of the filtered audit log records with the date and time, username, client IP address. event type, and message. See Table 21 on page 330 for a description of the information.The records are initially sorted by time in descending order, with the most recent events at the top of the list. Click on a column heading to sort the table information in ascending or descending sort order. Select the check boxes in the corresponding rows to select a filtered record. Select the check box in the column header row to select all filtered records in the dialog box.

5. Do one of the following:

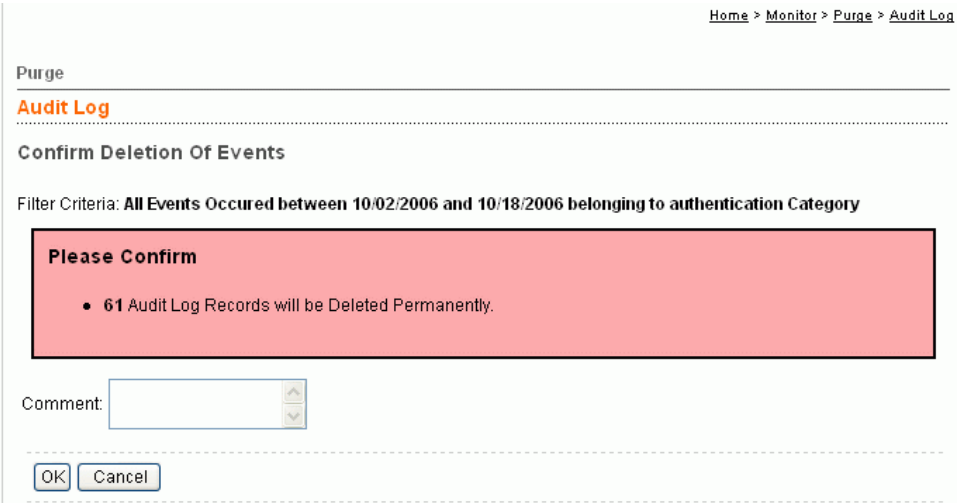
- Select the records you want to delete and click Delete Selected to purge the selected records.

  If you click Delete Selected, the Confirm Purge Audit Log Records dialog box appears listing the records you selected for deletion. Enter the reason for deleting audit log records in the Comment field.



- Click Delete All Filtered Records if you want to delete all the filtered records.

  If you click Delete All Filtered Records, the Confirm Purge All Audit Log Records dialog box appears with the filter criteria and the number of records that will be deleted permanently. Enter the reason for deleting the audit log records in the Comment field.



6. Click OK in the Confirm Purge All Audit Log Records dialog box to confirm purge of audit log records. The audit log records are removed from the audit log table in the JUNOScope database. Click Cancel to go back to the View Filtered Events dialog box.

Part 7
Performing Inventory Management

Chapter 29

Inventory Management System Overview

This chapter provides an overview of the JUNOScope Inventory Management System you use to keep track of changes to devices on the network as they occur. The Inventory Management System keeps track of items installed in devices, such as hardware, software components, and feature licenses.

The Inventory Management System scans for inventory items in real time or as part of an existing scheduled operation, and stores the inventory records in the JUNOScope database. For more information about scanning the device inventory, see "Scanning Inventory Data" on page 339.

The Inventory Management System can generate predefined inventory reports from the stored inventory records, or you can define your own report formats. You can save custom inventory reports, including user-specified definitions and controls. Reports are saved in the JUNOScope database, where all JUNOScope users can view them.

An Inventory Management System Demo lets you view and manipulate sample inventory reports so you can practice and learn the full potential of the system before scanning real production inventory data.

The Inventory Management System displays reports in a browser using HTML, and can also be exported to Extensible Markup Language (XML), Comma-Separated Values (CSV) text, Adobe PDF, and Microsoft Excel formats. For more information about the Inventory Management System report, see "Using Inventory Reports" on page 345.

An external inventory application can connect to the Inventory Management System database and extract inventory data, such as hardware, software, licensed features, and inventory scan events from the database by way of a Structured Query Language (SQL) interface. A unique username and password must be configured during the JUNOScope software installation to enable read-only access to the Inventory Management System database. For more information about extracting Inventory Management System data, see "Exporting Inventory Management System Data" on page 379.

You must have one of the following access privilege levels to use the Inventory Management System:

- Superuser—Generate reports, scan inventory, set up devices and schedules for inventory scanning, and save and delete inventory reports

- Read-write—Generate reports, scan inventory, and save and delete inventory reports
- Read-only—Generate reports

This chapter includes the following topics:

Prerequisites for Using the Inventory Management System

Before you can use the Inventory Management System, you must set up and populate access methods, devices, groups, and schedules in JUNOScope.

- To set up access methods, see “Setting Up Access Methods” on page 45.
- To set up devices, see “Setting Up Devices” on page 57.
- To set up groups, see “Setting Up Groups” on page 67.
- To set up schedules, see “Setting Up Schedules” on page 89.

NOTE: JUNOScope performs both hardware inventory scans and software inventory scans on root system domain (RSD) devices but performs only software inventory scans on a protected system domain (PSD) device. This is because RSD and PSD devices share certain hardware resources such as flexible PICs concentrators (FPCs), etc. If JUNOScope performs a hardware inventory scan on a PSD device, it will send a copy of the hardware inventory items to the RSD device. JUNOScope will not check if the device is a RSD device or a PSD device. To find out if a device is PSD or not, check the value in the model field of the device. A PSD device will have ’-PSD’ appended at the end.

Where To Go From Here

- To use the Inventory Management System to scan for device inventory items, see “Scanning Inventory Data” on page 339.
- To view and manipulate Inventory Management System reports of inventory items stored in the JUNOScope demo or production database, see “Using Inventory Reports” on page 345.
- To extract Inventory Management System data to an external inventory application using a read-only SQL interface, see “Exporting Inventory Management System Data” on page 379.

Chapter 30

Scanning Inventory Data

This chapter describes how to use the Inventory Management System to scan devices on the network and keep track of inventory items, such as hardware components in the chassis, installed software packages, and feature licenses.

The Inventory Management System scans for inventory items in real time or as part of an existing scheduled operation.

The Inventory Management System stores inventory data in the JUNOScope database.

To scan inventory data, you must have superuser or read-write access privilege levels.

This chapter includes the following topics:

Understanding Inventory Items

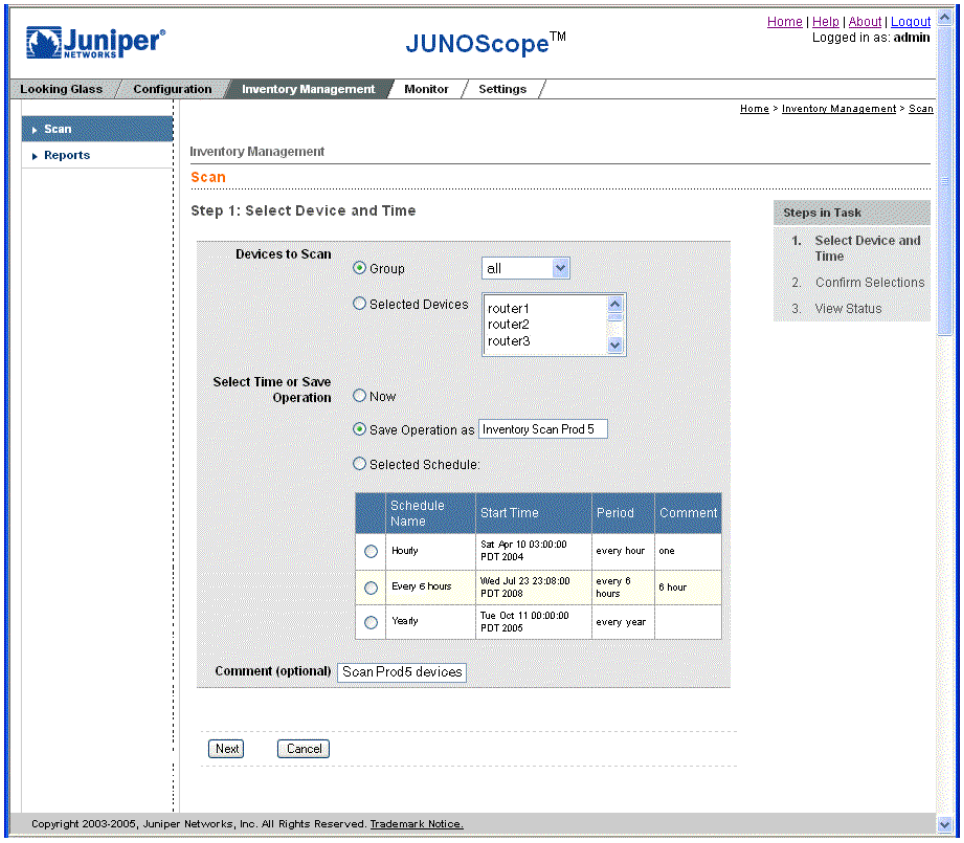
An inventory scan gathers a listing of all inventory items, such as:

- Hardware components installed in a routing platform, including part numbers and serial numbers
- Feature licenses for enabling software features on a routing platform
- JUNOS software and packages installed on a routing platform
- Inventory events that occur when an inventory scan is performed

Performing an Inventory Scan

To perform an inventory scan, follow these steps:

1. In the JUNOScope main window, click Inventory Management > Scan. The Scan—Select Device and Time dialog box appears.



2. Select the devices you want scanned. Select either the Group (default) or Selected Devices option button.

3. Click the down arrow to select the group or device(s) that you want scanned. You can select multiple groups or devices by Shift or Control-clicking each device name that you want.

NOTE: The Inventory Management System scans the inventory on both the TX Matrix platform and attached T640 routing nodes. The TX Matrix routing platform consists of the TX Matrix platform (also known as the switch-card chassis [SCC]) and the attached T640 routing nodes (also known as line-card chassis [LCC]).

---

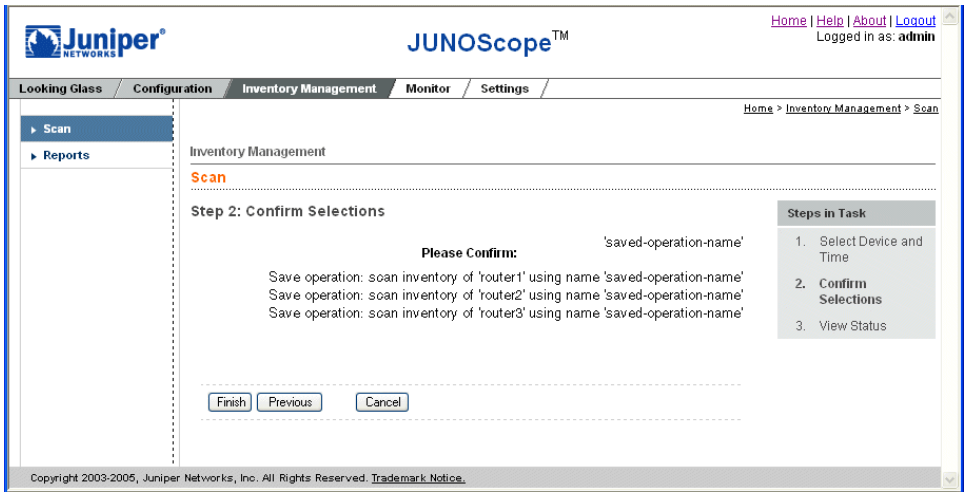
4. Select when you want the inventory scan to occur:

   - Now—(Default) Performs an inventory scan immediately after you confirm it.

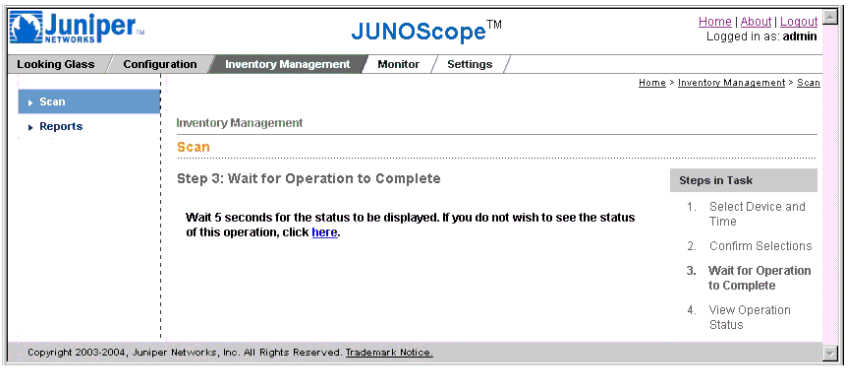
   - Save Operations as text box—Lets you save the inventory scan operation with a unique name so that you can combine it with other operations to run on devices.

   - Selected Schedule—Click an option button to schedule when you want inventory scanning to occur.

5. In the Comment text box, type an optional descriptive comment about the inventory scan that you want to perform.
6. Click Next. The Scan—Confirm Selections dialog box appears.

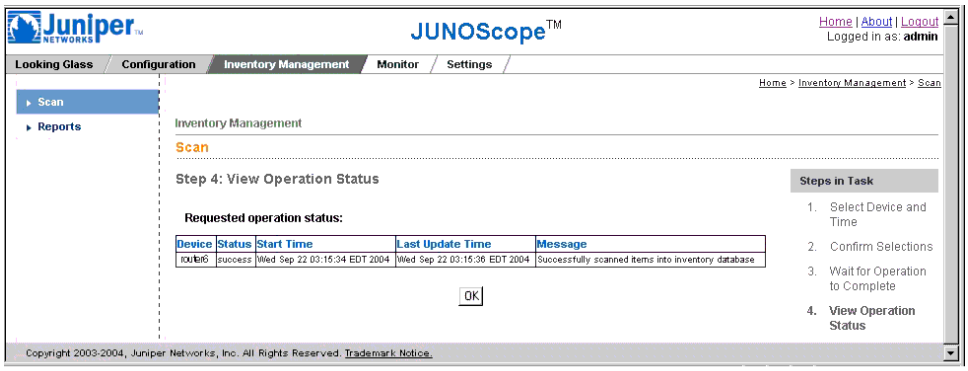


7. Click Finish to confirm the scan inventory operation. If you selected Now in Step 4, inventory scanning occurs immediately and the Scan—Wait for Operation to Complete message appears.



If you selected a predefined schedule, inventory scanning occurs when that schedule is specified to run.

When the scan inventory operation is complete, the Scan—View Operation Status dialog box appears displaying the status of the operation.



Understanding Inventory Scan Status Messages

The following inventory scan status output messages indicate that the operation was successful:

- Successfully scanned items into inventory database
- No change in inventory database

The following operation status output messages indicate that the inventory scan failed to process one or more inventory records in the database:

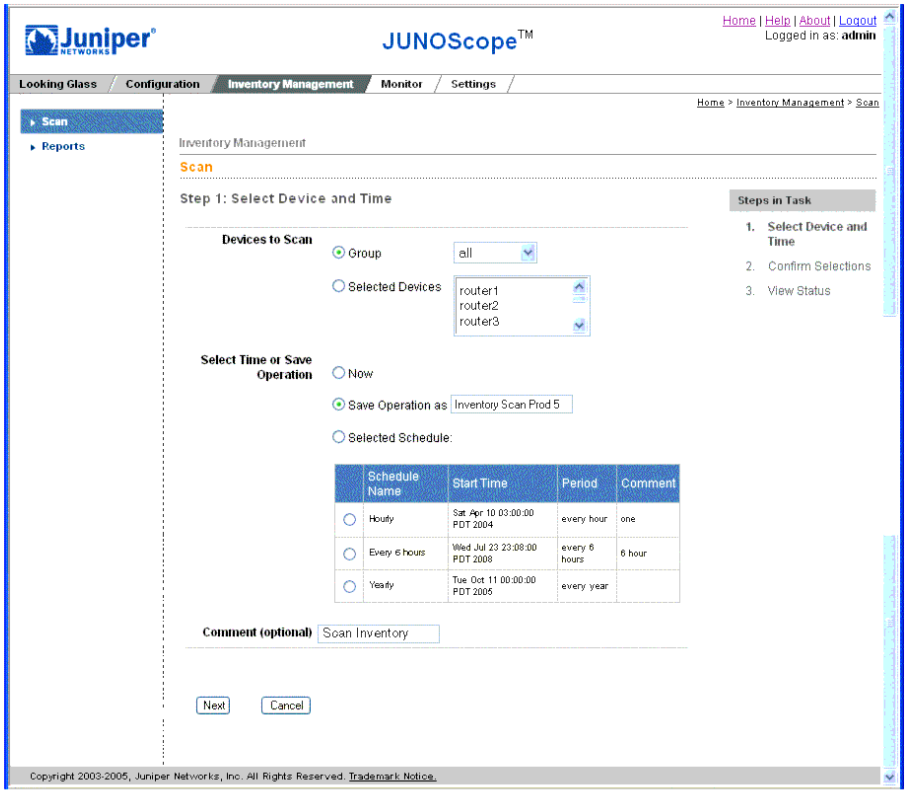
- Could not find inventory information for "*hostname*"
- Inventory database operation failed
- Could not open connection: *hostname*

Saving an Inventory Scan Operation

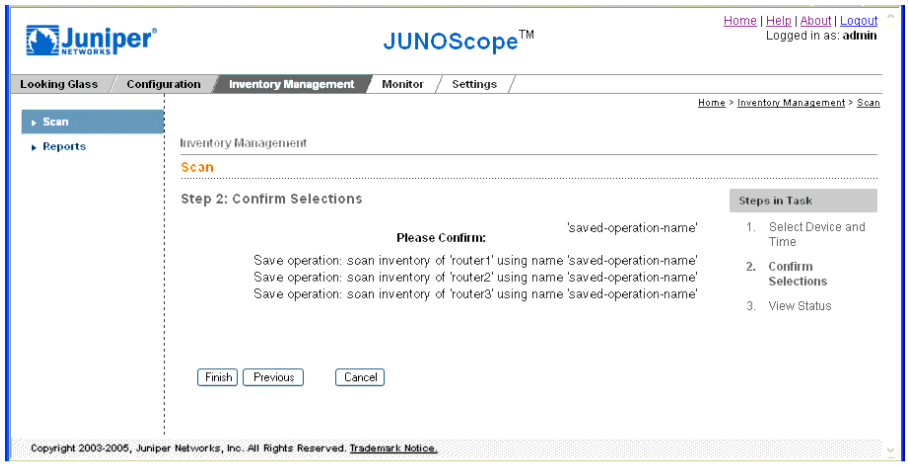
You can save inventory scan operations and combine them with other saved operations to run concurrently or sequentially on specific devices either immediately or at a specified time or interval.

To save an inventory operation, follow these steps:

1. From the JUNOScope main window, click Inventory Management > Scan. The Scan—Select Device and Time dialog box appears.



2. Select a group or one or more devices on which to scan inventory.
3. Click the Save Operation as option button and type a name for the saved inventory scan operation in the text box.
4. Click Next. The Scan—Confirm Selections dialog box appears.



5. Check to see that the selections for the scan operation you want to save are correct.
6. Click Finish. The Inventory Management menu appears.

   To view the saved archive operation, click Settings > Saved Operations. To work with saved operations, see “Using Task Manager (Saved Operations)” on page 167.

Where To Go From Here

- To view and manipulate Inventory Management System reports of inventory items stored in the JUNOScope demo or production database, see “Using Inventory Reports” on page 345.
- To extract Inventory Management System data to an external inventory application using a read-only SQL interface, see “Exporting Inventory Management System Data” on page 379.

Chapter 31

Using Inventory Reports

This chapter describes how to view and manipulate Inventory Management System reports of inventory data stored in the JUNOScope software database. Inventory data is stored when the Inventory Management System scans devices on the network for items, such as hardware components, software components, and feature licenses.

The Inventory Management System can generate predefined inventory reports from the stored inventory records, or you can define your own report formats. You can save custom inventory reports, including user-specified definitions and controls. Reports are saved in the JUNOScope database, where all JUNOScope users can view them.

An Inventory Management System Demo lets you view and manipulate sample inventory reports so you can practice and learn the full potential of the system before scanning real production inventory data.

The Inventory Management System displays reports in a browser using HTML, and can also be exported to Extensible Markup Language (XML), Comma-Separated Values (CSV) text, Adobe PDF, and Microsoft Excel formats.

You must have superuser, read-write, or read-only access privilege levels to use the Inventory Management System reports.

This chapter includes the following topics:

Understanding Report Data Sources

A data source is a database from which you can view inventory report information. The Inventory Management System provides two report data sources:

- Inventory—Includes all inventory items that are created when you perform an inventory scan on Juniper Networks devices on the network that has been added

to JUNOScope. You must perform an inventory scan of devices on the network for the Inventory data source to have any data. For more information, see "Scanning Inventory Data" on page 339.

- Demo—A demonstration database that includes sample inventory items that you can use to practice viewing and manipulating inventory reports. When you open a demo report, you see the word Demo in the title bar area to differentiate from your production inventory reports. Some of the reports shown in this chapter are generated using the Demo database.

To view Inventory Management System report data sources, from the JUNOScope main window, click Inventory Management > Reports.

This section includes the following topics:

Viewing a Report

You can view a report of inventory data that has been scanned and stored in the database from devices on your network. Additionally, you can view reports from the demonstration database. For information about scanning inventory items, see "Scanning Inventory Data" on page 339.

To view a report, follow these steps:

1. Click Inventory Management > Reports. The Select a Data Source page appears.
2. Click Inventory or Demo. The Select a Report page appears.
3. Click the Report that you want. The Report Results page appears with the report that you selected. The following report (Software Inventory—All) is generated from the Inventory Management System demo database.

NOTE: If a report remains idle for more than 30 minutes, any subsequent manipulation on the expired report will result in an error message " Report instance expired. Please select a data source again." Click Select a Data Source in the top right area of the title bar. Then select the report that you were viewing from the Select a Report page.

For information about types of Inventory reports, see "Understanding Report Data Sources" on page 345.

NOTE: Inventory reports display inventory results for both the TX Matrix platform and the attached T640 routing nodes. The TX Matrix routing platform consist of the TX Matrix platform (also known as the switch-card chassis [SCC]) and the attached T640 routing nodes (also known as line-card chassis [LCC]).

Understanding Types of Inventory Reports

The Inventory Management System provides the following types of reports:

- Events Inventory Reports on page 347
- Hardware Inventory Reports on page 348
- Licensing Inventory Reports on page 350
- Software Inventory Reports on page 351

Events Inventory Reports

Events reports list any changes or discrepancies found in an inventory scan as compared with the inventory data stored in the database.

Table 22 on page 347 describes the type of inventory events that occur when JUNOScope scans device inventory.

Table 22: Events Types

Event	Description
CREATE	Initial discovery of an inventory item.
ADD	Inventory item added to a device although it was previously associated with the same or a different device (applicable to hardware inventory items only).
DELETE	Inventory item removed from a device.
UPDATE	Change in an inventory item attribute.
UNKNOWN	Unable to store inventory item in the database due to a missing serial number, licensed feature name, or software package name.

NOTE: Physical Interface Cards (PICs) and Flexible PIC Concentrators (FPCs) are tracked during an inventory scan by their containing chassis and slot position within the chassis. Therefore, if you move a PIC from FPC 0 to FPC 1 within the same chassis or to a different chassis, a DELETE event is generated with the old location and an ADD event is generated with the new location.

Table 23 on page 348 describes the type of JUNOScope inventory event reports that are available. To view inventory reports, see “Viewing a Report” on page 346.

Table 23: Type of Events Reports

Report	Description
All	Displays all inventory event records stored in the database. The report displays records by device name, event type, item name, item description, event details, serial number, Routing Engine, and time. (See Table 24 on page 348 for a description of the report columns.)
Search	Lets you search for specific inventory event records by device name, event type, item name, hardware description, license description, event details, serial number, item name, item description, event details, serial number, routing engine, or time. When you select Search, the (Search) Specify Parameters dialog box appears where you can specify the inventory records you want searched. (See "Searching for Inventory Report Data" on page 352 for more information about searching for inventory report records.)

Table 24 on page 348 describes the Events report columns.

Table 24: Events Report Columns

Report Column	Description
Device	DNS name of device.
Type	Type of event. Event types include CREATE, ADD, DELETE, UPDATE, and UNKNOWN.
Item	Name of the inventory item scanned and stored in the JUNOScope database.
Description	Description of the inventory item scanned and stored in the JUNOScope database.
Event Details	Description of an action that caused an inventory event.
Serial Number	Component serial number. The serial number is not displayed for software or licensing inventory items.
Routing Engine	Routing Engine on which the JUNOS software package is installed. This column differentiates software inventory events associated with multiple Routing Engines in a given device.
Time	Date and time the event record was scanned and stored in the JUNOScope database.

Hardware Inventory Reports

Hardware inventory reports list the hardware components installed in a device or router chassis, including the part number and serial number.

Table 25 on page 349 describes the type of hardware inventory reports. To view inventory reports, see "Viewing a Report" on page 346.

Table 25: Types of Hardware Inventory Reports

Report	Description
All	Displays all hardware inventory records stored in the database. The report displays records by device name, router model number, hardware name, version, part number, Field Replaceable Unit (FRU) model number, Common Language Equipment Identifier (CLEI) code, serial number, hardware description, chassis identifier, module, submodule, sub-submodule, time created, and time last scanned. (See Table 26 on page 349 for a description of the report columns.)
Search	Lets you search for specific hardware inventory records by device name, router model number, hardware name, version, part number, Field Replaceable Unit (FRU) model number, Common Language Equipment Identifier (CLEI) code, serial number, hardware description, chassis identifier, module, submodule, sub-submodule, time created, and time last scanned. When you select Search, the (Search) Specify Parameters dialog box appears where you can specify the inventory records you want searched. (See "Searching for Inventory Report Data" on page 352 for more information about searching for inventory report records.)
Summary	Displays a listing of all device names by model number. (See Table 26 on page 349 for a description of the report columns.)

Table 26 on page 349 describes the Hardware Inventory report columns.

Table 26: Hardware Inventory Report Columns

Report Columns	Description
Device	DNS device name.
Model	Routing platform.
Name	Name of the hardware component.
Version	Version of the hardware firmware.
Part Number	Hardware component part number.
FRU Model Number	Field Replaceable Unit model number. The FRU Model Number will not be displayed if a JUNOS version earlier than 8.2 is intalled on the device.
CLEI code	Common Language Equipment Identifier code used to identify network hardware. The CLEI code will not be displayed if a JUNOS version earlier than 8.2 is installed on the device.
Serial Number	Hardware component serial number.
Description	Hardware component description.
Chassis	Routing platform chassis in which the hardware component is installed. Information is displayed in this column for the TX Matrix routing platform.
Module	Component installed in the chassis; for example, an FPC.

Table 26: Hardware Inventory Report Columns *(continued)*

Report Columns	Description
Sub module	Component installed inside another router component. A PIC is a submodule installed inside an FPC.
Sub sub module	Component installed inside a submodule. An SFP is a sub-submodule installed inside a PIC.
Created	Date and time the hardware item was scanned.
Last Scanned	Date and time the hardware item was previously scanned.

Licensing Inventory Reports

Licensing inventory reports list the feature licenses that have been installed on devices in the network, including the name of the licensed feature, number of licenses installed, number of licenses that are currently being used, and the number of licenses that are required to legally use the feature.

Table 27 on page 350 describes the type of licensing inventory reports. To view inventory reports, see "Viewing a Report" on page 346.

Table 27: Types of Licensing Inventory Reports

Report	Description
All	Displays all licensing inventory records stored in the database. The report displays records by device, model number, feature name, description, licenses installed, licenses used, licenses needed, time created, and time last scanned. (See Table 28 on page 350 for a description of the report columns.)
Search	Lets you search for specific licensing inventory records by device, model number, feature name, description, licenses installed, licenses used, licenses needed, time created, and time last scanned. When you select Search, the (Search) Specify Parameters dialog box appears for you to specify the inventory records you want searched. (See "Searching for Inventory Report Data" on page 352 for more information about searching for inventory report records.)
Summary	Displays the total number of feature license that are needed by feature name. (See Table 28 on page 350 for a description of the report columns.)

Table 28 on page 350 describes the Licensing Inventory report columns.

Table 28: Licensing Inventory Report Columns

Report Columns	Description
Device	DNS device name.
Model	Routing platform on which the feature license inventory item exists.

Table 28: Licensing Inventory Report Columns *(continued)*

Report Columns	Description
Feature Name	Feature license name.
Description	Feature license description.
Licenses Used	Feature licenses used on a device.
Licences Installed	Feature licenses installed on a device.
Licenses Needed	Feature used but not licensed.
Created	Date and time the feature license item was scanned.
Last Scanned	Date and time the feature license item was previously scanned.

Software Inventory Reports

Software Inventory reports list the JUNOS software and its packages that have been installed on devices in the network, including the package name, package description, JUNOS software version, the Routing Engine on which the software is installed, and the total number of devices on which each JUNOS version is installed. The Inventory Management System scans software inventory by package. A package is a collection of files that make up a software component.

Table 29 on page 351 describes the JUNOS software packages.

Table 29: JUNOS Software Packages

Package	Name
jkernel	JUNOS Kernel Software Suite
jbase	JUNOS Base OS Software Suite
jroute	JUNOS Routing Software Suite
jpfe	JUNOS Packet Forwarding Engine Support
jdocs	JUNOS Online Documentation
jcrypto	JUNOS Crypto Software Suite
jggsn	JUNOS GGSN Software
junos	JUNOS Base OS boot
jweb	JUNOS Web Management software

Table 30 on page 352 describes the types of software inventory reports. To view inventory reports, see “Viewing a Report” on page 346.

Table 30: Types of Software Inventory Reports

Report	Description
All	Displays all JUNOS software package inventory records stored in the database. The default report displays records by device name, model, Routing Engine on which the software package is installed, JUNOS software version, package name, package comment, time the record was created, and time the package was last scanned. (See Table 28 on page 350 for a description of the report columns.)
Search	Lets you search for specific JUNOS software package inventory records by device name, model, Routing Engine on which the software package is installed, package name, package description, time the record was created, and time the package was last scanned. When you select Search, the (Search) Specify Parameters dialog box appears where you can specify the inventory records you want searched. (See "Searching for Inventory Report Data" on page 352 for more information about searching for inventory report records.)
Summary	Displays the total number of devices on which each JUNOS version is installed. Inventory records are listed by software version, device name, model, and the Routing Engine on which the software is installed. (See Table 28 on page 350 for a description of the report columns.)

Table 31 on page 352 describes the Software Inventory report columns.

Table 31: Software Inventory Report Columns

Report Columns	Description
Device	DNS device name
Model	Routing platform on which the software package was scanned
Routing Engine	Routing Engine on which the software package is installed
JUNOS Version	Version of the JUNOS software
Package Name	Name of the software package
Package Comment	Description of the software package
Created	Date and time the software package inventory item was created
Last Scanned	Date and time the software package inventory item was previously scanned

Searching for Inventory Report Data

The Search Report option lets you specify the information that you want to appear in the report results. The Search—Specify Parameters dialog box lets you search for specific inventory items depending on the selected report type.

To search for inventory report data, follow these steps:

1. Click Inventory Management > Reports. The Select a Data Source page appears.
2. Click Inventory. The Select a Report page appears.
3. Click the Search under the report type that you want. The Specify Parameters dialog box appears.
4. Select the inventory item search operator in the drop-down list box next to the inventory item name. For more information about search operators, see Table 33 on page 359.
5. Select the inventory item description or value in the drop-down list box next to the search operator. Type or copy a particular description for which you want to search.
6. Click Submit Query. The Inventory Management System displays a report displaying the information for which you specified.
7. The Report Result page displays the search item and value. Click the edit link to edit and specify a different search, if necessary.

Navigating a Report

You can scroll through a report in the Report Result window or display specific device data.

Scrolling Through a Report

The Report Result window displays 50 lines of report data at a time in a window.

To scroll through a report, do one of the following:

- To scroll forward through a report one page at a time, click the right arrow (>).
- To scroll backward through a report one page at a time, click the left arrow (<).
- To scroll forward to the end of the report, click the double right arrows (> >).
- To scroll backward to the beginning of the report, click the double left arrows (< <).

Displaying Specific Device Data

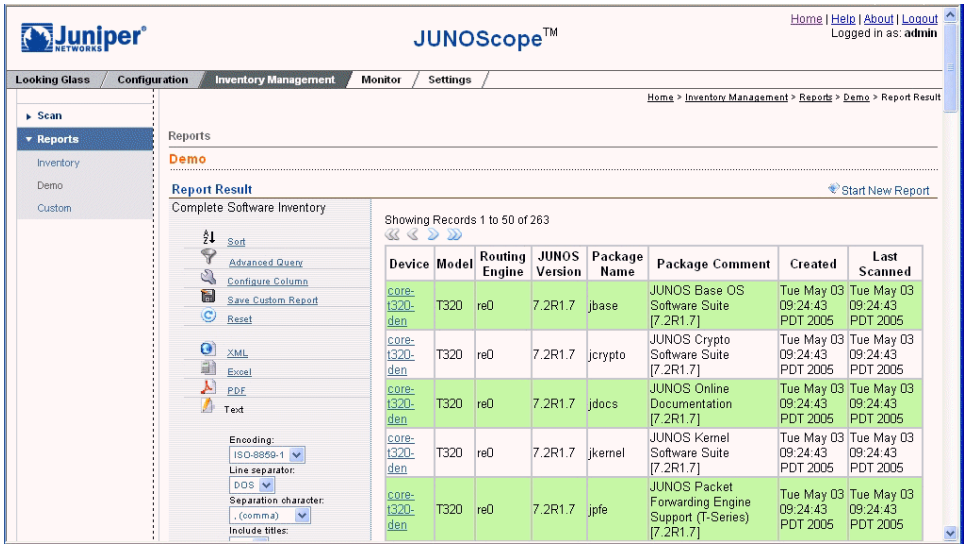
To display data for a specific device, in the report you are viewing, click the name of the device in the Device column. You can also view a specific device report by selecting a Device report under each inventory report type.

Starting a New Report

If the report you are viewing is not the one that you want, you can select to open a new report.

To start a new report, follow this step:

1. From any Report Results page, click Start New Report. The Start New Report command is located at the top right of the Report Results page title bar area.



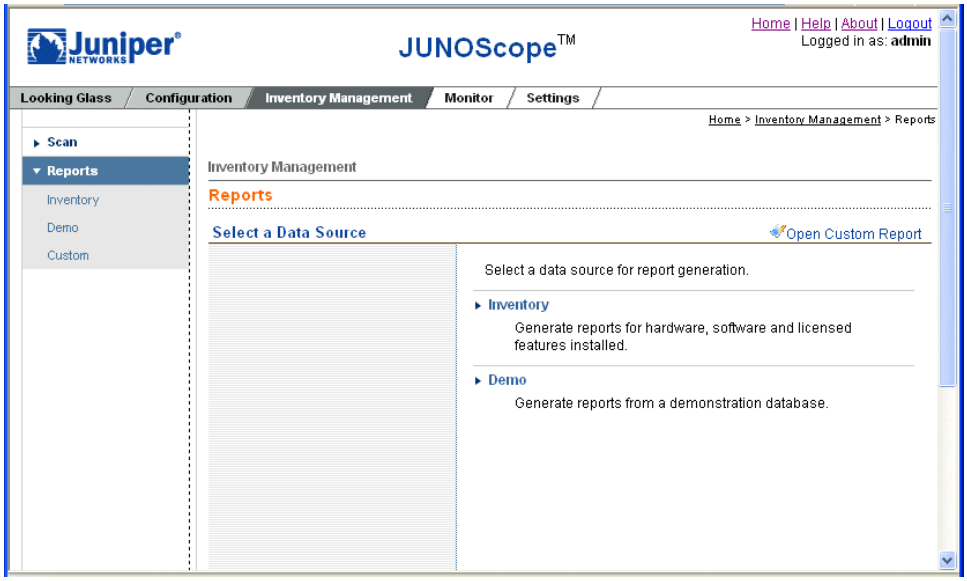
The Select a Report page appears. For more information about the type of inventory reports, see “Understanding Types of Inventory Reports” on page 347.

Opening a Custom Report

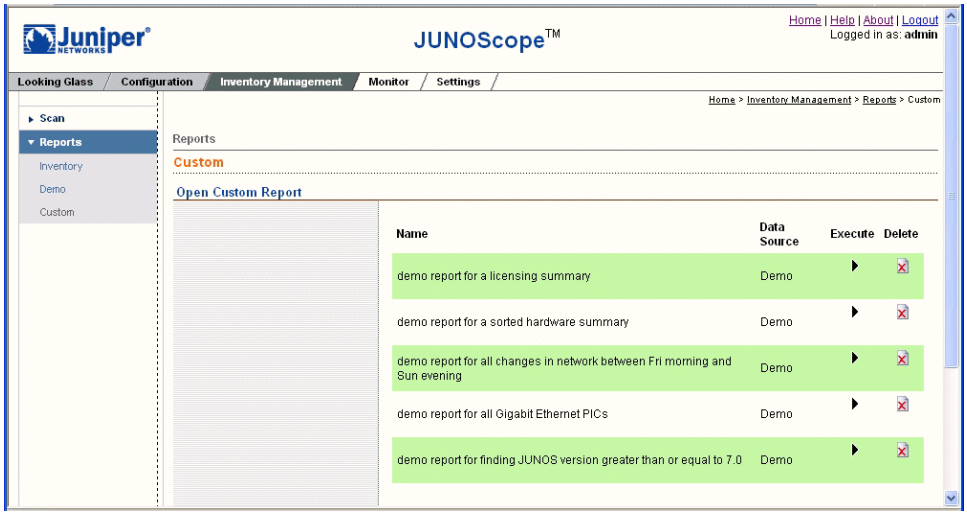
A custom report is one that you have saved with customizations. All JUNOScope users can open saved custom reports.

To open a custom report, follow these steps:

1. Click Inventory Management > Reports. The Open Data source page appears.



2. Do one of the following:
   - Click Custom in the command pane at the left.
   - Click Open Custom Report at the far right in the title bar area.
3. In the left command pane under Reports, click Custom. The Open Custom Report dialog box appears. If you have not saved a report, the dialog box looks like the following.



4. Select the filename of the report you want to open.
5. Click the Execute arrow next to the report name.

Manipulating Report Data

From any Report Results page, you can use the tools to manipulate report data for your specific needs. Table 32 on page 356 describes each tool.

Table 32: Report Tools

Tool	Name	Description
	Sort	Arranges inventory records in ascending sort order from small to big (where string 123 appears first, followed by string abc, then followed by string ABC); with the exception of event time in descending order (where the latest event appears first). For example, a sort by type will display ADD first, followed by CREATE, DELETE, and UNKNOWN. To sort a report, see "Sorting Report Data" on page 356 .
	Advanced Query	Queries report records to display only those based on the criteria that you specify. You can show the query as columns or rows. To filter a report, see "Querying Report Data" on page 358 .
	Configure Column	Changes the order in which columns appear in an inventory report. To configure report columns, see "Configuring Report Columns" on page 363 .
	Reset	Clears all previously set customized controls such as sort, advanced query, and configure column, then regenerates the report with the default controls.
	Save Custom Report	Saves a report with the customizations that you specified in a file with a unique name that you specify.
	XML	Displays a report in XML format. To view a report in XML format, see "XML" on page 365.
	Excel	Displays a report in Microsoft Excel. To view a report in Excel, see "Microsoft Excel" on page 365.
	PDF	Displays a report in an Adobe Acrobat viewer. To view a report in Adobe Acrobat in PDF format, see "Adobe Acrobat PDF" on page 366.
	Text	Displays a report in text format. To view a report in text format, see "Text" on page 366.

Sorting Report Data

You can customize a report using predefined or user-defined column sort orders.

To sort a report, follow these steps:

1. Select and run the report that you want.
2. In the Report Result window, click the Sort tool. The Sort window appears.
3. Do one of the following:
   - Select a predefined column sort order. See "Sorting by a Predefined Order" on page 357.

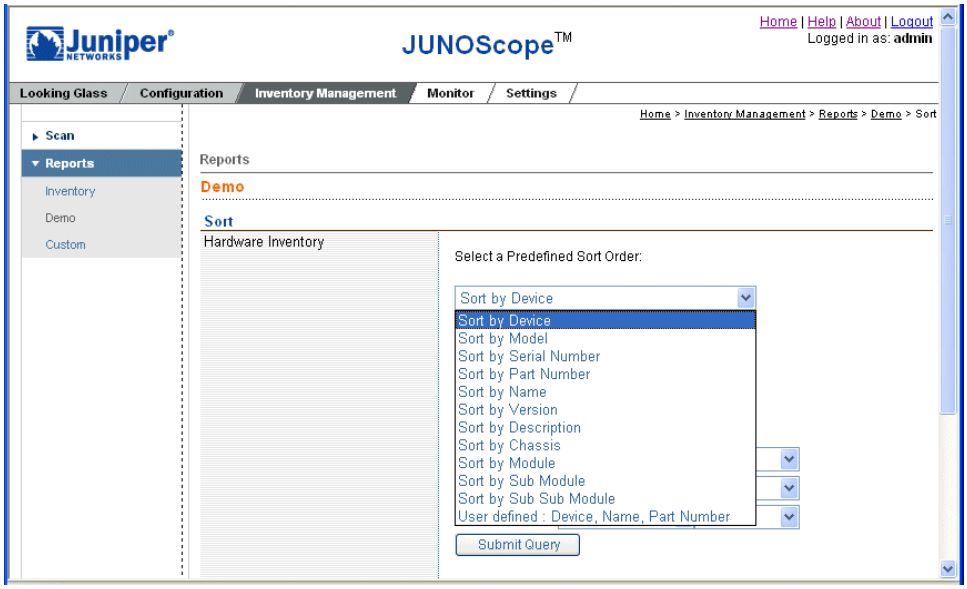
- Define your own column sort order. See “Sorting by User-Defined Order” on page 357.

Sorting by a Predefined Order

To sort a report by a predefined column sort order, follow these steps:

1. In the Select a Predefined Sort Order drop-down list box, select the predefined column sort option that you want. The column sort order options differ depending on the type of report you have selected—events, hardware inventory, licensing inventory, or software inventory.

   If you have selected a user-defined sort order, that option displays at the bottom of the Select a Predefined Sort Order drop-down list box.



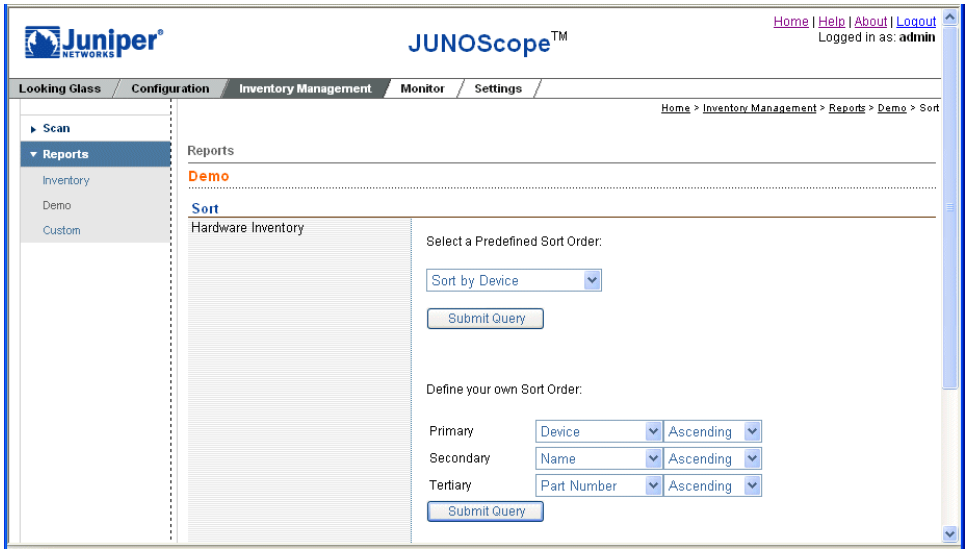
2. Click Submit Query.

Sorting by User-Defined Order

You can sort the records in the columns in primary, secondary, and tertiary order. For example, if two rows have the same values for the primary sort criteria, they will be sorted based on their values for the secondary sort criteria. Records are sorted alphabetically, numerically, or by time (the latest time is the largest value).

To sort by a user-defined column sort order, follow these steps:

1. Select the primary column item that you want sort. Click the down arrow to view the column selections.



2. Select the column sort order: ascending or descending.
3. Select the secondary and tertiary column items, then select the sort order. Click the down arrow to see the selections.
4. Click Submit Query.

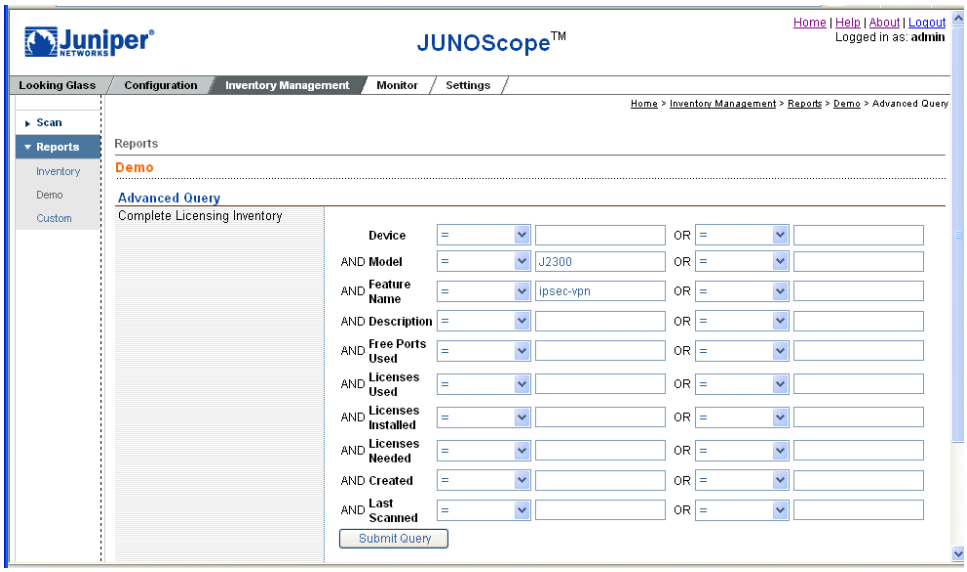
NOTE: If you leave a column sort level blank, sorting stops at the last level you specify. Contradicting sorts are ignored. Sort performs the primary sort level, while the secondary contradicting sort level is suppressed.

Querying Report Data

You can specify to display only specific report information in which you are particularly interested. You can show a query as either columns or rows. You can then specify the query criteria.

To perform an advanced query, follow these steps:

1. Select the report that you want. To run a report, see “Viewing a Report” on page 346.
2. In the Report Result window, click the Advanced Query tool. The Advanced Query dialog box appears.



3. Do one of the following:

   - For events reports, specify the query criteria for the device name, event type, item name, description, event details, serial number, Routing Engine, or time.
   - For hardware inventory reports, specify the query criteria for the device name, model, hardware name, hardware version, part number, serial number, hardware description, chassis ID, module, submodule, sub-submodule, time created. or time last scanned.
   - For licensing inventory reports, specify the query criteria for the device, model, feature name, feature description, free ports used, licenses used, licenses installed, licenses needed, time created, or time last scanned.
   - For software inventory reports, specify the query criteria for the device name, model number, Routing Engine on which the software package is installed, software version, package name, package description, time created, or time last scanned.
   - Select an Device query operator. Table 33 on page 359 provides a reference for the query operators you can select.

Table 33: Advanced Query Operators

Operator	Description
=	(The default operator) Searches for records that exactly equal the search criteria.
not =	Searches for records that do not match the search criteria.
between	Searches for records that fall between a specified range.
not between	Searches for records that do not fall between a specified range.
in	Searches for records that match any of the specified values (up to four).

Table 33: Advanced Query Operators *(continued)*

Operator	Description
not in	Searches for records that match none of the specified values (up to four).
<	Searches for records that are less than the search criteria.
< =	Searches for records that are less than or equal to the search criteria.
>	Searches for records that are greater than the search criteria.
> =	Searches for records that are greater than or equal to the search criteria.
empty	Searches for records that have an empty value in the specified column/field. For example, perform an advance query for events inventory with "serial number is not empty" and do one with "serial number is empty".
not empty	Searches for records that have a non-empty value in the specified column/field.
like	Searches for records that match the search criteria.
not like	Searches for records that do not match the search criteria.

NOTE: For the like and not like operators, use % as the wildcard for the matching target. For example, bad % would match badlands but not toobadlands. To match toobadlands, use %bAd%. The match is case insensitive.

4. In the Device search text box, type a device name in the Device search text box. You can also click the device name in the report to view all records for that report.
5. Select an event Type search operator.
6. In the Type search text box, type the event type that you want to see in the Type search text box.
7. Select a Time search operator.
8. In the Time search text box, type a time. For this procedure, type the current date and time. You can copy a specific date and time from a report and paste it into the search text box.

NOTE: The format for Time is *EEE MMM dd HH:mm:ss z yyyy* , where:

EEE = Day in week (for example, Tue.)

MMM = Month in year (for example, Jan.)

dd = Day in month (for example, 05)

HH = Hour in day (for example, 23)

mm = Minute in hour (for example, 20)

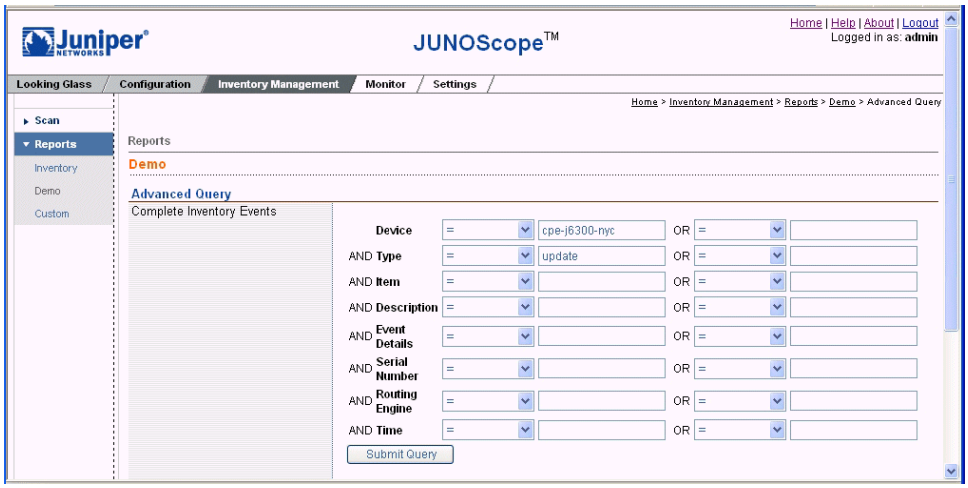
ss = Second in minute (for example, 47)

z = Time zone (for example, GMT)

yyyy = Year (for example, 2004)

9. Click Submit Query. The criteria you specified is displayed in the Report Result page.

   For example, the following is an all events report advanced query.



   The query produces the following report.

The like operator applies to columns with a string value such as device, type, item, description, event details, serial number, and Routing Engine in any Events Inventory reports. The like operator does not apply to Time, which has a type of Date.

For more information about using the like operator, see “Using the Like Device Query Operator” on page 362.

To search for all items created on or after 3-5-2004 8pm PST 2004, type the following in the search field: >= Fri Mar 05 20:00:00 PST 2004.

Using the Like Device Query Operator

The like operator uses % as the wildcard character. The following are several examples of how to use the like operator wildcard to display specific information.

Example 1 To search for all Gigabit Ethernet cards on the network, follow these steps:

1. On the Select a Reports page, select Hardware Inventory > All. The Report Result page appears.
2. Click Advanced Query. The Advanced Query dialog box appears.
3. In the And Description drop-down list box, select like.
4. In the text box next to the And Description drop-down list box, type **%G/E%**.
5. Click Submit Query. The Report Result page displays all of the Gigabit Ethernet cards by device.

Example 2 To search for all Gigabit Ethernet PICs on the network, follow these steps:

1. On the Select a Reports page, select Hardware Inventory > All. The Report Result page appears.
2. Click Advanced Query. The Advanced Query dialog box appears.
3. In the And Description drop-down list box, select like.
4. In the text box next to the And Description drop-down list box, type **%G/E%**.
5. In the And Sub Module drop-down list box, select like.
6. In the text box next to the And Sub Module drop-down list box, type **%PIC%**.
7. Click Submit Query. The Report Result page displays all of the Gigabit Ethernet PICs by device.

Example 3 To search for all 4X Gigabit Ethernet PICs on the network, follow these steps.

1. On the Select a Reports page, select Hardware Inventory > All. The Report Result page appears.
2. Click Advanced Query. The Advanced Query dialog box appears.
3. In the And Description drop-down list box, select like.
4. In the text box next to the And Description drop-down list box, type **%4X G/E%**.
5. Click Submit Query. The Report Result page displays all of the 4X Gigabit Ethernet cards by device.

Example 4 To search for a particular PIC, such as an 4X G/E, 1000Base-SX PIC on the network, follow these steps:

1. On the Select a Reports page, select Hardware Inventory > Search. The Specify Parameters page appears.
2. In the Description drop-down list box, select 4X G/E, 1000 BASE-SX. The drop-down list box includes a description of all hardware available on the network.

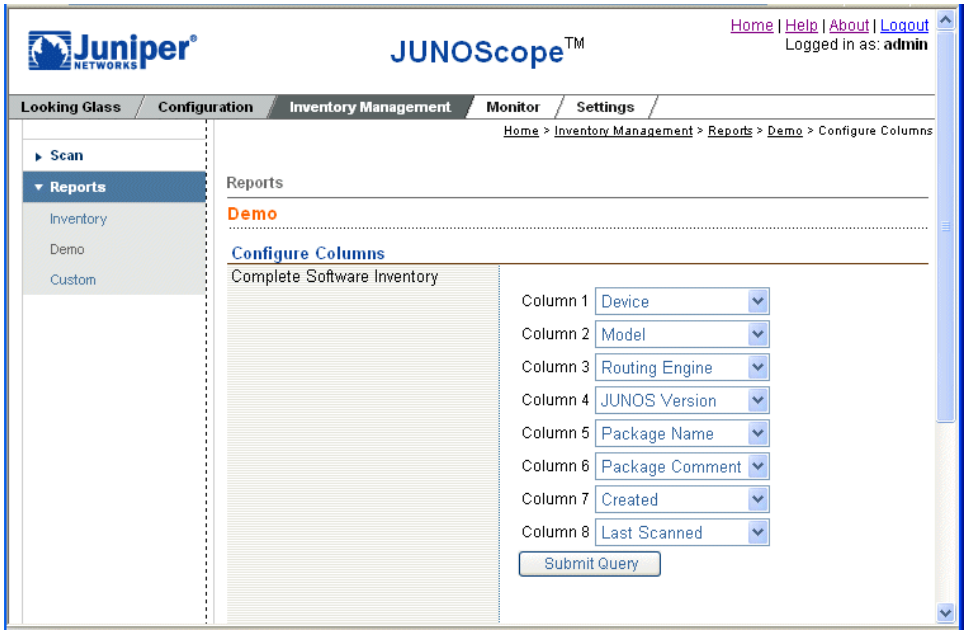
3. Click Submit Query. The Report Result page displays all of the 4X G/E, 1000Base-SX PICs by device name.

Configuring Report Columns

You can change the order in which columns appear in a displayed report.

To change the column order in a report, follow these steps:

1. Select the report that you want. To run a report, see "Viewing a Report" on page 346.
2. In the Report Result window, click Configure Column. The Configure Columns dialog box appears.



3. Configure the order of the columns as you want them to appear in your report by selecting a name for each column number. Use the drop-down text boxes to select column names.

   The column options differ depending on the type of report you have selected:

- For event reports, the default column display order is device, type, item, description, event details, serial number, and time.
  - For hardware inventory reports, the default column display order is device, model, name, version, part number, serial number, description, chassis ID, module, submodule, sub-submodule, created, and last scanned.
  - For licensing inventory reports, the default column display order is device, model, feature name, description, free ports used, licenses used, licenses installed, licenses needed, created, and last scanned.
  - For software inventory reports, the default sort order is device name, model number, Routing Engine on which the software image is installed, software

version, software package name, package description, date when the software inventory record was created, and the date when the software inventory record was last scanned.

NOTE: The report column sort order you specify remains in effect until you change it again.
If you leave a column name empty, that column and subsequent columns will not appear in the report.

Resetting Report Customizations

Use Reset to clear all customized controls previously set, such as sort, advanced query, and configure column, and regenerate the report with default controls.

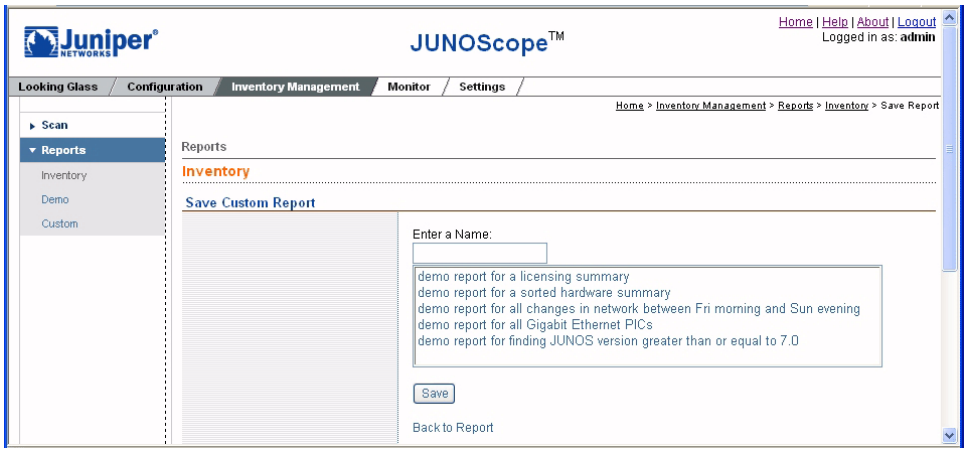
Saving a Custom Report

Use Save Custom Report to save any customization you make on a report, such as sort, advanced query, or configure columns. Saved reports are shared among all users. All saved reports are identified by their unique filenames.

NOTE: Users with superuser and read-write privileges can save custom inventory reports.

To save a report, follow these steps:

1. Select and run the report that you want.
2. Once you have a customized report (for example, sort, advance query, or configure columns), click Save. The Save Report dialog box appears.



3. Type a filename in the text box. The report name must always start with a letter, and can contain letters, numbers, and the characters . (period), - (dash), and _ (underscore). You can select a previously saved report to overwrite it.
4. Click Save or press Enter.

Deleting a Report

Users with superuser or read-only privileges can delete custom inventory reports.

To delete a report, follow these steps:

1. In the Report Results page, click Custom in the left command pane. The Save Custom Report dialog box appears.
2. Find the filename of the report you want to open.
3. Click the Delete [X] icon to the right of the report name.

Viewing Report Data

You can view inventory reports in Extensible Markup Language (XML), Adobe Acrobat Portable Document Format (PDF), Microsoft Excel, or text format. If you select PDF or Excel format, depending on the client (browser and operating system) MIME setting, Acrobat Reader or Excel will either appear inside the browser, or run as a standalone application.

XML

To view a report in XML, follow these steps:

1. Select and open the report you want.
2. In the Report Result window, click XML. The report appears in the Report Result window in XML. Save it using the File > Save menu of the browser.

Microsoft Excel

To view a report in Microsoft Excel, follow these steps:

1. Select and open the report you want.
2. In the Report Result window, click Excel. Microsoft Excel opens and displays the current report. You can manipulate the report in Excel, and save the file in XLS file format.

NOTE:

When you convert a report such as All Inventory Events to Microsoft Excel format, the time and date records in the Time column may not appear in the correct format. To format the Time column records correctly, follow these steps:

1. In Microsoft Excel, select the Time column.
2. Right-click to open the Format Cells dialog box.
3. Click the Number tab.
4. Select Time in the Category list box.
5. Select the correct time and date format in the Type list box.
6. Click OK.
7. Adjust the width of the Time column, if necessary, so that the entire value can be displayed.

   If the width of the Time column is narrower than the time value being displayed, a series of #### characters appear.

Adobe Acrobat PDF

To view a report in Adobe PDF, follow these steps:

1. Select and open the report you want.
2. In the Report Result window, click PDF. Adobe Acrobat Reader opens and displays the current report. You can manipulate the report in Adobe Acrobat, and save the file in PDF file format.

Text

You can view Inventory Management System reports in text format.

NOTE: You can view reports in text format for all report types except Hardware Inventory Summary and Licensing Inventory Summary.

Table 34 on page 367 describes the supported text format.

Table 34: Report Text Formatting Options

Text Format	Option	Description
Encoding	ISO-8859-1	Also called ISO-Latin or Latin-1, this character set is used for HTTP (the transport protocol for Web documents) and is also used in the creation of HTML documents.
	US-ASCII	American Standard Code for Information Interchange, the standard character set for use on the Internet.
	UTF-8	8-bit Unicode Transformation Format, a lossless, variable-length character encoding for Unicode.
	UTF-16	16-bit Unicode Transformation Format, a character encoding form that provides a way to represent a series of abstract characters from Unicode and ISO/IEC 10646 as a series of 16-bit words suitable for storage or transmission by way of data networks.
Line separator	DOS	DOS and Windows operating systems use carriage return and line feed (CR/LF) as the line separator.
	UNIX	UNIX uses LF as the line separator.
Separator character	, (comma)	Character used to separate report data columns.
	; (semicolon)	Character used to separate report data columns.
	tab	Character used to separate report data columns.
	| (pipe)	Character used to separate report data columns.
	space	Character used to separate report data columns.
	none	No character used to separate report data columns.
Include titles	Yes	Includes report data column titles.
	No	Does not include report data column titles.

To view a report in text format, follow these steps:

1. Select and open the report you want.
2. In the Report Result window, click the Text options that you want.
3. Click Get Text.

Where To Go From Here

- To use the Inventory Management System to scan for device inventory items, see “Scanning Inventory Data” on page 339.

- To extract Inventory Management System data to an external inventory application using a read-only SQL interface, see “Exporting Inventory Management System Data” on page 379.

Chapter 32

Scheduling Custom Inventory Reports and Viewing Archived Inventory Reports

This chapter describes how to schedule custom Inventory Management System reports—such as event, hardware, software, licensing—to run at a specified time without intervention. Custom inventory reports are generated when you select an existing report and save it using a unique name.

You can schedule custom inventory reports that you save by associated them with a schedule that is created using Settings > Schedules.

You can save scheduled custom inventory report operations and combine them with other operations—such as archive, restore, scan inventory, install image, or download image—using Task Manager (Settings > Saved Operations) to run at a specified time.

