Juniper Networks

Advanced Insight Solutions 1.0 User Guide

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-022698-01, Revision 1

JUNOS™ Advanced Insight Solutions User Guide, Release 1.0

Writer: Donice G. Evans-Mitchell
Editor: Stella Hackell
Cover design: Edmonds Design
Illustrator: Faith Bradford

Revision History
1 February 2008—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 Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and 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, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper 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 the 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 software on multiple computers requires multiple licenses, regardless of whether such computers 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 the Embedded Software on non-Juniper equipment; (j) use the 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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)).

Table of Contents

About This Guide

This preface provides the following guidelines for using the *Advanced Insight Solutions 1.0 User Guide* and related Juniper Networks, Inc., technical documents:

Objectives

This guide provides a reference for you to install, set up, and use the Advanced Insight Solutions (AIS) product. Advanced Insight Solutions (AIS) is a Juniper Networks product that provides reactive and proactive support for Juniper Networks routing platforms (devices) in customer networks that have been configured for and are running Advanced Insight Scripts (AI-Scripts), which are specialized JUNOS event scripts.

AIS consists of three major elements:

- Juniper Networks devices configured to run specialized AI-Scripts. AI-Scripts detect incident and intelligence information and send it to archive locations.
- The Advanced Insight Manager (AIM) application collects incident and intelligence information from archive locations and provides a single control point to manage information flow and to receive incident resolution and intelligence updates.

- Juniper Support Systems (JSS) receives incident case requests from AIM and sends intelligence updates based on intelligence information from devices, specialized tools, and engineering expertise.

NOTE: This guide documents Release 1.0 of the Advanced Insight Solutions product. For additional information about the JUNOS software—either corrections to or information that might have been omitted from this guide—see the AIS software release notes at http://www.juniper.net/.

Audience

This guide is designed for the AIS administrator and those who have access to manage Juniper Networks routing platforms.

To use this guide, you should have good UNIX or LINUX system administration skills and an understanding of the JUNOS configuration and command-line interface (CLI).

In addition, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration.

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, AIS currently supports the following routing platforms:

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

Documentation Conventions

Table 4 defines notice icons used in this guide.

Table 4: 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.

Table 5 defines the text and syntax conventions used in this guide.

Table 5: Text and Syntax Conventions (1 of 2)

Convention	Element	Example
Bold sans serif typeface	Represents text that you type.	To enter configuration mode, type the configure command: user@host> **configure**
`Fixed-width typeface`	Represents output on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic typeface	■ 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 sans serif typeface	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*
Sans serif typeface	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*>;
| (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*]

Table 5: Text and Syntax Conventions (2 of 2)

Convention	Element	Example

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 typeface	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**.

Advanced Insight Manager User Interface Elements

When describing AIM user interface elements, this manual uses the following terminology:

- Check box—A square box within a dialog box that you can select or clear to turn an option on or off.
- Command button—A rectangular button that starts an operation. A command button with ellipsis (. . .) means that another dialog box will appear with additional information that you must select before the operation can be completed.
- Page—A software user interface element that contains buttons, fields, tables, and other elements to let you view or provide the information required to perform an operation.
- Display box—A type of dialog box that displays the contents of a file or the differences between the contents of two files.
- Display field—An area in a dialog box that displays information necessary to perform an operation or a command.
- Drop-down list box—A closed version of a list box with a down arrow. Click the down arrow to display the list items.
- Text box—An area within a dialog box where you can type text or numbers required to perform an operation or a command.
- Option button—A round button that lets you select one item from a group of items. You can select only one button from a group of option buttons.
- Table—Items of information that are arranged by rows and columns.

- Window—The software user interface display area or page layout. A window can be divided into panes or boxes to display different information.

- Wizard—A series of dialog boxes that enable you to complete a process. For instance, the agenda wizard in Microsoft Word will prompt you to fill in the blanks until your task is complete.

Related Juniper Networks Documentation

Table 6 lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 7 lists the books included in the Network Operations Guide series.

Table 8 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 6: Technical Documentation for Supported Routing Platforms (1 of 4)

Document	Description
JUNOS Internet Software Configuration Guides	
Access Privilege	Explains how to configure access privileges in user classes by using permission flags and regular expression. Lists the permission flags along with their associated command-line interface (CLI operational mode commands and configuration statements.
Class of Service	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
CLI User Guide	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the *JUNOS System Basics Configuration Guide.*
Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
High Availability	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop routing (NSR) and graceful Routing Engine switchover (GRES).
MPLS Applications	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
Multicast Protocols	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
Multiplay Solutions	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.
Network Interfaces	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
Network Management	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.

Table 6: Technical Documentation for Supported Routing Platforms (2 of 4)

Document	Description
Policy Framework	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, forwarding options, and cflowd.
Routing Protocols	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
Secure Configuration Guide for Common Criteria and JUNOS-FIPS	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS Internet software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
Services Interfaces	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the routing platform.
Software Installation and Upgrade Guide	Describes the JUNOS software components and packaging, and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the *JUNOS System Basics Configuration Guide.*
System Basics	Describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
VPNs	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
Hierarchy and RFC Reference	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the *JUNOS System Basics Configuration Guide.*
Interfaces Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
Routing Protocols and Policies Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing protocols and policies, including firewall filters.
System Basics and Services Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as CoS, IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
System Log Messages Reference	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
J-Web Interface User Guide	Describes how to use the J-Web GUI to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
JUNOScript API Guide	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
JUNOS XML API Configuration Reference	Provides reference pages for the configuration tag elements in the JUNOS XML API.
JUNOS XML API Operational Reference	Provides reference pages for the operational tag elements in the JUNOS XML API.
JUNOS Configuration and Diagnostic Automation Guide	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.

Table 6: Technical Documentation for Supported Routing Platforms (3 of 4)

Document	Description
NETCONF API Guide	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
JUNOS Configuration and Diagnostic Automation Guide	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
JUNOScope Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software GUI, how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
J-series Services Router Documentation	
Getting Started Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the *Getting Started Guide* for your router model.
Migration Guide	Provides instruction for migrating an SSG 300M-series or SSG 500M-series security device running Screen OS software or a J-series router running JUNOS software to JUNOS software with Enhanced Services.
Interfaces and Routing Guide	Explains how to configure the interfaces on J-series Services Routers running MJUNOS Enhanced Services for basic IP routing with standard routing protocols. ISDN backup, digital subscriber line (DSL) connections and class-of-service (CoS) classification for safer, more efficient routing.
Security Configuration Guide	Explains how to configure J-series Services Routers running JUNOS software with Enhanced Services in virtual private networks (VPNs) and multicast networks; configure firewall NAT and ALGs; apply routing techniques such as zones, polices, stateful firewall filters, and IP Security (IPSec) tunnels; and configure screens and firewall authentication.
Administration Guide	Shows how to manage users and operations, monitor network performance, upgrade software, change routing and secure contexts, and diagnose common problems on J-series routers running JUNOS software and Enhanced Services.
Design and Implementation Guide	Provides guidelines and examples for designing and implementing IP Security (IPSec) VPNs, firewalls, and routing on J-series routers running JUNOS software and Enhanced Services.
Hardware Documentation	
Hardware Guide	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
PIC Guide	Describes the routing platform PICs. Each platform has its own PIC guide.
DPC Guide	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Advanced Insight Solutions (AIS) Documentation	
Advanced Insight Solutions Guide	Describes the Advanced Insight Solutions (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for incident case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.

Table 6: Technical Documentation for Supported Routing Platforms (4 of 4)

Document	Description
J-series Routing Platform Documentation	
Getting Started Guide	Provides an overview, basic instructions, and specifications for J-series routing platforms. The guide explains how to prepare our site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the Getting Started Guide for your router model.
Basic LAN and WAN Access Configuration Guide	Explains how to configure interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
Advanced WAN Access Configuration Guide	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPSec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
Administration Guide	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Release Notes	
JUNOS Release Notes	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
Hardware Release Notes	Describe the available documentation for the routing platform and the supported PICs, and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
JUNOScope Release Notes	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
AIS Release Notes	Summarizes AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
AIS AI-Script Release Notes	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
J-series Services Router Release Notes	Briefly describe the J-series Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.
JUNOS Enhanced Services Release Notes	Summarizes new features for a particular release, identify known hardware and software problems, provide information that might have been omitted from the manuals, and provide upgrade and downgrade instructions.

Table 7: JUNOS Internet Software Network Operations Guides (1 of 2)

Book	Description
Baseline	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
Interfaces	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.

Table 7: JUNOS Internet Software Network Operations Guides (2 of 2)

Book	Description
MPLS	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routers in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
MPLS Log Reference	Describes MPLS status and error messages that appear in the output of the show mpls lsp extensive command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
MPLS Fast Reroute	Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing.
Hardware	Describes tasks for monitoring M-series and T-series routing platforms.

Table 8: 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.
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.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at http://www.juniper.net/techpubs/docbug/docbugreport.html. 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

Requesting Support

For technical support, open a support case using the Case Manager link at http://www.juniper.net/customers/support or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Part 1

Advanced Insight Solutions Overview

Chapter 1

Advanced Insight Solutions Overview

Advanced Insight Solutions (AIS) is a Juniper Networks product that provides reactive and proactive support for Juniper Networks device operation by:

- Automatically detecting problem incidents and intelligence information
- Managing incidents to quick resolution by Juniper Support Systems (JSS) engineers and specialized tools
- Providing intelligence information updates to prevent problem incidents from occurring.

This chapter describes the Advanced Insight Solutions (AIS) major features and how it works.

This chapter includes the following topics:

AIS Key Benefits

AIS provides a comprehensive set of tools and processes designed to automate the delivery of reactive and proactive support services for Juniper Networks devices running on the networks. AIS, for full intended functionality, requires an annual subscription to Juniper Support Systems (JSS) support services and Advanced Insight Manager application licensing, and capacity licenses for the number of devices you want AIS to manage and support (see.

AIM provides the following key benefits:

- Advanced Insight Scripts (AI-Scripts)—These JUNOS operations (Op) scripts, that need to be installed and activated on Juniper Networks devices, reduce network downtime significantly by automatically detecting, collecting, and depositing incidents and intelligence information necessary for Juniper Support Systems (JSS) to quickly and efficient resolve cases and proactively identify customer-specific issues before they become problems.

- Advanced Insight Manager (AIM)—This application reduces the cost of service license agreements (SLAs) violations by providing a faster, more efficient reaction to incidents and intelligence information. Incidents and intelligence information is easily flagged to the right users so that they can quickly request case resolution from JSS and intelligence updates. AIM connects to where devices deposit incident and intelligence information and provides a central point of control for case resolution status and intelligence updates. Reaction policies can be designed to alert the network administrator or third-party network management system (NSM) of key incidents, alerts, and intelligence information. All communication between AIM and JSS occurs over a secure channel, and each transaction is authenticated and verified by JSS.

- JSS—Reduces the amount, severity, and duration of network outages by using the Juniper Networks engineering expertise and customized tools to quickly resolving cases and communicating case status with AIM. JSS quickly opens and resolves incident cases if the customer subscribes to the AIS Base Service (Incident-Driven Online Service). JSS sends alerts or intelligence updates or proactive recommendations if the customer subscribes to AIS Proactive Service Intelligence-Driven Online Service.

AIS Key Features

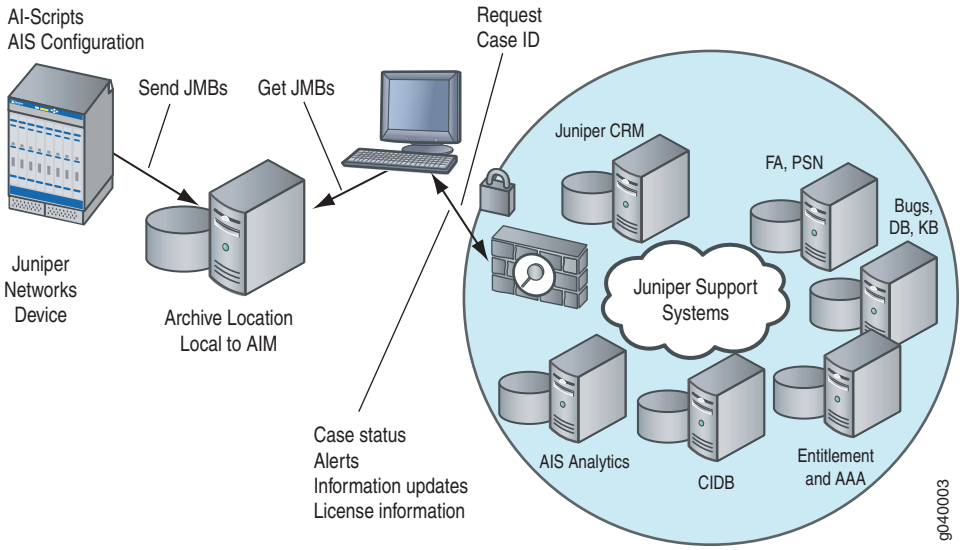
Advanced Insight Solutions (AIS) is a Juniper Networks product that provides reactive and proactive support for EX-series, J-series, M-series, MX-series, and T-series routing platforms (devices) in customer networks that have been configured for and are running Advanced Insight Scripts (AI-Scripts); specialized JUNOS event scripts.

This section contains the following information:

AIS Major Elements

AIS consists of three major elements (see Figure 1):

Figure 1: AIS Major Elements



AI-Scripts

Specialized AI-Script install packages must be installed on AIS-configured JUNOS devices. AI-Scripts, running on devices, automatically do the following:

- React to specific problem events that occur on devices and provide relevant information about the problems for analysis
- Periodically collect intelligence data useful in preventing future problems.
- Package all problem incident and intelligence data into a JMB and send it to a remote archive location so that it can be collected and displayed by AIM.

For more information about AI-Scripts, see “Installing and Understanding AI-Scripts” on page 35.

The Advanced Insight Manager (AIM) Application

The Advanced Insight Manager (AIM) application provides a gateway between JUNOS device archive locations and JSS. AIM provides the following features:

- Installs on a Sun Solaris or Red Hat Enterprise Linux server. Connect to it from a Web browser, such as Microsoft Internet Explorer 6, Netscape Navigator 6 or later with JavaScript enabled, or Mozilla Firefox.
- Processes incident JMBs through case ownership and case creation to quick resolution. You need an AIS Base Service (Incident-Driven Online Service) subscription.
- Processes intelligence JMBs to JSS for use to provide intelligence and alert updates. You need an AIS Proactive Service (Intelligence-Driven Online Service) subscription.

- Operates in fully functional, demo mode for 60 days with support for one organization and five devices.
- A license file is electronically sent to you. Loads the license file into AIM for activation of the licensed features purchased, such as:
  - Base Product—Required to use AIM beyond a 60-day demo period. Allows the operation of Incident Manager and Intelligence Manager and the creation of one organization.
  - Capacity—Required to control the number of devices that can send incident and intelligence JMBs.
  - Feature Licenses—Allow you to activate certain key AIM features

NOTE: Having a license in AIM does not automatically mean that you have a license to subscribe to the AIS Base or AIS Proactive services needed for full functionality of the Advanced Insight Manager (AIS) product.

- Multi-Site organizations provide a way to manage multiple sites with one AIM installation by dividing the network into multiple logical customer sites to participate in Advanced Insight Solutions (AIS) services.
- Using organization device group and archive location settings, you can optionally have JUNOScope Script System automatically install AI-Scripts on multiple devices.
- User privileges control access to AIM features. Access depends on which user group the user belongs to and which device groups the user group is associated with. AIM displays only the devices that the user has access to and incidents and intelligence messages for those devices.
- Sends AIM incident SNMP traps to specific network management systems based on configured trap destinations.
- Includes three main user interfaces to manage incidents, intelligence information, and reaction policies:
  - My AIM Home displays incidents, intelligence messages, and reaction policies owned by or flagged to a user.
  - Incident Manager displays incidents collected from JUNOS device remote archives. You create reaction policies to alert you when incidents occur, incidents are reported to JSS, a Case Management ID is assigned, or a case is updated by JSS. You can view incidents by organizations.
  - Intelligence Manager displays intelligence updates from JSS and Information JMBs collected from JUNOS device remote archives. You can view intelligence information by organizations.

For more information about using AIM, see “Setting Up Advanced Insight Manager” on page 47 and “Using Advanced Insight Manager” on page 105.

JSS

JSS, using Juniper Networks knowledge base, engineering expertise, and specialized tools, resolves incident cases that you open using AIM. JSS sends case resolution status to AIM. JSS receives intelligence information from devices on the network using AIM and sends intelligence updates and alerts to AIM so you can prevent incidents from occurring in the future.

All communication between AIM and JSS occurs over a secure channel, and each transaction is authenticated and verified by JSS.

To receive JSS functionality with AIM, you must subscribe to one or both of the JSS services:

- AIS Base Service (Incident-Driven Online Service)
- AIS Proactive Service (Intelligence-Driven Online Service)

For a description of these services, see "AIS Licensing and Service Subscriptions" on page 7.

AIS Licensing and Service Subscriptions

The AI-Scripts require no fees or licensing.

The AIM application requires the base, feature (optional), or capacity licenses based on the number of devices that need AIS support. AIM License Management displays the current license and services you have purchased once the license file is imported. For more information about AIM licensing, see "AIS License Management" on page 57.

To receive incident resolution and intelligence updates services from JSS, you must purchase the following annual subscriptions:

- AIS Base Service (Incident-Driven Online Service)—This service allows you to directly open incident cases. JSS sends you a case ID and case resolution status.
- AIS Proactive Service (Intelligence-Driven Online Service)—This service allows the customer to send a specified amount of intelligence information to JSS from information JMBs collected by AIM from device arch.ive locations. JSS sends the customer proactive information updates and alerts.

JSS services are provided for the following device classes. Capacity licenses are required for the number of devices the customer needs AIS support.

- Class 1—CPE and branch devices, e.g. J-series, M7i, M10i, M20, M120, EX-3200, EX4200
- Class 2—Edge and Aggregation devices, e.g. M40e, M320, MX-series
- Class 3—Core devices, e.g. T-series and TX

AIM Customer/Partner Engagement Models:

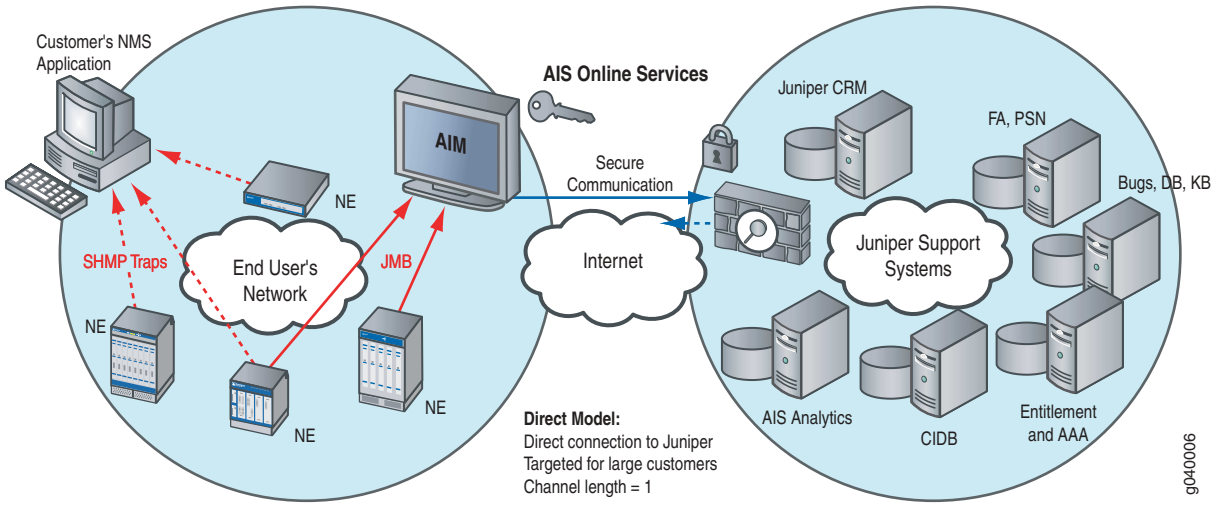
You can deploy AIS several ways depending on your customer support models:

- Direct Customer AIS Engagement Model on page 8
- Partner Deployed AIS Engagement Model on page 9
- Partner end-user-deployed

Direct Customer AIS Engagement Model

The AIS customer installs AIS software elements (AI-Scripts and AIM), and subscribes to AIS services. See “Installing Advanced Insight Manager” on page 23. See “Installing and Understanding AI-Scripts” on page 35. See “AIS Licensing and Service Subscriptions” on page 7. See Figure 2.

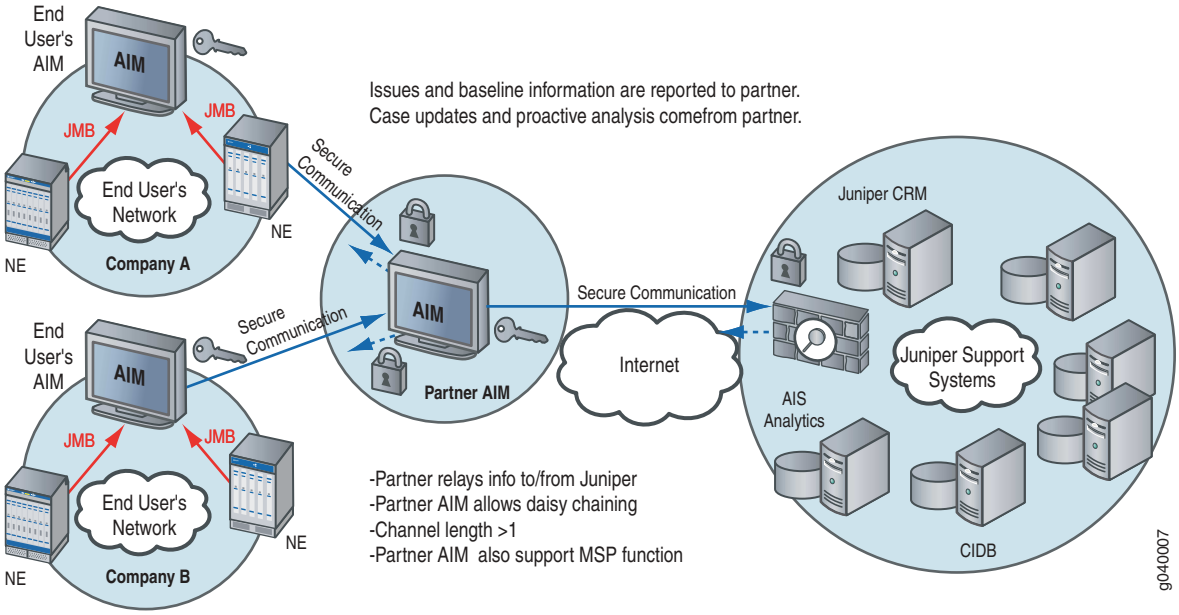
Figure 2: AIS Direct Customer Engagement Model



Partner Deployed AIS Engagement Model

The AIS Partner installs AIM software elements (AI-Scripts and AIM) to manage multiple end-users. All connections are through authenticated and encrypted protocols. Secure file transfers occur from multiple device archive locations to partner's AIM. HTTPS connection is made from AIM to JSS. See "Installing Advanced Insight Manager" on page 23. See "Installing and Understanding AI-Scripts" on page 35. See "AIS Licensing and Service Subscriptions" on page 7. See Figure 3.

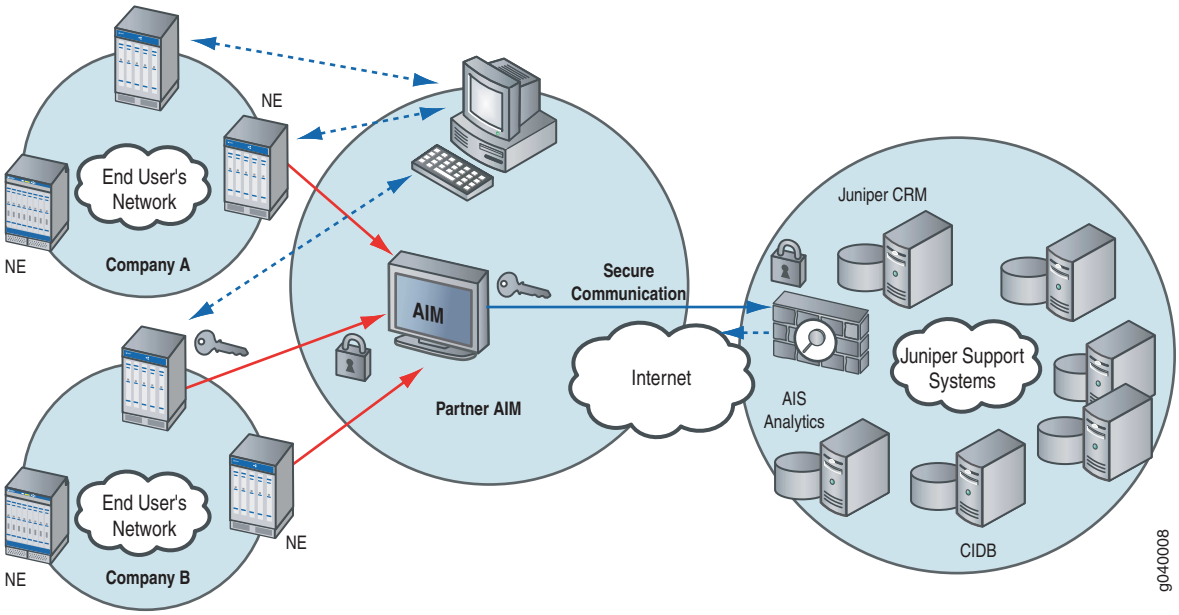
Figure 3: AIS Partner Deployed Engagement Model



Partner End-User Deployed AIS Engagement Model

- Partner End-User-Deployed—End-users deploy AIS software elements. AIM is managed by the partner. The partner connects to AIM installed in end-user site through Web client. A firewall hole or tunnel between end-user and AIM is necessary. The decision to contact Juniper to open a case, request a proactive analysis, etc. are managed by the partner. All connections are through authenticated and encrypted protocols. See Figure 4.

Figure 4: Partner End-User-Deployed Customer/Partner Engagement Model



JUNOScope 9.0 Software Script Management

(Optional) AIM integrates with the JUNOScope 9.0 Software through an API to automatically install an AI-Script install package to multiple devices. JUNOScope is an element management tool, used to support devices on the network. The customer can import devices managed by JUNOScope using AIM JUNOScope settings, then specify which devices on which to install AI-Script install packages using AIM Organizations settings. Install JUNOScope must be installed first on the same server that you install AIM.

How AIS Works

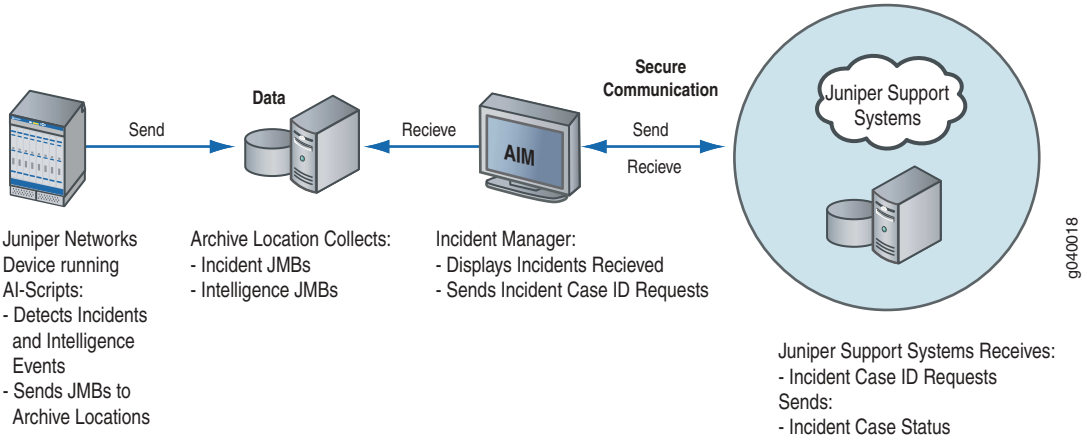
There are two distinct workflows within AIS: one for incident information; the other for intelligence information.

Incidence-Driven Analysis Workflow

AIM periodically polls the archive location for incident and intelligence information and displays the information for a single point of management in Incident and Intelligence Manager. The AIS incident-driven workflow occurs as follows (see Figure 5):

Figure 5: AIS Incident-Driven Workflow

:



1. A trigger event occurs and is detected on a device configured for and running AI-Scripts. An AI-Script is executed.

2. A tailored AI-Script builds a incident Juniper Message Bundle (JMB) with event and router data, and sends it to a designated AIM archive location.

3. AIM receives the incident JMB and displays it in Incident Manager. The incidents owned or flagged to a user displays in My AIM Home.

4. If the customer is enrolled in the AIS Base Service (Incident-Driven Online Service), incidents case IDs can be requested from JSS from Incident Manager to open a case with all relevant information for resolution.

