Advanced Insight Solutions User Guide

Release 1.3

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

Part Number: 530–027470–01, Revision 1

Advanced Insight Solutions 1.3

Writing: Donice G. Evans-Mitchell
Editing: Stella Hackell
Illustration: Faith Bradford
Cover Design: Edmonds Design

Revision History
16 January 2009—Revision 1

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

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

Part 2 Setting Up Advanced Insight Solutions

List of Figures

List of Tables

About This Guide

Objectives

This guide provides a reference for you to install, set up, and use the Advanced Insight Solutions (AIS) product. 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 several major elements:

- The Juniper Data Collector that collects data from Juniper Networks devices not capable of running AI-Scripts, such as M-series, T-series, and J-series devices. The Juniper Data Collector also collects data from E-Series devices running JUNOSe, and certain Netscreen Firewall/VPN devices running ScreenOS. The Juniper Data Collector collects data from archive locations on a periodic basis for proactive monitoring in Advanced Insight Manager. (For more details about specific E-Series and Netscreen Firewall/VPN devices supported, see the *Advanced Insight Solutions Release Notes*.
- AI-Scripts that are configured to run on Juniper Networks devices running JUNOS 9.0 or later. AI-Scripts detect incident and intelligence information and send it to archive locations for reactive and proactive monitoring in Advanced Insight Manager.
- 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 1.3 of the Advanced Insight Solutions product. For additional information about AIS—either corrections to or information that might have been omitted from this guide—see the *Advanced Insight Solutions Release Notes* at http://www.juniper.net/techpubs/.

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, switching and security platforms supported by AIS:

- EX-series
- J-series
- M-series
- MX-series
- T-series
- E-series
- Netscreen Firewall/VPN
- SSG Series

For the latest routing platforms supported, see the *AIS Release Notes*.

Documentation Conventions

Table 1 on page xxv defines notice icons used in this guide.

Table 1: Notice Icons

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

Table 2 on page xxv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

Table 2: Text and Syntax Conventions *(continued)*

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

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

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

Table 3 on page xxvi describes the user interface elements in Advanced Insight Manager. When describing AIM user interface elements, this manual uses the following terminology:

Table 3: Advanced Insight Manager User Interface Element Conventions

Element	Description
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.

Table 3: Advanced Insight Manager User Interface Element Conventions *(continued)*

Element	Description
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.

List of Technical Publications

Table 4 on page xxvii lists the software and hardware guides and release notes for Juniper Networks M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 5 on page xxxi lists the books included in the *Network Operations Guide* series. Table 6 on page xxxii lists the manuals and release notes supporting JUNOS software for J-series and SRX-series platforms. All documents are available at http://www.juniper.net/techpubs/.

Table 7 on page xxxiii 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 4: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	
Access Privilege	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
Broadband Subscriber Management Solutions	Describes residential subscriber management and how you can deploy solutions that include multisubscriber IP address assignment, service provisioning, authentication, authorization, accounting, and dynamic request services in your network

Table 4: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
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 active 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.
MX-series Layer 2 Configuration Guide	Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the *JUNOS Routing Protocols Configuration Guide*.
MX-series Layer 2 Solutions Guide	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
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.
Policy Framework	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.

Table 4: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
Protected System Domain	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
Routing Protocols	Provides an overview of routing concepts and describes how to configure 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 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 router.
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*.
Subscriber Access	Provides an overview of the subscriber access features of the JUNOS software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods.
System Basics	Describes Juniper Networks routing platforms and explains 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 policies and protocols, including firewall filters.

Table 4: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
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 class of service (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 graphical user interface (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.
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.
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's Physical Interface Cards (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.

Table 4: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
Advanced Insight Solutions (AIS) Documentation	
Advanced Insight Solutions Guide	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.
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 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	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.
AIS AI-Scripts Release Notes	Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.

Table 5: JUNOS Software Network Operations Guides

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.
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 routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.

Table 5: JUNOS Software Network Operations Guides *(continued)*

Book	Description
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.

To configure and operate a J-series Services Router or an SRX-series Services Gateway running JUNOS software, you must also use the configuration statements and operational mode commands documented in JUNOS configuration guides and command references. To configure and operate a WX Integrated Services Module, you must also use WX documentation.

Table 6: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation

Book	Description
J-series and SRX-series Platforms	
JUNOS Software Interfaces and Routing Configuration Guide	Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
JUNOS Software Security Configuration Guide	Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).
JUNOS Software Administration Guide	Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
JUNOS Software CLI Reference	Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices.

Table 6: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation *(continued)*

Book	Description
JUNOS Release Notes	Summarize new features and known problems for a particular release of JUNOS software, including JUNOS software for J-series and SRX-series devices.The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software.
J-series Only	
JUNOS Software Design and Implementation Guide	Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software.
J-series Services Routers Quick Start	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
JUNOS Software with Enhanced Services J-series Services Router Hardware Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
JUNOS Software Migration Guide	Provides instructions for migrating an SSG device running ScreenOS software to JUNOS software or upgrading a J-series device to a later version of the JUNOS software.
WXC Integrated Services Module Installation and Configuration Guide	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.

Table 7: 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.

Table 7: Additional Books Available Through http://www.juniper.net/books *(continued)*

Book	Description
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.

Obtaining Documentation

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

To order a documentation CD, which contains this guide, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the documentation CDs and at http://www.juniper.net/.

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

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 devices operating in service provider and enterprise networks by:

- Automatically detecting events (incidents) and intelligence information
- Managing incidents to quick resolution by Juniper Support Systems (JSS) engineers and specialized tools
- Providing intelligence information updates to prevent 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 “Juniper Networks J-Care Technical Services and AIS Functionality” on page 8.

AIM provides the following key benefits:

- Advanced Insight Scripts (AI-Scripts)—These JUNOS operation (op) scripts, that need to be installed and activated on Juniper Networks devices running JUNOS 9.0 or later, reduce network downtime significantly by automatically detecting, collecting, and depositing incidents and intelligence information into monitored archive locations, which allows Juniper Networks JTAC engineers to quickly and efficient resolve cases and proactively identify customer-specific issues before they become problems. For more detailed information about AI-Scripts, see "Installing and Understanding AI-Scripts" on page 47.
- Advanced Insight Manager (AIM)—This application reduces the cost of service license agreement (SLA) violations by providing a faster, more efficient reaction to incidents and intelligence information. Incident and intelligence information are easily flagged to the right users so that they can quickly request case resolution from JTAC and receive intelligence updates. AIM connects and monitors archive locations where devices deposit incident and intelligence information and provides a central point of control for case resolution status and intelligence updates. Reaction policies 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. For more information about using AIM, see "Using Advanced Insight Manager" on page 151.
- The Juniper Data Collector—This AIM service collects data from Juniper Networks devices running JUNOS 8.5 or earlier, such as M-series, T-series, and J-series devices. The Juniper Data Collector also collects data from E-series devices running JUNOSe, and certain Netscreen Firewall/VPN devices running ScreenOS. The Juniper Data Collector collects data from user-specified devices for proactive monitoring in Advanced Insight Manager. For more details about specific E-series and Netscreen Firewall/VPN devices supported, see the *Advanced Insight Solutions Release Notes*.
- JSS—Reduces the amount, severity, and duration of network outages by using the Juniper Networks engineering expertise and customized tools to quickly create cases and communicate case status to AIM.

AIS Key Features

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).

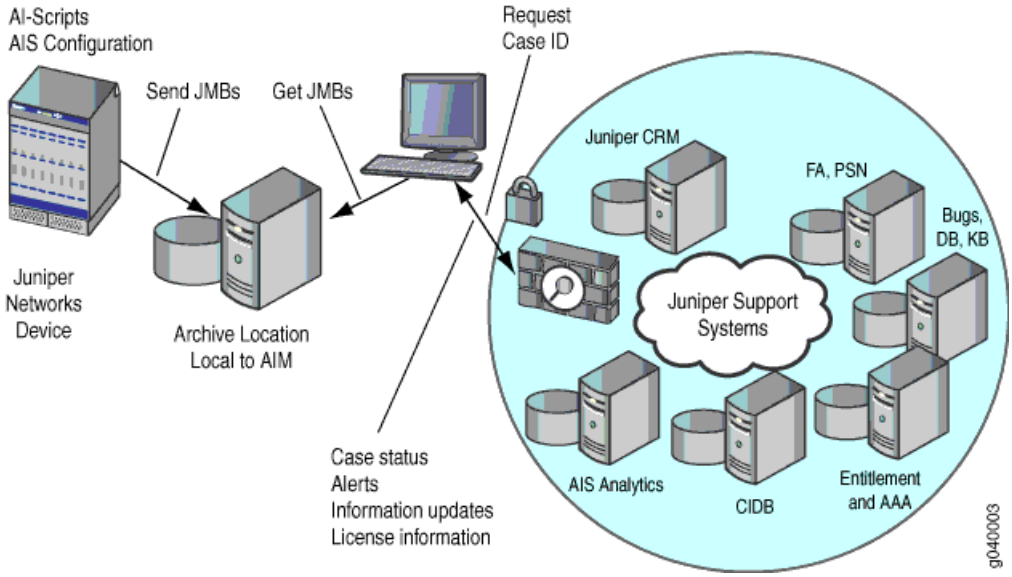
This section contains the following information:

AIS Major Elements

AIS consists of three major elements (see Figure 1 on page 5):

- AI-Scripts on page 5
- Advanced Insight Manager (AIM) Application on page 5
- Juniper Data Collector on page 7
- JSS on page 8

Figure 1: AIS Major Elements



AI-Scripts

Specialized AI-Script install packages must be installed on AIS-configured JUNOS devices running JUNOS 9.0 or later. AI-Scripts, running on devices, automatically do the following:

- React to specific problem events that occur on devices and collect 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 detailed information about AI-Scripts, see“Installing and Understanding AI-Scripts” on page 47.

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, or Mozilla Firefox 2.0.0.16 or later.
- Processes incident JMBs through detection, case ownership, and case creation to quick resolution.
- Processes (and filters according to certain specified settings) intelligence JMBs to JSS for use in providing intelligence and alert updates.
- 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. Load 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.
  - Multi-Site—Allows you to create multiple organizations, which provide a way to manage multiple sites with one AIM installation. Multiple organizations can be used to divide the network into logical customer sites to participate in Advanced Insight Solutions (AIS) services.
  - Partner Controller—Allows a Juniper Networks partner to run AIM to manage end customer's AIM installations. The partner determines what information should flow to and from the end customer.

AIM runs in three modes:

- Standard—The AIM user connects directly to JSS to send incident cases and to receive incident case resolution and intelligence updates.
- Partner Controller—In addition to running AIM in standard mode, the Juniper Networks partner is able to manage end customer AIMs and determine what information should flow to and from each end customer through the management of proxy device groups.
- End Customer—The AIM end customer connects to the partner's AIM, using the partner's secure URL (for example, https://partnerAIM:8443), and sends and receives information from the partner. The partner determines what information flows from the end customer's AIM to JSS. End customers run AIM normally, except that they can not do the following operations:
  - Register for JSS alerts and intelligence messages
  - Connect AIM directly to JSS
  - See the AIM service licenses
  - See the Technical Support Cases tab in Intelligence Manager
- Using organization device group and archive location settings, you can optionally connect to JUNOScope to 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.

- Using reaction policies, can send AIM incident SNMP traps to other network management systems based on configured trap destinations.
- Includes user interfaces to manage incidents, intelligence information, inventory, proactive cases, 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.
  - Inventory Manager—Displays all AIM devices associated to an organization by organization, device group, device name, Juniper Networks routing platform type, serial number, and software version number running. You can filter inventory data by organization or device group to show only the data that you are interested in viewing. You can view device detail information showing all the components installed in the device chassis. You can export inventory data in Microsoft Excel, comma-separated value, or XML format.
  - Proactive Case Manager—Used to submit a case to JSS to request upgrade information for upgrading one or more Juniper Networks devices to a specified software release. JSS personnel analyze proactive cases and provide recommended feedback.

For more information about using AIM, see “Using Advanced Insight Manager” on page 151.

Juniper Data Collector

The Juniper Data Collector is an AIM service that collects data from Juniper Networks devices running JUNOS 8.5 or earlier in archive locations for proactive monitoring in AIM. The Juniper Data Collector also collects data from non-JUNOS devices, such as E-series devices and Netscreen Firewall/VPN (ScreenOS) devices. Devices are added using AIM Settings > Organizations where you create directives device groups for adding Juniper Data Collector devices.

The Juniper Data Collector functions like Advanced Insight Scripts (AI-Scripts). However it only creates intelligence JMBs, not incidents.

In AIM Organizations, you add Juniper Data Collector devices as directives device groups. For more information about adding directive devices to AIM, see “Creating a Directives Group” on page 101.

JSS

JSS, using the Juniper Networks knowledge base, engineering expertise, and specialized tools, can create cases that you open using AIM. JSS sends case status to AIM. JSS receives intelligence information from devices on the network using AIM and sends intelligence updates and alerts for which you have registered to AIM.

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

Juniper Networks J-Care Technical Services and AIS Functionality

Juniper Networks J-Care Technical Services provide several levels of technical support for devices on the network. When the customer purchases certain J-Care Technical Services levels, AIS is available (AI-Scripts and certain AIM features). Table 9 shows the levels of J-Care Technical Services provided and the associated AI-Scripts and AIM features that are offered.

Table 8: J-Care Technical Services and AIS Functionality

J-Care Technical Service	AIS Features/Components
J-Care Essentials	N/A
J-Care Efficiency	AI-Scripts, AIM, Case Submission, Reports, Inventory Management
J-Care Continuity	AI-Scripts, AIM, Case Submission, Reports, Inventory Management, JSS (Insight JTAC)
J-Care Agility	AI-Scripts, AIM, Case Submission, Reports, Inventory Management, JSS (Insight JTAC), Proactive Product Reports (Intelligence)

The AIM application requires base, feature (optional), and capacity licenses. AIM License Management displays the current license and services after the license file is imported. For more information about AIM licensing, see “Using AIM License Management” on page 83.

AIM Customer/Partner Engagement Models

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

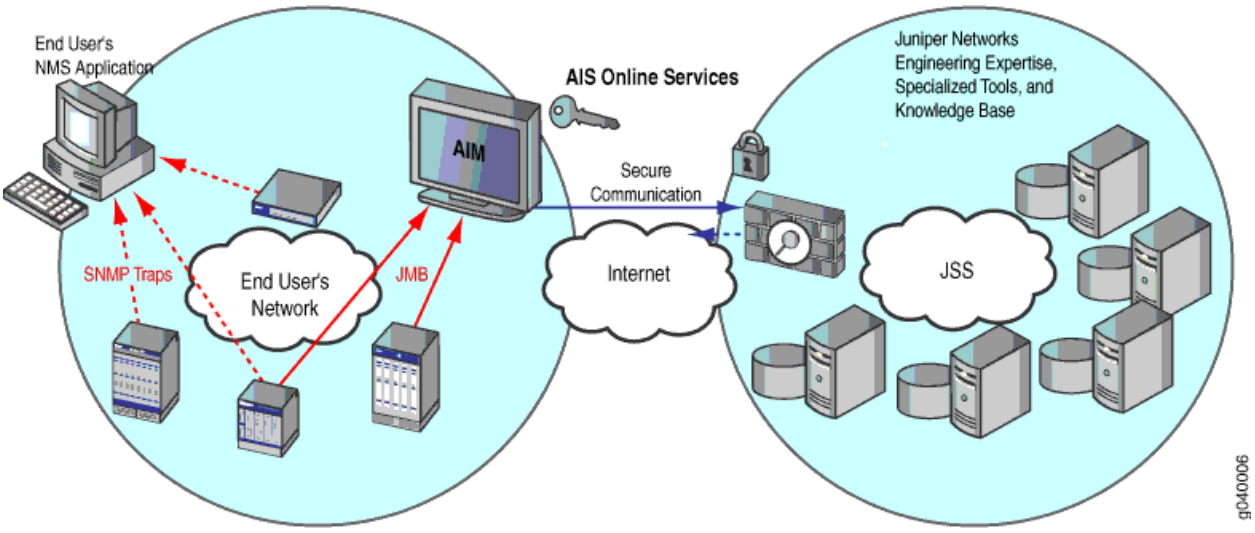
- Direct-Customer AIS Engagement Model on page 8
- Partner-Deployed AIS Engagement Model on page 10
- Partner End-Customer Deployed AIS Engagement Model on page 11

Direct-Customer AIS Engagement Model

You, the AIS direct customer, install AIS software elements (AI-Scripts and AIM), and subscribe to AIS services. See “Advanced Insight Solutions Overview” on page 3.

See “Installing and Understanding AI-Scripts” on page 47. See “Juniper Networks J-Care Technical Services and AIS Functionality” on page 8. See Figure 2 on page 9.

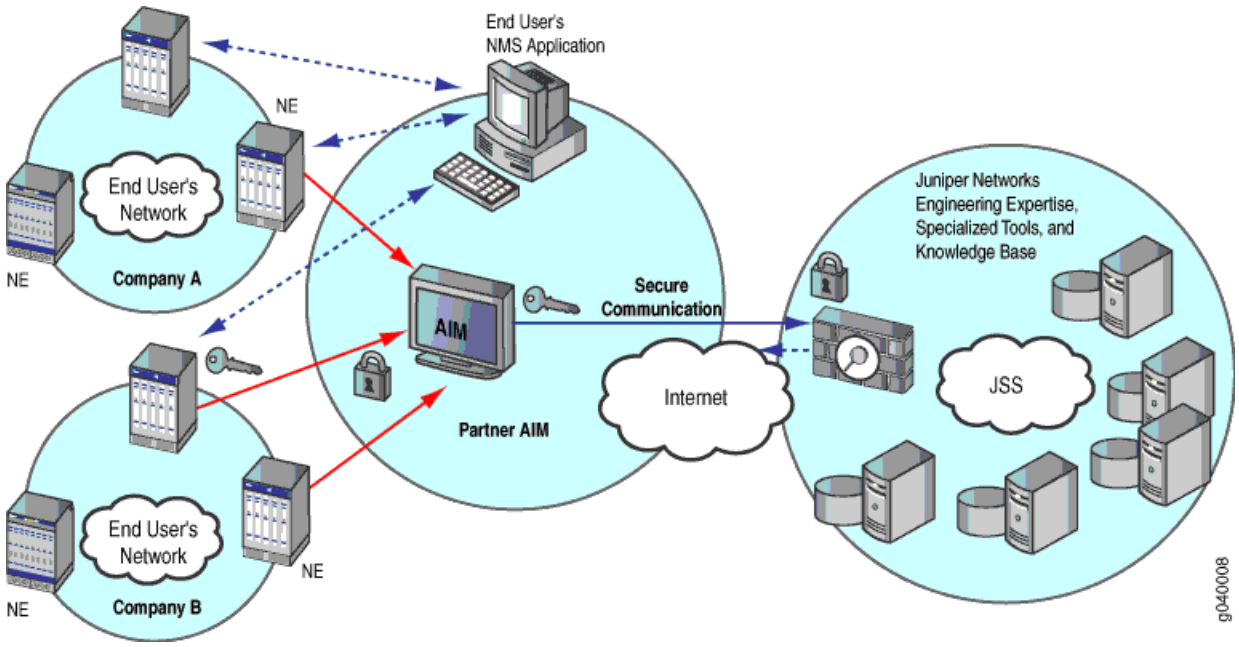
Figure 2: AIS Direct-Customer Engagement Model



Partner-Deployed AIS Engagement Model

The Juniper Networks partner installs AIM, with the Partner Controller license, to manage multiple end customers. The partner's AIM is used as an aggregation point for incidents from many customers. Each end customer installs AIM in their network. The end customers run AIM in the same way as it is run in the Direct Customer AIS engagement model, except instead of connecting directly to JSS, they connect to the Partner Controller AIM installation. The partner has the option of submitting cases on behalf of their end customers or handling them without engaging with JSS. All connections are through authenticated and encrypted protocols. Secure file transfers occur between the AIM end customer and partner installations. An HTTPS connection is made from the end customer AIM installation and the partner controller installation, as well as from the partner controller AIM installation and JSS. See “Advanced Insight Solutions Overview” on page 3. See “Installing and Understanding AI-Scripts” on page 47. See “Juniper Networks J-Care Technical Services and AIS Functionality” on page 8. See Figure 3 on page 10.

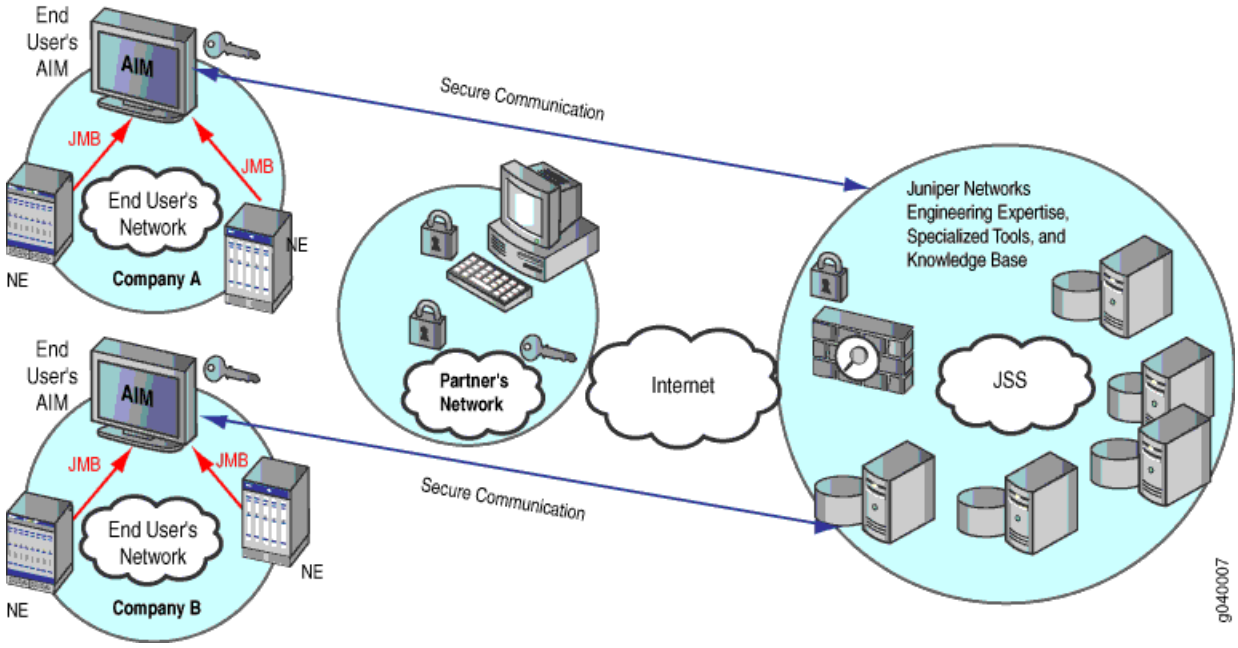
Figure 3: AIS Partner-Deployed Engagement Model



Partner End-Customer Deployed AIS Engagement Model

AIM is installed on each end user's network and accessed remotely by the partner through a Web client. There is no AIM at the partner location. Each end user's AIM communicates directly with JSS. The partner can choose to administer each end user's AIM individually or allow each end user to administer their own AIM. If the end user sends a case request to JSS (for example, if the end user has administrative privileges to their own AIM), the partner can view information by remotely logging in to an end user's AIM. A firewall hole or tunnel between the end-customer AIM and JSS is necessary. The partner also needs access to the end-customer AIM. All connections are through authenticated and encrypted protocols. See Figure 4 on page 11.

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



JUNOScope 9.0 or Later Software Script Management

(Optional) AIM integrates with the JUNOScope 9.0 or later software through an API to automatically install AI-Script installation 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 on which devices to install AI-Script install packages through AIM Organizations settings. If AIM and JUNOScope are run on the same server, it is recommended that JUNOScope be installed before installing AIM.

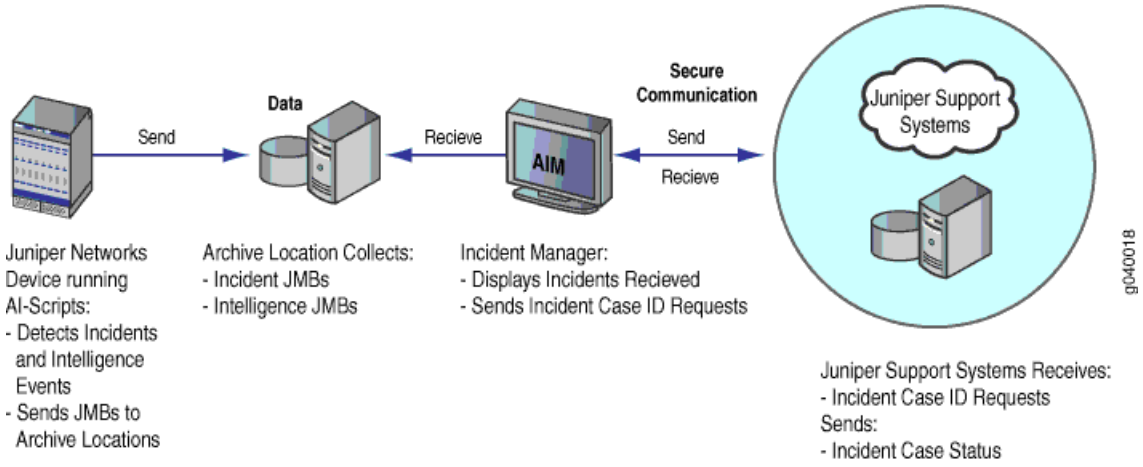
AIS Workflows

There are two distinct workflows within AIS: one for incident information; the other for intelligence information. AIM periodically polls the archive locations for incident and intelligence JMBs and displays the information in Incident Manager and Intelligence Manager.

Incident-Driven Analysis Workflow

The AIS incident-driven workflow occurs as follows (see Figure 5 on page 12):

Figure 5: AIS Incident-Driven Workflow



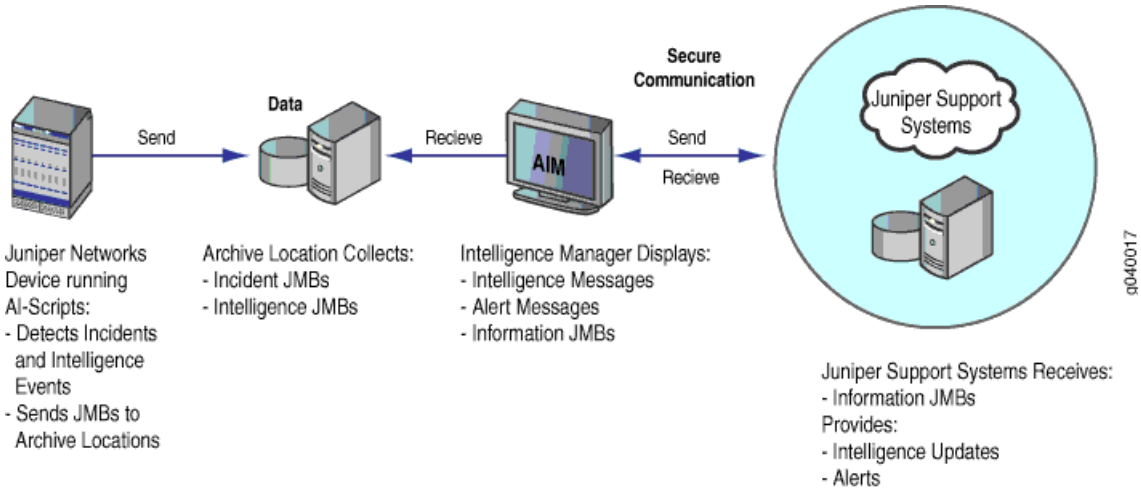
1. A trigger event occurs and is detected on a device configured for and running AI-Scripts. An AI-Script is executed.
2. An AI-Script builds an event JMB with event and router data, and sends it to a designated AIM archive location.
3. AIM receives the event JMB and displays it in Incident Manager. The incidents appear in My AIM Home where they can be assigned or flagged to an AIM user.
4. An AIM user submits an incident to JSS.
5. JSS creates and returns a case ID to AIM.
6. JTAC 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 163.