Once a custom inventory report is run, the Inventory Management System archives that report in the repository, so you can view it at a later time in Adobe PDF or Microsoft Excel format using Inventory Management > Repository > View. Additionally, you can view the custom inventory report operation status, including report name, username, status, start time, and status message, using Monitor > Status.

To schedule custom inventory reports and view inventory report status, you must have superuser and read-write privileges. All users can monitor custom inventory report status. To view custom inventory reports, you must have either superuser, read-write privileges.

If a custom report is archived successfully, a successful system log messages is generated. If a report can not be archived successfully, an error system log message is generated. For more information about JUNOScope system log messages, see "JUNOScope System Log Messages" on page 695.

This chapter includes the following topics:

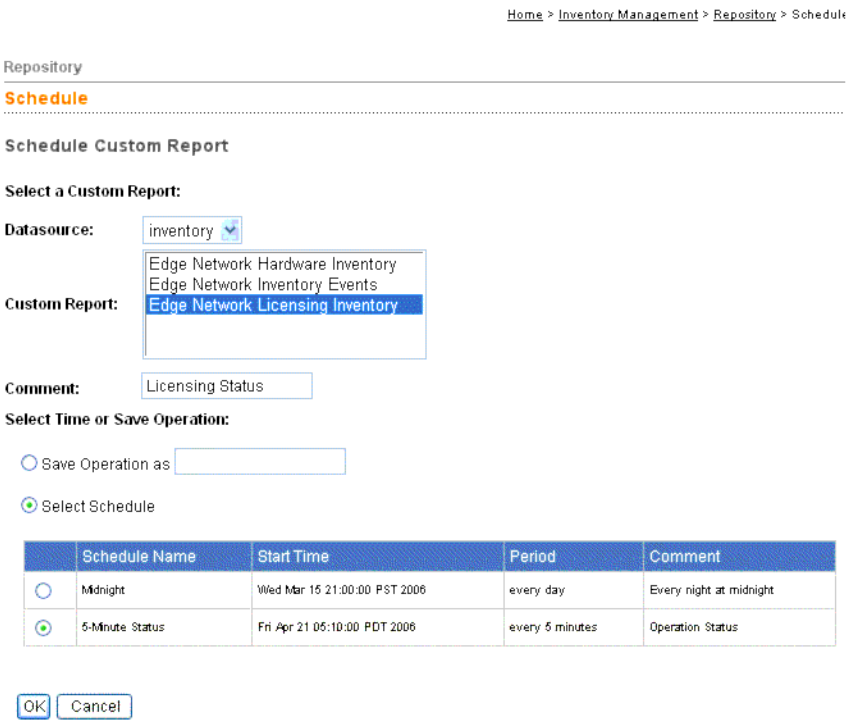
Scheduling a Custom Inventory Report

You can schedule custom inventory reports to run at a specified time. You cannot schedule predefined Inventory Management System reports, because no name has been associated with them.

A user with superuser privileges can create a report schedule using Settings > Repository > Schedule. A user with superuser and read-write privileges can associate a custom inventory report with that schedule.

1. In the JUNOScope main window, click Inventory Management > Repository > Schedule.

   The Schedule Custom Report dialog box appears.



2. Select a data source for the report.

   Demo is the only data source available until you perform an inventory scan on your network devices. Thereafter, the Inventory data source is available. For information about Inventory Management System data sources, see “Understanding Report Data Sources” on page 345.

3. Select a custom report.

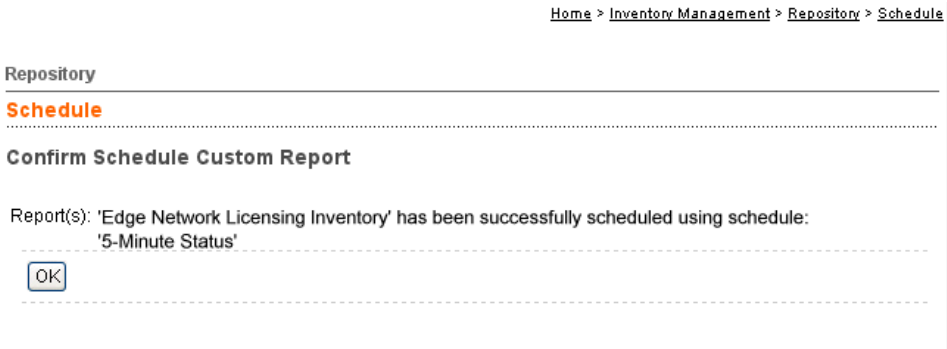
   A custom report is one that you have saved. Saved custom reports are listed in the Custom Report list box by name. To save a custom report, see “Saving a Custom Report” on page 364.

4. Click the Select Schedule option button, then select an existing schedule.

   Schedules that you have created using Settings > Schedules are listed in the Select Schedule table. If you have not created a schedule, see "Scheduling a Custom Inventory Report" on page 370.

5. Click OK.

   The Confirm Schedule Custom Report dialog box appears.



6. Ensure that the schedule inventory report options that you selected are correct, then click OK.

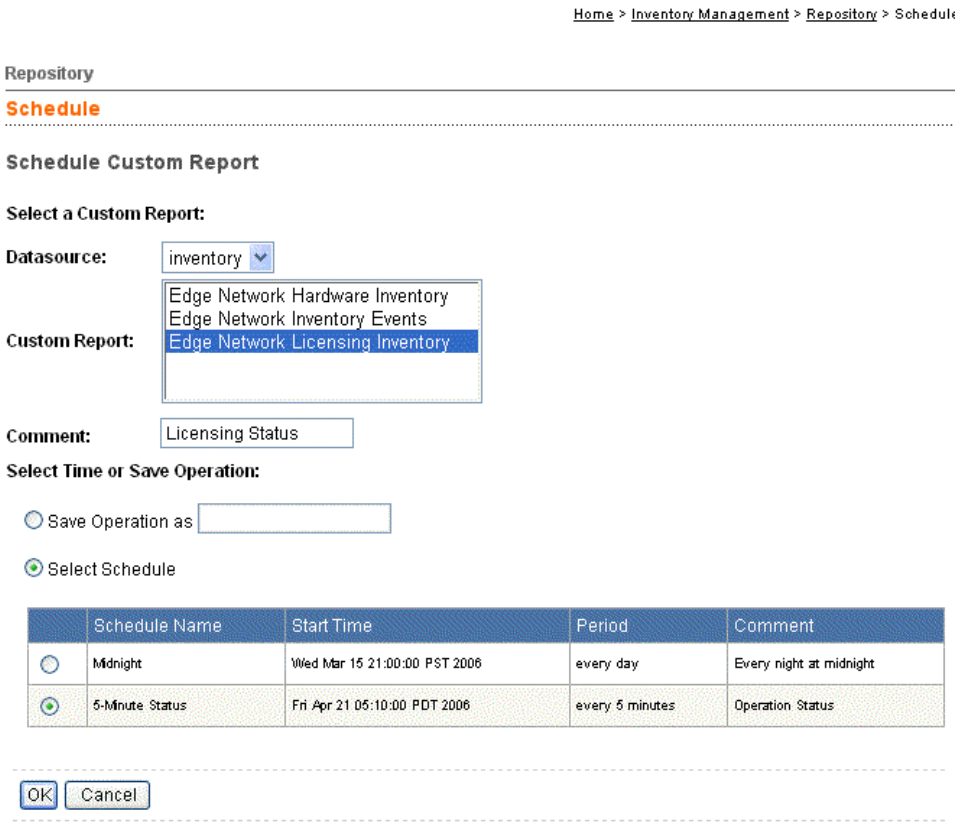
   The custom inventory report will run at the scheduled time that you specified. You return to the Schedule dialog box.

Saving Scheduled Custom Inventory Report Operations

You can save scheduled custom inventory report operations. Using Task Manager (Settings > Saved Operations), you can create compound operations from any simple and compound operations that you have saved, such as archive, restore, inventory scan, install image, or download image. For more information about working with saved operations, see "Using Task Manager (Saved Operations)" on page 167.

To save a custom inventory report operation, follow these steps:

1. In the JUNOScope main window, click Inventory Management System > Repository. The Schedule Custom Report dialog box appears.



2. Click the Save Operation as option button.
3. Type a name for the operation in the Save Operation as text box.
4. Click OK.

   The Confirm Save Schedule Report Operation dialog box appears.

5. Ensure that the save scheduled custom inventory operation options you selected to save are correct, then click OK.

   You return to the Schedule dialog box.

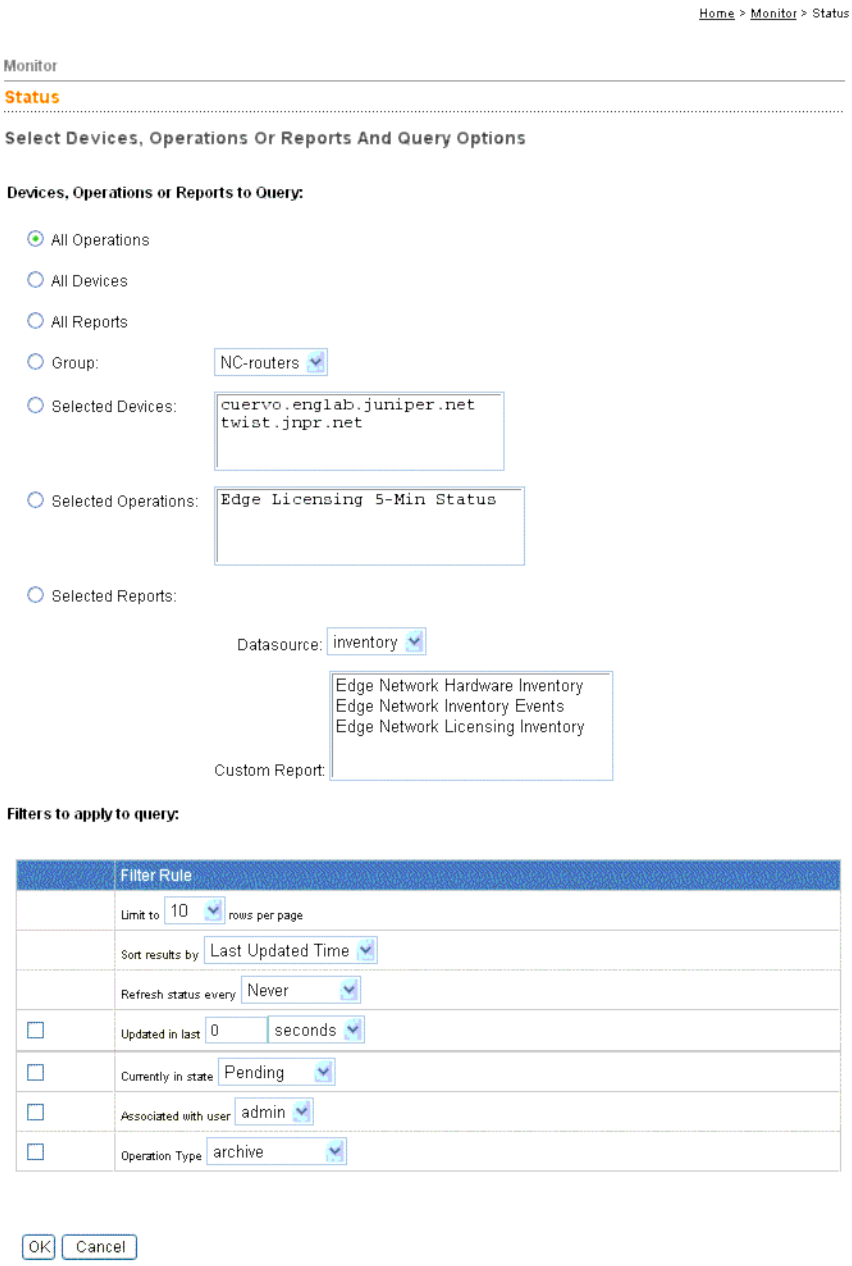
Monitoring Scheduled Custom Inventory Report Operation

All JUNOScope users can view the status of custom inventory reports that have run. The status of operations can be pending, connecting, working, writing, warning, success, or error.

To monitor the status of custom inventory report operations that have run, follow these steps:

1. In the JUNOScope main window, click Monitor > Status.

   The Status—Select Devices, Operations, Reports, and Query Options dialog box appears.

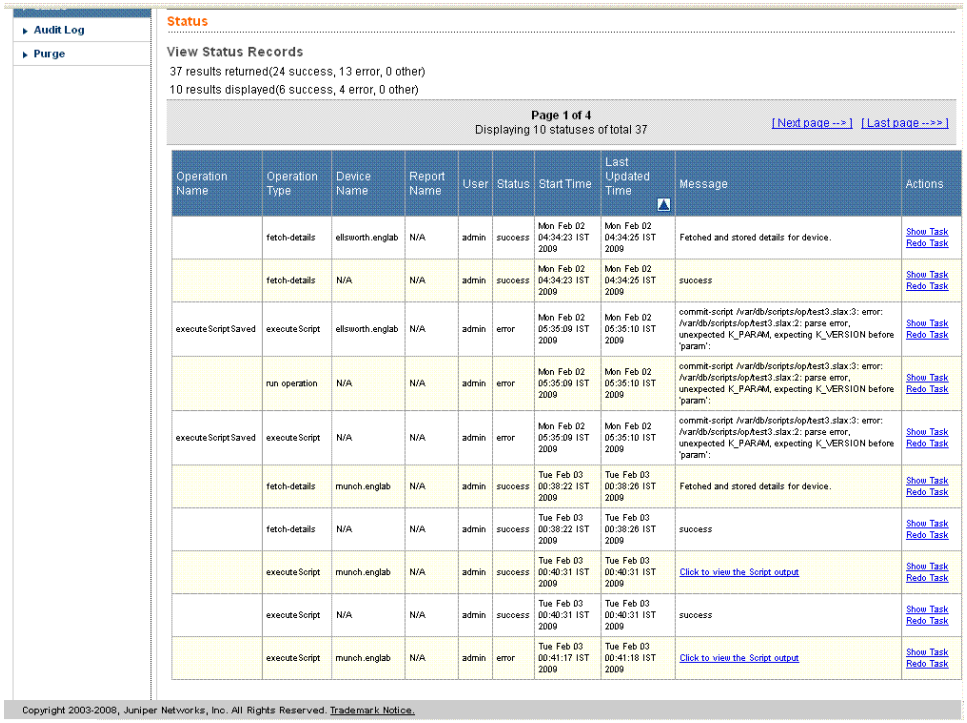


2. Select the operations to query.
3. Select the Groups or Devices to query.
4. Select the data source and the custom inventory reports to query.
5. Select the Filters to apply to view reports.

- Limit to <#> rows per page drop-down list box—Filters the operation status by the number of rows to display per page: 10, 25, 50, or 100. The default is 10 rows.
- Sort results by <*column name*> drop-down list box—Sorts the results by the last modified time, operation name, operation type, device name, username, status, start time, or message. The default is to sort by the last modified time.
- Refresh status every <*selected time*> drop-down list box—Updates the operation status at an interval that you specify: Never, 10 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, 15 minutes, 30 minutes, or 1 hour. The default is Never.
- Updated in last <*time period*> check box, text box, and drop-down list box—Filters the operation status results by the last time period that you specify. The default is 0 seconds. Select the check box to enable this filter rule. Type a time value in the time period text box. Click the down arrow to view the available time periods: seconds, minutes, hours, and days.
- Currently in *state* check box and drop-down list box—Filters the operation status by those that are currently in a particular state: pending, connecting, working, writing, success, and error. The default is Pending. Select the check box to enable this filter rule.
- Associated with *user* drop-down list box—Displays the operation status results for a selected username. The listed usernames that have been added using Settings > Users. Select the check box to enable this filter rule.
- Operation type drop-down list box—Displays the current JUNOScope operations that you can save, such as archive, restore, report, scan inventory, install, and download. The default is archive. Select the check box to enable this filter rule.

6. Click OK.

   The View Status Records dialog box appears with the status data that you queried.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

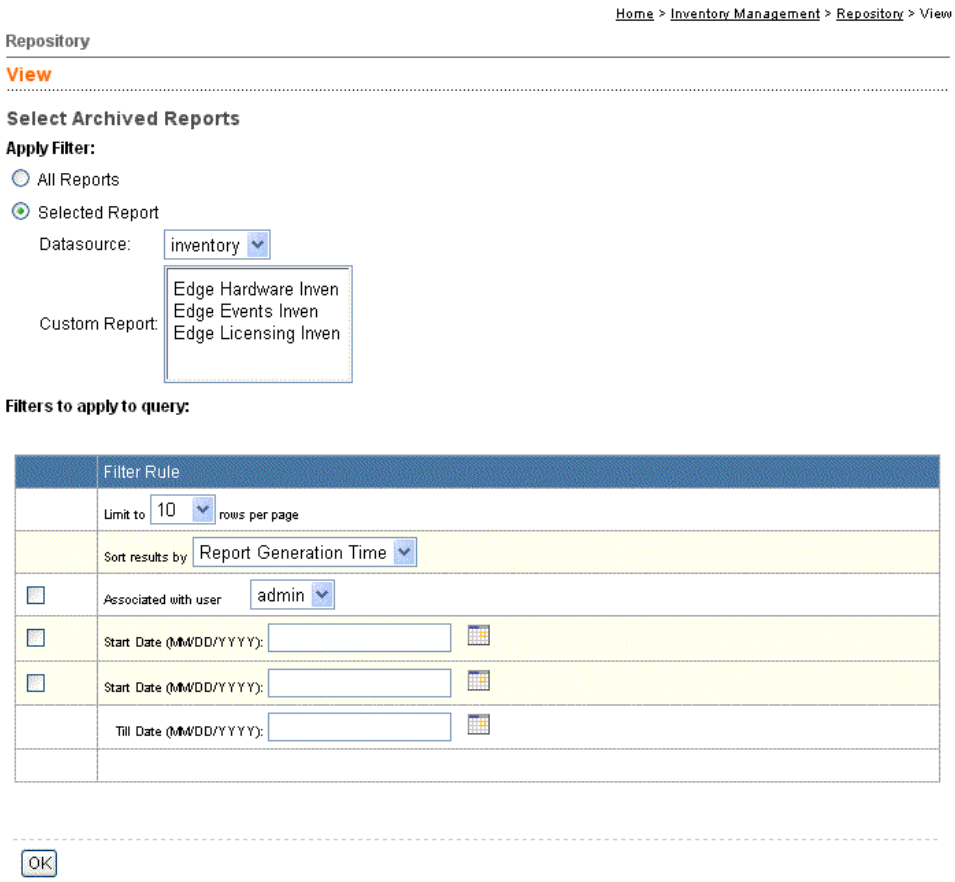
Viewing Archived Custom Inventory Reports

Once a custom inventory report runs, it is archived so you can view it later. If no custom inventory report operations have run, then you will not be able to see any archive report data. Only users with superuser and read-write access can view archived custom reports. Users with read-write privileges can view only those reports that are generated by that user. Users with superuser privileges can view reports generated by all users.

To view an archive report, follow these steps:

1. In the JUNOScope main window, click Inventory Management > Repository > View.

   The Select Archived Reports dialog box appears.



2. Select the report(s) to query.

   a. Select either the All Report or Selected Report option button.

   b. If you selected the Selected Report option button, select the data source, then select the custom report name in the Custom Report list box.

3. Select the Filters to apply to the status query:

   - Limit to <#> rows per page drop-down list box—Filters the operation status by the number of rows to display per page: 10, 25, 50, or 100. The default is 10 rows.

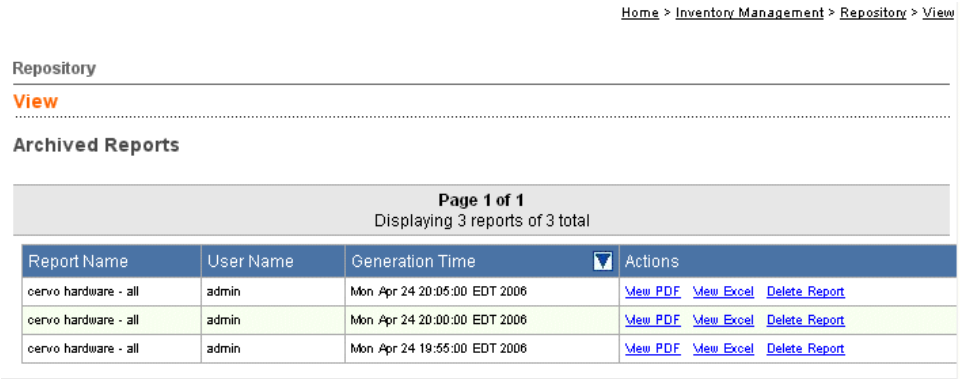
   - Sort results by <column name> drop-down list box—Sorts the results by the report generation time, report name, or username. The default is to sort by the report generation time.

   - Associated with *user* drop-down list box—Displays the operation status results that are associated with a selected username. The listed usernames have been added using Settings > Users. Select the check box to enable this filter rule.

- Start Datetext box and calendar—Specifies the beginning of a date range within which to view archived reports. Click the calendar icon to view the current month. Select the date that you want, then click OK. The date appears in the Start Date text box in *dd/mm/yyyy* format, where *dd* is the day, *mm* is the month, and *yyyy* is the year).
- Till Date text box and calendar—Specifies the end of a date range within which to view archived reports. Click the calendar icon to view a the current month. Select the date that you want then click OK. The date appears in the Start Date text box in *dd/mm/yyyy* format, where *dd* is the day, *mm* is the month, and *yyyy* is the year).

4. Click OK.

   The View Archived Reports dialog box appears.



   Archived reports are listed in the View Archived Reports dialog box by custom report name, username of the person who scheduled the report to run, and generation date when the report was run.

   - To view an archived report in Adobe Acrobat PDF format, click the View PDF link.
   - To view an archived report in Microsoft Excel format, click the View Excel link.
   - To delete an archived report, click the Delete Report link.

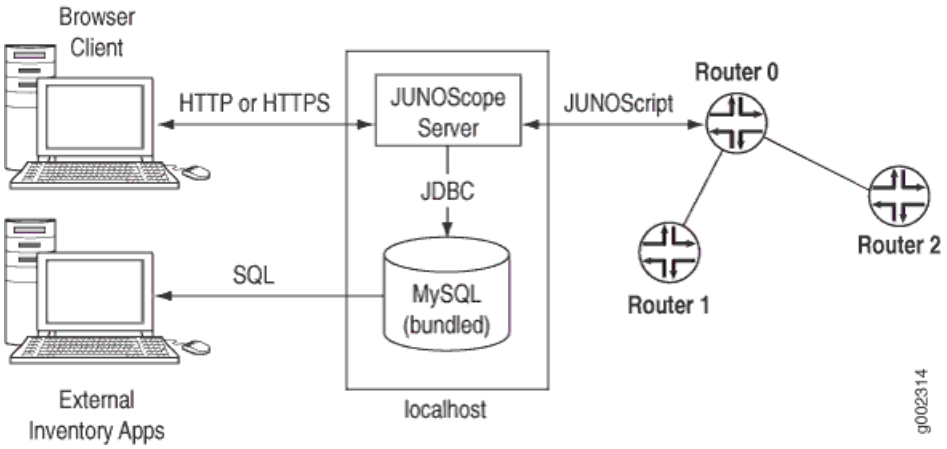
Chapter 33

Exporting Inventory Management System Data

This chapter is intended for users who are familiar with Relational Database Management Systems (RDBMS) and the Structured Query Language (SQL), who want to develop their own customer applications to access information from the JUNOScope Inventory Management System. It is not meant to be a complete SQL reference. Refer to your applicable SQL guides for complete reference information.

This chapter describes how an external inventory application can connect to the JUNOScope Inventory Management System database and extract Juniper Networks device inventory information by way of an SQL interface. The JUNOScope software is bundled with MySQL, an open source relational database management system (RDBMS). (See Figure 12 on page 379.) The query examples used in this chapter to extract inventory data are for MySQL.

Figure 12: Export Inventory Management System Data Topology Diagram



External inventory applications can extract inventory data, such as hardware, software, licensed features, and inventory scan events, from the JUNOScope Inventory Management System database. A unique username and password must be configured during the JUNOScope software installation to enable read-only access to the Inventory Management System database.

JUNOScope versions 7.4 and higher support extracting Inventory Management System database information to an external inventory application.

This chapter also describes the SQL database schema to facilitate data export, and also describes each database table.

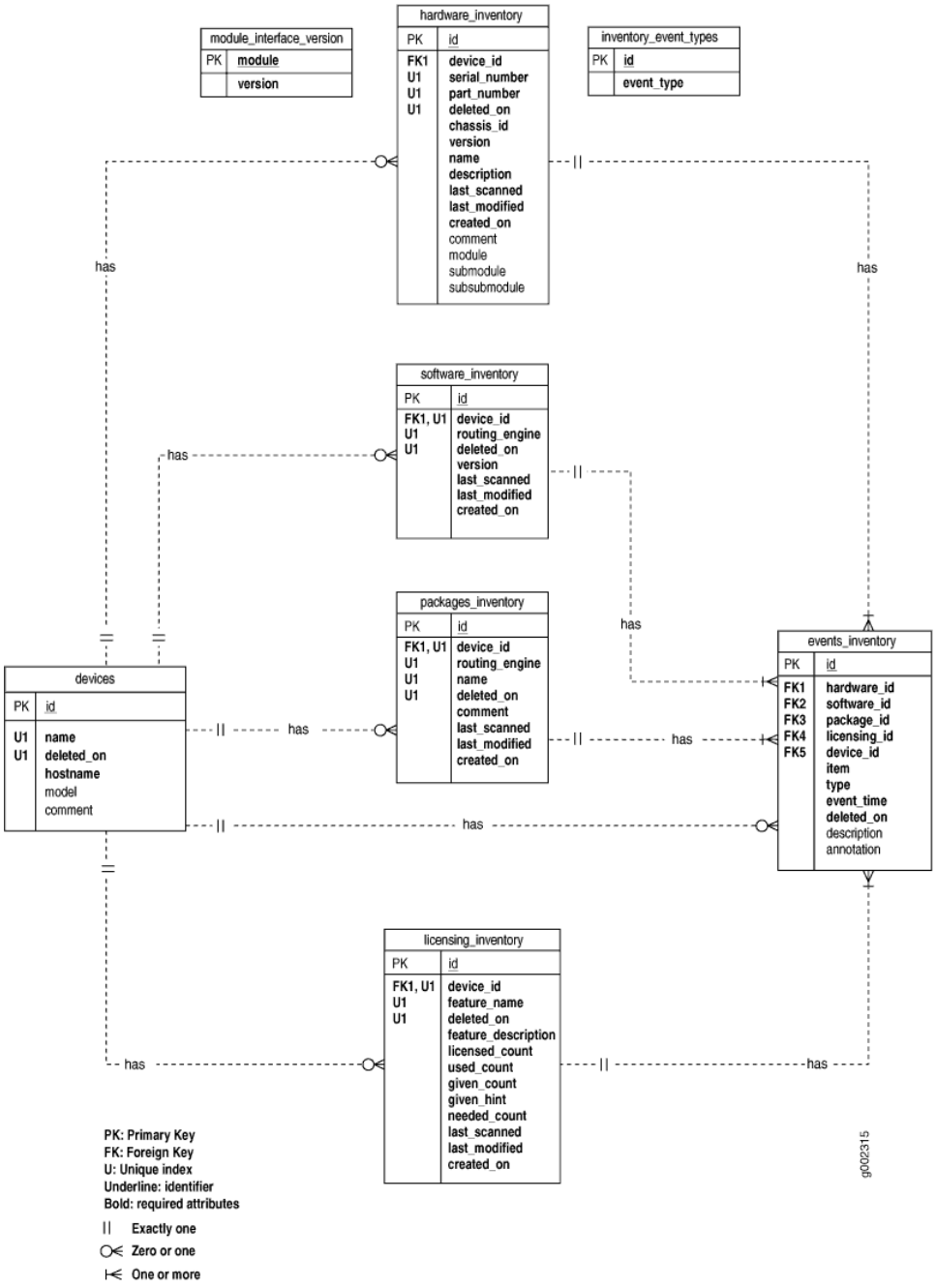
A demo Inventory Management System database is bundled with the JUNOScope installation, which consists of tables populated with sample inventory data. You can develop scripts or programs to practice extracting data from the demonstration database without having to scan real inventory data into the production Inventory Management System database. For more information about the demo tables, see "Demo Inventory Management System Database Tables" on page 390.

This chapter includes the following topics:

Inventory Management System Database Entity Relationship

Figure 13 on page 381 shows the JUNOScope Inventory Management System database entity relationship diagram.

Figure 13: Inventory Management System Database Entity Relationship Diagram



Enabling Access to the Inventory Management System SQL Interface

The JUNOScope software installer can enable or disable access to the Inventory Management System SQL interface during the JUNOScope installation process.

After the JUNOScope software is installed, the installer can enable or disable the SQL interface to the Inventory Management System by running the reconfiguration script jtk-setup.sh.

CAUTION: Once the Inventory Management System SQL interface username and password have been added during JUNOScope software installation, the JUNOScope software will not prompt again to add them for reconfiguration.

Changing the Username and Password and Creating Additional Users for the Inventory Management System SQL Interface

The database administrator can change the password of the database user already configured to access the Inventory Management System SQL interface. The database administrator can also create additional users to access the Inventory Management System SQL interface and grant the required privileges by using the sample SQL query below.

An SQL user with grant privileges (for example, root) can execute these statements:

```
-- grant read-only privilege to the inventory tables of @DBNAME@ for @DBUSER_IMS@,

-- per the specification of the interface module 'core' and 'ims'.
-- @DBNAME@ is the name of the database, e.g. 'jtk' or 'demo'
-- @DBUSER_IMS@ is the name of the database user for the SQL interface to IMS
-- @DBUSER_IMS_PASSWORD@ is the password of the database user for the SQL interface
 to IMS
GRANT SELECT (id) ON @DBNAME@.devices TO @DBUSER_IMS@@localhost IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (id) ON @DBNAME@.devices TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (id) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_NAME@" IDENTIFIED
BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (id) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (id) ON @DBNAME@.devices TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (name) ON @DBNAME@.devices TO @DBUSER_IMS@@localhost IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (name) ON @DBNAME@.devices TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (name) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_NAME@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (name) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (name) ON @DBNAME@.devices TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (hostname) ON @DBNAME@.devices TO @DBUSER_IMS@@localhost IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (hostname) ON @DBNAME@.devices TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (hostname) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (hostname) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (hostname) ON @DBNAME@.devices TO @DBUSER_IMS@@"%" IDENTIFIED BY
```

```
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (model) ON @DBNAME@.devices TO @DBUSER_IMS@@localhost IDENTIFIED BY
 '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (model) ON @DBNAME@.devices TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (model) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_NAME@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (model) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (model) ON @DBNAME@.devices TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (comment) ON @DBNAME@.devices TO @DBUSER_IMS@@localhost IDENTIFIED
BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (comment) ON @DBNAME@.devices TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (comment) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_NAME@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (comment) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (comment) ON @DBNAME@.devices TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT (deleted_on) ON @DBNAME@.devices TO @DBUSER_IMS@@localhost IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (deleted_on) ON @DBNAME@.devices TO @DBUSER_IMS@@"127.0.0.1"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (deleted_on) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (deleted_on) ON @DBNAME@.devices TO @DBUSER_IMS@@"@HOST_IP@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT (deleted_on) ON @DBNAME@.devices TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.module_interface_version TO @DBUSER_IMS@@localhost
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.module_interface_version TO @DBUSER_IMS@@"127.0.0.1"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.module_interface_version TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.module_interface_version TO @DBUSER_IMS@@"@HOST_IP@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.module_interface_version TO @DBUSER_IMS@@"%" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.hardware_inventory TO @DBUSER_IMS@@localhost IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.hardware_inventory TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.hardware_inventory TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.hardware_inventory TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.hardware_inventory TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.software_inventory TO @DBUSER_IMS@@localhost IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.software_inventory TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.software_inventory TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.software_inventory TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.software_inventory TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
```

```
GRANT SELECT ON @DBNAME@.packages_inventory TO @DBUSER_IMS@@localhost IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.packages_inventory TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.packages_inventory TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.packages_inventory TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.packages_inventory TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.licensing_inventory TO @DBUSER_IMS@@localhost IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.licensing_inventory TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.licensing_inventory TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.licensing_inventory TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.licensing_inventory TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.events_inventory TO @DBUSER_IMS@@localhost IDENTIFIED
BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.events_inventory TO @DBUSER_IMS@@"127.0.0.1" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.events_inventory TO @DBUSER_IMS@@"@HOST_NAME@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.events_inventory TO @DBUSER_IMS@@"@HOST_IP@" IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.events_inventory TO @DBUSER_IMS@@"%" IDENTIFIED BY
'@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.inventory_event_types TO @DBUSER_IMS@@localhost IDENTIFIED
 BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.inventory_event_types TO @DBUSER_IMS@@"127.0.0.1"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.inventory_event_types TO @DBUSER_IMS@@"@HOST_NAME@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.inventory_event_types TO @DBUSER_IMS@@"@HOST_IP@"
IDENTIFIED BY '@DBUSER_IMS_PASSWORD@';
GRANT SELECT ON @DBNAME@.inventory_event_types TO @DBUSER_IMS@@"%" IDENTIFIED BY
 '@DBUSER_IMS_PASSWORD@';
```

Inventory Management System Database Tables

The Inventory Management System database user has read-only access or SELECT privileges to the following JUNOScope Inventory Management System database tables:

The database user does not have access to other JUNOScope database tables that are not described in this document.

devices Table

The devices database table stores all Juniper Networks devices added in JUNOScope. For information about adding devices, see "Setting Up Devices" on page 57. Table 35 on page 385 shows the fields and columns in the devices table.

Table 35: devices Table

Field	Type	Null	Key	Default	Extra
id	int(11)		PRI		auto_increment
name	varchar(40)				
hostname	varchar(40)				
model	varchar(20)	Yes			
comment	text	Yes			
deleted_on	timestamp(14)	Yes			

hardware_inventory Table

The hardware_inventory database table stores information about all hardware components installed in devices added in JUNOScope. Table 36 on page 385 shows the fields and columns in the hardware_inventory table.

Table 36: hardware_inventory Table

Field	Type	Null	Key	Default	Extra
id	int(11)	PRI			auto_increment
device_id	int(11)			0	
chassis_id	varchar(20)				
version	varchar(20)				
part_number	varchar(20)				
serial_number	varchar(20)				
name	varchar(40)				
module	varchar(40)	Yes			
submodule	varchar(40)	Yes			

Table 36: hardware_inventory Table *(continued)*

Field	Type	Null	Key	Default	Extra
subsubmodule	varchar(40)	Yes			
description	varchar(40)				
comment	text	Yes			
last_scanned	timestamp(14)	Yes			
last_modified	timestamp(14)	Yes			
created_on	timestamp(14)	Yes			
deleted_on	timestamp(14)	Yes			

software_inventory Table

The software_inventory database table stores information about all JUNOS software packages installed on devices added in JUNOScope. Table 37 on page 386 shows the fields and columns in the software_inventory table.

Table 37: software_inventory Table

Field	Type	Null	Key	Default	Extra
id	int(11)		PRI		auto_increment
device_id	int(11)			0	
routing_engine	varchar(10)				
version	varchar(20)				
last_scanned	timestamp(14)	Yes			
last_modified	timestamp(14)	Yes			
created_on	timestamp(14)	Yes			
deleted_on	timestamp(14)	Yes			

packages_inventory Table

The packages_inventory database table stores all JUNOS software packages installed on devices added in JUNOScope. Table 38 on page 387 shows the fields and columns in the packages_inventory table.

Table 38: packages_inventory Table

Field	Type	Null	Key	Default	Extra
id	int(11)		PRI		auto_increment
device_id	int(11)			0	
routing_engine	varchar(10)				
name	varchar(20)				
comment	varchar(100)				
last_scanned	timestamp(14)	Yes			
last_modified	timestamp(14)	Yes			
created_on	timestamp(14)	Yes			
deleted_on	timestamp(14)	Yes			

licensing_inventory Table

The licensing_inventory database table stores information about all licensed features installed on devices added in JUNOScope. Table 39 on page 387 shows the fields and columns in the licensing_inventory table.

Table 39: licensing_inventory Table

Field	Type	Null	Key	Default	Extra
id	int(11)		PRI		auto_increment
device_id	int(11)			0	
feature_name	varchar(64)				
feature_description	varchar(64)				
licensed_count	int(11)			0	
used_count	int(11)			0	
given_count	int(11)			0	
given_hint	varchar(64)				
needed_count	int(11)			0	
last_scanned	timestamp(14)	Yes			
last_modified	timestamp(14)	Yes			
created_on	timestamp(14)	Yes			

Table 39: licensing_inventory Table *(continued)*

Field	Type	Null	Key	Default	Extra
deleted_on	timestamp(14)	Yes			

events_inventory Table

The events_inventory database table stores all events that occur during an inventory scan using the Inventory Management System. For more information about running an inventory scan, see "Scanning Inventory Data" on page 339. Table 40 on page 388 shows the fields and columns in the events_inventory table.

Table 40: events_inventory Table

Field	Type	Null	Key	Default	Extra
id	int(11)		PRI		auto_increment
device_id	int(11)			0	
hardware_id	int(11)			0	
software_id	int(11)			0	
package_id	int(11)			0	
licensing_id	int(11)			0	
item	varchar(40)				
type	varchar(10)				
description	text	Yes			
annotation	text	Yes			
event_time	timestamp(14)	Yes			
deleted_on	timestamp(14)	Yes			

inventory_events_types Table

The inventory_events_types database table stores all inventory scan event types. Table 41 on page 388 shows the fields and columns in the inventory_events_types table.

Table 41: inventory_events_types Table

Field	Type	Null	Key	Default	Extra
id	int(11)		PRI		auto_increment

Table 41: inventory_events_types Table *(continued)*

Field	Type	Null	Key	Default	Extra
event_type	varchar(10)				

module_interface_version Table

The module_interface_version database table stores and identifies the module name and version of the Inventory Management System database. Table 42 on page 389 shows the fields and columns in the module_interface_version table.

Table 42: module_interface_version Table

Field	Type	Null	Key	Default	Extra
module	varchar(40)		PRI		
version	int(11)			0	

For example, the module field can be either:

module = core, version = 1
module = ims, version = 1

The version field is incremented when an update is made to the documented SQL interface with respect to the module. An update occurs when:

- A new public column is added.
- The meaning of a public column changes.
- A public column is removed.

The module version identifies the public subset of the JUNOScope database schema.

Table-to-Module Mapping

Two modules are currently defined: *ims* and core.

ims Module

Version 1 of the ims module consists of the following tables:

- hardware_inventory Table on page 385
- “software_inventory Table” on page 386
- “packages_inventory Table” on page 386
- “licensing_inventory Table” on page 387

- "events_inventory Table" on page 388
- "inventory_events_types Table" on page 388

core Module

The core module (version 1) consists of the devices table listed in Table 35 on page 385.

Demo Inventory Management System Database Tables

The demo inventory tables are populated with sample data. Use the demo inventory tables to:

- Experiment and execute the sample query by way of the external SQL interface.
- See and generate sample reports based on the demo data. You can experiment and use Inventory Management System reports without scanning devices on the network.

The demo tables are separate from the normal JUNOScope tables, and belong to a different database; demo rather than jtk. The demo tables are created during the JUNOScope Inventory Management System software installation.

The following demo tables, similar to those described in "Inventory Management System Database Entity Relationship" on page 380, are created and populated with sample data.

- demo.devices
- demo.hardware_inventory
- demo.software_inventory
- demo.packages_inventory
- demo.licensing_inventory
- demo.events_inventory
- demo.inventory_event_types
- demo.module_interface_version

Demo Inventory Management System Reports

Several demo custom reports are packaged as part of the JUNOScope installation. Sample custom reports installed include:

- Licensing summary
- Sorted hardware summary
- All inventory changes in the network between Friday and Sunday

- All Gigabit Ethernet PICs
- All JUNOS Release 7.0 or higher

Connecting to the Inventory Management System SQL Interface

To connect to the Inventory Management System database using the MySQL client provided in the JUNOScope installation, type the following:

```
% <JTK_INSTALL>/mysql/bin/mysql \
        - -socket=<JTK_INSTALL>/data/db/mysql.sock \
        - -port=<DBPORT>\
        - -host=<HOSTNAME>\
        - -user=<DBUSER_IMS>\
        - -password=<DBUSER_IMS_PASSWORD> $<DBNAME>
```

Where:

- <JTK_INSTALL> is the path of the JUNOScope installation.
- <DBPORT> is the port number of the database connection. The default port number is 3306.
- <HOSTNAME> is the hostname of database server.
- <DBUSER_IMS> is the database user for read-only access to the Inventory Management System. This is the username that the JUNOScope administrator provided during the installation process.
- DBUSER_IMS_PASSWORD> < is the password for the Inventory Management System database user. This is the password that the JUNOScope administrator provided during the installation process.
- <DBNAME> is the database name jtk for accessing the production Inventory Management System database, or demo for accessing the demonstration database.

Querying All Hardware Inventory Items

All of the database query examples are specific to MySQL. If the underlying database is not MySQL, the query will be different.

To extract all active hardware inventory items stored in the Demo Inventory Management System database, use the following query. (Enter the entire MySQL command syntax on the same line.)

```
mysql>SELECT dev.name,
dev.model,
hw.name,
hw.version,
hw.part_number,
hw.serial_number,
hw.description,
hw.chassis_id,
hw.module,
```

```
hw.submodule,
hw.subsubmodule,
hw.last_scanned,
hw.created_on
FROM demo.hardware_inventory hw
   INNER JOIN demo.devices dev
ON hw.device_id = dev.id
WHERE hw.deleted_on = 0 AND dev.deleted_on = 0;
```

When an item is no longer active, the deleted_on field is updated with the time the entry was removed.

You can make an entry inactive in one of two ways:

- When the item is no longer part of the network (for example, a PIC is removed from a chassis).
- The row is administratively removed from the database by marking the deleted_on field to non-zero, making it virtually hidden from the user. This is not done by user action, but by manually setting the deleted_on field in the database.

The last_scanned field stores the timestamp of the item (row) when it was last updated and processed by the Inventory Management System, regardless of whether the item (row) itself was modified.

The created_on field stores the timestamp of the item (row) when it was first scanned and processed by the Inventory Management System. If this item is removed from one chassis and moved to another, the created_on timestamp will remain the same.

Querying All Hardware Inventory Items of a Device

To extract all active hardware inventory items of device XYZ, use the following query. (Enter the entire MySQL command syntax on the same line.)

```
mysql> SELECTdev.name,
dev.model,
hw.name,
hw.version,
hw.part_number,
hw.serial_number,
hw.description,
hw.chassis_id,
hw.module,
hw.submodule,
hw.subsubmodule,
hw.last_scanned,
hw.created_on
FROMdemo.hardware_inventory hw
    INNER JOINdemo.devices dev
 ONhw.device_id = dev.id
 WHEREhw.deleted_on = 0
  ANDdev.deleted_on = 0
  ANDdev.name = 'XYZ';
```

Querying JUNOS Software and Package Inventory Items

To extract all active software and package inventory items stored in the Inventory Management System, use the following query. (Enter the entire MySQL command syntax on the same line.)

```
mysql> SELECTdev.name,
dev.model,
sw.routing_engine,
sw.version,
pkg.name,
pkg.comment,
sw.last_scanned,
sw.created_on
FROMdemo.software_inventory sw
 INNER JOINdemo.packages_inventory pkg
 ONsw.device_id = pkg.device_id
 INNER JOINdemo.devices dev
 ONsw.device_id = dev.id
 WHEREsw.routing_engine = pkg.routing_engine
  ANDsw.deleted_on = 0
  ANDpkg.deleted_on = 0
  ANDdev.deleted_on = 0;
```

Querying All Licensed Feature Inventory Data

To extract all active licensed features inventory items stored in the Inventory Management System database, use the following query. (Enter the entire MySQL command syntax on the same line.)

```
mysql> SELECTdev.name,
dev.model,
lic.feature_name,
lic.feature_description,
IF(given_count, given_count, "") AS given,
lic.used_count,
lic.licensed_count,
lic.needed_count,
lic.last_scanned,
lic.created_on
 FROMdemo.licensing_inventory lic
    INNER JOINdemo.devices dev ON lic.device_id = dev.id
    WHERElic.deleted_on = 0 AND dev.deleted_on = 0;
```

Querying Inventory Events Data

To extract all active inventory events stored in the Inventory Management System database, use the following query. (Enter the entire MySQL command syntax on the same line.)

```
mysql> SELECTev.type,
ev.item,
```

```
ev.event_time,
ev.description AS details,
dev.name,
IF(ev.hardware_id != 0, hw.serial_number, "")
AS serial_number,
IF(ev.hardware_id != 0, hw.description,
IF(ev.software_id != 0, "",
IF(ev.package_id != 0, pkg.name,
IF(ev.licensing_id != 0,
lic.feature_description, ""))))
AS description,
IF(ev.software_id != 0, sw.routing_engine,
IF(ev.package_id != 0, pkg.routing_engine, ""))
AS routing_engine
FROM demo.events_inventory ev
    INNER JOIN demo.devices dev ON ev.device_id = dev.id
 LEFT JOIN demo.hardware_inventory hw ON ev.hardware_id = hw.id
 LEFT JOIN demo.software_inventory sw ON ev.software_id = sw.id
 LEFT JOIN demo.packages_inventory pkg ON ev.package_id = pkg.id
 LEFT JOIN demo.licensing_inventory lic
ON ev.licensing_id = lic.id
 WHERE ev.deleted_on = 0;
```

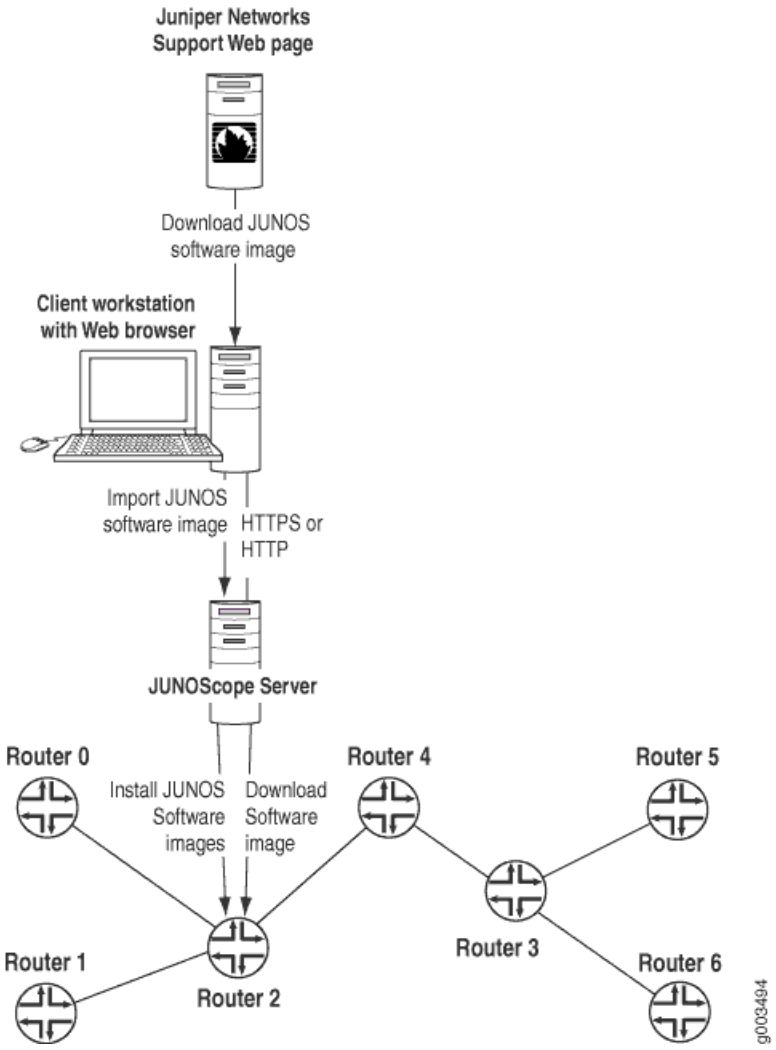
Part 8
Performing Software Management

Chapter 34

Using the Software Manager

This chapter describes how to use the Software Manager, a licensable module, to manage the installation and deployment of software images on devices in the network. See Figure 14 on page 397.

Figure 14: JUNOScope Software Manager Operations



You can download software images from the Juniper Networks Support Web page to the local file system of your workstation. You can import these software images into the JUNOScope server,

You can download a software image to a device or group of devices, and install that image immediately or at a scheduled time. You can install an image previously downloaded onto a device or directly from the JUNOScope server.

Using the Software Manager, the installation process occurs according to the installation options that you select; see Step 3. Once installation is complete, the Software Manager reboots the device, and verifies that the software that is running on the device matches the software image installed.

You must have superuser privileges to use the Software Manager.

The following topics describe how to manage software images:

- Importing a Software Image on page 398
- Managing Software Images on page 399
- Downloading a Software Image and Saving a Download Software Image Operation on page 400
- Installing a Software Image and Saving a Software Image Installation Operation on page 404
- Deleting a Software Image on page 414

Importing a Software Image

Before you can install a software image using the Software Manager, you must first download it from the Juniper Networks Support Web page to the local file system of your workstation, then import it into the JUNOScope server.

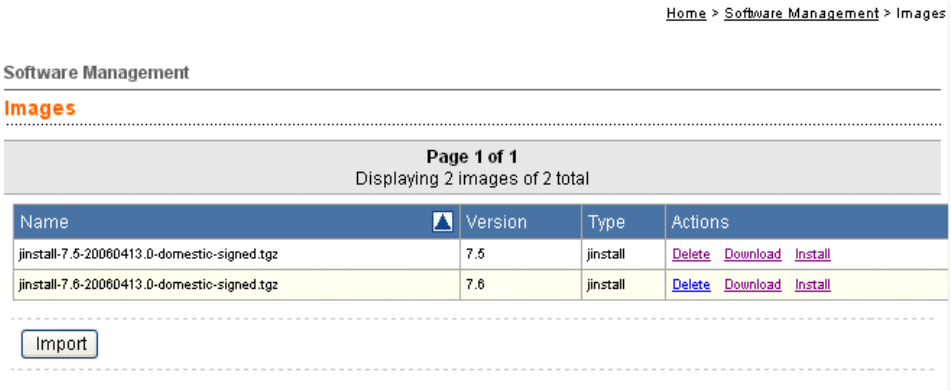
To download software images from the Juniper Networks software download page, you must have a service contract and an access account. If you do not have an access account, complete the registration form at the Juniper Networks Web site: https://www.juniper.net/registration/Register.jsp.

To import a software image into the JUNOScope software, follow these steps:

NOTE: To import a BXOS image, you must have installed IP Backhaul Manager license.

1. Download the software image you need from the Juniper Networks Support Web site, http://www.juniper.net/support/ to your workstation.
   a. Select the Canada and US, Worldwide, or JUNOS-FIPs editions.
   b. Select the software release that you want.
2. Log in to the JUNOScope software and click Software Management > Images.

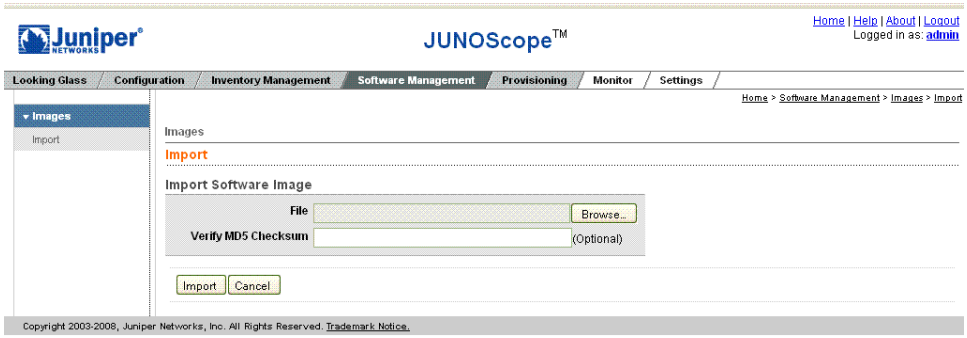
The Images dialog box appears. If you have not imported any software images, the Images dialog box is empty.



3. Enter the MD5 checksum value in the Verify MD5 Checksum field. The checksum can be obtained from http://www.juniper.net/customers/support/ when you download the image. This checksum value is compared with the checksum stored in JUNOScope to verify that the downloaded image is intact. This field is optional.

4. Click Import.

   The Import Software Image dialog box appears.



5. Use Browse to navigate to the software image file on the local file system that you want to import. For example, you can import a software image file, such as jinstall-7.5R2.8-domestic-signed.tgz, to install on M-series and T-series routing platforms.

6. Click Import.

   The JUNOS software imports the software image. This operation may take a while, depending on the size of the image and the connection speed between the local machine and the JUNOScope server. The imported software image file appears in the Images dialog box. For more information about how to manage software images in the Images dialog box, see “Managing Software Images” on page 399.

Managing Software Images

From the Images dialog box, you can:

- Import other software images into the JUNOScope software from the local file system. If you have not imported any software images, the Images dialog box is empty. For more information about importing software images see "Importing a Software Image" on page 398.
- Delete a software image by clicking the Delete link. For more information about deleting software images, see "Deleting a Software Image" on page 414.
- Download a software image to a device or a group of devices immediately or at a scheduled time by clicking the Download link. For more information about downloading software images, see "Downloading a Software Image and Saving a Download Software Image Operation" on page 400.

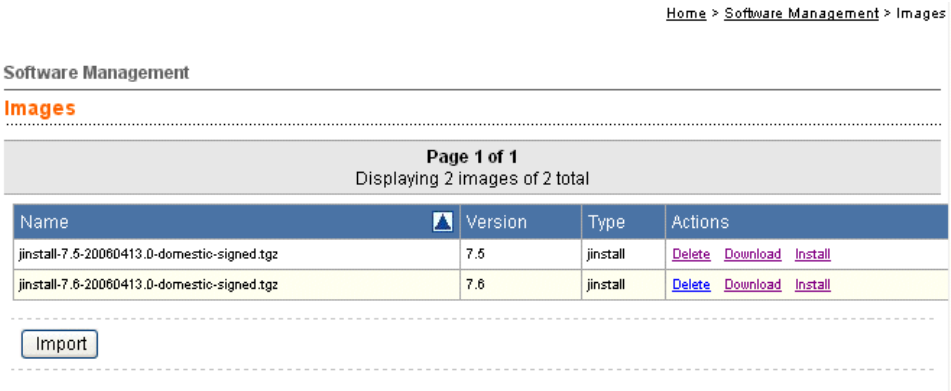
NOTE: Download option is not available for BXOS images.

- Install a software image to a device or a group of devices immediately or at a scheduled time by clicking the Install link. For more information about installing a software image, see "Installing a Software Image and Saving a Software Image Installation Operation" on page 404.

To view and manage software images, do the following:

- In the JUNOScope main window, click Software Management > Images.

  The Images dialog box appears.



  Imported software images are listed in the Images dialog box by image name, version, and type.

  You can sort the Images table data by clicking a column name. Clicking the column name toggles between ascending and descending sort order.

Downloading a Software Image and Saving a Download Software Image Operation

You can download a software image to a device or a group of devices immediately or at a scheduled time. You can save a software image download operation so that you can combine it with other operations. For example, you can combine saved download and install operations using the Task Manager (Saved Operations) and

schedule them to run simultaneously at a scheduled time. You can also ensure that the downloaded software is intact by verifying that the MD5 checksum of the downloaded software image matches that of the image stored in JUNOScope.

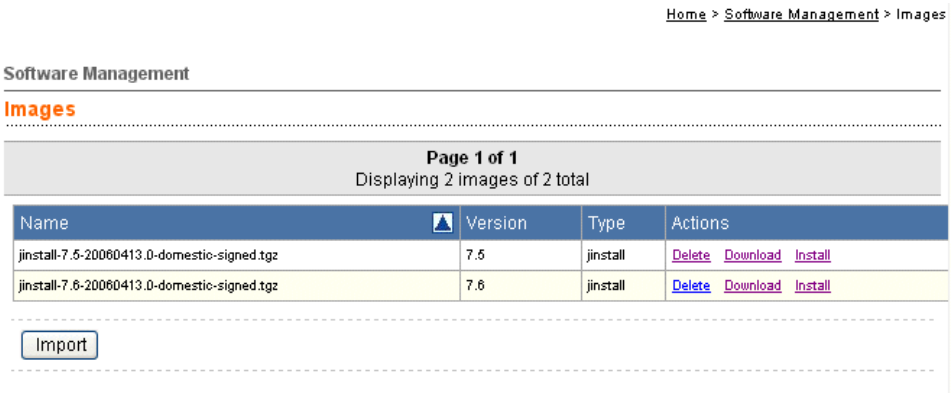
NOTE: Download option is not available for BXOS images.

To download a software image to a device and save a download software image operation, follow these steps:

1. In the JUNOScope main window, click Software Management > Images.

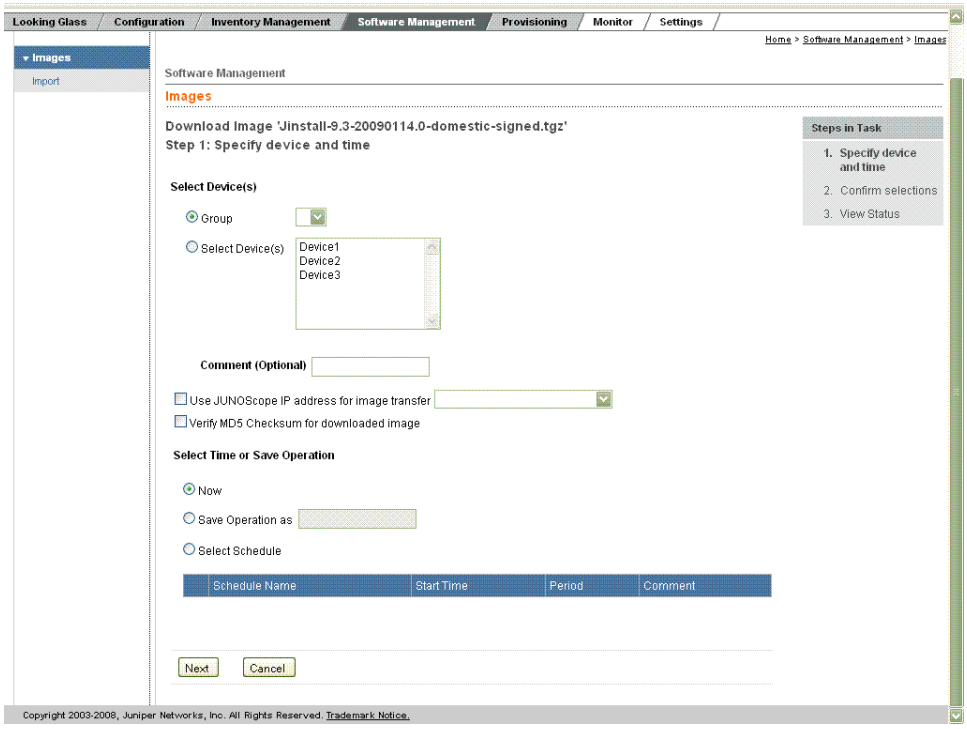
   The Images dialog box appears..

NOTE: For BXOS images, the Download link is not displayed.



2. Click the Download link for the software image that you want to download.

   The Download Image dialog box appears.

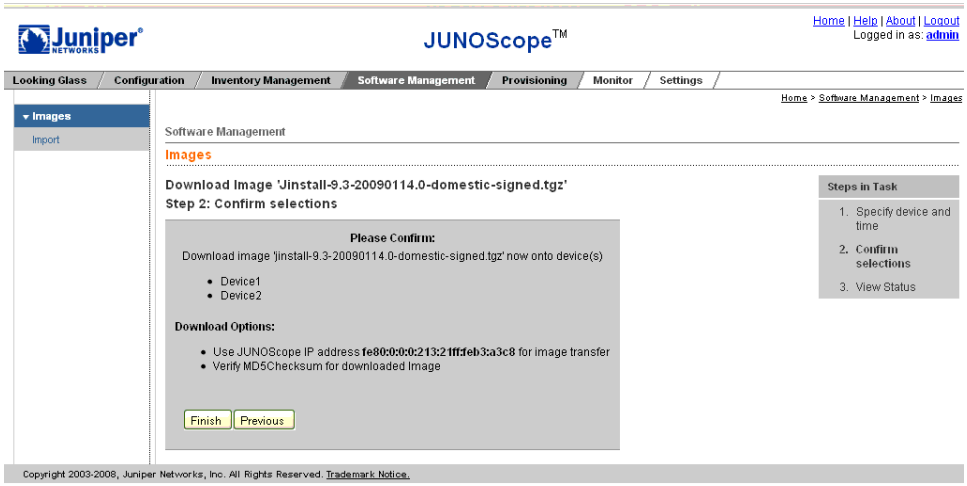


3. Select the Group or Select Device(s) option button.
4. Select the group or devices that you want from the Group or Select Device(s) list box. Shift + click to select multiple devices from the Select Device(s) drop-down list box.
5. In the Comment text box, type an optional descriptive comment about the software image download that you want to perform.
6. Select the Use JUNOScope IP address for image transfer option if you want the device(s)/group to connect to the JUNOScope server using the IP address of the JUNOScope server. The device(s)/group will use the IP address of the JUNOScope server instead of the JUNOScope server name.
7. Select the Verify MD5 Checksum for downloaded image option if you want to ensure that the downloaded software image is intact. If you select this option, the MD5 checksum of the downloaded image is compared with the checksum stored in JUNOScope. If they do not match, the operation fails and the error message "MD5 checksum of downloaded image does not match the image in JUNOScope" appears in the JUNOScope status wizard (Monitor > Status > View Status Records).
8. Select when you want the software image download to occur by clicking the appropriate option button:
   - Now—(Default) Performs a software image download immediately after you confirm it.
   - Save Operation as—Saves the current operation in the Settings > Saved Operations table so you can combine that operation with other JUNOScope operations or run that operation at a later time. Click the Save Operation as option button, then type an operation name in the text box.

- Select Schedule—Performs a software image download at the scheduled time interval. Select the schedule that you want in the schedule table.

9. Click Next.

   - The Please Confirm—Download Image dialog box appears if you selected the Now option.



   - The Please Confirm—Save Operation dialog box appears if you selected the Save Operation as option.