5. JSS creates a case. Any attachments are uploaded from AIM to JSS.

6. JSS returns a case ID to AIM.

7. JSS engineers work on the case and reports case status to AIM.

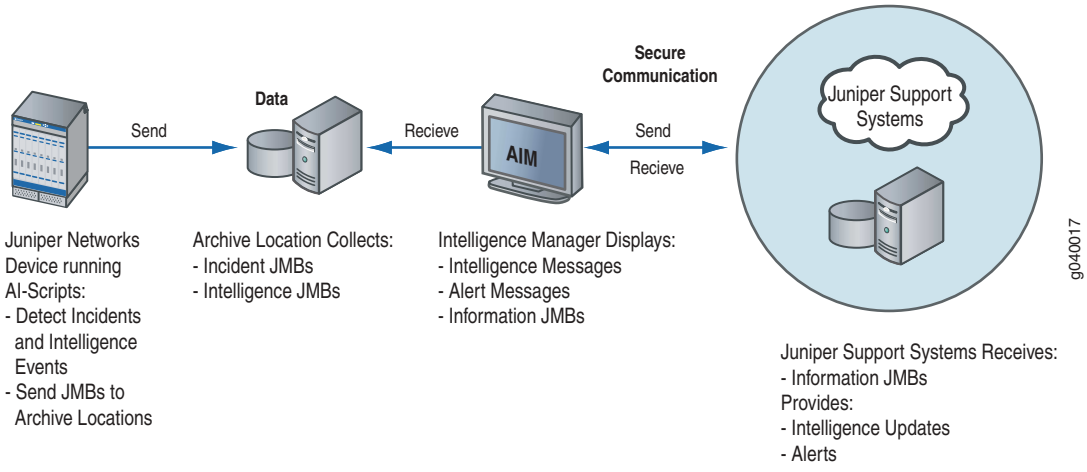
For more information about using Incident Manager, see “Using AIM Incident Manager” on page 131.

Intelligence-Driven Analysis Workflow

JSS receives intelligence JMBs from AIM and collects in the knowledge base. AIM periodically polls JSS for the availability of intelligence messages and created by Juniper personnel specifically for the customer. The intelligence-driven workflow occurs as follows (seeFigure 6):

Figure 6: AIS Intelligence-Driven Workflow

:



1. An intelligence trigger event is detected on a device running AI-Scripts
2. A tailored AI-Script builds and intelligence JMB and sends it to a designated archive location.
3. AIM periodically polls the archive location and receives the intelligence JMB.
4. The customer can specify how much information is shared with JSS using AIM settings.
5. AIM displays the intelligence JMB in Intelligence Manager Information JMBs.
6. If the customer is enrolled in AIS Proactive Service (Intelligence-Driven Online Service), the intelligence JMB is sent to JSS through a secure communication.
7. AIM periodically queries JSS for intelligence updates. Intelligence Updates are comprise of alerts (based on the AIM alert subscriptions) or intelligence updates created by Juniper personnel specifically for the customer.
8. JSS checks to see if there are any alerts or intelligence update messages destined for the customer's AIM.
9. JSS forwards any alerts or intelligence updates to AIM.
10. AIM receives the alerts or intelligence updates and displays them in Intelligence Manager Information Updates

For more information about using AIM Intelligence Manager, see "Using AIM Intelligence Manager" on page 139.

Part 2

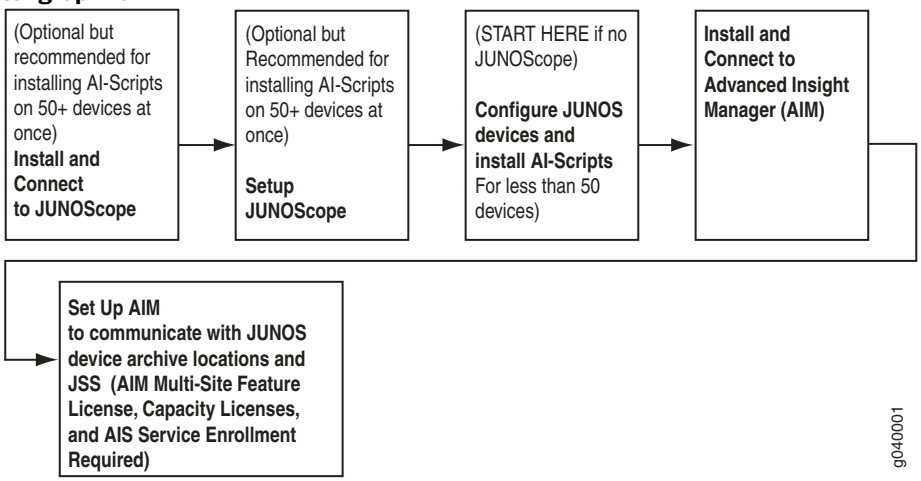
Setting Up Advanced Insight Solutions

Chapter 2

AIS Setup Sequence

This chapter describes the sequence required to set up Advanced Insight Solutions (AIS) successfully. (See Figure 7.)

Figure 7: Sequence for Setting Up AIS



This chapter includes the following sections:

NOTE: It does not matter whether AI-Scripts or AIM is installed first. However, for both, it is necessary, to know the archive location (archive-site destination) used for devices to send incident and intelligence JMBs and for AIM to retrieve this data. You can add the archive location to the device JUNOS configuration for both AI-Scripts and AIM after the initial installation, but the components are not really usable until the archive location is configured.

Installing the JUNOScope Software (Optional)

The JUNOScope Software is an element management application that provides tools for managing IP services for JUNOS devices on the network. If you want AIM to integrate with the JUNOScope 9.0 Software to automatically install AI-Script bundles on multiple devices at once, install the JUNOScope 9.0 or later software. You can install JUNOScope on a UNIX Sun Solaris or Red Hat Enterprise Linux server. The server should be the one that you will install the AIM application. Install JUNOScope first. For more information about installing the JUNOScope Software, see *"Installing and Setting Up JUNOScope Software for AIS" on page 19* and the *JUNOScope Software User Guide.*

Setting Up the JUNOScope Software (Optional)

Once you install the JUNOScope software, connect to it using a Web browser, then log in using the default administrator account. Change the user account, then add a aimuser user with read-write privileges. To set up the JUNOScope software, follow the steps in *"Installing and Setting Up JUNOScope Software for AIS" on page 19* and the *JUNOScope Software User Guide.* You can access the *JUNOScope Software User Guide* at http://www.juniper.net/

Installing AIM

Install the Advanced Insight Manager on a UNIX Sun Solaris or Red Hat Enterprise Linux server. If you are using the JUNOScope software to automatically install AI-Script install packages to multiple devices, install AIM on the same server as JUNOScope. Install JUNOScope first.

NOTE: It does not matter whether AI-Scripts or AIM is installed first. However, for both, it is necessary, to know the archive location (archive-site destination) used for devices to send incident and intelligence JMBs and for AIM to retrieve this data. You can add the archive location to the device JUNOS configuration for both AI-Scripts and AIM after the initial installation, but the components are not really usable until the archive location is configured.

Download the AIM software. Run the graphical or console AIM installer.

You must start the AIM application services before you can connect to AIM using a Web browser, see "AIM System Requirements" on page 24. Once connected, log in to the AIM application using the default AIM admin account.

The AIM installation generates a UUID (or Install ID). The Install ID is displayed at the end of AIM installation process on the Installation Complete screen.

For more information, see "Installing Advanced Insight Manager" on page 23.

Setting Up AIM

Configure AIM so that it communicates with device archive locations, JUNOScope Software (optional), and JSS. The Settings tab is where all AIM settings are configured. For more information about setting up AIM, see the following:

- Configuring AIM General Settings on page 49
- AIS License Management on page 57
- Configuring AIM Organizations and Device Groups on page 67
- Configuring Trap Destinations on page 85
- Setting Up AIM User Groups on page 99
- Setting Up AIM Users on page 89

Install AI-Scripts

AI-Scripts JUNOS configuration, installation, and activation must be performed on JUNOS devices to automatically detect incident and intelligence events occurring during operation. Download AI-Script install packages from the Juniper software download site to the local host running AIM.

NOTE: It does not matter whether AI-Scripts or AIM is installed first. However, for both, it is necessary, to know the archive location (archive-site destination) used for devices to send incident and intelligence JMBs and for AIM to retrieve this data. You can add the archive location to the device JUNOS configuration for both AI-Scripts and AIM after the initial installation, but the components are not really usable until the archive location is configured.

There are two ways to install AI-Scripts: automatically or manually.

- Automatic AI-Script installation is recommended for installing to many devices at once using the JUNOScope. You install AI-Scripts using AIM Organization settings (see “Automatically Installing AI-Script Bundles” on page 83. When installing AI-Scripts automatically, there is no manual intervention required.
- Manual AI-Script installation requires that you configure the device configuration before installing an install packages. You must perform manual AI-Script installation on each device separately. Therefore, manual AI-Script installation is not recommended for many network devices. For more information, see “Manually Configuring and Installing AI-Scripts on Devices” on page 41

Chapter 3

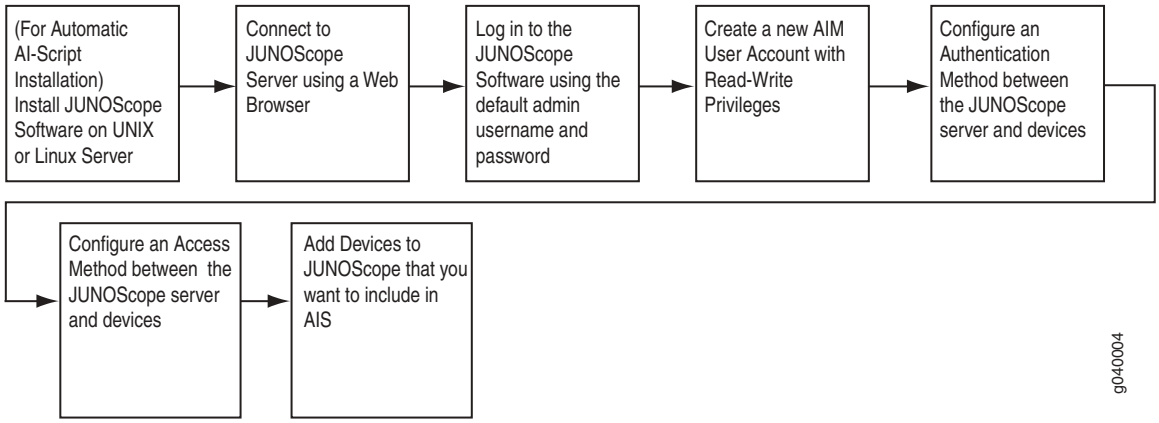
Installing and Setting Up JUNOScope Software for AIS

This chapter provides references on how to install and set up the JUNOScope 9.0 or later software to integrate with Advanced Insight Manager (AIM) to:

- Import devices managed by JUNOScope
- Automatically install AI-Script to multiple devices at once

Figure 8 shows the sequence to install and set up the JUNOScope software.

Figure 8: Automatic AI-Script Install Package Installation Using JUNOScope Script Management



Install the JUNOScope software on the same server as the Advanced Insight Manager (AIM) application. However, install JUNOScope software first.

This chapter includes the following sections

- Set Up an Authorization Method on page 20)
- Set Up an Access Method on page 21)
- Adding Devices on page 21)

Installing the JUNOScope Software

To install JUNOScope 9.0 Software or later, see the *JUNOScope Software User Guide,* Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software chapter. You can view the *JUNOScope Software User Guide* at www.juniper.net/techpubs/.

Connecting to the JUNOScope Software

After you have installed the JUNOScope software, connect to it using a supported Web browser, including Microsoft Internet Explorer 6 or Netscape Navigator 6 or later with JavaScript enabled. See the *JUNOScope Software User Guide,* Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software chapter, "Connecting to the JUNOScope Software from a Client Workstation and Logging In" section.

Logging In to the JUNOScope Software

Log into the JUNOScope software using the valid JUNOScope user name and login password. The username and password are the ones specified during installation. See the *JUNOScope Software User Guide,* Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software chapter, "Connecting to the JUNOScope Software from a Client Workstation and Logging In" section.

Adding an AIM User with Read-Write Privileges

Create an AIM user in JUNOScope with read-write privileges. You need to remember the AIM user name and password for AIM setup. (See *JUNOScope Software User Guide*, Setting Up User Local Authentication chapter.)

Set Up an Authorization Method

Setup an Authorization Method in the JUNOScope software for the devices you want to add.

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. (See *JUNOScope 9.0 Software User Guide*, Setting Up Authentication Information chapter.)

Set Up an Access Method

Setup an Access Method in the JUNOScope software for the devices you want to add.

You can 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. The JUNOScope software supports secure sockets layer (SSL) and clear-text access protocols. We recommend that you set up access methods before you set up devices. See *JUNOScope Software User Guide*, Setting Up Access Methods chapter.

Adding Devices

Add devices in the JUNOScope software that you want to participate in AIS. The JUNOScope software currently supports J-series, M-series, MX-series, and T-series devices.

See *JUNOScope Software User Guide*, Setting Up Devices chapter.

You can import devices managed by the JUNOScope software into the AIM software for automatic AI-Script install package installation.

Where To Go From Here?

- Install the AIM application. See “Installing Advanced Insight Manager” on page 23

Chapter 4

Installing Advanced Insight Manager

This chapter describes how to install the Advanced Insight Manager (AIM) application on a UNIX or LINUX host in your network, connect to AIM Web browser and log in, uninstall AIM.

This chapter also provides a reference for command options used to use the AIM services, including mysql, aimService, jboss, and allservices.

The AIS administrator can install AIM and the JUNOScope software on the same server. JUNOScope is not required, but is recommended to automatically configure JUNOS and install AI-scripts onto multiple devices at once. It is recommended that you install and set up the JUNOScope software before you install AIM. (See *"Installing and Setting Up JUNOScope Software for AIS" on page 19*.)

NOTE: It does not matter whether AI-Scripts or AIM is installed first. However, for both, it is necessary, to know the archive location (archive-site destination) used for devices to send incident and intelligence JMBs and for AIM to retrieve this data. You can add the archive location to the device JUNOS configuration for both AI-Scripts and AIM after the initial installation, but the components are not really usable until the archive location is configured.

This chapter includes the following sections:

AIM System Requirements

You can install the AIM application on a Sun Solaris or Red Hat Enterprise Edition Linux server. Ensure that the server on which you install the AIM application meets the minimum system requirements. For a Sun Solaris server, see Table 9. For a Linux server, see Table 10.

Sun Solaris Server System Minimum Requirements

Before you install the AIM application on a Sun Solaris server, ensure that the server meets the minimum system requirements shown in Table 9.

Table 9: AIM Minimum Sun Solaris Server System Requirements

System	Minimum Requirement
Operating system	Solaris 9.0 and above **NOTE: GNU Privacy Guard (GPG) is required to be installed on Solaris.**
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 AIM application software on a Linux server, ensure that the server meets the minimum system requirements shown in Table 10.)

Table 10: AIM 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

AIM application Client Workstation Requirements

Ensure that the client workstation from which you connect to the AIM application is running either Microsoft Internet Explorer 6 or Mozilla Firefox.

Information Requested During Installation

The AIM application installer prompts you for the following information:

- AIM Software License Agreement—You must accept the agreement.
- Install directory—The directory in which to install the AIM application.
- JBoss server port numbers—The ports (http and https) on which the JBoss server listens for requests to the AIM application. You can enter a port number from 1 to 65535. Port number 8080 is the default http port, and port 8443 is the default https port. This is the port number that you must provide when connecting to the AIM application from a Web browser, see "Connecting to the AIM Application and Logging In" on page 32.
- Database JNDI port number—The Java Naming and Directory Interface (JNDI) port on which the database listens for requests from the AIM Service. The port is checked for current use. If the port is in use, a warning is displayed and a new port number must be entered. Enter a port number from 1 to 65535.
- E-mail settings (SMTP Protocol and E-Mail Address)—The settings required for having e-mails sent from an AIM Reaction Policy when you select the Send Email to option.
- AIM Service RMI port number—The port on which the AIM Service will listen for requests from AIM application. Enter a port number from 1 to 65535. Port number 1122 is the default.
- Username and group for the installation directory—Prompted only if the install is performed by root.) Type the name and group (not root) of the user that owns the AIM application installation. The username and group of the user must exist on the workstation.
- MySQL Port Number—Port number for the locally installed MySQL database. You can enter a port number from 1 to 65535. Port number 3306 is the default.

NOTE: The AIM application and the JUNOScope software installations can not use the same mySQL port number. They are separate installations, each with their own mySQL sub-installation.

If the JUNOScope software mySQL instance is up and running, the AIM application installer detects that port 3306 is in use, displays a warning, and returns you to the port screen to input a different port number.

3306 is the mySQL default port number.

DNS Access

The installer checks for Domain Name System (DNS) access. If DNS Lookup fails for services.juniper.net, the installer places the following value in the ai_manager.rc file, for direct IP Address access:

homeBaseURL=https://207.17.137.247

Install ID and Licensing

The AIM installer will generate an Install ID for licensing purposes. The Install ID is displayed at the end of AIM installation on the Installation Complete screen. It can also be viewed in AIM on the License Management page under Settings. This ID is needed when contacting Juniper Networks to obtain a license file.

Downloading the AIM Application

To download the AIM application from the Juniper Networks download Web site, follow these steps:

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

   https://www.juniper.net/support/csc/swdist-encr/swdist-ais/

   There are two AIM installer files:

   - (Red Hat AIM Installer) RH_AIM1.0R1.tgz
   - (Sun Solaris AIM installer) SOL_AIM1.0R1.tgz

2. Log in to the Juniper Networks authentication system using your username and password supplied by a Juniper Networks representative.
3. Download the AIM application to your local host.
4. Extract the install.bin installer file from the downloaded <*download file name*>.tgz file.

Running the AIM Application Installer

You can run the AIM application installer from either a graphical user interface or from the console. The default is to run the graphical user interface.

Running the Graphical Installer

To run the AIM application installer graphical user interface, follow these steps:

1. Start the AIM application installation software using the following command:

   hostname% **<***installer location***>./install.bin**

   Replace *installer location* with the location of the install.bin executable.

2. Follow the onscreen instructions.

Running the Console Installer

To run the AIM application installer command-line interface, follow these steps:

1. Start the AIM application installer using the following command:

   hostname% **<***installer location***>./install.bin –i console**

   Replace *installer location* with the location of the install.bin executable.

2. Follow the console instructions.

Configuring the ai_manager.rc file

This section describes the modifications that can be made to the ai_manager.rc file in the /opt/aim/ directory for the following:

- Receiving Email from the AIM Application on page 28

The contents of the ai_manager.rc file are as follows (bold text indicates the values that can be modified):

```
;; Email Server Protocol Setting Parameters
;;
;; The AIM application will use Sun's default JavaMail provider and email
;; server protocol SMTP (Simple mail Transfer protocol) and POP (Post Office
;; protocol) to send and receive emails.
;;
;; The user will need to have the email account set up in order to send out the email
;; through AIM application as policy actions.
;;
smtp_protocol_value=smtp.juniper.net
sender=AIM@juniper.net
```

Receiving Email from the AIM Application

You are prompted for the E-mail settings (SMTP Protocol and E-Mail Address) during the AIM installation. This setting is necessary to receive e-mail from the AIM application when you set a Reaction Policy and select the Send Email to action. If you left the fields blank during the AIM installation process, you can add the values by modifying the ai_manager.rc file and adding the smtp_protocol_value and sender values as required (see “Configuring the ai_manager.rc file” on page 28). For the changes to take effect, you must restart the aimService (see “Starting and Stopping AIM Application Services” on page 29).

Starting and Stopping AIM Application Services

NOTE: For the jboss, aimService, and allservices scripts, if the DISPLAY environment variable is not set, or there is no "X" server installed on the system, do not use the console option. The console option attempts to start everything in a dtterm or xterm window.

You must start the following AIM application services before you can use a Web browser to connect and log in to the AIM application. You can start all services at once (see "Starting All Services Simultaneously" on page 29) or start them individually (see "Starting Each Service Individually" on page 29). If you start the services individually, start them in the following order:

1. mySQL—Open source database used to store information required for AIM application operation. For more detail about the command options for starting mySQL see "mysql" on page 30.

2. jboss—The underlying AIM application server. For more detail about the command options for starting jboss, see "jboss" on page 30.

3. aimService—Background service that is required to communicate with Juniper Support Systems. For more detail about the command options for starting aimService, see "aimService" on page 31.

Starting All Services Simultaneously

To start all of the services at once, use the following command:

```
user@host> /opt/aim/rc.d/allservices start
```

Starting Each Service Individually

To start each service individually, use the following commands:

```
user@host> /opt/aim/rc.d/mysql start
user@host> /opt/aim/rc.d/jboss start
```

NOTE: The jboss Service and database MUST be running before starting the aimService

```
user@host> /opt/aim/rc.d/aimService start
```

Stopping All Services Simultaneously

To stop all of the services at once, use the following command:

```
user@host> /opt/aim/rc.d/allservices stop
```

Stopping Each Service Individually

To stop each service individually, use the following commands:

```
user@host> /opt/aim/rc.d/aimService stop
user@host> /opt/aim/rc.d/jboss stop
user@host> /opt/aim/rc.d/mysql stop
```

Using AIM Application Services Scripts

This AIM application installer provides four scripts used for starting and stopping the required services:

- mysql on page 30)
- jboss on page 30)
- aimService on page 31)
- allservices on page 31)

mysql

The section provides a reference for the mysql command options. mysql is an open source database used to store information for AIM application operation. The mySQL server must be running prior to starting the JBoss service.

Command usage

mysql {[start|stop|check]}

- start—Starts the mySQL Server as a background process.
- stop—Stops the mySQL Server.
- check—States whether or not mySQL Server is currently running.

jboss

This section provides a reference for the jboss script command options. JBoss is the underlying server for the AIM application. The jboss Service is required to be running before starting the aimService.

Command usage

jboss {[start [console]]|stop|restart [console]|check|help}

- start—Starts the jboss Service as a background process.
- start console—Starts the jboss Service in a new window.
- stop—Stops the jboss Service.
- restart—Stops the jboss Service if it's running, and starts it again.

- restart console—Stops the jboss Service currently running and starts it again in a new console window.
- check—States whether or not the jboss Service is currently running.
- help—Displays the help message.

aimService

This section provides a reference for the aimService command options. aimService is the background service which is required to communicate with the Juniper Home Base.

Command Usage

aimService {[start [console]]|stop|restart [console]|check|help}

- start—Starts the AIM application service as a background process.
- start console — Starts the AIM application service in a new window.
- stop - Stops the AIM application service.
- restart - Stops the AIM application service if it's running, and starts it again.
- restart console - Stops the AIM application service currently running and starts it again in a new console window.
- check - States whether or not the AIM application service is currently running.
- help - Displays the help message.

allservices

This section provides a reference for the allservices command options. The allservices script starts all services, one at a time, in the sequence required for the successful use of the AIM application.

Command Usage

allservices {[start [console]]|stop|restart [console]|check|help}

- start - starts mySQL, Jboss Service, and the AIM application service as background processes.
- start console - starts mySQL in the background, then starts the jboss Service and the AIM application service in new windows.
- stop - stops mySQL, jboss Service, and the AIM application service.
- restart - stops mySQL, jboss Service, and the AIM application service if they are running, and starts them again.
- restart console - stops mySQL, jboss Service, and AIM application service if they're running, then starts mySQL in the background, and jboss and aimService in new windows.

- check - states whether or not mySQL, jboss Service, and AIM application services (on this workstation) are currently running.
- help - displays the help message.

Connecting to the AIM Application and Logging In

You can connect to the AIM application from a client workstation running a supported Web browser, see “AIM System Requirements” on page 24.

This section includes the following information:

Connecting to the AIM Application

To connect to the AIM application Web server and log in, follow these steps:

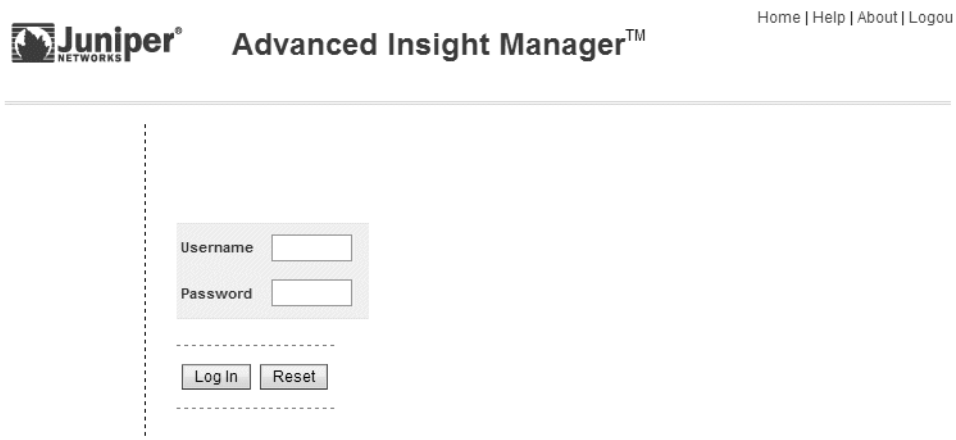
1. Start a Web browser.
2. Enter the following URL in the Address text box:

   http://<*installmachine*>:<*jbossport*>/AIManagerClient

   Replace *installmachine* with the name or IP address of the server on which the AIM application is installed, and *jbossport* with the port on which the AIM application Web server (JBoss) listens for **HTTP** requests. The default port number is 8080. For example:

   http:// myunixserver:8080/AIM
   or
   http:// 123.123.123.123:8080/AIM

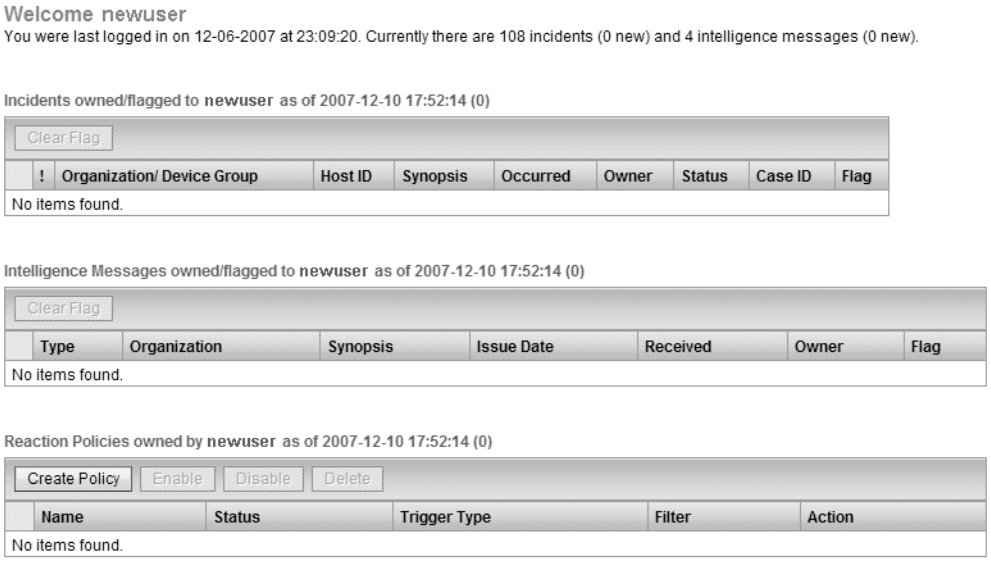
   The Advanced Insight Manager Login dialog box appears.



Logging In to the AIM Application

The default administrative username that you use to log in to the AIM application is admin. The initial password is aimadmin. The administrator can add new users for logging in and using the AIM application.

1. In the Username text box, type admin.
2. In the Password text box, type aimadmin.
3. Click Log In. The My AIM Home page appears.



Changing the AIM Administrator Password

The default AIM username is admin; the default password is aimadmin. You should the change the password to a more secure one.

To change the AIM administrator password, follow these steps:

1. Once logged into AIM, click the Settings tab.
2. Click Users in the left navigation tree. The Users page appears.
3. Select the admin user row in the Users Privileges table.
4. Click Edit. The User page appears.
5. Change the admin default password and confirm it.
6. Click Save Changes.

Uninstalling the AIM Application

You can uninstall the AIM application by running the uninstaller, located in the <*installation directory*>/AIM_Uninstaller directory.

To uninstall the AIM application, following these steps:

1. On the host where you installed the AIM application, use the following command:

   hostname% **<***installation directory***>/AIM_Uninstaller/AIMUninstaller**

AIM Application Installation Directory Structure

The following file and directory structure is created on the target AIM application software server:

```
INSTALL_DIR (Default – /opt/aim)
|-aim
|-ai_manager.rc (file used for configuring e-mail services)
|-LICENSE – text file containing the AIM licensing information
|-AIM_Uninstaller (directory containing the uninstaller)
|-README – text file detailing how to start the services
|-bin (directory used for installed utilities and scripts)
|-data (directory used for logs, actual database files, database
configuration sql scripts, etc.)
|-distfiles (directory containing the raw distributions of jboss
and mysql distributions)
|-jboss (directory used for JBoss installation)
|-jre (directory used for the JRE)
|-mysql (directory used for mySQL installation)
|-aimService (directory containing the lib and executable jar for
for the AIM Service)
|-rc.d (directory used for startup shell scripts)
```

Chapter 5

Installing and Understanding AI-Scripts

This chapter describes Advanced Insight Scripts (AI-Scripts) and how they operate in the Advanced Insight Solutions system. AI-Scripts are available to all Advanced Insight Solutions (AIS) customers with a valid support contract. This chapter describes how to install AI-Script install packages automatically (recommended for many devices) and manually (for few devices only) on Juniper Networks devices running JUNOS.