Intelligence-Driven Analysis Workflow

JSS receives informational JMBs from AIM and collects them in the knowledge base. AIM periodically polls JSS for the availability of intelligence messages consisting of informational (created by JTAC engineers specifically for the customer) or alert messages (based on the alerts for which the customer registered. The intelligence-driven workflow occurs as follows (see Figure 6 on page 13):

Figure 6: AIS Intelligence-Driven Workflow



1. An AI-Script builds an intelligence JMB and sends it to a designated archive location on a weekly basis.
2. AIM periodically polls the archive location and receives the intelligence JMB.
3. The customer can specify how much information is shared with JSS on the AIM General Settings page.
4. AIM displays the intelligence JMB in the Intelligence Manager Information JMBs.
5. AIM periodically queries JSS for intelligence updates. Intelligence Updates consist of alerts (based on the AIM alert subscriptions) or intelligence updates created by JTAC engineers specifically for the customer.
6. JSS checks to see if there are any alerts or intelligence update messages destined for the customer's AIM.
7. JSS responds to an AIM request with any alerts or intelligence updates for that installation.
8. AIM receives the alerts or intelligence updates and displays them in the Intelligence Manager Intelligence Updates tab.

For more information about using AIM Intelligence Manager, see "Advanced Insight Solutions Overview" on page 3.

Part 2
Setting Up Advanced Insight Solutions

Chapter 2

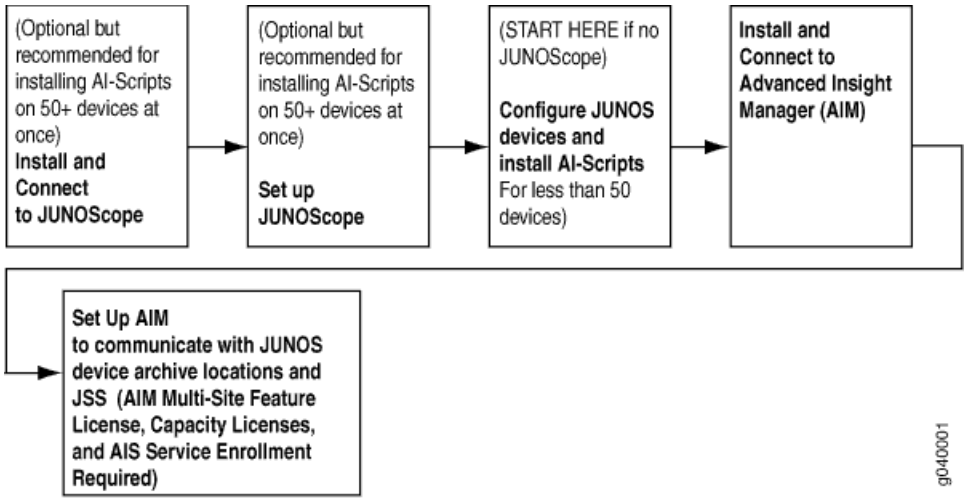
AIS Quick Setup Checklist

This chapter provides the information the AIS administrator needs to plan, design, and install the Advanced Insight Solutions (AIS) system successfully on the network. The AIS system elements that need installation and set up include:

- JUNOScope software (optional)
- Advanced Insight (AI-Scripts)
- Advanced Insight Manager (AIM)

Figure 7 on page 17 shows the sequence of key steps necessary to install and set up AIS.

Figure 7: AIS Installation Sequence



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 usable until the archive location is configured.

This chapter includes the following sections:

Before You Begin

Make sure of the following before you install the AIS components:

- The J-Care Technical Services/AIS order has been processed and the appropriate AIM authorization codes and serial number have been sent.
- You understand the level of AIS functionality based on the J-Care Technical Service ordered. See "Juniper Networks J-Care Technical Services and AIS Functionality" on page 8
- There is an AIS administrator. See "AIS Administrator/User Roles" on page 18.
- There is a dedicated AIM server that meets the AIM system requirements "AIM System Requirements" on page 30.
- AI-Scripts will be installed on supported Juniper Networks devices running JUNOS Release 9.0 or later.

AIS Administrator/User Roles

The design, setup, and implementation of the AIS system depends upon the existence of the following personnel and roles in the network operations center (NOC):

(Optional) JUNOScope Software Administrator

The JUNOScope software administrator is responsible for the installation, operation, and maintenance of the JUNOScope software and server. The JUNOScope software administrator is an IT personnel in the NOC responsible for the support of UNIX or Linux applications in both trial and production environments. The JUNOScope software administrator is responsible for:

- Integrating the JUNOScope software with AIM
- Creating the AIS user account in the JUNOScope software
- Adding devices for automatic AI-Script installation in JUNOScope
- Helping to configure JUNOScope software settings in AIM
- Helping to automatically installation AI-Scripts on multiple devices at once using the JUNOScope software.

AIS Administrator

The AIS Administrator is a member of the IT group within the NOC, and is responsible for the support of UNIX or Linux applications in both trial and production environments. The AIS administrator is responsible for the following AIS tasks:

- Designing and implementing the AIS system, including:
  - AI-Scripts installation, operation, and maintenance on Juniper Networks devices
  - JUNOScope software integration with AIM if automatic installation of AI-Scripts on multiple devices is desired.
  - AIM installation, operation, and maintenance to communicate effectively between device archive locations and JSS.
- Resolving escalated events from JUNOScope, AI-Scripts, and AIM.

AIM Administrator

The AIM administrator is an IT application support person who has AIM Admin Settings privileges in AIM. The AIM administrator is responsible for AIM configuration including:

- Managing user accounts
  - Setting up new user accounts, including setting individual permissions
  - Disabling accounts
  - Changing or updating accounts
- Assigning and updating reaction policies
- Assigning and updating alert registrations
- Managing AI-Script updates (using JUNOScope software)
- Managing AIM software updates and upgrades
- Tracking disk and systems resources on the AIM server for capacity planning

AIM User

The AIM user is responsible for monitoring problem and intelligence events from devices and intelligence messages from JSS and submitting cases to JSS for resolution. 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. AIM users have access to organizations and the devices contained in them based on their user group and device group associations. For more information about AIM user privileges, see “AIM User Privileges” on page 137.

AIS Design and Planning Checklist

This section provides a checklist for the AIS administrator to design and plan the AIS system.

Table 9: AIS Design and Planning Checklist

Task	Description/Comment
Design & Plan for AIS	
Read the AIS documentation	■ (Optional) *JUNOScope Software Release Notes*and the *JUNOScope Software User Guide* (See https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/) ■ *Advanced Insight Scripts (AI-Scripts) Release Notes* (See https://www.juniper.net/support/csc/swdist-encr/swdist-ais/ ■ *Advanced Insight Solutions (AIS) Release Notes* (See https://www.juniper.net/support/csc/swdist-encr/swdist-ais/ ■ *Advanced Insight Solutions User Guide* (See https://www.juniper.net/support/csc/swdist-encr/swdist-ais/

What you need	Access to the following systems and information is required to complete AIS installation:
	■ (Optional) Dedicated JUNOScope Linux or Solaris software server with appropriate permissions and requirements
	■ (Optional) JUNOScope software installer file
	■ (Optional) JUNOScope URL, AIS username and password added to JUNOScope for AIM, IP address for device-to-JUNOScope FTP connectivity, and devices managed
	■ Dedicated AIM Linux or Solaris server with appropriate permissions and requirements
	■ (Optional) FTP or file server for device archive locations
	  ■ NFS mounted to AIM host
	  ■ FTP login and password
	■ Clarify site ID and credentials
	■ AIM authorization codes and serial number sent by Juniper Networks
	■ Juniper Networks software download site URL and credentials
	■ AIM installer file
	■ AI-Scripts bundle file
	■ AI-Scripts installation, configuration, and verification (automatic or manual)
	■ AIM installation, set up, and verification
	■ Juniper License Management System (LMS) URL and credentials
	■ Juniper J-Care Technical Services contact information

What to install	■ (Optional) JUNOScope 9.0 Software or later ■ AI-Scripts 1.1 or later ■ AIM 1.1 or later ■ AIM License File
Security considerations	■ Set up firewall rules to allow outbound traffic from the AIM server to JSS on TCP port 443. ■ The local DNS should resolve support.net and services.juniper.net. ■ Determine the level of device configuration filtering required for JMBs in archive locations. See “Configuring General Settings” on page 67

Table 9: AIS Design and Planning Checklist *(continued)*

Task	Description/Comment
Determine AIS engagement model	■ Direct-Customer AIS Engagement Model—The AIS direct customer installs AIS software elements (AI-Scripts and AIM). ■ Partner-Deployed AIS Engagement Model—The AIS partner installs AIM software elements (AI-Scripts and AIM) to manage multiple users. The AIM server is used as an aggregation point for JMBs from many customers. The partner administers the AIM server and users (customers) have read-only access to AIM. ■ Partner End-User Deployed AIS Engagement Model—AIM is installed on each user's network and accessed remotely by the partner through a Web client. There is no AIM at the partner location. Each user's AIM communicates directly with JSS.
What organizations need AIS	■ Customers or sites that need AIS ■ Which devices are to be associated with the site ID and Juniper credentials (to define an organization)? ■ Number of, and names for, device groups
What devices need AIS	■ Juniper Networks devices meet the AI-Scripts system requirements, see "AI-Scripts System Requirements" on page 51. ■ Where will the archive locations for event and intelligence Juniper Message Bundles (JMBs) for each device be configured?
What users will use AIS	List the AIM users, including: ■ Needed permissions ■ Needed user groups ■ Associations with device groups ■ Initial reaction policies ■ Initial alert registrations

AIS Setup Checklist

Table 11 lists the key steps necessary to install and set up the components to run AIS. It includes references to more detailed information about each task.

Table 10: AIS Quick Set Up Checklist

AIS Install Task	Comments/Where To Find More Information
Download AIS Components	
1. Log into the Juniper Networks software download site and download the AIS components to install.	Download the following: ■ (Optional) JUNOScope Software: https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/ ■ AI-Scripts package: https://www.juniper.net/support/csc/swdist-encr/swdist-ais/ ■ Advanced Insight Manager (AIM): https://www.juniper.net/support/csc/swdist-encr/swdist-ais/

Table 10: AIS Quick Set Up Checklist *(continued)*

AIS Install Task	Comments/Where To Find More Information
(Optional) Install and Set Up the JUNOScope Software	
2. (Optional) Install the JUNOScope software if you have not already done so.	See the "Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software" section in the *JUNOScope Software Release Notes* or the chapter in the *JUNOScope Software User Guide*.
3. (Optional) Set up the JUNOScope software.	■ Add an AIM User with Read-Write Privileges; see the "User Local Authentication" chapter in the *JUNOScope Software User Guide*. ■ Set Up Authorization Information for devices, see the "Setting Up Authentication Information" chapter in the *JUNOScope Software User Guide*. ■ Set Up an Access Method for devices; see the "Access Method" chapter in the *JUNOScope Software User Guide*. ■ Add Devices; see the "Setting Up Devices" chapter in the *JUNOScope Software User Guide*
Install and Verify AI-Scripts	
4. Install AI-Scripts on Juniper Networks devices.	See "Manually Configuring and Installing AI-Scripts on Devices" on page 54.
5. Verify AI-Scripts operation.	See "Manually Configuring and Installing AI-Scripts on Devices" on page 54.
Install and Connect to AIM	
6. Install AIM.	See "Installing Advanced Insight Manager" on page 29.
7. Verify that AIM services are running.	See "Starting and Stopping AIM Application Services" on page 34.
8. Connect to AIM and log in.	See "Connecting to AIM and Logging In" on page 39.
Generate and Activate the AIS License Key	
9. Generate the AIM license file.	See "Activating Advanced Insight Solutions" on page 59.
10. Log in to AIM and create a new administrator user account.	■ See "Logging In to the AIM Application" on page 40. ■ See "Changing the AIM Administrator Password" on page 41.
11. Load the license file.	See "Activating Advanced Insight Solutions" on page 59.
12. Activate AIS capacity and service licenses.	See "Activating Advanced Insight Solutions" on page 59.
Set Up AIM	
13. Add AIM users.	See "Setting Up AIM Users" on page 135.
14. Add User Groups and associate users.	See "Setting Up AIM User Groups" on page 145.
15. Add organizations.	■ Configure organization credentials ■ Configure device groups ■ Configure archive locations ■ Associate devices to device groups ■ Associate user groups to device groups See "Configuring AIM Organizations and Device Groups" on page 91.

Table 10: AIS Quick Set Up Checklist *(continued)*

AIS Install Task	Comments/Where To Find More Information
16. Test device and AIM connectivity.	■ Connect to the AIM server in the archive location directory (for example, ls -l/opt/archives for *.xml JMB files. These files verify successful connectivity. ■ In AIM Intelligence Manager, look for information JMBs by choosing the Advanced Insight Solutions > Intelligence Manager > Information JMBs tab. Click View Detail to see device configuration details.
17. Test AIM and JSS connectivity.	See "Configuring AIM Organizations and Device Groups" on page 91.
18. (Optional) Configure AIM general settings.	See "Configuring General Settings" on page 67.
19. Configure and test JUNOScope settings.	See "Configuring JUNOScope Settings" on page 71.
20. (Optional) Upload AI-Scripts from AIM automatically.	■ See "Configuring General Settings" on page 67. ■ See "Configuring AIM Organizations and Device Groups" on page 91.
21. Configure trap destinations.	See "Configuring Trap Destinations" on page 131.
22. Set up reaction policies.	See "Creating Reaction Policies" on page 237.
23. Subscribe to Juniper Networks product alerts.	See "Associating Registered Alerts to an Organization" on page 122.
24. Populate My AIM Home.	■ See "Populating the Incidents Table" on page 155. ■ See "Populating the Intelligence Messages Table" on page 155. ■ See "Populating the Reaction Policies Table" on page 155.

Chapter 3

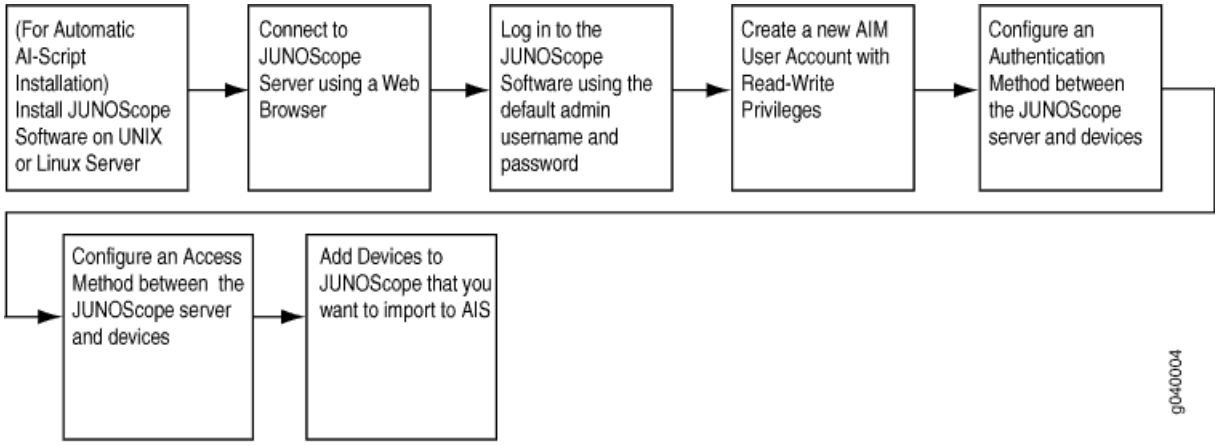
Installing and Setting Up JUNOScope Software for AIS

This chapter explains how to install and set up the JUNOScope 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 on page 25 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. Install JUNOScope software first. AIS requires JUNOScope 9.0 or later.

This chapter includes the following sections

Installing the JUNOScope Software

To install JUNOScope 9.0 Software or later, see the chapter about installing the software in the *JUNOScope Software User Guide*. 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 chapter about installing the software in the *JUNOScope Software User Guide*,

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 chapter about installing the software in the *JUNOScope Software User Guide*.

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 the chapter about setting up user local Authentication in the *JUNOScope Software User Guide*.

Set Up an Authorization Method

Set up 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 the chapter about setting up authentication information in the *JUNOScope 9.0 Software User Guide*.

Set Up an Access Method

Set up 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 the chapter about setting up an access method in the *JUNOScope Software User Guide*.

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 the chapter about Setting Up Devices in the *JUNOScope Software User Guide*,

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

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 using a Web browser, and log in. It also describes how to uninstall AIM.

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

If you are also installing the JUNOScope software, you can install AIM and JUNOScope on the same server. JUNOScope is not required, but is recommended to automatically configure JUNOS and install AI-scripts onto multiple devices at once. Install and set up the JUNOScope software before you install AIM. See "Advanced Insight Solutions Overview" on page 3.

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 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 . For a Sun Solaris server, see Table 11 on page 30. For a Linux server, see Table 12 on page 31.

Sun Solaris Server System Minimum Requirements

Before you install the AIM application on a Sun Solaris server, ensure that the server meets the minimum requirements shown in Table 11 on page 30.

Table 11: AIM Minimum Sun Solaris Server

System	Minimum Requirement
Operating system	Solaris 9.0 or later **NOTE: GNU Privacy Guard (GPG) is required to be installed.**
Processor	UltraSPARC III or equivalent
Speed	1.3 GHz or faster
RAM	1 gigabyte (GB)
Free disk space	Follow these guidelines for disk space allocation: ■ Up to 100 devices under management: Allocate at least 20 GB for archive location and at least 20 GB for AIM application (at least 40 GB if archive location is a local drive on the AIM server) ■ Between 100-1000 devices under management: Allocate at least 50 GB for archive location and at least 50 GB for AIM application (at least 100 GB if archive location is a local drive on the AIM server) ■ More than 1000 devices under management: Contact your Juniper Networks J-Care Technical Service representative

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 requirements shown in Table 12 on page 31.

Table 12: AIM Minimum Linux Server

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	Follow these guidelines for disk space allocation: ■ Up to 100 devices under management: Allocate at least 20 GB for archive location and at least 20 GB for AIM application (at least 40 GB if archive location is a local drive on the AIM server) ■ Between 100-1000 devices under management: Allocate at least 50 GB for archive location and at least 50 GB for AIM application (at least 100 GB if archive location is a local drive on the AIM server) ■ More than 1000 devices under management: Contact your Juniper Networks J-Care Technical Service representative

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 later or Mozilla Firefox 2.0.0.16 or later.

Information Requested During AIM 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. 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, as described in “Connecting to AIM and Logging In” on page 39.
- 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 you must enter a port number from 1 to 65535. The default port number is 1099.
- 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 the AIM application. Enter a port number from 1 to 65535. Port number 1122 is the default.
- Username and group for the installation directory—A non-root username and group, for example aimuser and aimgroup 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 cannot use the same mySQL port number. They are separate installations, each with their own mySQL sub-installation.

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

   user@host>*installer location*/**install.bin**

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

   user@host> *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 to Receive E-mail from AIM

To receive e-mail from the AIM application when you create a reaction policy, enter the ai_manager.rc file smtp_protocol_value and sender values as shown. The ai_manager. rc file is located in the /opt/aim/ directory.

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 to Receive E-mail from AIM” on page 33. For the changes to take effect, you must restart the aimService. See “Starting and Stopping AIM Application Services” on page 34.

The contents of the ai_manager.rcfile is as follows. Bold text indicates the values to enter):

```
;; 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.mycompany.net
sender=testaimuser@mycompany.net
```

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 34) or start them individually (see "Starting Each Service Individually" on page 35). If you start the services individually, start them in the following order:

1. mySQL—Open source database that stores information required for AIM application operation. For more detail about the command options for starting mySQL see "mysql" on page 35.
2. jboss—The underlying AIM application server. For more detail about the command options for starting jboss, see "jboss" on page 36.
3. aimService—Background service that communicates with Juniper Support Systems. For more detail about the command options for starting aimService, see "aimService" on page 36.
4. aimJDCService—Background service that starts the Juniper Data Collector. For more detail about the command options for starting aimJDCService, see "aimJDCService" on page 37.

Starting All Services Simultaneously

To start all 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 in order:

```
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 you start the aimService.

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

Stopping All Services Simultaneously

To stop all 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/aimJDCService stop
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 with command options for starting and stopping the required services:

- mysql on page 35
- jboss on page 36
- aimService on page 36
- aimJDCService on page 37
- Command Usage on page 37
- allservices on page 37

mysql

This 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 mySQL Server is 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, and starts it again.
- restart console—Stops the jboss Service and starts it again in a new console window.
- check—States whether the jboss Service is running.
- help—Displays a help message.

aimService

This section provides a reference for the aimService command options. The aimService is the background service required to communicate with the JSS.

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, and starts it again.
- restart console—Stops the AIM application service and starts it again in a new console window.
- check—States whether the AIM application service is running.
- help—Displays a help message.

aimJDCService

This section provides a reference for the aimJDCService command options. The aimJDCService is the service required to start the Juniper Data Collector.

Command Usage

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

- start—Starts the AIM JDC Service as a background process.
- start—Starts the AIM JDC Service as a background process.
- stop—Stops the AIM Service.
- restart—Stops the AIM JDC Service if it's running, and starts it again.
- restart console—Stops the AIM JDC Service currently running and starts it again in a new console window.
- check—States whether the AIM JDC Service is currently running.
- help—Displays a 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, 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 mySQL, jboss Service, and AIM application services (on this workstation) are running.
- help—Displays a help message.

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)
|-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)
|-aimJDCService (directory containing the lib and executable jar for
the AIM Juniper Data Collector (JDC) Service)
|---- directives  (subdirectory where JDC directives files need to be placed
       |--------- directive.rc  (the AIM 1.2 shipping directives file)
|-rc.d (directory used for startup shell scripts)
```

AIM Install Log

The AIM Install log lets you monitor the AIM installation operations and troubleshoot if an issue occurs.

Filename

Advanced_Insight_Manager_installLog.log

Description

This log file contains detailed information about actions that occur during the AIM installation, such as installation steps and license activation. This file is generated and updated during the AIM installation process. It is useful to determine why the AIM installation fails.

Sample

```
Install Begin: Thu Apr 10 19:12:34 PDT 2008
Install End:   Thu Apr 10 19:15:24 PDT 2008
Created with Zero G's InstallAnywhere 7.1 Enterprise Build 2788
Summary
-------
Installation: Successful.
493 SUCCESSES
0 WARNINGS
0 NONFATAL ERRORS
0 FATAL ERRORS
Action Notes: None.
Install Log Detail:
Install Action:  InstallAnywhere Variable  Status: SUCCESSFUL
Install Action:  InstallAnywhere Variable  Status: SUCCESSFUL
```

```
Install Action:  InstallAnywhere Variable  Status: SUCCESSFUL
...
Install File: /opt/aim/data/config/Key1.public.asc  Status: SUCCESSFUL
Execute Script/Batch file:  Install Public Key  Status: SUCCESSFUL
Execute Command:  su - $USERNAME$ -c "$GPG$ --import
$USER_INSTALL_DIR$$/$data$/$config$/$Key1.public.asc"
Status: SUCCESSFUL
Install Directory:  /opt/aim/data/db/  Status: SUCCESSFUL
Install File:  /opt/aim/data/my.cnf  Status: SUCCESSFUL
```

Connecting to AIM 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 30.

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:

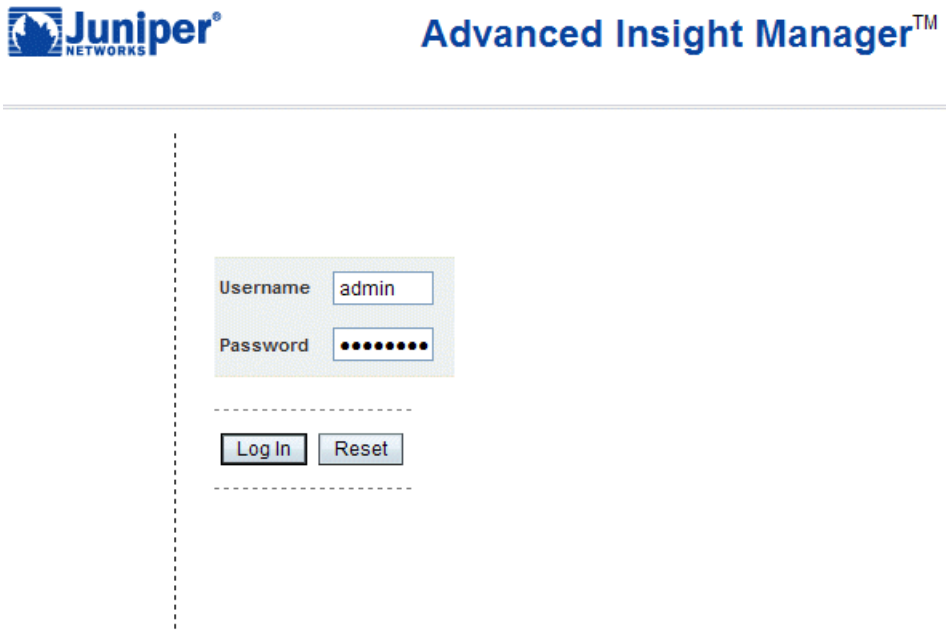
1. Start a Web browser.
2. Enter the following URL in the Address text box:

   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/AIManagerClient
   or
   http:// 123.123.123.123:8080/AIManagerClient

The Advanced Insight Manager Login dialog box appears.

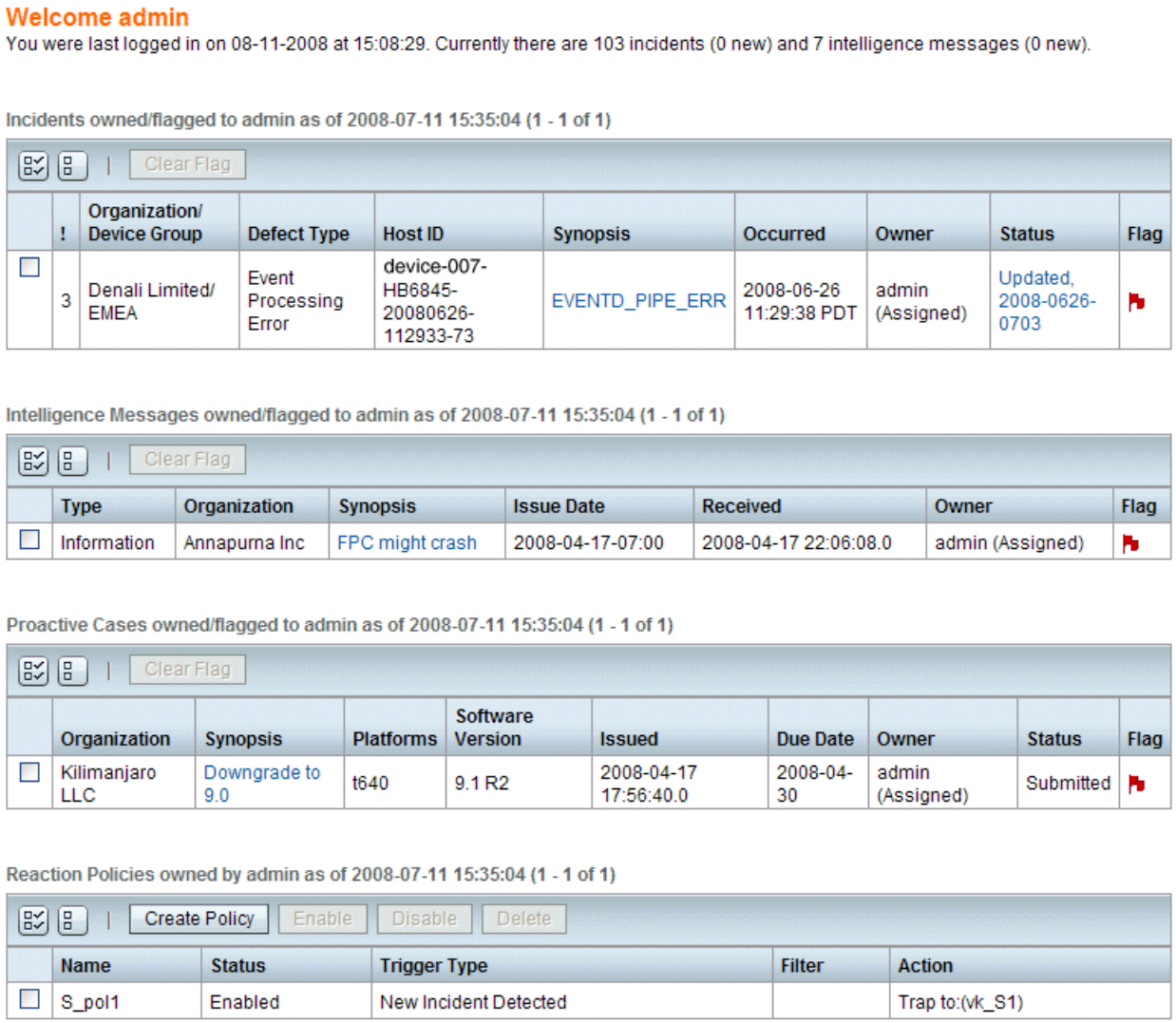


Logging In to the AIM Application

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. (Though each table is shown here with one record, the My AIM Home tables are empty when you log in the first time. See “Populating the Incidents Table” on page 155, “Populating the

Intelligence Messages Table" on page 155, "Populating the Proactive Cases Table" on page 155, and "Populating the Reaction Policies Table" on page 155.