10. Confirm that the download software image or save download software image options that you selected are correct.

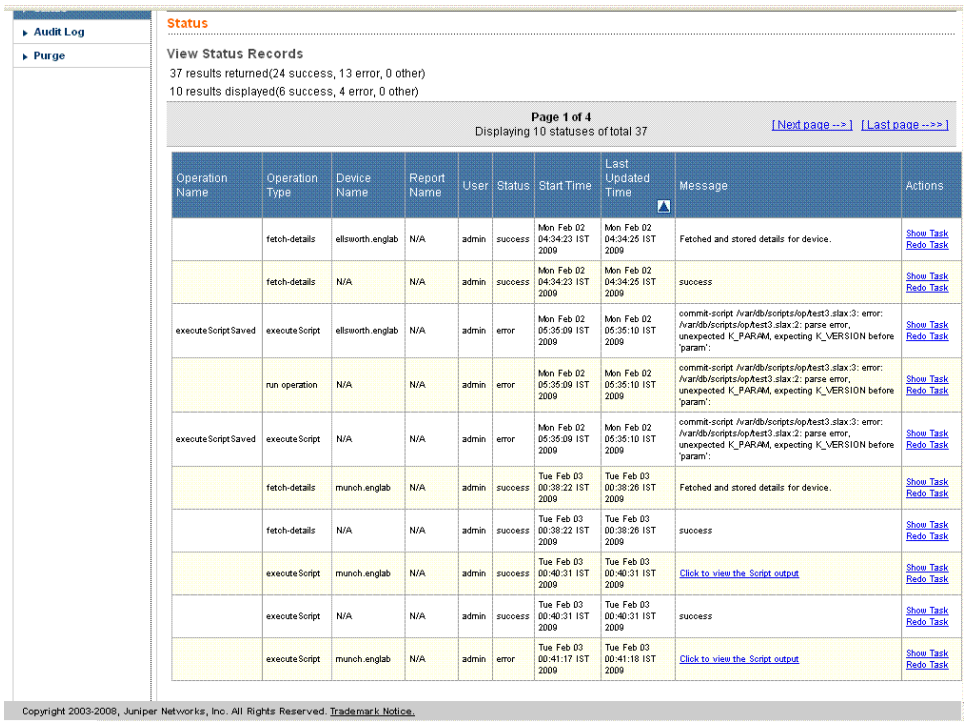
11. Click Finish to perform the operation that you confirmed.

    - If you selected the Now option, the software image is downloaded to the device or group of devices that you specified immediately

    - If you selected the Save Operation as option, the operation is saved and listed in the Settings > Saved Operations dialog box. To view the saved operation, click Settings > Saved Operations. For more information about saving operations, see “Using Task Manager (Saved Operations)” on page 167.

    - If you selected the Select Schedule option and selected a schedule, the software image is downloaded when the operation is scheduled to be run.

When the software image download process is complete, the Status—View Status Records dialog box appears.



Audit Log
Purge

Status

View Status Records

37 results returned(24 success, 13 error, 0 other)
10 results displayed(6 success, 4 error, 0 other)

Page 1 of 4
Displaying 10 statuses of total 37
[Next page -->>] [Last page -->>]

Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

Copyright 2003-2008, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.

The Status—View Status Records dialog box lists the software image download operation by operation name, operation type, report name, username, operation status, last updated time, and operation system log message. The software download operation status can be successful, failed, writing, pending, rebooting, connecting, or working.

12. Check the status of the operation that you specified, then click OK.

Installing a Software Image and Saving a Software Image Installation Operation

From the Images dialog box, you can install software images that have been imported into the JUNOScope software and downloaded to a device or a group of devices. You can install an image previously downloaded onto a device (supported only for JUNOS software images) or use the image directly from the JUNOScope server. In case of dual routing engines systems, you can select the routing engine on which the software image should be installed.

Using Software Manager, the installation process occurs according to the installation options that you select; see Step 3. If you select the Archive Data and Executable Areas (Snapshot) option, Software Manager performs a request system snapshot command before installing the software. If the command fails, the JUNOS software is not installed.

Once installation is complete, Software Manager reboots the device and reestablishes connection. Finally, Software Manager verifies that the software running on the device matches the software image installed.

This section covers the following topics:

- Installing a JUNOS Software Image on page 405
- Installing a BXOS Software Image on page 410

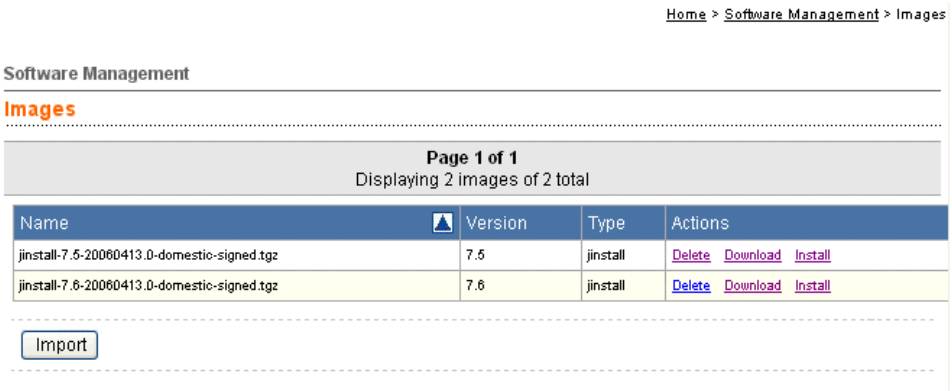
Installing a JUNOS Software Image

You can save an install software image operation so that you can combine it with other operations or run it at a later time.

To install a JUNOS software image and save an install software image operation, follow these steps:

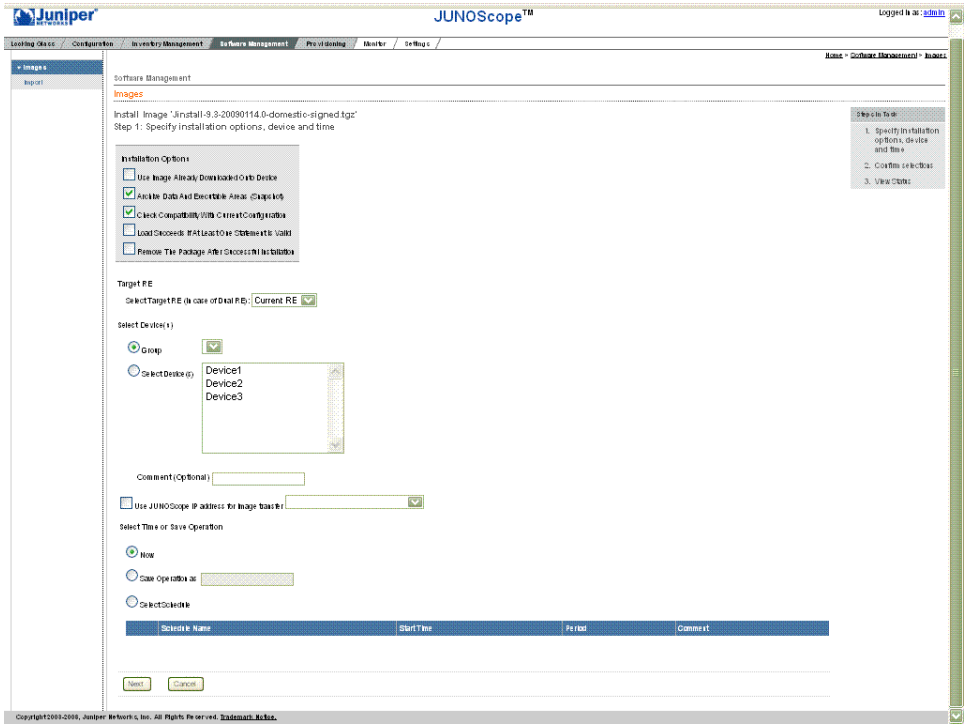
1. In the JUNOScope main window, click Software Management > Images.

   The Images dialog box appears.



2. Click the Install link for the JUNOS software image that you want to install.

   The Install Image dialog box appears.



3. Select the installation option(s) that you want.

   - Use Image Already Downloaded Onto Device—Installs an image that has already been downloaded to the /var/tmp directory of a device.

   - Archive Data And Executable Areas (Snapshot)—(Default) This option is the equivalent of the JUNOS software request system snapshot command. The command backs up the currently running and active file system partitions on the router to standby partitions that are not running. Specifically, the root file system (/) is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive. After you run the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

     The request system snapshot command can fail on J-series devices when there is no compact flash to back up the system.

   - Load Succeeds If At Least One Statement Is Valid —Activates a partial load and treats parsing errors as warnings instead of errors. Even if some of the statements (but not all) are invalid, the software installation succeeds. This option is the equivalent of using the request system software add <image> best-effort-load CLI command.

   - Remove The Package After Successful Installation—Allows the system to find enough room to upgrade a new software image. Use this option when installing a software image from a local directory on a device that has minimal storage space. This command is equivalent to the request system software add uplink CLI command.

4. Select the routing engine (R.E.) on which the software image should be installed, from the Select Target RE (in case of Dual RE): list. The options are Current RE, Master RE, and Backup RE. The Current RE option is selected by default.
   - Master—If a Routing Engine is configured as master, it has full functionality. It receives and transmits routing information, builds and maintains routing tables, communicates with interfaces and Packet Forwarding Engine components, and has full control over the chassis. Once a Routing Engine becomes master, it resets the switch plane (SSB, SCB, and SFM) and downloads its current version of the microkernel to the Packet Forwarding Engine components, guaranteeing software compatibility.
   - Backup—If a Routing Engine is configured to be the backup, it does not maintain routing tables or communicate with Packet Forwarding Engine or chassis components. However, it runs through its memory check and boot sequence to the point of displaying a login prompt. A backup Routing Engine supports full management access through the Ethernet, console, and auxiliary ports, and can communicate with the master Routing Engine. Additionally, a backup Routing Engine responds to the Routing Engine request chassis routing-engine master switch command. The backup Routing Engine maintains a connection with the master Routing Engine and monitors the master Routing Engine. If the connection is broken, you can switch mastership by entering the switchover command. If the master Routing Engine is hot-swapped out of the system, the backup takes over control of the system as the new master Routing Engine. Once a Routing Engine becomes master, it resets the switch plane and downloads its own version of the microkernel to the Packet Forwarding Engine components.

NOTE: The install operation fails if you select the backup RE option for a single RE device.

---

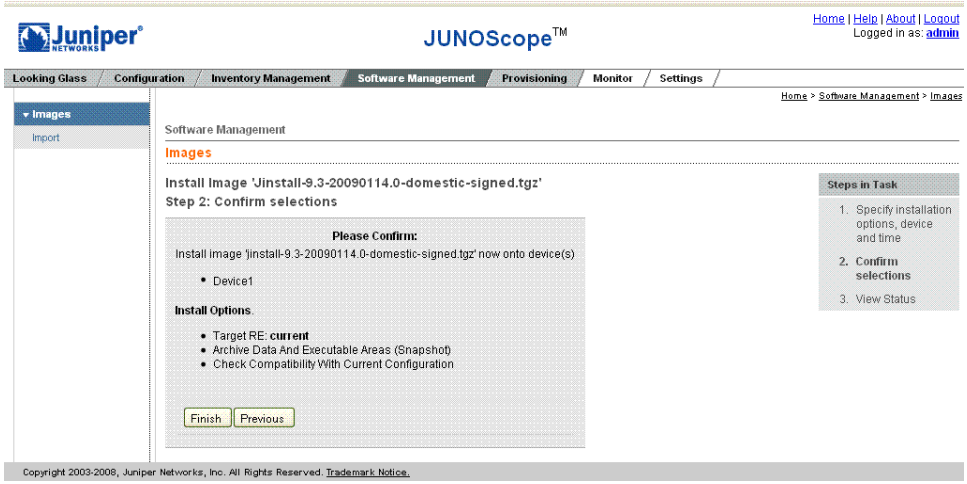
5. Select the Group or Select Device(s) option button.
6. Select the group or devices that you want from the Group or Select Device(s) list box. Shift + click to select multiple devices from the Select Device(s) drop-down list box.

NOTE: When you have selected a JUNOS image for installation, only JUNOS devices are listed in the list of devices. If you choose a device group that contains devices that run operating systems other than JUNOS, the Status page shows “Operation Not Supported” status for such devices.

---

7. In the Comment text box, type an optional descriptive comment about the software image installation operation.
8. Select the Use JUNOScope IP address for image transfer option if you want the device(s)/group to connect to the JUNOScope server using the IP address of the JUNOScope server. The device(s)/group will use the IP address of the JUNOScope server instead of the JUNOScope server name.

9. Select when you want the software image installation to occur and to save the operation by clicking the appropriate option button:
   - Now—(Default) Performs a software image installation immediately after you confirm it.
   - Save Operation as—Saves the current operation in the Settings > Saved Operations table so you can combine that operation with other JUNOScope operations or run that operation at a later time. Click the Save Operation as option button, then type an operation name in the text box.
   - Select Schedule—Performs a software image installation at the scheduled time interval. Select the Select Schedule option, then select the schedule that you want in the schedule table.
10. Click Next.
   - If you selected the Now option, the Please Confirm—Install Image dialog box appears.

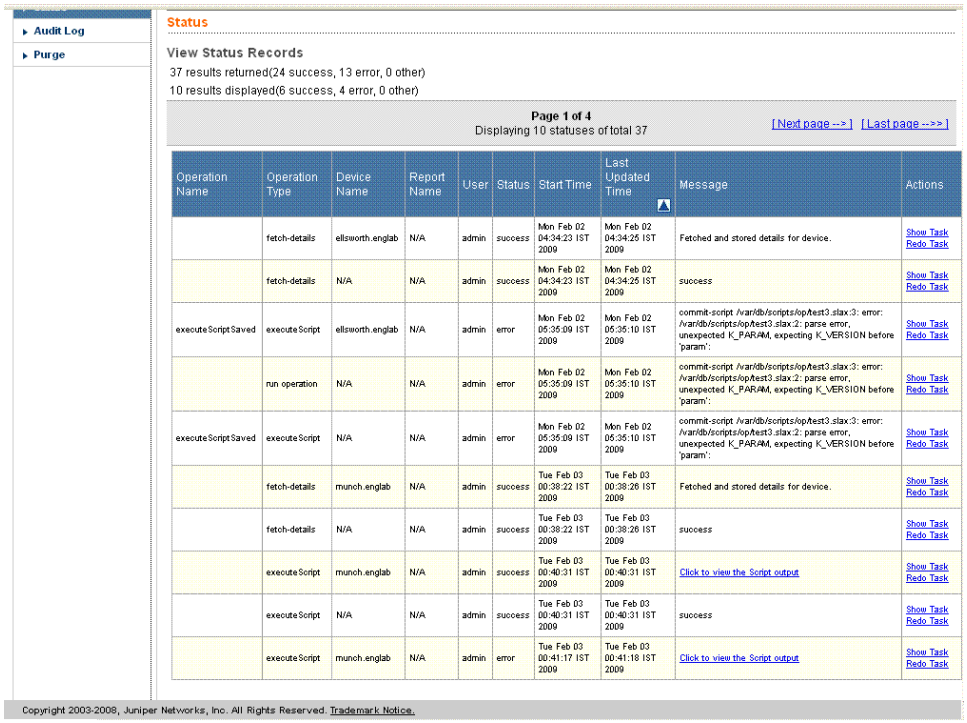


   - If you selected the Save Operation as option, the Please Confirm—Save Install Image dialog box appears.

11. Confirm that the software image install options that you selected are correct.
12. Click Finish to confirm the software image install operation that you specified.

- If you selected the Now option, software image installation occurs immediately.
- If you selected the Save Operation as option, the operation is saved in the Settings > Saved Operations table. To view the saved operation, click Settings > Saved Operations. For more information about managing saved JUNOScope operations, see “Using Task Manager (Saved Operations)” on page 167.
- If you selected the Select Schedule option, the software image installation occurs when the operation is scheduled to be run.

When the software image install process is complete, the Status—View Status Records dialog box appears.



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

The Status—View Status Records dialog box lists the software image download operation by operation name, operation type, report name, username, operation status, last updated time, and operation system log message. The Archive operation status can be successful, failed, writing, pending, connecting, or working.

The Software Manager reboots the device after the software is installed.

After the device reboots, connection must be reestablished with the device. If connection is not established within a specified time, a “ could not open connection” error message appears in the View Status Records dialog box table.

If connection is not established with the device it may because of one of the following reasons, and you may have to install the software manually:

- The request system snapshot command may not work on some devices.
- There may not be enough available disk space on the device.
- The newly installed software may not be compatible with the existing configuration.
- The newly installed software may not be compatible with the Physical Interface Cards (PICs) that are installed on the device.

13. Click OK.

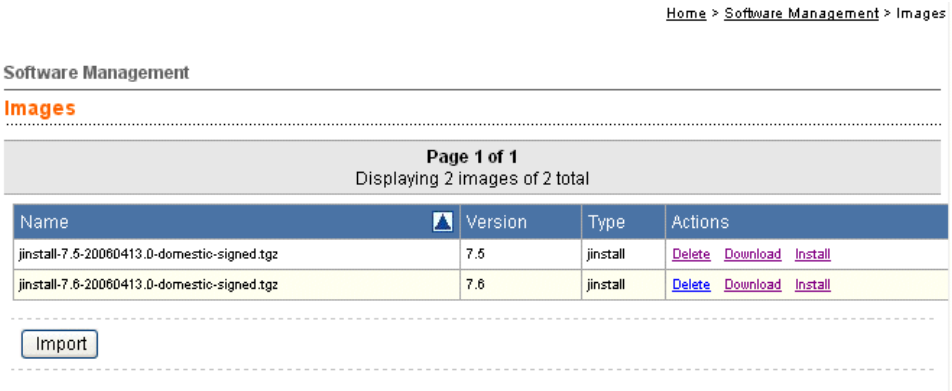
Installing a BXOS Software Image

The BXOS software installation follows a process that is different from the JUNOS software installation.

To install a BXOS software image from JUNOScope, follow these steps:

1. In the JUNOScope main window, click Software Management > Images.

   The Images dialog box appears.



2. Click the Install link for the software image that you want to install.

   The Install Image dialog box appears.

3. Choose the protocol, HTTP or HTTPS, for transferring the image from JUNOScope server to the device or device groups on which you want to install the image.

4. Specify the Installation Options:

   - Create a Snapshot of Primary Image—Check this check box if you want to copy the primary image as the backup before installing the new image. If this option is checked, the backup image on the FLASH memory is replaced with a copy of the primary image.
   - Persist Running Configuration—Check this box if you want to copy the running configuration to the start up configuration before installing the new image. When this option is checked, the running configuration is copied to the start up configuration.

5. Select the routing engine (R.E.) on which the software image should be installed. The options are Current RE , Master RE, and Backup RE. The Current RE is the default option.
   - Master—If a Routing Engine is configured as master, it has full functionality. It receives and transmits routing information, builds and maintains routing tables, communicates with interfaces and Packet Forwarding Engine components, and has full control over the chassis. Once a Routing Engine becomes master, it resets the switch plane (SSB, SCB, and SFM) and downloads its current version of the microkernel to the Packet Forwarding Engine components, guaranteeing software compatibility.
   - Backup—If a Routing Engine is configured to be the backup, it does not maintain routing tables or communicate with Packet Forwarding Engine or chassis components. However, it runs through its memory check and boot sequence to the point of displaying a login prompt. A backup Routing Engine supports full management access through the Ethernet, console, and auxiliary ports, and can communicate with the master Routing Engine. Additionally, a backup Routing Engine responds to the Routing Engine request chassis routing-engine master switch command. The backup Routing Engine maintains a connection with the master Routing Engine and monitors the master Routing Engine. If the connection is broken, you can switch mastership by entering the switchover command. If the master Routing Engine is hot-swapped out of the system, the backup takes over control of the system as the new master Routing Engine. Once a Routing Engine becomes master, it resets the switch plane and downloads its own version of the microkernel to the Packet Forwarding Engine components.

NOTE: BXOS devices are single RE machines. If you select any RE other than the Current RE option, the operation will fail.

---

6. Select the Group or Select Device(s) option button.
7. Select the group or devices that you want from the Group or Select Device(s) list box. Shift + click to select multiple devices from the Select Device(s) drop-down list box.

NOTE: When you have selected a BXOS image for installation, only BXOS devices are listed in the list of devices. If you choose a device groups that contains devices that run operating systems other than BXOS, the status page shows “Operation Not Supported” as the status for such devices.

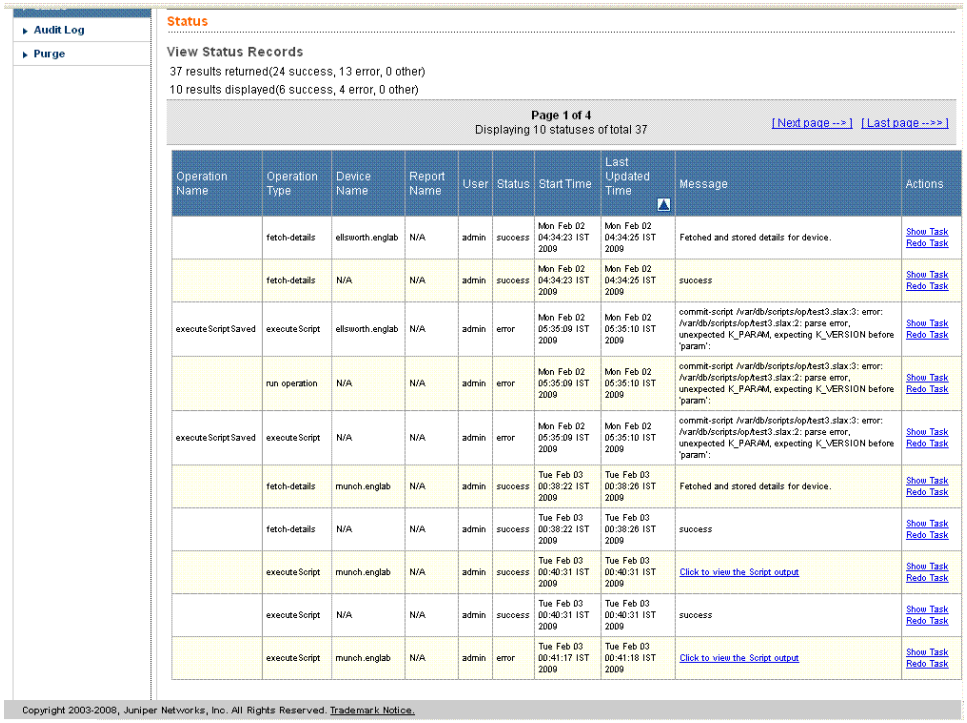
---

8. In the Comment text box, type an optional descriptive comment about the software image installation operation.
9. Select when you want the software image installation to occur and to save the operation by clicking the appropriate option button:
   - Now—(Default) Performs a software image installation immediately after you confirm it.

- Save Operation as—Saves the current operation in the Settings > Saved Operations table so you can combine that operation with other JUNOScope operations or run that operation at a later time. Click the Save Operation as option button, then type an operation name in the text box.
- Select Schedule—Performs a software image installation at the scheduled time interval. Select the Select Schedule option, then select the schedule that you want in the schedule table.

10. Click Next.
    - If you selected the Now option, the Please Confirm—Install Image dialog box appears.
    - If you selected the Save Operation as option, the Please Confirm—Save Install Image dialog box appears.
11. Confirm that the software image install options that you selected are correct.
12. Click Finish to confirm the software image install operation that you specified.
    - If you selected the Now option, software image installation occurs immediately.
    - If you selected the Save Operation as option, the operation is saved in the Settings > Saved Operations table. To view the saved operation, click Settings > Saved Operations. For more information about managing saved JUNOScope operations, see "Using Task Manager (Saved Operations)" on page 167.
    - If you selected the Select Schedule option, the software image installation occurs when the operation is scheduled to be run.

      When the software image install process is complete, the Status—View Status Records dialog box appears.



Audit Log
Purge

Status

View Status Records
37 results returned(24 success, 13 error, 0 other)
10 results displayed(6 success, 4 error, 0 other)

Page 1 of 4
Displaying 10 statuses of total 37
[Next page -->] [Last page -->>]

Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

Copyright 2003-2008, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.

The Status—View Status Records dialog box lists the software image download operation by operation name, operation type, report name, username, operation status, last updated time, and operation system log message. The Archive operation status can be successful, failed, writing, pending, connecting, or working.

The Software Manager reboots the device after the software is installed.

After the device reboots, connection must be reestablished with the device. If connection is not established within a specified time, a " could not open connection" error message appears in the View Status Records dialog box table.

If connection is not established with the device it may because of one of the following reasons, and you may have to install the software manually:

- The request system snapshot command may not work on some devices.
- There may not be enough available disk space on the device.
- The newly installed software may not be compatible with the existing configuration.
- The newly installed software may not be compatible with the Physical Interface Cards (PICs) that are installed on the device.

13. Click OK.

Deleting a Software Image

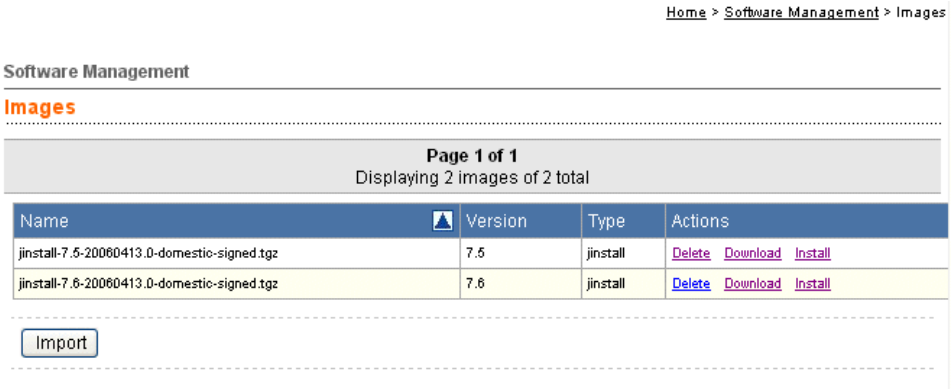
You can delete software images that are no longer needed from the Software Manager.

NOTE: You cannot delete a software image that is associated with an active operation schedule. To delete that image, you must click Manage Operations and delete the schedule associated with the image first, then delete the image using the following procedure.

To delete a software image, follow these steps:

1. In the JUNOScope main window, click Software Management > Images.

   The Images dialog box appears.



2. Click the Delete link for the software image that you want to delete.

   A confirmation dialog box appears.

3. Click OK.

   The image is deleted from the JUNOScope software. Any operations scheduled for the deleted image will fail unless you delete the scheduled operation using Monitor > Operations, see “Managing Operations” on page 313.

Part 9
Device Operational Monitoring Tools

Chapter 35

Using Looking Glass

This chapter describes how to use the Looking Glass tool kit, which provides a graphical user interface (GUI) for viewing device status and troubleshooting information from Juniper Networks routers, including general router, chassis, interface, route, system management, and routing protocol information.

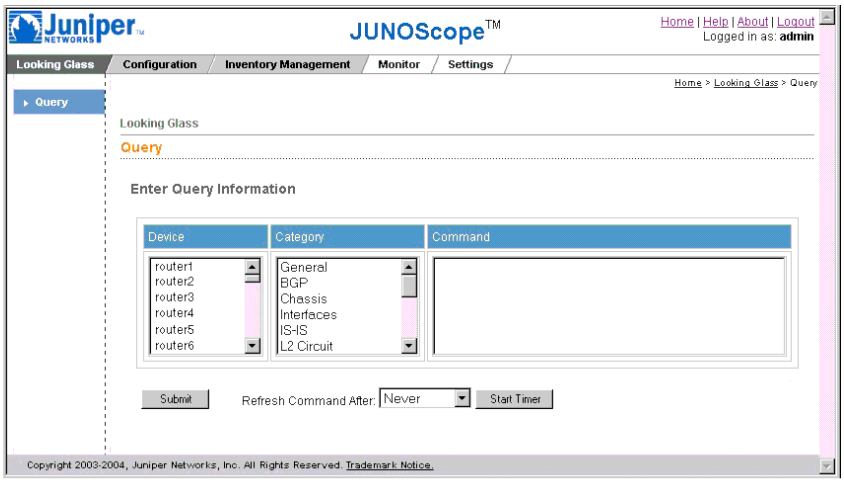
This chapter includes the following topics:

Viewing Router Operational Status Information

Use Looking Glass to view operational status and troubleshooting information for a selected router.

To view router operational status information, follow these steps:

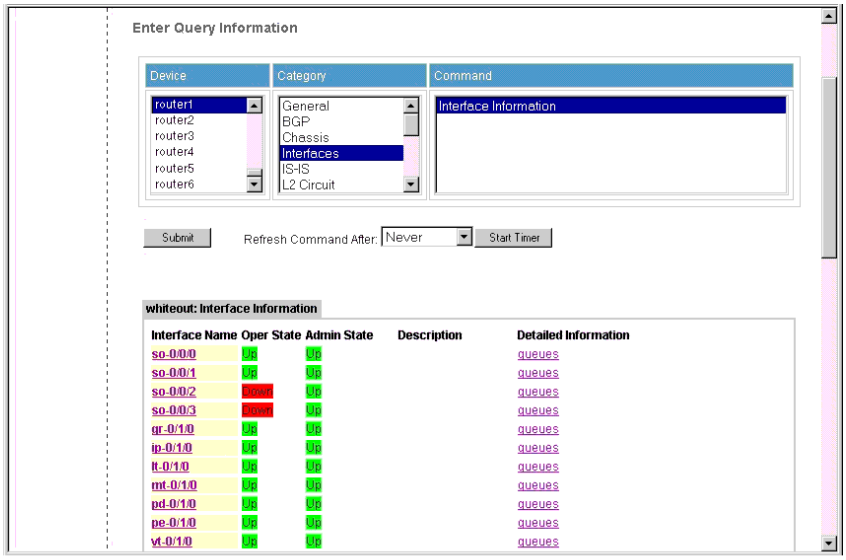
1. From the JUNOScope main window, click Looking Glass > Query. The Looking Glass Enter Query Information window appears.



2. In the Device list box, select the router that you want to monitor. The available routers in the list box are those added by the JUNOScope software administrator.

NOTE: You can view status and troubleshooting information from the TX Matrix routing platform, which consists of the TX Matrix platform (also known as the switch-card chassis [SSC]) and the attached T640 routing nodes (also known as the line-card chassis [LLC]).

3. In the Category list box, select the type of router command you want. See Table 43 on page 418 for a description of the available command categories.
4. In the Command list box, select the command that you want.
5. In the Refresh Command After drop-down list box, select how often you want Looking Glass to send a request to the router for the device command information. The default is Never. If you select 1 minute, Looking Glass will send a request for the device command information to the router every minute.
6. If you selected a Refresh Command After value, click Start Timer.
7. Click Submit. The device command results appear.



8. Click Query to return the Looking Glass settings to their defaults.

Looking Glass Device Commands

Table 43 on page 418 describes the Looking Glass device commands.

Table 43: Looking Glass Device Commands

Category	Device Command	Description
	Router Summary Information	Displays the current alarms, system uptime, and interface status information.
ASP	Stateful Firewall Flows	Displays the Adaptive Services (AS) Physical Interface Card (PIC) flow table entries.

Table 43: Looking Glass Device Commands *(continued)*

Category	Device Command	Description
	Stateful Firewall Flow Count	Displays a count of the matching flow table entries.
	Stateful Firewall Conversations	Displays stateful firewall conversation information.
	NAT Pool Information	Displays Network Address Translation (NAT) pool information.
	Service Set Memory Usage	Displays adaptive services interface memory utilization.
	Service Set CPU Usage	Displays service interface CPU utilization as a percentage.
BGP	BGP Neighbor Information	Displays information about Border Gateway Protocol (BGP) neighbors. Click a BGP neighbor for a detailed view.
	BGP Summary	Displays a summary of BGP and neighbor information.
Chassis	Alarm Status	Displays information about the current alarms, including alarm time, severity level, and description.
	Craft Interface Output	For routers with a craft interface, shows the operational status information that is currently displayed.
	Environment Information	Displays environmental information about the router chassis, including temperature and information about the fans, power supplies, and Routing Engine. The command output displays component environmental status colors. Green is OK, yellow is caution, red is alarm status.
	Hardware Summary	Displays a list of all the router hardware components, including the revision level, part number, serial number, and description. Click a hardware component for more specific hardware information.
	Routing Engine Information	Displays operational information about the Routing Engine.
Interfaces	Interface Information	Displays operational status information about all router interfaces. Click an interface name to view more detailed information about that interface.
IS-IS	IS-IS Adjacency Information	Displays information about Intermediate System-to-Intermediate System (IS-IS) neighbors.
	IS-IS Interface Information	Displays status information about the interfaces on which IS-IS is configured.
LDP	LDP Database	Displays entries in the Label Distribution Protocol (LDP) label database.
	LDP Interfaces	Displays the status of each interface on which LDP is enabled.
	LDP Neighbor	Displays a list of LDP neighbors.
	LDP Path	Displays the label-switched paths (LSPs) that the LDP created.
	LDP Route	Displays the entries in the LDP internal topology table. The internal topology table contains routes from inet.0 and inet.3 and is used when binding labels to Forwarding Equivalence Classes (FECs).
	LDP Session	Displays information about LDP sessions.

Table 43: Looking Glass Device Commands *(continued)*

Category	Device Command	Description
	LDP Statistics	Displays LDP statistics.
MPLS	MPLS LSP Information	Displays information about configured and active dynamic LSPs in which this router participates.
	MPLS LSP Statistics	Displays statistics about configured and active dynamic LSPs in which this router participates.
	MPLS LSP	Displays information about configured and active dynamic Multiprotocol Label Switching (MPLS) LSPs in which this router participates.
	MPLS Path	Displays the named paths used in dynamic MPLS that have been configured on this router.
	MPLS Interface	Displays information about interfaces on which MPLS is enabled. MPLS is enabled on an interface when the interface is configured in both the mpls and interface sections of the configuration hierarchy (with the set protocol mpls interface *interface-name* and set interface *interface-name* unit 0 family mpls statements, respectively).
	MPLS OSPF	Displays MPLS Constrained Shortest Path First (CSPF) statistics.
Multicast	Multicast Route	Displays the entries in the multicast forwarding table. You can display similar information with the show route table inet.1 command.
	Multicast RPF	Displays information about multicast reverse-path forwarding (RPF) calculations.
	Multicast Statistics	Displays multicast statistics. The input and output interface multicast statistics are consistent, but not timely. They are constructed from the forwarding statistics, which are gathered at 30-second intervals. Show Multicast Statistics will always lag true counts by up to 30 seconds.
	Multicast Usage	Displays usage information about the 10 most active Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM) groups.
OSPF	OSPF Database	Displays the entries in the Open Shortest Path First (OSPF) link-state database, including information about link-state advertisement (LSA) packets.
	OSPF Interface Information	Displays status information about the interfaces on which OSPF is configured.
	OSPF Neighbor Information	Displays information about OSPF neighbors.
	OSPF Route	Displays the entries in the OSPF routing table.
	OSPF Statistics	Displays OSPF statistics.
PIM	PIM Interfaces	Displays information about the interfaces on which PIM is configured.
	PIM Join	Displays information about PIM groups.
	PIM Neighbors	Displays information about PIM neighbors.
	PIM RPS	Displays information about PIM rendezvous points (RPs).
	PIM Source	Displays information about the PIM source RPF state.

Table 43: Looking Glass Device Commands *(continued)*

Category	Device Command	Description
	PIM Statistics	Displays PIM statistics.
Route	Display Route Summary	Displays summary statistics about the entries in the routing table.
RSVP	RSVP Interface Information	Displays the status for each interface on which the Resource Reservation Protocol (RSVP) is enabled, and displays packet statistics for each interface.
	RSVP Interface Details	Displays detailed status for each interface on which RSVP is enabled, and displays packet statistics for each interface.
	RSVP Neighbor Information	Displays a list of RSVP neighbors learned dynamically when exchanging RSVP packets. Once a neighbor is learned, it is never removed from the list of RSVP neighbors.
	RSVP Session Information	Displays information about RSVP sessions.
	RSVP Version Information	Displays information about the RSVP protocol settings, such as the version of the RSVP software, the refresh timer and keep multiplier, and local RSVP graceful restart capabilities on an LSP.
	RSVP Interface	Displays the status of each interface on which RSVP is enabled, and displays packet statistics for each interface.
	RSVP Neighbor	Displays a list of RSVP neighbors that were learned dynamically when exchanging RSVP packets. Once a neighbor is learned, it is never removed from the list of RSVP neighbors.
	RSVP Session	Displays information about RSVP sessions.
	RSVP Statistics	Displays RSVP packet and error statistics.
	RSVP Version	Displays information about the RSVP protocol settings, such as the version of the RSVP software, the refresh timer and keep multiplier, and local RSVP graceful restart capabilities on an LSP.
System	Storage Capacity	Displays statistics about the amount of free disk space in the router's file systems.
	Uptime	Displays the current time and information about how long the router, router software, and routing protocols have been running.
	Users	Displays information about the users who are currently logged in to the router.
	Version Information	Displays the hostname and version information about the software running on the router.
	System Commit	Displays the pending commit.
VPLS	VPLS Connection	Displays virtual private LAN service (VPLS) connection information.
VPN	l2circuit Connections	Displays status information about Layer 2 virtual circuits (VCs) from the local provider edge (PE) router to its neighbors.
	12vpn Connections	Displays Layer 2 virtual private network (VPN) connections.

Part 10
Device Configuration Management Tools

Chapter 36

Using the Configuration Browser

This chapter describes how to use the Configuration Browser tool kit, which provides a graphical user interface (GUI) for viewing the committed configuration of a selected device or router.

To use the Configuration Browser, you can have superuser, read-write, or read-only permissions.

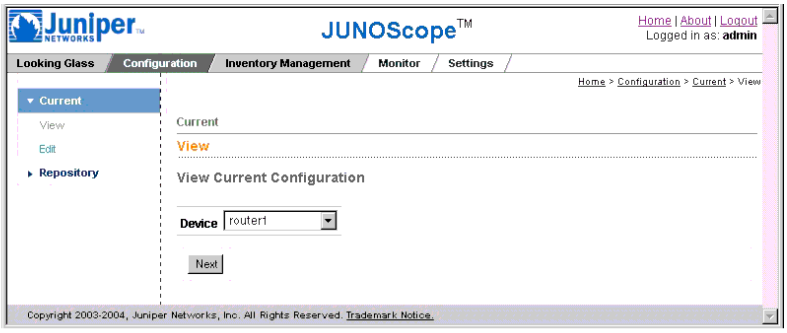
For more information about the router configuration, see the *JUNOS System Basics Configuration Guide*.

This chapter includes the following topics:

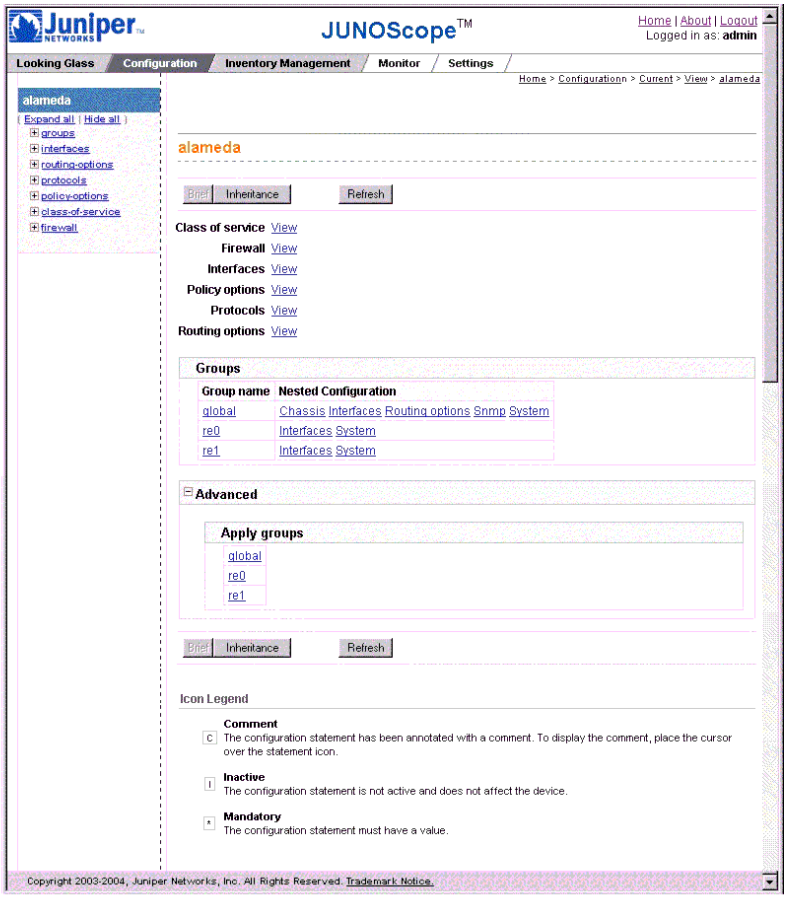
Displaying the Device Configuration

To display the Configuration Browser, follow these steps:

1. In the JUNOScope main window, click Configuration > Current > View. The View Current Configuration dialog box appears.



2. In the Device drop-down list box, select a device.
3. Click Next. The Configuration Browser window appears.



NOTE: When the Configuration Browser displays a router configuration, the right window pane displays the configuration first; then after a short delay, the left window pane displays the configuration hierarchy. Do not click in the left window pane until the configuration hierarchy appears.

Parts of the Configuration Browser Display

Figure 15 on page 427 defines the parts of the Configuration Browser window.

Figure 15: Parts of the Configuration Browser Window

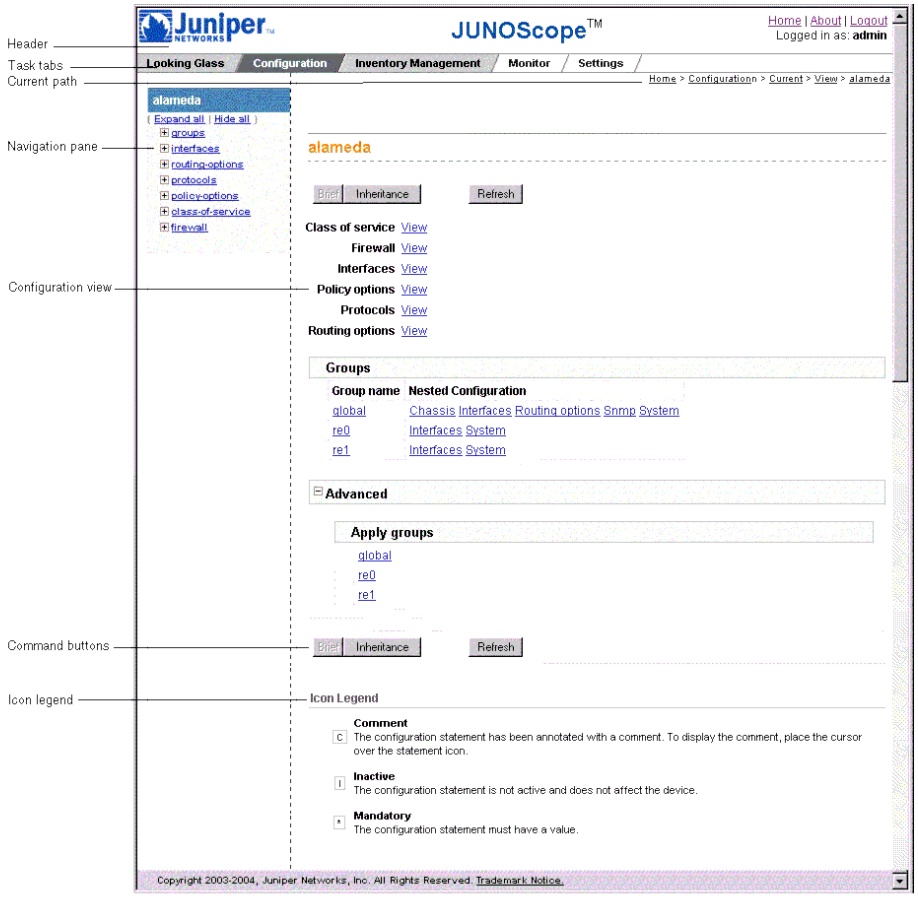


Table 44 on page 427 describes the parts of the Configuration Browser window.

Table 44: Parts of the Configuration Browser Window

Part	Description
Header	Includes the following items: ■ Juniper Networks logo—Click to go to the Juniper Networks Web site, www.juniper.net. ■ JUNOScope—Shows the name of this application. ■ Home—Click to go to the JUNOScope main window. ■ About—Displays the JUNOScope software release and copyright information. ■ Logout—Closes JUNOScope and displays the Login dialog box. ■ Logged in as: < *username* > —Displays the username used to log in to JUNOScope.

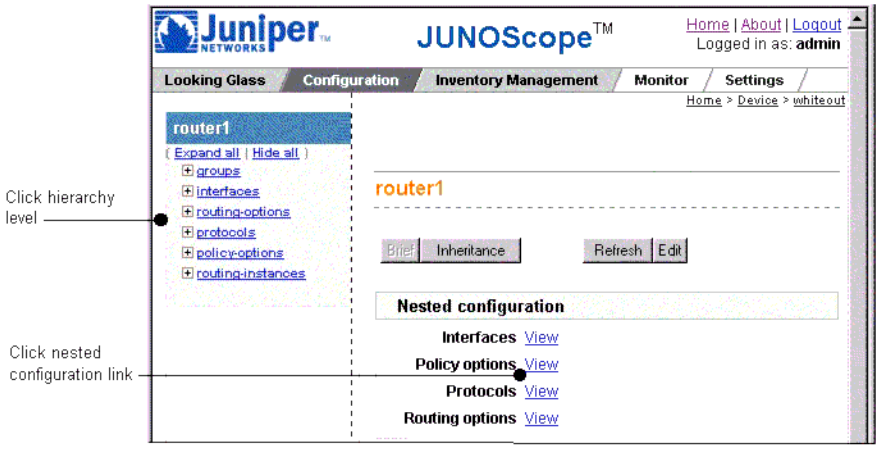
Table 44: Parts of the Configuration Browser Window *(continued)*

Part	Description
Task tabs	Displays the menu of JUNOScope main commands. Grey tabs are main application tasks that interact with routers or router data. White tabs indicate tasks for administering JUNOScope. Click a task tab to view its contents. ■ Looking Glass—Lets you display current operational information for a device, including device chassis, system software, interfaces, and routing protocols. ■ Configuration—Lets you view and edit the device configuration. Additionally, you can archive, compare, display, or restore selected device configurations. ■ Inventory Management—Scans selected devices for hardware and software installed and displays reports of the stored records. ■ Monitor—Lets you view scheduled and pending operations and the status of completed operations. ■ Settings—Lets you view and modify JUNOScope settings to manage devices.
Current path	Displays your location in the configuration statement hierarchy: ■ Home—Click to go to the JUNOScope main window. ■ Device—Displays the Configuration Browser window for you to select a different device configuration to view. ■ < *device name* > —Click to go the top level of the current device configuration statement hierarchy. ■ < *statement hierarchy* > —Displays your current level in the configuration.
Navigation pane	Displays the statement hierarchy levels of the configuration that have been configured. Provides an expanding and collapsing tree view of the configuration for a selected router. Click Hide All to collapse the configuration statement hierarchy levels to the top. Click a statement hierarchy level or [+] to view its configured substatements. Click Expand All to view all levels of the configuration.
Configuration view	Displays the current level of the configuration statement hierarchy. Displays the configuration container and leaf statements. Container statements contain other statements. Leaf statements do not contain other statements. Click a container statement link to view its contents.
Command buttons	Controls the statement hierarchy view: ■ Brief button—The default view, displays the basic hierarchy configuration. Only configured statements are displayed. ■ Inheritance button—Shows statements at the level at which they are inherited. ■ Refresh button—Displays the current committed configuration. ■ Edit button—Displays the configuration in the Configuration Editor for you to edit it. The Brief and Inheritance views remain in effect until you click another button.
Icon legend	Describes the icons that appear in the configuration view: ■ [c]—The configuration statement has a comment. Place the mouse cursor over the icon to display the comment. ■ [I]—The configuration statement and the configuration below this level are inactive. ■ [*]—Enter a value for the configuration statement. ■ [?]—Displays help for a configuration statement value.

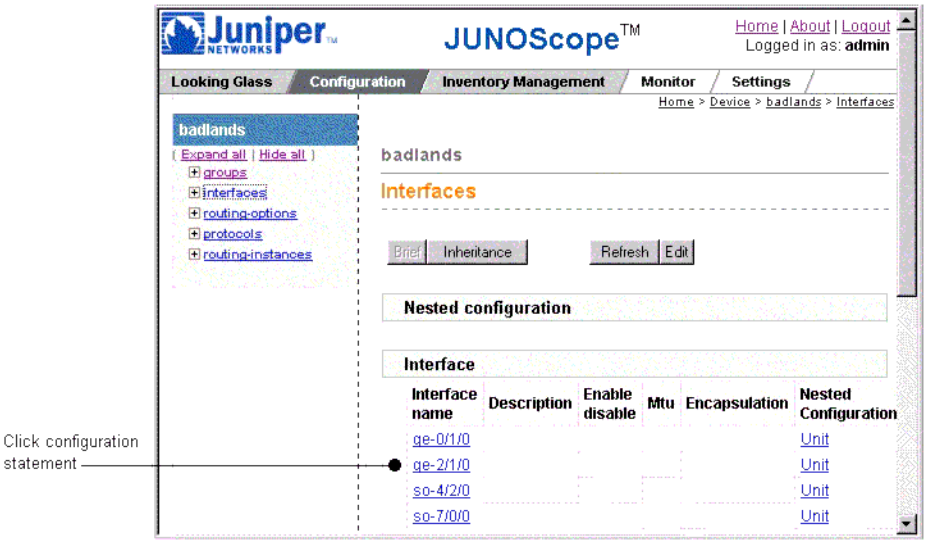
Using the Configuration View

To view a configuration hierarchy, follow these steps:

1. Click a configuration hierarchy level from the navigation pane or from the Nested configuration area in the Configuration view. The configuration for that hierarchy level appears.



2. Click a configuration statement to view its configuration.



The configuration appears in the Configuration View area.


Juniper NETWORKS
JUNOScope™
Home | About | Logout
Logged in as: admin
Looking Glass
Configuration
Inventory Management
Monitor
Settings
Home > Device > badlands > Interfaces > Interface ge-2/1/0
badlands
(Expand all | Hide all)
groups
interfaces
routing-options
protocols
routing-instances
Interfaces
Interface
Brief
Inheritance
Refresh
Edit
Interface name ge-2/1/0
Keepalive choices
Nested configuration
Vlan tag mode vlan-tagging
Vlan tagging Yes
Nested configuration
Unit
Interface unit number
Enable disable
Description
Encapsulation
Mtu
Nested Configuration
0
1
2

Chapter 37

Using the Configuration Editor

This chapter describes how to use the Configuration Editor tool kit, which provides a graphical user interface (GUI) for editing a configuration on a selected router.The Configuration Editor displays the complete top level of the configuration statement hierarchy in both list format and an expanding and collapsing tree format. To see the sublevels of the hierarchy, expand the statement or click Edit or Configure for the statement that you want to edit. You can modify the existing configuration or add a new configuration. Icons display in the configuration to identify where a configuration statement has been annotated, modified, is inactive, or must have a value. You can also use the Configuration Editor to commit the modified configuration, as well as discard any unwanted configuration changes.

To use the Configuration Editor, you must have superuser or read-write permissions. For more information about editing the a router's configuration, see the *JUNOS System Basics Configuration Guide*. See also Table 46 on page 434.

This chapter includes the following topics:

Displaying the Configuration Editor

To display the Configuration Editor, follow these steps:

1. In the JUNOScope main window, click Configuration > Current > Edit. The Edit Current Configuration dialog box appears.
2. In the Device drop-down list box, choose the device configuration you want to edit.

NOTE: The TX Matrix routing platform consists of the TX Matrix platform (also known as the switch-card chassis [SCC]) and the attached T640 routing nodes (also known as line-card chassis [LCC]). You can browse and edit the configuration on both the TX Matrix platform and the attached T640 routing nodes. You commit configuration edits to the TX Matrix platform.

3. Click Next. The Configuration Editor window appears.

Parts of the Configuration Editor Window

Figure 16 on page 432 defines the parts of the Configuration Editor window.

Figure 16: Parts of the Configuration Editor Window

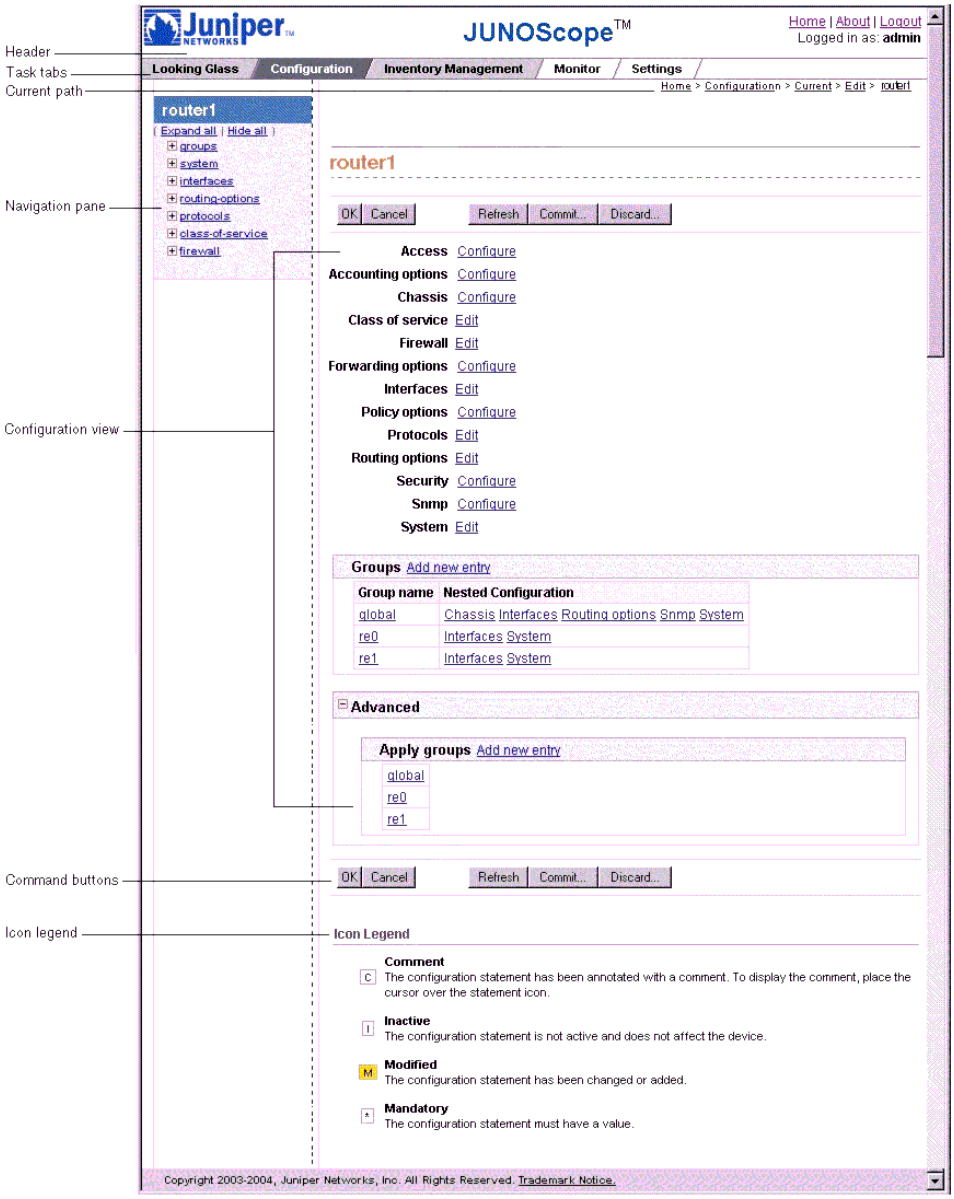


Table 45 on page 433 describes the parts of the Configuration Editor window.

Table 45: Parts of the Configuration Editor Window

Part	Description
Header	Includes the following items: ■ Juniper Networks logo—Click to go to the Juniper Networks Web site, www.juniper.net. ■ JUNOScope—Shows the name of this application. ■ Home—Click to go to the JUNOScope main window. ■ About—Displays the JUNOScope software release and copyright information. ■ Logout—Closes JUNOScope and displays the Login dialog box. ■ Logged in as: < *username* > —Displays the username used to log in to JUNOScope.
Task tabs	Displays the menu of JUNOScope main commands. Grey tabs are main application tasks that interact with routers or router data. White tabs indicate tasks for administering JUNOScope. Click a task tab to view its contents. ■ Looking Glass—Lets you display current operational information for a device, including device chassis, system software, interfaces, and routing protocols. ■ Configuration—Lets you view and edit the device configuration. Additionally, you can archive, compare, display, or restore selected device configurations. ■ Inventory Management—Scans selected devices for hardware and software installed and displays reports of the stored records. ■ Monitor—Lets you view scheduled and pending operations and the status of completed operations. ■ Settings—Lets you view and modify JUNOScope settings to manage devices.
Current path	Displays your location in the configuration statement hierarchy: ■ Home—Click to go to the JUNOScope main window. ■ Device—Displays the Configuration Browser window for you to select a different device configuration to view. ■ < *device name* > —Click to go the top level of the current device configuration statement hierarchy. ■ < *statement hierarchy* > —Displays your current level in the configuration.
Navigation pane	Displays the statement hierarchy levels of the configuration that have been configured. Provides an expanding and collapsing tree view of the configuration for a selected router. Click a statement hierarchy level or [+] to view its configured substatements. Click Expand All to view all levels of the configuration. Click Hide All to collapse the configuration statement hierarchy levels to the top.
Configuration view	Displays the current level of the configuration statement hierarchy. Displays the configuration container and leaf statements. Container statements contain other statements. Leaf statements do not contain other statements. Displays data for the current level of configuration. Click Edit to modify that configuration statement and any nested statements. The word Configure appears if a configuration statement has not been modified. Click Configure to edit the configuration of that statement and any nested statements.

Table 45: Parts of the Configuration Editor Window *(continued)*

Part	Description
Command buttons	Contains the buttons that control the view in the statement/hierarchy view: ■ OK—Saves changes and takes you to the parent statement level. Changes are kept local to the JUNOScope server until you click Commit. ■ Cancel—Discards any edits that you've made and takes you to the parent statement level. ■ Apply—Saves the changes you've made in the current window, but does not exit that window. You can make more changes and apply or cancel them. Apply does not change the configuration running on the router. Changes are kept local to the JUNOScope server until you click Commit. ■ Refresh button—Refreshes the cached configuration with the currently committed configuration. Your changes are maintained and continue to be displayed. ■ Commit—Displays a review screen that displaces the set of changes and prompts you to continue. If you confirm to continue, the configuration is checked for syntax errors, activated, and made operational on the selected router. ■ Discard—Displays a dialog box from which you can choose to discard changes below the current level in the configuration, discard all changes, or delete the configuration below the current level.
Icon legend	Describes the icons that appear in the configuration items: ■ [c]—The configuration statement has a comment. Place the mouse cursor over the icon to display the comment. ■ [I]—The configuration statement and the configurations below this level are inactive. ■ [M]—The configuration statement has been edited. ■ *—The configuration statement requires a mandatory value.

Editing the Configuration

Table 46 on page 434 identifies the statement hierarchy levels in the device configuration and the JUNOS software configuration guide where you can find configuration guidelines for editing.

Table 46: Configuration Guidelines for Editing the Configuration

Configuration Hierarchy Level	JUNOSSoftware for J-series, M-series, MX-series, and T-series Routing Platforms Configuration Guide
Access	*JUNOS System Basics Configuration Guide*
Accounting Options	*JUNOS Network Interfaces Configuration Guide*
Applications	*JUNOS Routing Protocols Configuration Guide*
Chassis	*JUNOS System Basics Configuration Guide*
Class of Service	*JUNOS Network Interfaces Configuration Guide*
Firewall	*JUNOS Policy Framework Configuration Guide*

Table 46: Configuration Guidelines for Editing the Configuration *(continued)*

Configuration Hierarchy Level	JUNOSSoftware for J-series, M-series, MX-series, and T-series Routing Platforms Configuration Guide
Forwarding Options	*JUNOS Routing Protocols Configuration Guide*
Interfaces	*JUNOS Network Interfaces Configuration Guide*
Policy Options	*JUNOS Policy Framework Configuration Guide*
Protocols	*JUNOS Routing Protocols Configuration Guide*
Routing Instances	*JUNOS Routing Protocols Configuration Guide*
Routing Options	*JUNOS Routing Protocols Configuration Guide*
Security	*JUNOS System Basics Configuration Guide*
Services	*JUNOS Network Interfaces Configuration Guide*
SNMP	*JUNOS Network Management Configuration Guide*
System	*JUNOS System Basics Configuration Guide*

To edit the configuration of a selected router using the Configuration Editor, follow these steps:

1. In the navigation pane or in the configuration view area, click the configuration statement hierarchy level that you want to edit.

   In the Nested Configuration area, the Edit link appears for statement hierarchy levels that have not been configured; the Configure link appears for statement hierarchy levels that have not been configured. The configuration for the statement hierarchy level that you chose appears.

2. Click the configuration statement link that you want to edit.
3. Do one of the following:
   - To change an existing configuration, click the Edit link next to the statement name.
   - To add a new configuration, click Configure or Add new entry next to the statement name.
   - To delete an existing configuration, click the Discard button in the button bar. You can discard all outstanding changes, discard all changes below the current edit point, or delete all configurations below the current edit point.

NOTE: To view help text about a configuration statement value that you want to edit, move the mouse curser over the [?] icon.

4. To edit a configuration statement or option, type text in the text field or select a drop-down list item.

NOTE: The [M] icon displays indicating that you modified the field's value. Help text displays when you place the cursor over the icon to indicate that the field was previously unconfigured. Click the modified icon to return the value to its unconfigured state.

5. Click OK. The Configuration Editor keeps a copy of all of the changes you make as part of your JUNOScope session. The router itself is not updated until you click Commit.

NOTE: If you end the Configuration Editor session without committing the configuration changes you made, JUNOScope saves them until the next session and prompts you to commit them.

6. Click Commit. JUNOScope sends the following commands to the JUNOScript server to be performed on the router:
   a. Lock the router configuration.
   b. Load the new configuration on the router, overriding (discarding) the old configuration.
   c. Issue a commit confirmed command.
   d. Issue a commit-configuration JUNOScript XML tag command.
   e. Unlock the configuration.

NOTE: If an error occurs, JUNOScope issues a rollback command, causing the configuration to revert to the last saved configuration.

Part 11

JUNOScope Window and Dialog Box Reference

Chapter 38

JUNOScope Main Window

This chapter describes the contents of the JUNOScope software main window.

JUNOScope Window Reference

Figure 17 on page 439defines the major areas of the JUNOScope main window.