Devices running AI-Scripts are the first component in the AIS system. AI-Scripts installed on Juniper Networks devices provide the intelligence needed to automatically detect and report problem (incident) and intelligence events to ensure maximum network uptime.

NOTE: It does not matter whether AI-Scripts or AIM is installed first. However, for both, it is necessary, to know the archive location (archive-site destination) used for devices to send incident and intelligence JMBs and for AIM to retrieve this data. You can add the archive location to the device JUNOS configuration for both AI-Scripts and AIM after the initial installation, but the components are not really usable until the archive location is configured.

This chapter includes the following sections:

AI-Script Overview

AI-Scripts provide the intelligence devices need to automatically detect and report incident and intelligence events to ensure maximum network uptime.

This section provides the following topics:

What AI-Scripts Do?

AI-Scripts do the following:

- React to specific incident events that occur on devices and provide relevant information about the problems for analysis
- Periodically collect data on events that can be used to predict and prevent risks in the future.
- Package all incident and intelligence event data into a structured format [a Juniper Message Bundle (JMB)] and send it to a remote archive location so that it can be collected and displayed by, the second component in the AIS system, Advanced Insight Manager (AIM). AIM can be configured to send event data to Juniper Support Systems (JSS), the third component in the AIS system. JSS collects incident and intelligence information from AIM and sends intelligence information back to AIM specifically for the customer.

AI-Script Modes

AI-Scripts operate in two distinct modes:

- Reactive (incident-driven)—A trigger event occurs and is detected on a device. An AI-Script is executed. An AI-Script builds a Juniper Message Bundle (JMB) with event and router data, and sends it to a designated AIM archive location (see Figure 9).

  Each AI-Script corresponds to a specific device event. The list of device events that can be detected and reported will evolve over time. For the latest device events supported by AI-Scripts, see the *Advance Insight Scripts Release Notes* at http://www.juniper.net/techpubs/
- Proactive (intelligence-driven)—AI-Scripts monitor device system resources for fluctuations that could signal a future problem. AI-Scripts collect intelligence data for analysis. A tailored AI-Script builds a JMB with intelligence data, and sends it to a designated remote AIM archive location.

Events Detected by AI-Scripts

AI-Scripts detect the following types of events:

- Common software events, including daemon and Packet Forwarding Engine crashes
- Common hardware events, such as PIC alarms
- Hardware platform-specific events, such ASIC issues

For more information about the type of incidents that are detected by a specific AI-Script package, see the *AI-Scripts Release Notes* located on the AIS documentation Web site.

Juniper Message Bundle Contents

The JMB bundle for both incident and intelligence events includes the following:

- Manifest—basic router and event data
- Trend data—device counters, statistics, and settings
- Attachments—show command output for the incident event.

AI-Script Tools

AI-Scripts use the following tools on JUNOS devices:

- Event policies
- Event scripts responsible for automating event policies
- Operation (Op) scripts
- JUNOScript
- Stylesheet Language Alternative Syntax (SLAX)

Event Policies

An event policy is an if-then-else construct that defines actions to be executed by the software on receipt of a system log message. For each policy, you can configure multiple actions, as follows:

- Ignore the event.
- Upload a file to a specified destination.
- Execute JUNOS software operational mode commands.
- Execute JUNOS event scripts (Op) scripts.

For more information about event policies, see the *JUNOS Configuration and Diagnostic Automation Guide*.

Operation (Op) Scripts

An op script automates network troubleshooting and network management by doing the following:

- Automatically diagnosing and fixing problems in your network
- Monitoring the overall status of a routing platform
- Customizing the output of operational mode commands
- Ensuring a routing platform is configured to avoid known problems in the JUNOS software
- Running automatically as part of an event policy that detects periodic error conditions
- Changing the device configuration in response to a problem

For more information about op scripts, see the *JUNOS Configuration and Diagnostic Automation Guide*.

JUNOScript

The JUNOScript API (application programming interface) is an Extensible Markup Language (XML) application that client applications use to request and change configuration information on routing platforms that run the JUNOS software. The operations defined in the API are equivalent to configuration mode commands in the JUNOS command-line interface (CLI). 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. For more information about JUNOScript, see the *JUNOScript API Guide*.

Stylesheet Language Alternative Syntax

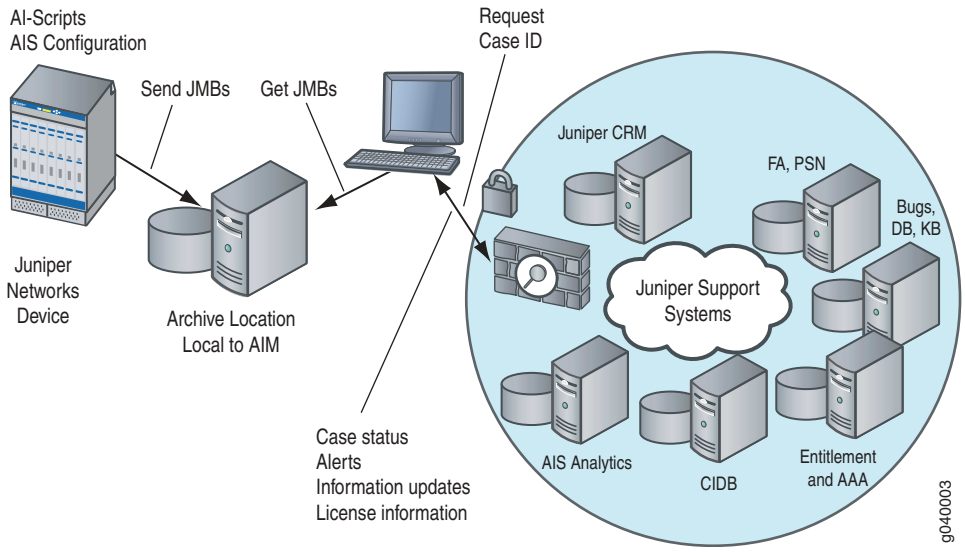
Stylesheet Language Alternative Syntax (SLAX) is a language for writing JUNOS commit and operation (op) scripts and is an alternative to Extensible Stylesheet Language Transformations (XSLT). SLAX has a distinct syntax, but the same semantics as XSLT.

SLAX has a simple syntax that follows the style of C and PERL. It provides a practical and succinct way to code, thus allowing you to create readable, maintainable commit and op scripts. SLAX removes programming instructions and XPath expressions from XML elements. XML angle brackets and quotation marks are replaced by parentheses and curly brackets ({ }), which are the familiar delimiters of C and PERL.

AI-Script Process Flow

Figure 9 shows the AI-Script process flow.

Figure 9: AI-Script Process Flow



The AIM Archive location can either be a local directory on the same system as AIM, or a directory which has been mounted from another system onto the system running AIM.

Advanced Insight Manager connects to the AIM archive location, retrieves, then displays the JMB information in Incident Manager for reactive services and Intelligence Manager for proactive services. For reactive services, AIM submits a case for resolution by JSS. For proactive services, JSS analyzes intelligence information, then sends AIM pertinent information to prevent problem events from occurring in the future.

Installing AI-Script Packages

There are two ways to install AI-Scripts:

- Automatically (recommended), using the JUNOScope Script Management feature to automatically install AI-Scripts to multiple devices at once. For more information about automatically installing AI-Scripts, see “Automatically Installing AI-Scripts to Multiple Devices At Once” on page 41.

- Manually by installing AI-Scripts on one device at time. For more information about manually installing AI-Scripts to devices, see “Manually Configuring and Installing AI-Scripts on Devices” on page 41.

Downloading AI-Script Install Packages and Release Notes

AI-Scripts are released in AI-Script install packages. AI-Script install packages are available for download from the AIS download site. Download also, the *Advanced Insight Scripts Release Notes*.

To download an AI-Script install package, follow these steps:

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

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

2. Log in to the Juniper Networks authentication system using the username and password supplied by Juniper Networks. 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 AI-Script install package. If you are installing an AI-Script install package manually, move the package to the /var/sw/pkg directory on the device. If you do not move the AI-Script install package to the device, you have to use ftp or scp in conjunction with the request system scripts add command. (Optional) Download the AI-Script install package to the same server as Advanced Insight Manager (AIM) if you will use the JUNOScope software to automatically install a package to a group of devices at once.

AI-Script Install Package Versioning

AI-Script install packages are versioned as follows:

jais-*m.nZx.x*-signed.tgz

For example:

jais-1.0R1.5-signed.tgz

The jais install package release information is described as follows:

- *m.n* is two integers that represent the software release number; *m* denotes the major release number; *n* the minor.
- *Z* is a capital letter that indicates the type of software release. In most cases, it is an R, to indicate that this is released software. If you are involved in testing prereleased software, this letter might be a B (for beta-level software).
- *x.x* is the software build number and spin number.

The collection of jais AI-Script files that comprise the install package are compressed into a tgz tarball file.

Each AI-Script install package supports up to 3 previous years of JUNOS software releases.

The show version CLI operational command displays the version of the AI-Script install package that is installed on a device.

The JMB contains the output of the show version CLI command to indicate the version of the AI-Script install package installed on a device.

Refer to the *AI-Script Release Notes* for current release information.

AI-Script Install Locations on Devices

AI-Scripts are installed on a device hard disk in the following location:

/var/db/scripts/event

AI-Scripts are installed on a device flash drive in the following location:

/config/scripts

NOTE: If you configure the load-scripts-from-flash option, the system reads event-scripts from /config/scripts/ directory otherwise the system reads event-scripts from the /var/db/scripts/ directory. The /var/run/scripts directory will always point to the right scripts directory based on the load-scripts-from-flash option.

Automatically Installing AI-Scripts to Multiple Devices At Once

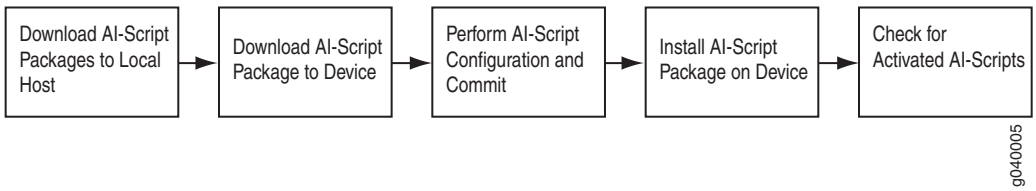
For more information about automatically installing AI-Scripts, see "Automatically Installing AI-Script Bundles" on page 83.

Manually Configuring and Installing AI-Scripts on Devices

Within AIM, devices that are configured for AIS manually will automatically be added to the device group that is associated with the AIM archive location that the JMB was sent. When the AIM detects a JMB for a device that is not managed by JUNOScope Script Management, it will note it.

Figure 10 shows the basic steps you must perform to manually configure install AI-Scripts to devices to automatically detect incidents that occur during operation and to collect incident data.

Figure 10: Basic Steps to Manually Configure and Install AI-Scripts on Devices



To manually configure and install AI-Scripts on Devices, follow these steps:

1. See "Downloading AI-Script Install Packages and Release Notes" on page 40.
2. Configure the device configuration as follows to activate AI-Scripts:

a. Enter the device CLI configuration mode. type the configure command or the edit command from the CLI operation mode. The CLI prompt changes from user@host> to user@host# and a banner appears to indicate the hierarchy level.

b. Configure an ais destination under group juniper-ais:

```
user@host# set groups juniper-ais event-options destination
juniper-junoscope {..}
```

This configuration determines the AIS remote archive location for a device.

c. Configure the commit script:

```
user@host# set groups juniper-ais system scripts commit file
jais-activate-scripts.slax optional
```

The AI-Script installer creates this script to activate AI-Scripts on the device.

d. Configure the allow-transients option to allow transient changes:

```
user@host# set groups juniper-ais system scripts commit
allow-transients
```

Transient changes are configuration changes made by commit scripts that do NOT appear in the config (except with special command)

e. Apply the juniper-ais group:

```
user@host# set apply-groups juniper-ais
```

This configuration applies the config-group juniper-ais.

f. (Optional) Configure the load-scripts-from-flash option:

```
user@host# set groups juniper-ais system scripts load-scripts-from-flash
```

NOTE: If you configure the load-scripts-from-flash option, the system reads event-scripts from /config/scripts/ directory otherwise the system reads event-scripts from the /var/db/scripts/ directory. The /var/run/scripts directory will always point to the right scripts directory based on the load-scripts-from-flash option.

3. Verify that the syntax of a configuration is correct, by use the configuration mode commit check command:

```
[edit]
user@host# commit check
configuration check succeeds
```

4. Commit the configuration. To save software configuration changes to the configuration database and activate the configuration on the router, use the commit configuration mode command. You can issue the commit command from any hierarchy level.

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

5. View the configuration:

```
groups {
    juniper-ais {
        system {
            scripts {
                commit {
                    allow-transients;
                    file jais-activate-scripts.slax {
                        optional;
                    }
                }
                load-scripts-from-flash;
            }
        }
        event-options {
            destinations {
                juniper-junoscope {
                    archive-sites {
                        "ftp://anonymous@10.7.0.124/aimdemo";
                    }
                . . .
```

6. If you have not moved the AI-Script to the device, do so now. See "Downloading AI-Script Install Packages and Release Notes" on page 40.

7. Install the AI-Script package. (For more information about working with AI-Script packages, see the Working With AI-Scripts on page 44.

```
request system scripts add <package-name>
```

8. Verify that the AI-Scripts are activated:

```
user@host$ show groups juniper-ais | display commit-scripts
```

```
user@host> show configuration groups juniper-ais | display commit-scripts
system {
    scripts {
        commit {
            allow-transients;
            file jais-activate-scripts.slax {
                optional;
            }
        }
    }
}
event-options {
    event-script {
        file problem-event-ui_commit.slax;
        file problem-event-pic_detach.slax;
        file problem-event-pfecrash.slax;
        file problem-event-dcrash.slax;
        file intelligence-event-main.slax;
}
    destinations {
        juniper-junoscope {
            archive-sites {
                "ftp://anonymous@10.7.0.124/aimdemo";
```

```
            }
        }
    }
}
```

Working With AI-Scripts

This section describes the basic commands you perform to install, delete, or rollback AI-Scripts.

- Installing an AI-Script Package on page 44
- Deleting an AI-Script Package on page 44
- Rolling back an AI-Script Package on page 44
- Not Saving Copies of AI-Scripts Package Files During Installation on page 44
- Removing AI-Script Packages After Installation on page 45

Installing an AI-Script Package

To install an AI-Script package to a router, use the following command:

```
user@host> request system scripts add <package-name>
```

Deleting an AI-Script Package

To delete an AI-Script from a router, use the following command:

```
user@host> request system scripts delete
```

Rolling back an AI-Script Package

After the deletion of an AI-Script jais package, you can rollback to the last installed jais package by using the following command:

```
user@host> request system scripts rollback
```

Not Saving Copies of AI-Scripts Package Files During Installation

To not save copies of AI-Script jais package files during installation, use the following command:

```
user@host> request system scripts add no-copy <package-name>
```

The AI-Script installer will not save a copy of a jais package in the /var/sw/pkg directory.I

NOTE: If you use the no-copy option during the jais installation, the jais package cannot be rolled back.

You can specify the no-copy option in AIM Device Group settings by selecting the no-copy check box.

Removing AI-Script Packages After Installation

To remove the AI-Script jais bundle after successful installation, use the following command:

```
user@host> request system scripts add unlink <package-name>
```

You can specify the unlink option in AIM Device Group settings by selecting the unlink check box.

Storing JMBs Locally On a Device

Use the following configuration to configure scripts to store JMBs locally on a device:

```
user@host-re0> show configuration groups juniper-ais
system {
    scripts {
        commit {
            allow-transients;
            file jais-activate-scripts.slax {
                optional;
            }
        }
    }
}
event-options {
    destinations {
        juniper-junoscope {
            archive-sites {
                "/var/tmp";               ---------------> location on the device
```

Part 3

Setting Up Advanced Insight Manager

Chapter 6

Configuring AIM General Settings

This chapter describes how to configure the Advanced Insight Manager (AIM) general settings, which also include JUNOScope and Script Bundle settings.

General Settings within AIM include parameters necessary for AIM to retrieve information from device archive locations for incident and intelligence messages, and from Juniper Support Systems (JSS) for case management and intelligence updates. General Settings allows the customer to set the port, amount, and frequency of information sharing with JSS.

JUNOScope settings allow AIM to integrate with the JUNOScope software Script Management feature to automatically install script bundles on multiple devices at once.

Script Bundle settings provide a central point for managing script bundles (also known as a AI-Script install packages) that have been downloaded from the Juniper Networks software download site. The script bundle must be local to the system running AIM. When configuring Device Groups, you can only associate one script bundle to a Device Group.

You must have AIM administrator privileges to configure General Settings.

This chapter includes the following topics:

Configuring General Settings

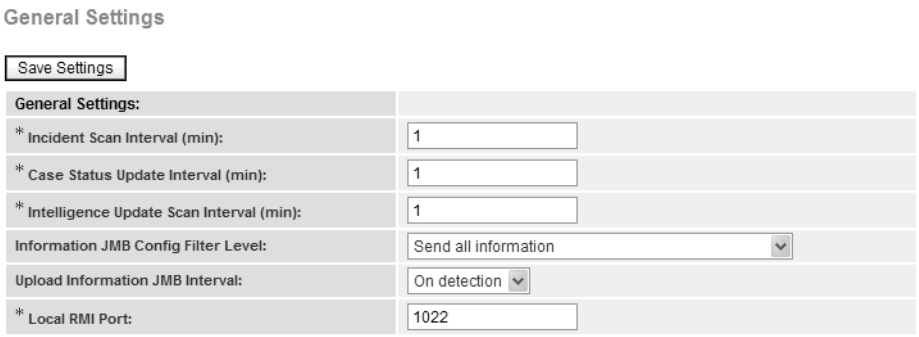
AIM General Settings allow the user to do the following:

- Set the interval used by AIM to scan device archive locations for Juniper Message Bundles (JMBs).
- Set the interval used by AIM to poll Juniper Support Systems for case status updates.
- Set the interval used by AIM to poll Juniper Support Systems for intelligence updates specific to the customer

- Set the amount of information sharing included in informational JMBs
- Set the interval used to send newly detected information JMBs to JSS
- Set the port on which the AIM Service listens for requests from the client. The default port number is the value set during the AIM installation.

To configure AIM General settings, follow these steps:

1. Click the Settings Tab. The General Settings page appears.



2. Add the required AIM General settings. See Table 11 and Table 12.
3. Click Save Settings. This action saves the AIM General settings that you modify and updates the AIM service with these new settings.

AIM General Settings Commands and Parameters

Table 11 describes the General Settings page command button.

Table 11: General Settings Command Button

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Settings	Saves any modified AIM general settings and updates the AIM service with these new settings.	AIM Admin Settings	Enabled if admin privileges	Saves settings that were modified.

Table 12 describes the AIM General Settings parameters.

Table 12: General Settings Parameters

Name	Description	Privileges	Range/ Length	Default
Incident Scan Interval (min):	Interval used to scan for new incidents in AIM archive locations.	AIM Admin Settings	0 = Off, 1 - 1440 (60 seconds - 24 hours)	3 minutes
Case Status Update Interval (min)	Interval used to poll for JTAC Case status updates from Juniper Support Systems Case Manager	AIM Admin Settings	1 - 1440 minutes (60 seconds - 24 hours)	4 minutes
Intelligence Update Scan Interval (min)	Interval used to poll for intelligence updates for this site in AIM archive locations.	AIM Admin Settings	1 - 1440 minutes (60 seconds - 24 hours)	3 minutes
Information JMB Config Filter Level	Specifies the amount of device configuration information in Juniper Message Bundles to share with Juniper: ■ Do not send ■ Send all information except configuration ■ Send all information with IP Addresses overwritten ■ Send all information	AIM Admin Settings	N/A	Do not send
Upload Information JMB Interval	Interval used to send any newly detected Intelligence JMBs to Juniper Support Systems: ■ On Detection ■ Daily ■ Weekly ■ Monthly	AIM Admin Settings	N/A	Monthly
Local RMI Port	Port on which the AIM Service listens for requests from the client	AIM Admin Settings	1-65535	1022

Configuring JUNOScope Settings

JUNOScope Settings allow the AIM application to integrate with the JUNOScope software Script Management feature to automatically install a script bundle (also known as an AI-Script install package) on multiple devices at once.

JUNOScope Settings include the following information:

- URL used to connect AIM to the JUNOScope software
- Username and password of JUNOScope AIM user with read-write privileges
- IP address used by the device to download script bundles from JUNOScope if DNS is disabled on the device

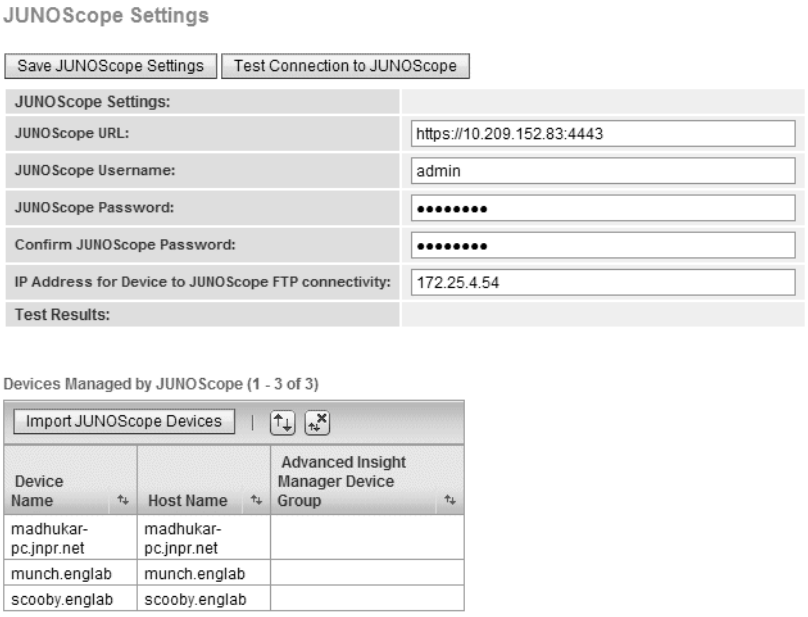
The AIM administrator must set up JUNOScope Settings before devices can be imported from JUNOScope. Devices appear in the Devices table when you click Import JUNOScope devices in the Devices Managed by JUNOScope table.

The AIM administrator can import all devices that are managed by the JUNOScope software. Only devices imported from JUNOScope will have JUNOScope Script Management capabilities, which includes:

- Automatically installing a script bundle on one or more devices in a device group.
- Ensuring that AIM archive locations for all devices in the device group are synchronized.

To configure JUNOScope Settings, follow these steps:

1. In the AIM navigation pane, click General > JUNOScope Settings. The JUNOScope Settings page appears. The JUNOScope Settings page has two sections: JUNOScope Settings and Devices Managed by JUNOScope.



2. Add the JUNOScope settings to connect AIM to the JUNOScope software server. See “JUNOScope Settings Table Description” on page 53.

3. Click Save JUNOScope Settings.

4. In the Devices Managed by JUNOScope table, click JUNOScope Devices. This action imports devices managed by JUNOScope into the AIM software. Any devices managed by the JUNOScope software are added. The JUNOScope software can install script bundles automatically to these devices. See “Devices Managed by JUNOScope Table Description” on page 54.

JUNOScope Settings Table Description

Table 13 describes the JUNOScope Settings command buttons.

Table 13: JUNOScope Settings Command Buttons

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Settings	First tests the connection to JUNOScope. If connection is successful, any modified parameters are saved.	AIM Admin Settings	Enabled if privilege	Displays the test results of the AIM connection to JUNOScope in the Test Results field: Successfully connected to JUNOScope server or An error message appears if settings are not saved.
Test Connection to JUNOScope	Uses the values in the JUNOScope settings fields to test the AIM connection to JUNOScope.	None	Always enabled	Displays test results of the AIM connection to JUNOScope in the Test Results field.

Table 14 describes the JUNOScope Settings table fields.

Table 14: JUNOScope Settings Table Parameter Descriptions

Name	Description	Privileges	Range/ Length	Default
JUNOScope URL	URL used to communicate with JUNOScope. Required for Script Bundle functionality	AIM Admin Settings	128 characters	Blank
JUNOScope Username	Log in ID to use for AIM communications with JUNOScope. This is the AIM user with read-write privileges created in the JUNOScope software. This setting is required for Script Bundle functionality	AIM Admin Settings	32 characters	Blank
JUNOScope Password	Password to use with the username	AIM Admin Settings	32 characters	Blank
Confirm JUNOScope Password	Password to type again for confirmation. The password must match the one in the password field	AIM Admin Settings	32 characters	Blank
IP Address for Device to JUNOScope FTP Connectivity	IP Address that the JUNOS devices use to transfer the Script Bundle from the JUNOScope server by way of FTP if DNS is not enabled on the device	AIM Admin Settings	32 characters	Blank
Test Results	Displays results from the Test Connection to JUNOScope command	Not allowed to modify	N/A	Blank

Devices Managed by JUNOScope Table Description

Table 15 describes the Devices Managed by JUNOScope table command button.

Table 15: Devices Managed by JUNOScope Command Button

Button Name	Description	Privileges	Enabled/ Disabled	Results
Import JUNOScope Devices	Request sent to JUNOScope to retrieve all the devices it manages and saves them in the AIM database	AIM Admin Settings	Enabled if you specify JUNOScope settings	Displays the devices imported from JUNOScope in the table.

Table 16 describes the Devices Managed by JUNOScope table fields.

Table 16: Devices Managed by JUNOScope Parameter Descriptions

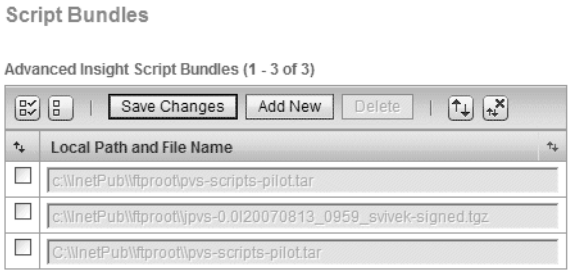
Name	Description	Privileges	Range/ Length	Default
Device Name	Name JUNOScope user assigned this device.	Not allowed to modify	N/A	N/A
Host Name	Identifier used for network communication between JUNOScope and the JUNOS device. For example it could be a hostname (host-name.juniper.net) or an IP Address	Not allowed to modify	N/A	N/A
Advanced Insight Manager Device Group	The AIM device group to which this device belongs. For information about setting up AIM device groups, see “Creating Device Groups” on page 72.	Not allowed to modify	N/A	N/A

Configuring Script Bundle Settings

Script Bundles settings provides a central point for managing script bundles (also known as AI-Script install packages) that have been downloaded from the Juniper Networks software download site. The script bundle must be located locally to the system running AIM. When configuring Device Groups, you can associate one script bundle to the Device Group that will be downloaded to all devices that belong to the device group. For more information about setting up AIM Device Groups, see “Creating Device Groups” on page 72.

To configure Script Bundle settings, follow these steps:

1. In Settings, click General > Script Bundles. The Script Bundles page appears.



2. Click Add New. A new row is added to the Script Bundles table. See Table 17 and Table 18.

3. Type the name and path (local to the system running the AIM Service) of the script bundle. The AIM Service verifies that it has access to the file. See Table 17 and Table 18.

NOTE: You cannot modify a script bundle once access to it has been verified and it has been saved in the database.

4. Click Save Changes. The script bundle location is saved to the database.

Script Bundles Commands and Parameters

Table 17 describes the command buttons on the Script Bundles page.

Table 17: Script Bundles Command Buttons

Button Name	Description	Privileges	Enabled/ Disabled	Results
Saves Changes	Saves an added script bundle and verifies that the AIM has access to that file.	AIM Admin Settings	Enabled if privilege	Displays an error message if the application could not access the file.
Add New	Adds a new script bundle to AIM.	AIM Admin Settings	Enabled if privilege	An empty row is inserted into the bottom of the table so the user can configure the new entry.
Delete	Removes all selected script bundles in the table	AIM Admin Settings	Enabled if privilege	Selected items are removed from the table

Table 18 describes the Script Bundles location on the local host where AIM is installed.

Table 18: Script Bundles Row Description

Name	Description	Privileges	Range/ Length	Default
Local Path and File Name	The name of the local path and file name where the script bundle is located on the machine running AIM. Note: A script bundle cannot be modified once access to it has been verified and it's location has been saved in the database.	AIM Admin Settings (only for creation)	128 characters and must be unique	Blank

Chapter 7

AIS License Management

This chapter describes the licenses and services required to get full functionality from Advanced Insight Solutions (AIS). For the latest AIS licensing information, see your AIS sales representative.

This chapter also describes how to activate and manage AIS licenses and subscriptions using the Advanced Insight Manager (AIM).

AIM Admin privileges are required for all License Management tasks.