Welcome admin

You were last logged in on 08-11-2008 at 15:08:29. Currently there are 103 incidents (0 new) and 7 intelligence messages (0 new).

Incidents owned/flagged to admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Clear Flag

	!	Organization/ Device Group	Defect Type	Host ID	Synopsis	Occurred	Owner	Status	Flag
☐	3	Denali Limited/ EMEA	Event Processing Error	device-007-HB6845-20080626-112933-73	EVENTD_PIPE_ERR	2008-06-26 11:29:38 PDT	admin (Assigned)	Updated, 2008-0626-0703	

Intelligence Messages owned/flagged to admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Clear Flag

	Type	Organization	Synopsis	Issue Date	Received	Owner	Flag
☐	Information	Annapurna Inc	FPC might crash	2008-04-17-07:00	2008-04-17 22:06:08.0	admin (Assigned)	

Proactive Cases owned/flagged to admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Clear Flag

	Organization	Synopsis	Platforms	Software Version	Issued	Due Date	Owner	Status	Flag
☐	Kilimanjaro LLC	Downgrade to 9.0	t640	9.1 R2	2008-04-17 17:56:40.0	2008-04-30	admin (Assigned)	Submitted	

Reaction Policies owned by admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Create Policy | Enable | Disable | Delete

	Name	Status	Trigger Type	Filter	Action
☐	S_pol1	Enabled	New Incident Detected		Trap to:(vk_S1)

Changing the AIM Administrator Password

You should change the default AIM password aimadmin to a more secure one.

To change the AIM administrator password, follow these steps:

1. 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, follow these steps:

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

   user@host>*installation directory*/**AIM_Uninstaller/AIMUninstaller**

Chapter 5

Understanding the Juniper Data Collector

This chapter describes the Juniper Data Collector, an AIM service that periodically collects proactive intelligence information from Juniper Networks devices. The Juniper Data Collector supports earlier versions of JUNOS devices running the standard JUNOS operating system. It supports E-series devices running JUNOSe and certain Netscreen Firewall/VPN devices running ScreenOS. It does not support EX-series devices or devices running JUNOS software with enhanced services. AI-Scripts, on the other hand, does support these devices. For a complete list of Juniper Networks devices supported by the Juniper Data Collector, see the *Advanced Insight Solutions Release Notes*.

The Juniper Data Collector only collects intelligence JMBs. It does not collect device configuration information.

You add devices supported by the Juniper Data Collector to AIM using the Settings > General Settings and Organizations user interfaces. Then you add the devices directives groups. Data collected from devices is displayed in AIM Intelligence Manager for monitoring. For more information about creating a directives group and adding devices in AIM organizations, see “Creating a Directives Group” on page 101.

The Juniper Data Collector and associated directives file are installed when you install the AIM application. The directives file tells the Juniper Data Collector what information to collect and the frequency of data collection.

You must have AIM administrator privileges to create organizations with directives device groups.

This chapter includes the following topics

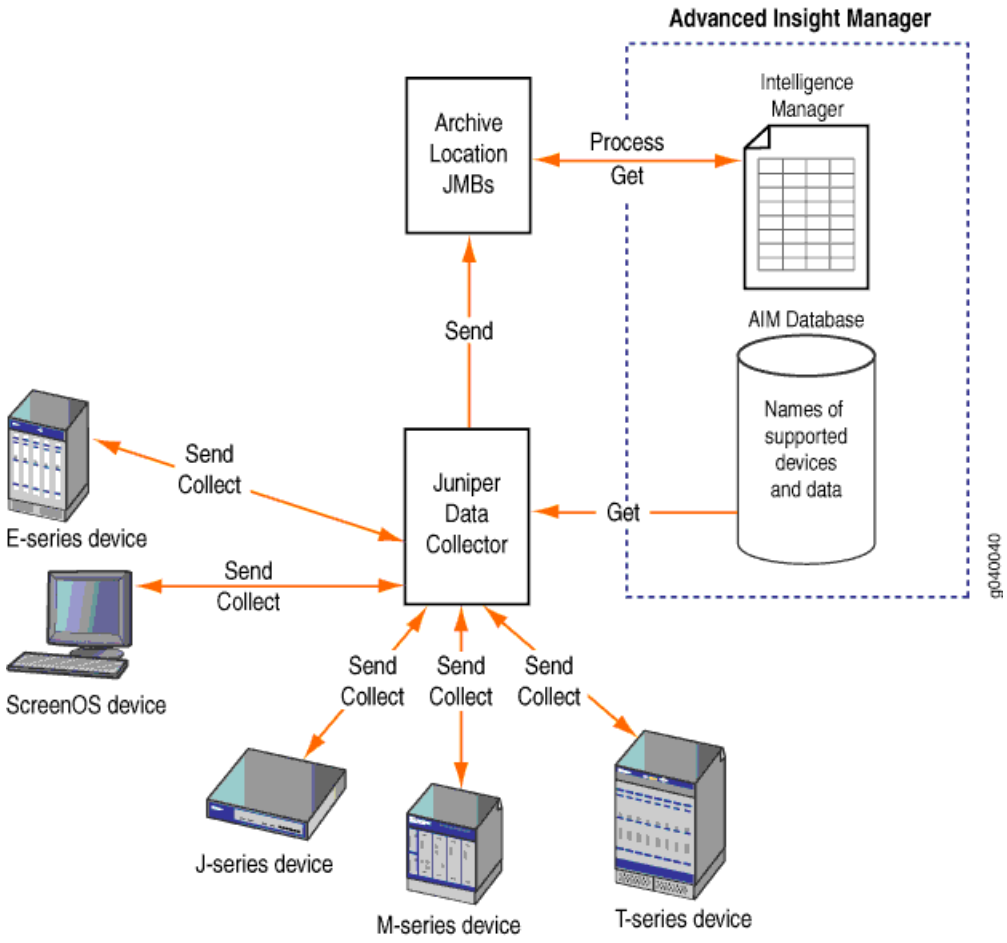
How the Juniper Data Collector Operates

The Juniper Data Collector does the following:

- Collects intelligence data periodically for proactive monitoring
- Packages all required collected data into a Juniper Message Bundle (JMB)
- Transfers the JMB to an archive location or folder on the AIM server (any existing directory with room to collect JMBs).

The Juniper Data Collector operates as follows (see Figure 9 on page 44):

Figure 9: Juniper Data Collector Operation Diagram



1. The Juniper Data Collector gets the configuration information, such as the names of supported devices, from the AIM database.
2. Periodically, the Juniper Data Collector performs a data collection, where it sends JUNOScript XML commands to a device and receives intelligence information that it packages into a JMB.

3. The Juniper Data Collector sends the JMB to an archive location so that AIM can collect and process it.

Creating a Directives Group

For detailed information about creating a directives group, see “Creating a Directives Group” on page 101.

Chapter 6

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 Software.

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: To use AIM and AI-Scripts, you must configure 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 during or after the initial installation, but the components are not really usable until the archive location is configured. You can install AIM and AI-Scripts in any order.

This chapter includes the following sections:

AI-Scripts 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 called 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 your network.

AI-Scripts 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 10 on page 51.

  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 *AI-Scripts Release Notes* at the AIS documentation Web site.
- 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 types of incidents that are detected by a specific AI-Script package, see the *AI-Scripts Release Notes* located on the AIS documentation Web site.

JMB Contents

The JMB 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-Scripts 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 operation (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

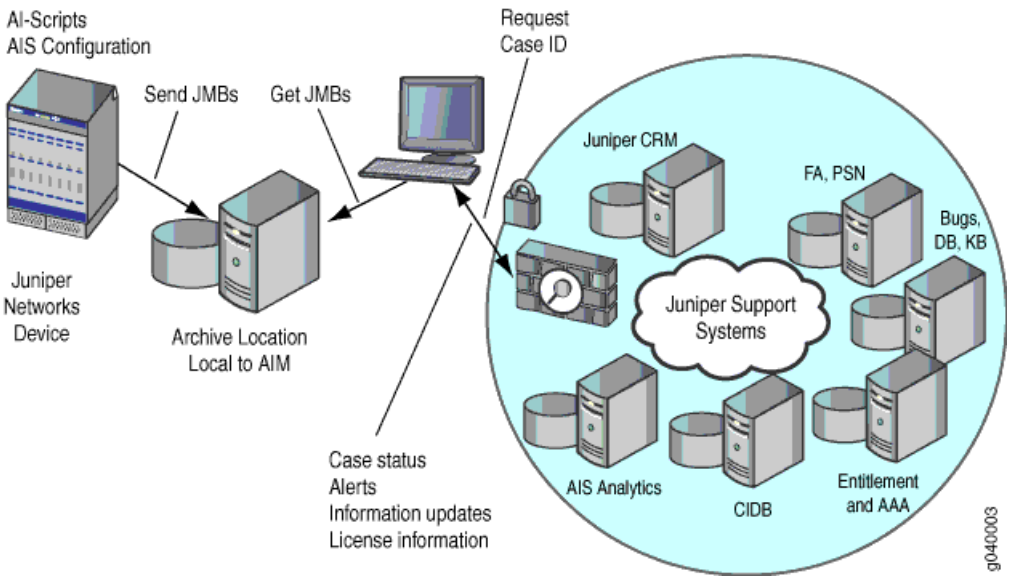
Stylesheet Language Alternative Syntax (SLAX) is a language for writing JUNOS commit and op scripts and is an alternative to Extensible Stylesheet Language Transformations (XSLT). SLAX has a distinct syntax, but the same semantics as XSLT.

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-Scripts Process Flow

Figure 10 on page 51 shows the AI-Scripts process flow.

Figure 10: AI-Scripts Process Flow



The AIM Archive location can either be a local directory on the same system as AIM, or a directory mounted from another system onto the system running AIM. The archive location directory should be used exclusively for JMBs and no other AIM files.

AIM 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-Scripts 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-Script Bundles” on page 53.
- 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 54.

AI-Scripts System Requirements

AI-Scripts run on Juniper Networks J-series, M-series, MX-series, T-series, EX-series, and SRX devices. Ensure that all devices on which you install AI-Scripts are running JUNOS Release 9.0 or later. For the latest AI-Scripts information, see the Advanced Insight Scripts (AI-Scripts) Release Notes.

Downloading AI-Scripts Install Packages and Release Notes

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

To download an AI-Scripts 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-Scripts install package.

   If you are installing an AI-Scripts install package manually, move the package to the /var/sw/pkg directory on the device. If you do not move the AI-Scripts install package to the device, you have to use ftp or scp in conjunction with the request system scripts add command.

   If you will use the JUNOScope software to automatically install a package to a group of devices at once, Download the AI-Scripts install package to the same server as Advanced Insight Manager (AIM).

AI-Scripts 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

- *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 AI-Script files that in 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/
```

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

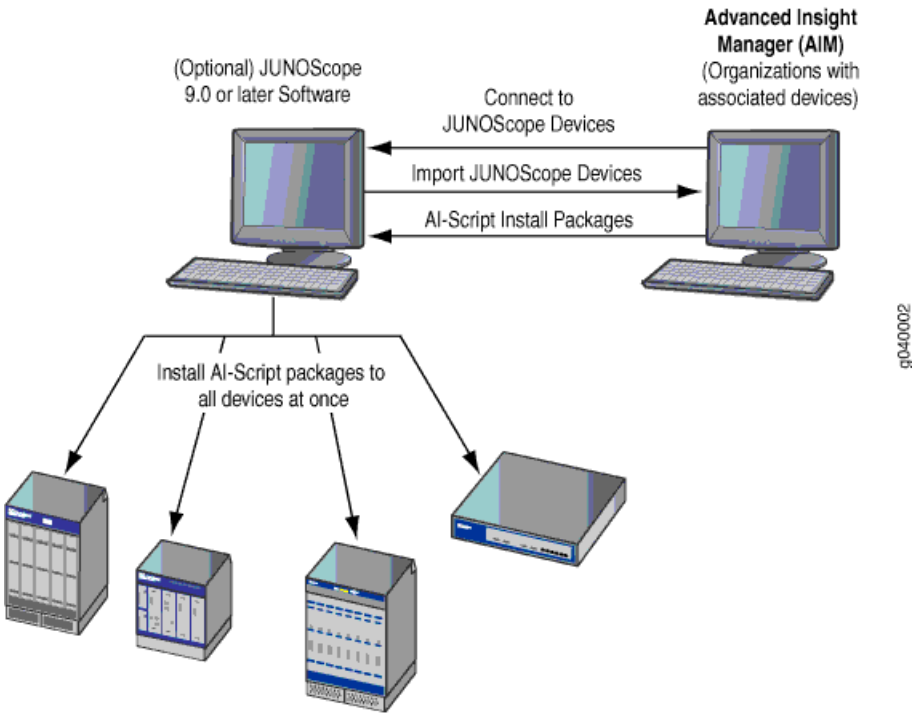
```
/config/scripts
```

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

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 11 on page 54.

Figure 11: 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 71.
2. Import devices that are managed by JUNOScope, see “Configuring JUNOScope Settings” on page 71.
3. Configure Script Bundles, see “Configuring Script Bundle Settings” on page 74.
4. Associate imported devices with a device group, see “Creating Device Groups” on page 98.
5. Configure the Script Bundle of the device group and set the No-copy and Unlink installation attributes, see “Creating Device Groups” on page 98.
6. Add archive locations specifying the upload command password attributes, see “Configuring Archive Locations” on page 114.
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 54.

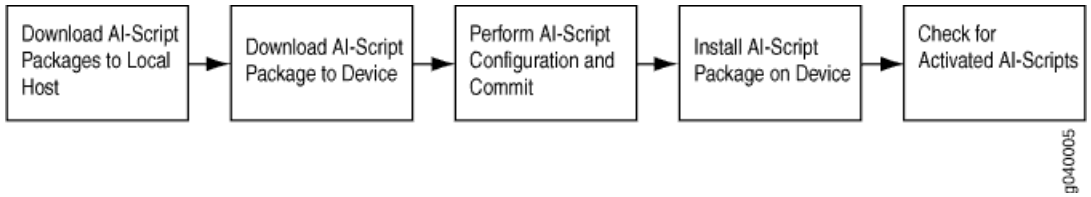
Manually Configuring and Installing AI-Scripts on Devices

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 to which 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 12 on page 55 shows the basic steps you must perform to manually configure and install AI-Scripts to devices.

Figure 12: Basic Steps to Manually Configure and Install AI-Scripts on Devices



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

1. Download the AI-Scripts install packages to the local host, then to the device. See "Downloading AI-Scripts Install Packages and Release Notes" on page 52
2. Configure the device by following these steps:
   a. Enter the configure command or the edit command to enter configuration mode. The CLI prompt changes from user@host> to user@host# and a banner appears to indicate the hierarchy level.
   b. Enter an ais destination under group juniper-ais:

      user@host# **set groups juniper-ais event-options destination juniper-aim {...}**

      This configuration determines the AIS archive location where JMBs are deposited for a device. The group namejuniper-ais is mandatory. The group destination name juniper-aim is mandatory.
   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. The optional setting is mandatory to prevent the configuration from committing if the jais-activate-scripts.slax file is not present. That file is not present until the scripts bundle is installed.
   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 committed configuration (except with a special command).
   e. Apply the juniper-ais group:

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

This configuration applies the configuration 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-flashoption, the system reads AI-Scripts from /config/scripts/ directory otherwise the system reads AI-Scripts from the /var/db/scripts/ directory. The /var/run/scripts directory will always point to the right scripts directory.

3. Verify that the syntax of a configuration is correct by using 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-Scripts Install Packages and Release Notes” on page 52.

7. Install the AI-Script package. (For more information about working with AI-Script packages, see “Working With AI-Scripts” on page 57).

request system scripts add *<package-name>*

8. Verify that the AI-Scripts are activated:

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-pfecrash.slax;
         file problem-event-dcrash.slax;
         file intelligence-event-main.slax;
         file SPD_EVLIB_CREATE_FAILURE.slax;
         file SPD_DAEMONIZE_FAILED.slax;
         file RPD_TASK_FORK.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 roll back AI-Scripts.

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*>**

Upgrading an AI-Script Package

To upgrade an AI-Script package, perform steps 1, 7, and 8 of “Manually Configuring and Installing AI-Scripts on Devices” on page 54.

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 roll back 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 prevent the installer from saving copies of AI-Script jais package files during installation, use the following command:

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

NOTE: If you use the no-copy option during the jais installation, the jaispackage 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.

Chapter 7

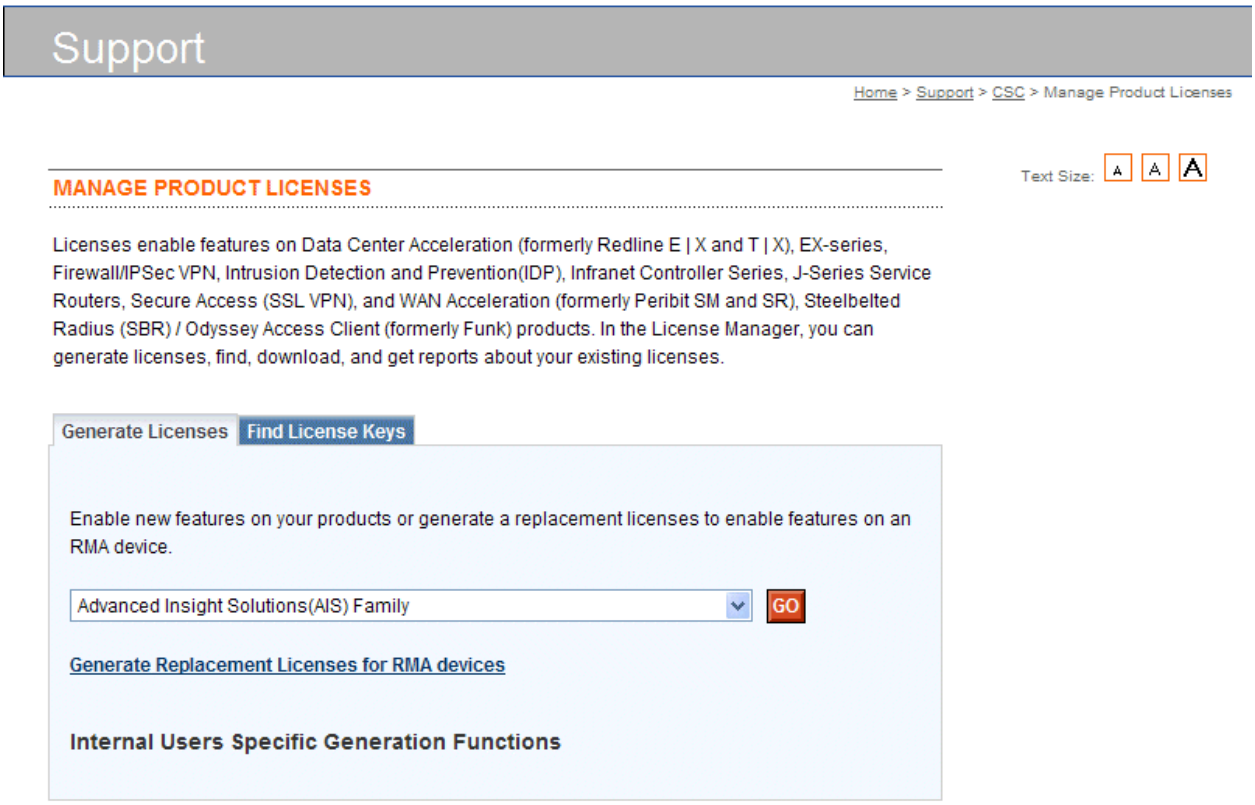
Activating Advanced Insight Solutions

This chapter describes how to activate Advanced Insight Solutions (AIS). The procedure you follow depends on how AIS is deployed and engaged on the network.

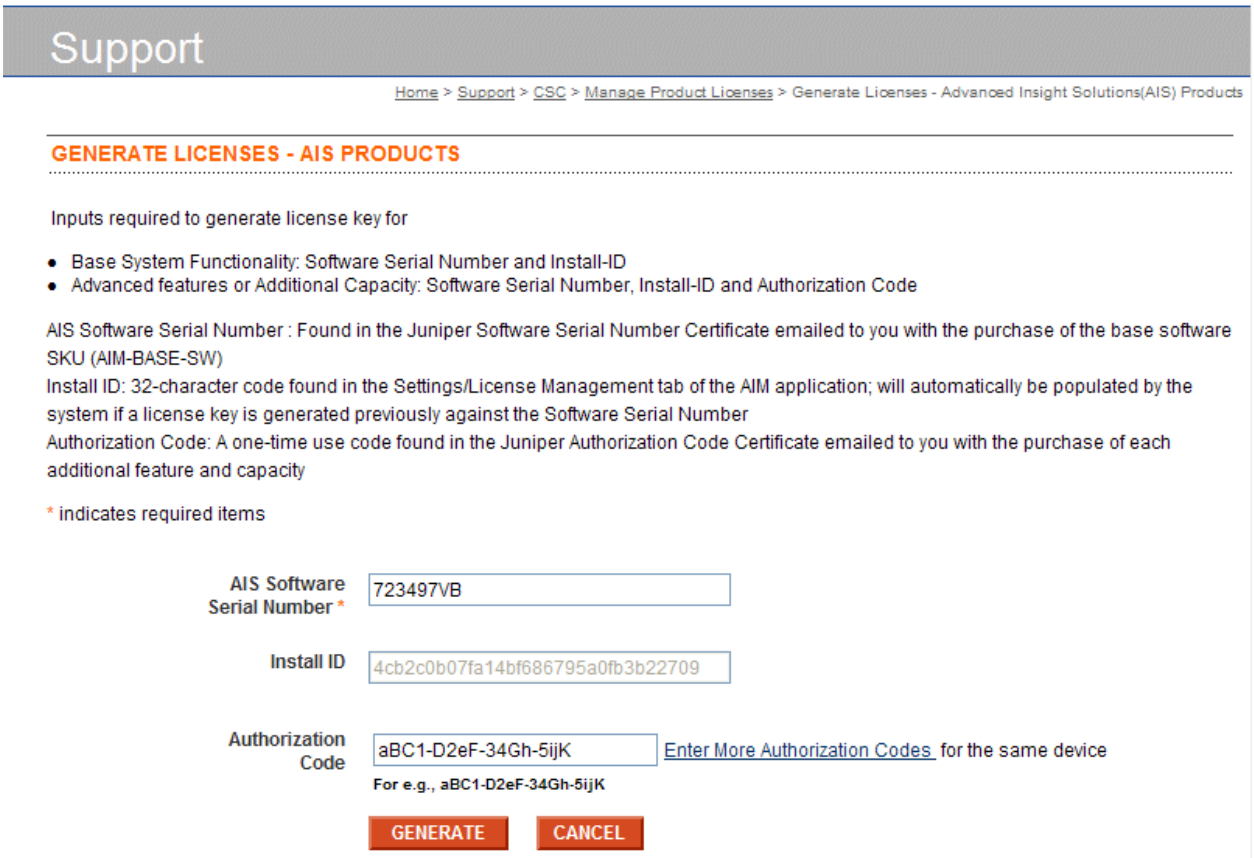
Activating AIS for the Direct Customer (Standard) and Partner Controller Engagement Models

To activate AIS licensing in AIM, follow these steps:

1. Log in to Juniper Networks Customer Support Center (CSC) Web application at https://www.juniper.net/SerialNumberEntitlementSearch/SerialNumberEntitlementAction.do, and verify your AIS product and service contracts.
2. Log in to the Juniper Networks License Management System (LMS) at https://www.juniper.net/lcrs/license.do. The Manage Product Licenses page appears.

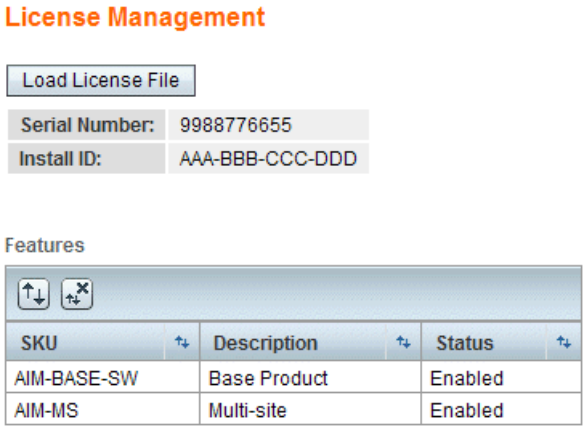


3. On the Generate Licenses tab, select Advanced Insight Solution (AIS) Family from the drop-down list box, and click GO. The Generate Licenses — AIS Products page appears.



4. Enter the AIS software serial number, AIM install ID, and AIS authorization code.
   - AIS Software Serial Number: Found in the Juniper Software Serial Number Certificate e-mailed to you with the purchase of the base software SKU, for example, AIM-BASE-SW.
   - Install ID: A 32-character code found in the AIM Settings > License Management page. The Install ID will automatically be entered by the system if a license key was generated previously against the Software Serial Number Authorization Code.
   - Software Serial Number Authorization Code: A one-time-use code found in the Juniper Authorization Code Certificate e-mailed to you.
5. Click Generate. This action generates the AIS license key file. You receive an e-mail with the AIS license key file attached.
6. Copy the AIS license key file to the root AIM install directory on the AIM operating system.
7. Rename the license file aim_license.

8. Log in to AIM as an admin user. See “Connecting to AIM and Logging In” on page 39.
9. In AIM, click the Settings tab, then click License Management in the navigation area. The License Management page appears.



10. 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 or replace a new AIM license, the functionality it enables is available immediately. You do not have to restart AIM.

For more information about managing licenses and services in AIM, see “Using AIM License Management” on page 83.

Activating AIS for the End-User Engagement Model

This section describes the process of activating AIM for the AIS End-User engagement model. It explains both the end-user and partner responsibilities.

AIS Partner Controller Responsibilities

To activate the end-user AIS product, the partner must follow these steps:

1. The partner sends AIM to the end customer.
2. The end customer installs AIM.
3. The end customer requests AIS services from the partner and provides the AIM install ID.
4. The partner requests an end-user license from Juniper Networks.
5. The partner, with AIM administrative privileges creates a new Proxy device group that is contained by a currently defined AIM organization in Settings > Organizations using the following settings:

- Alias
- Customer username (up to 128–character username for communication between the end-user and partner AIMs)
- Customer password (up to 32–character password for communication between the end-user and partner AIMs)
- Archive location for depositing customer JMBs

6. On the Organizations Credentials page, click Save Credentials.
7. The partner provides the end customer with the following:
   - Name—An alias used to create a proxy device group.
   - User name—A name used to create a proxy device group.
   - User password—A password used to create a proxy device group.
   - AIS license key license file—The aim_licensefile

AIS End-User Responsibilities

To activate AIS, the end user must follow these steps:

1. Request AIS service from your partner.

   The partner sends you the following information:
   - AIM software
   - Partner controller URL for AIM
   - Name
   - User name
   - User password
   - AIS license key license file (aim_license)
2. Install and start AIM.
3. The customer sends the AIM install ID to the partner.
4. Log in to AIM using the default username and password (admin/aimadmin) credentials.
5. The customer copies the aim_license license file to the root AIM install directory (for example/opt/aim).
6. In AIM, the customer navigates to Settings > License Management and clicks Load License File.
7. In AIM, the customer navigates to Setting > Organizations to add a new organization using the information from the partner.
8. Import the aim_license file.
9. In AIM, navigate to Settings > General Settings and adds the partner's URL.

On the Organizations page, the customer clicks Save Credentials. The action validates the organization credentials at the partner controller. For more information about creating organizations, see “Configuring AIM Organizations and Device Groups” on page 91

Part 3
Setting Up Advanced Insight Manager

Chapter 8

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 you 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:

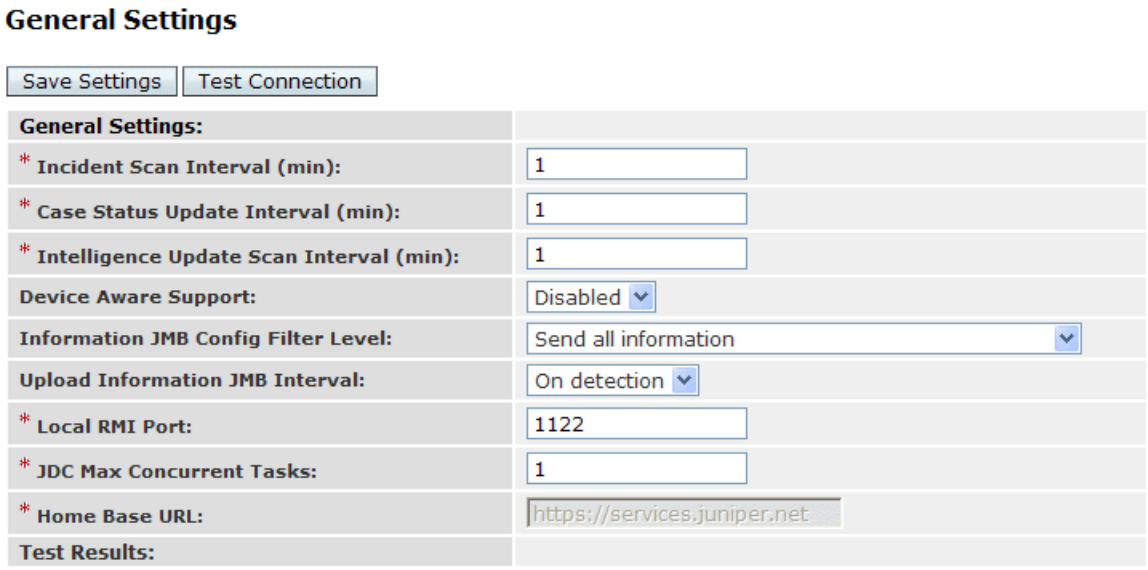
- Set the interval used by AIM to scan device archive locations for Juniper Message Bundles (JMBs).
- Set the interval used by AIM to poll JSS for case status updates.
- Set the interval used by AIM to poll JSS for intelligence updates specific to your site.
- Set the amount of information sharing included in informational JMBs. The default is Send only configuration indexes, which indicates the technologies present in the device configuration. (See “JMB Send Only Configuration Indexes Filter

Example” on page 70 for an example of the JMB Send only configuration indexes output.)

- 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. In AIM, click the Settings Tab. The General Settings page appears.



2. Add the required AIM General settings. See “AIM General Settings Page Description” on page 68.
3. Test the AIM connection settings. If the test is unsuccessful, check to see that you entered the correct Home Base URL.
4. 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 Page Description

Table 13 on page 68 describes the General Settings page command button.

Table 13: 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 14 on page 69 describes the AIM General Settings parameters.

Table 14: 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 JSS 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
Device Aware Support	Enables intelligence JMBs to flow to JSS, filtered according to the Information JMB Config Filter Level option selected. The default is Disabled, which allows no intelligence JMBs to be sent to JSS unless the Pro Service license exists. JSS accepts information JMBs regardless of Base or Pro Service. Information JMBs are counted against the device capacity licenses in AIM.	AIM Admin Settings	Enabled or Disabled	Disabled
Information JMB Config Filter Level	Specifies the amount of device configuration information in Juniper Message Bundles to share with Juniper: ■ Do not send—Sends no configuration information. ■ Send all information except configuration—Sends all device information except the configuration. ■ Send only configuration indexes—Sends only the device configuration technologies. (See "JMB Send Only Configuration Indexes Filter Example" on page 70 ■ Send all information with IP Addresses overwritten—Sends all device information, without IP addresses ■ Send all information—Sends all device information.	AIM Admin Settings	N/A	Do not send

Table 14: General Settings Parameters *(continued)*

Name	Description	Privileges	Range/Length	Default
Upload Information JMB Interval	Interval used to send any newly detected Intelligence JMBs to JSS: ■ 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
JDC Max Concurrent Tasks	Specifies the number of concurrent Juniper Data Collector tasks working in parallel to collect information from devices.	AIM Admin Settings	Up to 50	1
Home Base URL	The location where information JMBs are sent. If you load a Partner Controller license file, this URL is defaulted to JSS (https://services.juniper.net). If you run AIM in Direct customer mode, enter https://services.juniper.netIf you run AIM in End Customer mode, enter the partner's https URL (for example, https://*juniperpartner*.com:8443).	AIM Admin Settings	Enabled or Disabled	Disabled for Standard and Partner Controller AIM modes. Enabled for AIM End Customer mode.
Test Results	Displays the results of AIM General Settings to connect to JSS or a AIM partner.	■ Success - URL is responsive ■ No route to host ■ Connection refused ■ The Home Base server is temporarily unable to service your request	N/A	Blank

JMB Send Only Configuration Indexes Filter Example

If you select the Send Only Configuration Indexes Information JMB Config Filter Level option in AIM General Settings, the device configuration output displays only the

hierarchy tags. The following is an example of the Send Only Configuration Indexes option output.