Figure 17: JUNOScope Main Window

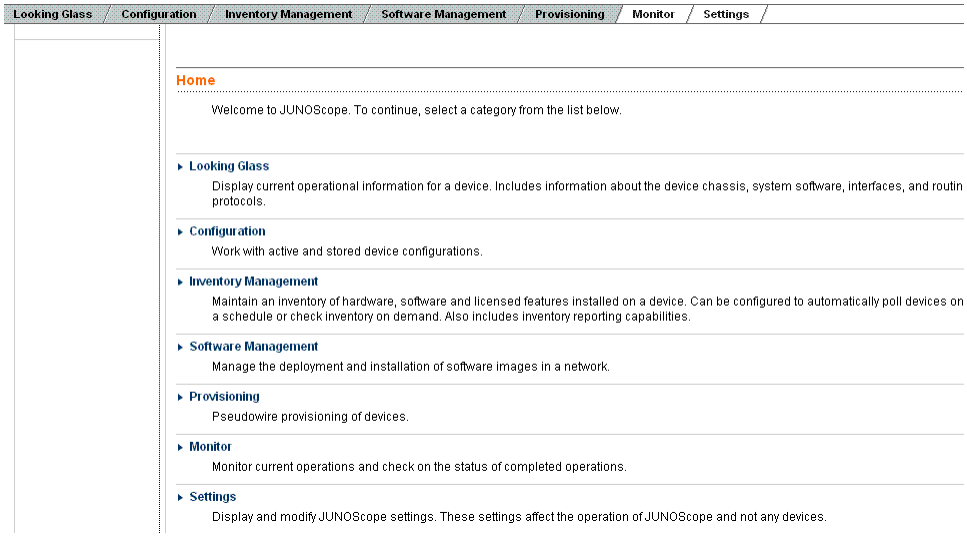


Table 47 on page 440 describes the parts of the JUNOScope main window.

Table 47: Parts of the JUNOScope Main Window

Part	Description
Header	Includes the following items: ■ Juniper Networks logo—Click to go to the Juniper Networks Web site, www.juniper.net. ■ JUNOScope—Shows the name of this application. ■ Home—Click to go to the JUNOScope main window. ■ About—Displays the JUNOScope software release and copyright information. ■ Logout—Closes JUNOScope and displays the Login dialog box. ■ Logged in as: < *username* > —Displays the username used to log in to JUNOScope.
Task tabs	Display the menu of JUNOScope main commands. Gray tabs are main application tasks that interact with routers or router data. White tabs indicate tasks for administering JUNOScope. Click a task tab to view its contents. ■ Looking Glass—Lets you display current operational information for a device, including device chassis, system software, interfaces, and routing protocols. ■ Configuration—Lets you view and edit the device configuration. Additionally, you can archive, compare, display, or restore selected device configurations. ■ Inventory Management—Scans selected devices for hardware and software installed and displays reports of the stored records. ■ Monitor—Lets you view scheduled and pending operations and the status of completed operations. ■ Settings—Lets you view and modify JUNOScope settings to manage devices.
Commands	Indicate the main JUNOScope commands (see the Task tabs section of this table for command descriptions). Click a command to view its submenu of commands.

NOTE: If you click the Reload or Refresh button in your Web browser while using the JUNOScope software, the browser displays the default home page instead of reloading or refreshing the currently displayed JUNOScope main window. Use the Home link in the JUNOScope main window instead to refresh.

Chapter 39

JUNOScope Dialog Box Reference

This chapter provides an alphabetical reference for the dialog boxes you use to perform JUNOScope software operations.

■ on page 519

Access Methods Dialog Box

Description Use the Access Methods dialog box to view the access methods that you have added to the JUNOScope software. The available access methods are listed by access method name, connection type (SSL, clear-text, or SSH), and authentication information name.

The Access Methods dialog box is empty until you add an access method.

Navigation Click Settings > Access Methods.

Permissions Superuser

Elements Access Methods table—Lists the access methods that you have added by access method name, connection type (JUNOScript over SSL, JUNOScript over clear-text, or NETCONF over SSH), and authentication information name. Select an access method to edit or delete.

Export Data Encryption Format options—Select one of the following ways to export authentication information from the JUNOScope software:

- Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
- Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export access methods information to another system.
- Export sensitive data unencrypted—Sensitive data is not encrypted at export.

Add button—Displays the Add Access Method dialog box so you can add a new access method.

Edit button—Displays the Edit Access Method dialog box so you can edit an existing access method. Select the access method that you want to edit, then click Edit.

Delete button—Deletes a selected Access Method entry from the Access Methods dialog box. You cannot delete authentication information that is currently being used by an access method. You must first delete the access method, then delete the authentication information. You cannot delete an access method if it is currently being used by a device. You must first delete the device, then delete the access method.

Export button—Displays the File Download dialog box to export the setup data in XML file format to the file system. The default access methods export filename is junoscope-access-methods.xml.

Import button—Displays the Import dialog box for you to specify the import XML file to import.

Access Methods—Add Access Method Dialog Box

Description Use the Add Access Method dialog box to add the information you need to connect the JUNOScope software to a router on the network, including an Access Method name for the JUNOScope software, an access method type (SSL, SSH, or clear-text), and the authentication information name from the JUNOScope software.

Navigation Click Settings > Access Methods. Click Add in the Access Methods dialog box.

Permissions Superuser

Elements Access Method Name text box—Type a name for the remote router access method for the JUNOScope software. This is the access method name used in the Add Device dialog box.

Access Method Type drop-down list box—Select a supported access protocol that is configured on the router, JUNOScript over SSL, NTECONF over SSH, or JUNOScript over clear-text.

Authentication Information drop-down list box—Select an authentication name to use for the access method. This is the same name that you created in the Add Authentication Information dialog box.

OK button—Displays the Access Methods dialog box with the new access method displayed.

Cancel button—Clears this dialog box without adding an access method.

Access Methods—Edit Access Method Dialog Box

Description Use the Edit Access Methods dialog box to edit the information necessary to connect the JUNOScope software to a router on the network, including an access method name for the JUNOScope software, an access method type (SSL or clear-text), and an authentication information name.

Navigation Click Settings > Access Methods. Select the access method that you want to edit in the Access Methods dialog box, and click Edit.

Permissions Superuser

Elements Access Method Name text box—Type a name for the remote router access method for the JUNOScope software. This is the access method name used in the Add Device dialog box.

Access Method Type drop-down list box—Select a supported access protocol that is configured on the router, JUNOScript over SSL, NTECONF over SSH, or JUNOScript over clear-text.

Authentication Information drop-down list box—Select an authentication name to use for the access method. This is the same name that you created in the Add Authentication Information dialog box.

OK button—Displays the Access Methods dialog box with the edited access method information.

Cancel button—Clears this dialog box without saving any editing changes.

Access Methods—Import Access Methods Dialog Box

Description Use the Import Access Methods dialog box to import access method setup information into the JUNOScope software without having to manually enter it. The default access methods import filename is junoscope-access.xml.

Navigation Click Settings > Access Methods. Click Import in the Access Methods dialog box.

Permissions Superuser

Elements File to import text box—Type the name of or browse to the access method XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Browse button—Displays the File Open dialog box so you can select the XML file to import.

Import button—Imports the selected access method data into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears this dialog box and displays the Access Methods dialog box.

Archive—Confirm Selections Dialog Box

Description Use the Archive—Confirm Selections dialog box to confirm whether you want to finish a selected operation, such as Archive.

Navigation Click Configuration > Repository > Archive. Select the device(s) or a group of devices from which you want to archive a configuration and a time to archive in the Archive—Select Device and Time dialog box, then click Next.

Permissions Superuser, read-write

Elements Please Confirm Operation display field—Displays the operation, the device or group from which the operation will be performed, and the schedule for your confirmation.

Finish button—Executes the operation. An operation progress message appears, then the Requested Operation Status dialog box appears displaying the status of the operation by device name, operation status, start time, last updated time, and the operation status message.

Previous button—Redisplays the previous operation dialog box and does not execute the operation.

Cancel button—Cancels the operation and redisplays the JUNOScope main window.

Archive—Select Device and Time Dialog Box

Description Use the Archive—Select Device and Time dialog box to archive or download the committed version of the configuration from a selected router or group of routers on your network to the JUNOScope software Concurrent Versions System (CVS) repository. You can save archive operations to combine them with other operations to run concurrently or sequentially at a specific time.

Navigation Click Configuration > Repository > Archive.

Permissions Superuser, read-write

Elements Devices to Archive section:

- Group check box and drop-down list box—Select a router group from which to archive a configuration file. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any router groups, the Groups drop-down list box is empty.
- Selected Devices check boxanddrop-down list box—Select a router from which to archive a configuration file. Click the Devices option button, then click the Devices drop-down list box to display the available routers added for JUNOScope software operations. If you have not added any routers, the Router drop-down list box is empty.
- Comment text box—Type a descriptive comment about the archive operation you want to run.

Select Time or Save Operation section:

- Now check box—Select to have an archive operation occur as soon as the command is executed. Click the Now option button.
- Save Operation as text box—Type a name for the archive operation that you want to save. The saved archive operation appears in the Saved Operations page with the name that you gave it. To view the Saved Operations page. click Settings > Saved Operations.
- Select Schedule check box and table—Select a particular schedule for an archive operation. Click the Selected Schedule check box, then select a schedule from the schedule table. The schedule table lists the available schedules added for JUNOScope software operations by schedule name, start time, period or interval, and comment.

Next button—Displays the Confirm Operations dialog box from which you can select to finish the archive operation or cancel it.

Cancel button—Clears this dialog box and redisplays the Configuration > Repository menu.

Archive — Confirm Selections Dialog Box

Description User the Confirm Selections dialog box to specify whether you wish to archive the startup configuration or the running configuration

Navigation Click Configuration > Repository > Archive and then click Next in the Select Device and Time dialog box after entering the details.

Permissions Superuser

Elements Archive Startup Configuration option button—Select this to archive the startup configuration on a BXOS device. This option is selected by default.

Archive Running Configuration option button—Select this to archive the running configuration on a BXOS device.

NOTE: The preceding options are available only when you have selected a BXOS device for archiving the configuration.

Finish button—Click this to complete the wizard.

Previous button—Click this to go back to the Select Device and Time dialog box.

Cancel button—Click this to cancel archival.

Archive—View Operation Status Dialog Box

Description Use the Archive—View Operation Status dialog box to view the results of an archive operation by device name, operation status, operation start time, last update time, and status message.

Navigation Click Configuration > Repository > Archive. Select the device and time for the archive in the Archive—Select Device and Time dialog box, and click Next. Confirm your selection in the Archive—Confirm Selections dialog box, and click Next. Wait for the operation to complete.

Permissions Superuser, read-write

Elements Archive Results table—Lists the archive results by device name, operation status, operation start time, last update time, and status message.

OK button—Displays the JUNOScope main window.

Archive Tags Dialog Box

Description Use the Archive Tags dialog box to create and manage archived configuration tags. The Archive Tags dialog box is empty until you create tags using the Add button.

Navigation Click Configuration > Repository > Archive Tags.

Permissions Superuser, read-write

Elements Name column—Name of the archived configuration tag.

Comment column—Comment entered while creating the archived configuration tag.

Actions column—Actions that you can perform on an archived configuration tag. The possible actions are:

- Edit link—Edits or renames the selected tag using the Edit Archive Tags dialog box.
- Copy link—Creates a copy of the selected tag, including all associated device configurations using the Copy Archive Tags dialog box.
- Delete link—Deletes the selected tag after you click OK confirming that you really want to delete it.
- Set Archive Tag link—Associates the selected tag to one or more devices using the Associate Archive Tags with Devices dialog box.

Add button—Creates a new archived configuration tag using the Add Archive Tag dialog box.

Archive Tags—Add Archive Tag Dialog Box

Description Use the Add Archive Tags dialog box to add an archived configuration tag.

Navigation Click Configuration > Repository > Archive Tags. Click Add in the Archive Tag dialog box.

Permissions Superuser, read-write

Elements Name text box—Type a unique name for the archived configuration tag. Follow these rules when adding an archive tag name or you will not be able to associate the tag with a device configuration:

- Tag name length must be no more than 40 characters.
- The first character of a tag name must be a letter.
- The rest of the tag name characters can be alphanumeric characters.
- The tag name can include a hyphen (-) or an underscore (_). Do not include a period (.).

Comment text box—Type an optional descriptive comment about the archived configuration tag you are adding.

OK button—Adds the archived configuration tag.

Cancel button—Clears the dialog box and displays the Archive Tags dialog box.

Archive Tags—Import Archive Tag Dialog Box

Description Use the Import Archive Tag dialog box to import archive tags into the JUNOScope software without having to manually enter them.

Navigation Click Configuration > Repository > Archive Tags. Click Import in the Archive Tag dialog box.

Permissions Superuser, read-write

Elements File text box—Lets you type or browse to the access method XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Browse button—Displays the File Open dialog box for you to select the XML file to import.

Import button—Imports the selected archive tag into the JUNOScope software and displays the Import Result dialog box.

Cancel button—Clears this dialog box and displays the Archive Tag dialog box.

Archive Tags—Associate Archive Tags with Devices Dialog Box

Description Use the Associate Archive Tags with Devices dialog box to associate archived configuration tags with available devices on the network that have been configured for JUNOScope.

Navigation Click Configuration > Repository > Archive Tags. Click the Set Archive Tag action link for the tag that you want to associate with devices.

Permissions Superuser, read-write

Elements Archive Tag Name display field—Name of the archived configuration tag.

Comment display field—Comment entered while creating the archived configuration tag.

Available Devices list box—Lists the devices available on the network that have been configured for JUNOScope that can be selected for association with archived tags.

Add/Remove buttons—Move devices from the Available Devices list box to the Selected Devices to Tag/Untag list box.

- Add button—Adds the selected available devices from the Available Devices list box to the Selected Devices to Tag/Untag list box. The Add button is disabled until you select one or more devices in the Available Devices list box.
- Remove button—Removes the selected device(s) from the Selected Devices to Tag/Untag list box to the Available Devices list box.
- Add All —Adds all the available devices from the Selected Devices list box to the Selected Devices to Tag/Untag list box without selecting them.
- Remove All —Removes all the devices from the Selected Devices to Tag/Untag list box without selecting them.

Selected Devices to Tag/Untag list box—Lists the devices you have selected to tag or untag with the archive tag.

View/Tag/Untag Selected Devices button—View all configuration revisions for each selected device in the Selected Devices to Tag/Untag list box, select a configuration revision, and tag or untag configuration revisions for each device iteratively.

Tag All Head Revisions button—Assign a tag to the head (latest) revision in the repository for all selected devices in the Selected Devices to Tag/Untag list box. If an existing tag is added to the head (latest) revision of a device, the tag is automatically removed from the old revision. If you click Tag All Head Revisions, the message "Successfully tagged head revision of selected devices" appears in the Associate Archive Tags with Devices dialog box after all the head revisions are tagged.

Untag All button—Untag all the configuration revisions for all selected devices in the Selected Devices to Tag/Untag list box. If you click Untag All, the message "Successfully untagged selected devices" appears after all the configuration revisions for the selected devices that are untagged.

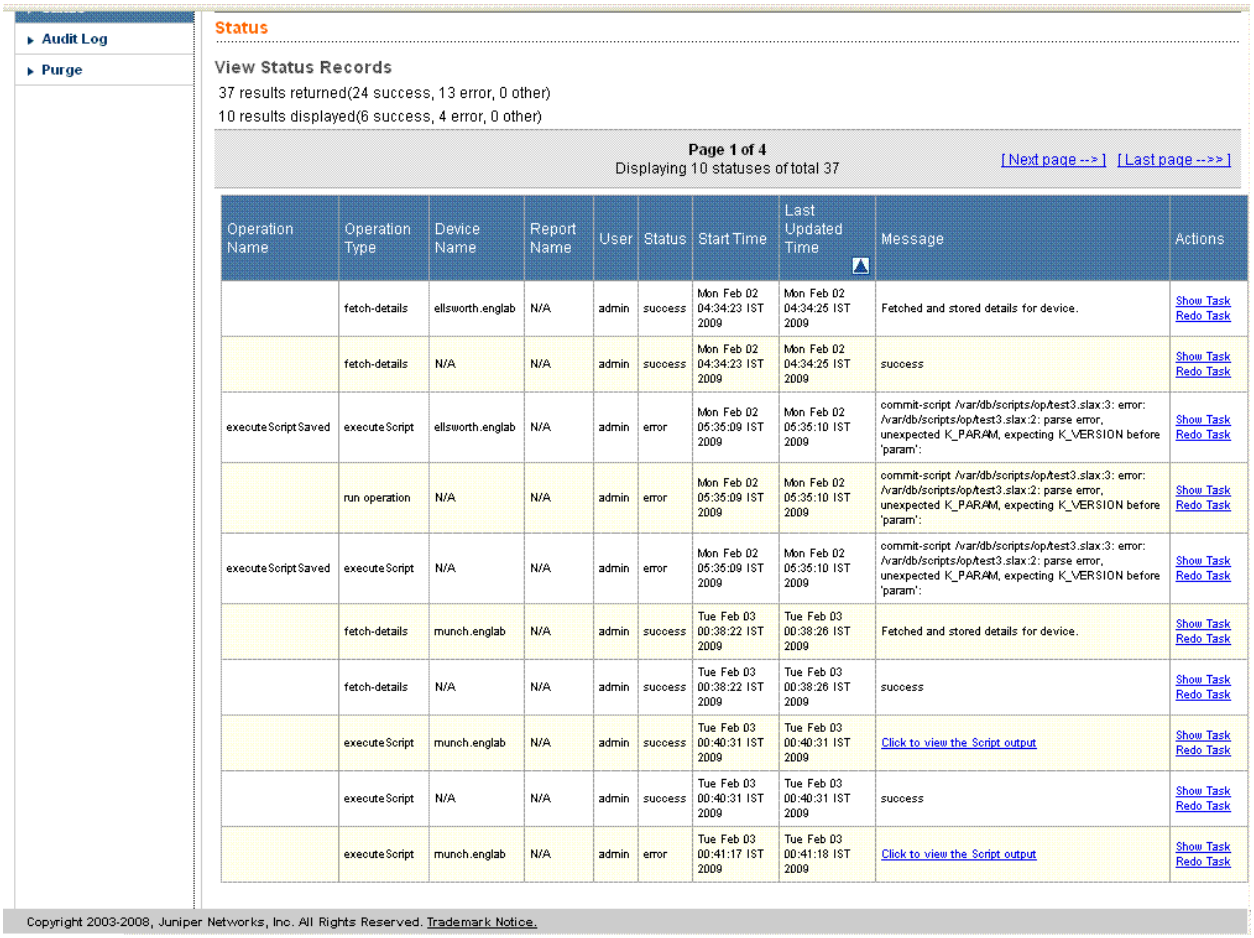
Finish button—Saves any changes made and displays the Archive Tags dialog box.

Archive Tags—Compare Configuration Dialog Box

Description Use the Compare Configuration dialog box to view the difference between configuration revisions of a device or group of devices. For example, you can compare the most current device configuration in the JUNOScope CVS repository with the one currently running on a selected device or group of selected devices.

Navigation There are two ways to navigate to the Compare Configuration dialog box:

- Click Configuration > Repository > Archived Tags. Click the Set Archive Tag link. Associate and tag the configurations you want in the Associate Archive Tags with Devices dialog box. Click View/Tag/Untag Each Selected. Select two configuration revisions you want to compare and click Compare in the Tag or Untag Configuration Revisions dialog box.
- Click Configuration > Repository > Audit Configurations. Select the configuration compare options—devices, source tag and target tag, and the time at which to audit the configuration. Click Compare. The Audit Configurations—Confirm Selections dialog box appears. Click Finish. The View Status Records dialog box appears. Click a link to view the differences between revision X and revision Y in the View Status Records dialog box. If there is no difference between the configuration versions, the following message appears " No differences between revision 'X' and 'Y'."



Operation Name	Operation Type	Device Name	Report Name	User	Status	Start Time	Last Updated Time	Message	Actions
	fetch-details	ellsworth.englab	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Mon Feb 02 04:34:23 IST 2009	Mon Feb 02 04:34:25 IST 2009	success	Show Task Redo Task
executeScriptSaved	executeScript	ellsworth.englab	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	run operation	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
executeScriptSaved	executeScript	N/A	N/A	admin	error	Mon Feb 02 05:35:09 IST 2009	Mon Feb 02 05:35:10 IST 2009	commit-script /var/db/scripts/op/test3.slax:3: error: /var/db/scripts/op/test3.slax:2: parse error, unexpected K_PARAM, expecting K_VERSION before 'param':	Show Task Redo Task
	fetch-details	munch.englab	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	Fetched and stored details for device.	Show Task Redo Task
	fetch-details	N/A	N/A	admin	success	Tue Feb 03 00:38:22 IST 2009	Tue Feb 03 00:38:26 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	Click to view the Script output	Show Task Redo Task
	executeScript	N/A	N/A	admin	success	Tue Feb 03 00:40:31 IST 2009	Tue Feb 03 00:40:31 IST 2009	success	Show Task Redo Task
	executeScript	munch.englab	N/A	admin	error	Tue Feb 03 00:41:17 IST 2009	Tue Feb 03 00:41:18 IST 2009	Click to view the Script output	Show Task Redo Task

Permissions Superuser, read-write

Elements Configuration Compare of Revision X to Revision Y on Device Name display field—Displays the differences between the two compared configuration file revisions. Displays the configuration revision number and the device name from which the configuration is displayed. By default, the compare archived configuration command compares the newer revision to the older one.

Archive Tags—Copy Archive Tag Dialog Box

Description Use the Copy Archive Tags dialog box to copy an archived configuration tag including all associated device configurations.

Navigation Click Configuration > Repository > Archive Tags. Click Copy in the Archive Tag dialog box.

Permissions Superuser, read-write

Elements Name text box—Lets you edit the name of the archived configuration tag. Follow these rules when adding an archive tag name or you will not be able to associate the tag with a device configuration:

- Tag name length must be no more than 40 characters.
- The first character of a tag name must be a letter.
- The rest of the tag name characters can be alphanumeric characters.
- The tag name can include a hyphen (-) or an underscore (_). Do not include a period (.).

Comment text box—Lets you edit the optional descriptive comment about the archived configuration tag you are editing.

OK button—Copies the archived configuration tag with all associated device configurations.

Cancel button—Cancels any changes that you have made, and displays the Archive Tags dialog box.

Archive Tags—Edit Archive Tag Dialog Box

Description Use the Edit Archive Tags dialog box to edit an existing archived configuration tag name and comment.

Navigation Click Configuration > Repository > Archive Tags. Click the Edit action link in the Archive Tag dialog box.

Permissions Superuser, read-write

Elements Name text box—Edits the name of the archived configuration tag.

Comment text box—Edits the optional descriptive comment about the archived configuration tag you are editing.

OK button—Saves the edited configuration tag.

Cancel button—Cancels the changes and displays the Archive Tags dialog box.

Archive Tags—Tag or Untag Configuration Revisions Dialog Box

Description Use the Tag or Untag Configuration Revision dialog box to tag or untag archived configuration revisions.

Navigation Click Configuration > Repository > Archive Tags. Click the Set Archive Tag action link for the tag that you want to associate with devices. The Associate Archive Tags with Devices dialog box appears. Click View/Tag/Untag Selected Devices.

Permissions Superuser, read-write

Elements Archive Tag Name display field—Displays the name of the archived configuration tag.

Comment display field—Displays the comment entered while creating the archived configuration tag.

Device display field—Displays the device selected to tag or untag using the archived configuration tag.

The Archive Configuration table—Displays the archived configurations that you want to tag for a selected device. You must have archived at least one configuration for selected devices, or the table will be empty. The table columns are defined as follows:

- Archive Date column—Displays the date on which the configuration was archived.
- Revision column—Displays the current version of a configuration revision.
- Tags Assigned column—Displays the tags assigned to a configuration revision.
- Actions column—Click Display to display the configuration file.

Tag button—Applies the tag to the configuration revision selected.

UnTag < *tag-name* > button—Removes the tag from the configuration revision selected if the tag has already been associated with the configuration revision.

Next Device button—Displays the Tag or Untag Configuration Revisions dialog box for the next device when you are tagging configuration revisions of multiple devices iteratively. You can tag configuration revisions of multiple devices iteratively using this command button. (Appears only when you tag multiple configuration revisions.)

Previous Device button—Displays the Tag or Untag Configuration Revisions dialog box for the previous device when you are tagging configuration revisions of multiple devices iteratively. (Appears only when you tag multiple configuration revisions.)

Compare button—Compares two selected configuration revisions.

Finish button—Saves any changes made and displays the Associate Archive Tags with Devices dialog box.

Archive Tags—View Configuration Dialog Box

Description Use the View Configuration dialog box to view the contents of a selected configuration file.

Navigation Click Configuration > Repository > Archived Tags. Click the Set Archive Tag link. Associate and tag the configurations you want in the Associate Archive Tags with Devices dialog box. Click View/Tag/Untag Each Selected. Select a configuration revision you want to view and click Display in the Tag or Untag Configuration Revisions dialog box.

Permissions Superuser, read-write

Elements Configuration Revision X.X display box—Displays the read-only contents of the selected configuration file revision. Displays the configuration revision number and the device name from which the configuration is displayed.

Previous button—Displays the previous Tag or Untag Configuration Revisions dialog box from which you can select another configuration file revision to display.

Audit Configurations—Confirm Selections Dialog Box

Description Use the Confirm Selections dialog box to confirm your selections and finish the selected operation.

Navigation Click Configuration > Repository > Audit Configurations. Select the options you want in the Audit Configurations—Select Device, Tags, and Time dialog box, then click Compare.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the source and target tags for the audit configurations, and the devices or groups from which the operation will be performed, and the schedule for your confirmation.

Finish button—Executes the operation. The Status—View Status Records dialog box appears displaying the status of the audit configurations operation. If there is a difference between the configurations that you selected to audit, a Click to view differences link appears in the Message column of the table for you to compare the different configuration revisions.

Previous button—Redisplays the previous operation dialog box and does not execute the operation.

Cancel button—Cancels the operation and redisplays the JUNOScope main window.

Audit Configurations—Select Devices, Tags, and Time Dialog Box

Description Use the Select Devices, Tags, and Time dialog box to select the devices and the archived configuration tags associated with these devices, and to schedule a time to audit the selected configurations.

Navigation Click Configuration > Repository > Audit Configurations.

Permissions Superuser

Elements Group check box and drop-down list box—Select a router group to audit configurations. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any router groups, the Groups drop-down list box is empty.

Selected Devices check box and drop-down list box—Select a router from which to audit configuration files. Click the Devices option button, then click the Devices drop-down list box to display the available routers added for JUNOScope software operations. If you have not added any routers, the Router drop-down list box is empty.

Source Tag drop-down list box—Select a source file for audit identified by tag name from the drop-down list box. The drop-down list box lists all the archived configuration tags that have been manually added and the implicit tags "Head Revision" and "Running". "Running" is the current configuration that JUNOScope will retrieve from the router, "Head Revision" is the most recent revision of a configuration file in the repository. If the "Running" option is selected, JUNOScope attempts to obtain the running configuration from the router, compare it with the latest revision in repository, and archive it as the "Head Revision" if they are different, before using it for comparison.

Target Tag drop-down list box—Select a target file for audit identified by tag name from the drop-down list box. The drop-down list box lists all the archived configuration tags that have been manually added and the implicit tags "Head Revision" and "Running".

Comment (Optional) text box—Type a descriptive comment about the audit operation you want to run.

Select Time or Save Operation section:

- Now check box—Select to have an audit operation occur as soon as the command is executed. Click the Now option button.
- Save Operation as text box—Type a name for the audit operation that you want to save. The saved audit operation appears in the Saved Operations page with the name that you gave it. To view the Saved Operations page, click Settings > Saved Operations.
- Select Schedule check box and table—Select a particular schedule for an audit operation. Click the Selected Schedule check box, then select a schedule from the schedule table. The schedule table lists the available schedules added for JUNOScope software operations by schedule name, start time, period or interval, and comment.

Compare button—Audits the selected configurations. The Confirm Selections dialog box from which you can confirm the selections is displayed.

Cancel button—Clears this dialog box and redisplays the Configuration > Repository menu.

Audit Partial Configurations—Confirm Selections Dialog Box

Description Use the Confirm Selections dialog box to confirm that the selections you made are correct.

Navigation Click Configuration > Repository > Audit > Audit Partial Configurations. Select the imported configuration file (baseline configlet) from the Select Partial Configuration dialog box and click Next. Select the devices, and schedule a time to audit the selected partial configurations from the Use the Select Devices and Time dialog box and click Next.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the partial configuration you selected, the devices or group from which the audit operation will be performed, and the schedule for your confirmation.

Finish button—Executes the operation. The Status—View Status Records dialog box appears displaying the status of the audit configurations operation. If there is a difference between the configurations that you selected to audit, a Click to view the audit result link appears in the Message column of the table for you to compare the different configuration revisions.

Previous button—Displays the previous Select Devices and Time dialog box and does not execute the operation.

Cancel button—Clears this dialog box and displays the Audit dialog box.

Audit Partial Configurations—Select Devices and Time Dialog Box

Description Use the Select Devices and Time dialog box to select a device or devices, and schedule a time to audit the selected partial configurations.

Navigation Click Configuration > Repository > Audit > Audit Partial Configurations. Select the imported configuration file (baseline configlet) in the Select Partial Configuration dialog box and click Next.

Permissions Superuser, read-write

Elements Group check box and drop-down list box—Select a device group on which to audit partial configurations. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any device groups, the Groups drop-down list box is empty.

Select Device(s) check box and drop-down list box—Select a device or devices from which to audit partial configurations. Click the Devices option button, then click the Devices drop-down list box to display the availabledevices added for JUNOScope software operations. If you have not added any devices, the Select Device(s) drop-down list box is empty.

Comment (Optional) text box—Type a descriptive comment about the audit operation you want to run.

Select Time or Save Operation section:

- Now check box—Select to have an audit operation occur as soon as the command is executed. Click the Now option button.
- Save Operation as text box—Type a name for the audit operation that you want to save. The saved audit operation appears in the Saved Operations page with the name that you gave it. To view the Saved Operations page, click Settings > Saved Operations.
- Select Schedule check box and table—Select a particular schedule for an audit operation. Click the Selected Schedule check box, then select a schedule from the schedule table. The schedule table lists the available schedules added for JUNOScope software operations by schedule name, start time, period or interval, and comment.

Next button—Displays the Confirm Selections dialog box.

Previous button—Displays the previous Select Partial Configuration dialog box.

Cancel button—Clears this dialog box and displays the Audit dialog box.

Audit Partial Configurations—Partial Configuration Audit Result Dialog Box

Description Use the Partial Configuration Audit Result Dialog Box to view the differences between a part of the running configuration file and a baseline configlet. You can view the differences in Colored Diff and Unidiff output formats.

Navigation Click Configuration > Repository > Audit > Audit Partial Configurations. Select the imported configuration file (baseline configlet) from the Select Partial Configuration dialog box and click Next. Select the devices, and schedule a time to audit the selected partial configurations from the Use the Select Devices and Time dialog box and click Next. Confirm that the selections you made are correct and click Next in the Confirm Selections dialog box.

Permissions Superuser, read-write

Elements Audit result using Partial Config 'X' on device 'Y' display field—Displays the differences between a part of the running configuration file and the baseline configlet. By default, the baseline configlet is compared to the corresponding part of the running configuration.

View type drop-down list box—Displays the view formats—Colored Diff and Unidiff—so you can change to a different display format. Colored Diff displays differences in configuration in color. Unidiff includes a minus sign (-) that represents a difference in one revision of the configuration file and a plus sign (+) that represents a difference in the other.

Audit Partial Configurations—Select Partial Configuration Dialog Box

Description Use the Select Partial Configuration dialog box to select the imported configuration file (baseline configlet) that you want to compare with a running configuration on the device.

Navigation Click Configuration > Repository > Audit > Audit Partial Configurations.

Permissions Superuser, read-write

Elements Imported Configuration Files drop-down list box—Select the imported configurtion file (baseline configlet) that you want to compare with a running partial configuration.

Imported Configuration Versions table—Select the imported configuration file revsion you want to compare with a running partial configuration by selecting the check box in the corresponding row in the Imported Configuration Versions table.

Next button—Displays the Select Devices and Time dialog box

Cancel button—Clears this dialog box and displays the Audit dialog box.

Authentication Information Dialog Box

Description Use the Authentication Information dialog box to view and change the valid username and password that is configured on a router to which you want to connect the JUNOScope software. The authentication information is listed by name, username, and access method.

Navigation Click Settings > Authentication Information.

Permissions Superuser

Elements Authentication Information table—Displays the authentication information for a valid username and password that is configured on a router to which you want to connect the JUNOScope software. The information is listed by authentication information name, username, and access method. Select an Authentication Information item to edit or delete.

Export Data Encryption Format options—Select one of the following ways to export authentication information from the JUNOScope software:

- Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
- Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export authentication information to another system.
- Export sensitive data unencrypted—Sensitive data is not encrypted at export.

Add button—Displays the Add Authentication Information dialog box from which you can add new authentication information, such as a valid username and password that are configured on a router to which you want to connect the JUNOScope software.

Edit button—Displays the Edit Authentication Information dialog box from which you can edit existing authentication information, such as a valid username and password that are configured on a router to which you want to connect the JUNOScope software. Select an authentication information entry to edit.

Delete button—Deletes a selected authentication information entry from the Authentication Information table. You cannot delete authentication information that is currently being used by an access method. You must first delete the access method, then delete the authentication information. You cannot delete an access method if it is currently being used by a device. You must first delete the device, then delete the access method. Select an authentication information entry to delete.

Export button—Displays the File Download dialog box to export the setup data in XML file format to the file system. The default authentication information export filename is junoscope-access-methods.xml.

Import button—Displays the Import dialog box for you to specify the XML file to import.

Authentication Information—Add Authentication Information Dialog Box

Description Use the Add Authentication Information dialog box to add the information a user needs for access to a router from the JUNOScope software. The required authentication information includes an authentication name for the JUNOScope software and a user login name and password that are configured on the router at the JUNOS software [edit system login] hierarchy level.

Navigation Click Settings > Authentication Information. Click Add in the Authentication Information dialog box.

Permissions Superuser

Elements Authentication Information Name text box—Type a unique name for the authentication information that you want to use in the JUNOScope software. This is the name that displays in the Add Access Method dialog box and the Authentication Information drop-down list box.

Username text box—Type a user login name that is configured on the router to which you want to connect. This must be the username of a valid user on the router.

Password text box—Type a user password that is configured on the router to which you want to connect. This must be the password of a valid user on the router.

Confirm Password text box—Retype the user password to confirm it.

OK button—Displays the Authentication Information dialog box with the new authentication information displayed.

Cancel button—Clears this dialog box without adding any new authentication information.

Authentication Information—Edit Authentication Information Dialog Box

Description Use the Edit Authentication dialog box to edit the information a user needs in order to access a router from the JUNOScope software. The required authentication information includes an authentication name for the JUNOScope software and a user login name and password that are configured on the router at the JUNOS software [edit system login] hierarchy level.

Navigation Click Settings > Authentication Information. Select the authentication information that you want to edit in the Authentication Information dialog box, and click Edit.

Permissions Superuser

Elements Authentication Information Name text box—Type a unique name for the authentication information that you want to use in the JUNOScope software. This is the name that displays in the Add Access Method dialog box and the Authentication Information drop-down list box.

Username text box—Type a user login name that is configured on the router to which you want to connect. This must be the username of a valid user on the router.

Password text box—Type a user password that is configured on the router to which you want to connect. This must be the password of a valid user on the router.

Confirm Password text box—Retype the user password to confirm it.

OK button—Displays the Authentication Information dialog box with the new authentication information that you added.

Cancel button—Clears this dialog box without adding any new authentication information.

Authentication Information—Import Authentication Information Dialog Box

Description Use the Import Authentication Information dialog box to import authentication setup information into the JUNOScope software without having to manually enter it. The default import filename for authentication information is junoscope-access.xml.

Navigation Click Settings > Authentication Information. Click Import in the Authentication Information dialog box.

Permissions Superuser

Elements File to import text box—Lets you type or browse to the access method XML file to import.

Key (if not included in data) text box—Type the key to decrypt the sensitive data that you want to import. The key is required if you selected not to include it when the data was exported. This key can be up to 16 characters long and is created during the JUNOScope installation.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Browse button—Displays the File Open dialog box for you to select the XML file to import.

Import button—Imports the selected authentication information data into the JUNOScope software and displays the Import Result dialog box.

Cancel button—Clears this dialog box and displays the Authentication Information dialog box.

Compare—Select Configurations Dialog Box

Description Use the Compare—Select Configurations dialog box to select two configuration file revisions to compare. By default, the Compare command compares a newer revision of a configuration with an older one, but you can select to have an older configuration file revision compared with a newer one.

Navigation Click Configuration > Repository > Compare. Select a device from which to compare configurations, or select an imported configuration filename and click Next.

Permissions Superuser, read-write

Elements Select Two Revisions to Compare table—Lists the configuration file revisions that have been stored in the JUNOScope CVS repository for a device or imported configuration filename. The table lists the archived revisions by date, revision, and comment.

Swap revisions (Compare older selected revision to newer?) check box—Select this check box to have the JUNOScope software compare an older configuration file revision to a newer one.

Compare Output Type drop-down list box—Select the way you want to view differences between configuration revisions: Colored Diff or Unidiff. Colored Diff displays differences in configuration revisions in color. Unidiff includes a minus sign (-) that represents a difference in one revision of the configuration file and a plus sign (+) that represents a difference in the other.

Previous button—Redisplays the Compare—Select Options dialog box for you to select a device from which to compare configuration revisions or an imported configuration filename for which to compare configuration revisions.

Next button—Displays the Compare—View Differences dialog box from which you can view the differences between the two configuration file revisions.

Cancel button—Clears this dialog box and redisplays the Configuration > Repository menu.

Compare—Select Options Dialog Box

Description Use the Compare—Select Options dialog box to select a device for which to compare two configuration file revisions or to select an imported configuration filename for which to compare two revisions. By default, the Compare Archive command compares a newer configuration file revision with an older one, but you can select to have an older configuration file compared to a newer one.

Navigation Click Configuration > Repository > Compare.

Permissions Superuser, read-write, read-only

Elements Configuration File drop-down list box—Archived Configuration is the default selection when you want to compare two device configuration files. Use this drop-down list box to select an imported configuration filename for which to compare two revisions. Click the down arrow to display a list of available filenames of configurations imported into the JUNOScope CVS repository. If you select an imported configuration filename, the Device drop-down list box is disabled.

Device drop-down list box—Select the device for which you want to compare two configuration files. Click the down arrow to display a list of available routers. If you select an imported configuration filename in the Configuration File drop-down list box, this list box is disabled.

Next button—Displays the Compare—Select Configurations dialog box from which you can select two configuration files to compare.

Cancel button—Clears this dialog box, and redisplays the Configuration > Repository menu.

Compare—View Differences Dialog Box

Description Use the Compare—View Differences dialog box to view the differences between configuration file revisions that have been stored in the JUNOScope software CVS repository. You can compare configuration revisions in Colored Diff and Unidiff output formats.

Navigation Click Configuration > Repository > Compare. Select the device from which you want to compare configurations or an imported configuration filename in the Compare—Select Options dialog box, and click Next. Select the two configurations you want to compare in the Compare—Select Configurations dialog box, and click Finish.

Permissions Superuser, read-write

Elements Configuration Compare of Revision X to Revision X on Device Name display field—Displays the differences between the two compared configuration file revisions. Displays the configuration revision level (for both archived and imported configuration files) and the device from which the configurations were archived (for archived configurations only).

By default, the Compare Archive command compares the newer revision to the older one, but you can select to have the JUNOScope software compare an older configuration file revision to a newer one.

Compare output type drop-down list box—Displays the compare formats—Colored Diff and Unidiff—so you can change to a different display format. Colored Diff displays differences in configuration revisions in color. Unidiff includes a minus sign (-) that represents a difference in one revision of the configuration file and a plus sign (+) that represents a difference in the other.

OK button—Displays the Compare—Select Configurations dialog box.

Configure LSP Paths Dialog Box

Description Use the Configure LSP Paths dialog box to add/delete/export/import LSP paths which will be used in creating MPLS/GRE tunnels.

Navigation Click Provisioning > MPSL/GRE Tunnels > Configure LSP Paths.

Permissions Superuser

Elements The table at the top of this dialog box lists the LSP paths existing in the system, with the following information:

- Name—Name of the LSP path
- Device—Device on which the LSP path is configured.
- State—Whether committed to the device or not.
- Comment—Descriptive comment.

Delete button—Select one or more LSP paths and click delete to delete them.

Add button—Click Add to go to the Add a New LSP Path dialog box.

Export button—Click this to export all LSP paths as an XML file.

Import button—Click this to import LSP Paths existing in an XML file.

Configure LSP Paths— Import LSP Paths Dialog Box

Description Use the Import LSP Paths dialog box to import LSP path details into the JUNOScope software without having to manually enter it.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure LSP Paths. Click Import in the Configure LSP Paths dialog box.

Permissions Superuser, read-write

Elements File text box— Lets you type or select the XML file you want to import.

Browse... button— Displays the File Open dialog box where you can select the XML file you want to import.

Import Options— Select the method to be used if a conflict occurs between the existing record stored in the JUNOScope server and the imported record. Select one of the following options:

- Ignore— (Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Import button—Imports the selected record into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears the Import LSP Paths dialog box and displays the Configure LSP Paths dialog box.

Configure LSP Paths—Add a New LSP Path Dialog Box

Description Use the Configure LSP Paths — Add a New LSP Path dialog box to add LSP paths which will be used in creating MPLS/GRE tunnels.

Navigation Click Provisioning > MPSL/GRE Tunnels > Configure LSP Paths, and then click Add.

Permissions Superuser

Elements Device Name drop-down list box—Displays the device names from which you can select one on which to add an LSP Path.

Name—Enter the name of the LSP path.

Comment—Enter a comment on the LSP path.

Enter a Node—Enter node information (IP addresses and adjacency) of the LSP path.

- Enter IP Address—Enter the IP address of the node.
- Strict/Loose adjacency—Select from the drop-down list whether the node is to follow strict or loose adjacency.

Add button—Click this button to add the node to the LSP path.

Next Hop—Displays the nodes you have added.

Remove button—Select a node and click Remove to remove that node from the LSP path.

Remove All button—Click Remove All to remove all nodes from the LSP path.

Move Up button—Select a node and click Move Up to move it up in the path.

Move Down button—Seclect a node and click Move Down to move it down in the path.

Save button—Saves the LSP path you have added.

Reset button—Resets the information you have entered.

Cancel button—Takes you to the previous dialog box (Configure LSP Paths).

Configure LSP Paths—Edit Details Of LSP Path Dialog Box

Description Use the Configure LSP Paths — Edit Details of LSP Path dialog box to modify details of LSP paths which will be used in creating MPLS/GRE tunnels.

Navigation Click Provisioning > MPSL/GRE Tunnels > Configure LSP Paths, and then click the LSP path name.

Permissions Superuser

Elements Device Name—Display only.

Name—Display only.

Comment—Enter a comment on the LSP path.

Enter a Node—Enter node information (IP addresses and adjacency) of the LSP path.

- Enter IP Address—Enter the IP address of the node.
- Strict/Loose adjacency—Select from the drop-down list whether the node is to follow strict or loose adjacency.

Add button—Click this button to add the node to the LSP path.

Next Hop—Displays the nodes you have added.

Remove button—Select a node and click Remove to remove that node from the LSP path.

Remove All button—Click Remove All to remove all nodes from the LSP path.

Move Up button—Select a node and click Move Up to move it up in the path.

Move Down button—Seclect a node and click Move Down to move it down in the path.

Save button—Saves the LSP path you have added.

Reset button—Resets the information you have entered.

Cancel button—Takes you to the previous dialog box (Configure LSP Paths).

Configure Protocols Dialog Box

Description Use the Configure Protocols dialog box to select a device on which to configure the protocol and the protocol to be configured.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols.

Permissions Superuser

Elements Device Name drop-down list box—Select a device on which you wish to configure the protocol.

Protocol drop-down list box—Select the protocol you wish to configure on the selected device.

Open button—Click this button to display the parameters of the selected protocol.

Export button—Click this to export the protocol configurations as an XML file.

Import button—Click this to import already exported protocol configurations from an XML file.

Configure Protocols— Import Protocol Details Dialog Box

Description Use the Import Protocols Details dialog box to import protocol details into the JUNOScope software without having to manually enter it.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols. Click Import in the Configure Protocols dialog box.

Permissions Superuser, read-write

Elements File text box— Lets you type or select the XML file you want to import.

Browse... button— Displays the File Open dialog box where you can select the XML file you want to import.

Import Options— Select the method to be used if a conflict occurs between the existing record stored in the JUNOScope server and the imported record. Select one of the following options:

- Ignore— (Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Import button—Imports the selected record into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears the Import Protocol Details dialog box and displays the Configure Protocols dialog box.

Configure Protocols (INET) Dialog Box

Description Use the Configure Protocols dialog box to configure protocols on devices for provisioning pseudowires.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols, then select INET from the Protocols drop-down list and click Open.

Permissions Superuser

Elements Device Name drop-down list box—Select the device on which you wish to configure the protocol.

Protocol drop-down list box—Select the prtocol (INET) and click Open.

Export button—Click this button to export the protocol in XML format.

Import button—Click this button to import protocols already configured and saved in XML format.

Enter Details for Protocol—Enter the details for the protocol:

- Select Interface—Select the interface(s) for the protocol. To select multiple protocols, press Shift and click the interfaces.
- Logical Unit—Enter the logical unit of the protocol.
- IP Address—Enter the IP address for the interface(s).
- Mask—Enter the IP address mask.

Add button—Click this button to add protocol details.

Details of Protocol on Interface—Displays the details you have added.

Remove button—Select an interface and click Remove to remove that interface's association with the protocol.

Remove All button—Click this button to remove all associations.

Save button—Click this button to save the details you have specified for the INET protocol.

Configure Protocols (ISIS) Dialog Box

Description Use the Configure Protocols dialog box to configure protocols on devices for provisioning pseudowires.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols, then select ISIS from the Protocols drop-down list and click Open.

Permissions Superuser

Elements Device Name drop-down list box—Select the device on which you wish to configure the protocol.

Protocol drop-down list box—Select the prtocol (LDP) and click Open.

Export button—Click this button to export the protocol in XML format.

Import button—Click this button to import protocols already configured and saved in XML format.

Enter Details for Protocol—Enter the details for the protocol:

- Enable on all Interfaces check box—Select this check box to enable the protocol on all interfaces.
- Select Interface—Select the interface(s) for the protocol. To select multiple protocols, press Shift and click the interfaces.
- Logical Unit—Enter the logical unit of the protocol.
- Disable—Select this check box if you wish to disable the interface.

Level drop-down list box—Select the level from the drop-down list box.

Add button—Click this button to add protocol details.

Details of Protocol on Interface—Displays the details you have added.

Remove button—Select an interface and click Remove to remove that interface's association with the protocol.

Remove All button—Click this button to remove all associations.

Save button—Click this button to save the details you have specified for the LDP protocol.

Configure Protocols (LDP) Dialog Box

Description Use the Configure Protocols dialog box to configure protocols on devices for provisioning pseudowires.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols, then select LDP from the Protocols drop-down list and click Open.

Permissions Superuser

Elements Device Name drop-down list box—Select the device on which you wish to configure the protocol.

Protocol drop-down list box—Select the prtocol (LDP) and click Open.

Export button—Click this button to export the protocol in XML format.

Import button—Click this button to import protocols already configured and saved in XML format.

Enter Details for Protocol—Enter the details for the protocol:

- Enable on all Interfaces check box—Select this check box to enable the protocol on all interfaces.
- Select Interface—Select the interface(s) for the protocol. To select multiple protocols, press Shift and click the interfaces.
- Logical Unit—Enter the logical unit of the protocol.
- Disable—Select this check box if you wish to disable the interface.

Add button—Click this button to add protocol details.

Details of Protocol on Interface—Displays the details you have added.

Remove button—Select an interface and click Remove to remove that interface's association with the protocol.

Remove All button—Click this button to remove all associations.

Save button—Click this button to save the details you have specified for the LDP protocol.

Configure Protocols (MPLS) Dialog Box

Description Use the Configure Protocols dialog box to configure protocols on devices for provisioning pseudowires.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols, then select MPLS from the Protocols drop-down list and click Open.

Permissions Superuser

Elements Device Name drop-down list box—Select the device on which you wish to configure the protocol.

Protocol drop-down list box—Select the prtocol (MPLS) and click Open.

Export button—Click this button to export the protocol in XML format.

Import button—Click this button to import protocols already configured and saved in XML format.

Enter Details for Protocol—Enter the details for the protocol:

- Enable on all Interfaces check box—Select this check box to enable the protocol on all interfaces.
- Select Interface—Select the interface(s) for the protocol. To select multiple protocols, press Shift and click the interfaces.
- Logical Unit—Enter the logical unit of the protocol.
- Disable—Select this check box if you wish to disable the interface.

Add button—Click this button to add protocol details.

Details of Protocol on Interface—Displays the details you have added.

Remove button—Select an interface and click Remove to remove that interface's association with the protocol.

Remove All button—Click this button to remove all associations.

Save button—Click this button to save the details you have specified for the MPLS protocol.

Configure Protocols (OSPF) Dialog Box

Description Use the Configure Protocols dialog box to configure protocols on devices for provisioning pseudowires.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols, then select OSPF from the Protocols drop-down list and click Open.

Permissions Superuser

Elements Device Name drop-down list box—Select the device on which you wish to configure the protocol.

Protocol drop-down list box—Select the prtocol (MPLS) and click Open.

Export button—Click this button to export the protocol in XML format.

Import button—Click this button to import protocols already configured and saved in XML format.

Enter Details for Protocol—Enter the details for the protocol:

- Enable on all Interfaces check box—Select this check box to enable the protocol on all interfaces.
- Select Interface—Select the interface(s) for the protocol. To select multiple protocols, press Shift and click the interfaces.
- Logical Unit—Enter the logical unit of the protocol.
- Disable—Select this check box if you wish to disable the interface.

Area—Enter the OSPF area.

Traffic Engineering (TE) check box—Select this check box to enable traffic engineering.

Add button—Click this button to add protocol details.

Details of Protocol on Interface—Displays the details you have added.

Remove button—Select an interface and click Remove to remove that interface's association with the protocol.

Remove All button—Click this button to remove all associations.

Save button—Click this button to save the details you have specified for the OSPF protocol.

Configure Protocols (RSVP) Dialog Box

Description Use the Configure Protocols dialog box to configure protocols on devices for provisioning pseudowires.

Navigation Click Provisioning > MPLS/GRE Tunnels > Configure Protocols, then select RSVP from the Protocols drop-down list and click Open.

Permissions Superuser

Elements Device Name drop-down list box—Select the device on which you wish to configure the protocol.

Protocol drop-down list box—Select the prtocol (RSVP) and click Open.

Export button—Click this button to export the protocol in XML format.

Import button—Click this button to import protocols already configured and saved in XML format.

Enter Details for Protocol—Enter the details for the protocol:

- Enable on all Interfaces check box—Select this check box to enable the protocol on all interfaces.
- Select Interface—Select the interface(s) for the protocol. To select multiple protocols, press Shift and click the interfaces.
- Logical Unit—Enter the logical unit of the protocol.
- Disable—Select this check box if you wish to disable the interface.

Node Protection (NP) check box—Select this check box to enable node protection.

Link Protection (LP) check box—Select this check box to enable link protection.

Add button—Click this button to add protocol details.

Details of Protocol on Interface—Displays the details you have added.

Remove button—Select an interface and click Remove to remove that interface's association with the protocol.

Remove All button—Click this button to remove all associations.

Save button—Click this button to save the details you have specified for the RSVP protocol.

Configuration File Associations—List of Configuration Associations Dialog Box

Description Use the List of Configuration Associations dialog box to view the list of configuration associations saved in the JUNOScope server. The configuration associations are listed by configuration file name, configuration file version, comment, and the criteria associated with the configuration file. The configuration associations are displayed in the order in which the set of criteria is compared with the device attributes. Use this dialog box to add/edit/reorder/delete/import/export configuration associations.

Navigation Click Configuration > Repository > Config Associations.

Permissions Superuser, read-write

Elements Config Name column— Lists the names of the configuration files used in the configuration association.

Config Version column— Lists the versions of the configuration files.

Comment column— Lists the comments entered while creating the configuration associations.

Criteria column—Lists the criteria of each of the configuration associations.

Delete button—Deletes selected configuration associations.

Add button— Displays the Add New Configuration Association dialog box where you can create a new configuration association.

Reorder button— Displays the Reorder Configuration Associations dialog box where you can change the order of the configuration associations.

Export button—Displays the File Download dialog box to export all the saved configuration associations in XML file format to the file system.

Import button— Displays the Import Config Associations dialog box where you can import configuration associations onto the JUNOScope server.

Configuration File Associations—Add New Configuration Association Dialog Box

Description Use the Add New Configuration Association dialog box to associate a set of criteria with a configuration file that exists in the JUNOScope server. This creates a configuration association. JUNOScope compares the device attributes with the criteria specified in each of these configuration associations. If they match, JUNOScope returns the associated configuration file to the device.

Navigation Click Configuration > Repository > Config Associations. Click Add in the List of Configuration Associations dialog box to open the Add New Configuration Association dialog box where you can create a new configuration file association.

Click Configuration > Repository > Config Associations. Click the Configuration files' name in the Config Name column in the List of Configuration Associations dialog box, to open the Edit Configuration Association dialog box where you can edit the configuration association.

Permissions Superuser, read-write

Elements Imported Configuration Files drop down list—Select the imported configuration file that you want to associate with a set of criteria.

Imported Config Versions table— Select the revision of the configuration file, that you want to associate with a set of criteria, by selecting the check box in the corresponding row in the Imported Configuration Versions table. This table changes when you select a different configuration file. If you select the Latest Revision option, JUNOScope always returns the last revised version of the configuration file i.e. the dynamic latest. This option is selected by default.

Comment text box— Type a brief description about the configuration.

Enter a Criteria column— Select the type of rule you want to set:

- Default—Select this option so that JUNOScope returns a default configuration file if none of the device attributes match the criteria in any of the configuration associations. You cannot associate any criteria with a configuration file that has been designated as the default configuration association.

NOTE: This option is not displayed if it was already selected for that configuration file in a previous configuration association.

- Device Attributes—Select this option to set a rule for a specific device parameter.
  - Device Attributes drop down list—Select the device parameter from this list. The options are Hostname, Model, OS Version, and Serial Number.
  - Rule drop down lists— Set a condition for the parameter by selecting a combination of the options from the two lists. The options for the first list are does, and does not. The options for the second list are contain, begin with, end with, and equal.
  - Rule text box— Type a value that the device attribute must match so that this configuration file is returned to the device.
- Device in Group—Select this option so that JUNOScope returns the associated configuration file if the requesting device belongs to the device group that you select from the drop down list.

Action column— Select an option to decide how you want the rules to be combined in the criteria list.

- Logic drop down list—Select one of these two options:
  - Select AND if you want the device to match both the rules that are combined by AND. This is the default selection.
  - Select OR if you want the device to match one of the rules that are combined by OR.
- Add button—Click to combine the rules using the option that you have selected in Logic drop down list, and to display the rules in the Criteria List.

Criteria List column—Displays the set of criteria.

Move Up button—Moves the selected rule in the Criteria List to one row above its current position.

Move Down button—Moves the selected rule in the Criteria List to one row below its current position.

Remove button—Removes the selected rule in the Criteria List from the criteria list.

Remove All button—Clears the Criteria List column.

Save button—Saves the configuration file association and displays the List of Configuration Association dialog box.

Reset button—Restores all the field values to their default value.

Cancel button—Clears this dialog box and displays the List of Configuration Associations dialog box.

Configuration File Associations—Edit Configuration Association Dialog Box

Description Use the Edit Configuration Association dialog box to edit an existing configuration association.

Navigation Click Configuration > Repository > Config Associations. Click the Configuration file name hyperlink in the Config Name column in the List of Configuration Associations dialog box, to open the Edit Configuration Association dialog box where you can edit the configuration association.

Permissions Superuser, read-write

Elements Imported Configuration Files drop down list—Select the imported configuration file that you want to associate with a set of criteria.

Imported Config Versions table— Select the revision of the configuration file, that you want to associate with a set of criteria, by selecting the check box in the corresponding row in the Imported Configuration Versions table. This table changes when you select a different configuration file. If you select the Latest Revision option, JUNOScope always returns the last revised version of the configuration file i.e. the dynamic latest. This option is selected by default.

Comment text box— Type a brief description about the configuration.

Enter a Criteria column— Select the type of rule you want to set:

- Default—Select this option so that JUNOScope returns a default configuration file if none of the device attributes match the criteria in any of the configuration associations. You cannot associate any criteria with a configuration file that has been designated as the default configuration association.

NOTE: This option is not displayed if it was already selected for that configuration file in a previous configuration association.

- Device Attributes—Select this option to set a rule for a specific device parameter.
  - Device Attributes drop down list—Select the device parameter from this list. The options are Hostname, Model, OS Version, and Serial Number.
  - Rule drop down lists— Set a condition for the parameter by selecting a combination of the options from the two lists. The options for the first list are does, and does not. The options for the second list are contain, begin with, end with, and equal.
  - Rule text box— Type a value that the device attribute must match so that this configuration file is returned to the device.
- Device in Group—Select this option so that JUNOScope returns the associated configuration file if the requesting device belongs to the device group that you select from the drop down list.

Action column— Select an option to decide how you want the rules to be combined in the criteria list.

- Logic drop down list—Select one of these two options:
  - Select AND if you want the device to match both the rules that are combined by AND. This is the default selection.
  - Select OR if you want the device to match one of the rules that are combined by OR.
- Add button—Click to combine the rules using the option that you have selected in Logic drop down list, and to display the rules in the Criteria List.

Criteria List column—Displays the set of criteria.

Move Up button—Moves the selected rule in the Criteria List to one row above its current position.

Move Down button—Moves the selected rule in the Criteria List to one row below its current position.

Remove button—Removes the selected rule in the Criteria List from the criteria list.

Remove All button—Clears the Criteria List column.

Save button—Saves the configuration file association and displays the List of Configuration Association dialog box.

Reset button—Restores the field values back to the last saved values of that configuration association.

Cancel button—Clears this dialog box and displays the List of Configuration Associations dialog box.

Configuration File Associations—Reorder Configuration Associations Dialog Box

Description Use the Reorder Configuration Associations dialog box to change the order in which the configuration associations are listed in the JUNOScope server. JUNOScope starts comparing the device attributes with the criteria of the configuration associations at the top of the list. You can select the order in which the criteria are checked by using this dialog box.

Navigation Click Configuration > Repository > Config Associations. Click Reorder in the List of Configuration Associations dialog box.

Permissions Superuser, read-write

Elements Return Latest Archived Config— Select to return the latest configuration file that was archived in JUNOScope for that device. This option is selected by default. When the device sends a request, JUNOScope returns the latest configuration file that is archived in the server for that device. If JUNOScope doesn't have a configuration file archived for that device, then it starts comparing the device attributes with the criteria.

Config Name column— Lists the names of the configuration files in the configuration association.

Config Version column— Lists the versions of the configuration files.

Comment column— Lists the comments entered while creating the configuration associations.

Criteria column—Lists the criteria of each of the configuration association.

Move Up button—Moves the selected row to one row above its current position.

Move Down button—Moves the selected row to one row below its current position.

Move First button—Moves the selected row to the top of the list of configuration associations

Move Last button—Moves the selected row to the bottom of the list of configuration associations.

Save button— Saves the order of configuration associations and displays the List of Configuration Association dialog box.

Reset button— Restores the order of the configuration associations to the last saved order.

Cancel button— Clears this dialog box and displays the List of Configuration Associations dialog box.

Configuration File Associations—Import Config Associations Dialog Box

Description Use the Import Config Associations dialog box to import configuration associations into the JUNOScope software without having to manually enter it.

Navigation Click Configuration > Repository > Config Associations. Click Import in the List of Configuration Associations dialog box.

Permissions Superuser, read-write

Elements File text box— Lets you type or select the XML file you want to import.

Browse... button— Displays the File Open dialog box where you can select the XML file you want to import.

Import Options— Select the method to be used if a conflict occurs between the existing configuration files stored in the JUNOScope server and the imported configuration files. Select one of the following options:

- Ignore—This option is not supported by the configuration association feature.
- Merge—This option is not supported by the configuration association feature.
- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Import button—Imports the selected configuration file into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears the Import Config Association dialog box and displays the List of Configuration Associations dialog box.

Configuration—Current—View—View Current Configuration Dialog Box

Description Use the View Current Configuration dialog box to select the router for which you want to view the configuration.

Navigation Click Configuration > Current > View.

Permissions Superuser, read-write, read-only

Elements Device drop-down list box —Select the router for which you want to view the configuration.

Next button—Displays the Configuration Browser dialog box.

Configuration—Current—Edit—Edit Current Configuration Dialog Box

Description Use the Edit Current Configuration dialog box to select the router for which you want to edit the configuration.

Navigation Click Configuration > Current > Edit.

Permissions Superuser, read-write

Elements Device drop-down list box—Select the router for which you want to edit the configuration.

Next button—Displays the Configuration Editor dialog box.

Configuration—Current—View—Configuration Browser Dialog Box

Description Use the Configuration Browser to view the contents of the committed configuration from a selected device.

Navigation Click Configuration > Current > View. Select a device and click Next in the Configuration Browser—View Current Configuration dialog box.

Permissions Superuser, read-write, read-only

Elements Navigation pane—Displays the statement hierarchy levels of the configuration that have been configured. Provides an expanding and collapsing tree view of the configuration for a selected router. Click Hide All to collapse the configuration statement hierarchy levels to the top. Click a statement hierarchy level or [+] to view its configured substatements. Click Expand All to view all levels of the configuration.

Configuration view pane—Displays the current level of the configuration statement hierarchy. Displays the configuration container and leaf statements. Container statements contain other statements. Leaf statements do not contain other statements. Click a container statement link to view its contents.

Command buttons—Controls the statement hierarchy view:

- Brief button—The default view, displays the basic hierarchy configuration. Only configured statements are displayed.
- Inheritance button—Shows statements at the level at which they are inherited
- Refresh button—Displays the current committed configuration.
- Edit button—Displays the configuration in the Configuration Editor for you to edit it.

  The Brief and Inheritance views remain in effect until you click another button.

Icon legend—Describes the icons that appear in the configuration view:

- [c]—The configuration statement has a comment. Place the mouse cursor over the icon to display the comment.
- [I]—The configuration statement and the configuration below this level are inactive.
- [*]—Enter a value for the configuration statement.
- [?]—Displays help for a configuration statement value.