This chapter includes the following sections:

Licensing and Services Required for AIS Elements

AIS consists of the following three distinct elements. With the exception of AI-Scripts, each element requires licensing, JSS support, or subscription services:

AI-Scripts

AI-Scripts are installed and activated on devices or routing platforms on your network. They detect incident and intelligence events and report them to archive locations so AIM can collect and manage them. AI-Scripts are free and require no licensing. For more information about configuring Juniper Networks devices to run AI-Scripts and for installation instructions, see “Installing and Understanding AI-Scripts” on page 35.

AIM Licensing

AIM requires a combination of feature and capacity licenses to achieve full functionality.

NOTE: AIM licenses do not provide access to AIS Base or AIS Proactive services needed for full functionality of the Advanced Insight Solutions (AIS) product. For full functionality of the Advanced Insight Solutions product, you need AIM licenses and subscriptions to AIS Proactive services.

AIM operates in fully functional, demo mode for 60 days. The demo mode allows AIM to support one multi-site organization and monitor five devices.

AIM requires the following licenses and a valid maintenance support contract described in Table 19.

Table 19: AIM Licenses and Services

License/Service Component	Description	Required/Optional
Base Product	Required to use AIM beyond a 60-day demo period. Allows the operation of Incident Manager and Intelligence Manager and the creation of one organization.	Required
Feature Licenses	Allows the operation of key AIM feature offerings. For example, the Multi-Site (Organizations) feature license is required for the creation of more than one organization within AIM.	Optional
Capacity Licenses	Required to increase the number of devices supported by AIM. Capacity licenses are available in bundles of 25, 50, and 100 devices. The maximum capacity for each AIM installation is 1000 devices.	Required
Maintenance Service	A support contract is required for AIM base product and feature phone support, which includes software upgrades and updates (see your AIS sales representative).	Optional

Juniper Support Systems

Juniper Support Systems (JSS) validates licensing, receives incident case requests, resolves incidents, analyzes and sends intelligence updates to prevent incidence occurrence.

JSS requires service subscriptions described in Table 20.

Table 20: AIS Service Subscriptions

License/Service Component	Description	Required/ Optional
AIS Base Service (Incident-Driven Online Service)	An annual subscription is required for full functionality of AIM with JSS for incident analysis and resolution.	Optional
AIS Proactive Service (Intelligence-Driven Online Service)	An annual subscription is required for full functionality of AIM with JSS for intelligence information analysis and information updates.	Optional

Juniper Networks Device Classes

AIS device capacity licensing is provided for the following Juniper Networks device classes:

- Class 1—Customer Premises Equipment (CPE) and branch devices (J-series, M7i, M10i, M20, M120, EX-3200, EX4200)
- Class 2—Edge and Aggregation devices (M40, M40e, M160, M320, MX240, MX480, MX960
- Class 3—Core devices (T320, T640, T1600, and TX-Matrix)

AIM License Management

AIM License Management lets you load a license management file representing all purchased AIM product elements.

The AIM License Management page displays:

- The AIM product serial number and the install ID
- The AIM feature licenses purchased
- The availability and number of devices purchased and the number of devices in use.
- The total number of services licenses purchased and the number of devices currently managed.

This section incudes the following information:

- "Activating AIS Licensing in AIM" on page 59
- "Managing AIM Licensing" on page 60
- "Managing Device Capacity Licenses" on page 62
- "Managing AIS Service Subscriptions" on page 63

Activating AIS Licensing in AIM

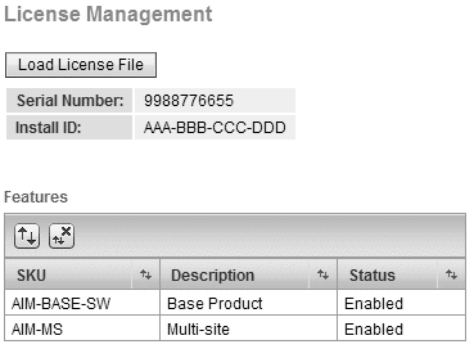
To activate AIS licensing in AIM, follow these steps:

1. Purchase the required AIS subscription services and AIM licenses for the appropriate amounts and classes of devices to be supported. See the Juniper Networks representative.
2. Install AIM. See "Installing Advanced Insight Manager" on page 23. AIM generates an install ID that you need to tell JSS to receive a license file.

   Contact Juniper Networks to purchase AIM licenses and service contracts.
3. Copy the AIM license file to the AIM install directory.

4. Log in to AIM as an admin user. See “Connecting to the AIM Application and Logging In” on page 32.

5. In AIM, click the Settings tab, then click License Management in the navigation area. The License Management page appears.



6. On the License Management page, click Load License File. The license file is imported into AIM. This action activates the features the license supports.

   Licensing is dynamic. Whenever you add a new AIM license, the functionality it enables is available without having to restart AIM.

   For more information about managing licenses and services in AIM, see the following:

   - “Managing AIM Licensing” on page 60
   - “Managing Device Capacity Licenses” on page 62
   - “Managing AIS Service Subscriptions” on page 63

Managing AIM Licensing

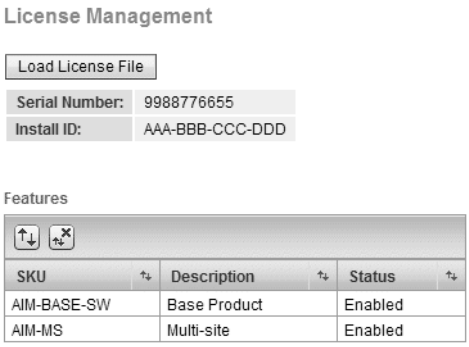
The AIM License Management page provides a point from which you can:

- Load the AIM license file that you receive from Juniper Networks.
- View the AIM serial number read from the license file.
- View the AIM installation ID number.
- View the AIM feature and capacity licenses purchased.

Managing AIM Feature Licenses

To view AIM feature and feature capacity licenses, do the following:

- Click the Settings tab, then click License Management in the navigation area. The License Management page appears.



For a description of the license management page elements, see "License Management Page Element Descriptions" on page 61.

License Management Page Element Descriptions

Table 21 describes the License Management page elements.

Table 21: License Manager Command Buttons and Field Descriptions

Element Name	Description	Privileges
Load License File button	Loads the license file sent to you by Juniper Networks. The license file includes all of the shelf keeping units (SKUs) or parts of the AIM product purchased.	AIM Admin
AIM Serial Number display field	Displays the AIM serial number read from the license file.	AIM Admin
AIM Install ID display field	Displays the AIM installation ID generated after successfully installing the application.	AIM Admin

Table 22 describes the AIM Features table columns.

Table 22: AIM License Manager Features Table Columns

Name	Description	Privileges
SKU	Shelf keeping unit code that identifies the AIM product ordered	AIM Admin
Description	Description of the SKU ordered	AIM Admin
Status	Whether the SKU is enabled or disabled	AIM Admin

AIM Feature License Messages

In AIM demo mode, the following message displays in the License Manager page to keep you informed of how much time is left before expiration:

> The Advanced Insight Manager is running in fully functional demo mode. There are XX days until expiration.

Where XX indicates the number of days left before AIM demo mode expiration.

Managing Device Capacity Licenses

The Capacity License page Summary of Current Usage table displays the total device class licenses purchased and the number of devices currently in use. The Capacity Licenses table displays the specific license SKUs purchased and the total device capacity of each one.

Juniper Support Services has the knowledge of whether or not to accept or reject the case or intelligence messages based on the service contracts.

To view the Capacity License page, do the following:

- Click the Settings tab, then click Capacity Licenses (under License Management) in the navigation area. The Capacity Licenses page appears.

  For example, this customer can manage 200 devices of each device class. The customer is only using AIM to manage four Class 1devices.

Capacity Licenses

Summary of Current Usage

Device Class Type	Licensed Capacity	Actual Usage
C1	200	4
C2	200	0
C3	200	0

Capacity Licenses

SKU	Count	Total Capacity
AIM-ADD-C1-200	1	200
AIM-ADD-C2-200	1	200
AIM-ADD-C3-200	1	200

  The SKUs are found in the AIM license file.

  For a description of the Summary of Current Usage table and the Capacity License table columns, see “Capacity Licenses Table Column Descriptions” on page 62.

Capacity Licenses Table Column Descriptions

Table 23 describes the columns in the Summary of Current Usage table.

Table 23: Summary of Current Usage Table Column Descriptions

Name	Description
Device Class Type	Identifies the Juniper Networks device class. See “Juniper Networks Device Classes” on page 59.
License Capacity	The number of devices that can be monitored in a device class.
Actual Usage	The number of devices of this class being monitored by AIM.

Table 24 describes the columns in the Capacity Licenses table.

Table 24: Capacity Licenses Table Column Descriptions

Name	Description
SKU	Shelf keeping unit (SKU) code that identifies the AIS capacity product ordered
Count	The number of capacity licenses purchased
Total Capacity	Total number of devices that can be monitored by AIM for that device class

AIM Device Capacity Licenses Messages

The following message displays in the Capacity Licenses page when device capacity exceeds 100 % usage, the following warning message appears:

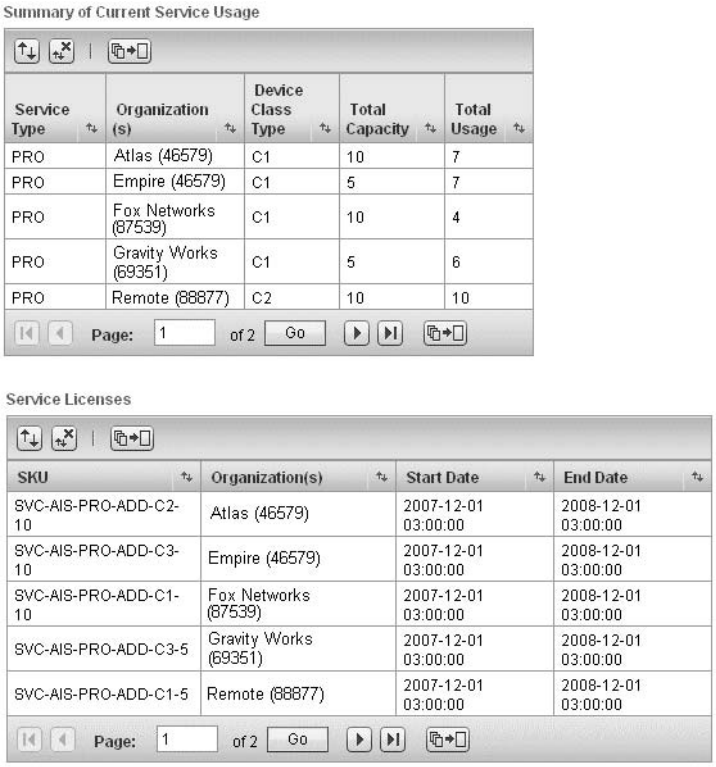
> Device Capacity Exceeded for Device Class C3. Additional AIM-ADD-C3-n license required. Please contact Juniper Support to Purchase more licenses.

Managing AIS Service Subscriptions

The Services Licenses page Summary of Current Service Usage table displays the type of service subscription, the device classes allowed to participate in the AIS service, the total number for devices that can be monitored using the service, and the total number of devices actually being monitored using the service. The Service Licenses table displays the AIS service licenses purchased, including the start and end date for each.

To view the Service Licenses page, do the following:

- Click the Settings tab, then click Services Licenses (under License Management in the navigation area). The Service License pages appears.


Summary of Current Service Usage

Service Type	Organization (s)	Device Class Type	Total Capacity	Total Usage
PRO	Atlas (46579)	C1	10	7
PRO	Empire (46579)	C1	5	7
PRO	Fox Networks (87539)	C1	10	4
PRO	Gravity Works (69351)	C1	5	6
PRO	Remote (88877)	C2	10	10

Page: 1 of 2 Go

Service Licenses

SKU	Organization(s)	Start Date	End Date
SVC-AIS-PRO-ADD-C2-10	Atlas (46579)	2007-12-01 03:00:00	2008-12-01 03:00:00
SVC-AIS-PRO-ADD-C3-10	Empire (46579)	2007-12-01 03:00:00	2008-12-01 03:00:00
SVC-AIS-PRO-ADD-C1-10	Fox Networks (87539)	2007-12-01 03:00:00	2008-12-01 03:00:00
SVC-AIS-PRO-ADD-C3-5	Gravity Works (69351)	2007-12-01 03:00:00	2008-12-01 03:00:00
SVC-AIS-PRO-ADD-C1-5	Remote (88877)	2007-12-01 03:00:00	2008-12-01 03:00:00

Page: 1 of 2 Go

For more information about the Summary of Current Service Usage table and the Service Licenses table, see “Service Licenses Table Column Descriptions” on page 64.

Service Licenses Table Column Descriptions

Table 25 describes the columns in the Summary of Current Usage table.

Table 25: Summary of Current Service Usage Table Column Descriptions

Name	Description	Default
Service Type	Identifies the AIS service subscription type purchased.	Display only column
Device Class Type	Identifies the Juniper Networks device classes to be monitored. See “Juniper Networks Device Classes” on page 59	Display only column
Total Capacity	The total number of devices that can be monitored by the AIS service.	Display only column
Total Usage	The total number of devices currently being monitored	Display only column

Table 26 describes the columns in the Summary of Current Usage table.

Table 26: Summary of Current Service Usage Table Column Descriptions

Name	Description	Default
SKU	Shelf Keeping Unit that identifies the name of the AIS service subscription purchased.	Display only column
Start Date	The date the AIS service subscription was purchases	Display only column
End Date	The expiration date of the AIS service subscription	Display only column

Service License Messages

When the AIS service capacity exceeds 100% usage, the following warning message appears on the Service License page:

> Device Capacity Exceeded for PRO Support of Device Class C1. Additional SVC-AIS-PRO-ADD-C1-n license required.
>
> Please contact Juniper Support to Purchase more licenses.

Chapter 8

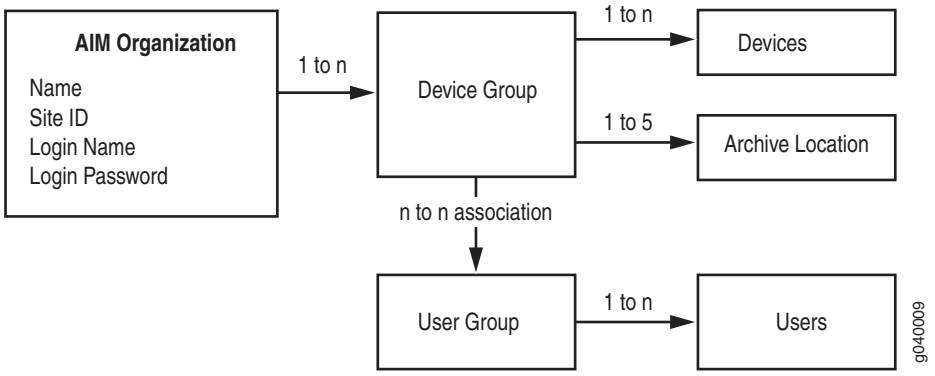
Configuring AIM Organizations and Device Groups

This chapter describes how to set up Advanced Insight Manager (AIM) Organizations and associated settings. An Organization represents a customer site in Juniper Support Systems (JSS). Organizations provide a way to manage multiple sites with one AIM installation by dividing the network into multiple logical customer site.

If you install the AIM Base Product license, you can create one Organization. Install the AIM Multi-Site feature license to create more than one Organization,

An AIM Organization requires a unique name, site ID, login name, and password to communicate with JSS. It also requires that you accept the Click-Through Agreement before proceeding. The site ID is an identifier used to denote the Customer Site field currently used in the JSS Clarify system. You can associate an Organization with one or more device groups providing a way to maintain groups of devices belonging to different customer networks. You can associate one or more devices to each device group. You can also associate a device group with one to five archive locations. You can associate an archive location with one device group at a time. You can associate a device group to one or more user groups. You can associate a user group to one or more AIM users. See Figure 11.

Figure 11: AIM Organization Creation Rules Diagram



Organizations contain device groups which are used to partition devices within one Organization. For more information about setting up a device group, see “Creating Device Groups” on page 72. Device groups are also used in conjunction with user groups to limit the access of users to certain groups of devices. See “Setting Up AIM Users” on page 89.

AIM integrates with Juniper Support Systems alert system by providing a way to register for alerts for each Organization. When alerts are registered through AIM, instead of the customer receiving e-mail messages, the alert messages are received by AIM then displayed in Intelligence Manager, see “Associating Registered Alerts with Organizations” on page 79 and.

(Optional) You can use AIM to install AI-Script bundles (also known as AI-Script install packages) on devices as long as JUNOScope software is installed. AIM communicates with JUNOScope to install AI-Script bundles on JUNOS devices managed by JUNOScope. To configure auto installation of AI-Script bundles to devices, see “Automatically Installing AI-Script Bundles” on page 83

You can also manually configure and install AI-Script bundles on each device separately.

Only users with AIM Admin Settings privileges can configure Organizations and device groups.

The chapter includes the following information:

Organization Prerequisites

Perform the following before creating an AIM Organization:

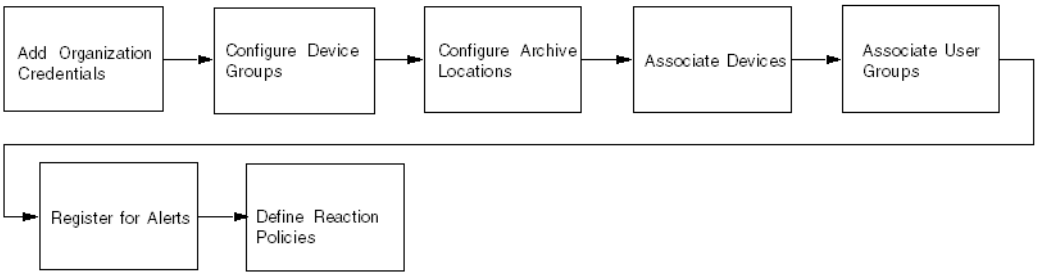
- Obtain a Site ID from Juniper Customer Support
- Obtain the Clarify username and password for the site from Juniper Customer Support.

- Download AI-Scripts Install Packages from the Juniper Networks Website to the local host file system.
- (Optional) In Setting > General > Script Bundles, select the AI-Script install packages that you want to install on JUNOS devices using the JUNOScope software Script Management.
- Configure the archive locations into which JUNOS devices will deposit JMB files. Verify that the AIM Service can access these locations as local directories (network file system (NFS) mount them if they are not local directories on the system).
- (Optional) In Settings > JUNOScope Settings: Devices Managed by JUNOScope settings, import Devices imported from JUNOScope
- Add AIM users
- Add AIM User groups
- Associate AIM users with user groups

Organization Configuration Sequence

Figure 12 shows the sequence required to create an organization.

Figure 12: AIM Organization Configuration Sequence

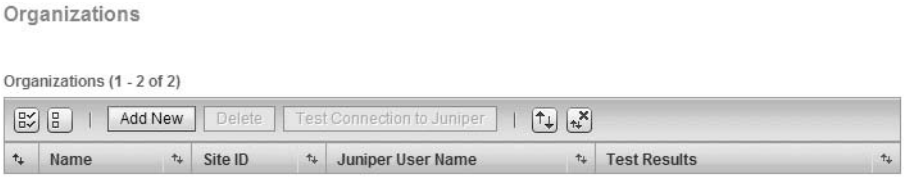


- Adding Organization Credentials on page 70
- Creating Device Groups on page 72
- Configuring Archive Locations on page 73
- Associating Devices to a Device Group on page 75
- Associating User Groups to Device Groups on page 77
- Associating Registered Alerts with Organizations on page 79

Adding Organization Credentials

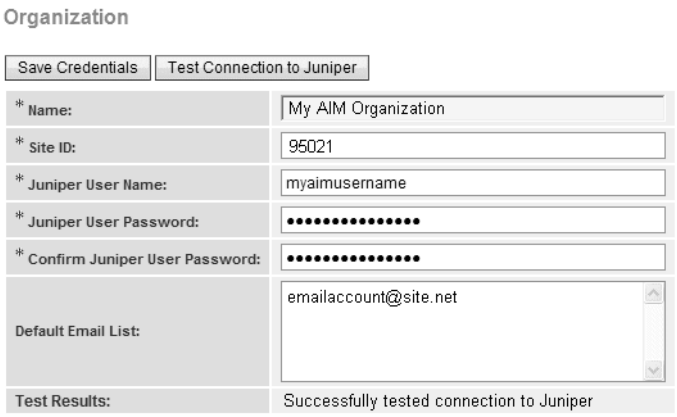
To create an AIM Organization, follow these steps:

1. Click the Settings tab, then click > Organizations in the navigation pane. The Organization page appears.



The Organizations table is empty until you create an Organization. Once you've created an organization, AIM Organizations table displays the names of existing Organizations listed alphabetically by name and includes site ID, Juniper user name, and results of the connection test between AIM and JSS.

2. Click Add New. The Organization page appears.



3. Type the Organization credentials in the provided fields. (See "Organization Page Field Descriptions" on page 71.)

4. Click Test Connection to Juniper. This command verifies the Organization Credential settings and displays the connection results. See Table 27.

5. Click Save Credentials. This action verifies and saves the Organization credentials, and displays the Device Groups, and Alert Registration tables. See Table 27.

AIM Organization Page Description

Table 27 defines the Organization page command buttons.

Table 27: Organization Page Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Credentials	Tests connection to JSS, and if successful, then saves organization name and authentication credentials in the database.	AIM Admin	If privileged	Saves the new organization credentials in the AIM database
Test Connection to Juniper	Uses the values in the fields to test the connection to JSS.	None	Always enabled	Displays the result of the test connection to JSS: success or failure.

Table 28 defines the Organization page fields.

Table 28: Organization Page Field Descriptions

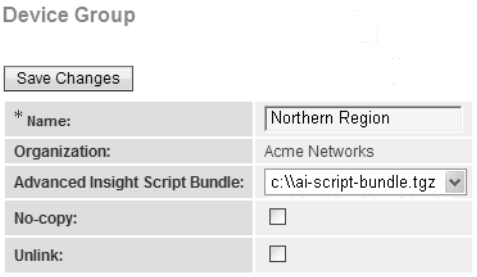
Name	Description	Privileges	Range/ Length	Default
Name	Name of the organization	AIM Admin	64 characters	Blank
Site ID	An identifier used to denote the Customer Site field currently used in the JTAC Clarify system	AIM Admin	80 characters	Blank
Juniper Username	Login to use for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases	AIM Admin	32 characters	Blank
Juniper User Password	Password to use with the username	AIM Admin	32 characters	Blank
Confirm Juniper User Password	Password must be typed in again and must match value in password field	AIM Admin	32 characters	Blank
Default email list	List of e-mail addresses to be used as the default e-mail list when a new case is submitted to Juniper. E-mail addresses should be separated by commas.	AIM Admin	65535 characters	Blank
Test Results	Displays results from the Test Connection to Juniper command: Success or failure	N/A	N/A	Blank

Creating Device Groups

Once the Organization credentials are verified and saved by clicking Save Credentials, the page expands and the Device Group and Registered Alerts tables appear below. The Device Group and Archive Locations tables are empty until you create device groups.

To create a device group, follow these steps:

1. In the Organization Device Group table, click Add New. The Device Group page appears.



2. Type the device group information in the fields and check boxes. (See “Organization Device Group Page Description” on page 72.

   The Organization to which the device group belongs displays in the Organization field. You can not modify the Organization name.

Organization Device Group Page Description

Table 29 defines the Organization page Device Group command buttons.

Table 29: Organization Device Group Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Saves device group parameters and archive locations. If an AI-Script bundle is specified, that bundle is installed on all the devices in the device group.	AIM Admin	If privileged	An error message is displayed if the device group and archive locations settings are not saved.

Table 30 defines the Organization page Device Group fields.

Table 30: Organization Device Group Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	Name of the device group	AIM Admin	32 characters	Blank
Organization	Name of the organization to which this device group belongs. The Organization to which the device group belongs displays in the Organization field. The organization name provides a link to the Organization detail screen. See "AIM Organization Page Description" on page 71.	You can not modify the Organization name.	N/A	Blank
Advanced Insight Script Bundle	Provides a drop-down list of all the AI-Script bundles managed by AIM.	AIM Admin	N/A	Blank
No-copy	Indicates the command to not save a copy of the AI-Script bundle file during installation on the device.	AIM Admin	Checked or unchecked	Blank
Unlink	Indicates the command to remove the AI-Script bundle after successful installation on the device.	AIM Admin	Checked or unchecked	Blank

Configuring Archive Locations

You can create up to five archive locations for a device group.

To configure a new archive location, follow these steps:

1. On the Device Group page, click Add New in the Archive Locations table. A new row appears in the Archive Locations table. The Archive Locations table is empty until you add archive locations.

2. Type the required information in the Archive Locations table column fields. See "Archive Locations Table Description" on page 74.

3. Click Test Access. The test results appear in the Test Results field. The test results are either Success or Failure.

4. Click Save Changes at the top of the Device Groups page. This command saves the device group parameters and the archive locations.

If you specify an AI-Script install package, that package is automatically installed on all the device in the group that were imported from JUNOScope,

Archive Locations Table Description

Table 31 defines the Archive Locations table command columns.

Table 31: Archive Locations Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Test Access	Tests access to the selected device archive local location pathname specified in the Local Location field.	AIM Admin	Enabled when you select an archive location in the Archive Location table.	The Test Access results are either: ■ Successfully accessed location. ■ Failure to access location.
Add New	Adds a new row in the Archive Location table	AIM Admin	Always enabled	
Delete	Removes the selected archive location	AIM Admin	Enabled when you select an archive location row in the Archive Location table.	

Table 32 defines the Archive Locations table fields.

Table 32: Archive Location Table Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Local Location	The name of the local path where the Juniper device sends incident and intelligence JMBs. This path is relative to the installation machine.	AIM Admin	128 characters	Blank filed
Test Results	Displays results from the Test Access command for this row. The test results are either: ■ Successfully accessed location. ■ Failure to access location.	Not allowed to modify	N/A	Blank display field
Upload Command	Command that will be specified to set the archive location on the JUNOS devices. This command will be used to transfer the JMB files to the archive location.	AIM Admin	128 characters	Blank field
Password	Password that will be used by the JUNOS devices when they run the upload command to transfer the JMB files to the archive location.	AIM admin	64 characters	Blank field

Associating Devices to a Device Group

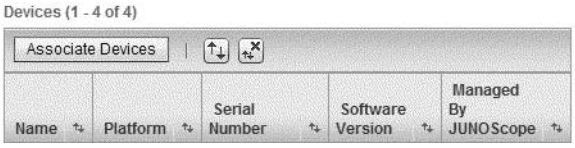
The Devices table displays the devices in the AIM application that are contained in a particular device group.

Devices can be associated to a device group in two ways:

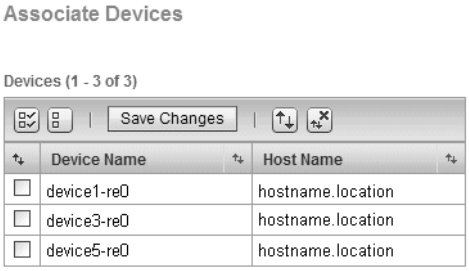
- When a JMB file is detected in any of the archive location of this device group, then the device that generated the JMB file is automatically added to the device group.
- Devices that have been imported from JUNOScope can be associated to the device group manually my the user.

To associate devices, follow these steps:

1. In the Devices table, click Associate Devices. The Devices table is empty until you associate devices to the device group.

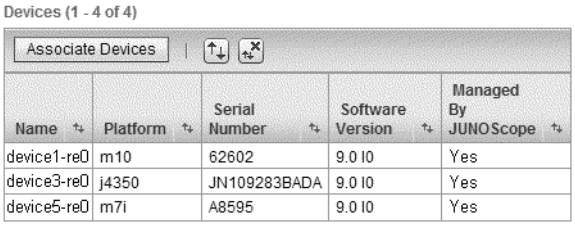


The Associate Devices page appears with the available devices.



2. In the Associate Devices table, select the devices you want to associate with the device group. The devices that appear in the table are those that were imported from JUNOScope. See “Configuring JUNOScope Settings” on page 51. See “Associate Devices Table Description” on page 77.

3. Click Save Changes. The newly associated devices now appear in the Device table by device name, routing platform type, serial number, software version, and whether they are managed by the JUNOScope software.



See “Devices Table Description” on page 76.

Devices Table Description

Table 33 defines the Device table command buttons.

Table 33: Devices Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled
Associate Devices	Displays the Associate Devices page where you can select device groups to associate with an organization.	AIM Admin	Always is enabled

Table 34 defines the Devices table column descriptions.

Table 34: Devices Table Column Descriptions

Name	Description	Privileges
Name	Name of the device	Not allowed to modify
Platform	Type of device (routing platform)	Not allowed to modify
Serial Number	Serial number of device	Not allowed to modify
Software Version	Operating software release and version running on the device	Not allowed to modify
Managed by JUNOScope	Whether device was imported from the JUNOScope software. Yes appears if the devices is managed by JUNOScope. The column is blank if the devices is not managed by JUNOScope. Indicates that AI-Script bundle will be installed on the device	Not allowed to modify

Associate Devices Table Description

Table 35 describes the command button in the Associate Devices table.

Table 35: Associate Devices Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled
Save Changes	Saves the selected devices to associate with an AIM Device Group as part of AIM Organization creation.	AIM Admin	Always is enabled

Table 36 describes the columns in the Associate Devices table.