```
- <attachment>
    <name>show configuration</name>
  - <output>
    - <![CDATA[
        <configuration>
            <version>9.1R1.8</version>
            <system>
        <host-name></host-name>
        <domain-name></domain-name>
        <domain-search></domain-search>
        <domain-search></domain-search>
        <backup-router>
        <address></address>
        </backup-router>
        <time-zone></time-zone>
        <undocumented><debugger-on-break/></undocumented>
        <undocumented><dump-on-panic>
        </dump-on-panic></undocumented>
        <ports>
        <auxiliary>
        <disable/>
        </auxiliary>
        </ports>
        <root-authentication>
        <encrypted-password></encrypted-password>
        </root-authentication>
        <name-server>
        <name></name>
        </name-server>
        <name-server>
        <name></name>
        </name-server>
        ...
```

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

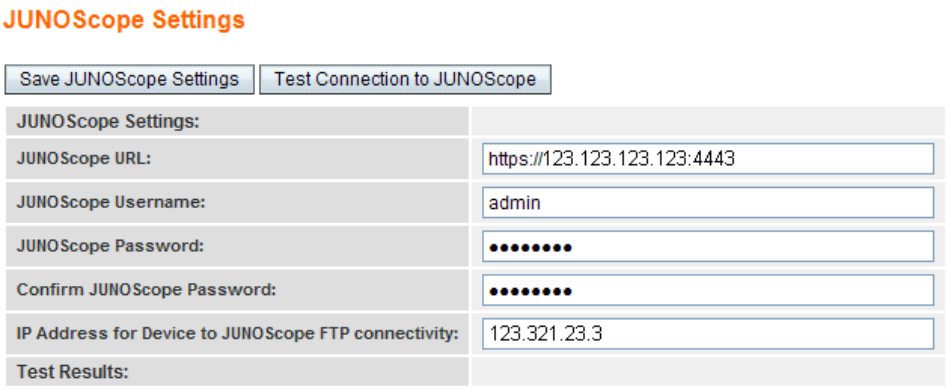
The AIM administrator must set up JUNOScope Settings before devices can be imported from JUNOScope. Devices appear in the Devices table when you click Import JUNOScope devices in the Devices Managed by JUNOScope table.

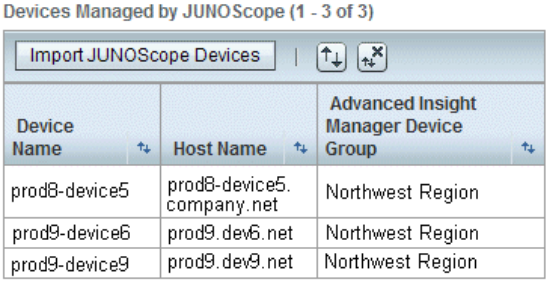
The AIM administrator can import all devices that are managed by the JUNOScope software. Only devices imported from JUNOScope will have JUNOScope Script Management capabilities, which include:

- 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 73.
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 74.

JUNOScope Settings Table Description

Table 15 on page 73 describes the JUNOScope Settings command buttons.

Table 15: 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 admin privileges	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 16 on page 73 describes the JUNOScope Settings table fields.

Table 16: 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 17 on page 74 describes the Devices Managed by JUNOScope table command button.

Table 17: 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 18 on page 74 describes the Devices Managed by JUNOScope table fields.

Table 18: Devices Managed by JUNOScope Parameter Descriptions

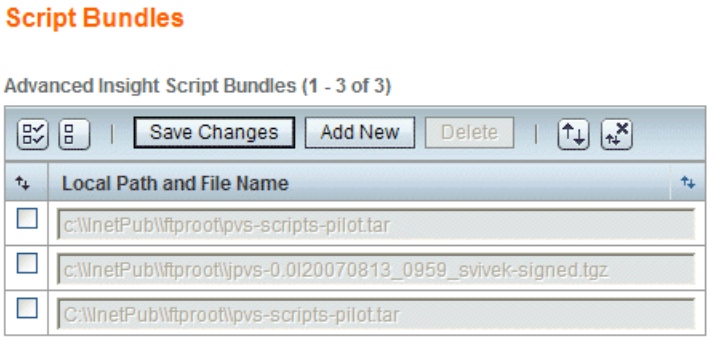
Name	Description	Privileges	Range/Length	Default
Device Name	Name JUNOScope user assigned this device.	Not allowed to modify	N/A	N/A
Host Name	Identifier used for network communication between JUNOScope and the JUNOS device. For example, it can be a hostname (host-name.juniper.net) or an IP address.	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 98.	Not allowed to modify	N/A	N/A

Configuring Script Bundle Settings

Script Bundle settings provide 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 98.

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 "Script Bundles Table Description" on page 75.
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 "Script Bundles Table Description" on page 75.

NOTE: You cannot modify a script bundle after 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 Table Description

Table 19 on page 75 describes the command buttons on the Script Bundles page.

Table 19: Script Bundles Table 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 admin privileges	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 admin privileges	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 admin privileges	Selected items are removed from the table.

Table 20 on page 76 describes the Script Bundles location on the local host where AIM is installed.

Table 20: Script Bundles Table Row Description

Name	Description	Privileges	Range/Length	Results
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 after 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 9

Using AIM Log Viewer

This chapter describes the AIM Log Viewer that allows you to view log files for monitoring and troubleshooting AIM operations. Each AIM log is represented by a tab in the viewer. AIM logs are located in the /opt/aim/data/logs/ subdirectory where you installed AIM.

You can modify AIM log file settings, such as priority level, the number of backup files that can be created, the maximum log file size, and the rollover interval for when a new log file is created.

You must have Admin privileges to use AIM Log Viewer.

Viewing a Log In Log Viewer

To view an AIM log file in Log View, follow these steps:

1. Click Settings > General > Logging. The AIM Log View main page appears with no logs selected.
2. Select the tab for the AIM log file you want to view. This chapter includes the following logs:

AIM Messages Exchange Log (AIManagerMSG Tab)

Filename

AIManagerMSG.log

Description

This log file tells the time specific events occur. For example (there are more than the following):

- Create case request
- Update intelligence info
- Validate login
- Retrieval of home base status
- When settings on the General Settings page have been saved, causing updates to the AIM Service
- How many informational and alert messages are retrieved from JSS
- When a case is created in Clarify
- When a case has been updated in Clarify

Sample

```
2008-06-05 12:44:57,087 INFO  [JPvSService] Received request for GetCaseStatus
2008-06-05 12:44:57,140 DEBUG [JPvSService] xmlToSend = <JSServiceRequest
xmlns="http://juniper.net/pvs/domain">
  <MsgVersion>1.0</MsgVersion>
  <JSHeader>
    <security>
      <username>foo@bar.com</username>
      <Password Removed from display>
    </security>
    <ServiceTxn>
      <ServiceName>PvSProbMgmtSvc</ServiceName>
      <ServiceVersion>1.0</ServiceVersion>
      <ServiceMethod>GetCaseStatus</ServiceMethod>
    </ServiceTxn>
  </JSHeader>
  <payload>
    <GetCaseStatusRequest>
      <SiteId>123</SiteId>
      <CaseIds>
        <id>2008-0522-1234</id>
        <id>2008-0523-2345</id>
        <id>2008-0524-3456</id>
        <id>2008-0525-4567</id>
        <id>2008-0526-5678</id>
        <id>2008-0527-6789</id>
        <id>2008-0528-7890</id>
        <id>2008-0529-8901</id>
        <id>2008-0530-9012</id>
        <id>2008-0531-0123</id>
        <id>2008-0601-1234</id>
      </CaseIds>
    </GetCaseStatusRequest>
  </payload>
</JSServiceRequest>
```

AIM JMB Log (AIManagerJMB Tab)

Filename

AIManagerJMB.log

Description

This log file contains entries detailing what time a JMB was processed and the reason (if any) that it was rejected.

Sample

```
2008-06-04 15:59:08,588 INFO  [ProcessPRB] New PRB file
:/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080603_225828.xml
2008-06-04 15:59:08,601 INFO  [ProcessPRB] Executing the following Command:
2008-06-04 15:59:08,601 INFO  [ProcessPRB] /bin/ksh /opt/aim/bin/sedExec.ksh
/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080601_030150
2008-06-04 15:59:13,685 INFO  [ProcessPRB] New PRB file
:/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080601_030150.xml
2008-06-04 15:59:13,693 INFO  [ProcessPRB] Executing the following Command:
2008-06-04 15:59:13,694 INFO  [ProcessPRB] /bin/ksh /opt/aim/bin/sedExec.ksh
/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080603_225501
2008-06-04 15:59:18,757 INFO  [ProcessPRB] New PRB file
:/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080603_225501.xml
2008-06-04 15:59:18,911 INFO  [EventPRB] File is processed and saved to db
:/var/ftp/sv_aimdev2/bones_ais_intel_20080604_225211.xml
2008-06-04 15:59:18,981 INFO  [EventPRB] File is processed and saved to db
:/var/ftp/sv_aimdev2/bones_ais_intel_20080527_235117.xml
2008-06-04 15:59:19,122 INFO  [EventPRB] File is processed and saved to db
:/var/ftp/sv_aimdev2/bones_ais_intel_20080528_042312.xml
2008-06-04 15:59:19,371 INFO  [EventPRB] File is processed and saved to db
:/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080603_225716.xml
2008-06-04 15:59:19,414 INFO  [EventPRB] File is processed and saved to db
:/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080603_225828.xml
2008-06-04 15:59:19,498 INFO  [EventPRB] File is processed and saved to db
:/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080601_030150.xml
2008-06-04 15:59:19,573 INFO  [EventPRB] File is processed and saved to db
:/var/ftp/sv_aimdev3/Pluto-re0_ais_intel_20080603_225501.xml
2008-06-04 15:59:19,724 INFO  [EventPRB] New Info JMB added to incident ![324,
325, 326, 327, 328, 329, 330]
2008-06-04 15:59:19,724 INFO  [EventPRB] Scan for JMB !
2008-06-04 16:00:02,329 INFO  [EventPRB] Scan for JMB !
2008-06-04 16:01:02,330 INFO  [EventPRB] Scan for JMB !
2008-06-04 16:02:02,330 INFO  [EventPRB] Scan for JMB !
2008-06-04 16:03:02,331 INFO  [EventPRB] Scan for JMB !
```

AIM Policy Log (AIManagerPolicy Tab)

Filename

AIManagerPOLICY.log

Description

This log file contains messages about when a Reaction Policy has been triggered and what action was taken when it occurred, for example, an e-mail was sent, a trap message was sent.

Sample

```
2008-06-04 19:08:55,878 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:08:55,884 DEBUG [PolicyEngine] Policy ID :8
2008-06-04 19:09:55,978 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:09:55,986 DEBUG [PolicyEngine] Policy ID :8
```

```
2008-06-04 19:10:55,841 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:10:55,846 DEBUG [PolicyEngine] Policy ID :8
2008-06-04 19:11:55,978 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:11:55,983 DEBUG [PolicyEngine] Policy ID :8
2008-06-04 19:12:55,997 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:12:56,005 DEBUG [PolicyEngine] Policy ID :8
```

Juniper Data Collector Log (AIMJDC Tab)

Filename

AIMJDC.log

Description

This log contains information and error messages for all communication between the Juniper Data Collector and Juniper Networks network devices, such as routing platforms, switches, and firewalls. It also shows the queuing tasks for all the events.

Sample