Configuration—Current—View—Configuration Editor Dialog Box

Description Use the Configuration Editor dialog box to edit the contents of the committed configuration from a selected device.

Navigation Click Configuration > Current > Edit. Select a device and click Next in the Edit Current Configuration dialog box.

Permissions Superuser, read-write

Elements Navigation pane — Displays the statement hierarchy levels of the configuration that have been configured. Provides an expanding and collapsing tree view of the configuration for a selected router. Click a statement hierarchy level or [+] to view its configured substatements. Click Expand All to view all levels of the configuration. Click Hide All to collapse the configuration statement hierarchy levels to the top.

Configuration view pane—Displays the current level of the configuration statement hierarchy. Displays the configuration container and leaf statements. Container statements contain other statements. Leaf statements do not contain other statements. Displays data for the current level of configuration. Click Edit to modify that configuration statement and any nested statements. The word Configure appears if a configuration statement has not been modified. Click Configure to edit the configuration of that statement and any nested statements.

Command buttons—Contains the buttons that control the view in the statement/hierarchy view:

- OK—Saves changes and takes you to the parent statement level. Changes are kept local to the JUNOScope server until you click Commit.
- Cancel—Discards any edits that you've made and takes you to the parent statement level.
- Apply—Saves the changes you've made in the current window, but does not exit that window. You can make more changes and apply or cancel them. Apply does not change the configuration running on the router. Changes are kept local to the JUNOScope server until you click Commit.
- Refresh button—Refreshes the cached configuration with the currently committed configuration. Your changes are maintained and continue to be displayed.
- Commit—Displays a review screen that displaces the set of changes and prompts you to continue. If you confirm to continue, the configuration is checked for syntax errors, activated, and made operational on the selected router.
- Discard—Displays a dialog box from which you can choose to discard changes below the current level in the configuration, discard all changes, or delete the configuration below the current level.

Icon legend—Describes the icons that appear in the configuration items:

- [c]—The configuration statement has a comment. Place the mouse cursor over the icon to display the comment.
- [I]—The configuration statement and the configurations below this level are inactive.
- [M]—The configuration statement has been edited.
- *—The configuration statement requires a mandatory value.

Delete—Confirm Deletion Dialog Box

Description Use the Confirm Deletion dialog box to confirm the selections for deletion are correct.

Navigation Click Configuration > Repository > Delete. Select the configuration files you want to delete in the Select Files dialog box and click Next.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the configuration files that will be deleted permanently from the CVS Repository.

OK button—Executes the operation. The Select Files dialog box appears with the deleted configuration file removed from the list of configuration files.

Previous button—Redisplays the Select Files dialog box.

Cancel button—Clears this dialog box and displays the Configuration repository dialog box.

Delete—Select Files Dialog Box

Description Use the Select Files dialog box to select an imported configuration file that you want to delete.

Navigation Click Configuration > Repository > Delete.

Permissions Superuser, read-write

Elements Name column—Lists the imported configuration files in the CVS repository.

Cancel button—Clears this dialog box and displays the Configuration Repository dialog box.

Next button—Display the Confirm Deletion dialog box.

Devices Dialog Box

Description Use the Devices dialog box to connect the JUNOScope software to routers on the network. The Devices dialog box is empty until you add routers. The Devices dialog box lists the added routers by device name, DNS name or IP address, access method, model number, location and comment.

We recommend that you set up authentication information and access methods before setting up routers or devices.

Navigation Click Settings > Devices.

Permissions Superuser

Elements Devices table—Lists the devices added to the JUNOScope software by device name, DNS name or IP address, access method, model number, and comment. You can sort devices data by table column name in ascending or descending order by clicking the table column name

Add button—Displays the Add Device dialog box so you can add a new router for JUNOScope software operations.

Copy button—Copies the selected device in the JUNOScope database. A 1 (one) appears after the copied device and increments sequentially each time you copy the same device. Select a device to copy.

Edit button—Displays the Edit Device dialog box so you can edit router information. Select a device to edit.

Delete button—Deletes a selected router or routers from the devices table. Select a device to delete.

Export button—Displays the File Download dialog box to export the setup data in XML file format to the file system. The default device export filename is junoscope-devices.xml.

Import button—Displays the Import dialog box for you to specify the import XML file to import.

Devices—Add Device Dialog Box

Description Use the Add Device dialog box to add supported Juniper Networks routing platforms for JUNOScope software operations.

Navigation Click Settings > Devices. Click Add in the Devices dialog box.

Permissions Superuser

Elements DNS Name or IP Address text box—Type a Domain Name System (DNS) name or IP address for the router you want to add.

Access Method drop-down list box—Select the remote access method for connecting to the router's JUNOScript server. Click the down arrow to display the available access methods: SSL, clear-text, Netconf.

Next button—Displays the Add Device—Verify Device Information dialog box to confirm that JUNOScope has connect to the specified device.

Cancel button—Clears this dialog box, and redisplays the Devices dialog box.

Devices—Edit Device Dialog Box

Description Use the Edit Device dialog box to edit router information stored in the database. You can edit the router name, Domain Name System (DNS) name or IP address, access method, model, location and comment.

Navigation Click Settings > Devices. Select the device that you want to edit in the Devices dialog box, and click Edit.

Permissions Superuser

Elements Device Name text box—Type a name for the router for the JUNOScope software. The router name must be 40 characters or less.

DNS Name or IP Address text box—Type a DNS name or IP address for the router you want to add.

Access Method drop-down list box—Select the remote access method (SSL or clear-text) for connecting to the router. Click the down arrow to display the available options.

Model drop-down list box—Select the router model. Click the down arrow to display the available device model options.

Location text box—Type the location of the device. This is an optional field.

Labels check boxes—Lists existing labels by category in the bottom area of the dialog box. All labels with no specified category are displayed under the category Miscellaneous. Click one or more label check boxes to associate the device with an existing label. A label is used to statically group multiple devices so that JUNOScope operations, such as archive and inventory scan, can be performed on them. You create labels using the Settings > Labels command. If no labels are configured, no labels are listed in this dialog box.

Comment text box—Type an optional descriptive comment about the router that you want to add. The comment must be 40 characters or less.

OK button—Adds the edited router information to the JUNOScope software database. The router is listed in the Devices dialog box.

Cancel button—Clears this dialog box and redisplays the Devices dialog box.

Devices—Edit Device Information Dialog Box

Description Use the Edit Device dialog box to edit router information stored in the database. You can edit the router name, Domain Name System (DNS) name or IP address, access method, model, location and comment.

Navigation Click Settings > Devices. Select the device that you want to edit in the Devices dialog box, and click Edit.

Permissions Superuser

Elements Device Name text box—Type a name for the router for the JUNOScope software. The router name must be 40 characters or less.

DNS Name or IP Address text box—Type a DNS name or IP address for the router you want to add.

Access Method drop-down list box—Select the remote access method (SSL or clear-text) for connecting to the router. Click the down arrow to display the available options.

Model drop-down list box—Select the router model. Click the down arrow to display the available device model options.

Location text box—Type the location of the device. This is an optional field.

Labels check boxes—Lists existing labels by category in the bottom area of the dialog box. Click one or more label check boxes to associate the device with an existing label. A label is used to statically group multiple devices so that JUNOScope operations, such as archive and inventory scan, can be performed on them. You create labels using the Settings > Labels command. If no labels are configured, no labels are listed in this dialog box.

Comment text box—Type an optional descriptive comment about the router that you want to add. The comment must be 40 characters or less.

Labels check boxes—Lists existing labels by category in the bottom area of the dialog box. Click one or more label check boxes to associate the device with an existing label. A label is used to statically group multiple devices so that JUNOScope operations, such as archive and inventory scan, can be performed on them. You create labels using the Settings > Labels command. If no labels are configured, no labels are listed in this dialog box.

OK button—Adds the edited router information to the JUNOScope software database. The router is listed in the Devices dialog box.

Previous button—Displays the previous Add Device dialog box.

Cancel button—Clears this dialog box and redisplays the Devices dialog box.

Devices—Import Devices Dialog Box

Description Use the Import Devices dialog box to import device setup information into the JUNOScope software without having to manually enter it. The default import filename for devices is junoscope-devices.xml.

Navigation Click Settings > Devices. Click Import in the Devices dialog box.

Permissions Superuser

Elements File to import text box—Lets you type or browse to the device XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

Browse button—Displays the File Open dialog box for you to select the XML file to import.

Import button—Imports the selected device data into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears this dialog box and displays the Devices dialog box.

Devices—Verify Device Information Dialog Box

Description Use the Verify Device Information dialog box to view information about the Juniper Networks router to which you want to connect, including hostname, model, JUNOS software and whether JUNOScope supports it, domain name, time zone, and number of installed Routing Engines.

Navigation Click Settings > Devices. Click Add in the Devices dialog box. Enter connection information in the Add Device—Enter Connection Information dialog box, and click Next.

Permissions Superuser

Elements The Device Information Download dialog box discovers and displays the following information about the router:

Hostname—The name of the router on the network.

Model—The router hardware model. The JUNOScope software supports Juniper Networks routing platforms.

JUNOS Internet software—The version of the JUNOS software installed and running on the router and whether the JUNOScope software supports it.

Domain name—A unique name that identifies the router on the network. Domain names always have two or more parts, separated by dots.

Time zone—The time zone within which the router is installed.

Number of Routing Engines—The number of Routing Engines installed in the router. Some router models support two Routing Engines.

Previous button—Displays the previous Add Device dialog box.

Next button—Displays the Add Device dialog box with all information about the device displayed.

Cancel button—Clears this dialog box and displays the Devices dialog box.

Display—Select Configuration Revision Dialog Box

Description Use the Display—Select Configuration Revision dialog box to select a configuration file revision to display. The configuration files are listed by date, revision, and comment. Select a configuration file to display it.

Navigation Click Configuration > Repository > Display. Select the device from which you want to view an archived configuration or an imported configuration filename in the Display—Select Options dialog box, and click Next.

Permissions Superuser, read-write

Elements Configuration table—Displays the configuration files stored in the JUNOScope CVS repository for the selected device or imported configuration filename. The configuration files are listed by date, revision, and comment. Click an archive revision to select it.

Previous button—Displays the previous Display—Select Options dialog box.

Next button—Displays the contents of the configuration file in the Display—View Configuration dialog box.

Cancel button—Clears this dialog box and redisplays the Configuration > Repository menu.

Display—Select Options Dialog Box

Description Use the Display—Select Options dialog box to select a router from which to view an archived configuration file or to select an imported configuration filename to display.

Navigation Click Configuration > Repository > Display.

Permissions Superuser, read-write, read-only

Elements Configuration File drop-down list box—Displays the default Archive Configuration option if you want to display an archived configuration and the filenames of configurations that you have imported into the JUNOScope software. If you select an imported configuration filename, the Device drop-down list box is disabled.

Device drop-down list box—Displays the available devices from which you can select to display an archived configuration file revision. If you select an imported configuration filename in the Configuration File drop-down list box, this drop-down list box is disabled.

Next button—Displays the Display—Select Configuration Revision dialog box from which you can select a configuration to display.

Cancel button—Clears this dialog box and redisplays the Configuration > Repository menu.

Display—View Configuration Dialog Box

Description Use the Display—View Configuration dialog box to view the contents of a selected configuration file.

Navigation Click Configuration > Repository > Display. Select a device from which to view an archived configuration or select the filename of an imported configuration file in the Display—Select Device dialog box, and click Next.

Permissions Superuser, read-write

Elements Configuration Revision X.X display box—Displays the read-only contents of the selected configuration file revision. Displays the configuration revision level (for both archived and imported configuration files) and the device name from which the configuration is displayed (for archived configuration files only).

Previous button—Displays the previous Display—Select Configuration Revisions dialog box from which you can select another configuration file revision to display.

Edit—Configuration Revision Dialog Box

Description Use the Configuration Revision dialog box to edit a configuration file.

Navigation Click Configuration > Repository > Edit. Select a device from which to edit the configuration, or select an imported configuration filename in the Select Options dialog box. Select the configuration revision in the Select Configuration Revision dialog box and click Next.

Permissions Superuser, read-write

Elements Configuration Revision display box—Displays the contents of the archived configuration file that you have selected to edit.

Cancel button—Clears this dialog box and displays the Configuration Repository dialog box.

Save button—Saves modifications to the archived configuration file.

Edit—Save Result Dialog Box

Description Use the Save Result dialog box to confirm whether an edited configuration file has been saved to the JUNOScope CVS repository.

Navigation Click Configuration > Repository > Edit. Select options and click Next in the Select Options dialog box. Select the configuration revision in the Select Configuration Revision dialog box and click Next. Modify the configuration file as required in the Configuration Revision dialog box and click Save.

Permissions Superuser, read-write

Elements Local File display field—Displays the name of the archived configuration file that has been modified.

Action Taken display field—Displays whether the archived configuration file has been modified.

OK button—Displays the Configuration Repository dialog box.

Edit—Select Configuration Revision Dialog Box

Description Use the Select Configuration Revision dialog box to select the revision of the configuration file you want to edit.

Navigation Click Configuration > Repository > Edit. Select Options and click Next in the Select Options dialog box.

Permissions Superuser, read-write

Elements Archived Date column—Lists the dates on which the configuration was archived.

Revision column—Lists the current revision of the configuration.

Comment column—Lists the optional comments entered while archiving the configuration.

Next button—Displays the Configuration Revision dialog box.

Cancel button—Clears this dialog box and displays the Configuration Repository dialog box.

Previous button—Displays the Select Options dialog box.

Edit—Select Options Dialog Box

Description Use the Select Options dialog box to select a configuration file to edit.

Navigation Click Configuration > Repository > Edit.

Permissions Superuser, read-write

Elements Configuration File drop-down list box—Lists the configuration files in the CVS repository.

Device drop-down list box—Lists the device or devices from which the configuration file has been archived.

Next button—Displays the Select Configuration Revision dialog box.

Cancel button—Clears this dialog box and displays the Configuration Repository dialog box.

Export—File Download Dialog Box

Description Use the File Download dialog box to export JUNOScope settings data to a file on the local file system. The dialog box displays the exported filename, file type, and the source hostname.

Navigation

- Authentication Information—Click Settings > Authentication Information, then click Export.
- Access Methods—Click Settings > Access Methods, then click Export.
- Configuration File Associations— Click Configuration > Repository > Config Associations, then click Export.
- Devices—Click Settings > Devices, then click Export.
- Groups—Click Settings > Groups, then click Export.
- Labels—Click Settings >Labels, then click Export.
- Schedules—Click Settings > Schedules, then click Export.
- Local Authentication—Click Settings > Users > Local Authentication, then click Export.
- User Group Authorization—Click Settings > Users > User Group Authorization, then click Export.
- Authentication Policy—Click Settings > Users > Authentication Policy, then click Export.
- Global Authentication Policy—Click Settings > Users > Authentication Policy > Global Authentication Policy, then click Export.
- RADIUS Configuration—Click Settings > RADIUS Configuration, then click Export.
- Import/Export Data—Click Settings > Import/Export Data, then click Export All Data.
- Saved Operations—Click Settings > Saved Operations, then click Export.

Permissions Superuser

Elements Filename display field—The JUNOScope software exports the following setup information to the following files:

File Type display field—The JUNOScope software exports all data in XML file format.

From display field—Displays the JUNOScope software server and domain name to which you are connected.

File Download read-only area—Displays the export data filename, file type, and source hostname.

Open button—Displays the contents of the export XML file.

Save button—Saves the exported setup data in an XML file to the file system.

Cancel button—Closes the File Download dialog box.

More Info button—Displays the system online Help for exporting a file.

Settings Data	Default XML Filename
Access methods	junoscope-access-methods.xml
Authentication information	junoscope-access-methods.xml
Devices	junoscope-devices.xml
Groups	junoscope-groups.xml
Schedules	junoscope-schedules.xml
Labels	junoscope-labels.xml
Users > Local Authentication	junoscope-users.xml
Users > User Group Authorization	junoscope-usergroups.xml
Users > Authentication Policy > User-Specific Authentication Policy	junoscope-auth-policy.xml
Users > Authentication Policy > Global Authentication Policy	junoscope-globalPolicy.xml
RADIUS Configuration	junoscope-radiusClients.xml
Import/Export Data	junoscope-all.xml
Saved Operations	junoscope-operations.xml

Group Members (Criteria Wizard) Dialog Box

Description Use the Group Members dialog box while defining group criteria rules to view the routers that are in the selected router group or groups that you specify.

Navigation Click Settings > Groups. Click Add, Copy, or Edit in the Groups dialog box. Click Criteria Wizard in the Add, Edit, or Copy Group dialog box. Click View Members in the Define Group Membership dialog box.

Permissions Superuser

Elements Group Members displayfield—Displays the routers that are in the selected router group(s).

OK button—Redisplays the Groups dialog box.

Group Members (Groups) Dialog Box

Description Use the Group Members (Groups) dialog box to view the routers that are in a selected router group or groups. You can select one or more groups.

Navigation Click Settings > Groups. Select one or more groups in the Groups dialog box, and click View Members.

Permissions Superuser

Elements Group Members displayfield—Displays the routers that are in the selected router group(s).

OK button—Redisplays the Groups dialog box.

Groups Dialog Box

Description Use the Groups dialog box to view the router groups that have been added for JUNOScope software operations. A group is comprised of routers that are associated by a common property, such as device name, hostname, model number, and comment. The group becomes active when you perform an archive.

The Groups dialog box is empty until you add a group.

Navigation Click Settings > Groups.

Permissions Superuser

Elements Group table—Lists the added router groups by group name, selection criteria, and comment. The group name is the name of the group for the JUNOScope software and must be 20 characters or less. The selection criteria defines how you want the group to be selected or queried from the device information stored in the JUNOScope software database. The comment is a description of the router group and can be any length. Select a group to copy, edit, or delete.

OK button—Redisplays the JUNOScope software main window.

View Members button—Displays the View Members dialog box from which you can view all of the routers that belong to a specified group.

Add button—Displays the Add Group dialog box from which you can add a new router group by typing a group name, defining a rule for selecting the group from the database, and adding a descriptive group comment.

Copy button—Copies the selected group in the JUNOScope database. A 1 (one) appears after the copied group and increments sequentially each time you copy the same group. Select a group to copy.

Edit button—Displays the Edit Group dialog box from which you can edit an existing router group by typing a new name, deleting an existing rule for selecting the group and adding a new one, adding to the existing rule, or typing a new group description. Select a group to edit.

Delete button—Deletes the selected group from the JUNOScope database. Select a group to delete.

Export button—Displays the File Download dialog box to export the setup data in XML file format to the file system. The default devices export filename is junoscope-groups.xml.

Import button—Displays the Import dialog box for you to specify the import XML file to import.

Groups—Add Condition Dialog Box

Description Use the Groups—Add Condition dialog box to define the comparison for selecting the routers in a group from the JUNOScope software database. The Add Group Criteria dialog box displays the previous rule and logic if you have already added a rule for selecting a group. If you have not added a group, the Previous Rule and Logic display text boxes are empty.

Navigation Click Settings > Groups. Click Add in the Groups dialog box. Click Criteria Wizard in the Add Group dialog box. Click Append in the Define Group Membership Criteria dialog box.

Permissions Superuser

Elements Previous Rule display field—Displays the previous rule that you created for selecting routers in a group from the JUNOScope software database. Displays “No previous rule” if you have not created one.

Logic (to previous rule) display field—Displays the logic for adding a new rule to an existing one. The logic can be either AND or OR. Displays “Not Applicable” if you have not added a rule to an existing one.

Comparisons drop-down list box—Select the router property that you want to compare for selecting the routers in a group. Click the down arrow to display the available comparison options: device name, device hostname, model, location,comment, and has Label.

NOTE: Use the has Label Comparison drop-down list box option to use a label as a rule to statically organize a group of devices. Select a label name in the associated drop-down list box.

Text Compare check box and drop-down list boxes—Defines a text rule for the comparison option that you selected. Use text comparisons for text type comparisons, including device name, hostname, model, location and comments.

- First drop-down list box—Defines what you want a text comparison to do. Click the down arrow to display the available options: does and does not.
- Second drop-down list box—Further define what you want a text comparison to do. Click the down arrow to display the available options: contains, begins with, ends with, or equals.
- Text Compare text box—Type the text that you want to compare in the rule.

Numeric Compare check box—Define a numeric rule for the comparison option that you selected. Use numeric compare for numeric type comparisons.

- First drop-down list box—Define what you want a numeric comparison to operate. Click the down arrow to display the available options: is or is not.
- Second drop-down list box—Further define what you want a numeric comparison to do. Click the down arrow to display the available options: greater than, less than, or equal to.
- Numeric Compare text box—Type a numeric value that you want to compare in the rule.

OK button—Adds the rule that you defined and displays the Edit Group Criteria dialog box with that rule listed in the Criteria Rules option button display field.

Cancel button—Clears this dialog box, and redisplays the Edit Group Criteria dialog box.

Groups—Add Group Dialog Box

Description Use the Add Group dialog box to add router groups for JUNOScope software operations. Groups are comprised of routers that are associated by some common factor, such as device name, model, hostname, or comment. A group is a separate entity that has no effect until you associate it with an operation, such as archive.

The Add Group dialog box populates the Groups dialog box with router groups.

Navigation Click Settings > Groups. Click Add in the Groups dialog box.

Permissions Superuser

Elements Group Name text box—Type the name of the router group that you want to add. The group name must be 20 characters or less.

Criteria Rules display field—Displays the selection criteria or rule(s) for selecting routers for a group from the JUNOScope software database. The selection criteria is a database query that you create. The Selection Criteria text box is blank until you add a rule. To add a rule, click Rules Criteria, and complete the selection criteria definition process.

Comment text box—Type an optional descriptive comment about the router group.

OK button—Adds the router group to the table in the Groups dialog box and to the JUNOScope software database. Otherwise, displays an error message telling you to click Rules Criteria to define a rule if you have not already done so.

Criteria Wizard button—Defines the query or rule for selecting routers for a group from the JUNOScope software database. Click Criteria Wizard to display the Edit Group Criteria dialog box.

Cancel button—Clears this dialog box, and redisplays the Groups dialog box.

Groups—Define Group Membership Dialog Box

Description Use the Define Group Membership dialog box to edit the existing router group information in the database, including the group name, selection criteria rule, and group comments.

Navigation Click Settings > Groups. Click Add in the Groups dialog box. Add a group name in the Add Groups dialog box, and click Criteria Wizard.

The Edit Group dialog box appears when you select a router group in the Groups dialog box and click Edit.

Permissions Superuser

Elements Group Name text box—Displays the existing group name. Select the group name and type a new one. The group name must be 20 characters or less.

Criteria Rule display field—Displays the rule for selecting the router group from the JUNOScope software database. To edit the rule, click Criteria Rule. The Edit Group Criteria dialog box appears.

Comment text box—Displays the group comment. Select the group comment and type a new one.

OK button—Adds the edited group information to the JUNOScope software database.

Criteria Wizard button—Lets you edit the group criteria rule and displays the Edit Group Criteria dialog box.

Cancel button—Clears this dialog box and redisplays the Groups dialog box without editing the group information.

Groups—Edit Group Membership Dialog Box

Description Use the Edit Group Membership dialog box to define and edit the rule for selecting a router group from the JUNOScope software database. The Edit Group Criteria dialog box is empty until you define a rule for selecting routers in a router group. If you have already added a rule, the Edit Group dialog box displays the existing rule and lets you provide logic (AND or OR) for adding a new rule and specifying the order of multiple rules.

Navigation Click Settings > Groups. Select a group to edit in the Groups dialog box, and click Edit. Edit the group information in the Edit Group dialog box, and click Criteria Wizard.

Permissions Superuser

Elements Criteria Rules display text box—Displays when you click OK in the Add Group dialog box. Displays the rule that you have defined for selecting a router group from the JUNOScope software database. The Criteria Rules display text box is empty if you have not defined a rule for a router group. In this case, click Append to add a selection rule.

Criteria Rules option button—Displays when you add a rule and click OK from the Add Group Criteria dialog box. Displays an option button and the rule that you defined. Click the button to select the rule and specify the logic for adding another rule. You can also append the selected rule to the end of the new rule, insert it after the selected rule, or insert a new rule before the selected rule.

Logic (if adding a new rule) drop-down list box—Displays when you add a rule and click OK from the Add Group Criteria dialog box. Displays only if you have created a selection rule. Click the down arrow to display the available options: AND or OR.

Exit Criteria Wizard button—Exits the Edit Group Criteria dialog box without adding a new rule and redisplays the Edit Group dialog box.

View Members button—Displays the View Members dialog box which lists the routers associated in a group.

Append button—Adds the selected rule to the end and displays the Add Group Criteria dialog box so you can define another rule for selecting a router group from the JUNOScope software database.

Insert After button—Inserts the new rule after the selected rule. You must select a rule before clicking this button.

Insert Before button—Inserts a new rule before the selected rule. You must select a rule before clicking this button.

Delete button—Deletes the selected rule. You must select a rule before clicking this button.

Cancel button—Clears this dialog box and redisplays the Add Group dialog box without adding a rule.

Groups—Import Groups Dialog Box

Description Use the Import Groups dialog box to import router group setup information into the JUNOScope software without having to manually enter it. The default import filename for groups is junoscope-groups.xml.

Navigation Click Settings > Groups. Click Import in the Groups dialog box.

Permissions Superuser

Elements File to import text box—Lets you type or browse to the device XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

Browse button—Displays the File Open dialog box so you can select the XML file to import.

Import button—Imports the selected device data into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears the Import Groups dialog box and displays the Groups dialog box.

Import/Export Data—Export All Data and Import All Data Dialog Box

Description Use the Export All Data and Import All Data dialog box to export all setup data from the JUNOScope software database to an XML file on the computer file system. The default export all filename is junoscope-all.xml. You can also use this dialog box to Import all settings data from another JUNOScope server. The Export All Data and Import All Data Dialog Box lets you specify the XML filename that you want to import. Click Browse to navigate to the JUNOScope data file that you want to import.

Navigation Click Settings > Import/Export Data.

Permissions Superuser

Elements Export Data Encryption Format options—Select one of the following ways to export all settings information from the JUNOScope software:

- Encrypt sensitive data and provide key at import time—Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import.
- Encrypt sensitive data and include decryption key—Sensitive data is exported encrypted, along with the key needed to decrypt the data. This lets you easily export all settings data to another system.
- Export sensitive data unencrypted—Sensitive data is not encrypted at export.

Export All Data button—Displays the File Download dialog box for exporting all of the JUNOScope software setup data to the file system.

File text box—Lets you type the filename of an XML file that to import. The default files that you can import are as follows:

Settings Data	XML Filename
Access methods	junoscope-access-methods.xml
Authentication information	junoscope-access-methods.xml
Devices	junoscope-devices.xml
Groups	junoscope-groups.xml
Schedules	junoscope-schedules.xml
Labels	junoscope-labels.xml
Users > Local Authentication	junoscope-users.xml
Users > User Group Authorization	junoscope-usergroups.xml
Users > Authentication Policy > User-Specific Authentication Policy	junoscope-auth-policy.xml
Users > Authentication Policy > Global Authentication Policy	junoscope-globalPolicy.xml
RADIUS Configuration	junoscope-radiusClients.xml
Import/Export Data	junoscope-all.xml
Saved Operations	junoscope-operations.xml

Browse button—Displays the File Open dialog box so that you can browse for and select an XML file to import.

Key text box—Type the key to decrypt the sensitive data that you want to import. The key is required if you selected not to include it when the data was exported. This key can be up to 16 characters long and is created during the JUNOScope installation.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.
- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.
- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: "The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Import All Data button—Imports the contents of the XML file that you selected to import into the JUNOScope software. You see the information in the appropriate setup dialog box.

Import—Confirm Selections Dialog Box

Description Use the Import—Confirm Selections dialog box to ensure that you have selected the right device configuration text file to import into the JUNOScope Concurrent Versions System (CVS) repository.

Navigation Configuration > Repository > Import. Select a device configuration file to import, type the filename for the file in the CVS repository, type an optional descriptive comment, then click Next.

Permissions Superuser, read-write

Elements Please Confirm device configuration file pathname display area—Displays the pathname of the device configuration file to import.

Finish button—Opens the Import—View Import Status dialog box that displays the status of the imported device configuration file.

Previous button—Opens the previous Import—Upload Configuration File dialog box so you can choose another device configuration file to import.

Cancel button—Clears this dialog box and displays the Configuration > Repository menu.

Import Results Dialog Box

Description Use the Import Status dialog box to view the status of settings data that has been imported into the JUNOScope database.

Navigation

- Settings > Authentication Information. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Access Methods. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Devices. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Groups. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Labels. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Schedules. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Users > Local Authentication. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Users > User Group Authorization. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Users > Authentication Policy. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Users > Authentication Policy > Global Authentication Policy. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > RADIUS Configuration. Click Import. Select a settings XML file to import, select an import option, then click Import.
- Settings > Import/Export. Select an XML file to import, key, and import options.

Permissions Superuser

Elements Results table—The table includes the following columns:

- Settings column—Displays the name of the settings operation for which data is imported into the JUNOScope database.
- Results column—Displays the results of the file imported into the JUNOScope database for a settings operation, including the number of records successfully imported or failed.
- Details column—If during import any of the existing rules are violated, the record will not be imported (failed), and appropriate error message is displayed.

OK button—Click OK to clear the Import Results dialog box. You return to the appropriate settings operation dialog box.

Import—Upload Configuration File Dialog Box

Description Use the Import—Upload Configuration File dialog box to select a device configuration ASCII text file or XML file that includes all or part of a configuration file to import from the local file system into the JUNOScope software CVS repository. The dialog box also lets you add a filename and an optional comment to identify the imported configuration file in the CVS repository.

Navigation Configuration > Repository > Import

Permissions Superuser, read-write

Elements Local File text box and Browse button—Click Browse to open the Choose File dialog box from which you can navigate and select a file to import, then click Open. The device configuration file that you select displays in the Local File text box.

Name in Repository text box—Type the name of imported device configuration file in the CVS repository that you specify. The filename that you create appears in the Configuration File drop-down list box in the Compare—Select Options, Display—Select Options, and Restore—Select Options dialog boxes.

Comment (Optional) text box—Type an optional comment to describe what changed in a particular device configuration file revision. For example, type updated name servers to include the West Coast data center.

Next button—Opens the Import—Confirm Selections dialog box from which you can ensure that you are importing the correct device configuration file, filename, and comment.

Cancel button—Clears this dialog box and displays the Configuration > Repository menu.

Import—View Import Status Dialog Box

Description Use the Import—View Import Status dialog box to view the status of a device configuration file imported into the JUNOScope CVS repository.

Navigation Configuration > Repository > Import. Select the device configuration file to import. Confirm the import file selections, and click Next.

Permissions Superuser, read-write

Elements Local File display field—Displays the imported device configuration file pathname.

Configuration display field—Displays the name of the imported device configuration file in the CVS repository.

Action Taken display field—Displays the status of the imported configuration file. The possible actions include:

- Added—The new configuration file was successfully imported, creating a new configuration in the repository.
- Changed—The configuration file was successfully imported as a new revision of an existing configuration in the repository.
- No changes—The configuration file was uploaded, but the file contents matched an existing configuration in the repository, so no action was taken.

NOTE: When you use two configuration names—the configuration file that exists on the user's local disk and the configuration as it exists in the repository—the association between the two names only lasts for one import operation.

If there are two different configuration files—a.conf and b.conf—the actions taken would be as follows:

```
Local file Configuration Action Taken     Revision
a.conf config1      -> Added  1.1
b.conf config1      -> Changed 1.2
b.conf config1      -> No changes
a.conf config1      -> Changed 1.3
a.conf config2      -> Added   1.1
```

Revision display field—Displays the revision level of the device configuration file in the CVS repository.

OK button—Opens the Import—Upload Configuration File dialog box.

Inventory Management System—Reports

Description Use the Inventory Management System Reports page to select the type of inventory report you want to generate. You can use the Report Result window tools to manipulate data for your specific needs. You can view reports in XML, Excel, PDF, and text output formats.

Navigation Inventory Management > Reports.

Permissions Superuser, read-write, read-only

Data Sources A data source is a database from which you can view inventory report information. The Inventory Management System provides two report data sources:

- Inventory—A database from which you can view items that are created when an Inventory Management System scan is performed on Juniper Networks devices on the network. An inventory scan must be performed before you can view any report data.
- Demo—A demonstration database that includes sample inventory items that you can use to practice viewing and manipulating inventory reports. When you open a demo report, you see the word Demo in the title bar area to differentiate from your production inventory reports.

Report Categories The Inventory Management System provides the following report categories:

- Inventory Events—Lists any changes or discrepancies found in an inventory scan as compared with the inventory data stored in the JUNOScope database.
- Hardware Inventory—Lists the hardware components installed in a device or a router chassis, including the part number, serial number, FRU model number, and CLEI code.
- Licensing Inventory—Lists the feature licenses that have been installed on devices in the network, including the name of the licensed feature, number of licenses installed, number of licenses that are currently being used, and the number of licenses that are required to legally use the feature.
- Software Inventory—Lists the software components installed in a device, including the JUNOS software version and software packages.

Report Types Each report category provides three types of inventory reports (except for Inventory Events, which provides two: All and Search).

Report	Description
All	Displays all inventory records stored in the database.
Search	Lets you search for specific inventory records by one or more attributes.
Summary	Displays a summary of records with a total.

Report Tools The Report Results window provides the following tools.

Tool	Description
Sort	Arranges inventory records by selecting one of the predefined sort orders from the drop-down list box, or you can define your own sort order.
Advanced Query	Queries report records to display only those based on the criteria that you specify. You can show the query as columns or rows.
Configure Column	Changes the order in which columns appear in an inventory report.
Save Custom Report	Saves a report with the customizations you specified in a file with a unique name that you specify.
Reset	Clears all previously set customized controls such as sort, advanced query, and configure column, then regenerates the report with the default controls.
XML	Displays a report in XML format.
Excel	Displays a report in Microsoft Excel
PDF	Displays a report in Adobe Acrobat Reader.
Text	Displays a report in text format. You can view reports in text format for all report types except Hardware Inventory Summary and Licensing Inventory Summary.

Inventory Management System—Repository—Confirm Save Schedule Custom Report Operation Dialog Box

Description Use the Confirm Save Schedule Custom Report dialog box to check the schedule custom report options you selected before the operation is executed. The dialog box displays the custom report name and the saved operation name.

Navigation Inventory Management System > Repository > Schedule. Select the Save Operation as option and name it. Click OK.

Permissions Superuser

Elements Saved operation display area—Displays the custom report that you selected to save, and the saved operation name that you specified.

OK button—Saves the schedule custom report operation.

Inventory Management System—Repository—Confirm Schedule Custom Report Dialog Box

Description Use the Confirm Schedule Custom Report dialog box to check the schedule custom report options you selected. The dialog box displays the custom report name and schedule name.

Navigation Inventory Management System > Repository > Schedule. Select the Save Operation as option and name it. Click OK.

Permissions Superuser

Elements Scheduled report display area—Displays the custom report name and the schedule name with which it is associated.

OK button—Schedules the custom report.

Inventory Management System—Repository—Schedule Custom Report Dialog Box

Description Use the Schedule Custom Report dialog box to schedule a custom report to be run at a specified time.

Navigation Inventory Management System > Repository > Schedule

Permissions Superuser

Elements Data source drop-down list box—Displays the data sources from which custom reports were generated. The available custom reports change depending on the data source you select. Click a data source in the drop-down list box to select it.

Custom Report list box—Displays the custom reports that you have saved. You must save an inventory report to view it in this list box.

Comment text box—Type an optional comment for the scheduled custom report.

Save Operation as option button and text box—Saves the schedule custom report operation so you can combine it with other operations and run it at a later time. To view a saved operation, click Settings > Saved Operations.

Select Schedule option—Schedules the selected custom report.

Schedule table—Associates a selected custom report with the selected custom report.

OK button—Schedules the custom report.

Cancel button—Closes this dialog box without scheduling the selected custom report. You return to the Inventory Management menu.

Inventory Management System—Scan—Confirm Selections Dialog Box

Description Use the Scan—Confirm Selections dialog box to confirm the options you selected for the Inventory Management System to scan the inventory of one or more selected devices for hardware, software, and feature licenses.

Navigation Click Inventory Management > Scan. Select the device(s) that you want scanned and a time to scan in the Scan—Select Device and Time dialog box, then click Next.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the name of the device(s) on which the scan operation will occur and the scheduled time.

Finish button—Executes the scan operation. An operation progress message appears, then the Scan—View Operation Status dialog box appears displaying the status of the operation by device name, operation status, start time, last updated time, and the operation status message.

Previous button—Redisplays the previous operation dialog box and does not execute the operation.

Cancel button—Cancels the operation and redisplays the Inventory Management menu.

Inventory Management System—Scan—Select Device and Time Dialog Box

Description Use the Inventory Management System Scan—Select Device and Time dialog box to perform an inventory scan. A scan gathers a listing of all inventory items, such as:

- Events—Lists any changes or discrepancies found in an inventory scan as compared with the inventory data stored in the JUNOScope database.
- Hardware—Lists the hardware components installed in a device or a router chassis, including the part number and serial number.
- Licensing—Lists the feature licenses that have been installed on devices in the network, including the name of the licensed feature, number of licenses installed, number of licenses that are currently being used, and the number of licenses that are required to legally use the feature.
- Software—Lists the software components installed in a device, including the JUNOS software version and software packages.

Navigation Inventory Management > Scan.

Permissions Superuser, read-write

Elements Steps In Task—Describes the basic steps to complete the inventory scan task.

Devices to Scan section—Lets you select a group or selected devices on which to scan inventory. The options include:

- Group option button and drop-down list box—(Default) Displays the groups from which you can perform an inventory scan. You can select only one group.
- Selected Devices button and drop-down list box—Displays the devices from which you can perform an inventory scan. You can select one or more devices. Control-click to select more than one device.

Select Time or Save Operation section—Lets you select when you want an inventory scan to occur: now or at a predefined time. It also lets you save a scan operation with a unique name.

- Now option button—(Default) Performs an inventory scan when you click Next and confirm.
- Save Operation as text box—Type a unique name for the scan operation you want to save. The saved scan operation appears in the Saved Operations page. To view the Saved Operations page, click Settings > Saved Operations.
- Selected Schedule option button—Lets you select a predefined Schedule table—Displays the schedules that have already been set up for JUNOScope operations. Click an option button to select a schedule when you want an inventory scan to occur.
- Schedule table—Displays the schedules that have already been set up for JUNOScope operations. Click an option button to select a schedule when you want an inventory scan to occur.

Comments text box—Type an optional comment about the inventory scan.

Next button—Displays the Scan—Confirm Selections dialog box.

Cancel button—Closes this dialog box and redisplays the Inventory Management menu.

Inventory Management System—View—Select Archived Reports Dialog Box

Description Use the Select Archived Reports dialog box to view the archived custom reports that have run.

Navigation Inventory Management System > Repository > View

Permissions Superuser, read-write

Elements Apply Filter options—This area includes the following options:

- All Reports option—Selects all custom reports from all data sources.
- Selected Report option—This option lets you select the archive report you want by selecting the following:
- Data source drop-down list box—Lists the Inventory Management System databases from which you can view custom reports.
- Custom Report list box—Lists the custom reports that you have saved in a data source.

Filters to apply to query options—These options let you refine the search for specific archive reports you want to view:

- Limit to < # > rows per page drop-down list box—Filters the operation status by the number of rows to display per page: 10, 25, 50, or 100. The default is 10 rows.
- Sort results by < *column name* > drop-down list box—Sorts the results by the report generation time, report name, or username. The default is to sort by the last modified time. The default is to sort by the report generation time.
- Associated with user drop-down list box—Displays the operation status results that are associated with a selected username. The listed usernames have been added using Settings > Users. Select the check box to enable this filter rule.
- Start Date text box and calendar—Specifies the beginning of a date range within which to view archived reports. Click the calendar icon to view the current month. Select the date that you want, then click OK. The date appears in the Start Date text box in *dd/mm/yyyy* format (where *dd* is the day, mm is the month, and *yyyy* is the year).
- Till Date text box and calendar—Specifies the end of a date range within which to view archived reports. Click the calendar icon to view a the current month. Select the date that you want, then click OK. The date appears in the Start Date text box in *dd/mm/yyyy* format (where *dd* is the day, *mm* is the month, and *yyyy* is the year).

OK button—Searches for the archived report(s) to display in the Archived Reports dialog box.

Inventory Management System—View—View Archived Reports Dialog Box

Description Use the View Archived Reports dialog box to see a list of the custom reports that have been archived. Archived custom reports have been scheduled and run.

Navigation Inventory Management > Repository View. Select the archived reports you want to view in the Select Archived Reports dialog box, and click OK.

Permissions Superuser, read-write. Users with read-write can view only those archived reports that are generated by that user. Users with superuser permissions can view archived reports generated by all users.

Elements Archived report table—Lists the archived reports that you specified in the Select Archived Reports dialog box according to the filter rules. Archived reports are listed in the table by the custom report name, the username of the user who scheduled the report, and when the report was run or generated. You can view archived reports in Adobe PDF and Microsoft Excel format. Delete an archived report by clicking the Delete Report link.

Labels Dialog Box

Description Use the Labels table dialog box to view existing text labels used to statically group multiple devices for JUNOScope operations. You can associate a label with devices and add, edit, and copy labels. You can also import and export labels to the local file system in XML format.

Navigation Settings > Labels

Permissions Superuser

Elements Labels table—View existing labels by name, category, and comment. From the table, you can perform actions such as edit, copy, and delete, and associate a label with one or more devices.

Edit link—Lets you edit the label in that row of the table. The Edit Label dialog box appears.

Copy link—Copies a label in that row of the table. The Copy Label dialog box appears.

Delete link—Removes a label from that row of the table. The label is deleted from the JUNOScope database provided no scheduled operation is using the label. If the label is being used by a scheduled operation, a message appears stating that the label is in use.

Associate Devices link—Displays the Associate Devices to Label dialog box from which you can select one or more devices to associate with a label.

Add button—Displays the Add Label dialog box for you to add a new label which consists of a unique name, category name, and comment.

Import button—Displays the Import Labels dialog box from which you can import label information in XML format from the local file system.

Export button—Displays the File Download dialog box so you can save the label to the JUNOScope database.

Labels—Add Label Dialog Box

Description Use the Add Label dialog box to add text labels used to organize and categorize multiple devices for running JUNOScope operations.

Navigation Settings > Labels. Click Add in the Labels table dialog box.

Permissions Superuser

Elements Name text box—Type a unique label name. A label must not match any existing label or group name used in the JUNOScope software. For example, you could use a network name, customer name, a specific service name, and so on. The label name can be up to 40 characters long.

Category text box—Type a category for the label. The category is used to logically group related labels. For example, you can specify the type of network, a customer location, or the type of device. The category name can be up to 40 characters long.

Comment text box—Type an optional comment. The comment should describe the purpose of the label.

OK button—Saves the label in the JUNOScope database and lists the name, category, and comment in the Labels table dialog box.

Cancel button—Displays the Labels table dialog box without adding a new label.

Labels—Associate Devices to Label Dialog Box

Description Use the Associate Devices to Label dialog box to associate a label with one or more devices. Labels provide a way to statically organize and categorize related devices.

Navigation Settings > Labels. In the Labels table dialog box, click the Associate Devices link for associating the label in that row with selected available devices.

Permissions Superuser

Elements Label Name display field—Displays the name of the label you are associating with devices.

Category display field—Displays the category of the label you are associating with devices.

Comment display field—Displays the comment for the label you are associating with devices.

Available Devices list box—Displays all of the devices added to the JUNOScope software. Select a device to add to the Selected Devices list box. Shift + click to select several devices in sequence from the Available Devices list box. Ctrl + click to randomly select several devices from the Available Devices list box. Double-click a device to immediately move it to the Selected Devices list box.

Selected Devices list box—Lists the devices you selected with which to associate the label. Shift + click to select several devices in sequence from the Available Devices list box. Ctrl + click to randomly select several devices from the Available Devices list box. Double-click a device to immediately move it to the Available Devices list box.

Add/Remove buttons:

- Add button—Adds the selected available devices to the Selected Devices list.
- Remove button—Clears the selected devices from the Selected Devices list box.
- Add All button—Selects all of the available devices and adds them to the Selected Devices list box.
- Remove All button—Clears all of the devices from the Selected Devices list box.

OK button—Associates a label with the selected devices.

Cancel button—Displays the Label table dialog box without changing any information.

Labels—Copy Label Dialog Box

Description Use the Copy Label dialog box to duplicate an existing label category and comment. You must rename the copied label with a unique name.

Navigation Settings > Labels. Click a label's Copy link in the Labels table.

Permissions Superuser

Elements Name text box—Type a unique label name. A label must not match any existing label or group name used in the JUNOScope software. For example, you could use a network name, customer name, a specific service name, and so on. The label name can be up to 40 characters long.

Category text box—Type a category for the label. The category is used to logically group related labels. For example, you can specify the type of network, a customer location, or type of device. The category name can be up to 40 characters long.

Comment text box—Type an optional comment in the Comment text box. The comment should describe the purpose of the label.

OK button—Saves the label in the JUNOScope database and lists the name, category, and comment in the Labels table dialog box.

Cancel button—Displays the Labels table dialog box without adding a new label.

Labels—Edit Label Dialog Box

Description Use the Edit Label dialog box to modify the name, category, or comment of an existing label.

Navigation Setting > Labels. Click the Edit link in the row of the label you want to edit.

Permissions Superuser

Elements Name text box—Type a unique label name. A label must not match any existing label or group name used in the JUNOScope software. For example, you could use a network name, customer name, a specific service name, and so on. A label name can be up to 40 characters long.

Category text box—Type a category for the label. The category is used to logically group related labels. For example, you can specify the type of network, the customer location, or the type of device The maximum characters allowed in a category name is 40.

Comment text box—Type an optional comment. The comment should describe the purpose of the label.

OK button—Saves the edited label in the JUNOScope database and lists the name, category, and comment in the Labels table dialog box.

Cancel button—Displays the Labels table dialog box without editing the existing label.

Labels—Import Labels Dialog Box

Description Use the Import Labels dialog box to import existing labels to the local file system in XML file format.

Navigation Settings > Label. Click Import in the Labels table dialog box.

Permissions Superuser

Elements File text box—Type or browse to the labels XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

Browse button—Displays the File Open dialog box from which you can select the XML file to import.

Import button—Imports the selected label data into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears this dialog box and displays the Labels table dialog box.

Load Configuration Dialog Box

Description Use the Load Configuration dialog box to deploy an imported partial configuration file to multiple routers and perform a simultaneous update of configurations on these devices.

Navigation Click Configuration > Repository > Load

Permissions Superuser, read-write

Elements Group option button and drop-down list box—Select a device group to which to deploy an imported configuration. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any device groups, the Groups drop-down list box is empty.

Select Device(s) check box and list box—Select a device or devices to which to deploy an imported configuration. Click the Select Device(s) option button, then select the devices to which you want to load configuration from the Select Device(s) list box. If you have not added any devices, the Select Device(s) list box is empty.

Load Action drop-down list box—Select whether you want to override, replace, or merge (default) the current configuration on the devices. The available options are:

- Override—Discards all of the current configuration and loads the selected configuration.
- Replace—Deletes the current configuration statement(s) and adds the selected configuration.
- Merge—(Default) Combines the selected configuration statement(s) with the current configuration. If there are conflicting statements, the statements in the incoming configuration override those in the current configuration.

Synchronize Routing Engines check box—Click to load the configuration on both the master and backup Routing Engine, if a router has two Routing Engines installed.

Comment (Optional) text box—Type a descriptive comment about the load configuration operation you want to run.

Select Configuration table—Lists the configuration files archived from a router or imported from the local file system by name, archive date, revision, and comment. Select a configuration to load to the selected device or group of devices.

Select Time or Save Operation area:

- Now option button—Runs the load configuration operation as soon as you click Next and confirm the operation settings.
- Save Operation as text box—Type a unique name for the load configuration operation you want to save. The saved load configuration operation appears in the Saved Operations page. To view the Saved Operations page, click Settings > Saved Operations.
- Next button—Displays the Confirm Load Configuration dialog box.

Load Configuration—Confirm Load Configuration Dialog Box

Description Use the Confirm Load Configuration dialog box to confirm your selections in the Load Configuration dialog box.

Navigation Click Configuration > Repository > Load

Permissions Superuser, read-write

Elements Please Confirm Operation display field—Displays the load configuration operation, the devices or group of devices on which the operation will be performed, and the schedule for you to confirm whether or not you want it to occur.

Sync the Startup Config with the Running check box—Select this check box if you wish to synchronize the running configuration with the startup configuration If this option is not selected, only the running configuration is updated after the load operation. This option is displayed only when you have selected a BXOS device for loading configuration

Finish button—Click Finish to load the configuration to the devices;

- If you selected the Now option while selecting the time to perform upload configuration then the View Status page appears with real time updates on the status of the operation.
- If you selected to save the upload configuration operation, you return to the Configuration > Repository > Load Configuration menu. To view the saved operation, click Settings > Saved Operations.

Previous button—Displays the previous Load Configuration dialog box.

Looking Glass

Description Use Looking Glass to view status and troubleshooting information from Juniper Networks routers, including router chassis, system-level, Adaptive Services PIC (ASP), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Multiprotocol Label Switching (MPLS), and Resource Reservation Protocol (RSVP) routing protocol status information.

Navigation Click Looking Glass > Query.

Permissions Superuser, read-write, read-only

Elements Device list box—Lists the routers that are available for you to monitor. Click a router to monitor it.

Category list box—Lists the available types of monitoring and troubleshooting commands. Click a command category to select it. The available commands for that category appear in the Command list box.

Command list box—Lists the available monitoring and troubleshooting commands for the selected command category. Click a command to select it.

Submit button—Issues or executes the device command that you selected and displays the device command output.

Refresh Command After drop-down list box—Select how often you want Looking Glass to send a request for the device command information to the router. The available options include: Never, 5 seconds, 10 seconds, 1 minute, 5 minutes, and 10 minutes. The default refresh option is Never. If you select 1 minute, Looking Glass will send a request for the device command information from the router every minute.

Monitor—Audit Log—Select Event Category, Type, or Username Dialog Box

Description Use the Monitor—Audit Log—Select Event Category, Type, or Username dialog box to filter and query the audit log records you want to view. The JUNOScope software records all authentication activities and privileged operations performed by authorized users in the Audit Log. Additionally, authentication activities and privileged operations are sent to the system log message server and to an optional RADIUS accounting server if it is configured.

Navigation Click Monitor > Audit Log.

Permissions Superuser

Elements Filters to apply to query options—Define the rule for viewing operation status. The filter rule options include:

- Limit to *number* of rows per page drop-down list box—Select how many record rows you want to display per audit log page: 10, 25, 50, or 100. The default is 10.
- Sort results by *item* drop-down list box—Select the column of data by which the audit log records will be sorted in the table: Time, Username, Client address, Event type, or Message. The default is Time.
- Refresh Events every *interval* drop-down list box—Select when the audit log data will be updated in the table: from Never up to 1 hour. The default is Never.
- Event Category drop-down list box—Select the events category to display: All, Authentication, or Privileged operations. Authentication activities include user login success, failure, logout, and session timeout. Privileged operations are changes to information in the system or in the network, such as restoring a configuration to a device or changing a user password. The default is All.
- Event Type drop-down list box—Displays the title of the event. This list box is dynamically populated based on the event category that you selected. For example, if you select the Authentication event category, all authentication event message types appear in this drop-down list box.
- Updated in last *time period* check box, text box, and drop-down list box—Select the audit log records that have been updated in the last specified length of time. You can select *n* seconds, minutes, hour, or days, where *n* represents the time you specify. The default is 0 seconds.
- Associated with user drop-down list box—Select records that are associated with a specified username.

OK button—Click OK to display the audit log records that you have filtered and queried. The Audit Log—View Events Records dialog box appears.

Monitor—Audit Log—View Events Records Dialog Box

Description Use the Monitor—Audit Log to view all authentication activities and privileged operations performed by authorized users. Authentication activities include user login success, failure, logout, and session timeout. Privileged operations change information in the system or in the network, such as restoring a configuration to a device or changing a user password.

Additionally, authentication activities and privileged operations are sent to the system log message server and to an optional RADIUS accounting server.

Navigation Click Monitor > Audit Log. Select the filter rules to display only the audit log records you want to view in the Audit Log—Select Event Category, Type, or User Name dialog box, and click OK.

Permissions Superuser

Elements The Audit Log displays events in a table sorted by:

Time column—The date and time when the event was logged. The format for date and time is dow mon *dd hh:mm:ss zzz yyyy*.

Where:

- *dow* is the day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat).
- *mon* is the month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec).
- *dd* is the day of the month (01 through 31), as two decimal digits
- *hh* is the hour of the day (00 through 23), as two decimal digits
- *mm* is the minute within the hour (00 through 59), as two decimal digits
- *ss* is the second within the minute (00 through 61, as two decimal digits.
- *zzz* is the time zone (and may reflect daylight saving time). If time zone information is not available, then *zzz* is empty—that is, it consists of no characters at all.
- *yyyy* is the year, as four decimal digits.

User name column—The name of the user who performed the action that was logged.

Client Address column—The IP address of the client from which the action occurred.

Event Type column—The title of the audit log message that is logged.

Message column—The description of the audit log message that is logged.

Monitor—Operations Dialog Box

Description Use the Monitor—Operations dialog box to view the status of operations that have run using an existing schedule and to verify the next time they will run.

An operation appears in the Monitor Operations dialog box when you run it using an existing schedule that you create using Settings > Schedule. An operation does not appear in Monitor Operations when you schedule an operation using the Now option.

If you have not scheduled any operations to run, this dialog box is empty.

Navigation Click Monitor > Operations.

Permissions Superuser, read-write, read-only

Elements Operations table—Displays the status of operations that have run by action name (a compound operation is labeled run operation), target device or report on which the operation ran (a compound operation name is displayed in this column), User, the name of user who run the operation, schedule name, when the operation is next scheduled to run, the last status, and an optional operation comment. If you click a link in the Last Status column, the Monitor > Status dialog box appears displaying the status of the operation.

Delete check box—Select the scheduled operation that you want to delete, then click Delete.

Delete button—Removes the selected operation scheduled to run from the JUNOScope software database. If a schedule is associated with an operation that is scheduled to run, you must delete the scheduled operation from this dialog box first, then delete the schedule from the Schedule dialog box. If a device or group is associated with an operation that is scheduled to run, you must delete the scheduled operation from this dialog box first, then delete the device or group from the Devices or Groups dialog boxes.

Monitor—Purge—Audit Log—Audit Log Records Filter Options Dialog Box

Description Use the Audit Log Records Filter Options dialog box to filter the event records you want to purge. Most JUNOScope operations add multiple audit log records in the Audit Log table. As more and more operations are performed, this table grows in size and consumes disk space on the JUNOScope software server. The data in the Audit Log table is useful only to administrators. From time to time, you must remove records that are no longer used in the Audit Log table, and reclaim disk space if you are an administrator.

Navigation Click Monitor > Purge > Audit Log.

Permissions Superuser

Elements Select Operation Age options—Lets you select all of the operations status records to purge or ones within a certain date range or a specified age. The area includes the following options:

- Date Range: From Date (MM/DD/YYYY)/To Date (MM/DD/YYYY) option text boxes—Type the date range within which to delete status records. Click the calendar icon view a calendar from which you can select a date and get the local time. Click Local Time to view the current time. Click OK in to insert the date that you selected.
- Months old Events option text box—Type the number months to go back and retrieve status records to purge.
- All Events option button—Selects all status records to purge.

Filters to apply to query options—Defines the rule for filtering audit log records. The filter rule options include:

- Limit to *number* of rows per page drop-down list box—Select how many record rows you want to display per audit log page: 10, 25, 50, or 100. The default is 10.

- Sort results by *column-name* drop-down list box—Select the column of data by which the audit log records will be sorted in the table: Time, Username, Client address, Event type, or Message. The default is Time.

- Event Category drop-down list box—Select the event category to display: Authentication, or Privileged Operations. Authentication activities include user login success, failure, logout, and session time-out. Privileged operations are changes of information in the system or in the network, such as restoring a configuration to a device or changing a user password. The default is Authentication.

- Event Type drop-down list box—This list box is dynamically populated based on the event category that you selected. For example, if you select the Authentication event category, all authentication event message types appear in this drop-down list box.

- Associated with user drop-down list box—Select records that are associated with a specified username.

Filter button—Filters the audit log records using the filter options you have selected. The View Filtered Audit Log Records dialog box appears.

Reset button—Clears all the values you selected and displays the default values.

Monitor—Purge—Audit Log—Confirm Purge All Filtered Audit Log Records Dialog Box

Description Use the Confirm Purge All Filtered Audit Log Records dialog box to confirm the deletion of all filtered event records.

Navigation Click Monitor > Purge > Audit Log. Select the filter options and click Filter to filter out the records you would like to delete. The View Filtered Audit Log Records dialog box appears. Click Delete All Filtered Records.

Permissions Superuser

Elements Filter Criteria display field—Displays the filter options that you selected to filter audit log records to be purged.

Please Confirm display field—Displays the number of Audit Log records that will be deleted permanently.

Comments text field—Type a reason for deleting the audit log records.

OK button—Confirms the deletion of all the filtered audit log records. The audit log records are removed from the audit log table in the JUNOScope database.

Cancel button—Displays the View Filtered Audit Log Records dialog box.

Monitor—Purge—Audit Log—Confirm Purge Audit Log Records Dialog Box

Description Use the Confirm Purge Audit Log Records dialog box to confirm the deletion of records you selected.

Navigation Click Monitor > Purge > Audit Log. Select the events you want to purge and the filter rules from the Audit Log Filter Options dialog box and click Filter. The View Filtered Audit Log Records dialog box appears. Select the records you want to delete and click Delete Selected Records.

Permissions Superuser

Elements Please Confirm display field—Displays the message that all the Audit Log records listed in the Audit Log Records table below will be deleted permanently.

Audit Log Records table—Displays the audit log records you selected for deletion. Shows details of events such as, date and time, username, client IP address, type, and message.

Comments text field—Type the reason for deleting the audit log records.

OK button—Confirms the deletion of the selected audit log records. The audit log records are removed from the audit log table in the JUNOScope database.

Cancel button—Displays the View Filtered Audit Log Records dialog box.

Monitor—Purge—Audit Log—View Filtered Audit Log Records Dialog Box

Description Use the View Filtered Audit Log Records dialog box to view the filter criteria and the list of the filtered audit log records with the date and time, username, client IP address. event type, and message.

Navigation Click Monitor > Purge > Audit Log. Select the filter options and click on Filter to filter out the records you would like to delete.

Permissions Superuser

Elements View Filtered Records table—Displays the filtered audit log records in the following columns:

Time column—The date and time that the event was logged. The format for date and time is *dow mon dd hh:mm:ss zzz yyyy*. Where:

- *dow* is the day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat).
- *mon* is the month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec).
- *dd* is the day of the month (01 through 31), as two decimal digits.
- *hh* is the hour of the day (00 through 23), as two decimal digits.
- *mm* is the minute within the hour (00 through 59), as two decimal digits.
- *ss* is the second within the minute (00 through 61), as two decimal digits.
- *zzz* is the time zone (and may reflect Daylight Saving Time). If time zone information is not available, then *zzz* is empty; that is, it consists of no characters at all.
- *yyyy* is the year, as four decimal digits.

User column—The name of the user who performed the action that was logged. The default user is admin.

Client Address column—The IP address of the client from which the action occurred.

Event Type column—The title of the audit log message that is logged.

Message column—The description of the audit log message that is logged.

Delete Selected button—Deletes the select the records.

Delete All Filtered Records—Deletes all filtered records.

Monitor—Purge—Status—Confirm Purge All Filtered Status Records Dialog Box

Description Use the Confirm Purge All Filtered Status dialog box dialog box to confirm the deletion of all filtered records.

Navigation Click Monitor > Purge > Status. Select the filter options and click Filter. The View Filtered Status Records dialog box appears. Select the records you want to delete and click Delete All Filtered Records.

Permissions Superuser

Elements Please Confirm display field—Displays the number of status records that will be deleted permanently.

Comments text field—Enter the reason for deleting the status records.

OK button—Confirms the purge of all filtered status records. The status records are removed from the status table in the JUNOScope database.

Cancel button—Displays the View Filtered Status Records dialog box.

Monitor—Purge—Status—Confirm Purge Status Records Dialog Box

Description Use the Confirm Purge Status Records dialog box to confirm the deletion of selected records.

Navigation Click Monitor > Purge > Status. Select the filter options and click on Filter to filter out the records you would like to delete. The View Filtered Status Records dialog box appears. Select the records you want to delete and click Delete Selected.

Permissions Superuser

Elements Please Confirm display field—Indicates that all the Status records listed in the Status Records table will be deleted permanently.

Status Records table—Displays the status records you selected for deletion. These are listed by operation name, operation type, device name, report name, username, final operation status, operation start time, last updated status time, and status message.

Comments text field—Enter the reason for deleting the status records.

OK button—Click OK to confirm purge of the selected status records. The status records are removed from the status table in the JUNOScope database.

Cancel button—Redisplays the View Filtered Status Records dialog box.

Monitor—Purge—Status—Purge Status Records Filter Options Dialog Box

Description Use the Status Records Filter Options dialog box to filter the status records you want to purge. Most Junoscope operations add multiple status records to the Status table. As more and more operations are performed, this table grows in size and consumes disk space on the JUNOScope software server. The data in the Status table is useful only to administrators. From time to time, you must remove records that are no longer used in the Status table, and reclaim disk space if you are an administrator.

Navigation Click Monitor > Purge > Status.

Permissions Superuser

Elements Select Operation Age options—Lets you select all of the operations status records to purge or ones within a certain date range or a specified age. The area includes the following options:

- Date Range: From Date (MM/DD/YYYY)/To Date (MM/DD/YYYY) option text boxes—Type the date range within which to delete status records. Click the calendar icon view a calendar from which you can select a date and get the local time. Click Local Time to view the current time. Click OK in to insert the date that you selected.
- Months old operations option text box—Type the number months to go back and retrieve status records to purge.
- All Operations option button—Selects all status records to purge.

Filters to apply to query options—Define the rule for filtering status records. The filter rule options include:

- Limit to number of rows per page drop-down list box—Filters the operation status by the number of rows to display per page: 10, 25, 50, or 100. The default is 10 rows.

- Sort results by *column name* drop-down list box—Sorts the results by the last updated time, operation name, operation type, device name, username, status, start time, or message. The default is to sort by the last modified time.

- Currently in *state* check box and drop-down list box—Filters the operation status by those that are currently in a particular state: pending, connecting, working, writing, warning, success, and error. The default is pending. Select the check box to enable this filter rule.