Table 36: Associate Devices Table Descriptions

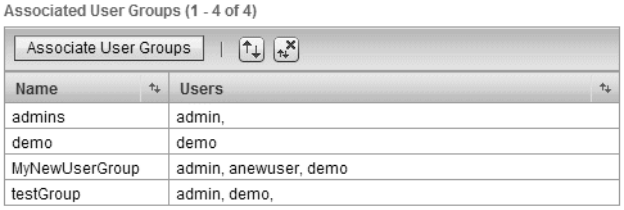
Button Name	Description	Privileges
Device Name	Name of the device to associate with an existing device group	AIM Admin
Host Name	The unique name by which a device is known on a network	AIM Admin

Associating User Groups to Device Groups

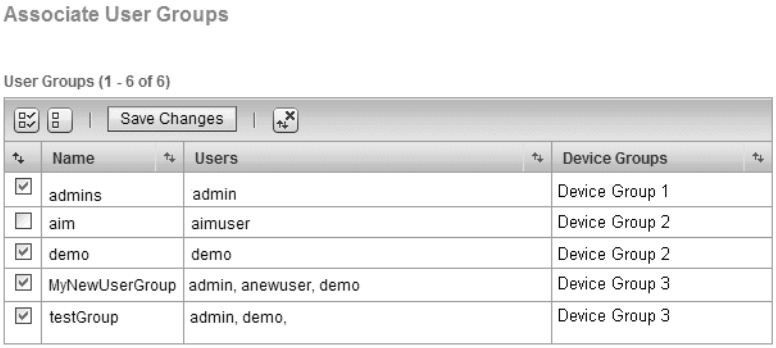
The Associate User Groups table displays the user groups that are currently associated with the device group. The Associate User Groups table displays the user group name and users belonging to it.

To associate users to a device group, follow these steps:

1. In the expanded Device Group page Associated User Groups table, click Associate User Groups.



   The Associated User Groups table is empty until you associate user groups to a device group. The Associate User Groups table appears.



2. Select the user groups you want to associate with the device group.

3. Click Save Changes. The selected user group(s) appear on the Associate User Group table. “Associate User Groups Table Description” on page 78.

Associate User Groups Table Description

Table 37 defines the Associate User Groups table command buttons.

Table 37: Associate Users Group Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Sets which user groups are associated with the device group and navigates the user back to the Device Group page	AIM Admin	Disabled until you select a user group.	Saves user groups associated with the device group

Table 38 defines the Archive Location table fields.

Table 38: Associate Users Group Table Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	Name of the user group to associate with the device group	AIM Admin	Not allowed to modify	N/A
Users	Name of users associated to the user group separated by commas	AIM Admin	Not allowed to modify	
Device Groups	Name of the device groups associated with a user group	AIM Admin	Not allowed to modify	

Associating Registered Alerts with Organizations

JSS Alerts that the customer registers for using http://www.juniper.net/alerts/ (scroll to the bottom of the page), can be associated with an Organization. The alerts the customer registers for are selected in the Alert Registration table. The customer can ensure that the requested alerts are selected to associate them with the current organization.

The AIM ties into the Juniper Support Systems (JSS) Alert system which allows customers to go the Juniper support web site and register for specific types of alerts are then be e-mailed to them.

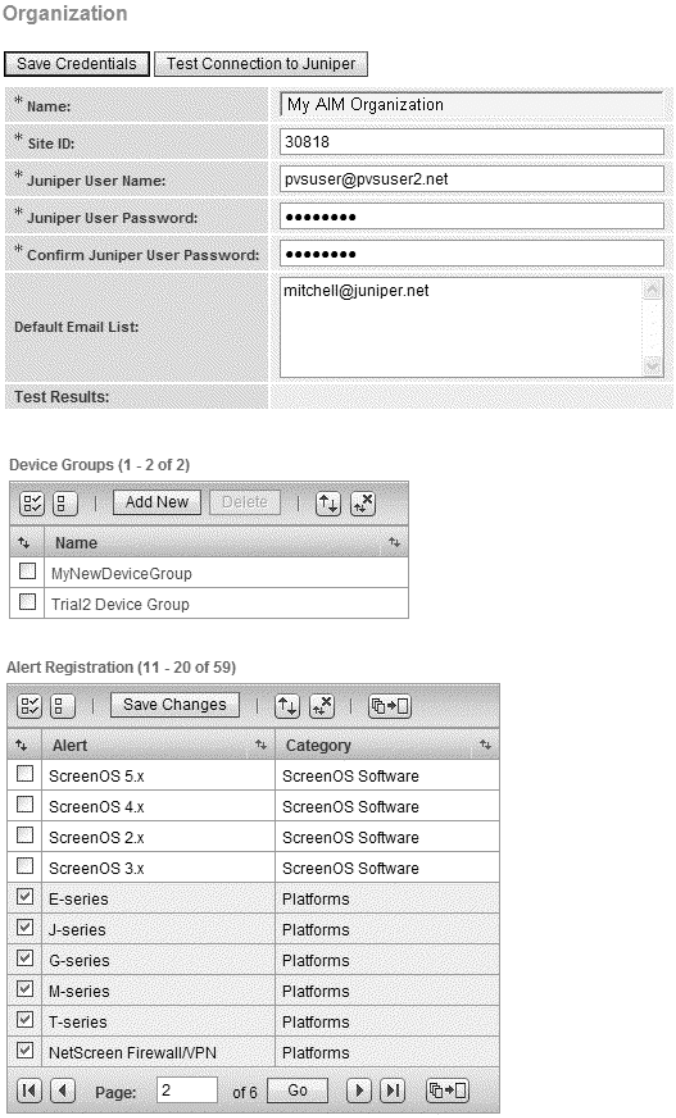
When you register for alerts in AIM, you receive the same information. The difference is instead of receiving the information in e-mail messages, alert messages are received by AIM and displayed in Intelligence Manager. This action provides the customer one central place to receive alerts, a way to manage who is responsible for following up on alerts by assigning alerts to AIM users.

When you click Scan for Impact on an Alert Detail page, you see which devices in the network are impacted by the information received (See “Scanning Intelligence Messages for Impact” on page 123).

When you navigate to the Organization Detail page (see later in this section), the alerts available to register for are retrieved from JSS and are displayed in the Alert Registration table. Those alerts that are checked in the table indicate the ones the organization is already registered to receive. Once you specify the alerts to register for, the Save Changes button registers those alerts with JSS for that Organization.

To associate registered alerts, follow these steps:

1. Click Settings > Organizations. The Organizations page appears. Click the name of the organization to register alerts. This action displays the Organizations page.



   The Alert Registrations table displays the alerts available to register for that are retrieved from Juniper Support Systems. The alerts that the Organization is already registered to receive are checked in the table. See “Alert Registration Table Description” on page 81.

2. Select the alerts that you want to be registered with the Organization.

3. Click Save Changes to register the specified alerts with Juniper Support Systems.

Alert Registration Table Description

Table 39 defines the Alert Registrations table command buttons.

Table 39: Alert Registration Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Registers the selected alerts with Juniper Support Systems	AIM Admin	Enabled when you select an alert.	Registers the selected alert with JSS.

Table 40 defines the Alert Registration table fields.

Table 40: Alert Registration Table Field Descriptions

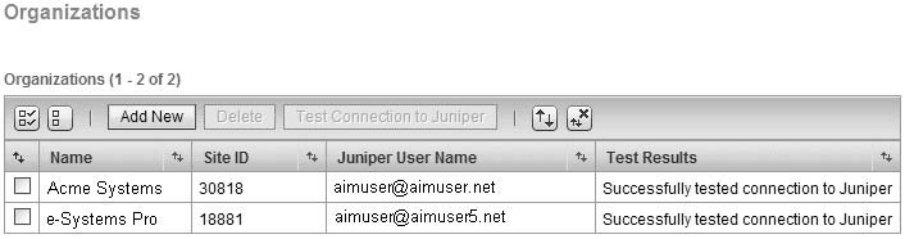
Name	Description	Privileges	Range/ Length	Default
Alert	Type of alert for which to register	Not allowed to modify	N/A	N/A
Category	Category to which the alert belongs	Not allowed to modify	N/A	N/A

Using the Organizations Table

The AIM Organizations table displays an alphabetized listing of organizations by site ID, Juniper user name, and JSSS connection to Juniper test results.

To view the Organizations table, do the following:

1. Click Settings > Organizations. The Organizations table appears with the organizations that have been created.



See “Organization Table Description” on page 82.

Organization Table Description

Table 41 describes the Organizations table command buttons.

Table 41: Organizations Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Add New	Initiates creation of a new Organization	AIM Admin Settings	Available if privilege	Displays initial creation screen of Organization
Delete	Deletes specified organizations	AIM Admin Settings	Available if privilege and one or more organizations are selected	Removes all of the selected organizations from the table.
Test Connection to Juniper	Uses the credentials of the selected organizations to test the connection to Juniper.	None	Enabled if one or more organizations are selected	Displays the result of the test connection to JSS (success or failure) for each of the selected Organizations in the Test Results column

Table 42 defines the Organizations table columns.

Table 42: Alert Registration Table Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	Name of the organization This field is a link and can be used to navigate to the detail screen of the organization	Not allowed to modify	N/A	N/A
Site ID	An identifier used to denote the Customer Site field currently used in the JTAC Clarify system	Not allowed to modify	N/A	N/A
Juniper Username	Login to use for communications with the JTAC Clarify system such as creating cases, and checking for updates to existing cases	Not allowed to modify	N/A	N/A
Test Results	Displays results from the Test Connection to Juniper command: Success or failure	Not allowed to modify	N/A	N/A

Viewing Organization Details

To view organization details page, do the following:

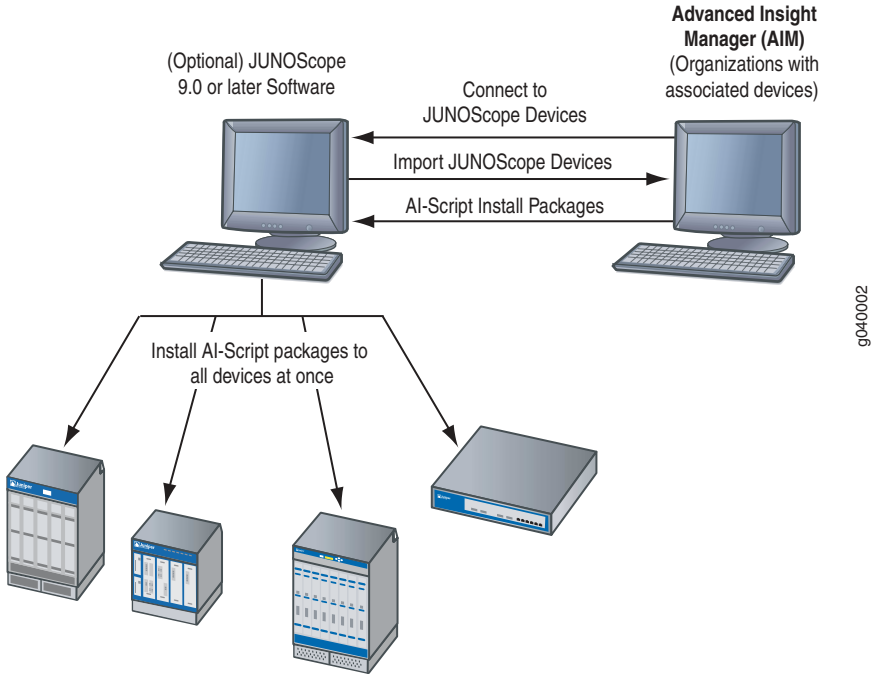
1. Click Settings > Organizations. The Organizations table appears with the organizations that have been created.

2. Click the Organization name link in the table. The to see the setting parameters. The Organization page appears with the credentials and other elements that have been associated, such as device groups and alerts. For more information, see “AIM Organization Page Description” on page 71, “Organization Device Group Page Description” on page 72, and “Alert Registration Table Description” on page 81.

Automatically Installing AI-Script Bundles

You can optionally use AIM to install AI-Script bundles (also known as AI-Script install packages) on devices as long as there is a JUNOScope software installation. AIM communicates with JUNOScope to install AI-Script bundles on JUNOS devices managed by JUNOScope. See Figure 13.

Figure 13: Automatic Installation of AI-Script Install Packages Using JUNOScope



To configure auto installation of AI-Script bundles to devices, follow these steps:

1. Configure the credentials used to communicate with JUNOScope, see "Configuring JUNOScope Settings" on page 51.

2. Import devices that are managed by JUNOScope, see "Configuring JUNOScope Settings" on page 51.

3. Configure Script Bundles, see "Configuring Script Bundle Settings" on page 54.

4. Associate imported devices with a device group, see "Creating Device Groups" on page 72.

5. Configure the Script Bundle of the device group and set the No-copy and Unlink installation attributes, see "Creating Device Groups" on page 72

6. Add archive locations specifying the upload command password attributes, see "Configuring Archive Locations" on page 73,

7. Press the Save Changes button, AIM sends a message to JUNOScope to install the selected script bundle on the associated devices.

If you do not want to use AIM to install AI-Script bundles, you can manually configure and install AI-Script bundles to each device separately. To install AI-Script bundles manually, see “Manually Configuring and Installing AI-Scripts on Devices” on page 41.

Chapter 9

Configuring Trap Destinations

This chapter describes how to specify a destination for SNMP traps sent when an AIM reaction policy is triggered that has the Send Trap action option specified (see “Creating a Reaction Policy” on page 125.

The traps sent to a network management station destination correspond to the trigger type of an AIM reaction policy that has been created. For example:

- New Event Detected
- Event Reported to Juniper
- JTAC Case ID Assigned
- JTAC Case Updated
- New Intelligence Update Received

For more information about AIM traps, see “Supported SNMP Traps” on page 154.

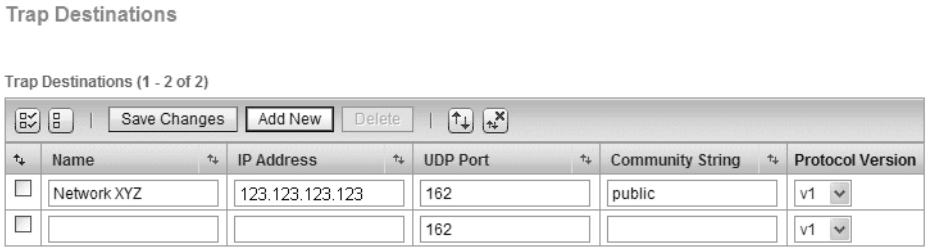
In AIM, the Trap Destinations table lists all of the trap destinations that have been created.

This chapter includes the following sections:

Adding a New Trap Destination

To create a new trap destination, follow these steps:

1. Click the Settings tab, then click Trap Destinations in the navigation area. The Trap Destinations page appears.



2. Click Add New. A new row appears in the Trap Destinations table.

3. Add the trap destinations information in the row fields. See “Trap Destinations Table Field Descriptions” on page 87 for trap destination parameters.

4. Click Save Changes.

Trap Destinations Table Field Descriptions

Table 43 describes the Trap Destinations table command buttons.

Table 43: Trap Destinations Command Buttons and Field Descriptions

Command Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Saves any changes made in the Trap Destinations table.	AIM Admin	Enabled when you add a new trap destination	Saves new changes.
Add New	Adds a new row in the Trap Destinations table.	AIM Admin	Always enabled	Adds a blank new row in Trap Destinations table.
Delete	Deletes the selected row(s) in the Trap Destinations table.	AIM Admin	Enabled when you select a trap destination row	Deletes selected trap destination row(s).

Table 44 describes the Trap Destinations table columns.

Table 44: Trap Destinations Table Columns

Name	Description	Privileges	Range/ Length	Default
Name	Unique name of trap destination.	AIM Admin		
IP Address	IP Address of network management station where AIM trap destination will be sent.	AIM Admin		
UDP Port	The User Data Protocol (UDP) port is a mechanism that allows a computer to simultaneously support multiple communication sessions with computers and programs on the network. A port directs the request to a particular service that can be found at that IP address.	AIM Admin		Port 162
Community String	A community string is a password that allows access to a network device. It defines what community of people can access the SNMP information that is on the device. The network operator responsible for the network device typically sets the community strings. The default strings 'public' and 'private' are usually assigned by default.	AIM Admin		
Protocol Version	Supported Simple Network Management Protocol (SNMP) versions: ■ v1 ■ v2c	AIM Admin		SNMPv1

Deleting a Trap Destination

To delete a trap destination, follow these steps:

1. Click the Settings tab, then click Trap Destinations in the navigation area. The Trap Destinations page appears.
2. Select the trap destination row(s) that you want to delete.
3. Click Delete.

   The traps that were supposed to be sent to the deleted trap destination will not be sent.

Chapter 10

Setting Up AIM Users

This chapter describes how to add users to Advanced Insight Manager (AIM). Users are able to view only incidents and intelligence messages to which they have appropriate permissions. Permissions are based on the user group(s) to which users are assigned and the association of those user groups to specified device groups. For more information about configuring user groups, see “Setting Up AIM Users” on page 89. For more information about configuring device groups, see “Creating Device Groups” on page 72.

Additionally, users can be assigned permissions that allow them access only to a subset of AIM operations. If the Multi-Site license is present, allowing for multiple organizations, users have access to organizations and the devices contained in them based on their user group and device group associations.

Incidents and Intelligence Updates assigned to users are filtered based on the user’s user group and device group associations.

An AIM user must have the following:

- Unique user name
- Unique Password
- Privileges that determine the operations that can be performed

The password for the administrator should not match the username, and should not be a word that can be easily guessed.

In general, AIM passwords should be:

- Easy to remember so that users are not tempted to write them down.
- Contain up to 32 characters, using at least two of the four defined character sets (uppercase, lowercase, numeric, other). The characters in the set "other" are those that can be entered using a single keystroke, or a keyboard character accessed using the Shift key, that does not fall into any of the other three groups.

This chapter includes the following sections:

Default AIM User Account

The default AIM user account is:

- Username: admin
- Password: aimadmin

The default AIM user account is granted all privileges and is the primary administrator account for the application. You cannot delete the default AIM user account, and privileges cannot be modified.

It is recommended that you change the default password after the AIM administrator logs in. The password can be up to 32 character.

Understanding AIM Ownership

AIM provides ownership for incidents and intelligence messages. Once an AIM user becomes owner, that user is responsible for keeping track of the progress of a case or updates from JSS to ensure that case is resolved or for what actions are needed for an intelligence message. The incident or intelligence message owner can also update the case status to reflect progress made.

When an AIM user has ownership and appropriate privileges, that user can do the following:

- Incidents
  - Edit priority and email list if incident is not submitted to JSS
  - Submit incident to JSS
  - Update owner status to reflect progress
- Intelligence Messages
  - Update owner status to reflect progress

There are three levels of user ownership that an AIM administrator can assign when adding or modifying user privileges (see Table 45).

Table 45: AIM Ownership Levels

Ownership Level	Description
None	User is not allowed to own or assign ownership to any AIM user.
Level I	User can voluntarily take ownership of any unassigned incidents or intelligence messages.
Level II	User can voluntarily take ownership of any incidents or intelligence messages regardless if assigned or unassigned.
Level III	User can either give or take away ownership of incidents or intelligence messages to any user.

AIM User Privileges

The AIM application enforces user privileges so that users can only have access the information to which they have privileges. Table 46 defines the AIM user privileges.

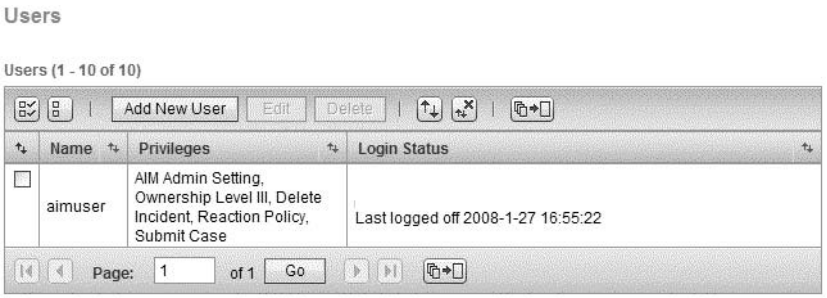
Table 46: AIM User Privileges

Privilege	Description
AIM Admin Setting	AIM administrators can perform the following tasks: If the logged in user does not have Admin privileges, these settings can only be viewed: ■ Connect AIM to JSS ■ Perform alert registration ■ Set archive locations incident detection interval ■ Set up and manage organizations ■ Set up and manage licensing ■ Create, edit, and delete trap destinations ■ Create, edit, and delete users ■ Create, edit, and delete user groups ■ Create, edit, and delete device groups ■ Associate device groups ■ Associate user groups
Ownership	Three levels of AIM user ownership are provided that the administrator can use when assigning new user privileges. See Table 45.
Delete Incident	AIM user can delete incidents in Incident Manager.
Reaction Policy	AIM user can manage all the policies he/she owns. It includes creation, deletion, disable, and enable policies. The policy will automatically be owned by the user who created it. If a user is deleted from AIM, all policies belonging to that user will be automatically deleted as well.
Submit Case	AIM user can submit any unassigned incidents to JSS.

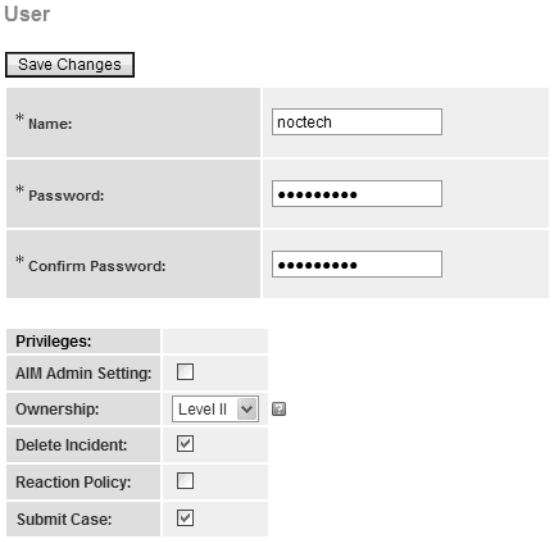
Adding a AIM User

To create an AIM user, follow these steps:

1. Click Settings > Users. The Users page appears with the default AIM admin user if you have added no other users. See “Default AIM User Account” on page 90.



2. Click Add New User. The User page appears.



3. Type the user name.

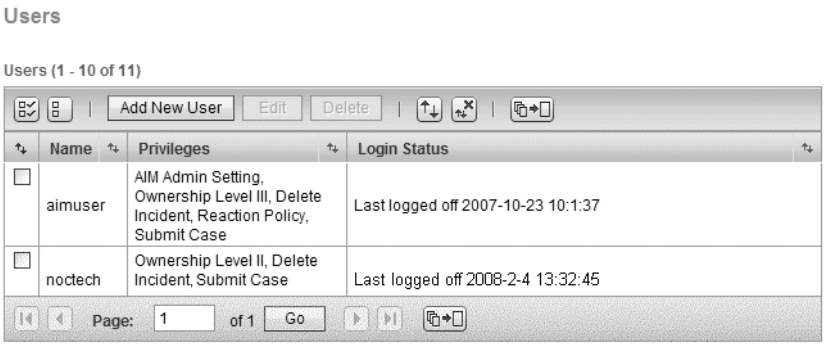
4. Type the user password.

5. Retype the password to confirm it.

6. Select the user privileges that you want. For more information about AIM user ownership, see Table 45. For more information about AIM user privileges, see Table 46.

7. Repeat Steps 2 through 6 for each new AIM user you add. For more information about the Add New User page, see

8. Click Save Changes. The AIM user settings are saved in the database and the new user appears in the Users table.



Add New User Page/Edit User Page Description

Table 47: Add New User Page/Edit User Page Command Button

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Saves the changes made to AIM user name, password, and privileges.	AIM Admin Settings	Enabled if admin privileges	Error message is displayed if settings were not saved

Table 50 describes the New User Field descriptions.

Table 48: Add New User Page/Edit User Page Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	AIM user name	AIM Admin Settings	32 characters	Blank on the Add User page. Display username only on the Edit User page
Password	AIM user password	AIM Admin Settings	32 characters	Blank
Confirm Password	Retyped AIM user password for confirmation	AIM Admin Settings	32 characters	Blank
AIM Admin Setting Privilege	See Table 46	AIM Admin Settings	N/A	Unchecked
Ownership Privilege	Three levels of AIM user ownership are provided that the administrator can use when assigning new user privileges: ■ Level I ■ Level II ■ Level III See Table 45.	AIM Admin Settings	N/A	None

Name	Description	Privileges	Range/ Length	Default
Delete Incident Privilege	AIM user can delete incidents in Incident Manager.	AIM Admin Settings	N/A	Unchecked
Reaction Policy Privilege	AIM user can manage all the policies he/she owns. It includes creation, deletion, disable, and enable policies. The policy will automatically be owned by the user who created it. If a user is deleted from AIM, all policies belonging to that user will be automatically deleted as well.	AIM Admin Settings	N/A	Unchecked
Submit Case Privilege	AIM user can submit any unassigned incidents to JSS.	AIM Admin Settings	N/A	Unchecked

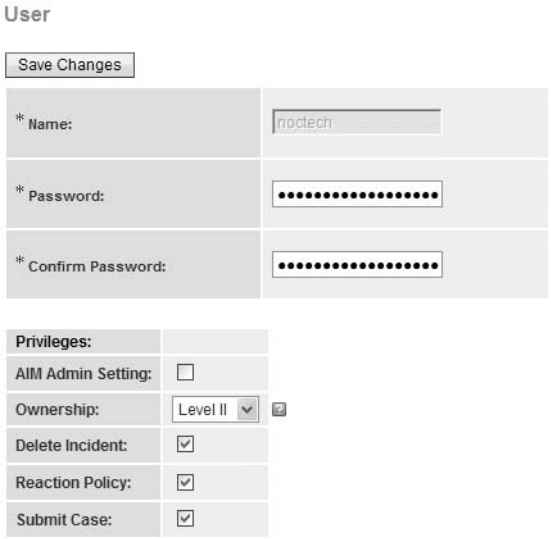
Editing a User

You can edit an AIM user password and privileges.

To edit an AIM user, follow these steps:

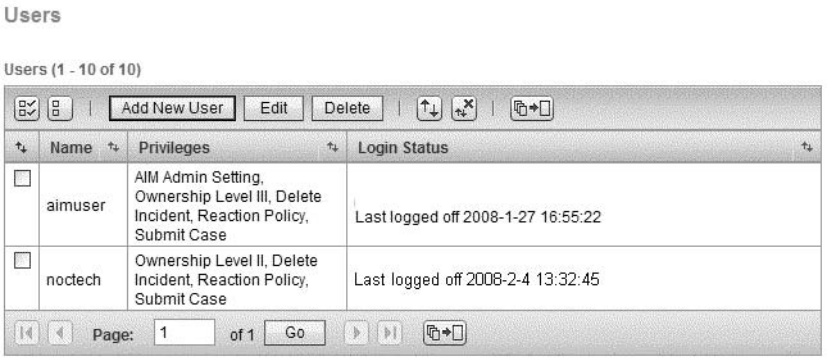
1. Click Settings > Users. The Users page appears.
2. Select the AIM user you want to edit. The Edit button is enabled.

3. Click Edit. The Edit User page appears.



4. Edit the user password or the privileges. To change a username, you must delete that user, then create a new one. For more information about the Edit User page, see "Add New User Page/Edit User Page Description" on page 93.

5. Click Save Changes. The user information is saved in the AIM database. The User table appears with the edited user information (except password information) added.

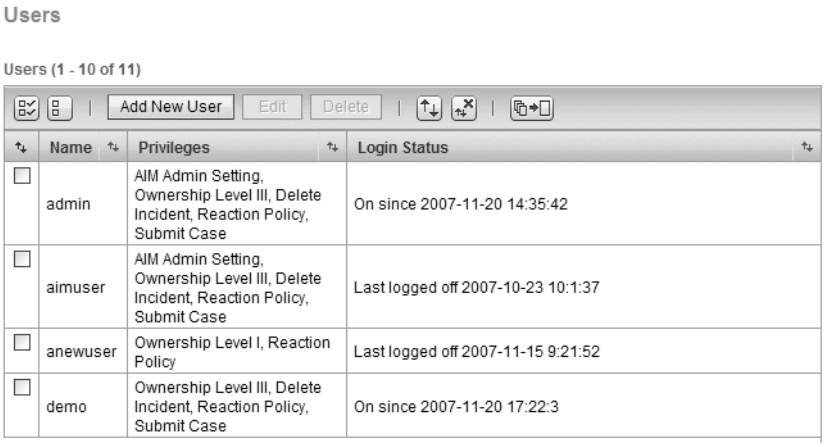


Using the User Table

The User page provides a single point to view and manage AIM user names, privileges, and login status of AIM users.

To view the User table, follow these steps:

1. Click Settings > Users. The Users page appears.



For more information about using the Users table, see

Users Table Description

Table 49 describes the User table command buttons.