```
2008-08-12 00:03:52,095 INFO  [SshSession] ExitCode: null
2008-08-12 00:03:52,165 INFO  [JobExecution] Removed event from jobQueue :3
2008-08-12 00:19:18,677 ERROR [JmbProcessor] Unable to connect to device
172.19.57.74 -- jdc ssh connect failed 172.19.57.74 There was a problem while
connecting to 172.19.57.74:22
2008-08-12 00:19:18,678 INFO  [JobExecution] Removed event from jobQueue :5
2008-08-12 00:19:25,058 ERROR [JmbProcessor] Unable to connect to device
172.19.57.169 -- jdc netconf connection error 172.19.57.169
2008-08-12 00:19:25,059 INFO  [JobExecution] Removed event from jobQueue :4
2008-08-13 00:00:00,018 INFO  [QueueTask] QueueTask is executing.
2008-08-13 00:00:00,021 INFO  [QueueTask] Queueing for eventId: 0
2008-08-13 00:00:00,023 INFO  [QueueTask] QueueTask is executing.
```

Modifying AIM Log Settings

The AIM Log Viewer allows you to modify AIM log file settings, including priority level, the number of backup files that can be created, the maximum log file size, and the rollover interval for when a new log file is created. For more details on configuring AIM log settings, see “AIM Log Viewer Page Parameters” on page 80

AIM Log Viewer Page Parameters

AIM Log Viewer Button Descriptions

Table 21 on page 80 describes the AIM Log Viewer button operation.

Table 21: AIM Log View Button Descriptions

Name	Description	Privilege Required	Enabled/Disabled	Results
Save Changes	Saves changes to the AIMLog.xml file on the server.	Admin	Enabled if the user has privileges	Changes are set in the running AIMLog.xml file and the running AIM Service or JDC Service.

Table 21: AIM Log View Button Descriptions *(continued)*

Name	Description	Privilege Required	Enabled/Disabled	Results
Refresh	Displays the most current selected AIM log file.	Admin	Enabled if the user has privileges	Displays the most current selected AIM log file.
Clear Logs	Deletes the selected AIM log file.	Admin	Enabled if the user has privileges	Deletes the selected AIM log file.

AIM Log View Field Descriptions

Table 22 on page 81 describes the AIM Log View field parameters.

Table 22: AIM Log Viewer Field Descriptions

Name	Description	Priviledge	Range/Length	Default
Priority	Sets the priority setting for log files: ■ Debug ■ Info ■ Warning ■ Error	Admin	■ Debug ■ Info ■ Warning ■ Error	Info
Backup File Count	Sets the maximum number of backup log files AIM will create. The index represents the number of files saved for the log file, for example: ■ AIManagerJMB.log1 ■ AIManagerJMB.log2 and so on,	Admin	1–500	1
Max File Size (KB)	Sets the maximum size a file is allowed to grow before rilling the log file to a new one	Admin	1024 to 2,097,152 KB (2 Gigs)	1024 KB
Date Pattern	Sets the roll over interval for when a new log is created.	Admin	■ None ■ Monthly ■ Weekly ■ Daily ■ Twice Daily ■ Hourly ■ Every Minute	None

Chapter 10

Using AIM License Management

When you purchase Juniper Networks J-Care Technical Services, AIS is available. The level of J-Care Technical Services that you purchase determines the level of AIS functionality (AI-Scripts, AIM, and JSS) that is available for you to use. See “Juniper Networks J-Care Technical Services and AIS Functionality” on page 8.

This chapter assumes that your J-Care Technical Services order has been processed and that you have the appropriate and valid AIS authorization codes to generate an AIS license file using the Juniper Networks License Management System Web application. It also describes how to activate your AIS licensing.

AIM runs in three operational modes that requires a license to operate:

- Base (Direct Customer)—the customers's AIM connects directly to JSS.
- Partner Controller—the partner's AIM allows the partner to create end user AIM sites and determine what information should flow to and from the end user's AIM.
- End User—The end user must be involved with a Juniper Networks partner. The end users AIM sends and receives information from the partner's AIM. The partner controls what information flows from the end user to JSS (with the exception of information JMBs.

AIM Admin Settings privileges are required to manage AIS licensing and services using AIM.

This chapter includes the following sections:

J-Care Technical Services Required for AIS

To access the full capabilities of AIS, you must order the appropriate J-Care Technical Support Services. For more information about the J-Care Technical Services licensing required for AIS functionality, see “Juniper Networks J-Care Technical Services and AIS Functionality” on page 8.

AIM Licensing

AIM requires a combination of J-Care Technical Services, AIM feature licenses, and device capacity licenses achieve full functionality.

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 J-Care Technical Services contract..

Table 23: 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. The maximum capacity for each AIM installation is 1000 devices.	Required

Using AIM License Management

To use AIM past the 60–day demo mode period and to activate AIS functionality ordered, you must load the AIM license file. This section describes how to activate the AIM license file representing all AIM product elements and how to manage AIM feature, device capacity, and J-Care Technical Services licenses.

- Using the AIM Licensing Page on page 84
- Managing Device Capacity Licenses on page 86
- Managing J-Care Technical Services on page 88

Using the AIM Licensing Page

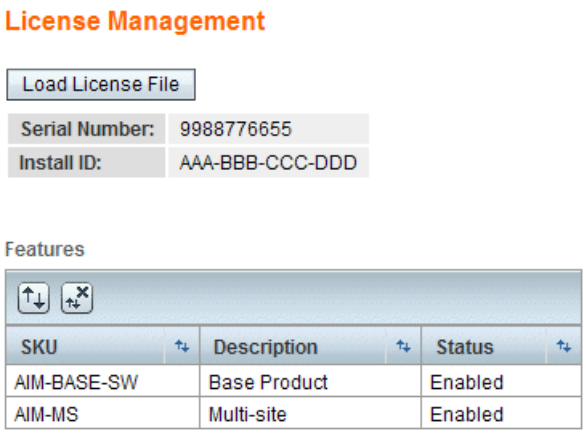
The AIM License Management page displays:

- The AIM product serial number
- The install ID
- The AIM feature licenses enabled

Using the AIM License Management Page, you can also load the AIS license file that you generated from the Juniper Networks License Management System (LMS) Web application.

To view the AIM License Management Page, do the following:

1. In AIM, click the Settings tab.
2. Click License Management in the navigation area. The License Management page appears.



In AIM demo mode, the following message appears in the License Management 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.

For a description of the license management page elements, see “License Management Page Element Descriptions” on page 85.

For more information about loading the AIS license key file, see “Activating Advanced Insight Solutions” on page 59.

License Management Page Element Descriptions

Table 24 on page 85 describes the License Management page elements.

Table 24: License Management Command Buttons and Field Descriptions

Element Name	Description	Privileges
Load License File button	Loads the license file sent to you by Juniper Networks.	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 25 on page 86 describes the AIM Features table columns.

Table 25: AIM License Management 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

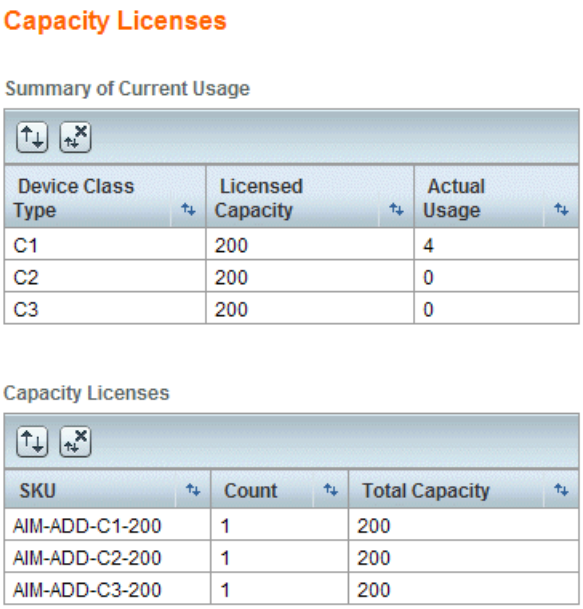
Managing Device Capacity Licenses

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

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 using AIM to manage four Class 1 devices.



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 87.

Capacity Licenses Table Column Descriptions

Table 26 on page 87 describes the columns in the Summary of Current Usage table.

Table 26: Summary of Current Usage Table Column Descriptions

Name	Description
Device Class Type	Identifies the Juniper Networks device class.
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 27 on page 87 describes the columns in the Capacity Licenses table.

Table 27: Capacity Licenses Table Column Descriptions

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

AIM Device Capacity Licenses Messages

The following type of message appears on the Capacity Licenses page when device usage of capacity exceeds 100%:

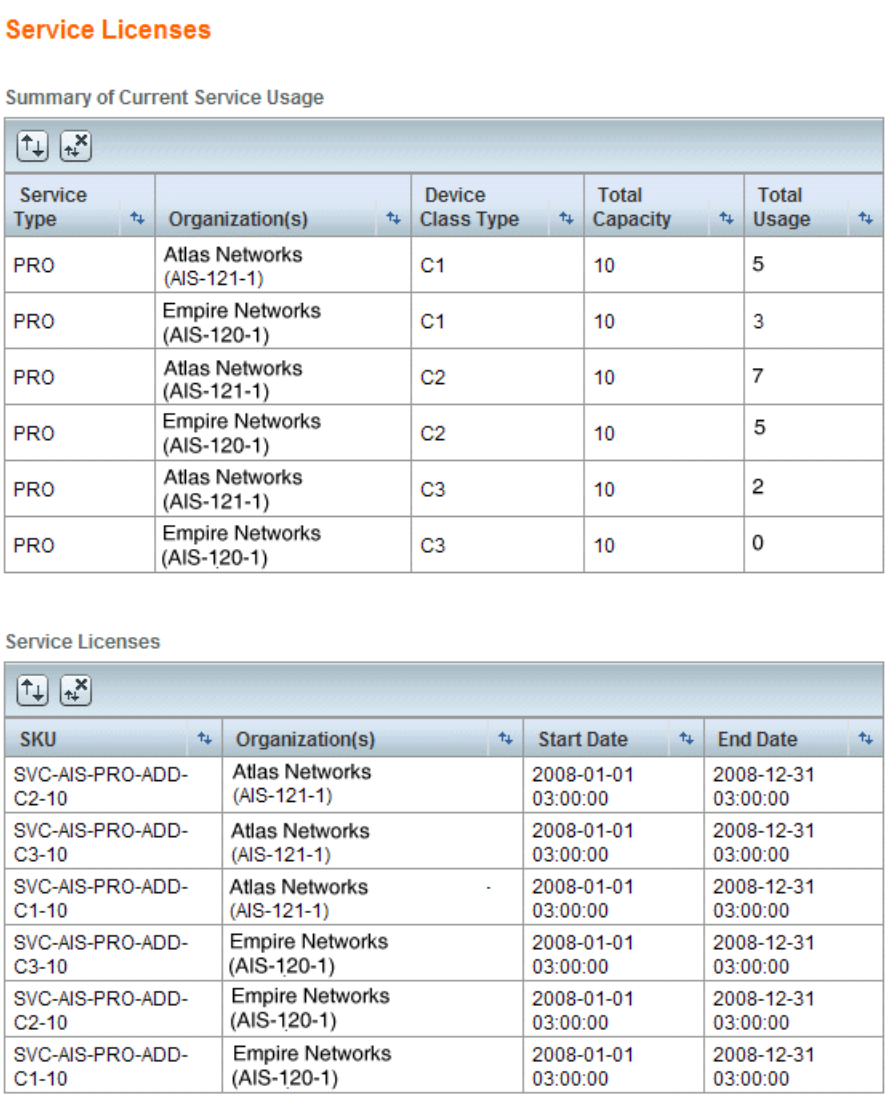
Device Capacity Exceeded for Device Class C3. Additional AIM-ADD-C3-n license required. Please contact Juniper Support to Purchase more licenses.

Managing J-Care Technical Services

The Services Licenses page Summary of Current Service Usage table displays the type of J-Care Technical Service ordered, the device classes allowed to participate in the AIS service, the total number of 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 Service Licenses (under License Management in the navigation area). The Service Licenses pages appears.



Service Licenses

Summary of Current Service Usage

Service Type	Organization(s)	Device Class Type	Total Capacity	Total Usage
PRO	Atlas Networks (AIS-121-1)	C1	10	5
PRO	Empire Networks (AIS-120-1)	C1	10	3
PRO	Atlas Networks (AIS-121-1)	C2	10	7
PRO	Empire Networks (AIS-120-1)	C2	10	5
PRO	Atlas Networks (AIS-121-1)	C3	10	2
PRO	Empire Networks (AIS-120-1)	C3	10	0

Service Licenses

SKU	Organization(s)	Start Date	End Date
SVC-AIS-PRO-ADD-C2-10	Atlas Networks (AIS-121-1)	2008-01-01 03:00:00	2008-12-31 03:00:00
SVC-AIS-PRO-ADD-C3-10	Atlas Networks (AIS-121-1)	2008-01-01 03:00:00	2008-12-31 03:00:00
SVC-AIS-PRO-ADD-C1-10	Atlas Networks (AIS-121-1)	2008-01-01 03:00:00	2008-12-31 03:00:00
SVC-AIS-PRO-ADD-C3-10	Empire Networks (AIS-120-1)	2008-01-01 03:00:00	2008-12-31 03:00:00
SVC-AIS-PRO-ADD-C2-10	Empire Networks (AIS-120-1)	2008-01-01 03:00:00	2008-12-31 03:00:00
SVC-AIS-PRO-ADD-C1-10	Empire Networks (AIS-120-1)	2008-01-01 03:00:00	2008-12-31 03:00:00

For more information about the Summary of Current Service Usage table and the Service Licenses table, see “Service Licenses Table Column Descriptions” on page 89.

Service Licenses Table Column Descriptions

Table 28 on page 89 describes the columns in the Summary of Current Usage table.

Table 28: 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.	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 29 on page 89 describes the columns in the Summary of Current Usage table.

Table 29: Summary of Current Service Usage Table Column Descriptions

Name	Description	Default
SKU	Shelf Keeping Unit. Code that identifies the name of the AIS service subscription purchased	Display only column
Start Date	The date the AIS service subscription was purchased	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 type of 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 11

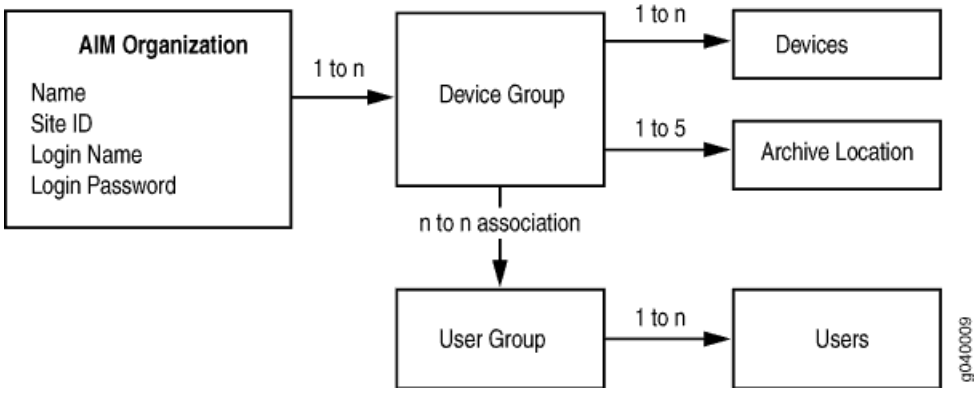
Configuring AIM Organizations and Device Groups

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 sites.

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 agreement to share confidential device information with JSS before proceeding. The site ID is an identifier used in the JSS 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 13 on page 91.

Figure 13: AIM Organization Creation Rules Diagram



Device groups are used to partition devices within one Organization. For more information about setting up a device group, see “Creating Device Groups” on page 98.

Device groups are also used in conjunction with user groups to limit the access of users to certain groups of devices. See “Advanced Insight Solutions Overview” on page 3.

AIM allows you to create several types of device groups:

- Device (Administrative)—A device group, visible in all AIM modes of operation, for devices upon which administrative AIM operations can be performed. A device can belong to only one device group.
- Directives—A devices group for devices supported by the Juniper Data Collector.
- Proxy—A device group that contains a Juniper partner's end customer. A proxy device group provides a way for the partner to control the incident and intelligence information that flows two and from an end customer. For each proxy device group, the partner should create a unique archive location for JMBs.

While you configure organizations or are running AIM in a preproduction environment, you can run AIM in test mode to avoid submitting production incident cases to JSS. The synopsis of any case sent to JSS will be prepended with [Test Case]. No JMBs will be sent while an organization is in test mode.

While creating an AIM organization, you can register for and associate JSS alerts. When alerts are registered through AIM, instead of you receiving e-mail messages, the alert messages are received by AIM and displayed in Intelligence Manager. See “Associating Registered Alerts to an Organization” on page 122.

(Optional) Using the AIM organization user interface, you can have AI-Script bundles automatically installed on multiple devices at once as long as the JUNOScope software is installed. AIM communicates with JUNOScope to install AI-Script bundles on devices that are managed by JUNOScope. To configure auto installation of AI-Script bundles to devices, see “Automatically Installing AI-Script Bundles” on page 53.

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

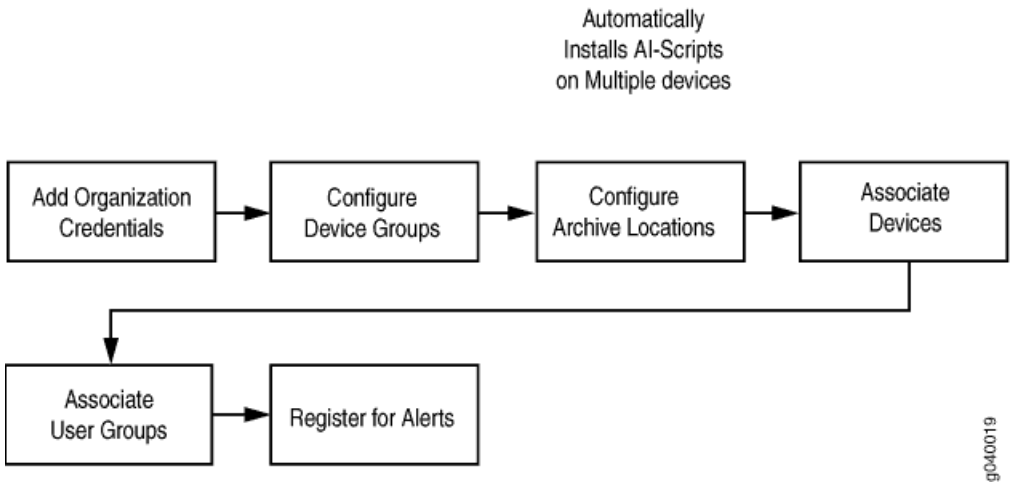
Perform the following before creating an AIM Organization:

- Obtain a Site ID from Juniper Networks, as described in “Activating Advanced Insight Solutions” on page 59.
- Obtain the username and password for the site from Juniper Networks, as described in “Activating Advanced Insight Solutions” on page 59.
- Download AI-Scripts Install Packages from the Juniper Networks Website to the local host file system, as described in “Configuring Script Bundle Settings” on page 74.
- (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. See “Configuring Script Bundle Settings” on page 74.
- 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). See “Configuring JUNOScope Settings” on page 71.
- (Optional) In Settings > JUNOScope Settings: Devices Managed by JUNOScope settings, import Devices imported from JUNOScope. See “Configuring JUNOScope Settings” on page 71
- Add AIM users, as described in “Adding a AIM User” on page 138
- Add AIM User groups, as described in “Creating a New User Group” on page 145
- Associate AIM users with user groups, as described in “Creating a New User Group” on page 145

Organization Configuration Sequence

Figure 14 on page 93 shows the sequence required to create an organization.

Figure 14: AIM Organization Configuration Sequence



For more information about configuring AIM organizations, see:

- Adding Organization Credentials on page 95
- Creating Device Groups on page 98
- Configuring Archive Locations on page 114
- Associating Devices to a Device Group on page 118
- Associating User Groups to Device Groups on page 121
- Associating Registered Alerts to an Organization on page 122

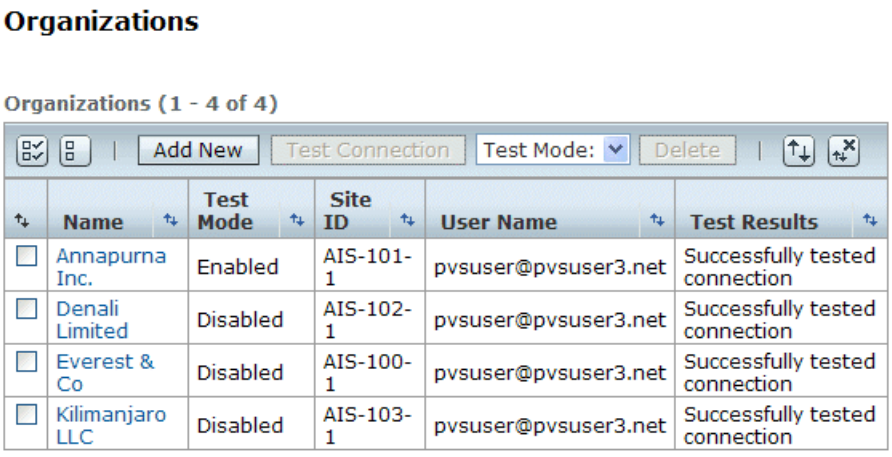
Running AIM Organizations In Test Mode

While creating an AIM organization with device groups or proxy device groups, you can enable a test mode that prevents AIM from submitting production incident cases to JSS. The synopsis of any incident sent to JSS from an organization in test mode will be prepended with [Test Case]. No informational JMBs are sent to JSS from devices that are associated to an organization in test mode.

You can enable test mode for one or more organizations from the Organizations table (see"Organizations Table Description" on page 126) or for the current organization from the Organization Credentials dialog box (see "Organization Credentials Page Description" on page 97).

To place an organization in test mode, follow these steps:

1. Click Settings > Organizations. The Organizations table appears. If the Organizations table is empty, see "Adding Organization Credentials" on page 95.

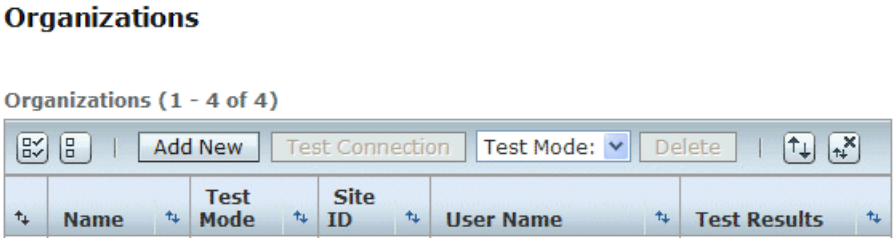


2. Select one or more organizations.
3. In the Organization table, select Enable from the Test Mode drop-down list box. This action places that organization as well as any proxy organizations (represented by Proxy Device Group) under that organization into test mode.

Adding Organization Credentials

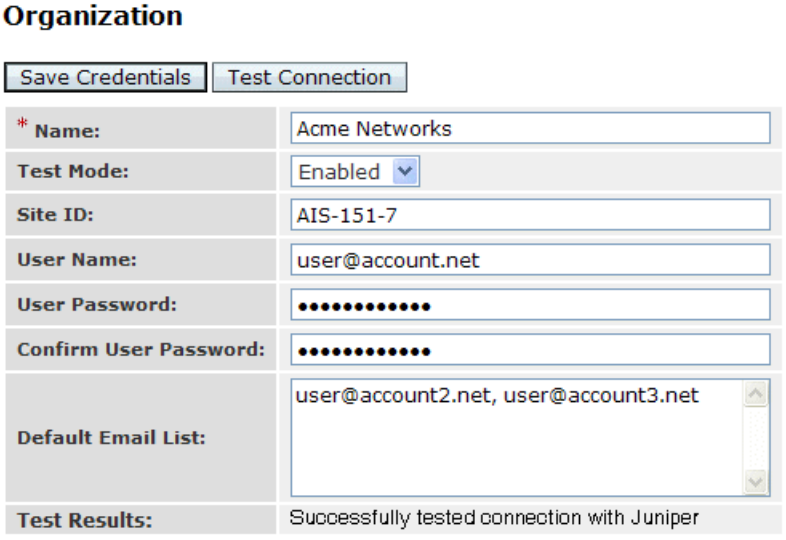
To create an AIM Organization, follow these steps:

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



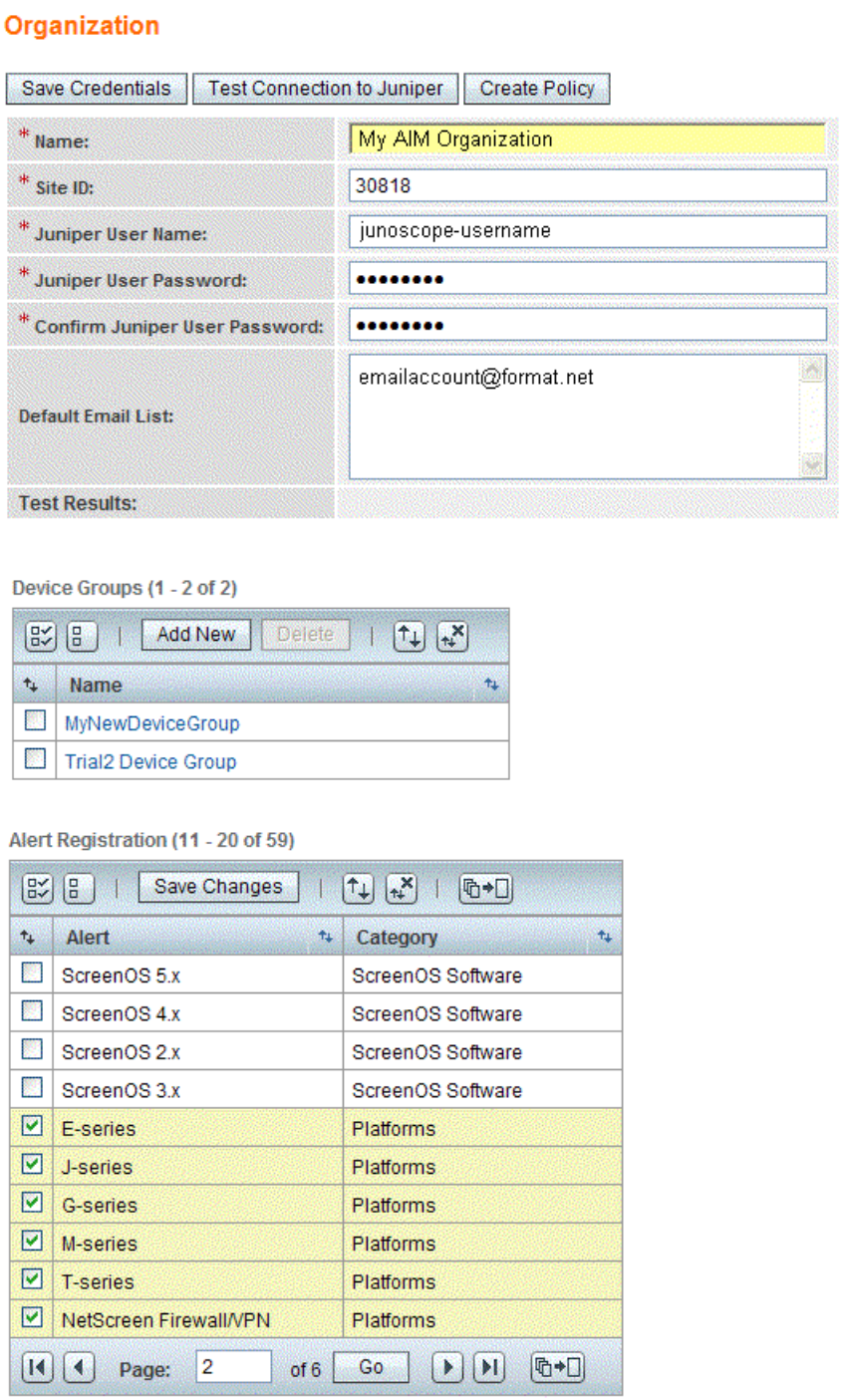
   The Organizations table is empty until you create an Organization. After you create an organization, AIM Organizations table displays the names of existing Organizations listed alphabetically by name and includes site ID, user name, and results of the connection test between AIM and JSS.

2. Click Add New. The Organization page appears.



3. Type the Organization credentials in the provided fields. See Table 31 on page 97.

4. Click Test Connection to Juniper. This command verifies the Organization Credential settings and displays the connection results. See Table 30 on page 97.
5. Click Save Credentials. This action verifies and saves the Organization credentials, and displays the Device Groups, and Alert Registration tables. See Table 30 on page 97.



For more information about the Device Groups table, see “Device Group Page Description” on page 113.

For more information about the Alert Registrations Table, see “Alert Registration Table Description” on page 125.

Organization Credentials Page Description

Table 30 on page 97 defines the Organization page command buttons.

Table 30: Organization Credentials Page Command Button Descriptions

Button Name	Description	Privileges	Enable/Disable	Results
Save Credentials	Tests connection to JSS, and if successful, then saves organization name and authentication credentials in the database.	AIM Admin Settings	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 31 on page 97 defines the Organization page fields.

Table 31: Organization Credentials Page Field Descriptions

Name	Description	Privileges	Range/Length	Default
Name	Name of the organization	AIM Admin Settings	64 characters	Blank
Test Mode	Enables or disables test mode for an organization as well as any proxy device group under that organization. Test mode prevents AIM from sending production incidents to JSS. The synopsis of any incident sent to JSS is prepended with [Test Mode]. No informational JMBs are sent to JSS from an organization in test mode.	AIM Admin Settings	Enabled or disabled when you select Enabled in the Test Mode drop-down list box.	Disabled
Site ID	An identifier used to denote the Customer Site field currently used in the JTAC Clarify system	AIM Admin Settings	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 Settings	32 characters	Blank
Juniper User Password	Password to use with the username	AIM Admin Settings	32 characters	Blank

Table 31: Organization Credentials Page Field Descriptions *(continued)*

Name	Description	Privileges	Range/Length	Default
Confirm Juniper User Password	Password must be typed in again and must match value in password field	AIM Admin Settings	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 Settings	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

You can create several types of AIM device groups:

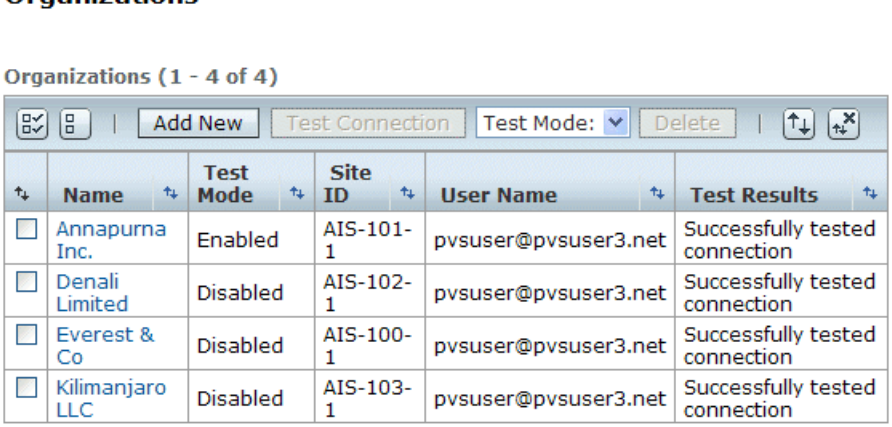
- Device—for devices upon which to perform AIM administrative operations. See “Creating a Device Group” on page 99.
- Directives—for devices that are supported by the Juniper Data Collector.
- Proxy—for devices in the end customer's network. You can create Proxy device groups when AIM is run in Partner Controller mode.

After you have verified and saved the Organization credentials by clicking Save Credentials, the page expands and the Device Group and Registered Alerts tables appear (for more information about associating registering alerts to an organization, see“Associating Registered Alerts to an Organization” on page 122). The Device Group and Archive Locations tables are empty until you create device groups.

Creating a Device Group

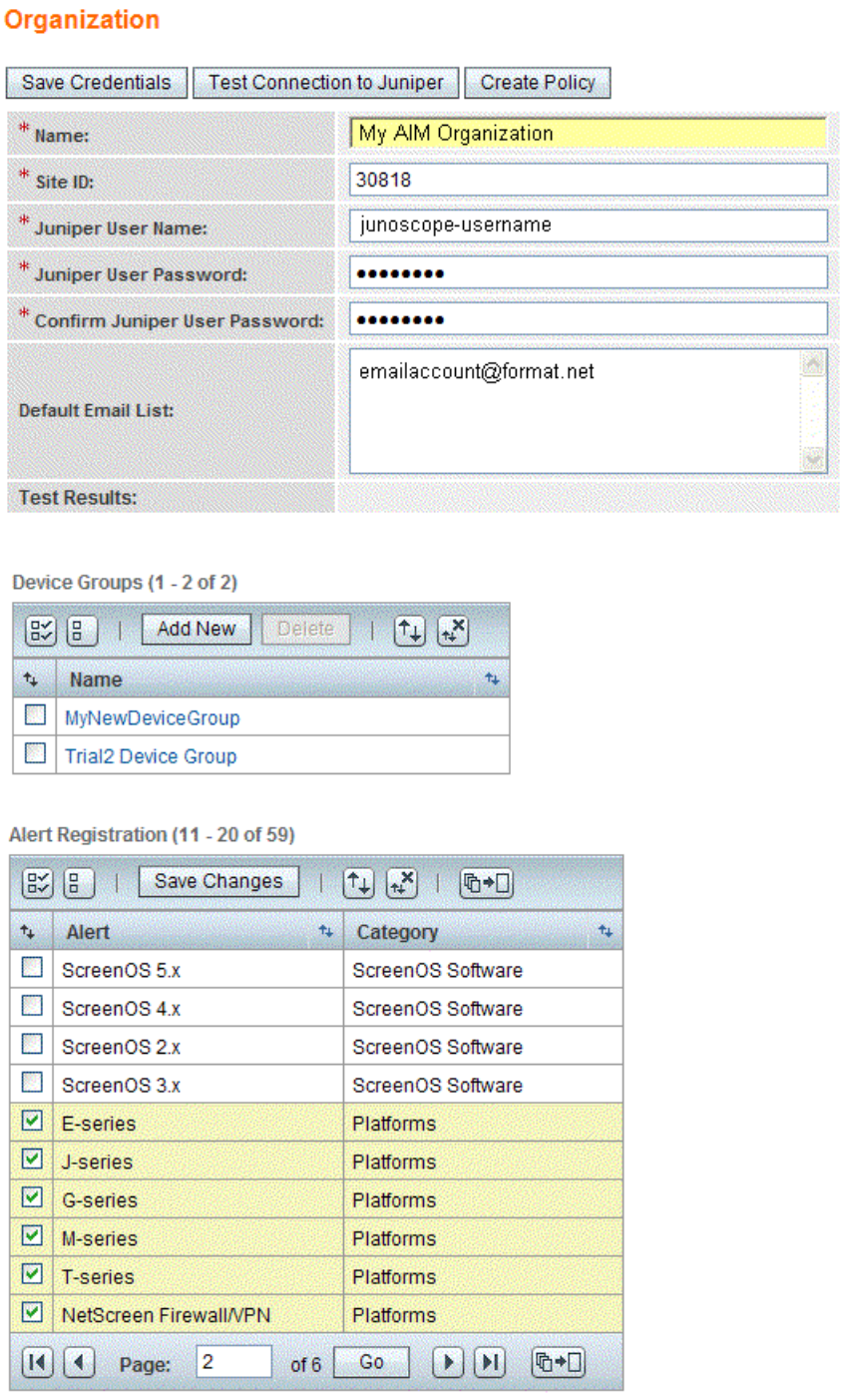
To create a device group, do one of the following:

1. Click Settings > Organizations. The Organizations table appears.

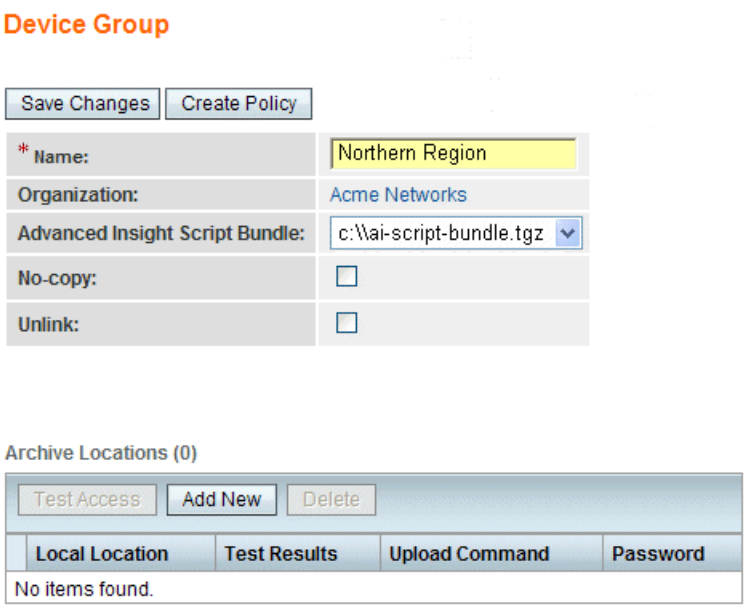


2. Create a new device group or add a device group to an existing organization.
   - To create a new organization and device group, click Add New. The Organization Credentials page appears for you to enter the settings for a new organization. Click Save Changes. The Device Groups and Alert Registration tables appear below the organization credentials area.

- To add a device group to an existing organization, click the organization name in the Organizations table. The Organization Details page, the Device Groups, and the Alert Registration tables appear.



3. In the Organization Device Group table, click Add New. The Device Group page appears with the Archive Locations table (for more information about the Archive Locations, table, see “Configuring Archive Locations” on page 114.



4. Type the device group information in the fields and check boxes. See “Device Group Page Description” on page 113“Device Group Page Description” on page 113

   The Organization to which the device group belongs appears in the Organization field. You cannot modify the Organization name.

Creating a Directives Group

A directives group is a group of devices from which the Juniper Data Collector can gather intelligence information. A device group is a group of devices from which AI-Scripts collects incident and intelligence information.

A device may belong to several directives groups. A device may belong to both a device group and a directives device group. If a device belongs to both types of groups, both AI-Script-driven and Juniper Data Collector-driven data collection occurs for that device.

The directives group specifies the archive locations into which the Juniper Data Collector deposits JMBs for devices in that group. The archive locations are folders on the local file system. If the Juniper Data Collector encounters a failure when uploading the JMB to a particular archive location, it uses the next location, retrying until there is either success or all archive locations fail. The JDC places a JMB into a single archive location.

The directives group has a Juniper Data Collector directives file (directives.rc) that specifies the data collection processing that is performed for the devices in the group.

An organization can contain several directives device groups. Organizations do not share directives device groups. Each organization must use its own archive locations to avoid intermingling of data between organizations.

When the Juniper Data Collector starts, it reads from the database the information for all of the directives groups. It determines from this information which devices to poll, which Juniper Data Collector directives files to use, and which archive locations to write the JMB file. When the user saves changes for a directives device group, the AIM sends a refresh message to the Juniper Data Collector to read the information for that particular directives device group.

You can create a directives group of supported Juniper Data Collector devices using the AIM Settings > General Settings and AIM Settings > Organizations user interfaces. You can add a supported device to one or more directives groups. For more detailed information about creating directives groups, see "Creating a Directives Group and Adding Devices" on page 103.

Before You Begin

Do the following before you create a directives group:

- Enable SSH access on the device, which by default is disabled. See "Enabling NETCONF Over SSH" on page 111.
- Ensure that the devices running JUNOS have the NETCONF protocol enabled. See "Ensuring NETCONF Over SSH Is Enabled" on page 109.
- Add the users you want to associate to a directives group in AIM Settings > Users and User Groups.
- Create a directory on the AIM server where you want the Juniper Data Collector to send device JMBs. For example, from a shell, enter the following command:

  mkdir –p /JDC/jmbarchive

- Know the network name, the host name, and the SSH username, the SSH password, and port number for each device you want to add to a directives group. For a JUNOSe device, you need the following:
  - SNMPv2c community string or SNMPv3 user credentials
  - a Telnet password
  - Enable 15 password

  For a JUNOS device, enable NETCONF.

Creating a Directives Group and Adding Devices

To create a directives group and add a supported device, follow these steps.

1. Configure the AIM General Settings for the Juniper Data Collector. Select Settings.

   Specify the JDC maximum number of concurrent tasks working in parallel to collect information from devices.

2. Create an AIM organization if one does not already exist. You can add a directives group to organizations that already have device groups for which AI-Scripts collect data.

   When you create an organization, the Devices Group and Alert Registration tables appear.

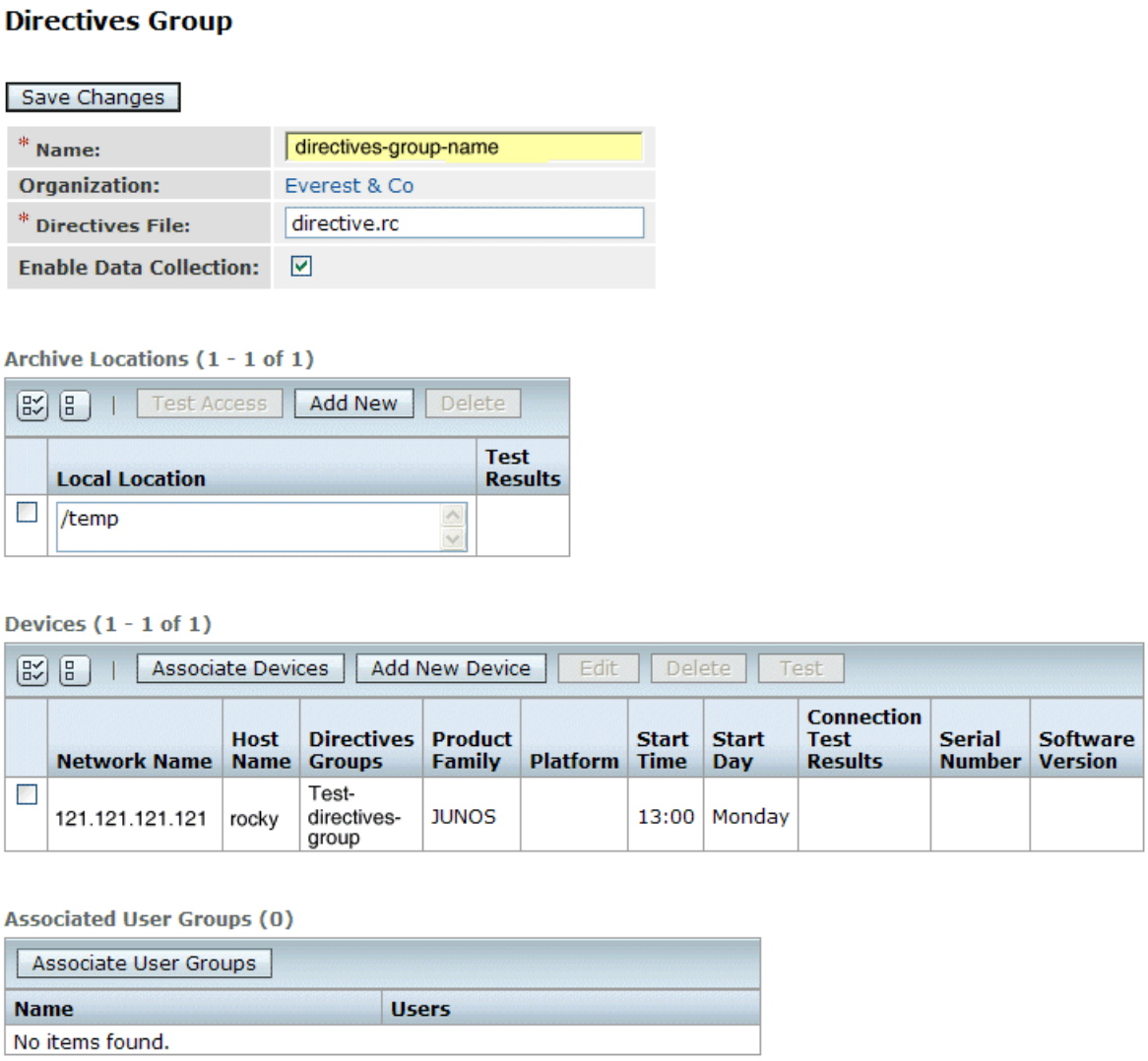
3. Create a Directives Group. In the Device Groups table, select Add New Directives Group from the drop-down list box. The Directives Group page appears.

4. On the Directives Group page, add the directives group name and the archive location pathname, then click Test Access. The AIM Directives Group page defaults to the directives file directive.rc. Access may fail if credentials, passwords, or user names are incorrect or if the network is not available. Click Save Changes. The Devices table and the Associate User Groups table appear.

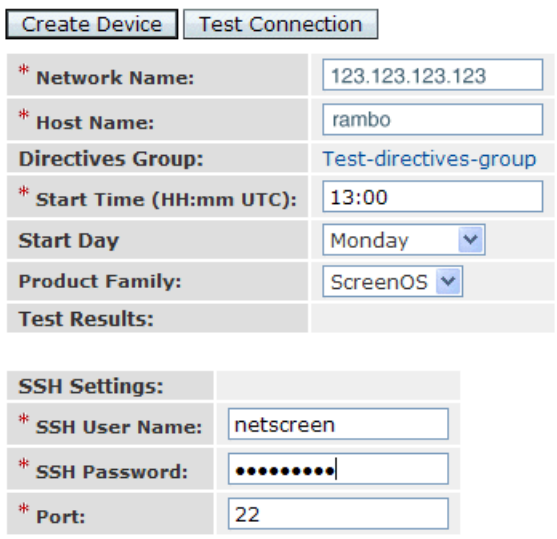
5. In the Devices table, either associate existing Juniper Data Collector supported devices or add new devices.

   - To associate devices to a directives group, click Associate Devices. The Associate Devices page appears with a list of the devices you added to AIM by host name and device name. Click Save Changes. The devices appear in the Directives Group Devices table.
   - To add a new device to the directives group, click Add New Device. The Create Device and Add to Directives Group page appears. Enter the new device settings and click Test Connection. If the connection is successful,

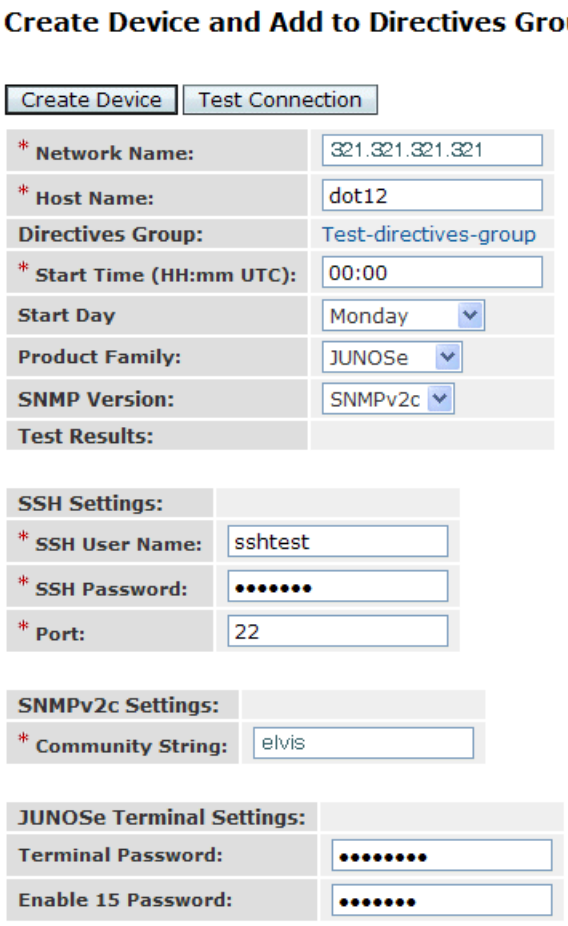
click Create Device. The new device appears in the Directives Group Devices table. (See “Directives Group Page Description” on page 106).



- To add a JUNOS or Netscreen device, add the appropriate settings. For more information, see “Create Device and Add to Directives Group Page Button Descriptions” on page 107 and Table 34 on page 108.



- To add a JUNOSe device, add the appropriate settings. For more information, see “Create Device and Add to Directives Group Page Button Descriptions” on page 107 and Table 34 on page 108.



6. In the Associate User Groups table, associate the user groups you want to access the directives group.
7. Click Save Changes. The directives group appears in the Organization Device Groups table.

Directives Group Page Description

Table 32 on page 106 describes the Directives Group Page settings.

Table 32: Directives Group Page Description

Name	Description	Privileges	Length/Range	Default
Save Changes	Saves the directives group settings and displays the Devices and Associated User Group tables.	AIM Admin Settings	N/A	N/A

Table 32: Directives Group Page Description *(continued)*

Name	Description	Privileges	Length/Range	Default
Name	The name of the directives group.	AIM Admin Settings	32 characters	blank
Organization	The name of the organization in which the directives group is being created.	AIM Admin Settings	N/A	N/A
Directives File	A configuration file that drives the Juniper Data Collector data collection process. The directives.rc file is installed during the AIM installation.	AIM Admin Settings	N/A	directive.rc
Enable Data Collection	This check box allows the Juniper Data Collector to collect information from supported devices.	AIM Admin Settings	N/A	This option is selected.

Create Device and Add to Directives Group Page Button Descriptions

Table 33 on page 107 describes the Create Device and Add to Directives Group page buttons.

Table 33: Create Device and Add to Directives Group Page Button Descriptions

Button Name	Description	Privileges	Enable/Disable	Results
Create Device	Displays the Create Device and Add to Directives Group page used to add a supported device to a directives group.	AIM Admin Settings	Enabled	■ The system message: Validation Error: Value is required.appears when you click the Create Device button without specifying the required fields on the Create Device and Add to Directives Group Page. ■ Clicking the Create Device button when all the required values are specified displays the Directive Group page.
Test Connection	Tests the connection between AIM and the device in a directives group.	AIM Admin Settings	Enabled	■ Connection Failed : SSH negotiation failed

Table 34 on page 108 describes the fields on the Create Device and Add to Directives Group page.

Table 34: Create Device and Add to Directives Group Page Field Descriptions

Name	Description	Privileges	Length/Range	Default
Network Name	The name AIM uses to reach the device (for example. an IP address or DNS name),	AIM Admin Settings	64 characters	Blank
Host Name	A name you give a device for convenience (for example, an IP address, DNS name, or any name you create).	AIM Admin Settings	128 characters	Blank
Directives Group	A unique name for the directives group. Click the link to return to the directives group.	Not allowed to modify	N/A	Display field
Directives Group				
Start Time (HH:mm:UTC)	The start time (Coordinated Universal Time) for Juniper Data Collector operations for the device.	AIM Admin Settings	HH:mm	00:00
Start Day	A weekday on which to start data collection.	AIM Admin Settings	Drop-down list box that displays the start day options from Sunday to Saturday	Sunday
Product Family	The Juniper Networks operating system running on the device (for example, JUNOS, JUNOSe, or ScreenOS.	AIM Admin Settings	Drop-down list box that displays the product family options: JUNOS, JUNOSe, or NetScreen (ScreenOS)	JUNOS
(JUNOSe) SNMP Version	The SNMP version configured on the device (for example. SNMPv2c or SNMPv3).	AIM Admin Settings	Drop-down list box that displays the SNMP version options: SNMPv2c or SNMPv3	SNMPv2c
Test Results	The AIM-to-device connection results.	Not allowed to modify	N/A	Blank display field
SSH Settings				
SSH User Name	A user name for authentication on the device.	AIM Admin Settings	32 characters	Blank
SSH Password	A password for authentication on the device.	AIM Admin Settings	32 characters	Blank
Port	The forwarding TCP port number for SSH.	AIM Admin Settings	1–65, 535	22
(JUNOSe) SNMPv2c Settings				

Table 34: Create Device and Add to Directives Group Page Field Descriptions *(continued)*

Name	Description	Privileges	Length/Range	Default
(JUNOSe) Community String	Authentication of clients is performed by a community string, a password.	AIM Admin Settings	32 characters	Blank
(JUNOSe) SNMPv3 Settings				
User Name	SNMPv3 user name	AIM Admin Settings	32 characters	Blank
Authentication Protocol	SNMPv3 authentication protocol	AIM Admin Settings	N/A	None
SNMPv3 Authentication key	SNMPv3 authentication key, needed if SHA or MD5 authentication is selected.	AIM Admin Settings	■ 20 (SHA) ■ 16 (MD5) ■ 0 (none)	Blank
Privacy Protocol	SNMPv2 Privacy Protocol	AIM Admin Settings	N/A	None
SNMPv3 Privacy Key	SNMPv3 privacy key, needed if DES is selected.	AIM Admin Settings	■ 16 (DES) ■ 0 (none)	Blank
JUNOSe Terminal Settings				
(JUNOSe) Terminal Password	Password used to access the JUNOSe device through telnet (if enabled on the device)	AIM Admin Settings	32 characters	Blank
(JUNOSe) Enable 15 Password	Password used to access all JUNOSe CLI commands for iJMB generation (if enabled on the device).	AIM Admin Settings	32 characters	Blank

Ensuring NETCONF Over SSH Is Enabled

To ensure that NETCONF over SSH is enabled on a JUNOS device, follow these steps:

1. Log in to the JUNOS device.
2. Enter the following CLI command:

```
user@host> show configuration
```

Output similar to the following appears:

```
system {
      host-name Neon;
      root-authentication {
```

```
            encrypted-password "$1$rQQ4q1eZ$
        }
          login {
            message "Please DO NOT change couser lab {
                uid 2000;
                class superuser;
                authentication {
                    encrypted-password "$1$m
                }
            }
            user lablab {
                uid 2001;
                class superuser;
                authentication {
                    encrypted-password "$1$w
                }
             }
          }
          services {
              ftp;
              ssh {
                  root-login allow;
                  protocol-version v2;
              }
              telnet;
              netconf {
                  ssh;
              }
              web-management {
                  http;
              }
          }
          syslog {
              user * {
                  any emergency;
              }
              file messages {
                  any any;
                authorization info;
              }
              file interactive-commands {
                  interactive-commands any;
              }
          }
      }
```

3. In the show configuration CLI command output, look for the following NETCONF over SSH configuration:

```
services {
          ftp;
          ssh {
              root-login allow;
              protocol-version v2;
          }
          telnet;
          netconf {
              ssh;
          }
```

If NETCONF is not configured, see “Enabling NETCONF Over SSH” on page 111.

Enabling NETCONF Over SSH

To enable NETCONF service over SSH, follow these steps:

1. Include one or both of the following statements at the indicated configuration hierarchy level.
   - To enable SSH access over the devoted port (32000) as specified by the IETF specification, include the ssh statement at the [edit system services netconf] hierarchy level.

     ```
     [edit system login user account-name authentication]
     user@host# top
     [edit]
     user@host# set system services netconf ssh
     ```

   - To enable access over the default SSH port (22), include the ssh statement at the [edit system services] hierarchy level. This configuration also enables SSH access to the device for all users and applications.

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

2. Commit the configuration.

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

3. Repeat the preceding steps on each JUNOS device where the client application establishes NETCONF sessions.

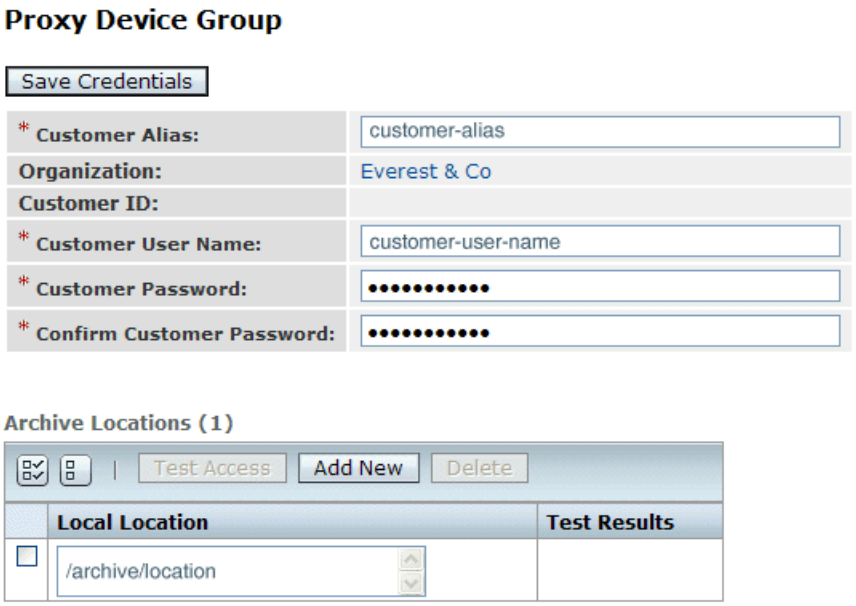
For more information about NETCONF, see the *JUNOS NETCONF API Guide*.

Creating a Proxy Device Group and Adding Devices

To create a proxy device group and add devices, follow these steps:

1. Click Settings > Organizations. The Organizations page appears.
2. In the Organization table, click an existing organization name or create a new one. The Organization details page appears. To create an organization, see “Adding Organization Credentials” on page 95.
   - If you create a new organization and save the credentials, the Organization Credentials details and Groups table appears.
   - If you click an existing organization name to add a Proxy Group, the Organization Credentials details and Groups table already exists.

3. In the Groups table, select Proxy Device Group in the Add New drop-down list box. The Proxy Device Group page appears with the Archive Locations table.



4. Enter the end customer alias, user name, and password in the Organization page. The end customer alias must be a unique alphanumeric name (you can use a through z, capital A through Z, and 0 through 9) with up to 80 characters.
5. Add an archive location where JMBs from the device will be stored. For every end user, the partner should create a proxy organization with a unique archive location for receiving JMBs. The archive location directory should be used exclusively for JMBs and no other AIM files.
6. Click Save Credentials. The Devices table and the Associated User Groups table appears.

   The associated devices are ones that have been managed and imported from the JUNOScope software or those that have been set up manually to send JMBs to the archive location.
7. In the Associated User Groups table, click Add New to associate the user groups that you want to have access to the Proxy device group. The User Groups page appears.
8. In the User Groups table, select one or more user groups that you want to associate to the user group.
9. Click Save Credentials.

Device Group Page Description

Table 35 on page 113 defines the Device Groups table command buttons.

Table 35: Device Group Page Button Descriptions

Button Name	Description	Privileges	Enable/Disable	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 36 on page 113 defines the Organization page Device Group fields.

Table 36: Device Group Page Field Descriptions

Name	Description	Privileges	Length/Range	Default
Name	Name of the device group	AIM Admin Settings	32 characters	Blank
Organization	Name of the organization to which this device group belongs. The organization name provides a link to the Organization detail screen. See "Organization Credentials Page Description" on page 97.	You cannot 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 Settings	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 Settings	Checked or unchecked	Blank
Unlink	Indicates the command to remove the AI-Script bundle after successful installation on the device.	AIM Admin Settings	Checked or unchecked	Blank

Proxy Device Group Page Description

Table 37 on page 114 describes the Proxy Device Group page buttons.

Table 37: Proxy Device Group Page Button Descriptions

Button Name	Description	Privileges	Enable/Disable	Results
Save Credentials	Tests connection to JSS, and if successful, then saves organization name and authentication credentials in the database. It also retrieves the end customer ID.	AIM Admin Settings	If privileged	Saves the new organization credentials in the AIM database
Create Policy	Lets you create a reaction policy associated with an organization. For example, you can create a reaction policy that triggers when a new intelligence message is received. For more information about creating a reaction policy, see "Creating Reaction Policies" on page 237.	Reaction Policy	Available after you click Save Changes	Opens the Reaction Policies page.

Table 38 on page 114 describes the fields on the Proxy Device Group page.

Table 38: Proxy Device Group Page Field Descriptions

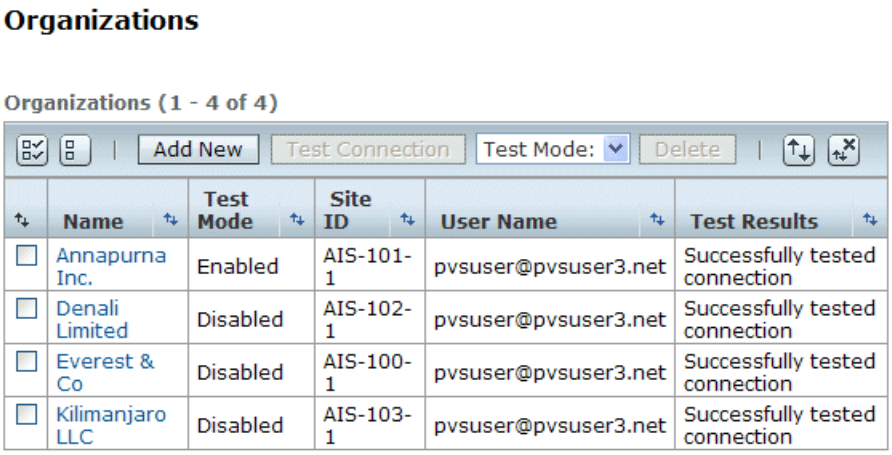
Field Name	Description	Privileges	Length/Range	Results
Customer Alias	A unique alphanumeric name for the customer (a through z, capital A through Z, and 0 through 9).	AIM Admin Settings	Up to 80 characters	
Organization	Name of the organization to which this proxy device group belongs. The organization name provides a link to the Organization detail screen. See "Organization Credentials Page Description" on page 97.	You cannot modify the Organization name.	N/A	N/A
Customer ID	A non-editable, 32–character ID generated by JSS and returned upon successful customer activation.	You cannot modify the customer ID.	32 characters	N/A
Customer User Name	A name for the customer.	AIM Admin Settings	60 characters	
Customer Password	The password for the customer.	AIM Admin Settings	32 characters	
Confirm Password	The password for the customer.	AIM Admin Settings	32 characters	

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. Click Settings > Organizations. The Organizations table appears.



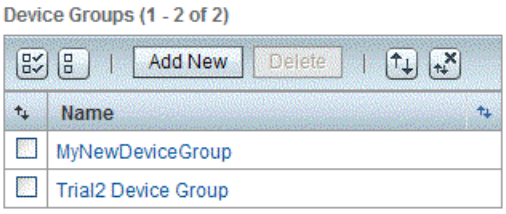
Organizations

Organizations (1 - 4 of 4)

Add New | Test Connection | Test Mode: | Delete

Name	Test Mode	Site ID	User Name	Test Results
Annapurna Inc.	Enabled	AIS-101-1	pvsuser@pvsuser3.net	Successfully tested connection
Denali Limited	Disabled	AIS-102-1	pvsuser@pvsuser3.net	Successfully tested connection
Everest & Co	Disabled	AIS-100-1	pvsuser@pvsuser3.net	Successfully tested connection
Kilimanjaro LLC	Disabled	AIS-103-1	pvsuser@pvsuser3.net	Successfully tested connection

2. Create an organization or view the details of an existing one. Either click Add New or click the organization name link˙. Either the Organization Credentials page appears for you to create a new organization. Click Save Changes. The Device Groups and Alert Registration tables appear. Or, click the organization name link. The Organization Details page, the Device Groups, and the Alert Registration tables appear.

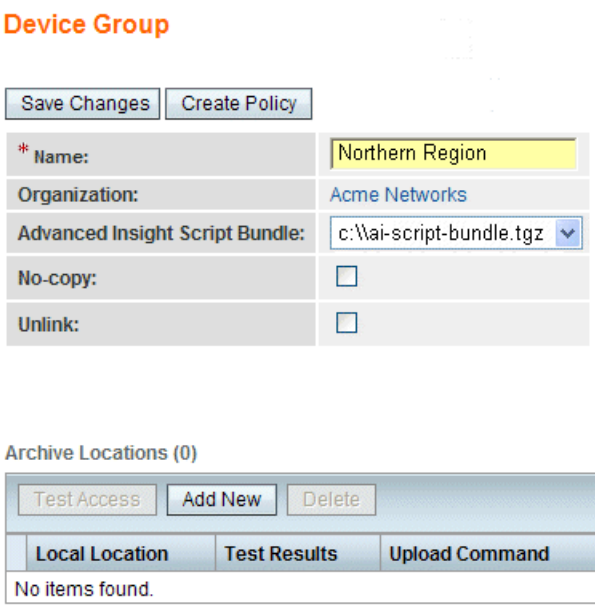


Device Groups (1 - 2 of 2)

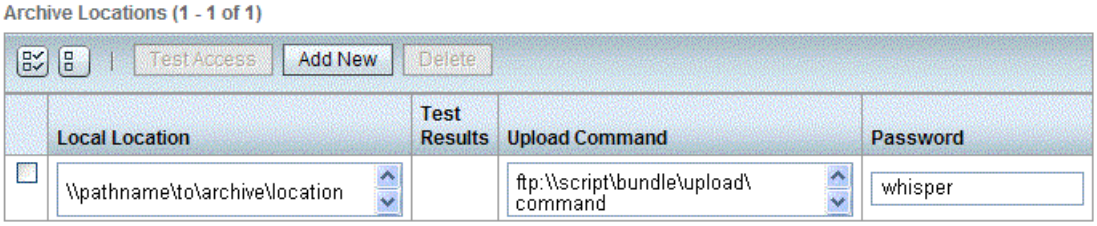
Add New | Delete

Name
MyNewDeviceGroup
Trial2 Device Group

3. In the Organization Device Group table, click Add New. The Device Group page appears with the Archive Locations table (for more information about the Archive Locations, table, see “Configuring Archive Locations” on page 114).



4. On the Device Group page, click Add New in the Archive Locations table. A new row appears in the Archive Locations table.



5. Type the required information in the Archive Locations table column fields. See “Archive Locations Table Description” on page 117.

NOTE: The archive location directory should be used exclusively for JMBs and no other AIM files.

6. Click Test Access. The test results appear in the Test Results field. The test results are either Success or Failure.
7. 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 devices in the group that were imported from JUNOScope,

Archive Locations Table Description

Table 39 on page 117 defines the Archive Locations table command columns.

Table 39: Archive Locations Table Command Button Descriptions

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

Table 40 on page 117 defines the Archive Locations table fields.

Table 40: Archive Location Table Field Descriptions

Name	Description	Privileges	Range/Length	Default
Local Location	The name of the local path where the device sends incident and intelligence JMBs. This path is relative to the installation machine. **NOTE:** The archive location directory should be used exclusively for JMBs and no other AIM files.	AIM Admin Settings	128 characters	Blank
Test Results	Displays results from the Test Access command for this row. The test results are either: ■ Successfully accessed location. ■ Failed to access location.	Not allowed to modify	N/A	Blank

Table 40: Archive Location Table Field Descriptions *(continued)*

Name	Description	Privileges	Range/Length	Default
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 Settings	128 characters	Blank
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 Settings	64 characters	Blank

Associating Devices to a Device Group

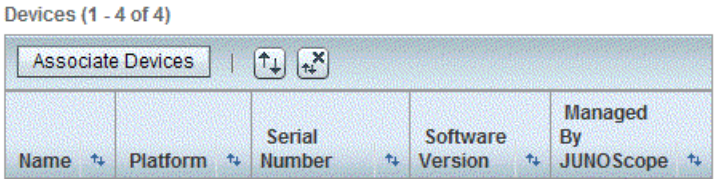
The Devices table displays the devices in the AIM application that are contained in a particular device group.

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

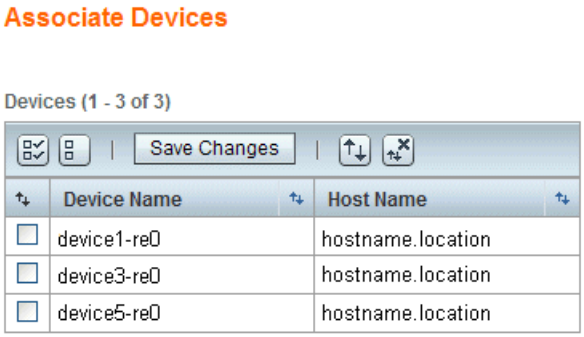
- When a JMB file is detected in any of the archive locations of this device group, the device that generated the JMB file is automatically added to the device group.
- Devices that have been imported from JUNOScope can be associated to the device group manually by the user.

To associate devices, follow these steps:

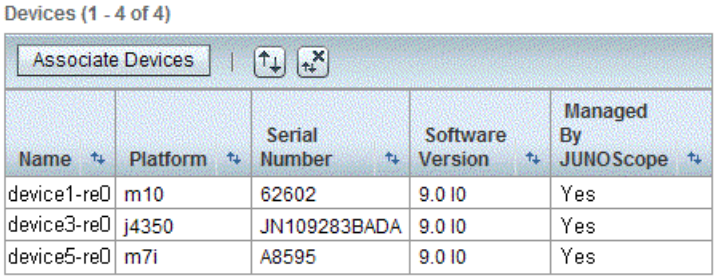
1. In the Devices table, click Associate Devices. The Devices table is empty until you associate devices to the device group.



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 71. See “Associate Devices Table Description” on page 120.
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 119.

Devices Table Description

Table 41 on page 119 defines the Device table command buttons.

Table 41: 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 Settings	Always is enabled

Table 42 on page 120 defines the Devices table column descriptions.

Table 42: 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 device is managed by JUNOScope. The column is blank if the device is not managed by JUNOScope. If the device is managed by JUNOScope, an AI-Script bundle will be automatically installed on that device.	Not allowed to modify

Associate Devices Table Description

Table 43 on page 120 describes the command button in the Associate Devices table.

Table 43: 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 Settings	Always is enabled

Table 44 on page 120 describes the columns in the Associate Devices table.

Table 44: Associate Devices Table Descriptions

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

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.

Associated User Groups (1 - 4 of 4)

Associate User Groups

Name	Users
admins	admin,
demo	demo
MyNewUserGroup	admin, anewuser, demo
testGroup	admin, demo,

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

Associate User Groups

User Groups (1 - 6 of 6)

Save Changes

	Name	Users	Device Groups
☑	admins	admin	Device Group 1
☐	aim	aimuser	Device Group 2
☑	demo	demo	Device Group 2
☑	MyNewUserGroup	admin, anewuser, demo	Device Group 3
☑	testGroup	admin, demo,	Device Group 3

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. See “Associate User Groups Table Description” on page 121.

Associate User Groups Table Description

Table 45 on page 122 defines the Associate User Groups table command buttons.

Table 45: 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 Settings	Disabled until you select a user group.	Saves user groups associated with the device group

Table 46 on page 122 defines the Archive Location table fields.

Table 46: Associate Users Group Table Field Descriptions

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

Associating Registered Alerts to an Organization

JSS Alerts that you register for using http://www.juniper.net/alerts/ can be associated with an Organization. The alerts you register for are selected in the Alert Registration table. You can ensure that the requested alerts are selected to associate them with the current organization.

The JSS Alert system allows customers to go the JSS support Web site and register for specific types of alerts to be e-mailed to them.

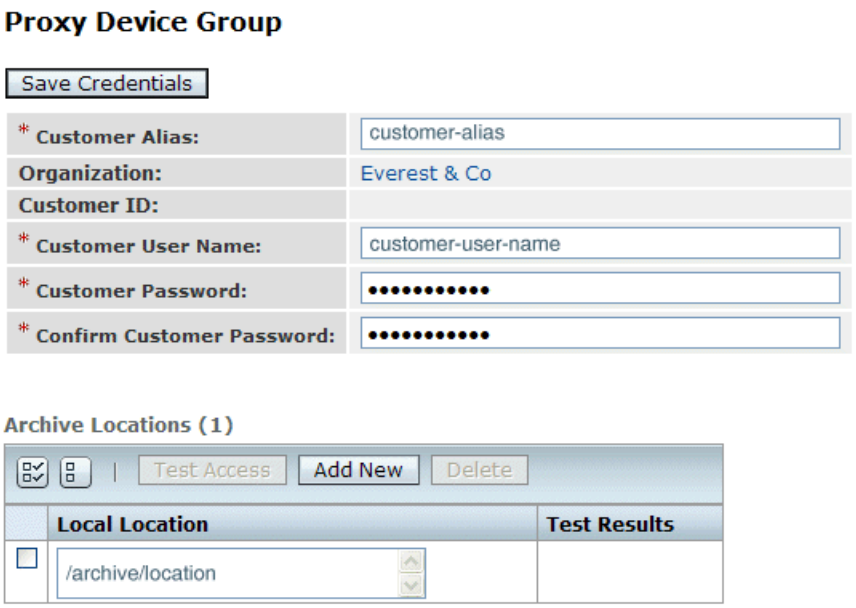
When you register for alerts in AIM, you receive the same information. The difference is instead of receiving the information in e-mail messages, alert messages are received by AIM and displayed in Intelligence Manager. This action provides you one central place to receive alerts and assign alerts to 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 199.

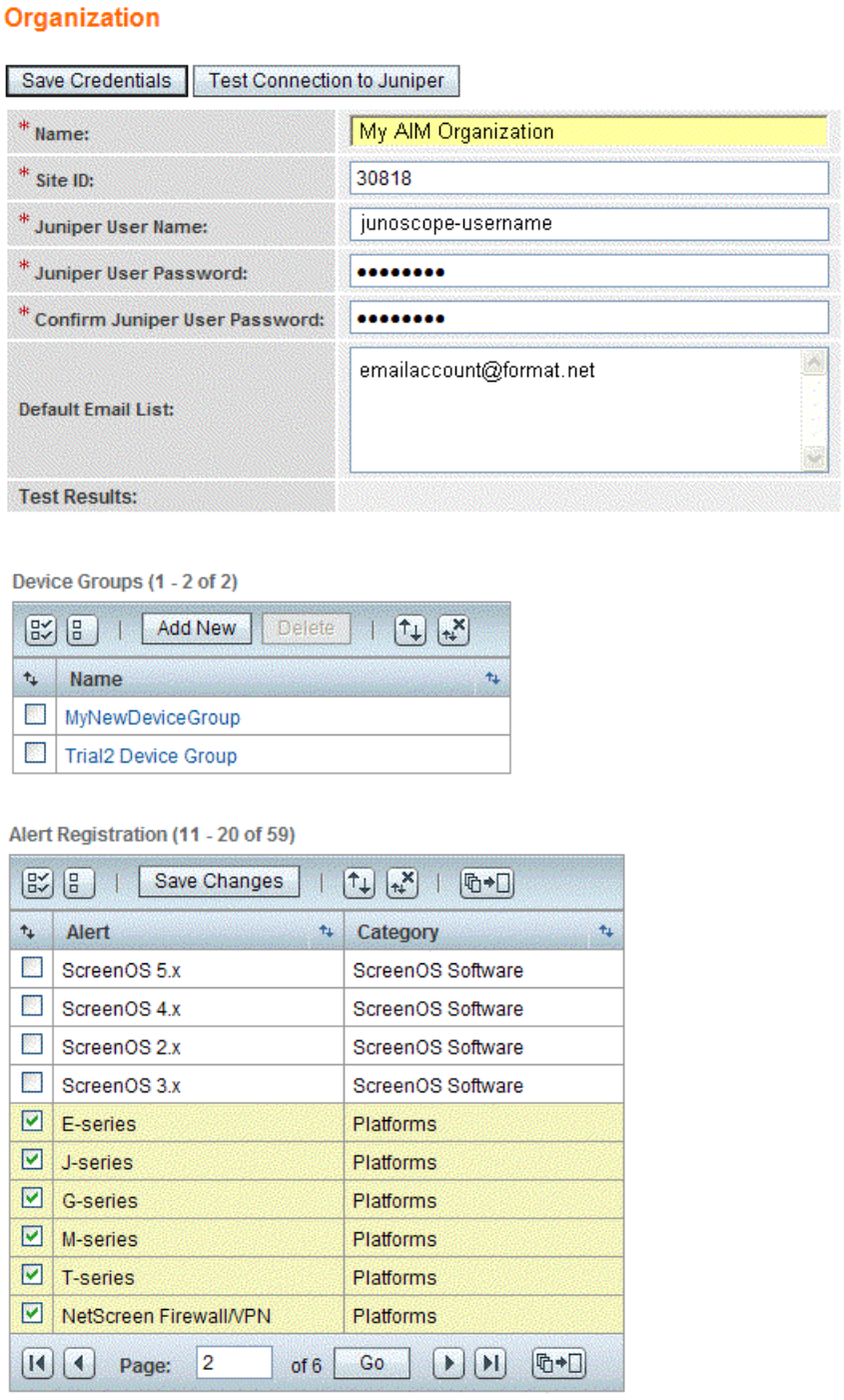
When you navigate to the AIM Organization Detail page, the alerts available to register for are retrieved from JSS and are displayed in the Alert Registration table. Those alerts that are checked in the table indicate the ones the organization is already registered to receive. Once you specify the alerts 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 table appears.



2. Click the name of the organization to register alerts. This action displays the Organization page.



The Alert Registrations table displays the alerts available to register for that are retrieved from JSS. The alerts that the Organization is already registered to receive are checked in the table. See “Alert Registration Table Description” on page 125.

3. Select the alerts that you want to be registered with the Organization.
4. Click Save Changes to register the specified alerts with JSS.

Alert Registration Table Description

Table 47 on page 125 defines the Alert Registrations table command buttons.

Table 47: Alert Registration Table Command Button Descriptions

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

Table 48 on page 125 defines the Alert Registration table fields.

Table 48: Alert Registration Table Field Descriptions

Name	Description	Privileges
Alert	Type of alert for which to register	Not allowed to modify
Category	Category to which the alert belongs	Not allowed to modify

Alerts and Information Message Flow Passing to the End User

This section describes the interaction between the partner and end user when alerts and intelligence message are sent from JSS.

- Partner Controller Alert and Informational Messages Passing to the End User on page 125
- End User on page 126

Partner Controller Alert and Informational Messages Passing to the End User

1. The partner registers for Juniper Networks alerts. See “Associating Registered Alerts to an Organization” on page 122
2. The partner receives alerts and informational messages from JSS.
3. The partner with AIM admin privileges determines which end users to send Juniper Networks alerts and informational messages.
    a. The partner can perform scan for impact to determine which end user Juniper Networks alerts and informational messages impact.

b. The partner can send a message to each end user that is stored in the AIM database.

4. When the request to get an intelligence message update is received from the end user, the partner sends a response to the end user that includes any new alerts and informational messages.

End User

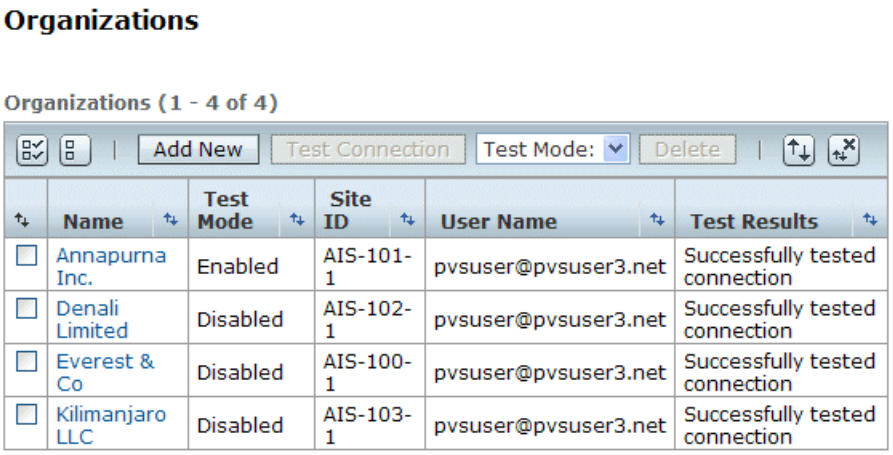
1. The end user's AIM periodically checks for Juniper Networks alerts and informational messages. The end user determines the interval for checking.
2. New alerts and informational messages are received and saved in the end user's AIM database.

Using the Organizations Table

The AIM Organizations table displays an alphabetized listing of organizations by site ID, user name, and JSS 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 “Organizations Table Description” on page 126.

Organizations Table Description

Table 49 on page 127 describes the Organizations table command buttons.

Table 49: 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 JSS.	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.