- Associated with user drop-down list box—Displays the operation status results that are associated with a selected username. The usernames that appear in the list box are the users that have been added using Settings > Users. Select the check box to enable this filter rule.

- Operation type drop-down list box—Displays the current JUNOScope operations that you can save, such as archive, restore, report, scan inventory, install, and download. The default is archive. Select the check box to enable this filter rule.

Filter button—Filters the status records using the filter options you have selected. The View Filtered Status Records dialog box appears.

Reset button—Clears all the values you selected and returns to the default values.

Monitor—Purge—Status—View Filtered Status Records Dialog Box

Description Use the View Filtered Status Records dialog box to view the filter criteria and the list of the filtered status records with the date and time, username, client IP address. event type, and message.

Navigation Click Monitor > Purge > Status. Select the records you want to purge and the filter rules from the Status Records Filter Options dialog box and click Filter.

Permissions Superuser

Elements View Filtered Records table—The table lists the filtered status records in the following columns:

- Operation Name—Saved operation name. The name that you give an operation when you save it to run at a later time using Settings > Saved Operations.
- Operation Type—The type of JUNOScope operation that was run. Some operations, such as software image install, have multiple actions. You can view all actions in an operation by clicking the Show Task link.
- Device Name—Name of the device on which an operation was run.
- Report Name—Name of the custom report that was scheduled and run.
- User—Username of the user who ran an operation.
- Status—The status of the operation that ran. The status can be pending, connecting, writing, rebooting, success, or error. The Message column describes the operation status.
- Start Time—The time the operation started.
- Last Updated Time—The time the operation status was polled and refreshed. You can sort this column by clicking the arrow in the column header.
- Message—Displays the status message for an operation that was run.

Delete Selected Records button—Deletes the selected record(s).

Delete All Filtered Records—Delete all the filtered records.

Monitor—Purge—Status—Select Device, Operations, Reports, Query Options Dialog Box

Description Use the Status—Select Device, Operations, Reports, Query Options dialog box to view the status of archive and restore operations that have run. With the Operations Status dialog box, you can select one or more routers for which to view the status and define a filter that displays status by the number of rows per page, defined properties, when last updated, and status in a defined state. You can also choose to have JUNOScope update the status by a defined number of seconds, minutes, or one hour.

Navigation Click Monitor > Status.

Permissions Superuser, read-write, read-only

Elements Devices, Operations, and Reports to Query option buttons—Select from the following option buttons to select the items you want to query:

All Operations option button—Select all available JUNOScope operations that have run.

All Devices option button—Select all routers on which operations have run.

All Reports option button—Selects all custom scheduled inventory reports that have run.

Group option button and drop-down list box—Select a group of routers for which to see the operation status. Click the down arrow to see the available groups.

Selected Devices option button and list box—Select one or more routers from the available routers list for which to see the operation status. Click the down arrow to see the available routers. Shift + click to select more than one router from the drop-down list box.

Selected Operations list box—Select specific operations of which to view status.

Selected Reports—Lets you select from the following options:

- Datasource drop-down list box—Selects the Inventory Management System database from which to view operation status.
- Custom Report list box—Selects a custom report to view operation status.

Filters to apply to query options—Define the rule for viewing operation status. The filter rule options include:

- Limit to *number* of rows per page drop-down list box—Filters the operation status by the number of rows to display per page. The default is 25 rows.
- Sort results by *item* drop-down list box—Sorts the results by the last modified time, start time, device name, status, operation, or message. The default is to sort by the last modified time.
- Refresh status every *interval* drop-down list box—Updates the operation status at an interval that you specify. The default is Never.
- Updated in last *time period* check box, text box, and drop-down list box—Filters the operation status results by the last time period that you specify. The default is 0 seconds. Select the check box to enable this filter rule. Type a time value in the text box. Click the down arrow to view the available time periods: seconds, minutes, hours, and days.
- Currently in state drop-down list box—Filters the operation status by those that are currently in a particular state: pending, connecting, working, writing, success, and error.
- Associated with user drop-down list box—Filters the operation status results by those that are associated with a selected username.
- Operation Type drop-down list box—Filters the operation status results by the type of JUNOScope operation that has run—archive, restore, report, scan inventory, install, or download. the default is archive.

OK button—Displays the Operation Status Results dialog box with the status of each operation that has run on the selected router(s) and according to the filter rule that you selected.

Monitor—Status—View Status Records Dialog Box

Description Use the View Status Records dialog box to display the status of all operations. The status table lists the operation run results by operation name, operation type, device name, Report name, username, run status, run start time, last updated time and status message. The status table also includes the actions column with Show Task and Redo Task hyperlinks. If the Show Task link is selected, a page that displays operation run results for that specific task appears. The Redo Task link takes you to the Redo Task wizard.

Navigation Click Monitor > Status.

Permissions Superuser, read-write, read-only

Elements View Status Records table—The table lists the operation run status in the following columns:

- Operation Name column—The name of the saved operation that was run.
- Operation Type column—The type of operation: archive, restore, or inventory scan.
- Device Name column—Name of the device DNS name or IP address upon which the operation will run.
- Report Name column—Name of the custom report that was scheduled and run.
- User column—Name of the user who has either run or scheduled the operation
- Status column—Status of the operation, including:

- Pending—The operation has been created and queued but has not started executing.
- Working—The operation is currently executing.
- Waiting—The operation has executed but is waiting for its children to complete.
- Aborted—The operation did not run and will not run because of the result of a previous operation.
- Success—The operation completed successfully.
- Warning—The operation has completed, but with a warning. A warning typically does not affect the execution of other related operations.
- Error—The operation has completed, but with an error. Typically, related operations will be aborted.
- Shutdown—The operation did not run because the system was shutdown.

Start Time column—Time since the operation started executing.

Last Updated Time column—Time the operation was last updated.

Message column—Message detailing the status of operation. It also contains the link to the output of an executed script.

Actions column—Displays the Show Task and Redo Task Links. Click the Show Task link to display a page that displays the operation run results for the task you selected. Click the Redo Task link to redo the task you selected.

Monitor—Status—Select the Operation in the Task for Redo Dialog Box

Description Use the Select the Operation in the Task for Redo dialog box to select the operation you want to redo.

Navigation Click Monitor > Status. Apply query options and filters in the Select Device and Query Options dialog box and click OK. Click the Redo task hyperlink in the Actions column of the View Status Records dialog box.

or

Click the Redo Task button in the View Status Records dialog box that appears after you perform an operation.

Permissions Superuser, read-write, read-only

Elements Select Operations drop–down list box—Lists the operations in the task that you can redo.

Next button—Displays the Select the Device(s) on which the Operation has to be Redone dialog box.

Cancel button—Clears this dialog box and displays the Select Devices, Operations or Reports and Query Options dialog box.

Monitor—Status—Select the Device(s) on which the Operation has to be Redone Dialog Box

Description Use the Select the Device(s) on which the Operation has to be Redone dialog box to select the devices on which you want to redo the operation.

Navigation Click Monitor > Status. Apply query options and filters in the Select Device and Query Options dialog box and click OK. Click the Redo task hyperlink in the Actions column of the View Status Records dialog box.

or

Click the Redo Task button in the View Status Records dialog box that appears after you perform an operation.

Select the operation you want to redo from the Select Operation drop-down list box and click Next in the Select the Operation in the Task for Redo dialog box.

Permissions Superuser, read-write, read-only

Elements Select Devices section:

- Success Devices list box—Lists all the devices on which the operation was successful.
- Failed Devices list box—Lists all the devices on which the operation failed.
- All Success Devices check box—Selects all devices on which the operation was successful.
- All Failed Devices check box—Selects all devices on which the operation failed.

Next button—Displays the Confirm Redo dialog box.

Previous button—Displays the Select the Operation in the Task for Redo dialog box.

Cancel button—Clears this dialog box, and displays the Select Devices, Operations or Reports and Query Options dialog box.

Monitor—Status—Confirm Redo Dialog Box

Description Use the Confirm Redo dialog box to confirm the selections you made for redoing the operation.

Navigation Click Monitor > Status. Apply query options and filters in the Select Device and Query Options dialog box and click OK. Click the Redo task hyperlink in the Actions column of the View Status Records dialog box.

or

Click the Redo Task button in the View Status Records dialog box that appears after you perform an operation.

Select the operation you want to redo from the Select Operation drop-down list box in the Select the Operation in the Task for Redo dialog box and click Next. Select the device or devices on which the operation has to be redone from the Select the Device(s) on which the Operation has to be Redone dialog box and click Next.

Permissions Superuser, read-write, read-only

Elements Please Confirm section—Displays the operation and the devices on which the operation will be redone.

Finish button—Displays the status of the Redo operation in the View Status Records dialog box.

Previous button—Displays the Select the Device(s) on which the Operation has to be Redone dialog box.

Cancel button—Clears this dialog box, and displays the Select Devices, Operations or Reports and Query Options dialog box.

MPLS/GRE Tunnel Provisioning — Select Device Dialog Box

Description MPLS/GRE Tunnel Provisioning wizard has four steps, of which Select Device is the first step. Use the MPLS/GRE Tunnel Provisioning — Select Device dialog box to select the source and destination devices to provision MPLS/GRE tunnels using the LSP paths you have configured.

Navigation Click Provisioning > MPLS/GRE Tunnels > MPLS/GRE Tunnel Provisioning.

Permissions Superuser, read-write

Elements Select Device Source allows you to select whether you wish to select devices directly or select a device group:

- Select Device(s) Directly option button—Select this option button if you wish to select devices directly. If you select this option button, select devices under Select Source/Destination Endpoint Devices.
- Select a Device Group option button—Select this option button and select a device group from the drop-down list box.

Find Devices that include the following: allows you to search and display available devices.

Select a Field drop-down list box—Select from: Device Name, Device Hostname, Model, Location, or Comment.

Select an Operator drop-down list box—Select an operator from the drop-down list box and enter a value in the text box beside it.

Show button—Click this button to display all the devices that meet the criteria you specified.

Clear button—Click this button to clear the list of devices.

Select Devices—Select at least two devices. Press the Shift key and click the device names to select multiple devices.

Next button—Click this button to go to the next step in the wizard.

MPLS/GRE Tunnel Provisioning — Add/Edit/Delete MPLS/GRE Tunnels Dialog Box

Description MPLS/GRE Tunnel Provisioning wizard has four steps, of which Add/Edit/Delete MPLS/GRE Tunnels is the second step. Use the Add/Edit/Delete dialog box to enter tunnel details or modify them, or delete a tunnel.

Navigation Click Provisioning > MPLS/GRE Tunnels > MPLS/GRE Tunnel Provisioning, and then click Next in the Select Device dialog box after entering the details.

Permissions Superuser, read-write

Elements Tunnel Type drop-down list box—Select a tunnel type from MPLS-RSVP, MPLS-LDP, and GRE.

Source Device drop-down list box—Select a source device for the MPLS/GRE tunnel.

Destination Device drop-down list box—Select a destination device for the MPLS/GRE tunnel.

Provide Source Endpoint Details: allows you to specify details such as LSP path and bandwidth for the source device.

- LSP Name—Enter the LSP name for the source device. This is required only for MPLS-RSVP.
- LSP Bandwidth—Enter the LSP bandwidth for the source device.
- Select a Primary Path—Select a primary path from the drop-down list box. This is required only for MPLS-RSVP.
- Select a Secondary Path—Select a secondary path from the drop-down list box. This is required only for MPLS-RSVP.
- Setup Priority—Select a setup priority from the drop-down list box.
- Reservation Priority—Select a reservation priority from the drop-down list box.
- QOS Priority—Select a QOS priority from the drop-down list box.
- Enable Fast Reroute—Select this check box to enable fast reroute. This is applicable only to MPLS-RSVP.
- Maximum Hop Count—Enter the maximum number of hops, if the tunnel type is MPLS-RSVP, and you have selected the Enable Fast Reroute check box.
- Enable Node Link Protection—Select this check box to enable node link protection.
- Enable Link Protection—Select this check box to enable link protection.
- Select GRE Interface—Select an interface from the drop-down list box if the tunnel type you selected is GRE.
- Logical Unit—Enter the logical unit of the GRE interface if the tunnel type you selected is GRE.

Provide Destination Endpoint Details: allows you to specify details such as LSP path and bandwidth for the destination device.

- Copy Source Endpoint Details—Select this check box if you wish to copy the source endpoint details for the destination endpoint.
- LSP Name—Enter the LSP name for the destination device. This is required only for MPLS-RSVP.
- LSP Bandwidth—Enter the LSP bandwidth for the destination device.
- Select a Primary Path—Select a primary path from the drop-down list box. This is required only for MPLS-RSVP.
- Select a Secondary Path—Select a secondary path from the drop-down list box. This is required only for MPLS-RSVP.

- Setup Priority—Select a setup priority from the drop-down list box.
- Reservation Priority—Select a reservation priority from the drop-down list box.
- QOS Priority—Select a QOS priority from the drop-down list box.
- Enable Fast Rerout—Select this check box to enable fast reroute. This is applicable only to MPLS-RSVP.
- Maximum Hop Count—Enter the maximum number of hops, if the tunnel type is MPLS-RSVP, and you have selected the Enable Fast Reroute check box.
- Enable Node Link Protection—Select this check box to enable node link protection.
- Enable Link Protection—Select this check box to enable link protection.
- Select GRE Interface—Select an interface from the drop-down list box if the tunnel type you selected is GRE.
- Logical Unit—Enter the logical unit of the GRE interface if the tunnel type you selected is GRE.

Add Entry button—Click this to add the tunnel or save modifications.

Edit button—Click this to make modifications to the tunnel details.

Delete button—Click this to delete the tunnel.

Force Deploy button—Click this to push the configuration details to the devices even if you have not modified them.

Previous button—Click this to go to step 1: Select Device dialog box.

Next button—Click this to go to step 3: Confirm Add/Edit/Delete MPLS/GRE Tunnels dialog box.

The tabular area at the bottom of the dialog box displays the tunnels configured between the devices selected in step 1: Select Devices:

- Select—Select a check box to edit the tunnel or delete it.
- State—New , Modified , and Unchanged
- Tunnel Type—Displays the tunnel type.
- Source Device—Dispays the source device name.
- Source LSP—Displays the source LSP path for MPLS-RSVP tunnels.
- Source GRE Intf—Displays the source GRE interface for GRE tunnels.
- Destination Device—Dispays the destination device name.
- Destination LSP—Displays the destination LSP path for MPLS-RSVP tunnels.
- Destination GRE Intf—Displays the destination GRE interface for GRE tunnels.

MPLS/GRE Tunnel Provisioning — Confirm Add/Edit/Delete MPLS/GRE Tunnels Dialog Box

Description MPLS/GRE Tunnel Provisioning wizard has four steps, of which Confirm Add/Edit/Delete MPLS/GRE Tunnels is the third step. Use the Confirm Add/Edit/Delete dialog box to confirm addition, modification, or deletion of a tunnel.

Navigation Click Provisioning > MPLS/GRE Tunnels > MPLS/GRE Tunnel Provisioning and click Next in the Select Device dialog box after entering the details, and then click Next in the Add/Edit/Delete MPLS/GRE Tunnels dialog box.

Permissions Superuser, read-write

Elements Confirm button—Click this to confirm creation, modification, or deletion of MPLS/GRE Tunnels.

Previous button—Click this to go back to the Add/Edit/Delete MPLS/GRE Tunnels dialog box.

The tabular area at the bottom of the dialog displays the following details:

- Operation—Creation, Modification, or Deletion.
- Tunnel Type—Displays the tunnel type.
- Source Device—Dispays the source device name.
- Source LSP—Displays the source LSP path for MPLS-RSVP tunnels.
- Source GRE Interface—Displays the source GRE interface for GRE tunnels.
- Destination Device—Dispays the destination device name.
- Destination LSP—Displays the destination LSP path for MPLS-RSVP tunnels.
- Destination GRE Interface—Displays the destination GRE interface for GRE tunnels.

MPLS/GRE Tunnel Provisioning — Select Time or Schedule Dialog Box

Description MPLS/GRE Tunnel Provisioning wizard has four steps, of which Select Time or Schedule is the fourth step. Use the Select Time or Schedule dialog box to set up the time or schedule for the creation, modification, or deletion of the tunnels carried out in the earlier steps of the wizard.

Navigation Click Provisioning > MPLS/GRE Tunnels > MPLS/GRE Tunnel Provisioning and click Next in the Select Device dialog box after entering the details, then click Next in the Add/Edit/Delete MPLS/GRE Tunnels dialog box, and then click Confirm in the Confirm Add/Edit/Delete MPLS/GRE Tunnels dialog box.

Permissions Superuser, read-write

Elements Select Time or Save Operation: allows you to save the operation or set up the time or schedule.

Now option button—Select this option to carry out the operation now.

Save Operation option button—Select this option and enter a name for the operation to save the configuration as a named operation.

Select Schedule option button—Select this option button and select a schedule from the table below to set up the operation to be carried out at the specified time.

The table at the bottom of the dialog box lists the schedules configured in the Settings tab, giving the following details:

- Schedule Name
- Start Time
- Period (frequency)
- Comment

OK button—Click OK after selecting an option to set up the schedule or save the operation.

Previous button—Click this to go back to the Confirm Add/Edit/Delete MPLS/GRE Tunnels dialog box.

Pseudowires — Templates Dialog Box

Description Use the Templates dialog box to define pseudowire templates, which can be later used to create pseudowires.

Navigation Click Provisioning > Pseudowires > Templates.

Permissions Superuser

Elements This dialog box displays the templates already defined: you can delete or export them, or import from an XML file if you have earlier exported some templates.

Delete button—Select one or more templates, and click this button to delete them.

Export button—Click this button to export all templates and save them as an XML file.

Import button—Click this button to import templates you saved (exported) as XML earlier.

Select Template Type drop-down list box—Select a template type from the drop-down list box and click Add.

Add button—Click this button after selecting the template type to define a template of that type.

Pseudowires — Templates — Add New SAToP Template Dialog Box

Description Use the Add New SAToP Template dialog box to add new SAToP templates, which can be later used to create pseudowires.

Navigation Click Provisioning > Pseudowires > Templates, select SAToP as the template type and click Add.

Permissions Superuser

Elements Name—Enter the name of the new SAToP template.

Comment—Enter a comment.

Payload Size (1-1024): —Enter a value between 1 and 1024.

Idle Pattern (0-255): —Enter a value between 00 and 255.

Excessive Packet Loss Threshold (1-100): —Enter a value between 1 and 100.

Excessive Packet Loss Sample Period (1000-65535 msec): —Enter a value between 1000 and 6535 milliseconds.

Jitter Buffer Latency (msec): —Enter a value in milliseconds.

Control Word check box—Select this check box to enable the control word.

Save button—Click this button to save the new SAToP template.

Cancel button—Click this button to go back to the Templates dialog box.

Pseudowires — Templates — Add New ATM Template Dialog Box

Description Use the Add New ATM Template dialog box to add new ATM templates, which can be later used to create pseudowires.

Navigation Click Provisioning > Pseudowires > Templates, select ATM as the template type and click Add.

Permissions Superuser

Elements Name text box—Enter the name of the new ATM template.

Comment text box—Enter a comment.

Bandwidth text box—Enter the bandwidth to be allocated to the pseudowire.

Control Word check box—Select this check box to enable the control word.

Mode drop down list- Allowed options are 1–to-1–vcc, n–to-1-vcc, 1–to-1–vpc, n-to-1-vpc, aal5–pdu and aal5–sdu

Maximum Cell Concatenation(1-28): text box— Enter the maximum number of ATM cells that can be concatenated before the packet switched network (PSN) packet is sent out.

Timeout(0-100 msec): text box— Enter the maximum time that the device should wait for the specified number of ATM cells to arrive for concatenation.

Sequence Number check check box— Select this to enable the sequence number check.

Sequence Number Switchover(1-255): text box— Enter a value between 1 and 255.

Encapsulation drop-down list box—Select an appropriate encapsulation type. Allowed options are atm-ccc-cell-relay and atm-ccc-vc-mux.

Save button—Click this button to save the new ATM template.

Cancel button—Click this button to go back to the Templates dialog box.

Pseudowires — Templates — Add New Ethernet Template Dialog Box

Description Use the Add New Ethernet Template dialog box to add new Ethernet templates, which can be later used to create pseudowires.

Navigation Click Provisioning > Pseudowires > Templates, select Ethernet as the template type and click Add.

Permissions Superuser

Elements Name—Enter the name of the new Ethernet template.

Comment—Enter a comment.

Bandwidth—Enter the bandwidth to be allocated to the pseudowire.

Control Word check box—Select this check box to enable the control word.

Encapsulation drop-down list box—Select an appropriate encapsulation type.

Save button—Click this button to save the new Ethernet template.

Cancel button—Click this button to go back to the Templates dialog box.

Pseudowires — Templates — Edit Details Of SAToP Template Dialog Box

Description Use the Edit Details Of SAToP Template dialog box to modify details of SAToP templates, which can be later used to create pseudowires.

Navigation Click Provisioning > Pseudowires > Templates, and click the template name.

Permissions Superuser

Elements Name—Enter the name of the SAToP template.

Comment—Enter a comment.

Payload Size—Enter a value between 1 and 1024.

Idle Pattern—Enter a value between 00 and FF.

Excessive Packet Loss Threshold—Enter a value between 1 and 100.

Excessive Packet Loss Sample Period—Enter a value between 1000 and 6535 milliseconds.

Jitter Buffer Latency—Enter a value in milliseconds.

Control Word check box—Select this check box to enable the control word.

Save button—Click this button to save the new SAToP template.

Cancel button—Click this button to go back to the Templates dialog box.

Pseudowires — Templates — Edit Details of ATM Template Dialog Box

Description Use the Edit Details of ATM Template dialog box to modify details of ATM templates, which can be later used to create pseudowires.

Navigation Click Provisioning > Pseudowires > Templates, and click the name of the template.

Permissions Superuser

Elements Name—Enter the name of the new ATM template.

Comment—Enter a comment.

Bandwidth—Enter the bandwidth to be allocated to the pseudowire.

Control Word check box—Select this check box to enable the control word.

Encapsulation drop-down list box—Select an appropriate encapsulation type.

Save button—Click this button to save the new ATM template.

Cancel button—Click this button to go back to the Templates dialog box.

Pseudowires — Templates — Edit Details of Ethernet Template Dialog Box

Description Use the Edit Details Of Ethernet Template dialog box modify details of Ethernet templates, which can be later used to create pseudowires.

Navigation Click Provisioning > Pseudowires > Templates, and click the template name.

Permissions Superuser

Elements Name—Enter the name of the new Ethernet template.

Comment—Enter a comment.

Bandwidth—Enter the bandwidth to be allocated to the pseudowire.

Control Word check box—Select this check box to enable the control word.

Encapsulation drop-down list box—Select an appropriate encapsulation type.

Save button—Click this button to save the new Ethernet template.

Cancel button—Click this button to go back to the Templates dialog box.

Pseudowires — Provision L2circuit Pseudowires — Select Device Dialog Box

Description The Provision Pseudowires wizard has four steps, of which Select Device is the first step. Use the Provision L2circuit Pseudowires— Select Device dialog box to select the source and destination devices across which pseudowires are to be configured.

Navigation Click Provisioning > Pseudowires > Provision L2circuit Pseudowires.

Permissions Superuser, read-write

Elements Select Device Source allows you to select whether you wish to select devices directly or select a device group:

- Select Device(s) Directly option button—Select this option button if you wish to select devices directly. If you select this option button, select devices under Select Source/Destination Endpoint Devices.
- Select a Device Group option button—Select this option button and select a device group from the drop-down list box.

Find Devices that include the following: allows you to search and display available devices.

Select a Field drop-down list box—Select from: Device Name, Device Hostname, Model, Location, or Comment.

Select an Operator drop-down list box—Select an operator from the drop-down list box and enter a value in the text box beside it.

Show button—Click this button to display all the devices that meet the criteria you specified.

Clear button—Click this button to clear the list of devices.

Select Devices—Select at least two devices. Press the Shift key and click the device names to select multiple devices.

Next button—Click this button to go to the next step in the wizard.

Pseudowires — Provision L2circuit Pseudowires — Add/Edit/Delete Pseudowires Dialog Box

Description Use the Add/Edit/Delete Pseudowires dialog box to create, modify, or delete pseudowires.

Navigation Click Provisioning > Pseudowires > Provision L2circuit Pseudowires, and then click Next in the Select Device dialog box after entering the details.

Permissions Superuser, read-write

Elements Source Device Name drop-down list box—Select a source device from the drop-down list box.

Destination Device Name drop-down list box—Select a destination device from the drop-down list box.

Interface Type drop-down list box—Select an interface type from the drop-down list box.

Select Template drop-down list box—Select a template you have earlier defined from the drop-down list box.

Select Tunnel drop-down list box—Select a tunnel you have earlier created from the drop-down list box.

Virtual Circuit ID—Enter the virtual circuit ID for the pseudowire.

Description—Enter a description of the pseudowire.

VPI—Common for both source and destination endpoints. Applicable only to ATM pseudowires.

VCI—Common for both source and destination endpoints. Applicable only to ATM pseudowires.

VLAN ID—Common for both source and destination endpoints. Applicable only to Ethernet pseudowires.

Provide Source Endpoint Details: allows you to enter details of the source endpoint as follows:

- CE Interface—Select the CE facing interface from the drop-down list box.
- Logical Unit—Enter the logical unit for the CE interface.
- LSP Name—Select an LSP from the drop-down list box.
- Select GRE Interface—Select a GRE interface from the drop-down list box if you have selected a GRE tunnel in the Select Tunnel drop-down list box.
- Logical Unit—Enter the logical unit for the GRE interface.

Provide Destination Endpoint Details: allows you to enter details of the destination endpoint as follows:

- CE Interface—Select the CE facing interface from the drop-down list box.
- Logical Unit—Enter the logical unit for the CE interface.
- LSP Name—Select an LSP from the drop-down list box.
- Select GRE Interface—Select a GRE interface from the drop-down list box if you have selected a GRE tunnel in the Select Tunnel drop-down list box.
- Logical Unit—Enter the logical unit for the GRE interface.

Add Entry button—Click this to add the pseudowire or save the modifications you made.

Edit button—Click this to make modifications to the pseudowire details.

Delete button—Click this to delete the tunnel.

Force Deploy button—Click this to push the configuration details to the devices even if you have not modified them.

Previous button—Click this to go to step 1: Select Device dialog box.

Next button—Click this to go to step 3: Confirm Add/Edit/Delete Pseudowires dialog box.

The table at the bottom of the wizard displays:

- State: State can be one of the following:
  - New: If the pseudowire is new.
  - Modified: If a exiting pseudowire is modified.
  - Unchanged: If a existing pseudowire is unchanged.
- Source Device Name
- Source CE Interface
- Destination Device Name
- Destination CE Interface
- Virtual Circuit ID

Pseudowires — Provision L2circuit Pseudowires — Confirm Add/Edit/Delete Pseudowires Dialog Box

Description Use the Confirm Add/Edit/Delete Pseudowires dialog box to confirm the operation you performed in the Add/Edit/Delete Pseudowires dialog box.

Navigation Click Provisioning > Pseudowires > Provision L2circuit Pseudowires and click Next in the Select Device dialog box, and then click Next in the Add/Edit/Delete Pseudowires dialog box after creating, modifying or deleting a pseudowire

Permissions Superuser, read-write

Elements Confirm button—Click this to confirm creation, modification, or deletion of pseudowires.

Previous button—Click this to go back to the Add/Edit/Delete Pseudowires dialog box.

The tabular area at the bottom of the dialog displays the following details:

- Operation—Creation, Modification, or Deletion.
- Virtual Circuit ID—Displays the virtual circuit ID.
- Source Device—Dispays the source device name.
- Source CE Interface—Displays the source CE interface.
- Destination Device—Dispays the destination device name.
- Destination CE Interface—Displays the destination CE interface.

Pseudowires — Provision L2circuit Pseudowires — Select Time or Schedule Dialog Box

Description Use the Select Time or Schedule dialog box to set up the time or schedule for the creation, modification, or deletion of the pseudowires carried out in the earlier steps of the wizard.

Navigation Click Provisioning > Pseudowires > Provision L2circuit Pseudowires and click Next in the Select Device dialog box after entering the details, then click Next in the Add/Edit/Delete Pseudowires dialog box, and then click Confirm in the Confirm Add/Edit/Delete Pseudowires dialog box.

Permissions Superuser, read-write

Elements Select Time or Save Operation: allows you to save the operation or set up the time or schedule.

Now option button—Select this option to carry out the operation now.

Save Operation option button—Select this option and enter a name for the operation to save the configuration as a named operation.

Select Schedule option button—Select this option button and select a schedule from the table below to set up the operation to be carried out at the specified time.

The table at the bottom of the dialog box lists the schedules configured in the Settings tab, giving the following details:

- Schedule Name
- Start Time
- Period (frequency)
- Comment

OK button—Click OK after selecting an option to set up the schedule or save the operation.

Previous button—Click this to go back to the Confirm Add/Edit/Delete Pseudowires dialog box.

Pseudowires — Filter and Test l2circuit Pseudowires Dialog Box

Description Use the Filter and Test l2circuit Pseudowires dialog box to filter pseudowires based on one of the many criteria provided and test them.

Navigation Click Provisioning > Pseudowires > Filter and Test l2circuit Pseudowires.

Permissions Superuser, read-write, read-only

Elements The following criteria are available for filtering pseudowires and displaying results:

- All Pseudowires—Displays all pseudowires.
- Select Device Groups—Displays pseudowires configured on the selected device groups. Press the Shift key to select multiple device groups.
- Select Devices—Displays pseudowires configured on the selected devices. Press the Shift key to select multiple devices. You must select at least two devices.
- Select Pseudowire Endpoints—Select pseudowire endpoints from the drop-down list boxes. Displays the pseudowires configured between the selected endpoints.
- Virtual Circuit ID—Displays the pseudowires with the Virtual Circuit ID you enter.

OK button—Click OK after specifying the filtering criterion to display results.

Pseudowires — Filter and Test l2circuit Pseudowires (results) Dialog Box

Description This dialog box lists the pseudowires according to the criteria you specified.

Navigation Click Provisioning > Pseudowires > Filter and Test l2circuit Pseudowires, and then click OK after specifying the criteria.

Permissions Superuser, read-write, read-only

Elements View button—Select a pseudowire from the list and click View to monitor the pseudowire.

Test button—Select a pseudowire and click Test to verify if the pseudowire is active.

The list of pseudowires provides the following information about the pseudowires.

- Source Device Name
- Source Interface
- Destination Device Name
- Destination Interface
- Virtual Circuit ID

Pseudowires — Filter and Test l2circuit Pseudowires (Test Results) Dialog Box

Description This dialog box displays the status of the pseudowire and a message from Junoscope.

Navigation Click Provisioning > Pseudowires > Filter and Test l2circuit Pseudowires and click OK after specifying the criteria, and then click Test after selecting one or more pseudowires.

Permissions Superuser, read-write, read-only

Elements Previous button—Click this to go back to the list of pseudowires (results) dialog box.

The table at the bottom of this dialog box displays the following information:

- Source Device
- Destination Device
- Virtual Circuit ID
- Status
- Message

Pseudowires — Filter and Test l2circuit Pseudowires (View Results) Dialog Box

Description This dialog box lists out the details of the source and destination end points of the selected pseudowire.

Navigation Click Provisioning > Pseudowires > Filter and Test l2circuit Pseudowires and click OK after specifying the criteria, and then click View after selecting one or more pseudowires.

Permissions Superuser, read-write, read-only

Elements Virtual Circuit Details

- Virtual Circuit Id: field— Displays the identify number of the virtual circuit

Source Endpoint Details

- Source Device: field— Displays the name of the source device
- Maximum Cell Concatenation: field— Displays the maximum number of ATM cells that can be concatenated before the packet switched network (PSN) packet is sent out.
- Control Word: field— Displays whether the control word was enabled or disabled.
- Encapsulation: field— Displays the encapsulation type.
- Bandwidth: field— Displays the bandwidth that was specified for the pseudowire.
- Mode: field— Displays the mode that was specified for the pseudowire.
- VCI: field— Displays the virtual circuit identifier of the pseudowire. This is only applicable for ATM pseudowires.
- Sequence Number Switchover: field— Displays whether the sequence number switchover was enabled or disabled.
- Timeout: field— Displays the maximum time that the device should wait for the specified number of ATM cells to arrive for concatenation.
- Sequence Number Check: field— Displays whether the sequence number check was enabled or disabled.
- VPI: field— Displays the virtual path identifier of the pseudowire. This is only applicable for ATM pseudowires.

Destination Endpoint Details

- Destination Device: field— Displays the name of the destination device
- Maximum Cell Concatenation: field— Displays the maximum number of ATM cells that can be concatenated before the packet switched network (PSN) packet is sent out.
- Control Word: field— Displays whether the control word was enabled or disabled.
- Encapsulation: field— Displays the encapsulation type.
- Bandwidth: field— Displays the bandwidth that was specified for the pseudowire.
- Mode: field— Displays the mode that was specified for the pseudowire.
- VCI: field— Displays the virtual circuit identifier of the pseudowire. This is only applicable for ATM pseudowires.
- Sequence Number Switchover: field— Displays whether the sequence number switchover was enabled or disabled.
- Timeout: field— Displays the maximum time that the device should wait for the specified number of ATM cells to arrive for concatenation.
- Sequence Number Check: field— Displays whether the sequence number check was enabled or disabled.

- VPI:field— Displays the virtual path identifier of the pseudowire. This is only applicable for ATM pseudowires.

Previous button— Click this button to go back to the Filter and Test L2circuit Pseudowire dialog box.

RADIUS Configuration—Add RADIUS Configuration Dialog Box

Description Use the Add RADIUS Configuration dialog box to add or copy a RADIUS server configuration to the JUNOScope software database. To save a copied RADIUS configuration, you must change either the RADIUS server DNS name or IP address and port number.

Navigation Click Settings > RADIUS Configuration. Then, click Add or Copy in the RADIUS Server Configuration dialog box.

Permissions Superuser

Elements RADIUS Server DNS Name or IP Address text box—Type the DNS name or IP address of the RADIUS server. The name must be less than 40 characters.

RADIUS Authentication Port No. text box—Type a unique port number for the RADIUS server. The default value for this field is 1812. The port number value must be between 1 and 65,535. The RADIUS server DNS name or IP address and port number combination must be unique to the system.

RADIUS Accounting Port No. text box—(This text box is disabled until you enable the RADIUS accounting port.) Type the RADIUS accounting port in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535. The RADIUS Accounting port number is optional. If the RADIUS Accounting port is disabled, the RADIUS Accounting Port No. column displays DISABLED in the RADIUS Configuration Entry table.

Enable RADIUS Accounting Port? check box—Click the check box to enable the specified RADIUS accounting server port. This action enables the RADIUS Accounting Port No. text box.

RADIUS Server Secret text box—Type the RADIUS server secret. The secret must be less than 40 characters.

Confirm RADIUS Server Secret text box—Retype the RADIUS server secret to confirm it.

OK button—Adds the RADIUS configuration entry to the JUNOScope software database and redisplays the RADIUS server Configuration dialog box with the new RADIUS server DNS name or IP address and RADIUS server port number listed in the table.

Cancel button—Clears this dialog box without adding a new RADIUS configuration entry.

RADIUS Configuration—Edit RADIUS Configuration Dialog Box

Description Use the Edit RADIUS Configuration dialog box to edit an existing configuration. You can change either the RADIUS server DNS name or IP address, port number, or the server secret.

Navigation Click Settings > RADIUS Configuration. Then, click Edit in the RADIUS Server Configuration dialog box.

Permissions Superuser

Elements RADIUS Server DNS Name or IP Address text box—Type the DNS name or IP address of the RADIUS server. The name must be less than 40 characters.

RADIUS Server Port Number text box—Changes the unique port number for the RADIUS server. The default value for this field is 1812. The port number value must be between 1 and 65,535. The RADIUS server DNS name or IP address and port number combination must be unique to the system.

RADIUS Accounting Port No. text box—(This text box is disabled if the RADIUS accounting port is disabled.) Type the RADIUS accounting port in the text box. The accounting port is the port from which the JUNOScope software maintains a record of the loggable activities a user has performed. The default port number is 1813. The port number value must be between 1 and 65,535. The RADIUS Accounting port number is optional. If the RADIUS Accounting port is disabled, the RADIUS Accounting Port No. column displays DISABLED in the RADIUS Configuration Entry table.

Enable RADIUS Accounting Port? check box—Click the check box to enable the specified RADIUS accounting server port. This action enables the RADIUS Accounting Port No. text box.

RADIUS Server Secret text box—Changes the RADIUS server secret. The secret must be less than 40 characters.

Confirm RADIUS Server Secret text box—Retype the RADIUS server secret to confirm it.

OK button—Adds the edited RADIUS configuration entry to the JUNOScope software database. The RADIUS dialog box reappears with the edited RADIUS configuration entry displayed in the table.

Cancel button—Clears this dialog box without changing the RADIUS configuration entry.

RADIUS Configuration—Import RADIUS Configuration Dialog Box

Description Use the Import RADIUS Configuration dialog box to import RADIUS server configuration records from another JUNOScope server. Importing RADIUS server configuration information is useful when you do not want to add entries manually. The default filename for RADIUS configuration data is junoscope-radiusClients.xml.

Navigation Click Settings > RADIUS Configuration. Then, click Import in the RADIUS Server Configuration dialog box.

Permissions Superuser

Elements File text box—Lets you type or browse to the RADIUS configuration XML file to import. The default filename is junoscope-radiusClients.xml.

Browse button—Displays the File Open dialog box so you can select the RADIUS configuration XML file to import.

Import button—Imports the selected RADIUS configuration data into the JUNOScope software database. The information is displayed in the Access Methods dialog box.

Cancel button—Clears this dialog box and displays the RADIUS Configuration dialog box.

Restore—Confirm Your Selections Dialog Box

Description Use the Restore—Confirm Your Selections dialog box to confirm whether you want to finish a selected operation, such as Restore Archive.

Navigation Click Configuration > Repository > Restore. Select the device to which you want to restore an archived configuration in the Restore—Select Device dialog box, and click Next. Select a configuration revision to restore in the Restore—Select Configuration Revision dialog box, and click Next.

Permissions Superuser, read-write

Elements Please Confirm Operation display field—Displays the operation, the device or group from which the operation will be performed, and the schedule for you to confirm whether or not you want it to occur.

Finish button—Executes the operation. An operation progress message appears, and the Requested Operation Status dialog box appears displaying the status of the operation by device name, operation status, start time, last updated time, and the operation status message.

Previous button—Redisplays the previous operation dialog box and does not execute the operation.

Cancel button—Cancels the operation and displays the Configuration > Repository menu.

Restore—Select Configuration Revision Dialog Box

Description Use the Restore—Selected Configuration Revision dialog box to select an available configuration to restore to the selected device. The available configurations are either archived from the selected device or imported from the local file system and stored in the JUNOScope software CVS repository. The configurations are listed by date, revision level, and comment.

Navigation Click Configuration > Repository > Restore. Select a device in the Restore—Select Options dialog box, and click Next.

Permissions Superuser, read-write

Elements Configuration Revisions table—Lists the configuration files archived from a router or imported from the local file system by date, revision level, and comment. Select a configuration to restore to the selected device.

Synchronize Routing Engines check box—On a router with redundant Routing Engines, the JUNOScope software synchronizes the restoration of a configuration on the master and backup Routing Engine. This option is not available when you have selected a BXOS device for restoring the configuration.

Sync the Startup config with Running check box— On a BXOS device, JUNOScope synchronizes the running configuration with the startup configuration if this option is selected. If this option is not selected, only the running configuration is updated after the restore operation. This option is displayed only when you have selected a BXOS device for restoring configuration.

Select Time or Save Operation area:

- Now option button—Runs the restore configuration operation as soon s you click Next and confirm the operation settings.
- Save Operation as text box—Type a unique name for the restore configuration operation you want to save. The saved restore operation appears in the Saved Operations page. To view the Saved Operations page, click Settings > Saved Operations.

Previous button—Redisplays the Restore—Select Options dialog box.

Next button—Displays the Restore—Confirm Your Selections dialog box so you can confirm the Restore operation.

Cancel button—Clears this dialog box and redisplays the Configuration > Repository menu.

Restore—Select Options Dialog Box

Description Use the Restore—Select Options dialog box to select the router to which you want to upload a configuration file stored in the JUNOScope software CVS repository.

Navigation Click Configuration > Repository > Restore.

Permissions Superuser, read-write

Elements Device list box—Select a device to which to restore a configuration. Click the down arrow to display the available devices.

Configuration File list box—Select the name of the imported configuration file to restore to the selected device. Click the down arrow to display filenames of the available imported configuration files.

Next button—Displays the Restore—Selected Configuration Revision dialog box from which you can select a configuration file to restore to the selected device.

Cancel button—Clears this dialog box and re-displays the Configuration > Repository menu.

Save—Select Configuration Revision Dialog Box

Description Use the Select Configuration Revision dialog box to select the configuration revision of the configuration file you want to save.

Navigation Click Configuration > Repository > Save. Select a device from which to save configuration, or select an imported configuration filename in the Select Options dialog box. Select the configuration revision in the Select Configuration Revision dialog box and click Next.

Permissions Superuser, read-write

Elements Archived Date column—Lists the dates on which the configuration was archived.

Revision column—Lists the current revision of the configuration.

Comment column—Lists optional descriptive comments about the configuration file.

Next button—Displays the File Download dialog box for confirmation of file download to a local machine.

Cancel button—Clears this dialog box and displays the Configuration Repository dialog box.

Previous button—Displays the Select Options dialog box.

Save—Select Options Dialog Box

Description Use the Select Options dialog box to select a configuration file that you want to save to a local machine.

Navigation Click Configuration > Repository > Save.

Permissions Superuser, read-write

Elements Configuration File list box—Lists the configuration files in the CVS repository. Select the name of the configuration file to save to the local machine.

Device list box—Lists the devices on which the configuration file is archived. Select a device from which to save the archived configuration file.

Next button—Click to display the Configuration Revision dialog box from which you can select the revision of a configuration file to save to a local machine.

Cancel button—Clears this dialog box and displays the Configuration Repository dialog box.

Saved Operations—Add Compound Operation Dialog Box

Description Use the Saved Operations Add Compound Operation dialog box to create compound operations from saved simple and compound archive, restore, and inventory scan operations and run them concurrently or sequentially.

Navigation Click Settings > Saved Operations. On the Saved Operations page, click Add.

Permissions Superuser, read-write

Elements Name text box—Type a unique name for the compound operation that you want to add.

Comment text box—Type a comment describing the compound operation that you want to add.

Concurrent option button—Runs the operations in a compound operation in parallel or in no specified order.

Sequential option button—Runs the operations in a compound operation in a specified order. For example, restore Router 1, archive Router 1, then scan Router 1.

Available Operations list box—Lists all simple and compound archive, restore, and inventory scan operations that have been saved. Shift + click or Ctrl + click to select multiple saved operations to add.

Actions buttons—The Actions area in the dialog box includes the following buttons:

- Add button—Moves the selected saved operation(s) from the Available Operation list box to the Selected Operations list box. This button is enabled when you select one or more saved operations in the Available Operations list box. Shift + click or Ctrl + click to select multiple saved operations to add.
- Remove button—Moves a selected simple or compound operation from the Selected Operations list box back to the Available Operations list box.This button is enabled when you select one or more saved operations in the Selected Operations list box.
- Add All button—Adds all of the saved simple and compound operations listed in the Available Operations list box to the Selected Operations list box at the same time.
- Remove All button—Moves all of the saved simple or compound operation listed in the Selected Operations list box back to the Available Operations list box at the same time.
- Move Up button—Moves a saved simple or compound operation up one line in the Selected Operations list box. This button is available only when you select to create a sequential compound operation.
- Move Down button—Moves a saved simple or compound operation down one line in the Selected Operations list box. This button is available only when you select to create a Sequential compound operation.

Selected Operations list box—Lists the simple or compound operations that you want to be included in a compound operation. If you are creating a sequential operation, the order of the operations listed in this list box is the order that the operations will be executed when run.

OK button—Saves a compound operation with the name, comment, run method, the operations you want to be included, and the order in which you want operations run.

Cancel button—Clears the Saved Operations Add Compound Operation dialog box with out adding a compound operation. The Saved Operations page appears.

Saved Operations—Assign Devices Dialog Box

Description Use the Saved Operations Assign Devices dialog box to assign devices to a saved operation and to determine when to run the saved operation: now, save it for later use, or at a scheduled interval.

Navigation Click Settings > Saved Operations. On the Saved Operations page, click Assign Devices.

Permissions Superuser, read-write

Elements Select Devices section:

- Group option button and drop-down list box—Enables you to select the group of devices to assign to the operation. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any router groups, the Groups drop-down list box is empty.
- Selected Devices option button and drop-down list box—Enables you to select a device to assign to the operation. Click the Devices option button, then select the devices in the Devices drop-down list box that you want to assign to the operation. Shift + click or Ctrl + click to select multiple devices. If you have not added any routers, the drop-down list box is empty.

Select Time or Save Operation section:

- Now check box—Select to have the operation occur as soon as the command is executed.
- Save Operation as text box—Type a name for the operation. The saved operation appears in the Saved Operations page under the assigned name. To view the Saved Operations page, click Settings > Saved Operations.
- Select Schedule area—Lets you select a schedule for when you want the operation to occur.

OK button— Depending on time that you selected, one of the following will occur.

- If you selected the Now option, the View Status Records dialog box is displayed.
- If you selected the Save Operation as option, the Confirm Run Saved Operation dialog box is displayed.
- If you selected the Select Schedule option and selected a schedule, the operation runs when the operation is scheduled to be run.

Cancel button—Clears this dialog box and redisplays the Saved Operation dialog box.

Saved Operations—Confirm Run Saved Operations Dialog Box

Description Use the Saved Operations Confirm Run Saved Operation dialog box to view the details of an operation that you have selected to run at a specified time. The dialog box displays the selected saved operation name and indicates that the operation has been successfully scheduled using the selected schedule name.

Navigation Click Settings > Saved Operations. On the Saved Operations page, click Run. In the Run Saved Operation dialog box click the Select Schedule button, select the option button for the schedule you want to use, then click Next.

Permissions Superuser, read-write

Elements Operation text area—Displays the selected saved operation name and indicates that the operation has been successfully scheduled using the selected schedule name.

OK button—Confirms the saved operation that you want to run has been successfully scheduled to run.

Saved Operations—Edit Compound Operation Dialog Box

Description Use the Edit Compound Operation dialog box to modify the setup of a saved compound operation that you have created. You can modify the compound operation name, comment, run method, what operations you want included, and the order in which you want operations in a sequential operation to run. You can only edit saved compound operations. You can't edit saved simple operations that consist of one operation that you want to run.

Navigation Click Settings > Saved Operations. On the Saved Operations page, click Edit.

Permissions Superuser, read-write

Elements Name text box—Modify the name for the compound operation.

Comment text box—Modify the comment for the compound operation.

Concurrent option button—Change whether you want the operations in the saved compound operation to run concurrently—in parallel or in no specified order.

Sequential option button—Change whether you want the operations in the saved compound operation to run sequentially—in a specified order. For example, restore Router 1, archive Router 1, then scan Router 1.

Available Operations list box—Lists the simple and compound operations that have been saved. Shift + click or Ctrl + click to select multiple saved operations to add.

Actions buttons—The Actions area in the dialog box includes the following buttons:

- Add button—Moves the selected saved operation(s) from the Available Operation list box to the Selected Operations list box. This button is enabled when you select one or more saved operations in the Available Operations list box. Shift + click or Ctrl + click to select multiple saved operations to add.

- Remove button—Moves a selected simple or compound operation from the Selected Operations list box back to the Available Operations list box.This button is enabled when you select one or more saved operations in the Selected Operations list box.

- Add All button—Adds all of the saved simple and compound operations listed in the Available Operations list box to the Selected Operations list box at the same time.

- Remove All button—Moves all of the saved simple or compound operation listed in the Selected Operations list box back to the Available Operations list box at the same time.

- Move Up button—Moves a saved simple or compound operation up one line in the Selected Operations list box. This button is available only when you select to create a sequential compound operation.

- Move Down button—Moves a saved simple or compound operation down one line in the Selected Operations list box. This button is available only when you select to create a Sequential compound operation.

Selected Operations list box—Lists the simple or compound operations that you want to include in a compound operation. If you are creating a sequential operation, the order of the operations listed is the order that the operations will be executed when run.

OK button—Saves the changes you made to a saved compound operation.

Cancel button—Clears the Saved Operations Add Compound Operation dialog box without saving changes to a compound operation. The Saved Operations page appears.

Saved Operations—Import Dialog Box

Description Use the Import Saved Operations dialog box to import existing saved operations to the local file system in XML file format.

Navigation Settings > Saved Operations. Click Import in the Saved Operations table dialog box.

Permissions Superuser

Elements File text box—Type or browse to the labels XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

Browse button—Displays the File Open dialog box from which you can select the XML file to import.

Import button—Imports the selected saved operations data into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears this dialog box and displays the Saved Operations table dialog box.

Saved Operations—Run Saved Operation Dialog Box

Description Use the Run Saved Operation dialog box to run a selected simple or compound operation immediately or at a scheduled time interval.

Navigation Click Settings > Saved Operations. On the Saved Operations page, click Run.

Permissions Superuser, read-write

Elements Name display area—Displays the name of the saved operation you want to run.

Comment text box—Displays the comment for the compound operation.

Select Time option buttons—Lets you select when you want the selected operation to run. The Select Time option buttons are as follows:

- Now option button—Runs the displayed saved operation immediately after you click the OK button.
- Select Schedule option button—Runs the displayed saved operation according to the schedule that you select in the available schedule table.

Available Schedule table—Displays the schedules that have been set up in JUNOScope. Click a schedule option button to select it. The operation will run at the scheduled time interval.

OK button—Runs the saved operation immediately or schedules it to be run at the scheduled interval.

Cancel button—Cancels the Run Saved Operation dialog box without running the selected operation.

Saved Operations—Saved Operations Dialog Box

Description Use the Saved Operations dialog box to view the saved simple and compound archive, restore, and inventory scan operations by name, comment, and actions.

You can save simple archive, restore, and inventory scan operations with a unique name in the respective JUNOScope user interfaces. You can save compound operations from the Add Compound Operation dialog box by clicking the Add button.

From the Saved Operations dialog box, you can add saved operations to create compound operation and run, delete, view, or edit them.

Navigation Click Settings > Saved Operations.

Permissions Superuser, read-write

Elements Available Saved Operations table—Lists the simple and compound operations that you have saved. The table includes the following columns:

Name column—The name of the saved simple or compound operation. The list is stored by saved operation name in ascending order. To sort operations in descending order, click the sort icon in the Name column header.

Comment column—The comment describing a saved simple or compound operation given when a simple operation is saved.

Actions column—Displays the actions you can perform on a saved simple or compound operation. The available actions are as follows:

- Run link—Displays the Run Saved Operation dialog box for you to determine when you want the operation to run: now or at a scheduled interval.
- Delete link—Deletes the saved operation from the Saved Operations table. If you want to delete an operation that is already scheduled to be run, click Monitor > Operations.
- View link—Displays the View Simple Operation dialog box from which you can view a simple operation name, operation type, comment, and the devices or groups upon which the operation will run. The View action is available for simple operations.
- Assign Devices link—Displays the Assign Devices for Running Saved Operation dialog box from which you can assign devices to a saved operation and to determine when you want the operation to run: now, save the operation for later, or at a scheduled interval.
- Edit link—Displays the Edit Compound Operation dialog box from which you can edit a compound operation name, comment, run method, what operations you want included, and the order in which a sequential operation runs. The Edit operation is only available for compound operations.

Add button—Displays the Add Compound Operation dialog box so you can combine saved simple and compound operations to make compound ones that can run concurrently or sequentially.

Export button—Displays the File Download dialog box to export the authentication policy data in XML file format to the computer file system. The default authentication policy export filename is junoscope-operations.xml.

Import button—Imports user saved operations data from the computer file system into the JUNOScope software. The Import Results dialog box appears.

Saved Operations—View Simple Operations Dialog Box

Description Use the View Simple Operation dialog box to view the settings of a saved simple operation, including operation name, operation type, comment, and the devices and groups upon which the operation will run.

Navigation Click Settings > Saved Operations. On the Saved Operations page, click View for an operation. If an operation has an Edit link instead, it is a compound operation.

Permissions Superuser, read-write

Elements Operation Name display area—Displays the name of the saved simple operation. You can save archive, restore, and inventory scan operations with a unique name.

Operation Type display area—Displays the type of saved simple operation. You can save archive, restore, and inventory scan operations.

Comment display area—Displays the comment to describe a saved simple operation. You can save archive, restore, and inventory scan operations.

Devices or Groups display area—Displays the names of the devices or groups upon which a simple operation will run.

Configuration display area—Displays the archived configuration or the name of the imported configuration file.

Revision display area—Displays the revision of the configuration file to be restored.

Load Action display area—Displays how the configuration was restored to the device: override, replace, or merge.

Synchronize Routing Engines display area—Displays whether the Routing Engines on the device are synchronized: true or false.

OK button—Clears the View Simple Operation dialog box and redisplays the Saved Operations page.

Schedules Dialog Box

Description Use the Schedules dialog box to view the list of schedules created for operations, such as archive. The Schedules dialog box is empty until you add a schedule. The Schedules dialog box lists schedules by schedule name, start time, time interval, and comment. From the Schedules dialog box, you can add new and edit existing schedules.

Navigation Click Settings > Schedules.

Permissions Superuser

Elements Schedule table—The schedule table in the Schedules dialog box is populated when you add schedules for operations, such as archive. Each schedule is listed by schedule name, start time, time interval, and comment. Select a schedule to copy, edit, or delete.

Add button—Displays the Add Schedule dialog box so you can add a new schedule for JUNOScope operations, such as archive.

Copy button—Copies the selected schedule in the JUNOScope database. A 1 (one) appears after the copied schedule and increments sequentially each time you copy the same schedule. Select a schedule to copy.

Edit button—Displays the Edit Schedule dialog box so you can edit an existing operations schedule. Select a schedule to edit.

Delete button—Deletes an existing schedule. Select the schedule that you want to edit before clicking Delete. If a schedule is used in an operation, you must first delete the operations that are using that schedule from the Manage Operations task, then delete the schedule from the Schedules dialog box. Select a schedule to delete.

Export button—Displays the File Download dialog box to export the setup data in XML file format to the computer file system. The default schedules export filename is junoscope-schedules.xml.

Import button—Displays the Import dialog box for you to specify the import XML file to import.

Schedules—Add Schedule Dialog Box

Description Use the Add Schedule dialog box to add a schedule for an operation, such as archive.

A schedule is an independent entity that has no effect until you use it for an operation, such as archive. When you set up a schedule you are not doing anything operation related. You can use the same schedule for multiple operations. When you want to see information about when an operation ran and when it is scheduled to run again, use the Manage Operations command.

Navigation Click Settings > Schedules. Click Add in the Schedules dialog box.

Permissions Superuser

Elements Schedule Name text box—Type a descriptive name for the schedule you want to add. The name must be 20 characters or less.

Start Date drop-downlist boxes—Specify the date when you want an operation to run. The scheduler defaults to the current date. Select the month from the drop-down list box, the day from the drop-down list box, and type the year in the text box.

Start Time drop-downlist boxes—Specify the time when you want an operation to run. The scheduler uses a 24-hour clock and defaults to 00:00:00. Select the hour, minutes, and seconds from the drop-down list boxes.

Time Interval drop-downlist box—Select when you want the operation to reoccur. Click the down-arrow to see the available time interval options.

Comment text box—Type an optional descriptive comment about the schedule. The comment must be 20 characters or less.

OK button—Adds a new schedule in the Schedules dialog box.

Cancel button—Clears this dialog box without adding a new schedule.

Schedules—Edit Schedule Dialog Box

Description Use the Edit Schedule dialog box to change an existing schedule for an operation, such as archive.

Navigation Click Settings > Schedules. Select the schedule that you want to edit in the Schedules dialog box, and click Edit.

Permissions Superuser

Elements Schedule Name text box—Type a descriptive name for the schedule you want to add. The name must be 20 characters or less.

Start Date drop-down list boxes—Specify the date when you want an operation to run. The scheduler defaults to the current date. Select the month from the drop-down list box, the day from the drop-down list box, and type the year in the text box.

Start Time drop-down list boxes—Specify the time when you want an operation to run. The scheduler uses a 24-hour clock and defaults to 00:00:00. Select the hour, minutes, and seconds from the drop-down list boxes.

Time Interval drop-down list box—Select when you want the operation to recur. Click the down-arrow to see the available time interval options.

Comment text box—Type a descriptive comment about the schedule. The comment must be 20 characters or less.

OK button—Saves the changes and redisplays the Schedules dialog box.

Cancel button—Clears this dialog box without saving any schedule changes.

Schedules—Import Schedules Dialog Box

Description Use the Import Schedules dialog box to import schedule setup information into the JUNOScope software without having to manually enter it. The default import filename for schedules is junoscope-schedules.xml.

Navigation Click Settings > Schedules. Click Import in the Schedules dialog box.

Permissions Superuser

Elements File to import text box—Lets you type or browse to the XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

Browse button—Displays the File Open dialog box so you can select the XML file to import.

Import button—Imports the selected device data into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears this dialog box and displays the Schedules dialog box.

Scripts—Compare—Compare Dialog Box

Description Use the Compare dialog box to compare the revisions of a script.

Navigation Click Configuration > Repository > Scripts. Select a script and click Compare in the Actions column in the Scripts dialog box. Select the revisions of the script you want to compare in the Select Revision dialog box and click Compare.

Permissions Superuser, read-write

Elements Compare of revision X to revision Y display field—Displays the differences between the two compared script files. Displays the name of the script and the revision numbers which are being compared. By default, the newer revision is compared to the older one, The latest revision appears on the left; the older revision on the right. The differences between the two configurations are highlighted. See the Legend for an explanation of the highlighting.

Scripts—Compare—Select Revision Dialog Box

Description Use the Select Revision dialog box to select the revisions of a script you want to compare.

Navigation Click Configuration > Repository > Scripts. Select a script and click Compare in the Actions column in the Scripts dialog box.

Permissions Superuser, read-write

Elements Modified Date column—Lists the dates on which scripts were modified.

Revision column—Lists the current revision number of the scripts.

Comment column—Lists the optional comments entered while importing the scripts.

Compare button—Compares the revisions of the script.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Scripts—Delete—Confirm Deletion Dialog Box

Description Use the Confirm Deletion dialog box to confirm the deletion of a script.

Navigation Click Configuration > Repository > Scripts. Select the script you want to delete and click Delete in the Scripts dialog box.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the script or scripts that are being deleted permanently from the CVS repository,

Scripts—Deploy—Confirm Selection Dialog Box

Description Use the Confirm Selections dialog box to confirm the selections you made for the deploy operation.

Navigation Click Configuration > Repository > Scripts. Select the script you want to deploy and click Deploy in the Actions column in the Scripts dialog box. Select the revision of the script you want to deploy in the Select Script Revision and Options dialog box and click Next. Select the router or group of routers to which to deploy and the time at which to perform the deploy operation and click Next in the Specify Devices and time dialog box.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the script that is being deployed and the devices or groups to which it is being deployed. It also lists the deploy options that you have selected.

Finish button—Executes the operation. The Status—View Status Records dialog box appears displaying the status of the deploy operation.

Previous button—Redisplays the Specify Devices and Time dialog box.

Scripts—Deploy—Select Script Revision and Options Dialog Box

Description Use the Select Script Revision and Options dialog box to select the script you want to deploy to a router or group of routers.

Navigation Click Configuration > Repository > Scripts. Select the script you want to deploy and click Deploy in the Actions column in the Scripts dialog box.

Permissions Superuser, read-write

Elements Modified Date column—Lists the dates on which scripts were modified.

Revision column—Lists the current revision number of the scripts.

Comment column—Lists the optional comments entered while importing the scripts.

Enable Script check-box—Enables the script you are deploying.

Deploy on both REs.(In case of Dual RE device) check-box—Enables you to deploy the script on to both the routing engines (in case of dual routing engines).

Verify MD5 Checksum for downloaded script option button—Select this option if you want to ensure that the downloaded software script is intact. The MD5 checksum for the downloaded script is compared with the checksum value stored in JUNOScope. If they do not match, the operation fails and the error message is displayed.

Next button—Displays the Specify Devices and Time dialog box from which you can select the devices to which to deploy the script and the time at which to perform the deploy operation.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Scripts—Deploy—Specify Devices and Time Dialog Box

Description Use the Specify Devices and Time dialog box to select the devices to which to deploy a script and the time at which to perform the deploy operation.

Navigation Click Configuration > Repository > Scripts. Select the script you want to deploy and click Deploy in the Actions column in the Scripts dialog box. Select the revision of the script you want to deploy in the Select Script Revision and Options dialog box and click Next.

Permissions Superuser, read-write

Elements Select Devices section:

- Group option button and drop-down list box—Select a router group to which to deploy a script. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any router groups, the Groups drop-down list box is empty.
- Selected Devices option button and drop-down list box—Select a router to which to deploy a script. Click the Devices option button, then select the devices in the Devices drop-down list box to which to deploy a script. If you have not added any routers, the drop-down list box is empty.

Use JUNOScope IP address for image transfer check-box— Select this option if you want the device(s)/group to connect to the JUNOScope server using the IP address of the JUNOScope server. The device(s)/group will use the IP address instead of the JUNOScope server name to connect to the server. Select the IP address from the drop-down list.

Select Time or Save Operation section:

- Now check box—Select to have the deploy operation occur as soon as the command is executed.
- Save Operation as text box—Type a name for the deploy operation that you want to save. The saved deploy operation appears in the Saved Operations page with the name that you gave it. To view the Saved Operations page, click Settings > Saved Operations.

Next button—Displays the Confirm Operations dialog box from which you can select to finish the archive operation or cancel it.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Previous button—Redisplays the Select Script Revision and Options dialog box where you can select another revision.

Scripts—Disable—Confirm Selection Dialog Box

Description Use the Confirm Selection dialog box to confirm the selections you made for the deploy operation.

Navigation Click Configuration > Repository > Scripts. Select the script you want to disable and click Disable in the Actions column in the Scripts dialog box. Select the router or group of routers to which to deploy and the time at which to perform the deploy operation and click Next in the Specify Devices and Time dialog box.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the script that is being disabled, and the devices or groups from which it is being disabled, for your confirmation.

Finish button—Executes the operation. The Status—View Status Records dialog box appears displaying the status of the deploy operation.

Previous button—Redisplays the Specify Devices and Time dialog box.