Table 49: User Table Command Buttons

Button Name	Description	Privileges	Enabled/ Disabled	Results
Add New User	Displays User page used to add a new AIM user	AIM Admin Settings	Enabled if admin privileges	Displays User page
Edit	Displays User page used to edit user password and privileges. You must select one user to edit the parameters. **Note:** You cannot edit default admin user privileges. You cannot edit a user name.	AIM Admin Settings	Enabled if admin privileges and if user is selected	Displays User page
Delete	Removes the selected user from the User table and the AIM database.	AIM Admin Settings	Enabled if admin privileges and if user is selected	Deletes selected user

Table 50 describes the Users table columns.

Table 50: Users Table Columns

Name	Description	Privileges	Range/ Length	Default
Name	Name of AIM user.	Not allowed to modify	N/A	N/A

Name	Description	Privileges	Range/ Length	Default
Privileges	AIM privileges assigned to user, see Table 46 for description of AIM user privileges.	Not allowed to modify	N/A	N/A
Login Status	Date and time AIM user has been logged in to the application. Also, date and time when AIM user last logged out of the application.	Not allowed to modify	N/A	N/A

Deleting a User

To delete an AIM user, follow these steps:

1. Click Settings > Users. The Users page appears.
2. Select the AIM user you want to delete. The Delete button is enabled.
3. Click Delete.
4. Click Save Changes. The user is removed from the AIM database.

Chapter 11

Setting Up AIM User Groups

This chapter describes how to set up Advanced Insight Manager (AIM) user groups. User groups contain a list of selected users. The user group name must be unique within the AIM installation. AIM users should be created before AIM user groups. User group members are selected from the existing pool of AIM users. For more information about creating users, see “Setting Up AIM Users” on page 89.

Once created, user groups can be associated with device groups. This can be done on the User Group Settings page, or on the Device Group Settings Page. For more information about creating AIM device groups, see “Creating Device Groups” on page 72.

To create AIM user groups, you must be the AIM administrator or have AIM Admin Settings enabled in the user settings.

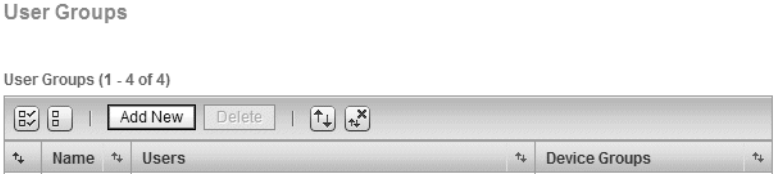
This chapter includes the following information:

Creating a New User Group

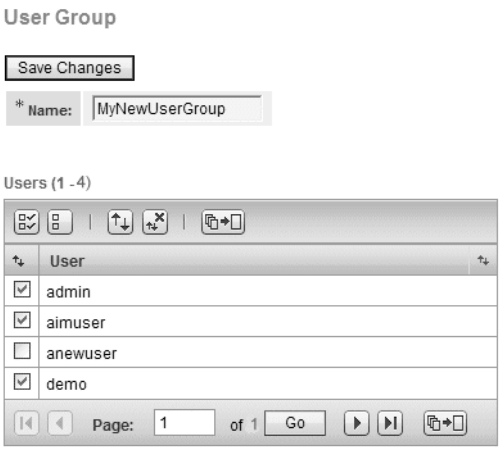
You must be the AIM administrator or have AIM Admin Setting privileges to create a user group. When you create a user group, the User Group table appears without the Associated Device Groups table displayed.

To create an AIM user group, follow these steps:

1. Click Settings > User Groups. The User Group page appears. The User Group table is empty until you add a new user group.



2. Click Add New. The User Group page appears.

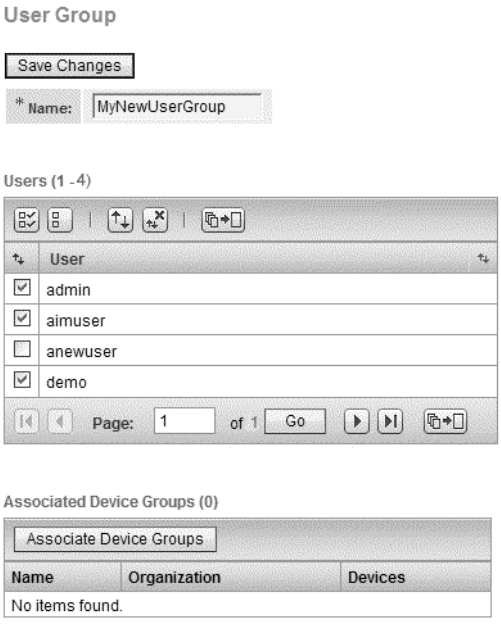


3. In the Name field, type a unique name for the user group.

4. In the Users table, select the users you want to add to the user group.

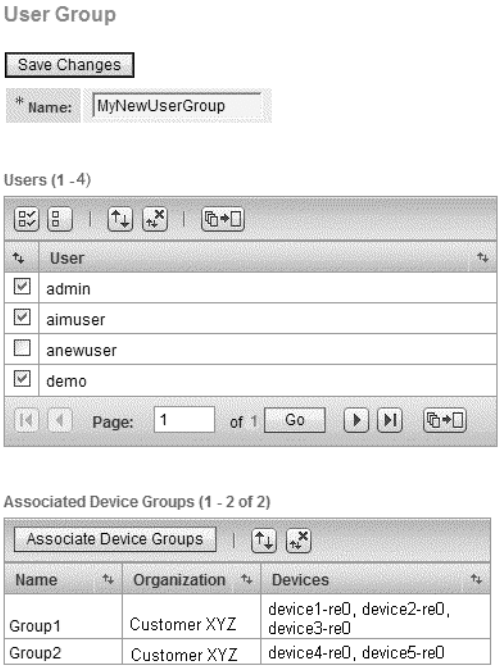
5. Click Save Changes. This saves the new user group settings. For more information about the User Group page, see “User Group Page Description” on page 102.

   The Associate Device Groups table appears below the User’s table.

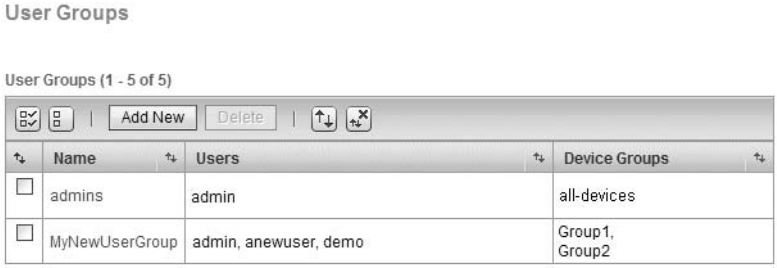


6. Click Associate Device Groups. The Associate Device Groups page appears. Device groups can be associated with one or more user groups.

7. Select the device groups that you want to associated to the user group. Click Save Changes. The User Group page appears with the selected users and the device groups that have been associated with the AIM user group.



8. Click Save Changes. The new user group appears in the User Groups table.



9. Repeat Steps 2 through 8 to create more user groups. For more information on the User Groups table, See “Associate Device Groups Table Element Descriptions” on page 103 and “User Group Table Elements Descriptions” on page 102.

User Group Page Description

Table 51 describes the User Group page columns.

Table 51: User Group Page Element Description

Element	Description	Privileges	Enabled/ Disabled	Results
Save Changes command button	Saves the user group.	AIM Admin Settings	Enabled if admin privileges	Error message is displayed if settings were not saved
Name field	Unique user group name	AIM Admin Settings	32 characters	Blank
User Table	Displays the names of existing AIM users from which you can select to be in the new user group	AIM Admin Settings	Enabled if admin privileges	Selected users will be associated with this User Group when you click Save Changes
Associated Device Groups table command button	Displays the Associate Device Groups page, from which existing device groups can be selected for association to this user group	AIM Admin Settings	Enabled if admin privileges	Displays page to set which device groups are associated
Associate Device Groups table	Lists the existing AIM device groups by name, organization, and devices that are included	Not allowed to modify	Enabled if admin privileges	N/A

User Group Table Elements Descriptions

Table 52 describes the User Group table elements.

Table 52: User Group Table Command Button Description

Button Name	Description	Privileges	Enabled/ Disabled	Results
Add New	Displays User Group page used to add a new AIM user group. When you first add a user group, the User Group table is empty and the Associate Device Group table does not appear.	AIM Admin Settings	Enabled if admin privileges	Displays User Groups page
Delete	Deletes a selected user group	AIM Admin Settings	Enabled if admin privileges	Deletes user group from User Group table and the database

Table 53 describes the User Group table columns.

Table 53: User Group Table Column Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	Unique name of user group. Click user group name link to view the User Group page so you can modify the user group name, users, and associated device groups.	Not allowed to modify	N/A	N/A
Users	List of existing users selected to be in user group.	Not allowed to modify	N/A	N/A
Device Groups	List of existing device groups that have been associated with the user group	Not allowed to modify	N/A	N/A

Associate Device Groups Table Element Descriptions

Table 54 describes the Associate Device Groups table command button.

Table 54: Associated Device Groups Table Command Button Description

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Saves modifications to a user group in the Associate Device Groups table	AIM Admin Settings	Enabled if admin privileges	Device groups selected are associated with the user group, then the User Group Detail page appears.

Table 55 describes the Associate Device Groups table columns.

Table 55: Associated Device Groups Table Columns Descriptions

Name	Description	Privileges	Enabled/ Disabled	Results
Name	Name of the device groups available to associate	Not allowed to modify	N/A	N/A
Organization	Name of the organization with which the device group is associated	Not allowed to modify	N/A	N/A
Device	Lists the devices that are included in the device group	Not allowed to modify	N/A	N/A

Deleting a User Group

To delete a User Group, follow these steps.

1. Click Settings > User Groups. The User Group page appears. The User Group table is empty until you add a new user group.

2. Select the user group(s) that you want to delete.

3. Click Delete. This action removes the AIM user group with all associations from the database.

Part 4

Using Advanced Insight Manager

Chapter 12

Using My AIM Home

This chapter describes the information that you view on My AIM Home page to manage incidents, intelligence messages, and reaction policy information that is specifically assigned to a user.

Incidents are problem events that have occurred on the network and are owned and flagged to you, the current user. You can open cases to solve these incidents. The incidents shown in My AIM Home are a subset of the ones displayed in Incident Manager.

Intelligence messages are alerts and or information entries owned and flagged to you that are sent from Juniper Support Systems (JSS), after analysis of incident information, to help you to proactively manage risks on your network. These intelligence messages are a subset of those displayed in the Intelligence Update tab of Intelligence Manager.

Reactive Policies are actions to be taken in response to any changes or updates detected by the AIM application. Only those reaction policies created by you are displayed in My AIM Home.

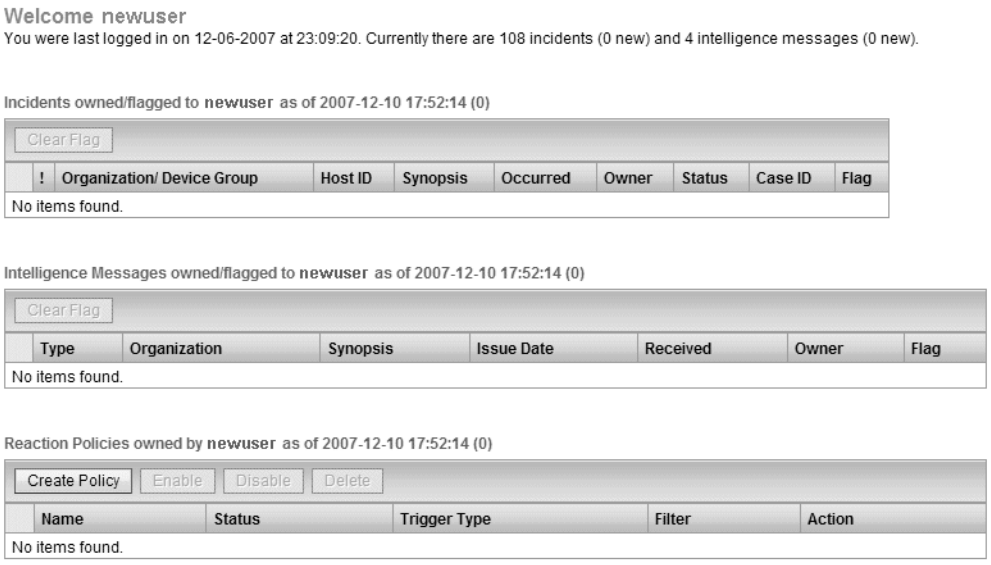
When you first log in to the AIM application, you see the My AIM Home page. The My AIM Home is populated only if the AIM application has been set up to connect to the archive location of a device, and setup to connect to JSS for incident case management and intelligence information, see “Configuring AIM General Settings” on page 49. On the populated My AIM Home page, you can view all the relevant information you need to know about the incident and intelligence information that have been collected for a device assigned to the current user, and the reaction policies that define what actions to take when certain incidents are received.

This chapter includes the following sections:

Viewing My AIM Home

When you first log into the AIM application, you see the My AIM Home page. At a glance, you can view all relevant information you need to know about the incidents and intelligence information that has been collected, and reaction policies that define what actions to take about certain incidents.

The tables on the My AIM Home page are empty until you populate them with the information with which you need to work. See "Populating the Incidents Table" on page 108, "Populating the Intelligence Messages Table" on page 108, and "Populating the Reaction Policies Table" on page 109.



Populating the Incidents Table

The Incidents table is blank until an incident is owned by or flagged to a user.

- To own an incident, see "Assigning an Incident Owner" on page 115.
- To flag an incident to a user, see "Flagging an Incident To a User" on page 114.

Populating the Intelligence Messages Table

The intelligence messages table is blank until a user is owned or flagged an incident.

- To own an incident, see "Assigning an Intelligence Message Owner" on page 120.
- To flag an incident to a user, see "Flagging Intelligence Messages To Users" on page 122.

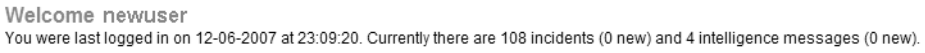
Populating the Reaction Policies Table

The Reaction Policies table is blank until you create a reaction policy.

To create a reaction policy, see “Creating a Reaction Policy” on page 125.

Using the Welcome Notification Area

The My AIM Home Welcome notification area displays the state of the AIM application when you log in.



The Welcome notification area displays the following information:

- Your AIM login user name
- Time when you last logged in
- Number of incidents currently active in the system
- Number of incidents detected since you last logged in
- Number of intelligence messages active in the system
- Number of intelligence messages detected since the user’s last log on.

Using AIM Tables

This section describes the standard actions in AIM tables, see “Using the Table Selection, Sort, and Display Icons” on page 109. It also describes the standard navigation actions in each AIM table, see “Navigating in AIM Tables” on page 110).

Using the Table Selection, Sort, and Display Icons

Table 56 describes the icons that represent actions used to manipulate data in AIM tables. These icons are located along the top and bottom of each table.

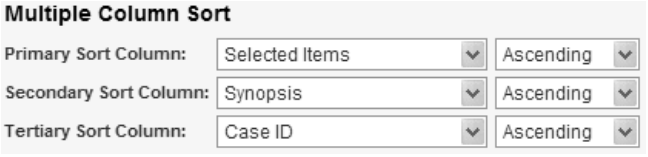
Table 56: AIM Table Data Selection, Sort, and Display Icons

Icon	Name	Description
	Select All	Selects all rows currently displayed in a table.
	Deselect All	Deselects all rows currently displayed in a table.

Icon	Name	Description
	Multiple Column Sort	Displays the Multiple Column Sort area at the top of a table. Sorts a table according to the primary, secondary, and tertiary columns selected in ascending or descending order. (See “Using the Multiple Column Sort Area” on page 110.)
	Clear All Sorts	Removes all sorts that have been performed on table data.
	Sort Data to One Page	Displays all table data on one page.
	Sort Data on Multiple Pages	Displays all table data on multiple pages

Using the Multiple Column Sort Area

The AIM table Multiple Column Sort area appears when you click the Multiple Column Sort icon in a table (see Table 56). You can sort table data according to the primary, secondary, and tertiary sort columns selected in ascending or descending order. The Selected Items option sorts only selected rows in the table.



Navigating in AIM Tables

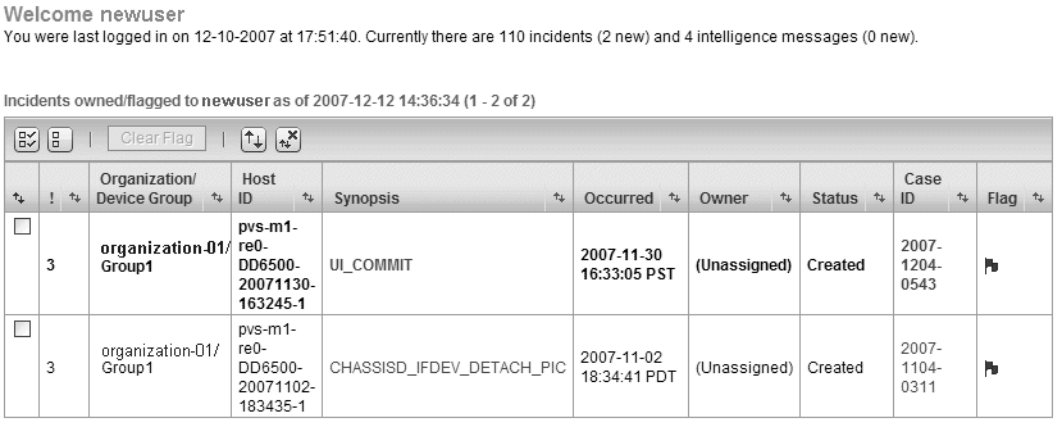
The navigation area at the bottom of each AIM table lets you move quickly through data to what you want to see.

From left to right in the table navigation area, you can:

- Go to the first page
- Go back to the previous page
- Go to a specific page typed in the Page text box, then click Go
- View the total number of pages in table
- Go forward to the next page
- Go to the last page

Using the Incidents Table

The Incidents table displays a list of the incidents, that have been collected from in archive location, that are specifically owned by or flagged to the user. To own an incident, see “Assigning an Incident Owner” on page 115; to flag an incident to a user, see “Flagging an Incident To a User” on page 114.



The Incidents table columns include the information and functionality described in Table 57.

Table 57: My AIM Home Incident Table Column Descriptions

Column	Description	Range/Length	Default
!	Priority of the incident.	1—4	Set by the JUNOS device; may be overridden by a Reaction Policy.
Organization/Device Group	Name of the AIM organization and the associated device group name.		
Host ID	Unique identifier representing the specific incident occurrence.	N/A	Set by the JUNOS system or AIM application if there are multiple PRBs.
Synopsis	Textual description of the incident. This field is a link used to navigate to the detail screen of the selected incident. For more information about viewing the selected incident, see “Viewing Incident Detail” on page 112.	N/A	Set by the JUNOS system
Occurred	Time that the JUNOS device detected the incident	Date, time, and time zone in the following format: yyyy-mm-dd 08:22:39 time zone	N/A

Column	Description	Range/Length	Default
Owner	User currently assigned ownership for this incident, as well as the owner's status regarding the incident in the following format: Format: owner (status) See "Assigning an Incident Owner" on page 115 for how to assign an owner to an incident	Owner—Any valid user AIM application software user Status—Assigned, In progress, or Completed	Unassigned
Status	Status of this incident with regards to the AIM Application system. It relates to the interactions between the AIM application and JTAC case status. For more information about changing the incident status, see "Changing Incident Owner Status" on page 116	Initial, Submitted, Created, or Updated	Initial
Case ID	Case ID assigned by Juniper Case Management. This field is a hot link used to navigate into Juniper Case Management. For more information about Juniper Case Management, see "Submitting a Case" on page 113.	N/A	Empty until the case is created.
Flag	Indicates if this entry has been flagged to the user for inspection. For more information about flagging an incident to a user, see"Flagging an Incident To a User" on page 114	N/A	Empty until the case is created.

Viewing Incident Detail

For each incident listed in the My AIM Home Incident table, you can view more detailed information needed for analysis and resolution.

To view an incident detail page, do the following:

- In the Incident table on the My AIM Home page, click the link in the incident Synopsis column. You can also click the incident synopsis from Incident Manager. The Incident Details page appears.

Submitting a Case

From the Incident Detail page, you can easily submit a request for an incident case ID from Juniper Support Systems (JSS) for resolution. See “Understanding AIM Ownership” on page 90 and “AIM User Privileges” on page 91.

To submit a case ID request to JSS for an incident, follow these steps:

1. On the Incident Detail page, click Submit Case.

   You see the following message:

   Successfully submitted case to Juniper: Create Case returned transaction ID

   Thereafter, the case ID appears in the incident Case ID column.

Creating a Reaction Policy

An AIM Reaction Policy lets a user specify the response that AIM should take when an incident or intelligence message is received. You can specify the following when creating a reaction policy:

- Trigger types that cause AIM to react to an incident
- Filters to specifically determine which incidents or intelligence messages to which you want AIM to react to
- What actions to take once the specified incident or intelligence message is received.

For more detailed information about creating a reaction policy, see “Creating a Reaction Policy” on page 125.

Flagging an Incident To a User

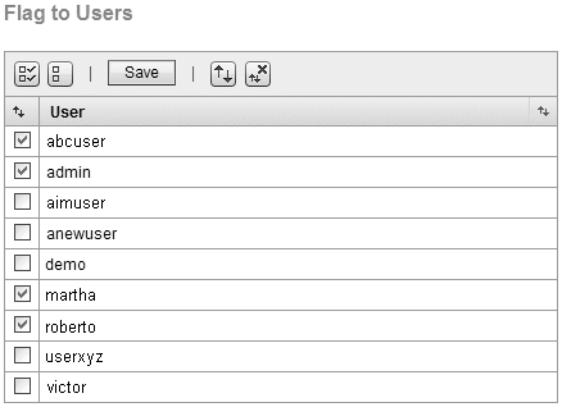
You can flag an incident to a user. Flagging or owning an incident, displays that incident in My AIM Home. You can also flag an incident to a user from the Incident Manager user interface (see _____).

Incidents that are bold indicate that they have been flagged to you since the last time you logged into AIM.

To flag an incident to a user from My AIM Home, follow these steps:

1. From My AIM Home, click the incident synopsis link. The Incident Detail page appears.

2. On the Incident Detail page, click Flag to Users. The Flag To Users page appears.



3. On the Flag to Users page, select the user(s) to which you want to flag the incident.

4. Click Save. A flag appears in the incident Flag column in My AIM Home.

Viewing a Juniper Message Bundle

The Juniper Message Bundle (JMB) contains the information that Juniper Support Systems (JSS) needs to analyze and resolve cases and to prevent the incident from reoccurring. For more information about the JMB, see “Juniper Message Bundle Contents” on page 37.

To view an incident’s Juniper message bundle, follow these steps:

1. From My AIM Home or Incident Manager, click the incident synopsis link. The Incident detail page appears.

2. On the Incident detail page, click View JMB. The JMB detail page appears.

View JMB: pvs-m1-re0_PvS_prob_20071201_003445.xml

(Information as received by Router)

MANIFEST

Host Event ID:	pvs-m1-re0-DD6500-20071130-163245-1
Service Type:	event
Event Time:	2007-11-30 16:33:05 PST
Problem Class:	support
Problem Synopsis:	UI_COMMIT
Problem Description:	Error on commit.
Problem Severity:	3
Problem Priority:	3
Core File Path:	
Serial Number:	

Router Information	
Product Name:	m7i
Host Name:	pvs-m1-re0
OS Platform:	junos

Master Routing Engine	
Name:	Routing Engine 0
Mastership State:	Online Master

Assigning an Incident Owner

You can own Incidents so that you can have responsibility for following the incident resolution process to completion. See “Understanding AIM Ownership” on page 90. See also “AIM User Privileges” on page 91.

To own an incident, follow these steps:

1. From My AIM Home or Incident Manager, click the incident synopsis link. The Incident detail page appears.

2. On the Incident detail page, select an AIM user from the Owner drop-down list.

3. Click Save Changes.

Changing Incident Owner Status

The incident owner can specify the incident status, that is either:

- Unassigned—Incident is not owned by an AIM user
- Assigned—Incident is owned by an AIM user
- In Progress—Incident case ID has been assigned and resolution is in progress.
- Completed—Incident has been resolved

To specify incident owner status, follow these steps:

1. From My AIM Home or Incident Manager, click the incident synopsis link. The Incident detail page appears.

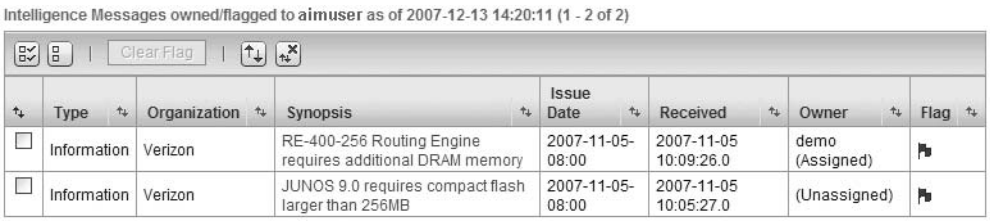
2. On the Incident detail page, select the incident status from the Status drop-down list.

3. Click Save Changes.

Using the Intelligence Messages Table

The Intelligence Messages table displays the three types of intelligence information for risk analysis, mitigation, and proactive recommendations:

- Information from the network
- Information from the Juniper Networks knowledge base
- Information from the field



The Intelligence Messages table columns include the information and functionality described in Table 58.

Intelligence Messages Table Description

Table 58 describes the Intelligence Messages table columns.

Table 58: My AIM Home Intelligence Messages Table Column Descriptions

Column	Description	Range/Length	Default
Type	Type of intelligence message received from Juniper Support Systems (JSS).	Alert or Information	N/A
Synopsis	Textual description of the intelligence message. This field is a link used to navigate to the intelligence message detail page.	N/A	Set by the JSS
Issue Date	Time that the intelligence message was issued from JSS.	Date, time, and time zone in the following format: yyyy-mm-dd 08:22:39 time zone	N/A
Received	Time that the intelligence message was received by the AIM application.	Date, time, and time zone in the following format: yyyy-mm-dd 08:22:39 time zone	N/A
Owner	User currently assigned ownership for this intelligence message, as well as the owner's status regarding the intelligence message resolution in the following format: Format: owner (status) See "Assigning an Incident Owner" on page 115 for how to assign owner to an intelligence message.	Owner—Any valid user login for the AIM application Status—Assigned, In progress, or Completed	Unassigned
Flag	Indicates if this entry has been flagged to the user for inspection. See "Flagging Intelligence Messages To Users" on page 122 for how to flag an intelligence message to a user.	N/A	N/A

Viewing Intelligence Message Details

To view intelligence message details, do the following:

- In the Intelligence Message Synopsis column on the My AIM Home page, click the incident synopsis link. The Information Entry page appears.

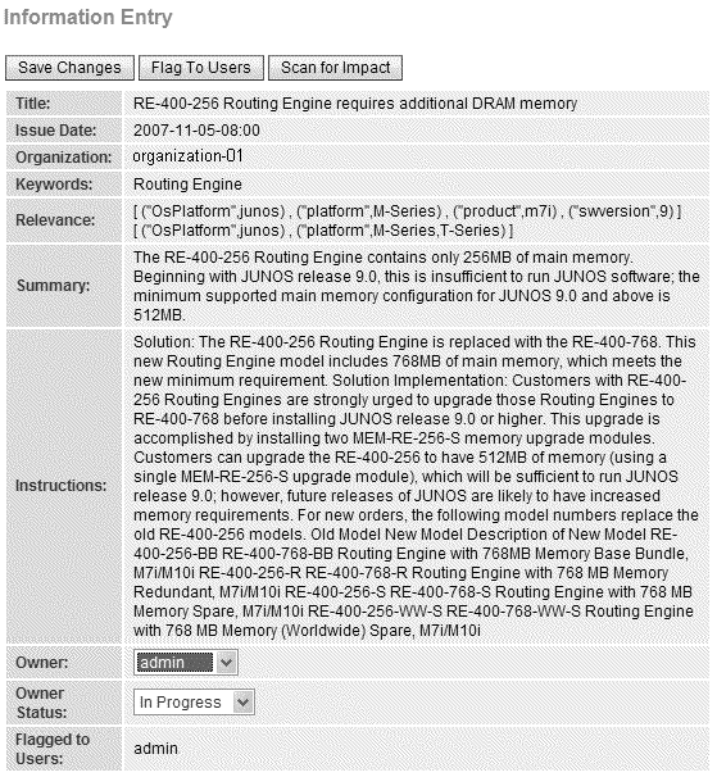


Table 61 describes the fields on the Information Entry page.

Information Entry Table Description

Table 61 describes the Information Entry table fields.

Table 59: Information Entry Table Field Descriptions

Column	Description	Range/Length	Default
Title	Textual title of this intelligence message	N/A	N/A
Issue Date	Time that the Intelligence Message was issued	Date and time	N/A
Keywords (Information Entry)	List of words specified by JTAC engineer that describe the key components this Information Entry is regarding.	N/A	N/A
Relevance (Information Entry)	Set of one or more relevance entries. Each entry contains some combination of one or more of each of the following: serial numbers, platforms, hardware versions, software versions, general comments.	N/A	N/A
Source (Alert)	Indicates the source of the alert.	N/A	N/A

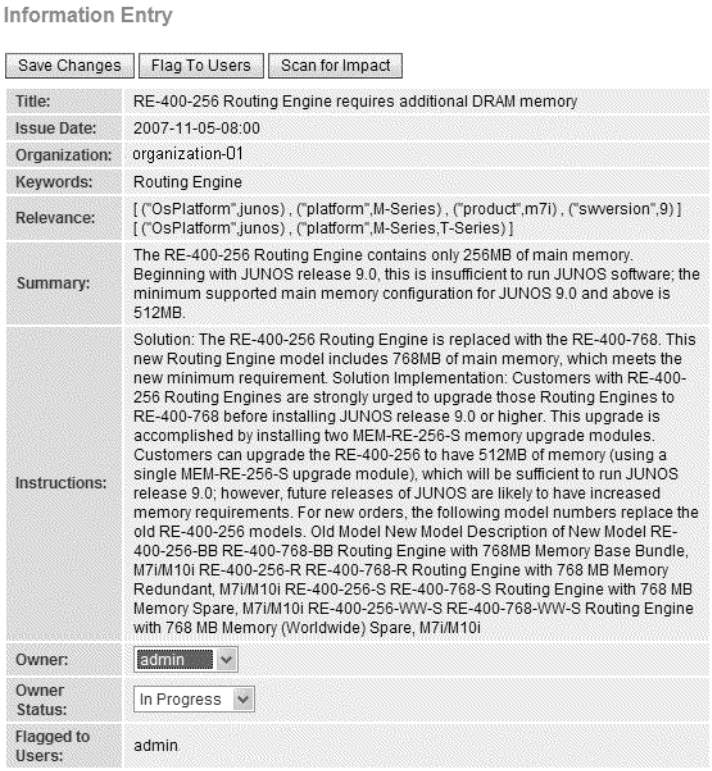
Column	Description	Range/Length	Default
Products Affected (Alert)	Specifies one or more of the products affected by the alert.	N/A	N/A
Platforms Affected (Alert)	Specifies one or more of the platforms affected by the alert.	N/A	N/A
Summary	Textual summary of intelligence message.	N/A	N/A
Instructions	Instructions specified by the JTAC engineer.	N/A	N/A
Alert Link (Alert)	This field is a link and can be used to navigate into the Juniper Support web page for this specific alert.	N/A	N/A
Owner	User that has currently been assigned ownership for this intelligence message	Any valid user login for AIM	Blank
Owner Status	Owner's status regarding the intelligence message	Unassigned, Assigned, In Progress, Completed	Unassigned
Flagged to Users	List of users that this intelligence message has been flagged to	N/A	Blank

Assigning an Intelligence Message Owner

You can own intelligence messages so you have responsibility for implementing them to prevent incidents from occurring in the future. See “Understanding AIM Ownership” on page 90. See also “AIM User Privileges” on page 91.

To assign ownership of an intelligence message, follow these steps:

1. From My AIM Home or Intelligence Manager, click the intelligence message synopsis link. the Information Entry page appears.



Information Entry

Save Changes | Flag To Users | Scan for Impact

Title:	RE-400-256 Routing Engine requires additional DRAM memory
Issue Date:	2007-11-05-08:00
Organization:	organization-01
Keywords:	Routing Engine
Relevance:	[("OsPlatform",junos) , ("platform",M-Series) , ("product",m7i) , ("swversion",9)] [("OsPlatform",junos) , ("platform",M-Series,T-Series)]
Summary:	The RE-400-256 Routing Engine contains only 256MB of main memory. Beginning with JUNOS release 9.0, this is insufficient to run JUNOS software; the minimum supported main memory configuration for JUNOS 9.0 and above is 512MB.
Instructions:	Solution: The RE-400-256 Routing Engine is replaced with the RE-400-768. This new Routing Engine model includes 768MB of main memory, which meets the new minimum requirement. Solution Implementation: Customers with RE-400-256 Routing Engines are strongly urged to upgrade those Routing Engines to RE-400-768 before installing JUNOS release 9.0 or higher. This upgrade is accomplished by installing two MEM-RE-256-S memory upgrade modules. Customers can upgrade the RE-400-256 to have 512MB of memory (using a single MEM-RE-256-S upgrade module), which will be sufficient to run JUNOS release 9.0; however, future releases of JUNOS are likely to have increased memory requirements. For new orders, the following model numbers replace the old RE-400-256 models. Old Model New Model Description of New Model RE-400-256-BB RE-400-768-BB Routing Engine with 768MB Memory Base Bundle, M7i/M10i RE-400-256-R RE-400-768-R Routing Engine with 768 MB Memory Redundant, M7i/M10i RE-400-256-S RE-400-768-S Routing Engine with 768 MB Memory Spare, M7i/M10i RE-400-256-WW-S RE-400-768-WW-S Routing Engine with 768 MB Memory (Worldwide) Spare, M7i/M10i
Owner:	admin
Owner Status:	In Progress
Flagged to Users:	admin

2. On the Information Entry page, select an AIM user from the Owner drop-down list.

3. Click Save Changes.

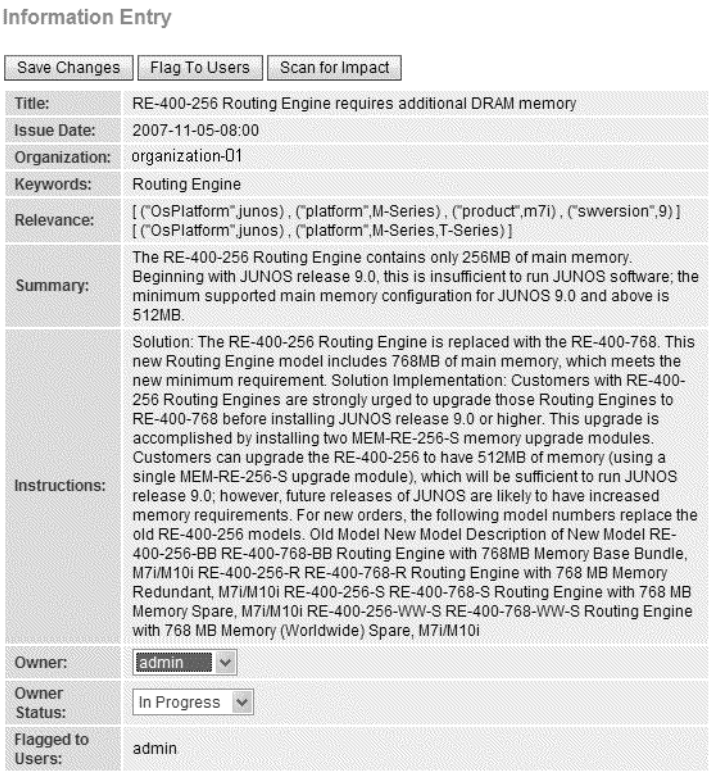
Changing Intelligence Message Owner Status

The intelligence message owner can specify the status, that is either:

- Unassigned—intelligence message is not owned by an AIM user
- Assigned—intelligence message is owned by an AIM user
- In Progress—intelligence message case ID has been assigned and resolution is in progress.
- Completed—intelligence message has been resolved

To specify intelligence message status, follow these steps:

1. From My AIM Home or Incident Manager, click the intelligence message synopsis link. The Information Entry page appears.



2. On the Incident detail page, select the incident status from the Status drop-down list.

3. Click Save Changes.

Flagging Intelligence Messages To Users

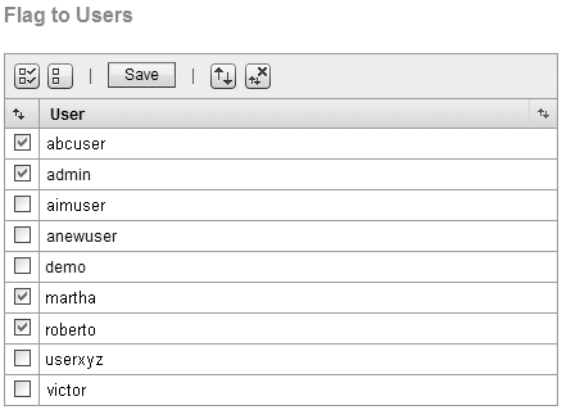
You can flag an intelligence message to a user. Flagging or owning an intelligence message, displays that message in My AIM Home. You can also flag an incident to a user from the Incident Manager user interface (see “Flagging an Intelligence Update To a User” on page 144).

Intelligence Messages that are bold indicate that they have been flagged to you since the last time you logged into AIM.

To flag an intelligence message to a user from My AIM Home, follow these steps:

1. From My AIM Home, click the intelligence message synopsis link. The Incident Detail page appears.

2. On the Incident Detail page, click Flag to Users. The Flag To Users page appears.



3. On the Flag to Users page, select the user(s) to which you want to flag the incident.

4. Click Save. A flag appears in the incident Flag column in My AIM Home.

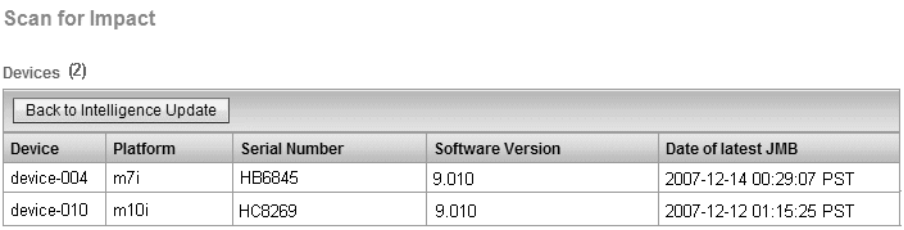
Scanning Intelligence Messages for Impact

The Scan for Impact command lets AIM search for any device for which an intelligence message applies and displays it in the Scan for Impact table. The Scan for Impact table also displays the date of the last intelligence Juniper Message Bundle (JMB) received.

To scan an intelligence message for impact, follow these steps:

1. From My AIM Home, click the intelligence message synopsis link. The Incident Detail page appears.

2. On the Incident Detail page, click Scan for Impact. The Scan for Impact page appears.



   The devices are listed in the Scan for Impact table alphabetically.

3. Click Back to Intelligence Update.

   Table 60 describes the columns in the Scan for Impact table.

Scan for Impact Table Description

Table 60 describes the columns in the Scan for Impact table.

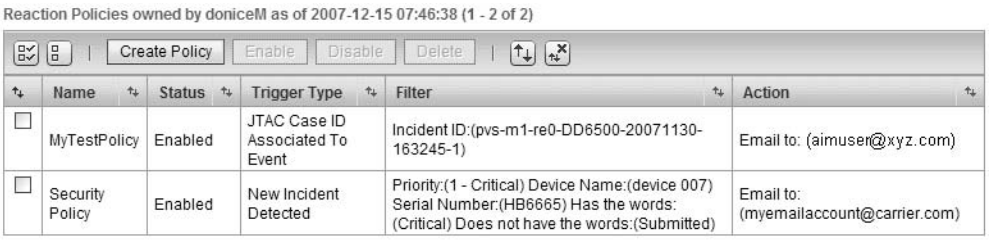
Table 60: Scan for Impact Table Column Descriptions

Column	Description	Range/Length	Default
Device	Name of device that the intelligence update might impact	N/A	N/A
Platform	Platform of device	N/A	N/A
Serial Number	Serial number of device	N/A	N/A
Software Version	Software version running on the device	N/A	N/A
Date of Latest JMB	Date and time that the last JMB was received that applies to the intelligence message	N/A	N/A

Using the Reaction Policies Table

The Reaction Policies table provides at a glance look at actions to take in response to any changes or updates detected by the AIM application:

- The type of trigger that has to happen for the policy to be applied.
- The filter that must be passed for the policy to be applied
- The actions to take if the policy is triggered and the filter is passed



The Reaction Policies table columns include the information and functionality described in Table 61.

Reaction Policies Table Description

Table 61 describes the columns in the Reaction Policies table.

Table 61: Reaction Policies Table Column Descriptions

Column	Description	Range/Length	Default
Name	A unique policy name within all the policies owned by the same user.	32 characters	N/A
Owner	user who created the reaction policy.	N/A	N/A
Status	Whether the policy is running or not.	Enabled or Disabled	N/A

Column	Description	Range/Length	Default
Trigger Type	The type of trigger that has to happen for this policy to be applied.	New Event Detected, Event Reported to Juniper, JTAC Case ID Assigned, JTAC Case Updated, or New Intelligence Update Received	N/A
Filter	Specifies the filter that must be passed for this policy to be applied.	See <_____ for filter definitions	N/A
Action	Indicates the actions that will be taken if this policy is triggered and the filter is passed.	See _____ for action definitions	N/A

Creating a Reaction Policy

Reaction policies let you specify what incidents you want AIM to reaction on and what action you want taken. See also “AIM User Privileges” on page 91.

To create a reaction policy, follow these steps:

1. From My AIM Home Reaction Policies table, click Create Policy. You can also create a Reaction Policy by clicking Reaction Policies in the AIM navigation pane. The Reaction Policy wizard appears.

2. Type a reaction policy name, then select a trigger. Table ____ describes the trigger options.

3. Click Next Step. The Create Reaction Policy Set Filter page appears.

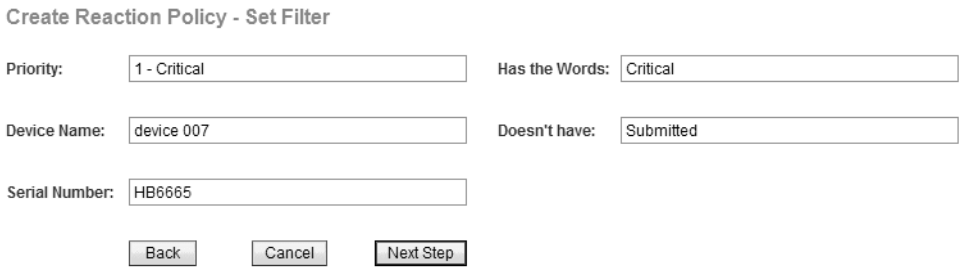
   Table 61 describes the fields on the Create Reaction Policy Set Filter page.

Reaction Policy Name and Trigger Description

Table 61 describes the Reaction Policy Name field and Trigger options.

Table 62: Reaction Policy Name and Trigger Descriptions

Column	Description	Range/Length	Default
Name field	Name of policy, which must be unique within all the policies owned by the same user.	32 characters	N/A
Trigger Type options	■ Specifies the type of trigger that has to happen for this policy to be applied. ■ New Intelligence Update Received trigger is only available if create policy was initiated from the Reaction Policies page ■ New Event Detected trigger is NOT available if any incidents were specified when create policy was initiated	■ New Event Detected ■ Event Reported to Juniper ■ JTAC Case ID Assigned, ■ JTAC Case Updated ■ New Intelligence Update Received	N/A



4. Type the required information in the Create Reaction Policy - Set Filter page. For field descriptions, see Table 63.

Reaction Policy Set Filter Description

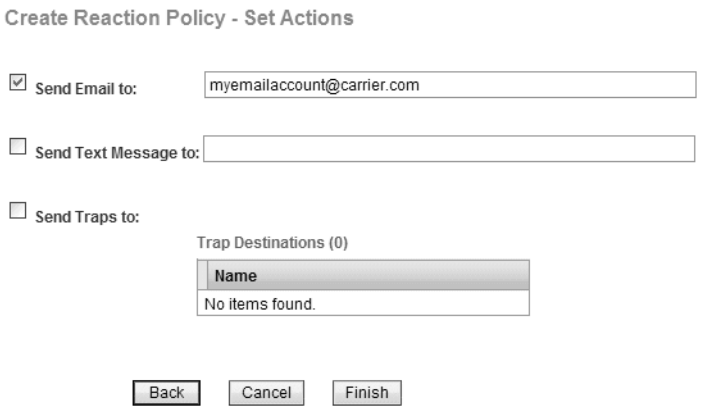
Table 63 describes the Reaction Policy Set Filter page description.

Table 63: Create Reaction Policy Set Filter Field Descriptions

Column	Description	Range/Length	Default
Priority	Matches the priority of incident of the incident ■ 1—Critical ■ 2—High ■ 3—Medium ■ 4—Low	256 characters	Blank
Has the words	For all trigger types: Matches the specified words against any of the fields in the incident or the intelligence update	256 characters	Blank
Device Name	For incident specific trigger types: Matches the name of the device the incident occurred on.	256 characters	Blank

Column	Description	Range/Length	Default
Doesn't have	For all trigger types: Makes sure the specified words are not in any of the fields of the incident or the intelligence update	256 characters	Blank
Serial Number	For all trigger types: Matches serial number of the device the incident occurred on, OR matches the serial number specified in the relevance of the intelligence message	256 characters	Blank

5. Click Next Step. The Create Reaction Policy Set Actions page appears.



6. Select the action you want AIM to take when the reaction policy criteria is met. See Table 64.

Reaction Policy Set Actions Description

Table 64 describes the options on the Reaction Policies Set Actions page.

Table 64: Reaction Policy Set Actions Page Description

Column	Description	Range/Length	Default
Send Email to	List of email addresses that will be sent an email message if the policy is triggered and passes the specified filter.	65535 characters	Send Email to
Send Text Message to	List of email addresses that will be sent a text message if the policy is triggered and passes the specified filter.	65535 characters	Send Text Message to
Send Traps to	List of trap destinations that will be sent AIM SNMP traps if the policy is triggered and passes the specified filter. Trap destinations in the table are those created in Settings > Trap Destinations.	N/A	N/A

7. Click Finish. The Reaction Policies table appears.

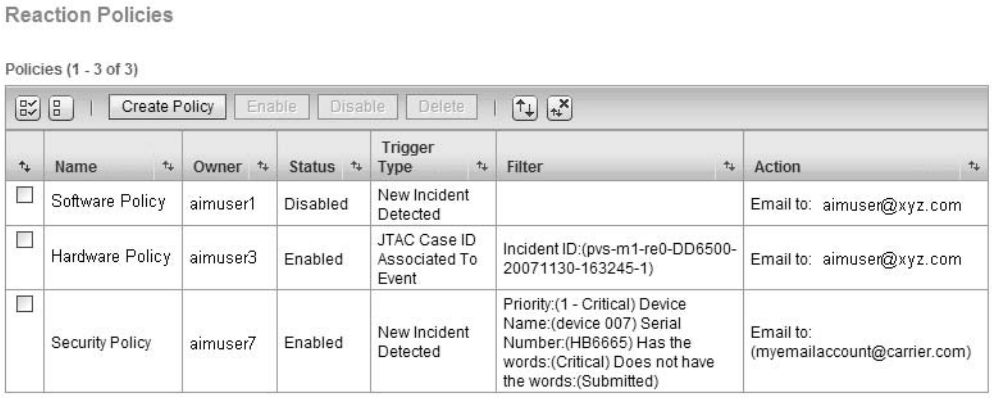


Table 65 describes the Reaction Policies table.

Reaction Policies Table Description

Table 65 describes the Reaction Policies table command buttons.

Table 65: Reaction Policy Table Command Button Descriptions

Element Name	Description	Privileges	Enabled/ Disabled	Results
Create Policy	Displays the Reaction Policies wizard for you to perform all the steps to create reaction policy.	AIM Admin	Enabled	
Enable	Activates the selected reaction policies).	AIM Admin	Enabled when you select a reaction policy	
Disable	Deactivates a selected reaction policy.	AIM Admin	Enabled when you select a reaction policy	
Delete	Removes a selected Reaction Policy	AIM Admin		

Table 66 describes the columns in the Reaction Policies table.

Table 66: Reaction Policies Table Column Descriptions

Column	Description	Range/Length	Default
Name	Name of policy that must be unique within all policies owned by the same user.	32	N/A
Owner	User who created the reaction policy	N/A	N/A
Status	Indicates whether the reaction policy is running or not	Enabled or Disabled	N/A

Column	Description	Range/Length	Default
Trigger	Specifies the type of trigger that has to occur for the reaction policy to be applied.	■ New Event Detected ■ Event Reported to Juniper ■ JTAC Case ID Assigned ■ JTAC Case Updated ■ New Intelligence Update Received	N/A
Filter	Specifies the filter that must be passed for this reaction policy is triggered and the filter is passed.	See Table 64.	N/A
Action	Specifies the action taken if this reaction policy is triggered and the filter has passed.		N/A

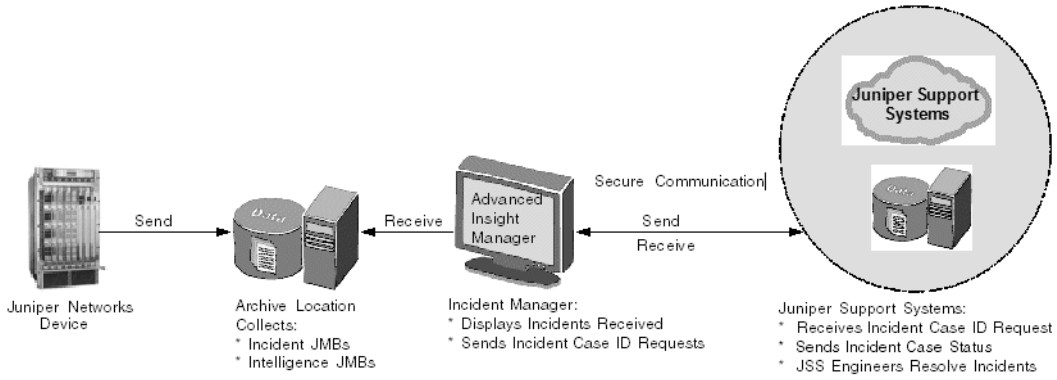
Chapter 13

Using AIM Incident Manager

The Incident Manager provides a view of all incidents received by Advanced Insight Manager. Incidents are displayed alphabetically by organization name and device group.

Figure ___ shows the data flow through which AIM receives incident JMBs and manages them through successful case resolution.

Figure 14: Incident Manager Data Flow Diagram



Juniper Networks devices, configured with specialized AI-Scripts, periodically send incident and intelligence Juniper Message Bundles (JMBs) to a configured archive location. AIM connects to the archive location and periodically receives the incident and intelligence JMBs. Incident Manager displays all of the incident JMBs received. The incident owner sends an incident case ID request to JSS. JSS sends a case ID and opens a case for Juniper engineers to work on a resolution and to send case status back to Intelligence Manager.

To use Incident Manager, you must have AIM admin and AIM ownership privileges. You must also have the AIS Base (Incident-Driven Online Service subscription.

From Incident Manager, you can:

- View an incident detail
- View incident owner
- View incident status

- View case ID
- View whether an incident has been flagged to a user. Clear Flag—Removes the flag from any of the selected Incidents.
- View whether an incident has been submitted to Juniper Support Systems (JSS) for a case to be opened to receive a case ID. Submit Case—submits the selected Incident to JSS so that a case will be created. Submitting a case is only valid if only one incident is selected and if that incident has not already been submitted to the Juniper Homebase.
- Create Policy—Initiates creation of a Reaction Policy. If any Incidents are selected, the policy created will be scoped to just those incidents specified. If no Incidents are selected, then the policy will be applied to all the Incidents in the system.
- Delete any selected Incidents

This chapter includes the following sections:

Viewing Incident Manager

You can select to display incidents by all AIM organizations or by ones that you have created. For more information about creating AIM organizations, see "Configuring AIM Organizations and Device Groups" on page 67.

Any incident displayed in bold in Incident Manager indicates that incident has been detected, assigned, or flagged to the user since the last time the user was logged into AIM.

To view the Incident Manager table, do the following:

- Click Incident Manager in the AIM navigation area. The Incident Manager table appears.

Incident Manager Table Element Descriptions

Table 67 describes the Incident Manager table command buttons.

Table 67: Incident Manager Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Submit Case	Submits the selected Incident to Juniper so that a JTAC case will be created. Note that this action is only valid if only one incident is selected and if that incident has not already been submitted to the Juniper Homebase.			
Create Policy	Initiates creation of a Reaction Policy. If any Incidents are selected, the policy created will be scoped to just those incidents specified. If no Incidents are selected, then the policy will be applied to all the Incidents in the system.			
Clear Flag	Removes the flag from any of the selected Incidents.			

Button Name	Description	Privileges	Enabled/ Disabled	Results
Delete	Removes any selected Incidents			
Organization drop-down list	Lets you select to view incidents for all organizations or by ones that you select that have been created in AIM.			

Table 68 describes the columns in the Incident Manager table.

Table 68: Incident Manager Table Column Descriptions

Column	Description	Range/Length	Default
!	Indicates the priority of the incident received	1-4	Set by the JUNOS device, may be overridden by a Reaction Policy
Host ID	Unique identifier representing the specific incident occurrence.	N/A	Set by the JUNOS system or JUNOScope application if multi-PRB
Platform	Indicates the platform of the device the incident occurred on.	N/A	Set by the JUNOS System
Synopsis	Textual description of the incident. This field is a link and can be used to navigate to the detail screen of the selected Incident. Figure 10 Incident Detail	N/A	Set by the JUNOS system
Occurred	Time that the JUNOS device detected the incident	Date and time	N/A
Owner	User that has currently been assigned ownership for this incident, as well as the owner's status regarding the incident Format: owner (status) See 2.5 Incident Detail for how to assign an owner to an incident	Owner—Any valid user login for AIM Status—assigned, in progress, completed	Unassigned
Status	The status of this incident with regards to AIM. It relates to the interactions between the AIM and the JSS case status.	Initial, Submitted, Created, Updated	Initial
Case ID	The case ID assigned by the Juniper Case Management system. This field is a link and can be used to navigate into the JSS Case Management application. Figure 11 JTAC Case ID - Link to Juniper Case Management	N/A	Empty until case created.
Flag	Indicates if this entry has been flagged to the user for inspection.	N/A	N/A

- For more information about submitting a case request, see “Submitting a Case Request” on page 135
- For more information about creating a reaction policy when an incident is received, see “Creating a Policy” on page 136

- For more information about clearing a flag to a user, see “Clearing a Flag” on page 136
- For more information about viewing incidents by AIM organizations, see “Viewing Incidents by Organization” on page 136
- For more information about viewing incident detail, see “Viewing Incident Detail” on page 137

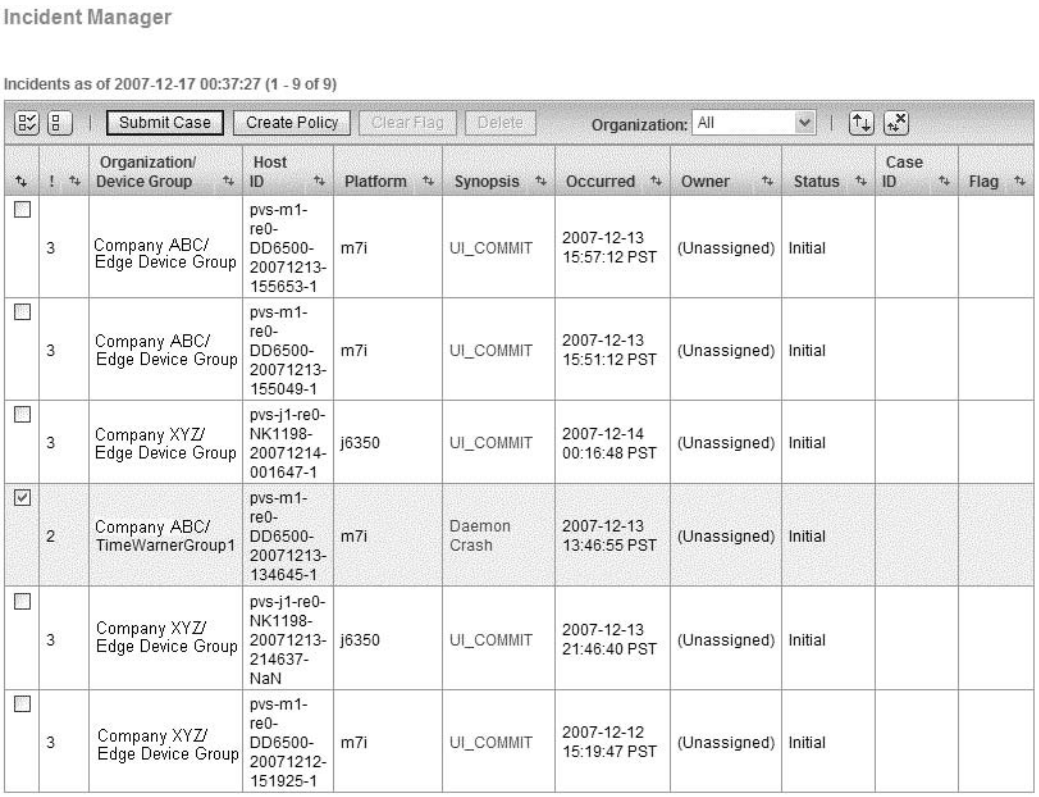
Submitting a Case Request

From the Incident Manager table, you can easily submit a case request from Juniper Support Systems (JSS). Once a case ID is assigned, the Case ID appears in the following places:

- My AIM Home, Incident Manager table
- Incident Manager table
- Incident Detail page

To submit a case ID, follow these steps:

1. From Incident Manager, select an incident for which you want to submit a case ID request. The Submit Case button is enabled.



Click Submit Case. You see the following message:

Successfully submitted case to Juniper: Create Case returned transaction ID

Thereafter, Incident Manager displays the status as Submitted. Then the status changes to Created and the case ID appears in the Case ID column. Finally, the incident is bold.