Scripts—Disable—Specify Devices and Time Dialog Box

Description Use the Specify Devices and Time dialog box to select the devices from which to disable commit scripts and op scripts and the time at which to perform the disable operation.

Navigation Click Configuration > Repository > Scripts. Select the script you want to disable and click Disable in the Actions column in the Scripts dialog box.

Permissions Superuser, read-write

Elements Select Disable Options section:

Disable on both REs.(In case of Dual RE device) check-box—Enables you to disable the script from both the routing engines (in case of dual engines).

Select Devices section:

- Group option button and drop-down list box—Select a router group from which to disable a script. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any router groups, the Groups drop-down list box is empty.
- Selected Devices option buttonanddrop-down list box—Select a router from which to disable a script. Click the Devices option button, then select the devices in the Devices drop-down list box from which to disable a script. If you have not added any routers, the drop-down list box is empty.

Select Time or Save Operation section:

- Now check box—Select to have the disable operation occur when the command is executed.
- Save Operation as text box—Type a name for the disable operation that you want to save. The saved disable operation appears in the Saved Operations page with the name that you gave it. To view the Saved Operations dialog box, click Settings > Saved Operations.

Next button—Displays the Confirm Selection dialog box from which you can select to finish the deploy operation.

Previous button—Redisplays the Select Script Revision and Options dialog box where you can select another revision.

Cancel button—Clear this dialog box and redisplays the Scripts dialog box.

Scripts—Edit—Edit Dialog Box

Description Use the Edit dialog box to edit a script in the JUNOScope CVS repository.

Navigation Click Configuration > Repository > Scripts. Select a script and click Edit in the Actions column in the Scripts dialog box. Select the revision of the script you want to edit in the Select Revision dialog box and click Edit.

Permissions Superuser, read-write

Elements Edit display box—Displays the contents of the script file that you have selected to edit.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Save button—Saves modifications to the script.

Scripts—Edit—Save Result Dialog Box

Description Use the Save Result dialog box to confirm whether an edited configuration file has been saved to the JUNOScope CVS repository.

Navigation Click Configuration > Repository > Edit. Select options and click Next in the Select Options Dialog Box. Select the configuration revision in the Select Configuration Revision dialog box and click Next. Modify the configuration file as required in the Configuration Revision dialog box and click Save.

Permissions Superuser, read-write

Elements Local File display field—Displays the name of the archived configuration file that has been modified.

Action Taken display field—Displays whether the archived configuration file has been modified.

OK button—Displays the Configuration Repository dialog box.

Scripts—Edit—Select Revision Dialog Box

Description Use the Select Revision dialog box to select the revision of the script you want to edit.

Navigation Click Configuration > Repository > Scripts. Select a script and click Edit in the Actions column in the Scripts dialog box.

Permissions Superuser, read-write

Elements Modified Date column—Lists the dates on which scripts were modified.

Revision column—Lists the current revision number of the scripts.

Comment column—Lists the optional comments entered while importing the scripts.

Edit button—Allows you to edit a revision of the script.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Scripts—Execute—Specify Devices and Time Dialog Box

Description Use the Specify Devices and Time dialog box to select the devices on which the script should be executed and the time at which to perform the execution operation.

Navigation Click Configuration > Repository > Scripts. Select the script you want to execute and click Execute in the Actions column in the Scripts dialog box.

Permissions Superuser, read-write

Elements Select details for Script Execution section:

- Parameter Name field—Enables you to enter the parameter name
- Parameter Value field—Enables you to enter the parameter value.
- Add button—Click to add the parameter to the list.
- List of Parameters for Script Execution list—Displays all the parameters for script execution. The parameters are displayed in this format – parameter name:parameter value
- Remove button—Click to remove the selected parameter from the list.
- Remove All button— Click to remove all the parameters from the list.
- Drop-down list and field box— Select the pattern type (success or failure) from the list and enter a pattern value in the field. After the script executes successfully, JUNOScope searches for this value in the output of the script execution and displays the status message in the Status dialog box.

Select Devices section:

- Group option button and drop-down list box—Select a router group on which the script is to be executed. Click the Group option button, then click the Group drop-down list box to display the available groups for JUNOScope software operations. If you have not added any router groups, the Groups drop-down list box is empty.
- Selected Devices option button and drop-down list box—Select a router on which the script is to be executed. Click the Devices option button, then select the devices in the Devices drop-down list box on which the script is to be executed. If you have not added any routers, the drop-down list box is empty.

Select Time or Save Operation section:

- Now check box—Select to have the execution operation occur as soon as the command is executed.
- Save Operation as text box—Type a name for the execution operation that you want to save. The saved execution operation appears in the Saved Operations dialog box with the name that you gave it. To view the Saved Operations dialog box, click Settings > Saved Operations.
- Select Schedule area—Lets you select a schedule for when you want the script execution operation to occur.

Next button—Displays the Confirm Script Execution Selection dialog box from which you can either select to finish the script execution operation or cancel it.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Previous button—Redisplays the Select Script Revision and Options dialog box where you can select another revision.

Scripts—Execute—Confirm Script Execution Selection Dialog Box

Description Use the Confirm Selection dialog box to confirm the selections you made for the execution operation.

Navigation Click Configuration > Repository > Scripts. Add the required parameters, select the router or group of routers on which the script should be executed, and the time at which to perform the execute operation, and click Next in the Specify Devices and Time dialog box.

Permissions Superuser, read-write

Elements Please Confirm display field—Displays the script that is being executed, and the devices or groups on which it is executed, for your confirmation.

Finish button—Executes the operation. The Status—View Status Records dialog box appears displaying the status of the execution operation.

Previous button—Redisplays the Specify Devices and Time dialog box.

Scripts—Import—Import Dialog Box

Description Use the Import dialog box to import a JUNOS script into the JUNOScope CVS repository.

Navigation Click Configuration > Repository > Scripts. Click Import in the Scripts dialog box.

Permissions Superuser, read-write

Elements Local File text box—Browse to the location on your local machine where you have stored the script to be imported.

MD5 Checksum For Verification (Optional) textbox —Lets you enter the MD5 checksum for the imported script. The checksum can be obtained from http://www.juniper.net/customers/support/ when you download the script. This checksum value is compared with the checksum stored in JUNOScope to verify that the downloaded script is intact. This field is optional.

Script Type drop-down list box—Select the script type from the Script Type drop-down list box

Comment text box—Type an optional comment for the script.

Import button—Imports to import the script into the JUNOScope CVS repository.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Scripts—Import—Import Result Dialog Box

Description Use the Import Result dialog box to confirm the import of the JUNOS script into the JUNOScope CVS repository.

Navigation Click Configuration > Repository > Scripts. Click Import in the Scripts dialog box. Click Import in the Import dialog box.

Permissions Superuser, read-write

Elements Local File display field—Displays the name of the local script file that has been imported into the JUNOScope CVS repository.

Action Taken display field—Displays whether the script has been added to the JUNOScope CVS repository.

Revision display field—Displays the version number of the script that has been added to the JUNOScope CVS repository.

Scripts—Scripts Dialog Box

Description Use the Scripts dialog box to view a list of all JUNOS-based scripts saved in the JUNOScope CVS repository.

Navigation Click Configuration > Repository > Scripts.

Permissions Superuser, read-write

Elements Name column—Lists all JUNOS-based scripts saved in the JUNOScope CVS repository by name.

Type column—Lists the type of scripts saved in the JUNOScope CVS repository. There are three types of scripts:

- Commit—A commit script enforces custom configuration rules. Each time a new candidate configuration is committed, the script inspects the configuration. If a configuration violates your custom rules, the script corrects the problem.
- Op—An Op script automates network troubleshooting and network management. They can perform any function available through the remote procedure calls (RPCs) supported by two APIs: the JUNOS extensible markup language (XML) API and the JUNOScript API.
- Event—Event scripts are operation (op) scripts invoked in response to event notifications like system log messages and Simple Network Management Protocol (SNMP) traps received by the event process.

Actions column—Lists the actions that can be performed on the scripts saved in the JUNOScope CVS repository. You can do the following:

- View—View all JUNOS-based scripts saved in the JUNOScope CVS repository.
- Edit—Edit JUNOS-based scripts saved in the JUNOScope CVS repository.
- Compare—Compare different revisions of JUNOS-based scripts saved in the JUNOScope CVS repository.
- Deploy—Deploy a JUNOS script in the JUNOScope CVS repository to a router or group of routers,
- Disable—Disable commit scripts, op scripts and event scripts.
- Execute—Execute an op script.

Import button—Imports a JUNOS script into the JUNOScope CVS repository.

Delete button—Deletes the script from the JUNOScope CVS repository.

Scripts—View—Select Revision Dialog Box

Description Use the Select Revision dialog box to select the revision of the script you want to view.

Navigation Click Configuration > Repository > Scripts. Select a Script and click View in the Actions column in the Scripts dialog box.

Permissions Superuser, read-write

Elements Modified Date column—Lists the dates on which scripts were modified.

Revision column—Lists the current revision number of the scripts.

Comment column—Lists the optional comments entered while importing the scripts.

View button—Displays a revision of the script.

Cancel button—Clears this dialog box and redisplays the Scripts dialog box.

Scripts—View—View Dialog Box

Description Use the View dialog box to view a script in the JUNOScope CVS repository.

Navigation Click Configuration > Repository > Scripts. Select a script and click View in the Actions column in the Scripts dialog box. Select the revision of the script you want to view in the Select Revision dialog box. Click View in the Select Revision dialog box.

Permissions Superuser, read-write

Elements View display box—Displays the contents of the script file.

Previous button—Redisplays the Select Revision dialog box so you can select another revision.

OK button—Redisplays the Scripts dialog box.

Software Manager—Download Image Confirmation Dialog Box

Description Use the Download Image Confirmation dialog box to confirm that the settings you selected to download as a software image to a device or a group of devices is correct. The dialog box displays the image name that you selected to download and lists the device names or group to which the software image will be downloaded.

Navigation Click Software Management > Images. The Images dialog box appears. Click the Download link for the image you want to download, then click Next.

Permissions Superuser

Elements Please Confirm display area—Displays the image name that you selected to download and lists the device names to which the software image will be downloaded. It also lists the download options that you have selected.

Finish button—Executes the software image download operation.

Previous button—Returns you to the Download Images dialog box where you select options for downloading a software image.

Software Manager—Download Image Dialog Box

Description Use the Download Image dialog box to select the options for downloading a software image to a device or a group of devices.

Navigation Software Management > Images. Then click the Download link for the software image you want to download.

Permissions Superuser

Elements Selected Devices area—Displays the available devices and groups of devices to which you can download a software image.

- Group option button and drop-down list box—Displays the available groups that have been created using Settings > Groups. Click the option button to select it, then select a group from the drop-down list box.

- Selected Devices option button and drop-down list box—Displays the devices to which you can download a software image. Click the option button to select it, then select one or more devices from the drop-down list box. Use Ctrl + click to select multiple devices.

Comment (Optional) text box—Type an optional description for the download software image operation.

Use JUNOScope IP address for image transfer option button — Select this option if you want the device(s)/group to connect to the JUNOScope server using the IP address of the JUNOScope server. The device(s)/group will use the IP address instead of the JUNOScope server name to connect to the server. Select the IP address from the drop-down list.

Verify MD5 Checksum for downloaded image option button—Select this option if you want to ensure that the downloaded software image is intact. The MD5 checksum for the downloaded image is compared with the checksum value stored in JUNOScope. If they do not match, the operation fails and the error message is displayed in the View Status Record dialog box.

Select Time or Save Operation area—Lets you schedule when you want the download software image operation to run and save the download software image operation to combine with other operations or run at a later time.

- Now option button—Runs the operation immediately after you confirm it.

- Save Operation as option button and text box—Saves the operation to the Settings > Saved Operations table. Click the option button to select it, then type a name for the operation in the text box. The saved operation name maximum length is 40 characters.

- Select Schedule area—Lets you select a schedule for when you want the download software image operation to occur.

- Schedule table—Lists the available schedules that have been created using Settings > Schedules. Select a schedule for downloading a software image.

Next button—Displays the Confirm Software Download dialog box if you selected the Now schedule option. Displays the Confirm Save Download Image dialog box if you selected the Save Operation as option. Runs the download image operation at the specified interval if you selected the Select Schedule option.

Cancel button—Returns you to the Images dialog box.

Software Manager—Images Dialog Box

Description Use the Images dialog box to view and manage the supported software images that you have imported into the JUNOScope software for downloading or installing on one or more Juniper Networks devices.

Navigation Click Software Management > Images.

Permissions Superuser

Elements Images table—Lists the supported software images that you have imported into the JUNOScope software. Software images are listed by name, version, and type. You can perform delete, download, and install actions on images.

Import button—Displays the Import Software Image dialog box from which you can select the software image file you want to import. For import, the software image file must exist on the local machine where the Web browser is running.

Software Manager—Import Software Image Dialog Box

Description Use the Import Software Image dialog box to import supported software images into the JUNOScope software for downloading or installing on one or more devices. You can import software images that have been downloaded from the Juniper Networks software download page.

Navigation Click Software Management > Images, then click Import.

Permissions Superuser

Elements File text box and Browse button—Lets you navigate to a software image to import on the local workstation file system.

Verify MD5 Checksum (optional) textbox —Lets you enter the MD5 checksum for the imported image. The checksum can be obtained from http://www.juniper.net/customers/support/ when you download the image. This checksum value is compared with the checksum stored in JUNOScope to verify that the downloaded image is intact. This field is optional.

Import button—Imports the selected software image file.

Cancel button—Closes the Import Software Image dialog box without importing a software image.

Software Manager—Install Image Confirmation Dialog Box

Description Use the Install Image Confirmation dialog box to confirm that the settings you selected to install a software image on a device or a group of devices is correct. The dialog box displays the image name that you selected to install and lists the device names on which the software image will be installed.

Navigation Click Software Management > Images. The Images dialog box appears. Click the Install link for the image you want to install, then click Next.

Permissions Superuser

Elements Please Confirm display area—Displays the image name that you selected and lists the device names on which the software image will be installed. It also lists the installation options that you have selected.

Finish button—Executes the software image install operation.

Previous button—Returns you to the Install Image dialog box where you select options for installing a software image.

Software Manager—Install Image Dialog Box

Description Use the Install Image dialog box to select the options for installing a software image on one or more devices.

Navigation Software Management > Images. Then click the Install link for the software image to install.

Permissions Superuser

Elements Installation Options—Provides the options for installing software images:

- Use Image Already Downloaded Onto Device check box—Installs an image that has already been downloaded to the /var/tmp directory of a device.
- Archive Data And Executable Areas (Snapshot) check box—(Default) This option is the equivalent of the JUNOS software request system snapshot command. The command backs up the currently running and active file system partitions on the router to standby partitions that are not running. Specifically, the root file system (/) is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive. After you run the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

  The request system snapshot command can fail on J-series devices when there is no compact flash to back up the system.
- Check Compatibility With Current Configuration check box—(Default) Validates the software image that you want to install against the current configuration as a prerequisite to installing the software image. If the current configuration is not compatible with the software image, the installation will not continue. This is equivalent to using the JUNOS request system software add validate CLI command. This is the default behavior when the software image being added is a different release.
- Load Succeeds If At Least One Statement Is Valid check box—Activates a partial load and treats parsing errors as warnings instead of errors. Even if some of the statements (but not all) are invalid, the software installation succeeds. This option is the equivalent of using the request system software add <image> best-effort-load CLI command.
- Remove The Package After Successful Installation check box—Allows the system to find enough room to upgrade a new software image. Use this option when installing a software image from a local directory on a device that has minimal storage space. This command is equivalent to the request system software add uplink CLI command.

Target RE area—Displays the available routing engines (Current, Master, and Backup) on which you can download a software image.

Select Target RE (in case of Dual RE): drop-down list box—Displays the routing engines (Current, Master, and Backup) on which you can install a software image in case of Dual Routing Engine. Click the routing engine to select it.

Selected Devices area—Displays the available devices and groups of devices on which you can download a software image.

- Group option button and drop-down list box—Displays the available groups that have been created using Settings > Groups. Click the option button to select it, then select a group from the drop-down list box.

- Selected Devices option button and drop-down list box—Displays the devices on which you can install a software image. Click the option button to select it, then select one or more devices from the drop-down list box. Use Ctrl + click to select multiple devices.

Comment (Optional) text box—Type an optional description for the install software image operation.

Use JUNOScope IP address for image transfer option button and drop-down list—Select this option if you want the device(s)/group to connect to the JUNOScope server using the IP address of the JUNOScope server. The device(s)/group will use the IP address of the JUNOScope server instead of the JUNOScope server name. Select the IP address from the drop-down list.

Select Time or Save Operation area—Schedules an install software image operation to run and saves the download software image operation so you can combine it with other operations or run it at a later time.

- Now option button—Runs the operation immediately after you confirm it.

- Save Operation as option button and text box—Saves the operation to the Settings > Saved Operations table. Click the option button to select it, then type a name for the operation in the text box. The saved operation name maximum length is 40 characters.

- Select Schedule area—Lets you schedule when you want the operation to occur.

- Schedule table—Lists the available schedules that have been created using Settings > Schedules. Select a schedule for installing a software image.

Next button—Displays the Confirm Software Install dialog box if you selected the Now schedule option. Displays the Confirm Save Install Image dialog box if you selected the Save Operation as option. Runs the install image operation at the specified interval if you selected the Select Schedule option.

Cancel button—Returns you to the Images dialog box.

Transfer on Commit—Configuring Transfer on Commit—Select Group or Device(s) Dialog Box

Description Use the Select Group or Device(s) Dialog Box to select the group or devices on which to enable transfer-on-commit.

Navigation Configuration > Repository > Transfer on Commit > Configure Transfer on Commit.

Permissions Superuser, Read-write.

Elements Group drop-down list box—Select the group on which you want to enable transfer-on-commit.

Select Device(s) list box—Select the device or devices on which you want to enable transfer-on-commit.

Configured Devices list box—Displays the device or devices on which transfer-on-commit has already been enabled.

Next button—Displays the Confirm Selections dialog box.

Cancel button—Clears the selections you made in this dialog box.

Transfer on Commit—Configuring Transfer on Commit—Confirm Selections Dialog Box

Description Use the Confirm Selections dialog box to confirm the selections for performing the transfer-on-commit.

Navigation Configuration > Repository > Transfer on Commit > Configure Transfer on Commit. Select the group or devices on which to enable transfer-on-commit and click Next.

Permissions Superuser, Read-write.

Elements Please Confirm display area—Displays the name of the device or devices on which transfer-on-commit will be enabled.

Finish button—Executes the configure transfer-on-commit operation. The Status—View Status Records dialog box appears displaying the status of the configure transfer-on-commit operation.

Cancel button—Cancels the operation and displays the Transfer on Commit menu.

Previous button—Displays the Select Group or Device(s) dialog box.

Transfer on Commit—Removing Transfer on Commit—Select Device(s) Dialog Box

Description Use the Select Device(s) dialog box to select the device or devices on which you want to disable the transfer-on-commit configuration.

Navigation Configuration > Repository > Transfer on Commit > Remove Transfer on Commit.

Permissions Superuser, Read-write.

Elements Select Device(s) list box—Select the device or devices on which you want to disable transfer-on-commit.

Next button—Displays the Confirm Selections dialog box.

Cancel button—Cancels the operation and displays the Transfer on Commit menu.

Transfer on Commit—Removing Transfer on Commit—Confirm Selections Dialog Box

Description Use the Confirm Selections dialog box to confirm the devices on which to disable transfer-on-commit.

Navigation Configuration > Repository > Transfer on Commit > Remove Transfer on Commit. Select the devices on which to disable transfer-on-commit and click Next.

Permissions Superuser, Read-write.

Elements Please Confirm display area—Displays the name of the device or devices on which transfer-on-commit will be disabled and confirms that the JUNOScope server has been removed as the transfer-on-commit server.

Finish button—Executes the remove transfer-on-commit operation. The Status—View Status Records dialog box appears displaying the status of the remove transfer-on-commit operation.

Cancel button—Cancels the operation and displays the Transfer on Commit menu.

Previous button—Displays the Select Device(s) dialog box.

Transfer on Commit—Archive Unmatched Configuration—Select Unmatched Configuration Dialog Box

Description Use the Select Unmatched Configuration dialog box to select a transferred configuration that could not be matched to any of the devices managed in JUNOScope.

Navigation Configuration > Repository > Transfer on Commit > Archive Unmatched Configuration.

Permissions Superuser, Read-write.

Elements Select Config drop-down list box—Select a transferred configuration that could not be matched to any of the devices managed in JUNOScope.

Next button—Displays the View Config and Select Device dialog box.

Cancel button—Cancels the operation and displays the Transfer on Commit menu.

Transfer on Commit—Archive Unmatched Configuration—View Configuration and Select Device Dialog Box

Description Use the View Configuration and Select Device dialog box to view the unmatched configuration and select the device to which you want to archive the unmatched configuration.

Navigation Configuration > Repository > Transfer on Commit > Archive Unmatched Configuration. Select the configuration you want to match in the Select Unmatched Configuration dialog box and click Next.

Permissions Superuser, Read-write.

Elements Unmatched Configuration display box—Displays the contents of the selected unmatched configuration file in a read only field.

Archive to Device drop-down list box—Select the device to which you want to archive the unmatched configuration.

Next button—Displays the Confirm Selections dialog box.

Previous button—Displays the Select Unmatched Configuration dialog box.

Cancel button—Cancels the operation and displays the Transfer on Commit menu.

Transfer on Commit—Archive Unmatched Configuration—Confirm Selections Dialog Box

Description Use the Confirm Selections dialog box to confirm your selection of the unmatched configuration and the device to which you want to archive the unmatched configuration.

Navigation Configuration > Repository > Transfer on Commit > Archive Unmatched Configuration. Select the configuration you want to match in the Select Unmatched Configuration dialog box and click Next. View the unmatched configuration and select the device to which you want to archive the unmatched configuration from the View Configuration and Select Device dialog box and click Next.

Permissions Superuser, Read-write.

Elements Please Confirm display area—Displays the name of the unmatched configuration file you selected and the device to which you want to archive the unmatched configuration.

Finish button—Executes the archive unmatched configuration operation. The Transfer on Commit—View Status dialog box appears displaying the status of the archive unmatched configuration operation.

Previous button—Displays the View Configuration and Select Device dialog box.

Cancel button—Cancels the operation and displays the Transfer on Commit menu.

Transfer on Commit—Archive Unmatched Configuration—View Status Dialog Box

Description Use the View Status dialog box to display the status of the archive unmatched configuration operation.

Navigation Configuration > Repository > Transfer on Commit > Archive Unmatched Configuration. Select the configuration you want to match in the Select Unmatched Configuration dialog box and click Next. View the unmatched configuration and select the device to which you want to archive the unmatched configuration from the View Configuration and Select Device dialog box and click Next. Confirm your selection of the unmatched configuration and the device to which you want to archive the unmatched configuration in the Confirm selections dialog box and click Finish.

Permissions Superuser, Read-write.

Elements Status display area—Displays the status of the archive unmatched configuration operation.

OK button—Displays the Transfer on Commit menu.

Transfer on Commit—Archive Site

Description Use the Archive Site dialog box to configure the JUNOScope server for transfer-on-commit, set up the archive site for archiving configurations, and schedule the archive site scanning operation.

Navigation Settings > Transfer on Commit.

Permissions Superuser.

Elements JUNOScope Server Directory text box—Enter the directory to which committed configurations will be transferred.

Credentials for Transfer text boxes:

- User Name text box—Enter the user name to be used by the device to connect to the JUNOScope server.
- Password text box—Enter the password to be used by the device to connect to the JUNOScope server.
- Confirm Password text box—Confirm the password to be used by the device to connect to the JUNOScope server.

Protocol drop-down list box—Select the protocol to be used for connecting to the JUNOScope server. You can choose the scp or ftp protocol. To use the scp protocol, the ssh v1or v2 daemon must be running on the JUNOScope server.

Port text box—Displays the port numbers used for connecting to the server for the protocol selected. Port 21 for ftp and port 22 for scp. You can edit the port text box and change the port number.

Key Type drop-down list box—Select the key type if you are using the scp protocol to connect to the JUNOScope server.

Public Key text box—Enter the public key if you are using the scp protocol to connect to the JUNOScope server.

Archive Site Host option:

- Use DNS Name button—Select if you want to connect to the JUNOScope server using the DNS name.
- Use IP Address button— Select if you want to connect to the JUNOScope server using the IP address.

Archive Site Scanning Schedule table:

- Schedule Name column— Displays the names of the scanning schedules that can be selected.
- Start Time column— Displays the time when the scanning operation is scheduled to start.
- Period column— Displays the frequency at which the schedule will run.
- Comment column—Displays the comment entered when the schedule was created.

OK button—Updates the changes made using the Archive Site dialog box.

Reset button—Discards the changes you made using the Archive Site dialog box.

User Group Authorization—Add/Edit User Group Authorization Dialog Box

Description Use the Add/Edit User Group Authorization dialog box to add one or more users to a user group or edit the users in a user group.

Navigation Settings > Users > User Group Authorization. Click Add in the User Group Authorization dialog box.

Permissions Superuser

Elements User Group Name text box—For pre-defined user groups (administrator, read-write user, read-only user, and nobody), the user group name is a display field. For user-defined user groups, type the name of the user group to which you are adding users.

Permission drop-down list box—Select the permission level assigned to the user group.

Comment text box—For pre-defined user groups (administrator, read-write user, read-only user, and nobody), the comment is a display field. For user-defined user groups, type an optional descriptive comment about the users you are associating with the user group.

Add Users from User Group drop-down list box—Select an existing user group from which usernames are available to add to the user group you want to create.

Add to Selected Users button—Adds the usernames from a selected user group to the Selected Users list box.

Available Users list box—Lists the JUNOScope users you can add to the user group.

Add/Remove buttons—Buttons to move the usernames in the Available Users list box to the Selected Users list box and vise versa.

Selected Users list box—Lists the JUNOScope users you have selected to add to the user group.

OK button—Adds the selected users to the user group.

Cancel button—Clears this dialog box and displays the User Group Authorization dialog box.

User Group Authorization—Associate Device Groups to User Group Dialog Box

Description Use the Associate Device Groups to a User Group dialog box to associate device groups with a user group so that the user group has access to these device groups.

Navigation Settings > Users > User Group Authorization. Click the Device Group Mgmt link in the Actions column in the User Group Authorization dialog box.

Permissions Superuser

Elements User Group Name display field—The name of the user group with which you are associating device groups.

Permission display field—The permission level assigned to the user group.

Comment display field—The optional descriptive comment about the user group you added while creating the user group.

Add to Selected Devices button—Adds the device names from a selected label or device group to the Selected Devices list box.

Available Device Groups list box—Lists the available device groups that you can associate with the user group.

Add/Remove buttons—Buttons to move device groups from the Available Device Groups list box to the Selected Device Groups list box and vise versa.

Selected Device Groups list box—Lists the device groups you have selected to associate with the user group.

OK button—Associates the selected device groups to the user group.

Cancel button—Clears this dialog box and displays the User Group Authorization dialog box.

User Group Authorization—Associate Devices to User Group Dialog Box

Description Use the Associate Devices to User Group Dialog Box to associate devices with a user group so that the user group has access to these devices.

Navigation Settings > Users > User Group Authorization. Click Device Mgmt in the Actions column in the User Group Authorization dialog box.

Permissions Superuser

Elements User Group Name display field—The name of the user group with which you are associating devices.

Permission display field—The permission level assigned to the user group.

Comment display field—The optional descriptive comment you added while creating the user group.

Add Devices from Label/Group drop-down list box—Select an existing label or group that you want, then click Add to Selected Devices to add devices from an existing label or group.

Available Devices list box—Lists the available devices that you can associate with the user group.

Add/Remove buttons—Buttons to move devices from the Available Devices list box to the Selected Devices list box.

Selected Devices list box—Lists the devices you have selected to associate with the user group so that the user group has access to these devices.

OK button—Associates the selected devices with the user group.

Cancel button—Clears the dialog box and displays the User Group Authorization dialog box.

User Group Authorization—Import User Group Authorization Dialog Box

Description Use the Import User Group Authorization dialog box to import user group data into the JUNOScope server from a junoscope-usergroup.xml file that you have saved to the local file system.

Navigation Settings > Users > User Group Authorization. Click Import in the User Group Authorization dialog box.

Permissions Superuser

Elements File text box—Either browse to or type the name of the XML file that you want to import. For example, you can import the default junoscope-usergroups.xml export file from another JUNOScope server or use the provided sample export-import-sample.xml XML file on the JUNOScope server to generate a file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

Import button—Imports user group data into the JUNOScope server and displays the Import/Export Data dialog box.

Cancel button—Clears this dialog box and displays the User Group Authorization dialog box.

User Group Authorization—User Group Authorization Dialog Box

Description Use the User Group Authorization dialog box to set up authorization to access devices for JUNOScope User Groups. You can also export JUNOScope user group settings to an XML file on the local file system and import user group data into the JUNOScope server from a junoscope-usergroup.xml file that you have saved to the local file system.

Navigation Settings > Users > User Group Authorization.

Permissions Superuser

Elements User Group column—Lists the names of the existing user groups in alphabetical order. Click the column header to sort the table alphabetically in ascending and descending order. There are four predefined user groups:

- Administrator—A user group that has full access to the JUNOScope software (Settings menu) and read and write privileges to JUNOScope managed devices. The initially configured JUNOScope installer and administrative user is always part of this user group. The administrator user group has read-write access to all devices. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having a superuser permission level is added to this user group.

- Read-write user—A user group that has read-write privileges to JUNOScope managed devices and operations. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having read-write permission is added to this user group.

- Read-only user—A user group that has only read privileges to JUNOScope managed devices and operations. If you import JUNOScope settings or upgrade from a release earlier than JUNOScope 8.2, any user having read-only permission is added to this user group.

- Nobody—A user group that can only log in to the JUNOScope software. The nobody user group does not have access to any JUNOScope managed devices. No devices or device groups can be associated with this user group.

Permission column—The permission level assigned to the user group. The four permission levels available are:

- Superuser—Performs all JUNOScope management functions, manage user accounts, views and modifies JUNOScope settings, and has full access to devices.
- Read-write—Has full access to devices with all functions available, but cannot set up JUNOScope settings.
- Read-only—Can view a device configuration, but cannot modify it, or perform any operation.
- None—Is denied access to any devices and can only log in.

Users column—Displays the users assigned to a user group.

Devices column—Displays devices to which the user group has access.

Groups column—Displays the groups to which the user group has access.

Actions column—Displays the following command links:

- Edit link—Displays the Add/Edit User Group dialog box to associate users with an existing user group.
- Associate Devices link—Displays the Associate Devices to User Group dialog box to associate devices with a user group.
- Associate Device Groups link—Displays the Associate Device Group to User Group to associate device groups with a user group.
- Delete link—Deletes a user group.

Add button—Displays the Associate Users to a User group dialog box so you can associate users with a user group.

Export button—Displays the File Download dialog box so that you can export JUNOScope user group settings to an XML file on the local file system.

Import button—Displays the Import User Groups dialog box so that you can import user group data into the JUNOScope server from a junoscope-usergroup.xml file that you have saved to the local file system.

Users—Authentication Policy Dialog Box

Description Use the Users—Authentication Policy dialog box to view and edit the JUNOScope software user access policy, which applies to:

- All users already configured in the JUNOScope software using Settings > Users > Local Authentication
- All remote RADIUS users who have successfully logged in the JUNOScope software
- All new users created using Settings > Users > Local Authentication

An authentication policy includes the following data:

- Status—The user's ability to access the JUNOScope software: Locked or Unlocked.
- Maximum login attempts—The number of consecutive login failure attempts allowed.
- Access window—A maximum time interval within which the failure attempts are done, depending on the authentication policy.

A default authentication policy is automatically generated for all users. The JUNOScope administrator can edit a user authentication policy.

Navigation Click Settings > Users > Authentication Policy.

Permissions Superuser

Elements The Authentication Policy table displays the following information:

Username column—The name of the user successfully logged in to the JUNOScope software.

Status column—The user account status can be either LOCKED or UNLOCKED. If a user account is LOCKED, that user is denied access to the system even if a user provides a valid username and password. The user is denied access until the JUNOScope administrator changes the status to UNLOCKED.

Actions column—Displays an Edit link that you can use to edit the user account maximum login attempts and access window.

Export button—Displays the File Download dialog box to export the authentication policy data in XML file format to the computer file system. The default authentication policy export filename is junoscope-auth-policy.xml.

Import button—Imports user authentication policy data from the computer file system into the JUNOScope software. The Import Results dialog box appears.

Users—Authentication Policy—Edit Authentication Policy Dialog Box

Description Use the Users—Authentication Policy—Edit Authentication Policy dialog box to edit a user account authentication policy maximum login attempts and access window.

Navigation Click Settings > User > Authentication Policy. Click the Edit link in the Actions column.

Permissions Superuser

Elements Status drop-down list box—The user account status can be either UNLOCKED (the default) or LOCKED. If a user account status is UNLOCKED, the user can successfully log in to the JUNOScope software by providing a valid username and password. If the account status is LOCKED, the user is denied access to the JUNOScope software, even if the user provides a valid username and password. The " The user account is currently locked. Please contact the system administrator." message appears.

Maximum Login Attempts text box—The maximum number of consecutive failure login attempts allowed within the access window for a user. If a user reaches the maximum number of login attempts, the user status automatically becomes LOCKED. This field can have a value from 0 to 100. If the maximum login attempts is 0, the authentication policy for the user will not be active, the user account will be assumed to be UNLOCKED, and the normal login mechanism will be applied. For the JUNOScope administrator (the initially configured user), the user account is always UNLOCKED.

Access Window text boxes—The access window for a user account starts when the first login failure occurs for the user account and runs until one of the following occurs:

- A user successfully logs in. The access window is then reset.
- A user tries unsuccessfully to log in for the maximum number of login attempts. The user account is then LOCKED and the access window is reset.

  The Access Window field can have a minimum value of 0 (for example, all the minute(s), hour(s), and second(s) fields having a value of 0) and a maximum value of 24 hours (for example, the hour(s) field can have a maximum value of 24, while the minute(s) and second(s) fields have a maximum value of 59). The default value is 0.

  However, individually, the hour(s) field can have a value of from 0 to 24, the minute(s) field can have a value of from 0 to 59, and the second(s) field can have a value of from 0 to 59. If the Access Window field is 0, the authentication policy for the user account will not be active, and the normal login mechanism will always be applied for user accounts whose Access Window field is set to 0.

  The timer for the access window starts when an invalid login attempt is made on a user account. If a user account is not locked and no further invalid login attempt is tried for that account, the timer for the access window is automatically reset either after a time period equal to the access window or if the user successfully logs in to JUNOScope within the access window period.

OK button—Saves the user account authentication policy changes.

Users—Authentication Policy—Import Dialog Box

Description Use the Import dialog box to import existing authentication policy data from the local file system to the JUNOScope database.

Navigation Settings > Users > Authentication Policy. Click Import in the Authentication Policy table dialog box.

Permissions Superuser

Elements File text box—Type or browse to the authentication policy XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers. The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

Browse button—Displays the File Open dialog box from which you can select the XML file to import.

Import button—Imports the selected saved operations data into the JUNOScope software and displays the Import Results dialog box.

Cancel button—Clears this dialog box and displays the Authentication Policy dialog box.

Users—Authentication Policy—Global Authentication Policy—Edit/View Global Authentication Policy

Description Use the Edit/View Global Authentication Policy dialog box to configure and edit global authentication policies.

Navigation Click Settings > Users > Authentication Policy > Global Authentication Policy

Permissions Superuser

Elements Maximum Login Attempts text box—Indicates the maximum number of consecutive failure login attempts allowed within the access window for a user. If a user reaches the maximum number of login attempts, the user status automatically becomes locked. This field can have a value from 0 to 100. If the maximum login attempts is 0, the authentication policy for the user will not be active, the user account will be assumed to be unlocked, and the normal login mechanism will be applied. If a user account status is unlocked, the user can successfully log in to the JUNOScope software by providing a valid username and password. If the account status is locked, the user is denied access to the JUNOScope software, even if the user provides a valid username and password. The message " The user account is currently locked. Please contact the system administrator," is displayed.For the JUNOScope administrator (the initially configured user), the user account is always unlocked.

Access Window text boxes—The access window for a user account starts when the first login failure occurs for that account and runs until one of the following occurs:

- A user successfully logs in. The access window is then reset.
- A user tries unsuccessfully to log in for the maximum login attempts. The user account is then locked and the access window timer is reset.

  The Access Window field can have a minimum value of 0 (for example, all the field minute(s), hour(s), and second(s) having a value of 0) and a maximum value of 24 hours, for example, the hour(s) field can have a maximum value of 24, while the minute(s) and second(s) fields have a value of 0). The default value is 0. However, individually, the hour(s) field can have a value from 0 to 24, the minute(s) field can have a value of from 0 to 59, and the second(s) field can have a value from 0 to 59. If the Access Window field is 0, the authentication policy for the user account will not be active, and the normal login mechanism will always be applied.

  The timer for the access window starts when an invalid login attempt is made on a user account. If a user account is not locked and no further invalid login is attempted for that account, the timer for the access window is automatically reset either after a time period equal to the access window or if the user successfully logs in to JUNOScope within the access window period.

  If the authentication policy for a user account is set up with 3 Maximum Login Attempts and a 1-hour Access Window, the clock for the Access Window starts at the first unsuccessful attempt when the user types an invalid password to log in. If the user makes three unsuccessful attempts within 1 hour, then the user account will be LOCKED at the third unsuccessful attempt and will be redirected to the " The user account is currently locked. Please see the system administrator" message. Any further attempts by the user to log in using the username, even with a valid password, will be denied.

Add button—Expands the dialog box so that you can allow or deny specific clients access to JUNOScope. The following items appear when you click Add:

- Network text box—The IP address of the client machines that should be allowed or denied access to the JUNOScope software. Specify either a specific client address, in which case the user must use the wildcard of 32 (128 for IPv6), or the specific first valid client address, in which case you must use the mask as the number of bits that should exactly match the given IP address.

- Mask drop-down list box—The network mask of the client machines that should be allowed or denied access to the JUNOScope software. Specifies the number of bits in the client IP that should match the given IP address.

- Allow drop-down list box—Lets you determine whether to deny or allow access to the client machine if the IP address is matched.

- Comment text box—Identifies the Access Control List entry. You can provide a comment to identify each Access Control List entry or to provide a reason for allowing or denying access.

- Actions buttons—The Move Up and Move Down options used for ordering Access Control List entries. When a user logs in, the IP address of the user's machine is compared with the access list in sequence until a match is found. If a match is found, then the action specified (Allow/Deny) is performed, and the process does not continue. However, if no match is found, the client is allowed access by default. Since order plays an important role in the access list, use the Move Up and Move Down options to change the order of Access Control List entries. Use the Delete option to delete an Access Control List entry.

Save button—Saves the global authentication policy changes to the database.

Reset button—Clears all the values you have entered and restores the last saved values.

Export button—Displays the File Download dialog box so that you can export global authentication policy data to a file on the local file system. The default global authentication policy filename is junoscope-globalPolicy.xml.

Import button—Displays the Import dialog box so that you can import global authentication policy data from a file on the local file system.

Users—Authentication Policy—Global Authentication Policy—Import Global Authentication Policy Dialog Box

Description Use the Global Authentication Policy Import dialog box to import authentication information from another JUNOScope server.

Navigation Settings > Users > Authentication Policy > Global Authentication Policy. Click Import in the Edit/View Global Authentication Policy Dialog Box.

Permissions Superuser

Elements File text box—Either browse to or type the name of the XML file that you want to import. For example, you can import the default schedules.xml export file from another JUNOScope server or use the provided sample junoscope-globalPolicy.xml XML file on the JUNOScope server to generate a file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers, The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record merges with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are reset to the default values, then the imported data is updated in the database. Before the override operation occurs, a message window appears with the following confirmation prompt: " The import with override option will delete all the existing records. Do you want to continue?" Select Yes or No to continue.

NOTE: Access Control Lists are always deleted no matter what import method selected, as they are meaningful only as a chunk. Access Control List data that is imported is added after validation of the data.

Users—Local Authentication Dialog Box

Description Use the Users—Local Authentication dialog box to view the users who have access privileges or permission to use the JUNOScope software. The Users—Local Authentication dialog box lists users by username and permissions. The JUNOScope software provides three permissions for performing operations: Superuser, read-write, and read-only.

Users with Superuser permission can perform all JUNOScope software operations: administration, configuration management, status, and Looking Glass. Users with read-write permission can perform configuration management, status, and Looking Glass operations. Users with read-only permission can perform only Looking Glass operations.

Navigation Click Settings > Users > Local Authentication.

Permissions Superuser

Elements Users table—Lists the local users by username and the user groups to which they belong. If no users have been added, the table is empty. Select a user to copy, edit, or delete.

Add button—Displays the Local Authentication—Add User dialog box so you can add a new JUNOScope software user.

Copy button—Copies the selected user in the JUNOScope database. A 1 (one) appears after the copied user and increments sequentially each time you copy the same user. Select a user to copy.

Edit button—Displays the Edit User dialog box so you can change JUNOScope software user information. Select a user to edit.

Delete button—Removes a JUNOScope software user. Select a user from the table before clicking Delete. Select a user to delete.

Export button—Displays the File Download dialog box to export the setup data in XML file format to the computer file system. The default users export filename is users.

Import button—Displays the Import dialog box for you to specify the XML file to import.

Users—Local Authentication—Add User Dialog Box

Description Use the Users—Local Authentication—Add User dialog box to add a new user for JUNOScope software operations. Adding a new user requires a username, password, and permission level.

Navigation Click Settings > Users. Click Add in the Users—Local Authentication dialog box.

Permissions Superuser

Elements Username text box—Type the name of the user you want to add. The username must be 20 characters or less.

Password text box—Type a unique password for the user. The password must be between 6 and 128 characters.

A JUNOScope software password should meet the following restrictions:

- Allow the full range of ASCII characters (except control characters).
- Enforce a minimum of 6 characters.
- Require a change in the character set, including uppercase, lowercase, numeric, and punctuation.

Confirm Password text box—Retype the user password to confirm it.

User Group list box—Select the permissions or access privileges for the user, for JUNOScope software operations. Click the down-arrow to display the available options: adminstrator, read-write user, and read-only user.

No user privilege level is required to perform network planning tasks for the JUNOScope software. Planning tasks can be performed in the network operations center (NOC) by a network designer or engineer. These network planning tasks include the following:

- Determine which routers to connect to and manage
- Determine which users can access and use the software, and their permission levels
- Configure the JUNOS software on each router for the supported JUNOScript access protocols
- Configure the JUNOS software on each router for a digital certificate for the JUNOScript server
- Configure the JUNOS software on each router for each user you want to use the JUNOScope software
- Determine how often you want archive operations to occur on routers

  Table 48 on page 679 describes the authorization a user group has to perform JUNOScope software tasks and to access devices on the network that have been configured for element management.

Table 48: JUNOScope User Group Permissions and Access Privileges

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Install, reinstall, upgrade, or downgrade JUNOScope software	X	—	—	—	The JUNOScope software installation is performed by the application installer.
Upgrade JUNOScope from a previous release	—	—	—	—	If the installer upgrades the JUNOScope software from an earlier version, existing users are assign to one of the three pre-defined user groups (administrator, read-write user, read-only user), based on their existing permission level. In other words, users with superuser permission are put into the administrator user group; users with read-write permission are put to the read-write user user group; users with read-only permission are put into the read-only user user group.
Looking Glass					
Query	X	X	X	X	Looking Glass reports require read-write or read-only permissions to a selected device. When a user, under a given user group, runs a query, the Device list is populated only with devices with read or read-write access.
Configuration Manager					
Configuration Browser	X	X	X	X	Read-write or read-only permission is required for a user to browse a device configuration. The Device drop-down list box is populated only with devices with read-write or read-only access.
Configuration Editor	X	X	—	—	Read-write permission is required for a user to edit a device configuration. The Device drop-down list box is populated only with devices with read-write access.
Archive	X	X	—	—	Read-write permission is required for a user in a user group to archive a configuration in the JUNOScope repository. The Group and Select Device(s) drop-down list boxes are populated only with groups or devices with read-write access.
Archive Tag	X	X	—	—	Superuser or read-write permission is required to use Archive Tags. The Selected Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.

Table 48: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Audit Configurations	X	X	—	—	Superuser or read-write permission is required to use Audit Configurations. The Selected Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.
Audit Partial Configuration	X	X	—	—	Superuser or read-write permission is required to use Audit Partial Configurations. The Select Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.
Import	X	X	—	—	Read-write permission is required for a user to import a configuration into the JUNOScope repository. Importing a configuration does not have any association with a device, therefore the user group requirement for import is read-write access for any device.
Compare	X	X	X	X	Read-write or read-only permission is required for a user to compare configuration file versions in the JUNOScope repository. The Device drop-down list box is populated only with devices with read-write or read-only access.
Display	X	X	X	X	Read-write or read-only permission is required for a user to view a configuration file in the JUNOScope repository. The Device drop-down list box is populated only with devices with read-write or read-only access.
Load Configuration	X	X	—	—	Read-write permission is required for a user to deploy an imported configuration file to multiple routers and perform a simultaneous update of configurations on these devices. The Select Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.
Restore	X	X	—	—	The Device drop-down is populated only with devices with read-write access.
Delete	X	X	—	—	

Table 48: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
					Superuser or read-write permission is required to delete an imported configuration file. The name column lists the imported configuration files in the CVS repository.
Edit	X	X	—	—	Superuser or read-write permission is required to edit a configuration file. The Configuration File drop-down list box lists archived configuration files and the Device drop-down list box lists the devices from which the configuration file has been archived.
Save	X	X	—	—	Superuser or read-write permission is required to save a configuration file to a local machine. The Configuration File drop-down list box lists archived configuration files and the Device drop-down list box lists the devices from which the configuration file has been archived.
Scripts	X	X	—	—	Superuser or read-write permission is required to manage JUNOS-based scripts. JUNOS-based scripts such as commit scripts, operation (op) scripts, and event scripts can be imported into the JUNOScope CVS repository from the local file system and deployed to a group of routers.You can also view, edit, compare, and disable these scripts.
Inventory Management					
Scan	X	—	—	—	The Group and the Select Device(s) drop-down is populated only with groups or devices with read-write access.
Reports > Inventory	X	X	X	X	The Device drop-down in the Search and Advanced Query dialog boxes are limited to those devices with read or read-write access. In the Custom Report page, only those reports created by users in the same user group are visible. Read-only users cannot save or delete custom reports.
Reports > Demo	X	X	X	X	Read-only users cannot save or delete custom reports.
Repository > Schedule	X	X	—	—	Superuser or read-write permission is required.
Repository > View	X	X	—	—	

Table 48: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
					Superuser or read-write permission is required.
Software Manager					
Images	X	—	—	—	Device read-write access is required for users in a user group to perform operations, including image import, download, install, and delete.
Monitor					
Operations	X	X	X	X	Only those operations scheduled by users in the same user group are visible. Users in the Administrator user group can view all operations. Read-only users cannot delete operations.
Status	X	X	X	X	The Group and Selected Device drop-down list boxes are limited to those devices with read-only or read-write access. Even when All Devices is selected, a subset of the device operation status is shown, based on the user group. Users in the administrator user group can view all status.
Audit Log	X	—	—	—	Users in the administrator user group can only view Audit Log events.
Purge	X	—	—	—	Users in the administrator user group can purge Status records and Audit Log events.
Settings					
Authentication Information	X	—	—	—	Only users in the administrator user group can view this page.
Access Methods	X	—	—	—	Only users in the administrator user group can view this page.
Devices	X	—	—	—	Only users in the administrator user group can view this page.
Groups	X	—	—	—	Only users in the administrator user group can view this page.
Labels	X	—	—	—	Only users in the administrator user group can view this page.
Schedules	X	—	—	—	Only users in the administrator user group can view this page.

Table 48: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Users > Local Authentication	X	—	—	—	Only users in the administrator user group can view this page.
Users > User Group Authorization	X	—	—	—	Only users in the administrator user group can view this page.
User > Authentication Policy > Global Authentication	X	—	—	—	Only users in the administrator user group can view this page.
User > Authentication Policy > User Authentication Policy	X	—	—	—	Only users in the administrator user group can view this page.
RADIUS Configuration	X	—	—	—	Only users in the administrator user group can view this page.
Import/Export Data	X	—	—	—	Only users in the administrator user group can view this page.
Saved Operations	X	X	—	—	Only those operations saved by users in the same user group are visible in the Available Operations list box, in the Add Compound Operations dialog box.

OK button—Adds the user to the JUNOScope software database and redisplays the Users—Local Authentication dialog box with the new username and permissions listed in the table.

Cancel button—Clears this dialog box without adding a new user and redisplays the Users—Local Authentication.

Users—Local Authentication—Edit User Dialog Box

Description Use the Users—Local Authentication—Edit User dialog box to edit user information for accessing the JUNOScope software operations.

Navigation Click Settings > Users > Local Authentication. Select the user you want to edit in the Users—Local Authentication dialog box, and click Edit.

Permissions Superuser

Elements Username text box—Edit the name of the selected user. The username must be 20 characters or less.

Password text box—Type a unique password for the user. The password must be between 6 and 128 characters.

A JUNOScope software password should meet the following restrictions:

- Allow the full range of ASCII characters (except control characters).
- Enforce a minimum of 6 characters.
- Require a change in the character set, including uppercase, lowercase, numeric, and punctuation.

Confirm Password text box—Type the password again to confirm it.

User Group list box—Select the list of user groups the to which the user belongs.

No user privilege level is required to perform network planning tasks for the JUNOScope software. Planning tasks can be performed in the network operations center (NOC) by a network designer or engineer. These network planning tasks include the following:

- Determine which routers to connect to and manage
- Determine which users can access and use the software, and their permission levels
- Configure the JUNOS software on each router for the supported JUNOScript access protocols
- Configure the JUNOS software on each router for a digital certificate for the JUNOScript server
- Configure the JUNOS software on each router for each user you want to use the JUNOScope software
- Determine how often you want archive operations to occur on routers

Table 49 on page 686 describes the authorization a user group has to perform JUNOScope software tasks and to access devices on the network that have been configured for element management.

Table 49: JUNOScope User Group Permissions and Access Privileges

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Install, reinstall, upgrade, or downgrade JUNOScope software	X	—	—	—	The JUNOScope software installation is performed by the application installer.
Upgrade JUNOScope from a previous release	—	—	—	—	If the installer upgrades the JUNOScope software from an earlier version, existing users are assign to one of the three pre-defined user groups (administrator, read-write user, read-only user), based on their existing permission level. In other words, users with Superuser permission are put into the administrator user group; users with read-write permission are put to the read-write user user group; users with read-only permission are put into the read-only user user group.
Looking Glass					
Query	X	X	X	X	Looking Glass reports require read-write or read-only permissions to a selected device. When a user, under a given user group, runs a query, the Device list is populated only with devices with read or read-write access.
Configuration Manager					
Configuration Browser	X	X	X	X	Read-write or read-only permission is required for a user to browse a device configuration. The Device drop-down list box is populated only with devices with read-write or read-only access.
Configuration Editor	X	X	—	—	Read-write permission is required for a user to edit a device configuration. The Device drop-down list box is populated only with devices with read-write access.
Archive	X	X	—	—	Read-write permission is required for a user in a user group to archive a configuration in the JUNOScope repository. The Group and Select Device(s) drop-down list boxes are populated only with groups or devices with read-write access.
Archive Tag	X	X	—	—	Superuser or read-write permission is required to use Archive Tags. The Selected Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.

Table 49: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Audit Configurations	X	X	—	—	Superuser or read-write permission is required to use Audit Configurations. The Selected Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.
Audit Partial Configuration	X	X	—	—	Superuser or read-write permission is required to use Audit Partial Configurations. The Select Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.
Import	X	X	—	—	Read-write permission is required for a user to import a configuration into the JUNOScope repository. Importing a configuration does not have any association with a device, therefore the user group requirement for import is read-write access for any device.
Compare	X	X	X	X	Read-write or read-only permission is required for a user to compare configuration file versions in the JUNOScope repository. The Device drop-down list box is populated only with devices with read-write or read-only access.
Display	X	X	X	X	Read-write or read-only permission is required for a user to view a configuration file in the JUNOScope repository. The Device drop-down list box is populated only with devices with read-write or read-only access.
Load Configuration	X	X	—	—	Read-write permission is required for a user to deploy an imported configuration file to multiple routers and perform a simultaneous update of configurations on these devices. The Select Device(s) drop-down list box is populated only with devices with read-write access. The group drop-down list box is populated with device groups with read-write access.
Restore	X	X	—	—	The Device drop-down is populated only with devices with read-write access.
Delete	X	X	—	—	

Table 49: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
					Superuser or read-write permission is required to delete an imported configuration file. The name column lists the imported configuration files in the CVS repository.
Edit	X	X	—	—	Superuser or read-write permission is required to edit a configuration file. The Configuration File drop-down list box lists archived configuration files and the Device drop-down list box lists the devices from which the configuration file has been archived.
Save	X	X	—	—	Superuser or read-write permission is required to save a configuration file to a local machine. The Configuration File drop-down list box lists archived configuration files and the Device drop-down list box lists the devices from which the configuration file has been archived.
Scripts	X	X	—	—	Superuser or read-write permission is required to manage JUNOS-based scripts. JUNOS-based scripts such as commit scripts, operation (op) scripts, and event scripts can be imported into the JUNOScope CVS repository from the local file system and deployed to a group of routers.You can also view, edit, compare, and disable these scripts.
Inventory Management					
Scan	X	—	—	—	The Group and the Select Device(s) drop-down is populated only with groups or devices with read-write access.
Reports > Inventory	X	X	X	X	The Device drop-down in the Search and Advanced Query dialog boxes are limited to those devices with read or read-write access. In the Custom Report page, only those reports created by users in the same user group are visible. Read-only users cannot save or delete custom reports.
Reports > Demo	X	X	X	X	Read-only users cannot save or delete custom reports.
Repository > Schedule	X	X	—	—	Superuser or read-write permission is required.
Repository > View	X	X	—	—	

Table 49: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
					Superuser or read-write permission is required.
Software Manager					
Images	X	—	—	—	Device read-write access is required for users in a user group to perform operations, including image import, download, install, and delete.
Monitor					
Operations	X	X	X	X	Only those operations scheduled by users in the same user group are visible. Users in the Administrator user group can view all operations. Read-only users cannot delete operations.
Status	X	X	X	X	The Group and Selected Device drop-down list boxes are limited to those devices with read-only or read-write access. Even when All Devices is selected, a subset of the device operation status is shown, based on the user group. Users in the administrator user group can view all status.
Audit Log	X	—	—	—	Users in the administrator user group can only view Audit Log events.
Purge	X	—	—	—	Users in the administrator user group can purge Status records and Audit Log events.
Settings					
Authentication Information	X	—	—	—	Only users in the administrator user group can view this page.
Access Methods	X	—	—	—	Only users in the administrator user group can view this page.
Devices	X	—	—	—	Only users in the administrator user group can view this page.
Groups	X	—	—	—	Only users in the administrator user group can view this page.
Labels	X	—	—	—	Only users in the administrator user group can view this page.
Schedules	X	—	—	—	Only users in the administrator user group can view this page.

Table 49: JUNOScope User Group Permissions and Access Privileges *(continued)*

JUNOScope Operation	Superuser	Read-Write	Read-Only	None	Comments
Installation					
Users > Local Authentication	X	—	—	—	Only users in the administrator user group can view this page.
Users > User Group Authorization	X	—	—	—	Only users in the administrator user group can view this page.
User > Authentication Policy > Global Authentication	X	—	—	—	Only users in the administrator user group can view this page.
User > Authentication Policy > User Authentication Policy	X	—	—	—	Only users in the administrator user group can view this page.
RADIUS Configuration	X	—	—	—	Only users in the administrator user group can view this page.
Import/Export Data	X	—	—	—	Only users in the administrator user group can view this page.
Saved Operations	X	X	—	—	Only those operations saved by users in the same user group are visible in the Available Operations list box, in the Add Compound Operations dialog box.

OK button—Adds the edited user information to the JUNOScope software database. The Users—Local Authentication dialog box redisplays with the edited username and permissions.

Cancel button—Clears this dialog box without changing user information and redisplays the JUNOScope main window.

Users—Local Authentication—Import Users Dialog Box

Description Use the Users—Local Authentication—Import Users dialog box to import user setup information into the JUNOScope software without having to manually enter it. The default import filename for users is junoscope-users.xml.

Navigation Click Settings > Users. Click Import in the Users—Local Authentication dialog box.

Permissions Superuser

Elements File to import text box—Lets you type or browse to the XML file to import.

Browse button—Displays the File Open dialog box so you can select the XML file to import.

Import Options—Select an import method to be used if a conflict occurs between existing records stored in the JUNOScope server and imported records when synchronizing JUNOScope settings imported from multiple servers. The available import method options include:

- Ignore—(Default) An existing record stored in the JUNOScope server takes precedence over any imported record. The imported record is ignored and the existing record is not affected. Any imported record that does not exist in the JUNOScope server is inserted.

- Merge—If a record exists in the JUNOScope server and also exists in the imported record, the imported record is merged with the existing record and is augmented as necessary. If an imported record is in conflict with an existing record, the imported record takes precedence over the existing record. The existing record is merged with the imported record; however, the fields of the imported record take precedence over the fields of the existing record. Any imported record that does not exist in the JUNOScope server is inserted.

- Override—All records in the JUNOScope server are deleted, then all imported records are inserted. Before the override operation occurs, a message window appears with the following confirmation prompt: “The import with override option will delete all the existing records. Do you want to continue?” Select Yes or No to continue.

Import button—Imports the selected saved operations data into the JUNOScope software and displays the Import Results dialog box.

When importing users, if the password is not encrypted, the passwords must meet the following restrictions:

- Allow the full range of ASCII characters (except control characters).
- Enforce a minimum of 6 characters.
- Require a change in the character set, including uppercase, lowercase, numeric, and punctuation.

  If password checking fails, the import will fail. After the import operation is completed, the Import Results dialog box displays the import results and reason for failure.

Cancel button—Clears this dialog box and displays the Users—Local Authentication dialog box.

Part 12

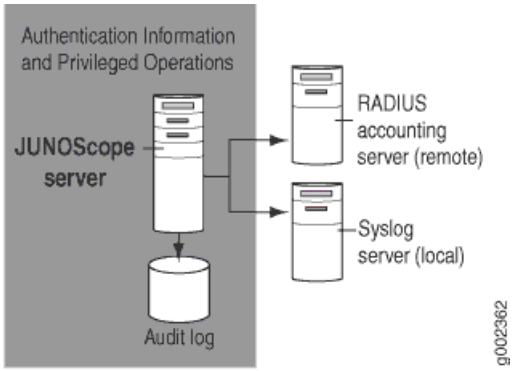
System Log Messages and RADIUS Accounting Attributes

Chapter 40

JUNOScope System Log Messages

JUNOScope events are stored in the JUNOScope database and are subsequently sent to the system log server and an optional RADIUS accounting server if one is configured (see Figure 18 on page 695).

Figure 18: JUNOScope Security-Enhanced Sensitive Data Logging



The JUNOScope software generates events or system log messages based on the status of the following operations, and forwards them to the local system log server.

- User login success
- User login failure attempt
- User account automatically locked
- User account locked and unlocked by the JUNOScope administrator using Users > Authentication Policy
- A new user account added, existing user account deleted, or existing user account password changed using Users > Local Authentication
- A new device is deleted or existing device is edited or deleted using Settings > Devices
- A label association is changed using Settings > Labels
- A configuration is committed to a device using Configuration > Current > Edit
- Completed Archive operations—When an archive of a device is performed the first time or some change in configuration is done after the last successful archive of that device.

- Completed Inventory Scan operations—When an inventory scan is performed the first time or after a change in the inventory after the last successful scan.
- Completed Restore operations—When a configuration is successfully restored on a device.
- The success or failure of a JUNOScope operation—This information is reflected in the system log message severity level.
- The final status of each leaf operation shown on the Monitor Status Page. For example, for an operation named archive edge routers, which consists of a group of edge routers edge1, edge2, and edge3, the success (or failure) status of archive edge1, archive edge2, and archive edge3 will be forwarded to the system log.
- All information recorded in the JUNOScope View Status page (Monitor > Status).

Each system log message identifies the JUNOScope software process that generated the message and briefly describes the operation or error that occurred.

This chapter includes the following topics:

Configuring JUNOScope System Log Output

The JUNOScope system log output is enabled during installation by default.

During the JUNOScope installation process, the installer is prompted for the following:

```
Please enter the syslog facility (local0-local7) [local2]:
```

The syslog facility indicates a pipe where the syslog daemon (syslogd) sends the JUNOScope software system log messages that it receives. The administrator can enter the values local0, local1, local2, local3, local4, local5, local6, or local7 that correspond to a logging facility. The default is local2, which is logging facility 2.

The JUNOScope administrator can change the syslog facility at any time by reconfiguring JUNOScope using the jtk-setup.sh script.

Interpreting JUNOScope System Log Messages

The syntax of a JUNOScope system log message is as follows:

```
timestamp message-source:code:message-text
```

Table 50 on page 697 defines each JUNOScope system log message field.

Table 50: JUNOScope System Log Message Field Syntax

Field	Description
timestamp	Time when the message was logged.
message-source	The identifier of the process or component that generated the message. The format of the *message-source* field is: hostname process[process-ID] Where *process* is identified by source code module (for example, junoscope) concatenated by the HTTP port where JUNOScope is running.
code	Code that uniquely identifies the message. The name begins with a prefix that indicates the generating software process or library.
message-text	Text of the message.

Sample System Log Output

The following is a sample JUNOScope software system log message output:

```
Jun 20 13:00:05 valhalla2 junoscope7080[9348]: JUNOSCOPE_LOGIN_FAILURE:
  Login failed using username: 'admin'
```

Table 51 on page 697 defines the sample JUNOScope software system log message fields.

Table 51: Sample JUNOScope Software Log Message Fields

Field	Description
Jun 20 13:00:05	Timestamp (time when the message was logged)
valhalla2	Hostname
junoscope7080[9348]:	Source code module concatenated with the HTTP port where JUNOScope is running and the process ID
JUNOSCOPE_LOGIN_FAILURE	Error message tag
Login failed using username: 'admin'	Log message

JUNOScope System Log Messages

This section describes the JUNOScope software system log messages.

- Start/Stop the JUNOScope Software Messages on page 698
- Login/Logout JUNOScope Software Messages on page 699
- Authentication Policy Change Messages on page 702

Start/Stop the JUNOScope Software Messages

JUNOSCOPE_STARTUP

Audit Log Message JUNOScope started: server address: '<server_ address' https port no: '<https port no>' time: '<time when junoscope started>

System Log Message JUNOSCOPE_STARTUP
JUNOScope started: server address: '<server address>' https port no: '<https port no>' time: '<time when JUNOScope started' by username: '<user name> 'client address: '<client address>'

Description The JUNOScope software was started.