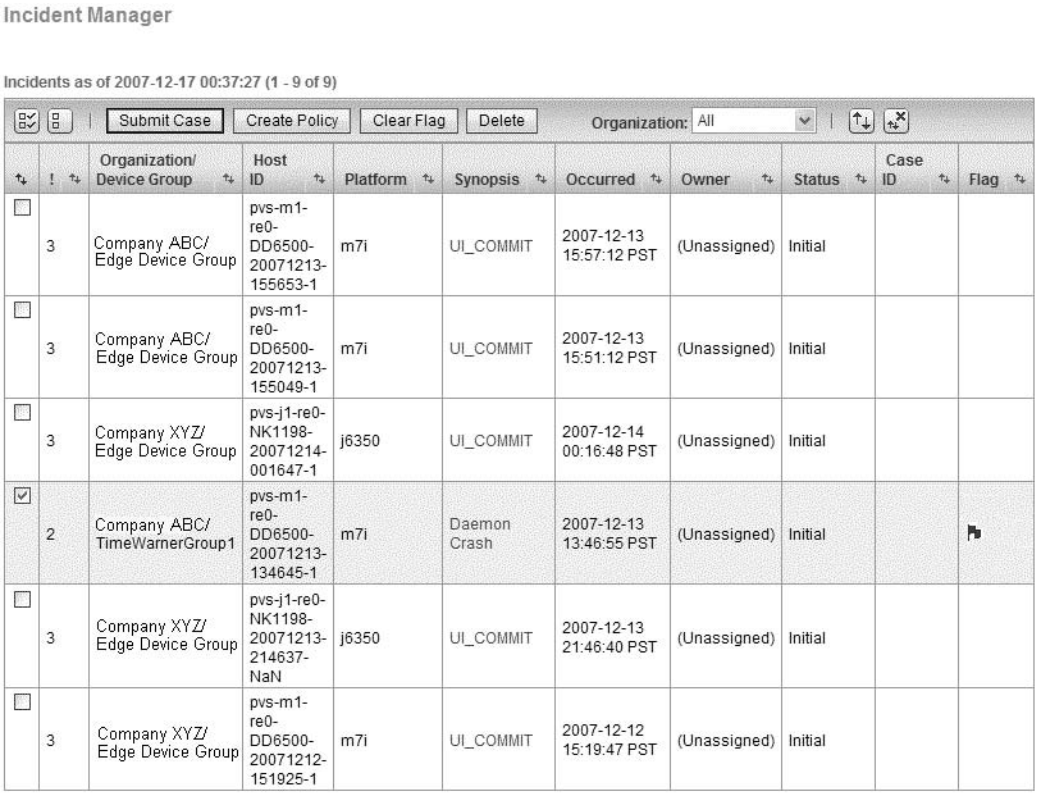
Creating a Policy

For more information about “Creating a Reaction Policy” on page 125.

Clearing a Flag

To clear and flag to a user, follow these steps:

1. In the Incident Manager table, select the incident with the flag that you want to delete. The Clear Flag button is enabled.



2. Click Clear Flag. The flag is removed, and that incident will no longer appear in the Incidents table in My AIM Home.

Viewing Incidents by Organization

You can view incidents by only the ones that have been collected for a specified AIM organization.

To view incidents by AIM organization, do the following:

- On the Incident Manager table, select the organization that you want from the Organization dro9p down list.

Incident Manager

Incidents as of 2007-12-17 00:37:27 (1 - 9 of 9)

Submit Case | Create Policy | Clear Flag | Delete | Organization: All

	!	Organization/ Device Group	Host ID	Platform	Synopsis	Occurred	Owner	Status	Case ID	Flag
☐	3	Company ABC/ Edge Device Group	pvs-m1-re0-DD6500-20071213-155653-1	m7i	UI_COMMIT	2007-12-13 15:57:12 PST	(Unassigned)	Initial		
☐	3	Company ABC/ Edge Device Group	pvs-m1-re0-DD6500-20071213-155049-1	m7i	UI_COMMIT	2007-12-13 15:51:12 PST	(Unassigned)	Initial		
☐	3	Company XYZ/ Edge Device Group	pvs-j1-re0-NK1198-20071214-001647-1	j6350	UI_COMMIT	2007-12-14 00:16:48 PST	(Unassigned)	Initial		
☐	2	Company XYZ/ Edge Device Group	pvs-m1-re0-DD6500-20071213-134645-1	m7i	Daemon Crash	2007-12-13 13:46:55 PST	(Unassigned)	Initial		
☐	3	Company XYZ/ Edge Device Group	pvs-j1-re0-NK1198-20071213-214637-NaN	j6350	UI_COMMIT	2007-12-13 21:46:40 PST	(Unassigned)	Initial		
☐	3	Company XYZ/ Edge Device Group	pvs-m1-re0-DD6500-20071212-151925-1	m7i	UI_COMMIT	2007-12-12 15:19:47 PST	(Unassigned)	Initial		

Viewing Incident Detail

For more information about viewing incident details, see"Viewing Incident Detail" on page 112.

Viewing Incident Juniper Message Bundle (JMB)

For more information about viewing and incident JMB, see "Viewing a Juniper Message Bundle" on page 114.

Assign an Incident Owner

For more information about assigning an incident owner, see "Assigning an Intelligence Message Owner" on page 120.

Change Incident Owner Status

For more information about changing an incident owner status, see "Changing Incident Owner Status" on page 116.

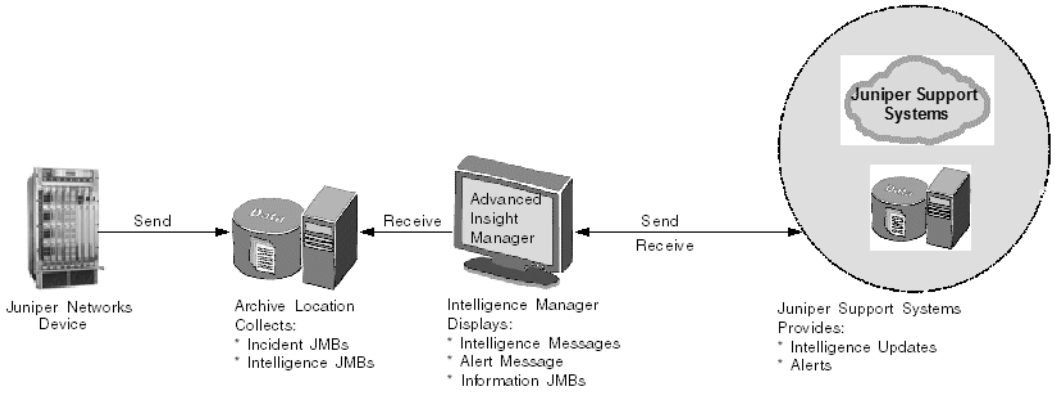
Chapter 14

Using AIM Intelligence Manager

Intelligence Manager consists of two user interfaces or tabs: Intelligence Updates and Information JMBs. Intelligence Updates provides a view of all intelligence update messages received by Advanced Insight Manager (AIM) from Juniper Support Systems (JSS). Information JMBs provides a view of all intelligence Juniper Message Bundles (JMBs) or messages received from Juniper Networks device archive locations.

Figure 15 shows the flow through which Intelligence Manager gets the intelligence information that is displayed on the Intelligence Updates and Information JMBs tabs.

Figure 15: Intelligence Manager Data Flow Diagram



Juniper Networks devices, configured with specialized AI-Scripts, periodically send incident and intelligence Juniper Message Bundles (JMBs) to a configured archive location. AIM connects to the archive location and periodically receives the incident and intelligence JMBs. Intelligence Manager displays the Intelligence JMBs. Juniper Support Systems receives the intelligence JMB information using a secure communication with AIM. JSS sends intelligence information updates and alerts to AIM Intelligence Manager, which is displayed on the Information Updates tab.

You must have AIM admin and AIM ownership privileges to use Intelligence Manager. You must also have the AIS Proactive (Intelligence-Driven Online Service subscription.

Intelligence Manager—Information JMBs let you do the following:

- View information JMB details

- View the information JMB contents

Any intelligence message or information JMB displayed in bold indicates that it was detected, assigned, or flagged to you since the last time the you logged into AIM.

Intelligence updates are displayed alphabetically by information type and organization. Information JMBs are displayed alphabetically by organization and device group.

You can select to display all intelligence messages and information JMBs by all AIM organizations or by ones that you have created. For more information about creating AIM organizations, see “Configuring AIM Organizations and Device Groups” on page 67.

This chapter includes the following sections:

Viewing Intelligence Updates

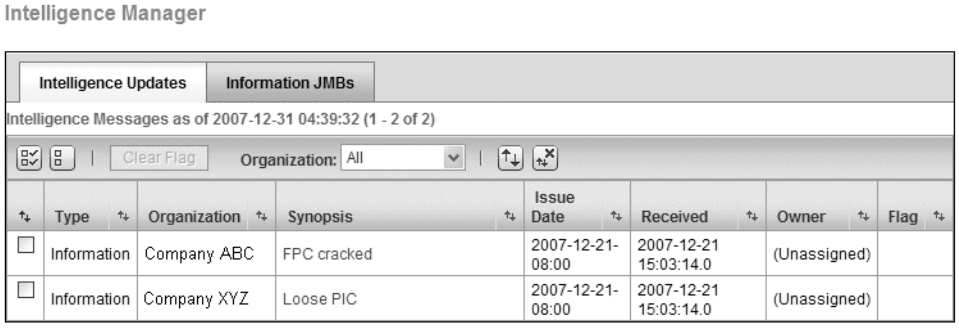
Intelligence Manager—Intelligence Updates displays all intelligence update messages received by Advanced Insight Manager (AIM) from Juniper Support Systems (JSS).

Intelligence Manager—Intelligence Updates lets you do the following:

- View all intelligence messages and alerts received from JSS
- View intelligence message or alert details
- Flag an intelligence message or alert to a user
- Clear an intelligence message or alert flag
- Scan all devices managed by AIM for intelligence message or alert impact
- Assign an intelligence message or alert owner
- Change owner status

To view Intelligence Updates, follow these steps:

- Click Intelligence Manager in the navigation area. The Intelligence Updates tab appears by default.



For more information on the Intelligence Updates tab description, see "Intelligence Updates Tab Description" on page 141.

Intelligence Updates Tab Description

Table 69 describes the Intelligence Updates tab elements.

Table 69: Intelligence Updates Tab Element Descriptions

Element Name	Description	Privileges	Enabled/ Disabled	Results
Clear Flag button	Removes the flag from any selected Intelligence Messages.	AIM Admin	Enabled when you select an intelligence update.	Clears flag
Organization drop-down list box	Lets you select the AIM organization (site) for which you want to display intelligence messages.	AIM Admin	Always enabled	Displays intelligence updates for selected organization.

Table 70 describes the columns in the Incident Manager table.

Table 70: Intelligence Updates Table Column Descriptions

Column	Description	Default
Type	Indicates what type of Intelligence Message received from Juniper: ■ Alerts—JTAC Technical Bulletins based on the alerts for which you have registered from JSS. ■ Information—Proactive messages from JSS to prevent incidents from occurring	N/A
Organization	Name of the customer site for which AIM is monitoring device archive locations	N/A
Synopsis	Provides a detailed description of the intelligence message on the Information Entry page when you click the link	Set by the JUNOS system

Column	Description	Default
Issue Date	Date and time that the Intelligence Message was issued	N/A
Received	Date and time that the Intelligence Message was received by AIM	N/A
Owner	User assigned ownership for this intelligence message, as well as the status of the intelligence message. An owner is any valid user login for AIM. Status option include: ■ Unassigned ■ Assigned ■ In progress ■ Completed Format: owner (status)	Unassigned
Flag	Indicates whether this intelligence update entry has been flagged for a user for inspection.	N/A

View Intelligence Update View by Organization

You can view intelligence updates by organizations that have been created (if the Multi-Site feature has been purchased). By default you view intelligence updates by all organizations.

To view intelligence updates by organizations, follow these steps:

1. Click Intelligence Manager in the navigation area. The Intelligence Updates tab appears by default.

2. In Intelligence Updates, select the organization you want from the Organization drop-down list box. Only the intelligence updates for the organization you select appear. The default is all organizations.

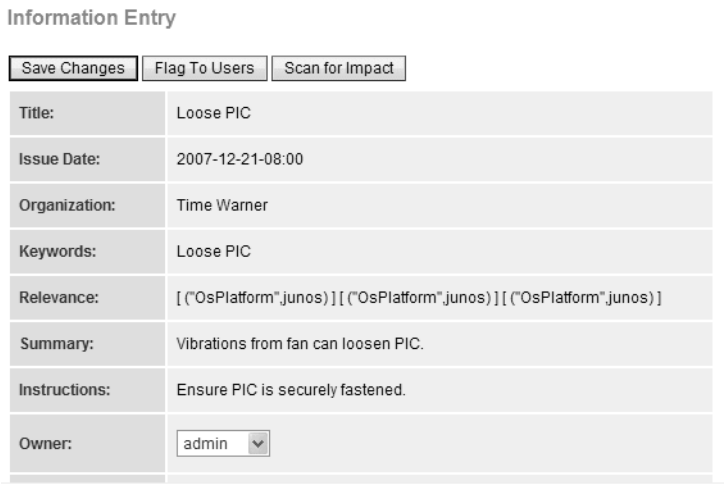
Viewing Intelligence Update Synopsis

You can view more detailed information about each information update.

To view more detailed information about an intelligence message, follow these steps:

1. Click Intelligence Manager in the navigation area. The Intelligence Updates tab appears by default.

2. In Intelligence Updates, click the link in the Synopsis column. The Information Entry page appears.



For more information about the Information Entry fields, see “Information Entry Page Field Descriptions” on page 143.

Information Entry Page Field Descriptions

Table 71 describes the fields in the Information Entry page.

Table 71: Information Entry Field Descriptions

Common Entry Fields	Description
Title	Title of this intelligence message
Issue Date	Date and time that the Intelligence Message was issued
Organization	The name of the customer site for which the intelligence message belongs
Summary	Textual summary of intelligence message.
Instructions	Instructions specified by the JTAC engineer.
Owner drop-down list box	Lists the available valid user login names for the AIM system. The field is blank by default.
Information Entry Fields	**Description**
Keywords	List of words specified by JTAC engineer that describe the key components this Information Entry is regarding.
Relevance	Set of one or more relevance entries. Each entry contains some combination of one or more of each of the following: serial numbers, platforms, hardware versions, software versions, general comments.
Alert Entry Fields	**Description**
Source	Indicates the source of the alert message
Products Affected	Specifies one or more of the products affected by the alert message

Common Entry Fields	Description
Platforms Affected	Specifies one or more of the routing platforms affected by the alert message
Alert Link	This field is a link that can be clicked to navigate into the Juniper Support Web page for this specific alert

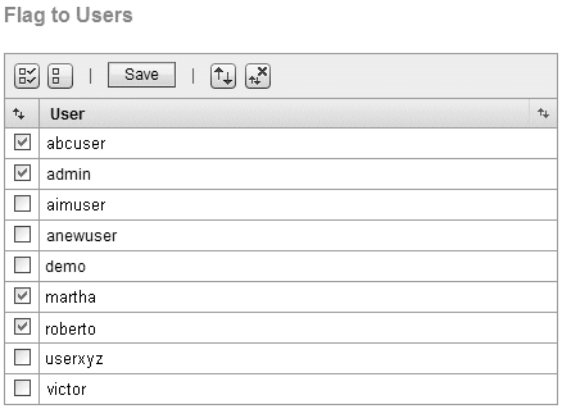
Flagging an Intelligence Update To a User

To flag an incident to a user from Intelligence Updates Information Entry page, follow these steps:

1. Click Intelligence Manager in the navigation area. The Intelligence Updates tab appears by default.

2. In Intelligence Updates, click the intelligence message Synopsis link. The Information Entry page appears.

3. Click Flag to Users. The Flag To Users page appears.



4. On the Flag to Users page, select the user(s) to which you want to flag the intelligence update.

5. Click Save. A flag appears in the intelligence update Flag column on the Information Updates tab. The incident appears in the My AIM Home page for each flagged user for inspection.

Scanning Devices for Impact

For instructions on how to scan for impact, see “Scanning Intelligence Messages for Impact” on page 123.

Assigning an Intelligence Update Owner

For instruction on how to assign an intelligence update to an owner, see “Assigning an Intelligence Message Owner” on page 120.

Changing Owner Status

For instructions on how to change intelligence update owner status, see “Changing Owner Status” on page 145.

Clearing a Flag

1. Click Intelligence Manager in the navigation area. The Intelligence Updates tab appears by default.
2. Select the incident with the flag that you want to delete. The Clear Flag button is enabled.
3. Click Clear Flag. The flag is removed from the Intelligence Updates table and the Intelligence Update will not appear in My AIM Home Intelligence Messages table.

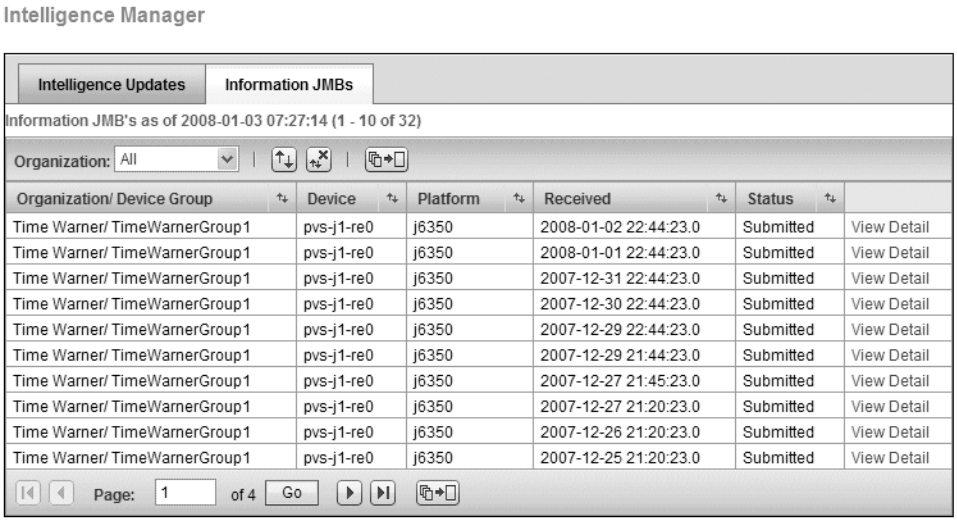
Viewing Information JMBs

The Information JMBs tab allows you to do the following:

- View all information JMBs received from device archive locations.
- View all information JMBs by organization
- View information JMBs contents

To view Information JMBs, do the following:

- In Information Manager, click the Information JMBs tab. the Information JMBs table appears.



For more information about the Information JMBs table, see “Information JMBs Table Description” on page 146.

Information JMBs Table Description

Table 72 describes the Intelligence Updates table button and drop-down list box elements.

Table 72: Intelligence Updates Table Element Descriptions

Element Name	Description	Privileges	Enabled/ Disabled	Results
Organization drop-down list box	Lets you select the AIM organization (site) for which you want to display intelligence messages.	AIM Admin	Always enabled	Displays intelligence updates for selected organization.
View Detail link	Displays the Information Detail page for an information JMB entry.			

Table 70 describes the columns in the Information JMBs table.

Table 73: Information JMBs Table Column Descriptions

Column	Description
Device	Name of device that the Information PRB is from.
Platform	Platform of device
Received	Date and time this Information PRB was detected by JUNOScope
Status	Indicates whether this Information PRB was sent to Juniper Homebase. Status is either: Initial or Submitted.

Viewing Information JMBs by Organization

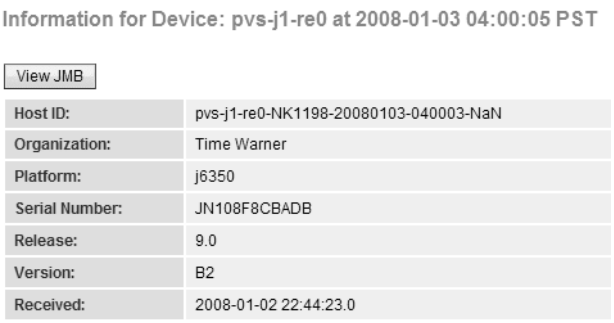
To only view Information JMBs by a specific organization, do the following:

- In the Information JMBs table, select the organization that you want in the Organizations drop-down list box.

Viewing Information JMB Details

To view more detailed information about a specific Information JMB, do the following:

1. Click the Information JMBs tab. The Information JMBs page appears
2. On the Information JMB page, click the View Details link. the Information for Device page appears.



For more information about the Information for Device page, see “Information for Device Field Descriptions” on page 147.

Information for Device Field Descriptions

Table 74 describes the Information for Device page field descriptions.

Table 74: Information for Device Field Descriptions

Element Name	Description	Privileges	Enabled/ Disabled	Results
View JMB button	Displays the View JMB page	AIM Admin	Always enabled	Displays the JMB contents

Table 70 describes the columns in the Information JMBs table.

Table 75: Information JMBs Table Column Descriptions

Column	Description	Range/Length	Default
Host ID	The name of the device from which an information JMB exists		
Organization	The organization within which the information JMB exists		
Platform	The routing platform for the information JMB		
Serial Number	Serial number on the device		
Release	JUNOS software release level		
Version	JUNOS software version		
Received	Time and date the information JMB was received by AIM		

Viewing JMB Content

You can view the contents of an information JMB collected by AIM from the device archive location.

To view an information JMB contents, follow these steps:

1. In Intelligence Manager, click the Information JMB tab. The Information JMBs table appears.

2. In the Information JMBs table, click the View JMB linking in the Information JMBs table. the Information for the Device page appears.

3. On the Information for Device page, click View JMB. the View JMB page appears.

View JMB: pvs-j1-re0_PvS_intel_20080103_120013.xml

(Information as received by Router)

MANIFEST

Host Event ID:	pvs-j1-re0-NK1198-20080103-040003-NaN
Service Type:	intelligence
Event Time:	2008-01-03 04:00:05 PST
Problem Class:	support
Problem Synopsis:	
Problem Description:	
Problem Severity:	
Problem Priority:	
Core File Path:	
Serial Number:	
Router Information	
Product Name:	j6350
Host Name:	pvs-j1-re0
OS Platform:	junos-es
Master Routing Engine	
Name:	Routing Engine 0
Mastership State:	Online Master

The Information JMB includes the following information based upon how much information the customer wants to share with JSS about a device:

- Manifest—basic router and event data
- Trend data—device counters, statistics, and settings
- Attachments—show command output for the incident event.

Part 5

Advanced Insight Manager Management Information Base (MIB)

Chapter 15

Advanced Insight Manager Management Information Base (MIB)

Advanced Insight Manager supports the Juniper Advanced Insight Manager enterprise-specific Management Information Bases (MIB). This MIB defines the traps sent by Advanced Insight Manager to a remote network management system, see “AIM MIB Supported SNMP Traps” on page 154. The traps sent correspond with the trigger type of a reaction policy. For more information about creating a reaction policy in AIM, see “Creating a Policy” on page 136.

This chapter includes the following sections:

AIM MIB Contents

The MIB file will be named jnx-ai-manager.mib and have the following contents:

```
--
-- Juniper Enterprise Specific MIB: Advanced Insight Manager MIB
--
-- Copyright (c) 2007, Juniper Networks, Inc.
-- All rights reserved.
--
-- The contents of this document are subject to change without notice.
--


JUNIPER-AI-MANAGER-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE
        FROM SNMPv2-SMI
    DisplayString
        FROM SNMPv2-TC
    jnxAdvancedInsightMgr
        FROM JUNIPER-SMI;

jnxAIManager MODULE-IDENTITY

    LAST-UPDATED "200710090000Z"
    ORGANIZATION "Juniper Networks, Inc."
    CONTACT-INFO
```

```
                "        Juniper Technical Assistance Center
                 Juniper Networks, Inc.
                 1194 N. Mathilda Avenue
                 Sunnyvale, CA 94089
                 E-mail: support@juniper.net"

        DESCRIPTION
                "The MIB modules representing Juniper Networks'
            implementation of enterprise specific MIBs
            supported by a single SNMP agent."
        REVISION    "200710090000Z" -- 09-Oct-07
        DESCRIPTION
                "Added Advanced Insight Manager identification objects."

        ::= { jnxAdvancedInsightMgr 1 }


    -- Juniper Advanced Insight Manager MIB
    --

    -- Top level objects

        jnxAIMDescr OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..63))
        MAX-ACCESSread-only
        STATUS  current
        DESCRIPTION
                "Description of Advanced Insight notification."
        ::= { jnxAIManager 1 }

        jnxAIMHostName OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..63))
        MAX-ACCESSread-only
        STATUS  current
        DESCRIPTION
            "Device associated with Advanced Insight
            notification."
        ::= { jnxAIManager 2 }

        jnxAIMOrganization OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..63))
        MAX-ACCESSread-only
        STATUS  current
        DESCRIPTION
            "Organization associated with Advanced Insight
            notification."
        ::= { jnxAIManager 3 }

        jnxAIMIncidentHostID OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..63))
        MAX-ACCESSread-only
        STATUS  current
        DESCRIPTION
            "HostID of incident associated with Advanced
            Insight notification."
        ::= { jnxAIManager 4 }

        jnxAIMCaseID OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..63))
        MAX-ACCESSread-only
        STATUS  current
        DESCRIPTION
            "CaseID (assigned by Juniper) associated with
```

```
        Advanced Insight notification."
    ::= { jnxAIManager 5 }

    jnxAIMIssueDate OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..63))
    MAX-ACCESSread-only
    STATUS  current
    DESCRIPTION
        "Issue Date of the intelligence message associated
        with Advanced Insight notification."
    ::= { jnxAIManager 6 }

--
-- definition of Advanced Insight Manager traps
--

jnxAIManagerNotifications  OBJECT IDENTIFIER ::= { jnxAIManager 0 }


    jnxAIMNewIncidentDetected NOTIFICATION-TYPE
    OBJECTS { jnxAIMDescr,
              jnxAIMHostName,
              jnxAIMOrganization,
              jnxAIMIncidentHostID }
    STATUS  current
    DESCRIPTION
        "A jnxAIMNewIncidentDetected trap signifies that
        a new incident has been detected."
    ::= { jnxAIManagerNotifications 1 }

    jnxAIMIncidentReportedToJuniper NOTIFICATION-TYPE
    OBJECTS { jnxAIMDescr,
              jnxAIMHostName,
              jnxAIMOrganization,
              jnxAIMIncidentHostID }
    STATUS  current
    DESCRIPTION
        "A jnxAIMIncidentReportedToJuniper trap signifies
        that an incident has been reported to Juniper."
    ::= { jnxAIManagerNotifications 2 }

    jnxAIMCaseIDAssigned NOTIFICATION-TYPE
    OBJECTS { jnxAIMDescr,
              jnxAIMHostName,
              jnxAIMOrganization,
              jnxAIMIncidentHostID,
              jnxAIMCaseID }
    STATUS  current
    DESCRIPTION
        "A jnxAIMCaseIDAssigned trap signifies that an
        incident has been assigned CaseID."
    ::= { jnxAIManagerNotifications 3 }

    jnxAIMCaseUpdated NOTIFICATION-TYPE
    OBJECTS { jnxAIMDescr,
              jnxAIMHostName,
              jnxAIMOrganization,
              jnxAIMIncidentHostID,
              jnxAIMCaseID }
    STATUS  current
    DESCRIPTION
        "A jnxAIMCaseUpdated trap signifies that
        a case has been updated."
```

```
    ::= { jnxAIManagerNotifications 4 }

    jnxAIMNewIntelligenceMessage NOTIFICATION-TYPE
    OBJECTS { jnxAIMDescr,
              jnxAIMOrganization,
              jnxAIMIssueDate }
    STATUS  current
    DESCRIPTION
        "A jnxAIMNewIntelligenceMessage trap signifies
        that a new intelligence message has been received."
    ::= { jnxAIManagerNotifications 5 }
END
```

Supported SNMP Traps

The AIM MIB supports the SNMP traps shown in Table 76. These traps are organized first by trap name, SNMP trap OID, then attributes.

Table 76: AIM MIB Supported SNMP Traps

Trap Name	snmpTrapOID	Attributes
jnxAIMNewIncidentDetected	.1.3.6.1.4.1.2636.9.1.0.1	jnxAIMDescr jnxAIMHostName jnxAIMOrganization jnxAIMIncidentHostID
jnxAIMIncidentReportedToJuniper	.1.3.6.1.4.1.2636.9.1.0.2	jnxAIMDescr, jnxAIMHostName, jnxAIMOrganization, jnxAIMIncidentHostID
jnxAIMCaseIDAssigned	.1.3.6.1.4.1.2636.9.1.0.	jnxAIMDescr, jnxAIMHostName, jnxAIMOrganization, jnxAIMIncidentHostID, jnxAIMCaseID
jnxAIMCaseUpdated	.1.3.6.1.4.1.2636.9.1.0.4	jnxAIMDescr, jnxAIMHostName, jnxAIMOrganization, jnxAIMIncidentHostID, jnxAIMCaseID
jnxAIMNewIntelligenceMessage	.1.3.6.1.4.1.2636.9.1.0.5	jnxAIMDescr, jnxAIMOrganization, jnxAIMIssueDate

Part 6
Index

■ Index on page 157

Index

A