RADIUS Attributes
- Acct-Status-Type: Start
- Juniper-JUNOScope-Priv-Op: JUNOSCOPE_STARTUP
- Juniper-JUNOScope-Target: < https URL for JUNOScope >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_SHUTDOWN

Audit Log Message JUNOScope shutdown: server address: '<server_ address' https port no: '<https port no>' time: '<time when junoscope started>'

System Log Message JUNOSCOPE_SHUTDOWN:
JUNOScope shutdown: server address: '<server address>' https port no: '<https port no>' time: '<time when JUNOScope started>' by username: '<user name>' client address: '<client address>'

Description The JUNOScope software was shut down.

RADIUS Attributes:

- Acct-Status-Type: Stop
- Juniper-JUNOScope-Priv-Op: JUNOSCOPE_SHUTDOWN
- Juniper-JUNOScope-Target: < https URL for JUNOScope >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Login/Logout JUNOScope Software Messages

JUNOSCOPE_LOGIN_FAILURE

System Log Message JUNOSCOPE_LOGIN_FAILURE:
Failed to login: username: '<user name>' client address: '<client address>'

Description The user failed to login because of an invalid username or password.

RADIUS Attributes (For RADIUS, this is implemented as two messages: a session start followed immediately by a session end.)

- Message 1:
  Acct-Status-Type: Start
  Juniper-JUNOScope-Client-Address: < client address >
- Message 2:
  Account-Status-Type: Stop
  Account-Terminate-Cause: User Error
  Juniper-JUNOScope-Login-Failure-Reason: < Authentication Failure | User Account Locked >
  Juniper-JUNOScope-Client Address: < client address >

Type Error

Severity Error

Action Contact the system administrator.

JUNOSCOPE_LOGIN_SUCCESS

System Log Message JUNOSCOPE_LOGIN_SUCCESSFUL:
User logged in: username: '<user name>' client address: '<client address>'

RADIUS Attributes (For RADIUS, this is implemented as two messages: a session start followed immediately by a session end.)

- Message 1:
  Acct-Status-Type: Start
  Juniper-JUNOScope-Client-Address: < client address >
- Message 2:
  Account-Status-Type: Stop
  Account-Terminate-Cause: User Error
  Juniper-JUNOScope-Login-Failure-Reason: < Authentication Failure | User Account Locked >
  Juniper-JUNOScope-Client Address: < client address >

Type Error

Severity Error

Action Contact the system administrator.

RADIUS Attributes (For RADIUS, this is implemented as two messages: a session start followed immediately by a session end.)

- Message 1:
  Acct-Status-Type: Start
  Juniper-JUNOScope-Client-Address: < client address >
- Message 2:
  Account-Status-Type: Stop
  Account-Terminate-Cause: User Error
  Juniper-JUNOScope-Login-Failure-Reason: < Authentication Failure | User Account Locked >
  Juniper-JUNOScope-Client Address: < client address >

Type Error

Severity Error

Action Contact the system administrator.

Description A user successfully logged in.

RADIUS Attributes Acct-Status-Type: Start
Juniper-JUNOScope-Client Address: < client address >

Type Event

Severity Info

JUNOSCOPE_LOGOUT

Audit Message User logged in.

System Log Message UNOSCOPE_LOGOUT:
User logged out: username: '<user name>' client address: '<client address>'J

Description A user logged out.

RADIUS Attributes Acct-Status-Type: Stop
Juniper-JUNOScope-Client Address: < client address >

Type Event

Severity Info

JUNOSCOPE_SESSION_TIMEOUT

System Log Message JUNOSCOPE_SESSION_TIMEOUT:
User session timed out: username: '<user name>' client address: '<client address>'

Description A user successfully logged in.

RADIUS Attributes

- Acct-Status-Type:
  Start
- Acct-Terminate-Cause:
  Session Timeout

Type Event

Severity Info

JUNOSCOPE_USER_AUTO_LOCKED

Audit Message User locked: username: “ <user name>’

System Log Message JUNOSCOPE_USER_AUTO_LOCKED:
User locked: username: '<user name>' client address: '<client address>'

Description A user is automatically locked from logging in to the JUNOScope software because the number of consecutive login failure attempts within the configured Access Window equals the Maximum Login Attempts value.

RADIUS Attributes (For RADIUS, this event is implemented as two messages: a session start followed immediately by a session end.)

- Message 1:
  Acct-Status-Type: Start
  Juniper-JUNOScope-Client-Address: < client address >
- Message 2:
  Acct-Status-Type: Stop

User-Name: < user name >
Juniper-JUNOScope-Login-Failure-Reason: < user locked | login failure >
Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Authentication Policy Change Messages

JUNOSCOPE_USER_LOCKED_BY_ADMIN

Audit Message User locked: username: ‘<user name>’ by user: ‘<admin user name>’

System Log Message JUNOSCOPE_USER_LOCKED_BY_ADMIN:
User locked: username: '<user name>' client address: '<client address>' by user:'<admin user name>

Description A user is locked from logging in to the JUNOScope software by the administrator using the Authentication Policy user interface.

RADIUS Attributes

- Account-Status-Type: Interim-Update
- Juniper-JUNOScope-Target: < user name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_USER_UNLOCKED_BY_ADMIN

Audit Message User unlocked: username: ‘<user name>’ by user: ‘<admin user name>’

System Log Message JUNOSCOPE_USER_LOCKED_BY_ADMIN:
User unlocked: username: '<user name>' client address: '<client address>' by user:'<admin user name>

Description A user is unlocked from logging in to the JUNOScope software by the administrator using the Authentication Policy user interface.

RADIUS Attributes

- Acct-Status-Type: Interim-Update User-Name: < user name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_GLOBAL_POLICY_CHANGED

Audit Message Global policy changed.

System Log Message JUNOSCOPE_GLOBAL_POLICY_CHANGED:
Global Policy Changed.

Description The global policy changed.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: GLOBAL_POLICY_CHANGED
- Juniper-JUNOScope-Target: Global Policy
- Juniper-JUNOScope-Client-Address: <client address>

Type Event

Severity Info

Users Setup Messages

JUNOSCOPE_USER_CREATED

Audit Message User created: user: ‘<new user name>’

System Log Message JUNOSCOPE_USER_CREATED:
User created: user: '<new user name>' by username: '<user name>' client address: '<client address>'

Description A new user was created.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: USER_CREATED
- Juniper-JUNOScope-Target: <user name>
- Juniper-JUNOScope-Client-Address: <client address>

Type Event

Severity Info

JUNOSCOPE_USER_DELETED

Audit Message User deleted: user: ‘<deleted user name>’

System Log Message JUNOSCOPE_USER_DELETED:
User deleted: user: '<deleted user name>' by username: '<user name>' client address: '<client address>'

Description A user was deleted.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: USER_DELETED
- Juniper-JUNOScope-Target: < user name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_USER_PASSWORD_CHANGED

Audit Message Password changed: user: ‘<user name>’

System Log Message JUNOSCOPE_USER_PASSWORD_CHANGED:
Password changed: user: '<user name>' by username: '<user name>' client address: '<client address>'

Description A user's password was changed.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: USER_PASSWORD_CHANGED
- Juniper-JUNOScope-Target: < user name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

User Group Authorization Messages

JUNOSCOPE_USERGROUP_CREATED

Audit Log Message User group created: user group: '<user group name>'

System Log Message JUNOSCOPE_USERGROUP_CREATED
User group created: user group: '<user group name' by username: '<user name>' client address: '<client address>'

Description A new user group has been created.

JUNOSCOPE_USERGROUP_PERM_CHANGED

Audit Message User group permission changed: user group name: '<user group_name>'

System Log Message JUNOSCOPE_USERGROUP_PERM_CHANGED

User group permission changed: user group name: '<user group name>' by username: '<user name>' client address: '<client address>'

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Priv-Op: USERGROUP_CREATED
- Juniper-JUNOScope-Target: <user group name>
- Juniper-JUNOScope-Client-Address: <client address>
- Juniper-JUNOScope-Client-Address: <client address>

Type Event

Severity Info

Description The user group permission has changed.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Priv-Op: USERGROUP_PERM_CHANGED
- Juniper-JUNOScope-Target: <user group name>
- Juniper-JUNOScope-Client-Address: <client address>

Type Event

Severity Info

JUNOSCOPE_USERGROUP_DELETED

Audit Log Message User group deleted: user group name: '<user group_name>'

System Log Message JUNOSCOPE_USERGROUP_DELETED
User group deleted: user group name: '<user group name>' by username: '<user name>' client address: '<client address>'J

Description The user group has been deleted.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Priv-Op: USERGROUP_PERM_CHANGED
- Juniper-JUNOScope-Target: <user group name>
- Juniper-JUNOScope-Client-Address: <client address>

Type Event

Severity Info

JUNOSCOPE_USERGROUP_USER_ASSOC_CHANGED

Audit Log Message User group to user association added/removed: user group name: '<user group_name>' user name: '<association changed user name>'

System Log Message JUNOSCOPE_USERGROUP_USER_ASSOC_CHANGED
User group to user association added/removed: user group name: '<user group name>' username: '<association changed user name>' by username: '<user name>' client address: '<client address>'

Description The user group to user association has been either removed or added.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Priv-Op: USERGROUP_PERM_CHANGED
- Juniper-JUNOScope-Target: < user group name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

RADIUS Configuration Messages

JUNOSCOPE_RADIUS_CONFIG_ADDED

Audit Message RADIUS configuration added: RADIUS server address: '<RADIUS server address>'

System Log Message JUNOSCOPE_RADIUS_CONFIG_ADDED:
RADIUS configuration added: RADIUS server address: <RADIUS server address> client address: '< client address> '

Description A new RADIUS configuration entry was added.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- JUNIPER-JUNOScope-Target: < RADIUS server address >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_RADIUS_CONFIG_CHANGED

Audit Message RADIUS configuration changed: RADIUS server address: '<RADIUS server address>'

System Log Message JUNOSCOPE_RADIUS_CONFIG_CHANGED:
RADIUS configuration changed: RADIUS server address: <RADIUS server address> client address: '< client address>'

Description An existing RADIUS configuration entry was edited.

RADIUS Attributes:
- Acct-Status-Type: Interim-Update
- JUNIPER-JUNOScope-Target: < RADIUS server address >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_RADIUS_CONFIG_DELETED

Audit Message RADIUS configuration deleted: RADIUS server address: '<radius server address>'

System Log Message: JUNOSCOPE_RADIUS_CONFIG_DELETED:
RADIUS configuration deleted: RADIUS server address:<RADIUS server address> client address: '< client address>'

Description An existing RADIUS configuration entry was deleted.

RADIUS Attributes:
- Acct-Status-Type: Interim-Update
- JUNIPER-JUNOScope-Target: < RADIUS server address >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Authentication Information Setup Messages

JUNOSCOPE_AUTH_INFO_CHANGED

Audit Message Authentication information changed: name: '<authentication information name>'

System Log Message JUNOSCOPE_AUTH_INFO_CHANGED:
Authentication information changed: name: '<auth info name>' by username: '<user name>' client address: '<client address>'

Description Device authentication information was changed.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: AUTH_INFO_CHANGED
- Juniper-JUNOScope-Target: < auth info name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Access Methods Setup Messages

JUNOSCOPE_ACCESS_METHOD_CHANGED

Audit Message Access method changed: name: access method: ‘<access method name>’

System Log Message JUNOSCOPE_ACCESS_METHOD_CHANGED:
Access method changed: access method: '<access method name>' by username: '<user name>' client address: '<client address>'

Description An access method was changed.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: ACCESS_METHOD_CHANGED
- Juniper-JUNOScope-Target: < access method name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Labels Setup Messages

JUNOSCOPE_LABEL_ASSOC_CHANGED

Audit Message Label association added/removed: label: ‘<Label name>’ device: ‘<device name>’

System Log Message JUNOSCOPE_LABEL_ASSOC_CHANGED:
Label associations changed: label: '<label name>' by username: '<user name>' client address: '<client address>'

Description The devices associated with a label were changed.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: LABEL_ASSOC_CHANGED
- Juniper-JUNOScope-Target: < label name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Configuration Edit Messages

JUNOSCOPE_COMMIT_PERFORMED

Audit Message Commit done on device <device name>

System Log Message JUNOSCOPE_COMMIT_PERFORMED:
Commit performed: device: '<device name>' by username: '<user name>' client address: '<client address>'

Description A user committed a configuration on a device.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: COMMIT_PERFORMED
- Juniper-JUNOScope-Target: < device name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Archive Configuration Messages

JUNOSCOPE_ARCHIVE_CONNECTION_ERROR

System Log Message JUNOSCOPE_ARCHIVE_CONNECTION_ERROR:
Could not connect to device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description An archive operation failed because the connection could not be established with the device.

Type Error

Severity Error

Action Contact System Administrator

JUNOSCOPE_ARCHIVE_NO_ACCESS_INFO_ERROR

System Log Message JUNOSCOPE_ARCHIVE_NO_ACCESS_INFO_ERROR:
Could not find access information for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description An archive operation failed because no access information for the device was found.

Type Error

Severity Error

Action Contact System Administrator

JUNOSCOPE_ARCHIVE_NO_CHANGE

System Log Message JUNOSCOPE_ARCHIVE_NO_CHANGE:
No change in configuration for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description No change in the configuration was found after the last archive.

Type Event

Severity Info

JUNOSCOPE_ARCHIVE_SUCCESS

Audit Message Successfully archived device: '<device name>' revision: '<revision>'

System Log Message JUNOSCOPE_ARCHIVE_SUCCESS:
Successfully archived device: '<device name>' revision: '<revision>' operation name: '<operation name>' operation type:'<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description A user successfully archived a device configuration.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: ARCHIVE_SUCCESS
- Juniper-JUNOScope-Target: < device name >

Type Event

Severity Info

JUNOSCOPE_ARCHIVE_SYSTEM_ERROR

System Log Message JUNOSCOPE_ARCHIVE_SYSTEM_ERROR:
A System error occurred during archive operation for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description An archive operation failed because a system error occurred.

Type Error

Severity Error

Action Contact System Administrator

Inventory Scan Messages

JUNOSCOPE_SCAN_CONNECTION_ERROR

System Log Message JUNOSCOPE_SCAN_CONNECTION_ERROR:
Could not open connection to device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description An Inventory Management System scan operation failed because a connection could not be established with the device.

Type Error

Severity Error

Action Contact System Administrator

JUNOSCOPE_SCAN_NO_ACCESS_INFO_ERROR

System Log Message JUNOSCOPE_SCAN_NO_ACCESS_INFO_ERROR:
Could not find access information for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description An Inventory Management System scan failed because no access information for the device was found.

Type Error

Severity Error

Action Contact System Administrator

JUNOSCOPE_SCAN_NO_CHANGE

System Log Message JUNOSCOPE_SCAN_NO_CHANGE:
No change in inventory database for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description No change in inventory was found after the last scan.

Type Event

Severity Info

JUNOSCOPE_SCAN_SUCCESS

System Log Message JUNOSCOPE_SCAN_SUCCESS:

Successfully scanned items into inventory database for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description A device was successfully scanned.

Type Event

Severity Info

JUNOSCOPE_SCAN_SYSTEM_ERROR

System Log Message JUNOSCOPE_SCAN_SYSTEM_ERROR:
A System error occurred during inventory scan operation for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description An Inventory Management System scan operation failed because a system error occurred.

Type Error

Severity Error

Action Contact System Administrator

Inventory Reports Messages

JUNOSCOPE_REPORT_SUCCESS

System Log Message JUNOSCOPE_REPORT_SUCCESS:
Successfully generated report: '<report name>' username: '<username>'

Description A custom report is successfully archived

Type Event

Severity Info

JUNOSCOPE_REPORT_ERROR

System Log Message JUNOSCOPE_REPORT_ERROR:
Error while generating report: '<report name>' username: '<username>'

Description Failed to archive a custom report

Type Error

Severity Error

Action Contact System Administrator

Restore Configuration Messages

JUNOSCOPE_RESTORE_CONNECTION_ERROR

System Log Message JUNOSCOPE_RESTORE_CONNECTION_ERROR:
Could not open connection to device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description A restore configuration operation failed because a connection could not be established with the device.

Type Error

Severity Error

Action Contact System Administrator

JUNOSCOPE_RESTORE_NO_ACCESS_INFO_ERROR

System Log Message JUNOSCOPE_RESTORE_NO_ACCESS_INFO_ERROR:
Could not find access information for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description A restore operation failed because no access information for the device was found.

Type Error

Severity Error

Action Contact System Administrator

JUNOSCOPE_RESTORE_SUCCESS

Audit Message Successfully restored device: '<device name>'

System Log Message JUNOSCOPE_RESTORE_SUCCESS:
Successfully restored configuration for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description A user successfully restored a configuration to a device.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: RESTORE_SUCCESS
- Juniper-JUNOScope-Target: < device name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_RESTORE_SYSTEM_ERROR

System Log Message JUNOSCOPE_RESTORE_SYSTEM_ERROR:
A System error occurred during restore operation for device: '<device name>' operation name: '<operation name>' operation type: '<operation type>' username: '<username>' start time:'<start time>' last updated time: '<last updated time>'

Description A restore operation failed because a system error occurred.

Type Error

Severity Error

Action Contact System Administrator

Devices Setup Messages

JUNOSCOPE_DEVICE_ADDED

Audit Message Device added: device: '<device name>'

System Log Message JUNOSCOPE_DEVICE_ADDED:
Device added: device: '<device name>' by username: '<user name>' client address: '<client address>'

Description A new device was added.

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: DEVICE_ADDED
- Juniper-JUNOScope-Target: <device name>
- Juniper-JUNOScope-Client-Address: <client address>

Type Event

Severity Info

JUNOSCOPE_DEVICE_CHANGED

Audit Message Device added: device: '<device name>'

System Log Message JUNOSCOPE_DEVICE_CHANGED:
Device changed: device: '<device name>' by username: '<user name>' client address: '<client address>'

Description The device setup information has changed.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: DEVICE_CHANGED
- Juniper-JUNOScope-Target: < device name >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_DEVICE_DELETED

Audit Message Device deleted: device: '<deleted device name>'

System Log Message JUNOSCOPE_DEVICE_DELETED:
Device deleted: device: '<device name>' by username: '<user name>' client address: '<client address>'

Description A device was deleted.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: DEVICE_DELETED
- Juniper-JUNOScope-Target: < device name >

Type Event

Severity info

Software Manager Messages

JUNOSCOPE_SOFTWARE_IMAGE_INSTALL

Audit Message Successfully installed image ‘<target version>’ on ‘<router>’

System Log Message JUNOSCOPE_SOFTWARE_IMAGE_INSTALL
Successfully installed image ‘<target-version>’ on ‘<router>’

Description A software image was successfully installed on a device.

RADIUS Attributes
- Acct-StatusType: 3
- Juniper-JUNOScope-Privileged-Command: SOFTWARE_IMAGE_INSTALL_SUCCESS
- Juniper-JUNOScope-Target: ‘ < deviceType > ’
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity info

JUNOSCOPE_SOFTWARE_IMAGE_INSTALL_ERROR

System Log Message JUNOSCOPE_SOFTWARE_IMAGE_INSTALL_ERROR
Installation failed: software ‘<package-info>’ is running instead of expected ‘<target-version>’ on ‘<hostname>’

Description A software image installation failed.

Type Event

Severity Error

Action Contact system administrator

JUNOSCOPE_SOFTWARE_IMAGE_DOWNLOAD

Audit Message Successfully downloaded image ‘<image-name> to target ‘router>’

System Log Message JUNOSCOPE_SOFTWARE_IMAGE_DOWNLOAD
Successfully downloaded image ‘<image-name>’ to target ‘<router>’

Description A software image has been downloaded on a device.

RADIUS Attributes

- Acct-StatusType: 3
- Juniper-JUNOScope-Privileged-Command: SOFTWARE_IMAGE_DOWNLOAD_SUCCESS
- Juniper-JUNOScope-Target: < device >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_SOFTWARE_IMAGE_DOWNLOAD_ERROR

System Log Message JUNOSCOPE_SOFTWARE_IMAGE_DOWNLOAD_ERROR
Download failed for image ‘<image-name>’

Description A software image download failed.

Type Event

Severity Error

Action Contact system administrator

JUNOSCOPE_SOFTWARE_IMAGE_IMPORT

System Log Message JUNOSCOPE_SOFTWARE_IMAGE_IMPORT

Successfully imported image %image by user %username

Description A software image was successfully imported.

RADIUS Attributes
- Acct-StatusType: 3
- Juniper-JUNOScope-Privileged-Command: SOFTWARE_IMAGE_IMPORT_SUCCESS

Type Event

Severity Info

JUNOSCOPE_SOFTWARE_IMAGE_IMPORT_ERROR

System Log Message JUNOSCOPE_SOFTWARE_IMAGE_IMPORT_ERROR
Import failedI

Description A software image import failed.

RADIUS Attributes
- Acct-StatusType:
- Juniper-JUNOScope-Privileged-Command:
- Juniper-JUNOScope-Target:

Type Event

Severity Error

Action Contact system administrator

JUNOSCOPE_SOFTWARE_IMAGE_DELETE

System Log Message JUNOSCOPE_SOFTWARE_IMAGE_DELETE
User %username deleted image %image

Description A user deleted a software image.

RADIUS Attributes
- Acct-StatusType: 3
- Juniper-JUNOScope-Privileged-Command: SOFTWARE_IMAGE_DELETE_SUCCESS

Type Event

Severity Info

Purge Log Messages

JUNOSCOPE_PURGE_AUDITLOG

Audit Message Purging Audit Log records. No. of records purged: '<No. of auditlog records purged>' comment: '<comment >' Username: '<user name>' Time:'<date and time when the event occurred>'

System Log Message JUNOSCOPE_PURGE_AUDITLOG
Purging Audit Log records. No. of records purged: '<No. of auditlog records purged>' comment: '<comment >' Username: '<user name>' Time:'<date and time when the event occurred>'

Description Purging Audit Log records.

RADIUS Attributes

- Acct-StatusType: Interim-Update
- Juniper-JUNOScope-Privileged-Command:PURGE_AUDITLOG
- Juniper-JUNOScope-Target: < No. of auditlog records purged >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_PURGE_STATUS

Audit Message Purging Status Log records. No. of records purged: '<No. of status records purged>' comment: '<comment >' Username: '<user name>' Time:'<date and time when the event occurred>'

System Log Message JUNOSCOPE_PURGE_STATUS:
Purging Status records. No. of records purged: '<No. of status records purged>' comment: '<comment >' Username: '<user name>' Time:'<date and time when the event occurred>'

Description Purging status records.

RADIUS Attributes

- Acct-StatusType: Interim-Update
- Juniper-JUNOScope-Privileged-Command:PURGE_STATUS
- Juniper-JUNOScope-Target: < No. of status records purged >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Audit Configuration Messages

JUNOSCOPE_CONFIG_AUDIT_DIFFERENCE

Audit Message There are difference for device: '<device name>' revisions '<revision1>' and '<revision2>'

System Log Message JUNOSCOPE_CONFIG_AUDIT_DIFFERENCE
Difference(s) found in configuration revisions <revision1> and <revision2> for device: <device> operation name: <operation_name> operation type: <operation_type> username:<username> start time: <start_time> last modified time: <last_modified>

Description Config Audit: Differences found.

RADIUS Attributes
- Acct-StatusType: Interim-Update
- Juniper-JUNOScope-Privileged-Command: CONFIG_AUDIT_DIFFERENCE
- Juniper-JUNOScope-Target: < device >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_CONFIG_AUDIT_NO_DIFFERENCE

Audit Message There are difference for device: '<device name>' revisions '<revision1>' and '<revision2>'

System Log Message JUNOSCOPE_CONFIG_AUDIT_NO_DIFFERENCE:
No difference in configuration revisions <revision1> and <revision2> for device: <device> operation name: <operation_name> operation type: <operation_type> username:<username> start time: <start_time> last modified time: <last_modified>

Description Config Audit: No differences found.

RADIUS Attributes
- Acct-StatusType: Interim-Update
- Juniper-JUNOScope-Privileged-Command: AUDIT_NO_DIFFERENCE
- Juniper-JUNOScope-Target: < device >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_PARTIAL_CONFIG_AUDIT_DIFF

Audit Message Difference(s) found between partial configuration<partial Config> revision: <revision>and running configuration on device: <device>done by username: <username>client address: <client_address>

System Log Message JUNOSCOPE_PARTIAL_CONFIG_AUDIT_DIFF:
Difference(s) found between partial configuration<partial Config> revision: <revision>and running configuration on device: <device>done by username: <username>client address: <client_address>

Description Partial Config Audit: Differences Found.

RADIUS Attributes
- Acct-StatusType: Interim-Update
- Juniper-JUNOScope-Privileged-Command: PARTIAL_CONFIG_AUDIT_DIFFERENCE
- Juniper-JUNOScope-Target: < device >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

JUNOSCOPE_PARTIAL_CONFIG_AUDIT_NO_DIFF

Audit Message No difference(s) found between partial configuration<partial Config> revision: <revision>and running configuration on device: <device>done by username: <username>client address: <client_address>

System Log Message JUNOSCOPE_PARTIAL_CONFIG_AUDIT_NO_DIFF:
No difference(s) found between partial configuration<partial Config> revision: <revision>and running configuration on device: <device>done by username: <username>client address: <client_address>

Description Partial Config Audit: No differences Found.

RADIUS Attributes
- Acct-StatusType: Interim-Update
- Juniper-JUNOScope-Privileged-Command: PARTIAL_CONFIG_AUDIT_NO_DIFFERENCE
- Juniper-JUNOScope-Target: < device >
- Juniper-JUNOScope-Client-Address: < client address >

Type Event

Severity Info

Advanced Insight Scripts Messages

JUNOSCOPE_PVS_EXPORT_DEVICES

Audit Message Export devices to user: '%username' client address:'%client_address'

System Log Message Export devices to user: '%username' client address: '%client_address'

Description All JUNOScope managed devices are exported to PvS Gateway.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_EXPORT_DEVICES

Type Event

Severity Info

JUNOSCOPE_PVS_BUNDLE_UPLOAD

Audit Message Successfully uploaded PvS bundle %filename by user %username

System Log Message Successfully uploaded PvS bundle %filename by user %username

Description A PvS bundle is uploaded into the JUNOScope repository.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_BUNDLE_UPLOAD_SUCCESS

Type Event

Severity Info

JUNOSCOPE_PVS_BUNDLE_UPLOAD_ERROR

Audit Message Upload failed: %message

System Log Message Upload failed: %message

Description A PvS bundle failed to upload into the JUNOScope repository.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_BUNDLE_UPLOAD_ERROR

Type Event

Severity Error

JUNOSCOPE_PVS_BUNDLE_INSTALL

Audit Message Successfully installed PvS bundle on target %device

System Log Message Successfully installed PvS bundle on target %device

Description A PvS bundle is installed successfully on the device.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_BUNDLE_INSTALL_SUCCESS

Type Event

Severity Info

JUNOSCOPE_PVS_BUNDLE_INSTALL_ERROR

Audit Message Installation failed for PvS bundle %bundlename

System Log Message Installation failed for PvS bundle %bundlename

Description A PvS bundle failed to install.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_BUNDLE_INSTALL_ERROR

Type Event

Severity Error

JUNOSCOPE_PVS_BUNDLE_UNINSTALL

Audit Message Successfully uninstalled PvS bundle on target %device

System Log Message Successfully uninstalled PvS bundle on target %device

Description A PvS bundle is uninstalled successfully on the device

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_BUNDLE_UNINSTALL_SUCCESS

Type Event

Severity Info

JUNOSCOPE_PVS_BUNDLE_UNINSTALL_ERROR

Audit Message PvS bundle uninstallation failed on target %device

System Log Message PvS bundle uninstallation failed on target $device

Description The PvS bundle failed to uninstall.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_BUNDLE_UNINSTALL_ERROR

Type Event

Severity Error

JUNOSCOPE_PVS_UPDATE_ARCHIVE_SITE

Audit Message Successfully updated archive sites on target %device

System Log Message Successfully updated archive sites on target %device

Description PvS archive locations are successfully configured on device.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_UPDATE_ARCHIVE_SITES_SUCCESS

Type Event

Severity Info

JUNOSCOPE_PVS_UPDATE_ARCHIVE_SITE_ERROR

Audit Message Update archive sites failed for reason: %reason

System Log Message Update archive sites failed for reason: %reason

Description PvS archive locations failed to configure on devices.

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Operation: PVS_UPDATE_ARCHIVE_SITES_ERROR

Type Event

Severity Error

Configuration Association Messages

JUNOSCOPE_CONFIG_AASOCIATED

System Log Message JUNOSCOPE_CONFIG_ASSOCIATED: Config Associated

Config Name= ’<Config Name>’

Version= ’<Config Version>’

Criteria= ’<Criteria Used>’

Time: ’<time>’

RADIUS Attributes
- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: CONFIG_ASSOCIATED
- Juniper-JUNOScope-Target: ’ < Config name Version > ’

Description A configuration file was associated for a criteria.

Type Event

Severity Info

JUNOSCOPE_CONFIG_ASSOCIATION_DELETED

System Log Message JUNOSCOPE_CONFIG_ASSOCIATION_DELETED: Config Association Deleted

Config Name= '<Config Name>'

Version= '<Config Version>'

Criteria= '<Criteria>'

Time: '<time>'

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: CONFIG_ASSOCIATION_DELETED
- Juniper-JUNOScope-Target: ' < Config name Version > '

Description A configuration file association was deleted

Type Event

Severity Info

JUNOSCOPE_CONFIG_ASSOCIATION_REORDERED

System Log Message JUNOSCOPE_CONFIG_ASSOCIATION_REORDERED: Config Association Reordered

Time: '<time>'

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: CONFIG_ASSOCIATION_REORDERED

Description The order of the configuration file associations in the list was changed

Type Event

Severity Info

JUNOSCOPE_CONFIG_RETURNED

System Log Message JUNOSCOPE_CONFIG_RETURNED: Config Returned

Device Attributes= Hostname: <hostname> Serial Number: <Serial No.> Model: <model> OS Version: <os version>

Configuration= '<name> <version>'

Time: '<time>'

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: CONFIG_RETURNED
- Juniper-JUNOScope-Target: ' < Config name Version > '

Description A configuration file was returned in response to a request from the device

Type Event

Severity Info

JUNOSCOPE_NO_CONFIG_ASSOCIATED

System Log Message JUNOSCOPE_NO_CONFIG_ASSOCIATED: Association not found

Device Attributes= Hostname: <hostname> Serial Number: <Serial No.> Model: <model> OS Version: <os version>

Time: '<time>'

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: NO_CONFIG_ASSOCIATED
- Juniper-JUNOScope-Target: ' < Config name Version > '

Description No configuration file association was found for the device attributes

Type Event

Severity Info

JUOSCOPE_RETURN_LATEST_ARCHIVED_CONFIG

System Log Message JUNOSCOPE_RETURN_LATEST_ARCHIVED_CONFIG: Return latest configuration archived from device option is %set. Username: '%username' Time: '%time'

Time: '<time>'

RADIUS Attributes

- Acct-Status-Type: Interim-Update
- Juniper-JUNOScope-Privileged-Command: RETURN_LATEST_ARCHIVED_CONFIG
- Juniper-JUNOScope-Target: Config Association

Description The return latest configuration archived option was set.

Type Event

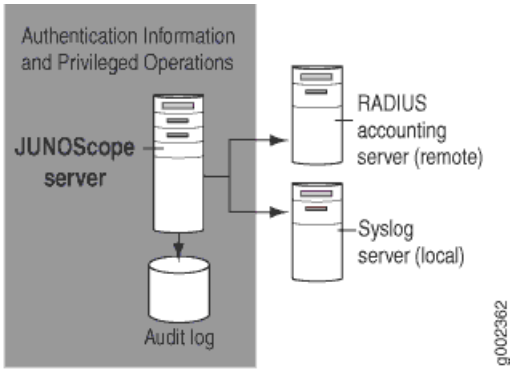
Severity Info

Chapter 41

RADIUS Accounting Attributes

RADIUS attributes corresponding to JUNOScope events are logged to a remote RADIUS accounting server if it is configured in JUNOScope and running. (See Figure 19 on page 727.)

Figure 19: JUNOScope Security-Enahanced Sensitive Data Logging



If the system log daemon is down, event messages sent to the system log server are not logged. If all the RADIUS accounting servers are down, event message attributes sent to the RADIUS accounting servers are not logged.

Interpreting RADIUS Accounting Attributes

All RADIUS accounting messages include the following attributes:

- NAS-Identifier—The server hostname connected with the server HTTP port number.
- Acct-Session-Id—The Tomcat Web container session ID or the global scheduled session ID.
- Acct-Status-Type—Start for login, Stop for session termination, and Interim-Update for all other messages.
- User-Name—The name of the user currently logged in (for interactive commands) or the name of the user who scheduled an operation (for

scheduled commands).

- Juniper-JUNOScope-Schedule—The name of the schedule for any records (including start and stop) associated with the run of a schedule. For all interactive sessions, this attribute is not present.

Additional RADIUS Attributes

Depending on the message, the following additional RADIUS attributes may be present:

- Acct-Terminate-Cause—Indicates whether the session ended because of a deliberate logout or a session timeout.
- Juniper-JUNOScope-Privileged-Operation—The symbolic name for the operation that was performed.
- Juniper-JUNOScope-Target—The name of the object affected by the privileged operation.
- Juniper-JUNOScope-Login-Failure-Reason—The reason for login failure: 'user locked' or 'login failure'.

The RADIUS accounting server expects all accounting records to occur in the context of a session. Since JUNOScope operations can be performed on a schedule after a user's session is no longer valid, a new session is created for each scheduled task. A session start message is sent before the scheduled task executes; a session end message is sent after the task completes.

Part 13
Managing JUNOScope Application Data

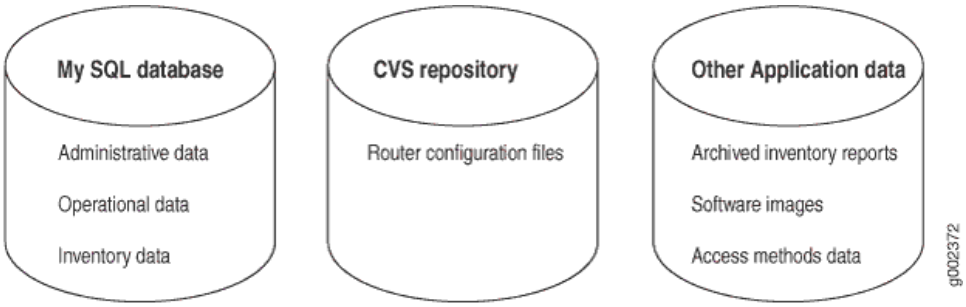
Chapter 42

Backing Up and Restoring the JUNOScope Application Data

This chapter describes how to back up and restore application data stored by JUNOScope to prevent data loss in the event of a disaster.

Figure 20 on page 731 shows the application data that you can back up and restore.

Figure 20: JUNOScope Application Data to Back Up and Restore



You can back up and restore the following JUNOScope application data in the MySQL database:

- Administrative settings—Settings data that can be imported and exported.
- Operational data—Monitor > Operstions, Monitor > Status, and Monitor > Audit Log data.
- Inventory data—Inventory Management > Scan data, including demostration inventory data.

You can also back up and restore archived device configuration files in the Configuration Version System (CVS) repository. Archived device configuration files are generated when you use Configuration > Repository > Archive or import a configuration file by using Configuration > Repository > Import.

You can also back up and restore archived inventory reports and imported JUNOS software images. Archived inventory reports are generated when you schedule an inventory management system report using Inventory Management > Repository > Schedule. These are the reports that you see when you use Inventory Management > Repository > View. JUNOS software images are stored when you import them using Software Management > Images.

The JUNOScope software supports only full MySQL database backups; not incremental ones.

You do not need to shut down the JUNOScope server while you back up the MySQL database and repositories. You do, however, need to temporarily shut down the JUNOScope server when you restore them.

It is recommended that you back up and restore the database and data repositories simultaneously and at a time when the operational activities of the JUNOScope server are at a minimum.

You can automate backup and restore tasks within a UNIX shell script, which could then be run at specified times by the cron utility.

This chapter includes the following sections:

Backing Up JUNOScope Application Data

Periodically, when the operational activities of the JUNOScope server are at a minimum, you should back up the JUNOScope application data. We recommend that you back up the database and data repositories simultaneously to ensure data consistency between the JUNOScope router configuration repository and the MySQL database.

NOTE: The database root username and password is mandatory to backup and restore the database using the msqldump command.

To back up JUNOScope application data, follow these steps:

1. Change to the directory where the JUNOScope software is installed:

   % **cd <JTK_INSTALL>**

2. Using the mysqldump command, back up the contents of the JUNOScope MySQL database:

   % **./mysql/bin/mysqldump –socket=data/db/mysql.sock **
   **–user=root **
   **–password=pw **
   **–opt **
   **–all-databases **
   > /path-to-backup/junoscope-db-backup.sql

   <JTK_INSTALL> is the path of the JUNOScope installation, < *pw* > is the database root user's password (created during JUNOScope installation, and < *path-to-backup/junoscope-db-backup.sql* > is the name and location of the backup file you create.

   For example:

```
% cd <JTK_INSTALL>
% ./mysql/bin/mysqldump –socket=data/db/mysql.sock/
–user=root/
–password=foobar /
–opt –all-databases /
> /opt/backups/jnscp/dbdump.sql
```

This command example backs up the contents of the MySQL database using the password foobar and creates a file called dbdump.sql in the /opt/backups/jnscp/ directory.

3. Navigate to the JUNOScope data directory:

```
%cd <JTK_INSTALL>/data
```

<JTK_INSTALL>/data is the path where the JUNOScope application data is stored,

4. Back up the contents JUNOScope router configuration repository CVS root directory using a UNIX backup utility or the tar command:

```
% tar cf /path-to-backup/junoscope-data-backup.tarcvsroot archivedreports images
  access-methods.xml
```

< *path-to-backup* > is the directory where you want to store the backup, < *junoscope-data-backup.tar* > is the name of the backup tar file to create.

Restoring JUNOScope Application Data

You should restore the JUNOScope application data when the operational activities of the JUNOScope server are at a minimum, We recommend that you restore the database and data repositories simultaneously to ensure data consistency between the JUNOScope router configuration repository and the MySQL database.

To restore the JUNOScope application data, follow these steps:

1. Change directories to where the JUNOScope software is installed:

```
% cd <JTK_INSTALL>
```

<JTK_INSTALL> is the location of the JUNOScope installation.

2. Shut down the JUNOScope server:

```
% ./jtk/rc.d/jtk stop
```

3. Start the JUNOScope MySQL database:

```
% ./jtk/rc.d/mysql start
```

4. Restore the contents of the JUNOScope MySQL database:

```
% ./mysql/bin/mysql –socket=data/db/mysql.sock
–user=root
–password=pw
< /path-to-backup/junoscope-db-backup.sql
```

For example:

```
% ./mysql/bin/mysql –socket=data/db/mysql.sock
–user=root
–password=foobar
< /opt/backups/jnscp/dbdump.sql
```

5. Stop the JUNOScope MySQL database:

```
%./jtk/rc.d/mysql stop
```

6. Change directories to where the JUNOScope application data is stored:

```
%cd <JTK_INSTALL>/data
```

7. Restore the contents of the CVS repository and other data directories:

```
% mv cvsroot cvsroot.old
% mv archivedreports archivedreports.old
% mv images images.old
%mv access-methods.xml access-methods.xml.old
%cd <JTK_INSTALL>/tomcat/work/Standalone/localhost/jtk/cocoon-files
%mv cvs-top cvs-top.old
```

8. Restore the CVS repository from an earlier backup or extracting from an existing tar file:

```
%cd <JTK_INSTALL>/data
% tar xf / path-to-backup / junoscope-data-backup.tar
```

< *path-to-backup* > is the directory where the backup is stored. < *junoscope-data-backup.tar* > is the name of an existing backup tar file.

9. Restart the JUNOScope server:

```
% ./jtk/rc.d/jtk start
```

Part 14

Integrating External Web Applications with JUNOScope

Chapter 43

Launching JUNOScope Operations from External Web Applications

This chapter describes how to launch JUNOScope from an external Web application, and go directly to a specified JUNOScope operation without having to log in using the JUNOScope server login page, via an addressable URL. This chapter also describes how to query for device information using the URL interface, how to view device information without standard tabs or side bars, and how to use the JUNOScope URL Interface Demo application. If you use other management applications and want to perform JUNOScope operations, you can provide URLs in your application to operations in JUNOScope.

This chapter includes the following topics:

Accessing a JUNOScope Operation from an External Web Application

You can access a JUNOScope operation directly from an external Web application using a URL without having to browse to the feature. You can provide the URL to the JUNOScope operation in your application and be directed to the JUNOScope server login page. Once you submit valid credentials, you can go directly to the JUNOScope operation and skip the JUNOScope home page.

To access a JUNOScope operation, for example Looking Glass, using the URL interface, follow these steps:

1. Start your Web browser.
2. Enter the following Looking Glass URL in your Web browser Address text box:

   https://*hostname:port-number*/jtk/ui/index/looking-glass

   Where *hostname* is the name of the server on which the JUNOScope software is installed, and *port-number* is the port on which the JUNOScope Web server listens for HTTPS requests. If you do not specify a port number, the default port 8443 is used. The JUNOScope Login dialog box appears.

3. Log in using your JUNOScope username and password. The Looking Glass window appears.

Table 1 lists URLs to the JUNOScope operations that can be accessed using the URL interface, and the permissions required to access these URLs.

Table 52: JUNOScope Operations accessible using the URL Interface

Menu	Permissions	URL
Looking Glass	Read-only users / Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/index/looking-glass**
Looking Glass	Read-only users / Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/looking_glass/ show-portal**
Looking Glass	Read-only users/ Read-write users / Administrator	**https://hostname:port-number/jtk/ui /looking_glass/3Fdarg%3D% 2dargt% 3D%26device%3D <*devicename*>%26component%3D General% 26command%3D Device +Summary+Information% 26refresh %3D012**
Configuration	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ /jtk/ui/index/config**
Configuration > Current	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/index/current**
Configuration > Current > View	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/browser/view**
Configuration > Current > View	Read-only users/ Read-write users / Administrator	**https://hostname:port-number/ jtk/ui/browser/ view?device=<*devicename*>**
Configuration > Repository	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/index/repository**
Configuration > Repository > Compare	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wizard/ compare?cocoon-action-start=true**
Configuration > Repository > Display	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wizard/ display?cocoon-action-start=true**
Inventory Management	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/index/inventory**
Inventory Management > Reports	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/jtk/xreporter/en-US/ datasources**
Inventory Management > Reports > Inventory	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/xreporter/en-US/ reportcatalog?dataSourceId=ims-ds**

Table 52: JUNOScope Operations accessible using the URL Interface *(continued)*

Menu	Permissions	URL
Inventory Management Reports > Demo	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/xreporter/en-US/ reportcatalog?dataSourceId=demo-ds**
Inventory Management Reports > Custom	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/xreporter/en-US/ savedreports**
Monitor	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/index/monitor**
Monitor > Operations	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wizard/ operation?cocoon-action-start=true**
Monitor > Status	Read-only users/ Read-write users / Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wiz/status/**
Configuration > Current > Edit	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/browser/edit**
Configuration > Current > Edit	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/browser/ edit?device=<*devicename*>**
Configuration >Repository > Archive	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wizard/ archive?cocoon-action-start=true**
Configuration > Repository > Archive Tags	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wiz/archive-tag-list/1**
Configuration > Repository > Audit Configurations	Read-write user/ Administrator	**https://*hostname:port-number* / jtk/ui/cm/wiz/ archive-tags?op=audit-config**
Configuration > Repository > Import	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wizard/ import?cocoon-action-start=true**
Configuration > Repository > Restore	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wizard/ restore?cocoon-action-start=true**
Configuration > Repository > Delete	Read-write user/ Administrator	**https://*hostname:port-number* / jtk/ui/cm/wiz/ config?op=config-delete-select**
Configuration > Repository > Save	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wiz/ config?op=config-download-select**
Configuration > Repository > Edit	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wiz/ config?op=config-edit-select**

Table 52: JUNOScope Operations accessible using the URL Interface *(continued)*

Menu	Permissions	URL
Configuration > Repository > Scripts	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wiz/ script?op=scriptList**
Inventory Management > Scan	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/ims/wizard/ scan?cocoon-action-start=true**
Inventory Management > Repository	Read-write user/ Administrator	**https://*hostname:port-number* / jtk/ui/index/ xreporter-select-repository**
Inventory Management > Repository > Schedule	Read-write user/ Administrator	**https://*hostname:port-number*/jtk/ui/ admin/wiz/ schedule-report/**
Inventory Management > Repository > View	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/admin /wiz/ report-filter/**
Software Management	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/index/swmgr**
Software Management > Images	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/swmgr/ wiz/image-list/1**
Settings	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/index/settings**
Settings > Saved Operations	Read-write user/ Administrator	**https://*hostname:port-number*/ jtk/ui/admin /wiz/operation-list/1**
Monitor > Audit Log	Administrator	**https://*hostname:port-number*/ jtk/ui/cm/wiz/events/**
Monitor > Purge	Administrator	**https://*hostname:port-number* /jtk/ui/index/purge**
Monitor > Purge > Status	Administrator	**https://*hostname:port-number* /jtk/ui/cm/wiz/ purge?op=statusPurge**
Monitor > Purge > Audit Log	Administrator	**https://*hostname:port-number* /jtk/ui/cm/wiz/ purge?op=eventsPurge**
Settings > Authentication Information	Administrator	**https://*hostname:port-number* /jtk/ui/admin/ wizard/access% 3Fcocoon-action-start% 3Dtrue% 26cocoon-xmlform-view% 3DauthenticationList**
Settings > Access Methods	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wizard/ access?cocoon-action-start=true**
Settings > Devices	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wizard/ devices?cocoon-action-start=true**

Table 52: JUNOScope Operations accessible using the URL Interface *(continued)*

Menu	Permissions	URL
Settings > Groups	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wizard/ groups?cocoon-action-start=true**
Settings > Labels	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wiz/ label-list/1**
Settings > Schedules	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wizard/ schedules?cocoon-action-start=true**
Settings > Users	Administrator	**https://*hostname:port-number* /** **jtk/ui/index/usersSettings**
Settings > Users > Local Authentication	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wizard/ users?cocoon-action-start=true**
Settings > Users > User Group Authorization	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wiz/ authorization/1?op=list**
Settings > Users > Authentication Policy	Administrator	**https://*hostname:port-number* /jtk/ui/index/authPolicy**
Settings > Users > Authentication Policy > Global Authentication Policy	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wiz/ globalAuthPolicy?op=edit**
Settings > Users > Authentication Policy > User-Specific Authentication Policy	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wiz/ auth-policy-list/1**
Settings > Radius Configuration	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wizard/ radiusClients?cocoon-action-start=true**
Settings > Import/Export Data	Administrator	**https://*hostname:port-number* /jtk/ui/admin/wizard/ exim-wiz%3Fcocoon-action-start%3Dtrue%26 table_name%3Dall**

You can also access any of the JUNOScope operations listed inTable 52 on page 738 directly from an external Web application using a URL, without logging in using the JUNOScope server login page. You can provide the URL to the JUNOScope operation in your application with the username and password added to the URL. You will be directed to the JUNOSCope operation without having to log in a second time.

To access a JUNOScope operation, for example Looking Glass, without logging in using the JUNOScope sever, follow these steps:

1. Start your Web browser.
2. Enter the following Looking Glass URL, with the username and password added, in your Web browser Address text box:

   https://*hostname:port-number* /jtk/noauth-auth?username=<*username*> &password =<*password*>&redirectLoc=ui/index/looking-glass

   Where *hostname* is the name of the server on which the JUNOScope software is installed, *port-number* is the port on which the JUNOScope Web server listens for HTTPS requests (if you do not specify a port number, the default port 8443 is used), and <*username*> and <*password*> are credentials you use to log in to the server. The Looking Glass window appears.

NOTE: For features that involve multiple screen selection, including wizards, only URLs to the initial screen are supported.

Querying for Information Using the URL Interface

You can directly query for information from JUNOScope, provided the query can be represented in the form of a URL. You can use a URL with request parameters as arguments to fetch real-time statistics.

To query for information, follow these steps:

1. Start your Web browser.
2. Enter the following Looking Glass URL, with request parameters as arguments, in your Web browser Address text box:

   https://*hostname:port-number* /jtk/ui/index/looking-glass/query% 3Fdarg%3D%26dargt%3D %26device%3D<*ValidDeviceName*> %26component%3DGeneral%26command%3D Device+Summary+Information%26refresh%3D012

   Where *hostname* is the name of the server on which the JUNOScope software is installed, *port-number* is the port on which the JUNOScope Web server listens for HTTPS requests, and <*Valid DeviceName*> is the name of the device being queried. The device being queried should have been added to JUNOScope.

   The Looking Glass window appears with the device summary information for the device.

Viewing Device Information without Standard Tabs or Side Bars

To view the Looking Glass window without the standard tabs or side bars, follow these steps:

1. Start your Web browser.
2. Enter the following URL in your Web browser Address text box:

   https://*hostname:port-number*/jtk/portal/looking_glass/show-portal

   Where *hostname* is the name of the server on which the JUNOScope software is installed, and *port-number* is the port on which the JUNOScope Web server listens for HTTPS requests,

   The Looking Glass Enter Query Information window appears without the standard tabs or side bars. You can enter query information and click Submit to get query results.

To query for information and view the query results in the Looking Glass window without the standard tabs or side bars, follow these steps:

1. Start your Web browser.
2. Enter the following URL in your Web browser Address text box:

   **https://*hostname:port-number*
/jtk/portal/looking_glass/query?darg=&dargt=&device= <*ValidDeviceName*>
&component=General&command= Device+Summary+Information&refresh=5**

   Where hostname is the name of the server on which the JUNOScope software is installed, port-number is the port on which the JUNOScope Web server listens for HTTPS requests, and < Valid DeviceName > is the name of the device being queried. The device being queried should have been added to JUNOScope.

   The Looking Glass window appears with the query results but without the standard tabs or side bars.

Using the JUNOScope URL Interface Demo Web Application

The JUNOScope URL Interface demo Web application demonstrates how an external Web application or standalone management application can access JUNOScope directly through a browser without using the JUNOScope login page. You can download the demo Web application from the JUNOScope download site:

http://www.juniper.net/support/csc/swdist-encr/swdist-jtk/

See the *ReadMe for the JUNOSCOPE URL Interface Demo Web application* (available along with the demo Web application) for set up instructions.

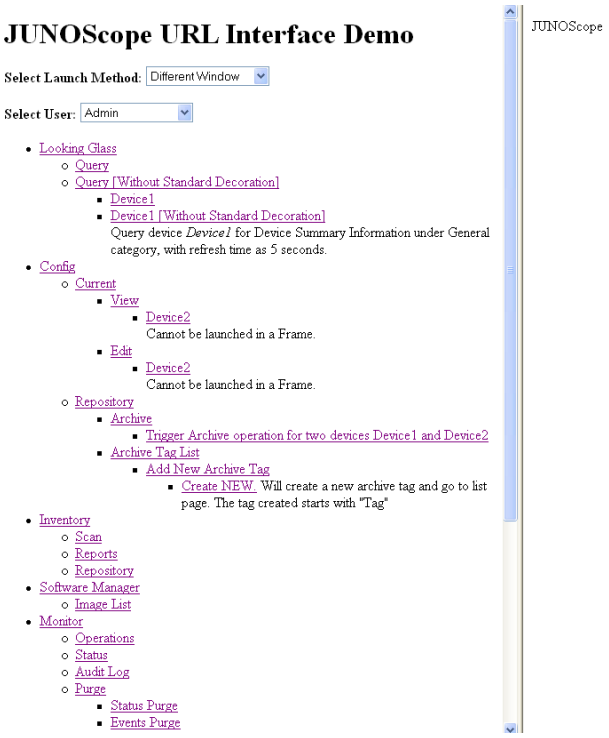
To launch the demo application after setting it up, follow these steps:

1. Enter the following URL in the browser:

   https://*hostname*:*port-number*/jtk-url-interface-demo-1.0/

   Where *hostname* is the name of the server on which the demo instance of JUNOScope software is installed, and *port-number* is the port on which the JUNOScope Web server listens for HTTPS requests. If you do not specify a port number, the default port 8443 is used.

2. Press Enter. The JUNOScope URL Interface Demo window appears.



3. Select a launch method from the Select Launch Method drop-down list box in the JUNOScope URL Interface Demo window:

   The Select Launch Method drop-down list box lists the following options:

   - Select Different Window— Select the option and click on a feature hyperlink to launch that feature in a separate window.
   - In Pop-up—Select the option and click on a feature hyperlink to launch that feature in a pop-up window.
   - Frame on the Right—Select the option and click on a feature hyperlink to launch that feature in the right frame of the JUNOScope URL Interface Demo window.
   - Same Window— Select the option and click on a feature hyperlink to launch that feature in the left frame of the JUNOScope URL Interface Demo window.

4. Select a user role from the Select User drop-down list box to view the privileges associated with the user role.

   The Select User drop-down list box lists the user roles: Admin, Read-Write User, and Read-Only User.

5. Click on a hyperlink in the left frame of the JUNOScope URL Interface Demo window to launch that JUNOScope operation.

   All JUNOScope operations that can be launched using the JUNOScope URL Interface Demo Web application are listed as hyperlinks in the left frame of the JUNOScope URL Interface Demo window. Select a launch method and a user role and click on a hyperlink to launch that operation.

Implementing the URL Interface

You can implement the URL Interface feature by using the sample code in this section:

- Adding Hyperlinks to JUNOScope Operations in External Web Applications on page 745
- Launching JUNOScope Operations in a New Window on page 745
- Launching JUNOScope Operations in a Pop-Up Window on page 746
- Launching JUNOScope Operations in a Frame on page 746
- Concealing the Username and Password in a URL on page 747

Adding Hyperlinks to JUNOScope Operations in External Web Applications

You can add hyperlinks to JUNOScope operations in your application by using the following sample code:

```
<a href='https://hostname:port-number/jtk/
noauth-auth?username=<username>&password=
<password>&redirectLoc=ui/index/looking-glass'> Looking Glass
</a>
```

This sample code adds a hyperlink to Looking Glass in your application, allowing you to access Looking Glass without logging in using the JUNOScope sever.

Launching JUNOScope Operations in a New Window

You can launch JUNOScope operations in a new window by using the following sample code:

```
<a href="#"
onclick="launchInNewWindow('ui/index/looking-glass')">Looking-glass</a>
                                    <script
language="JavaScript"type="text/javascript">
                                     var JUNOScopeLink=
"https://<JUNOScope Server>:<Port>/jtk/
noauth-auth?username=<username>&password=<password>&redirectLoc="
                                      function launchInNewWindow(link ) {
```

```
                    var newWin = open(JUNOScopeLink + link);
                   return false;
                }
 </script>
```

Launching JUNOScope Operations in a Pop-Up Window

You can launch JUNOScope operations in a new pop-up window by using the following sample code:

```
<a href="#"  onclick="openInPopUp('ui/index/looking-glass')">Looking-glass</a>
                <script language="JavaScript" type="text/javascript">
                 var JUNOScopeLink =
"https://<JUNOScope
Server>:<Port>/jtk/noauth-auth?username=<username>&password=<password>&redirectLoc="

             function openInPopUp( link ) {
                    var newWin = open(JUNOScopeLink + link, "JUNOScopeURL",


"location=1,status=1,menubar=1,scrollbars=1,resizable=1,height=600,width=700");
                   return false;
                }
 </script>
```

Launching JUNOScope Operations in a Frame

You can launch JUNOScope operations in a frame in the current window by using the following sample code:

```
<a href="#"  onclick="openInFrame('ui/index/looking-glass')">Looking-glass</a>
               <script language="JavaScript" type="text/javascript">
                   var JUNOScopeLink =
"https://<JUNOScope
Server>:<Port>/jtk/noauth-auth?username=<username>&password=<password>&redirectLoc="

                   function openInFrame( link ) {
                      parent.right.location = JUNOScopeLink + link;

                      // replace "right" with the frame name
                       return false;
                     }
        </script>
```

NOTE: You cannot launch the Configuration > Current > Edit operation in a frame.

NOTE: When JUNOScope is launched for the first time, a session is created. Subsequent launches of JUNOScope operations using the URL interface do not require the username and password in the URL until the session expires. However, if you wish to log in using a different user profile, then you will have to log out first. Otherwise, the current login ID and user session are used. Use the following link to logout: https://*hostname:port-number*/jtk/logout

Concealing the Username and Password in a URL

You can provide URLs to JUNOScope operations in your Web application with the username and password added to the URL. You will be directed to the JUNOSCope operation without having to log in using the JUNOScope server login page. (See Figure 21 on page 747.) However you can choose to conceal the username and password in the URL. (See Figure 22 on page 748.)

Figure 21: Data Flow with JUNOScope Credentials

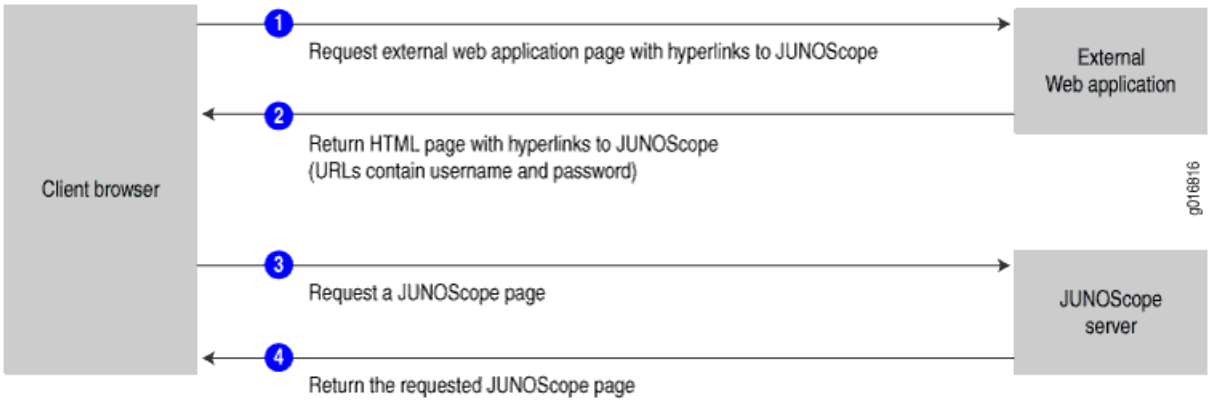
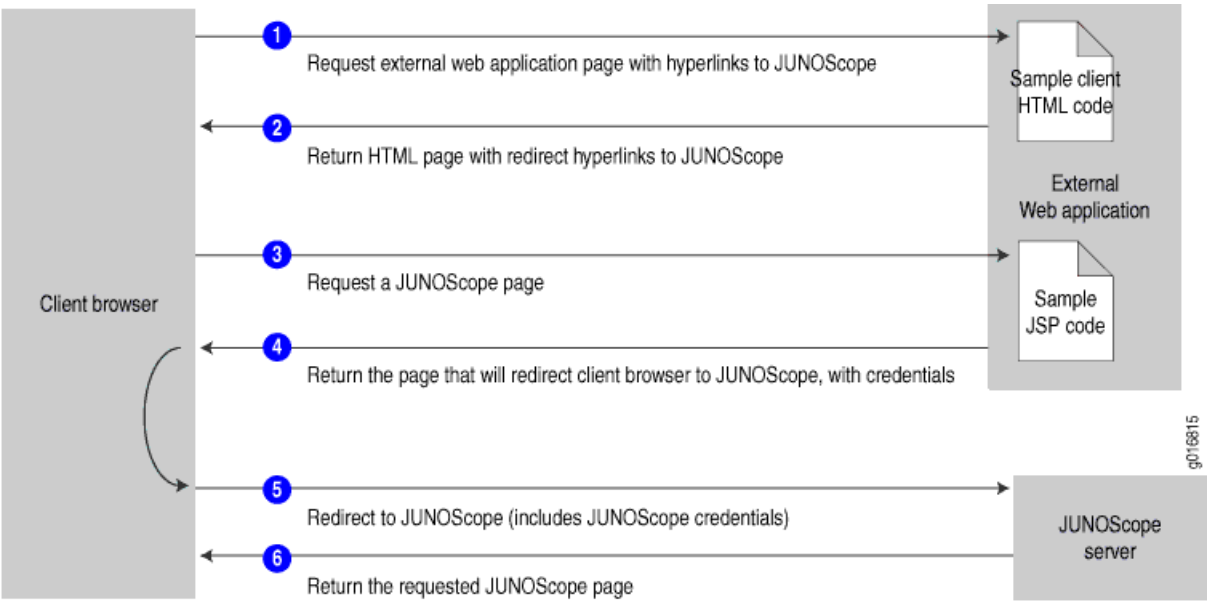


Figure 22: Data Flow with JUNOScope Credentials Concealed via HTTP Redirect



To conceal the username and the password in the URL, the HTTP request by the client browser, for the external Web application page with hyperlinks to JUNOScope opertaions should be returned to the client browser with redirect hyperlinks.

You can use the following sample client HTML code to return the HTTP request to the client browser with redirect hyperlinks:

```
<html>
            <body bgcolor="white">
               <a
href='http://<yourServer>:<Port>/redirect?redirectLoc=ui/index/looking-glass'>
Looking Glass</a>
                 <!--
                     replace above <yourServer> with the server name/IP  and
<port> with
the port where     the redirect jsp is available.
                  -->
             </body>
       </html>
```

You can use the sample JSP code below to return the page that will redirect the client browser to JUNOScope, with credentials:

```
<html>
          <body bgcolor="white" onLoad="goToJUNOScope();">
             Redirecting to Junoscope.             </body>
          <Script language="javascript">
           var logoutRequired= <%=request.getParameter("logoutRequired")%>;
                function goToJUNOScope() {
                  if( logoutRequired ) {

document.all.logoutFrame.src="<%=urlInterface.RedirectHelper.getJUNOScopeServer()%>"+"/jtk/logout";
```

```
                }
                var server = "https://JUNOScopeServer:8443/";
        var userName = 'username';
        var password = 'password';
       var redirectLoc = '<%=request.getParameter("redirectLoc")%>';
       var fullURL =
server+"/jtk/noauth-auth?username="+userName+"&password;="+password+"&redirectLoc;="+redirectLoc;

       window.location = fullURL;
       return false;
      }
           </Script>
       </html>
```

Part 15
Index

Index

Symbols

A

B

C

D

J

L

M

N

O

P

Q

R

S

T

U

V

X