Test Mode	Enables or disables test mode for an organization as well as any proxy device group under that organization. Test mode prevents AIM from sending production incidents to JSS. The synopsis of any incident sent to JSS is prepended with [Test Mode]. No informational JMBs are sent to JSS from an organization in test mode.	AIM Admin Settings	Enabled when you select an organization in the table.	Disabled
Create Policy	Lets you create a reaction policy associated with an organization. For example, you can create a reaction policy that triggers when a new intelligence message is received. For more information about creating a reaction policy, see “Creating Reaction Policies” on page 237	Reaction Policy	Available after you click Save Changes	Opens the Reaction Policies page.

Table 50 on page 127 defines the Organizations table columns.

Table 50: Organizations Table Field Descriptions

Name	Description	Privileges
Name	Name of the organization. This field is a link to navigate to the detail screen of the organization.	Not allowed to modify
Test Mode	Indicates whether test mode for an organization has been enabled or disabled.	Not allowed to modify
Site ID	An identifier used to denote the Customer Site field currently used in the JTAC Clarify system	Not allowed to modify

Table 50: Organizations Table Field Descriptions *(continued)*

Name	Description	Privileges
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
Test Results	Displays results from the Test Connection to Juniper command: Success or failure	Not allowed to modify

Viewing Organization Details

To view the organization details page:

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 Organization page shows the credentials and other elements that have been associated, such as device groups and alerts. For more information, see "Organization Credentials Page Description" on page 97, "Device Group Page Description" on page 113, and "Alert Registration Table Description" on page 125.

Chapter 12

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 Reaction Policies” on page 237. In AIM Settings > Trap Destinations, all of the trap destinations that have been created are listed in the Trap Destinations table.

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

To create and manage trap destinations, you must have AIM Admin Settings privileges.

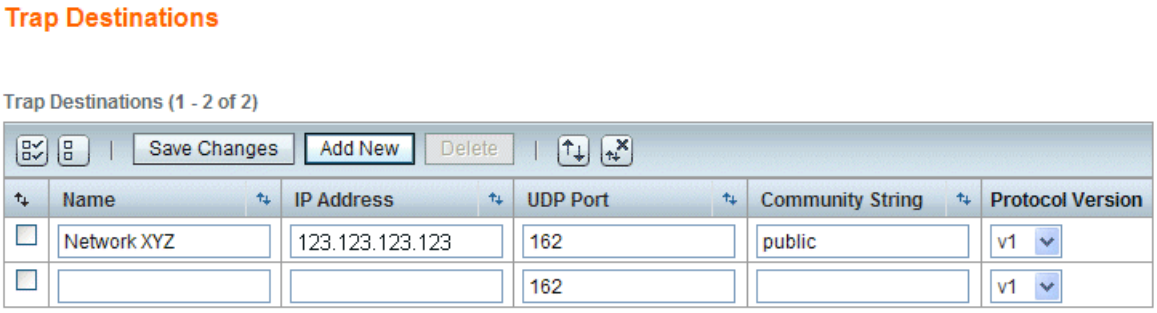
For more information about AIM traps, see “Supported SNMP Traps” on page 250.

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 132 for trap destination parameters.
4. Click Save Changes.

Trap Destinations Table Field Descriptions

Table 51 on page 132 describes the Trap Destinations table command buttons.

Table 51: Trap Destinations Command Buttons and Field Descriptions

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

Table 52 on page 132 describes the Trap Destinations table columns.

Table 52: Trap Destinations Table Columns

Name	Description	Privileges	Range/Length	Default
Name	Unique name of trap destination.	AIM Admin Settings	32 characters	Blank
IP Address	IP Address of network management station where AIM trap destination will be sent.	AIM Admin Setting	1 to 65535	Blank

Table 52: Trap Destinations Table Columns *(continued)*

Name	Description	Privileges	Range/Length	Default
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	32 characters	Port 162
Community String	A community string is a password that allows access to a network device. It defines the community of people that can access the SNMP information on the device. The network operator responsible for the network device typically sets the community strings. The default strings, 'public' and 'private'.	AIM Admin	32 characters	Blank
Protocol Version	Supported Simple Network Management Protocol (SNMP) versions: ■ v1 ■ v2c	AIM Admin	SNMP v1, v2c, and v3	SNMP v1

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 13

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 “Advanced Insight Solutions Overview” on page 3. For more information about configuring device groups, see “Creating Device Groups” on page 98.

To create and manage AIM users, you must have AIM Admin Settings privileges.

You can assign permissions that allow users access only to a subset of AIM operations. If the Multi-Site license is present, allowing 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 do 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.

Understanding AIM Ownership

AIM provides ownership for incidents and intelligence messages when an AIM user owns a message, that user is responsible for keeping track of the progress of a case or updates from JSS. 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 e-mail 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 53 on page 136.

Table 53: AIM Ownership Levels

Ownership Level	Description
None	User is not allowed to own or assign ownership to any AIM user.

Table 53: AIM Ownership Levels *(continued)*

Ownership Level	Description
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 whether they are 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 54 on page 137 defines the AIM user privileges.

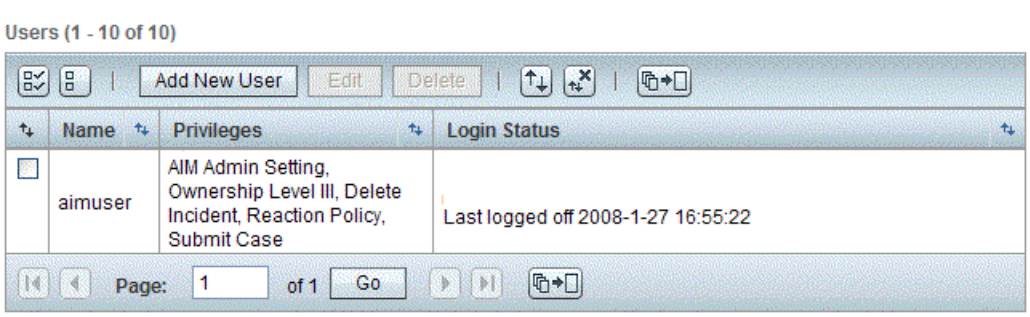
Table 54: AIM User Privileges

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 53 on page 136.
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.

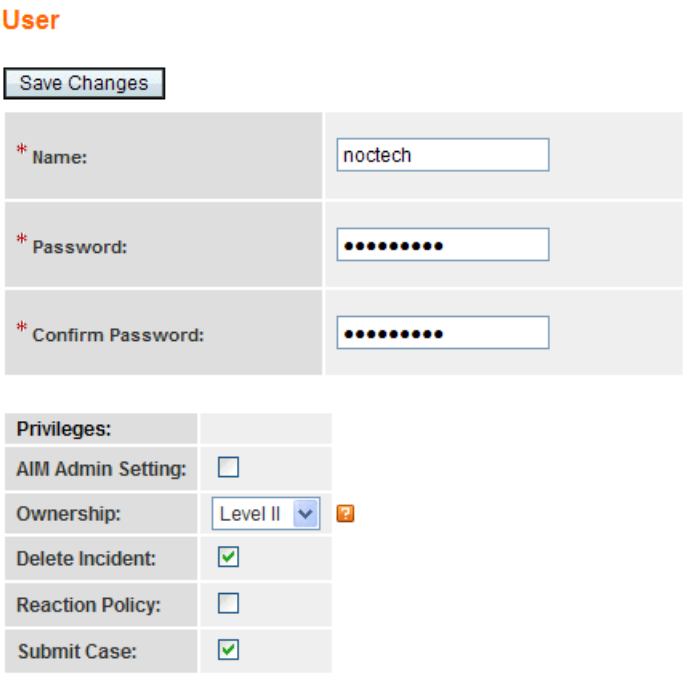
Adding a AIM User

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 136.

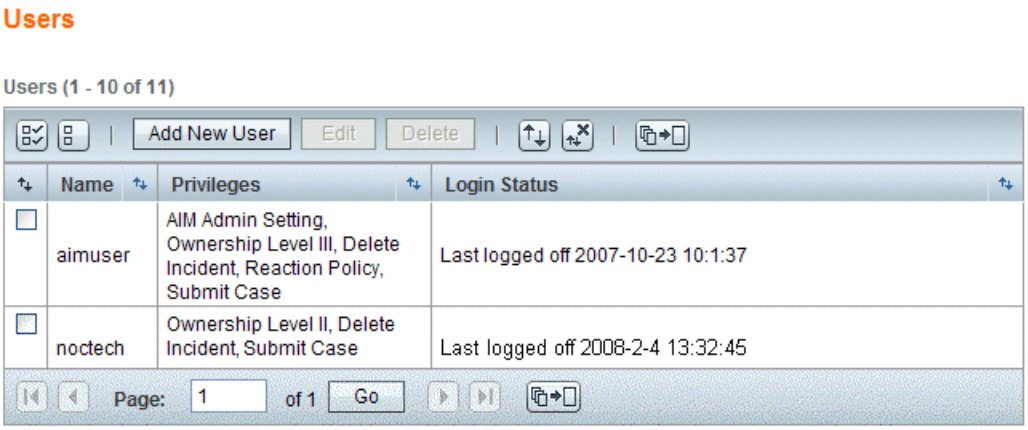


2. Click Add New User. The User page appears.



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 53 on page 136. For more information about AIM user privileges, see Table 54 on page 137.

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 55: 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 56 on page 139 describes the New User Field descriptions.

Table 56: 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 54 on page 137	AIM Admin Settings	N/A	Unchecked

Table 56: Add New User Page/Edit User Page Field Descriptions *(continued)*

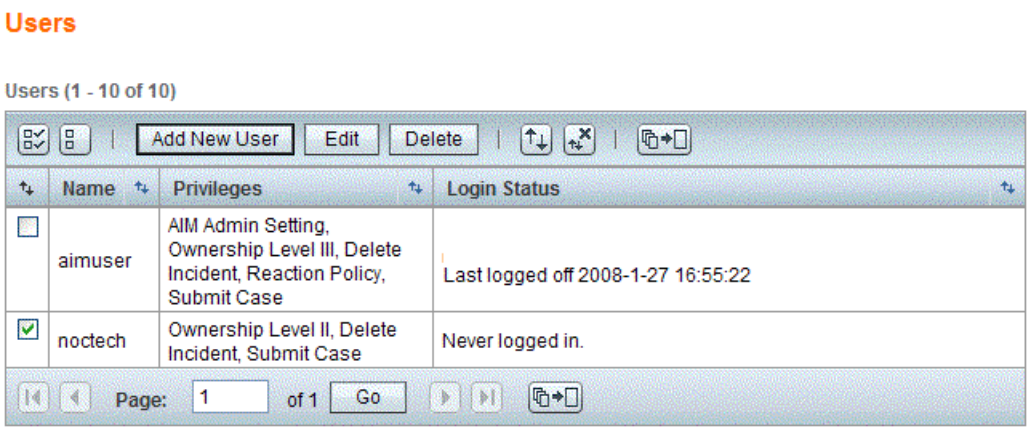
Name	Description	Privileges	Range/Length	Default
Ownership Privilege	Three levels of AIM user ownership are provided that the administrator can use when assigning new user privileges: ■ Level I ■ Level II ■ Level III See Table 53 on page 136.	AIM Admin Settings	N/A	None
Delete Incident Privilege	AIM 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

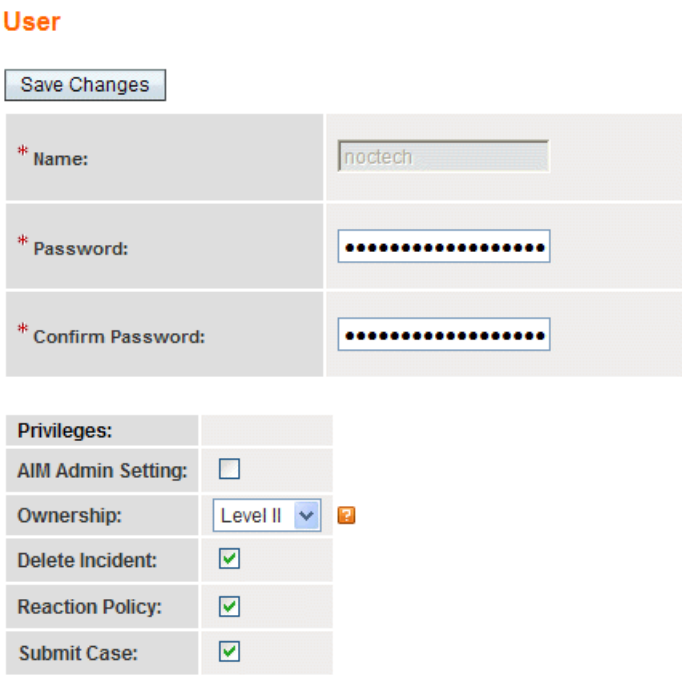
You can edit an AIM user password and privileges.

To edit an AIM user, follow these steps:

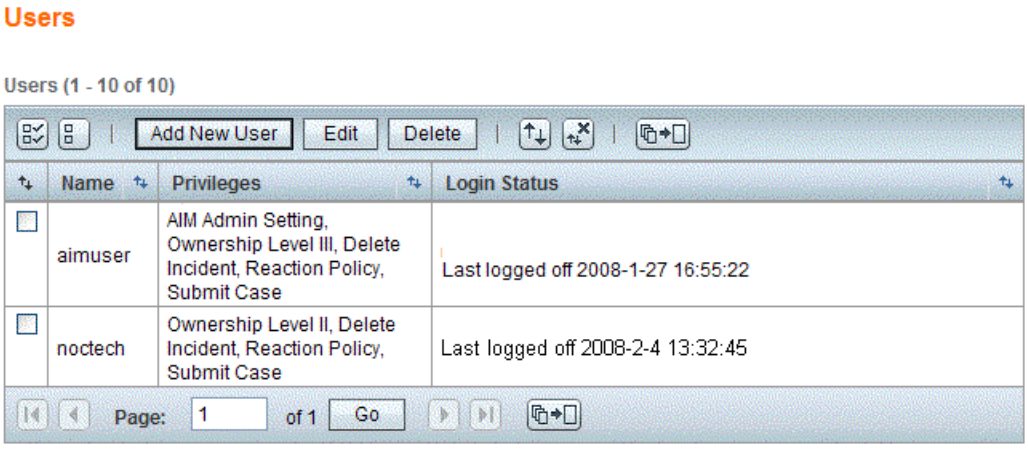
1. Click Settings > Users. The Users page appears.
2. Select the AIM user you want to edit. The Edit button is enabled.



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 139.
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.

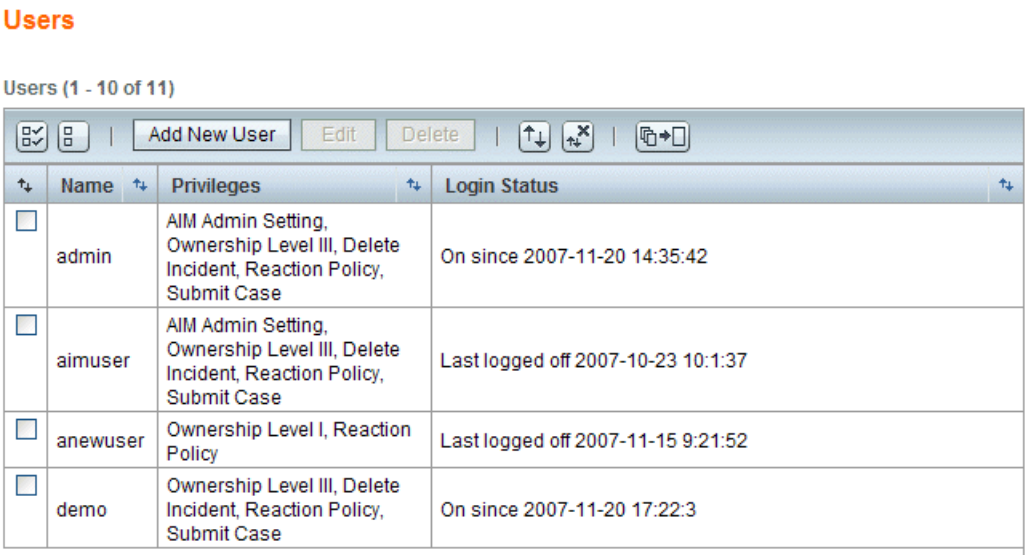


Using the User Table

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” on page 142

Users Table Description

Table 57 on page 142 describes the User table command buttons.

Table 57: 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 58 on page 143 describes the Users table columns.

Table 58: Users Table Columns

Name	Description	Privileges
Name	Name of AIM user.	Not allowed to modify
Privileges	AIM privileges assigned to user, see Table 54 on page 137 for description of AIM user privileges.	Not allowed to modify
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

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 14

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. You must create AIM users before creating AIM user groups. User group members are selected from the existing pool of AIM users. For more information about creating users, see “Advanced Insight Solutions Overview” on page 3.

You can associate user groups with device groups using the User Group Settings page or the Device Group Settings Page. For more information about creating AIM device groups, see “Creating Device Groups” on page 98.

To create AIM user groups, you must have Admin Settings privileges.

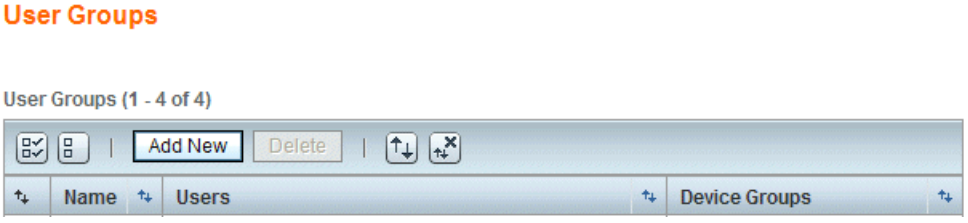
This chapter includes the following information:

Creating a New User Group

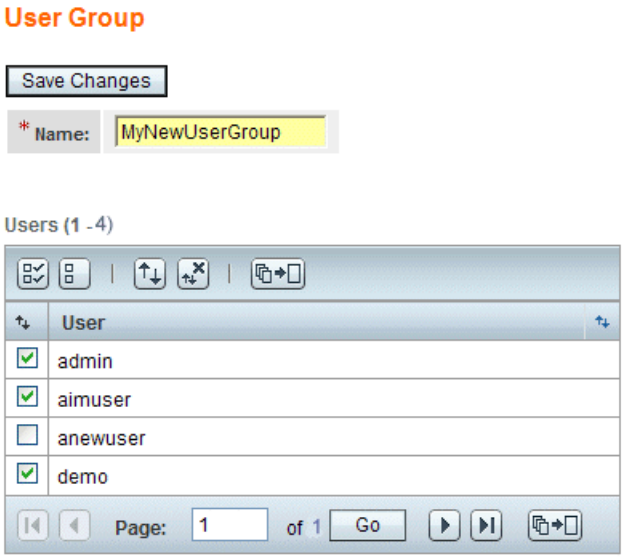
You must be the AIM administrator or have AIM Admin Setting privileges to create a user group. When you create a user group, the User Group table appears without the Associated Device Groups table displayed.

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.

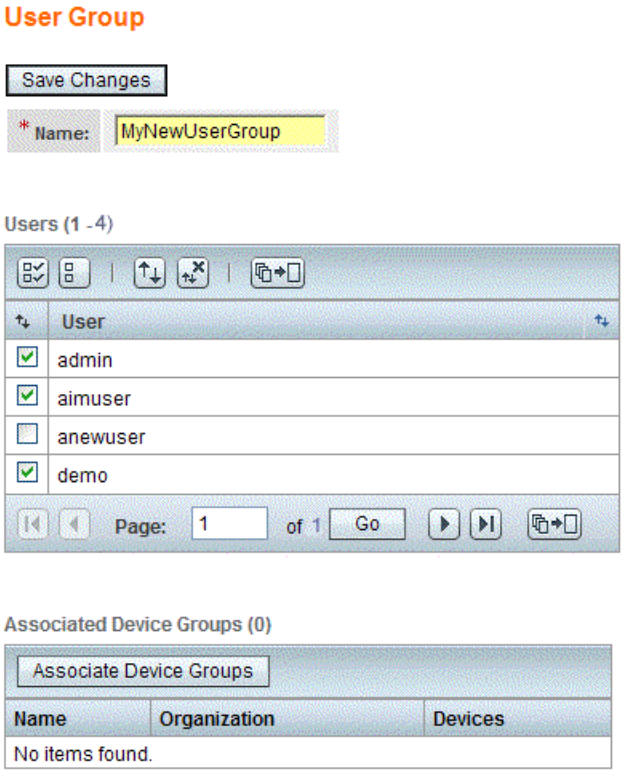


2. Click Add New. The User Group page appears.

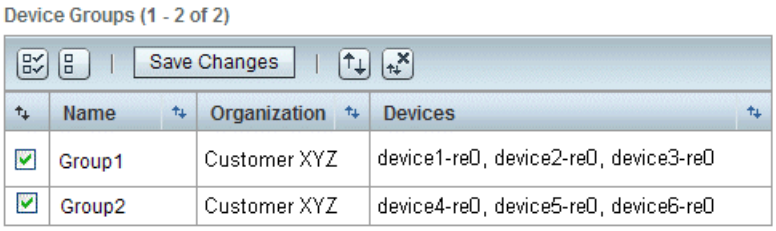


3. In the Name field, type a unique name for the user group.
4. In the Users table, select the users you want to add to the user group.
5. Click Save Changes. This saves the new user group settings. For more information about the User Group page, see “User Group Page Description” on page 148.

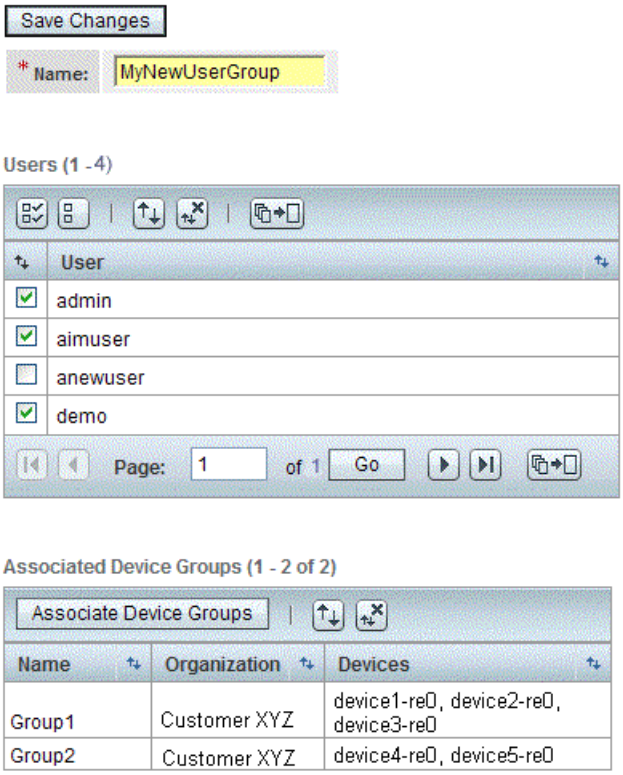
   The Associate Device Groups table appears below the User’s table.



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 149 and “User Group Table Elements Descriptions” on page 148.

User Group Page Description

Table 59 on page 148 describes the User Group page columns.

Table 59: 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
Users 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
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
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

User Group Table Elements Descriptions

Table 60 on page 149 describes the User Group table elements.

Table 60: 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 61 on page 149 describes the User Group table columns.

Table 61: User Group Table Column Descriptions

Name	Description	Privileges
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
Users	List of existing users selected to be in user group.	Not allowed to modify
Device Groups	List of existing device groups that have been associated with the user group	Not allowed to modify

Associate Device Groups Table Element Descriptions

Table 62 on page 149 describes the Associate Device Groups table command button.

Table 62: 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 63 on page 150 describes the Associate Device Groups table columns.

Table 63: Associated Device Groups Table Columns Descriptions

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

Deleting a User Group

When you delete a user from a user group, that user no longer has access to AIM incidents, intelligence updates, and proactive cases. A message in My AIM Home notifies that user about the access change when that user first logs in to AIM.

To delete a user group, follow these steps.

1. Click Settings > User Groups. The User Group page appears.
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 15

Using My AIM Home

This chapter describes the information that you view on the 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.

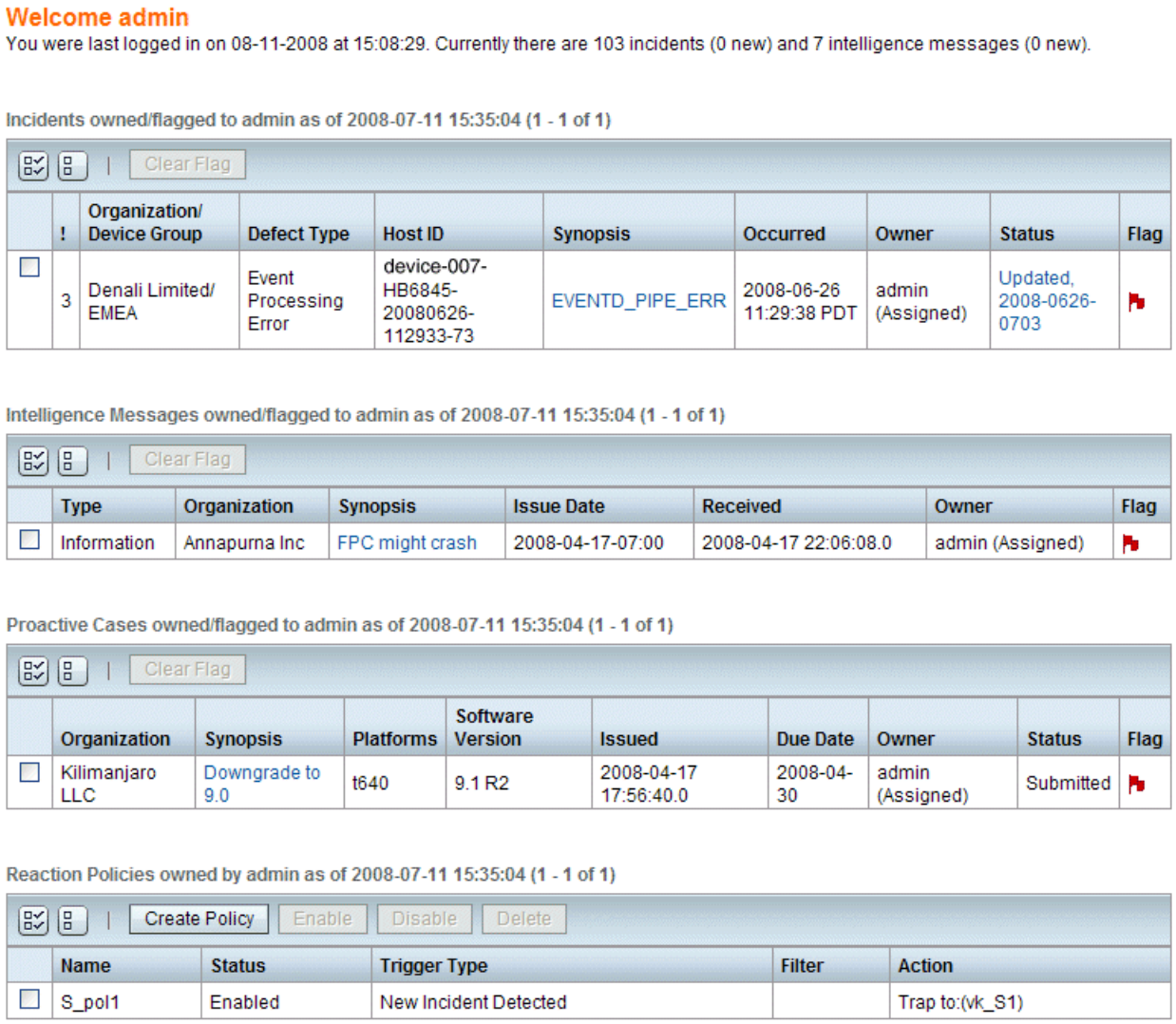
When you first log in to the AIM application, you see the My AIM Home page. The My AIM Home is populated only if the AIM application has been set up to connect to the archive location of a device, and setup to connect to JSS for incident case management and intelligence information, see “Advanced Insight Solutions Overview” on page 3. 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 155, “Populating the Intelligence Messages Table” on page 155, “Populating the Proactive Cases Table” on page 155, and “Populating the Reaction Policies Table” on page 155..



Welcome admin

You were last logged in on 08-11-2008 at 15:08:29. Currently there are 103 incidents (0 new) and 7 intelligence messages (0 new).

Incidents owned/flagged to admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Clear Flag

	!	Organization/ Device Group	Defect Type	Host ID	Synopsis	Occurred	Owner	Status	Flag
☐	3	Denali Limited/ EMEA	Event Processing Error	device-007-HB6845-20080626-112933-73	EVENTD_PIPE_ERR	2008-06-26 11:29:38 PDT	admin (Assigned)	Updated, 2008-0626-0703	

Intelligence Messages owned/flagged to admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Clear Flag

	Type	Organization	Synopsis	Issue Date	Received	Owner	Flag
☐	Information	Annapurna Inc	FPC might crash	2008-04-17-07:00	2008-04-17 22:06:08.0	admin (Assigned)	

Proactive Cases owned/flagged to admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Clear Flag

	Organization	Synopsis	Platforms	Software Version	Issued	Due Date	Owner	Status	Flag
☐	Kilimanjaro LLC	Downgrade to 9.0	t640	9.1 R2	2008-04-17 17:56:40.0	2008-04-30	admin (Assigned)	Submitted	

Reaction Policies owned by admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Create Policy | Enable | Disable | Delete

	Name	Status	Trigger Type	Filter	Action
☐	S_pol1	Enabled	New Incident Detected		Trap to:(vk_S1)

If an AIM user is removed from a user group, that user will be notified by a message on the My AIM Home page the first time they log in to AIM. When a user is removed

from a user group, that user no longer has access to incidents, intelligence updates, and proactive cases.

If AIM is running in AIM Partner Controller Mode two additional tables appear in My AIM Home: Create Cases and Intelligence Updates. The Create Cases table shows the technical support cases that need to be approved by the end user. Each table includes an approval button.

Populating the Incidents Table

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

- To assign an incident to user, see "Assigning an Incident Owner" on page 186.
- To flag an incident to a user, see "Flagging An Incident to a User" on page 176

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 Update Owner" on page 200.
- To flag an incident to a user, see "Flagging an Intelligence Update To a User" on page 198.

Populating the Proactive Cases Table

The Proactive Cases table is blank until you create a proactive case, own, or until it is flagged to your attention.

- To create a proactive case, see "Using AIM Proactive Case Manager" on page 219
- To assign a proactive case owner, see "Assigning a Proactive Case Owner and Changing Status" on page 232
- To flag a proactive case to a user, see "Flagging a Proactive Case to a User" on page 233

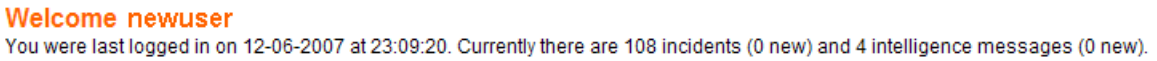
Populating the Reaction Policies Table

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

To create a reaction policy, see "Creating a Reaction Policy" on page 238.

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 156. It also describes the standard navigation actions in each AIM table; see "Navigating in AIM Tables" on page 157.

Using the Table Selection, Sort, and Display Icons

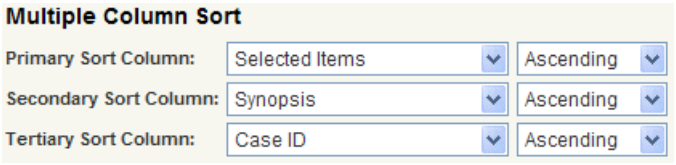
Table 64 on page 156 describes the icons that represent actions used to manipulate data in AIM tables. These icons are located along the top and bottom of each table.

Table 64: 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.
	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 156.
	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

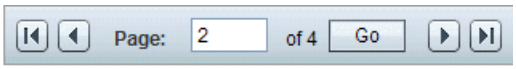
Using the Multiple Column Sort Area

The AIM table Multiple Column Sort area appears when you click the Multiple Column Sort icon in a table. 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.



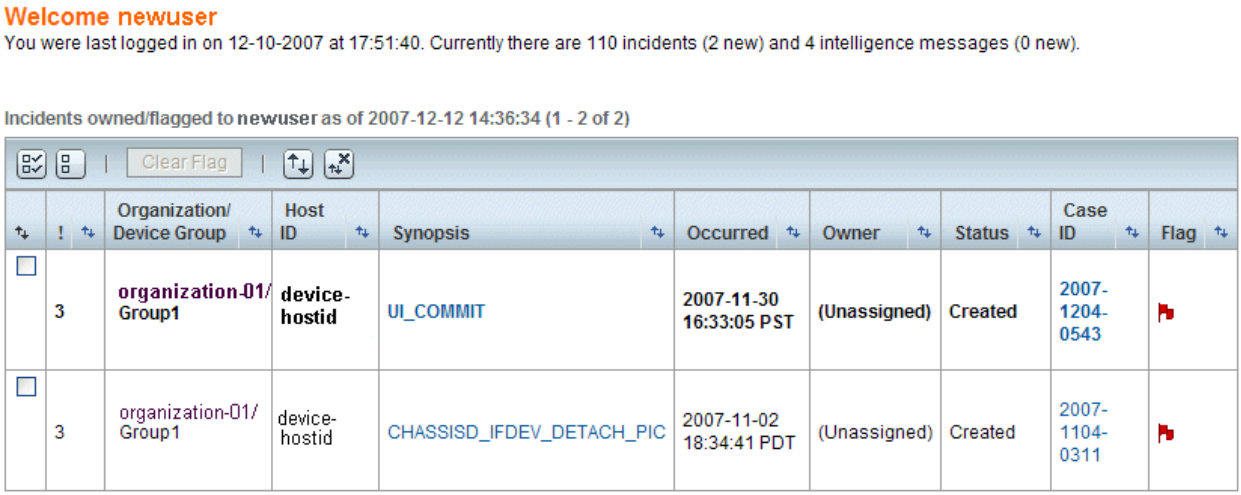
From left to right in the table navigation area, you can:

- 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 an archive location and are specifically owned by or flagged to the user.

- To assign an incident to user, see “Assigning an Incident Owner” on page 186.
- To flag an incident to a user, see “Flagging An Incident to a User” on page 176.



For information about using the Incidents table, see “Using AIM Incident Manager” on page 163.

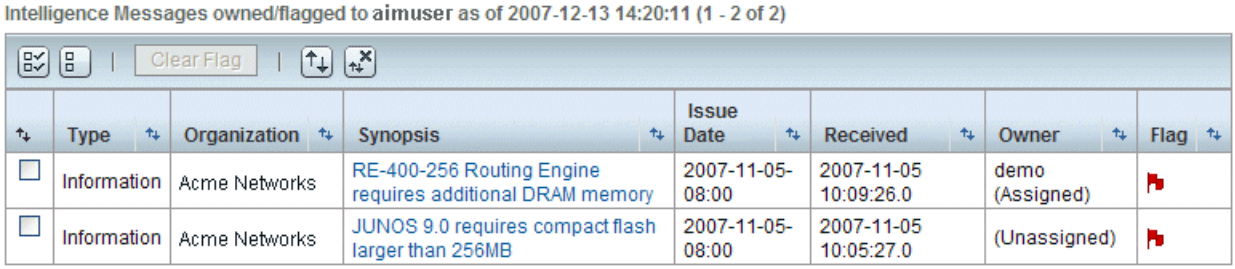
Using the Intelligence Messages Table

The Intelligence Messages table displays the three types of intelligence information that appear in AIM:

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

The intelligence Messages table displays the messages that are owned and flagged to the user.

- To own an incident, see “Assigning an Intelligence Update Owner” on page 200.
- To flag an incident to a user, see “Changing Intelligence Update Owner Status” on page 201.

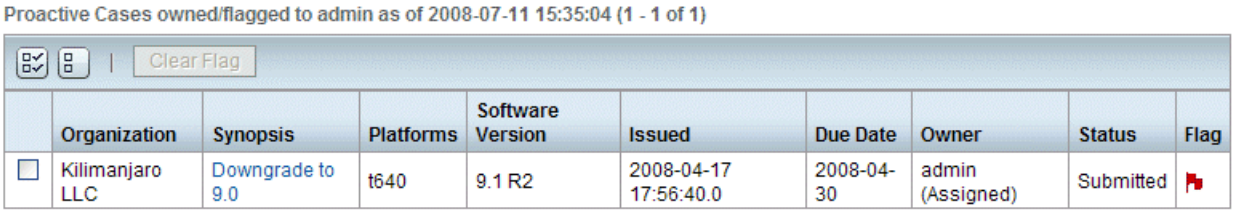


For more information about using the Intelligence Messages table, see “Using AIM Intelligence Manager” on page 191.

Using the Proactive Case Table

The Proactive Cases table displays the cases that are owned and flagged to the user.

- To own a proactive case, see “Assigning a Proactive Case Owner and Changing Status” on page 232.
- To flag a proactive case to a user. see “Flagging a Proactive Case to a User” on page 233.


Proactive Cases owned/flagged to admin as of 2008-07-11 15:35:04 (1 - 1 of 1)

Clear Flag

	Organization	Synopsis	Platforms	Software Version	Issued	Due Date	Owner	Status	Flag
☐	Kilimanjaro LLC	Downgrade to 9.0	t640	9.1 R2	2008-04-17 17:56:40.0	2008-04-30	admin (Assigned)	Submitted	

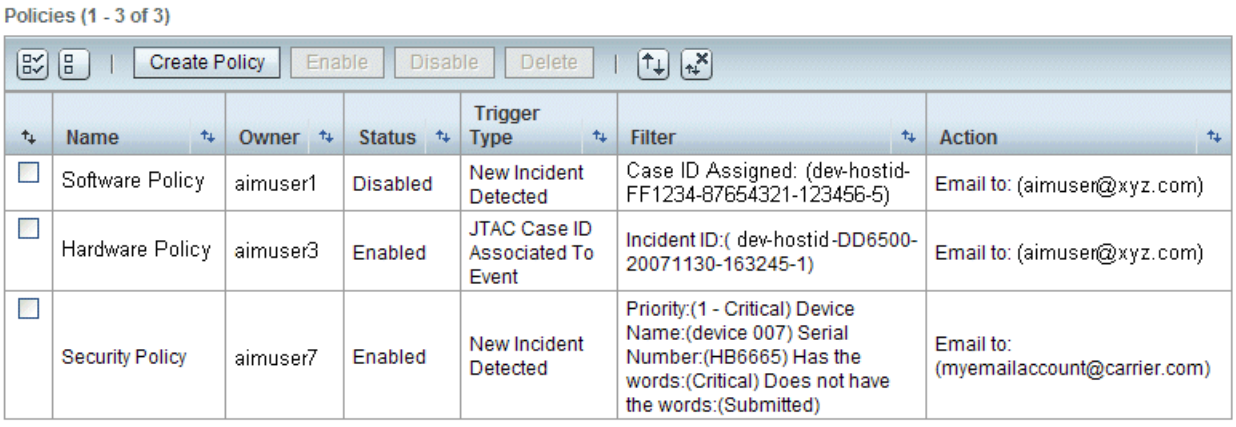
For more information about using the Proactive Cases table, see “Using the Proactive Case Table” on page 159

Using the Reaction Policies Table

The Reaction Policies table provides shows 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

Reaction Policies


Policies (1 - 3 of 3)

Create Policy | Enable | Disable | Delete

	Name	Owner	Status	Trigger Type	Filter	Action
☐	Software Policy	aimuser1	Disabled	New Incident Detected	Case ID Assigned: (dev-hostid-FF1234-87654321-123456-5)	Email to: (aimuser@xyz.com)
☐	Hardware Policy	aimuser3	Enabled	JTAC Case ID Associated To Event	Incident ID:(dev-hostid-DD6500-20071130-163245-1)	Email to: (aimuser@xyz.com)
☐	Security Policy	aimuser7	Enabled	New Incident Detected	Priority:(1 - Critical) Device Name:(device 007) Serial Number:(HB6665) Has the words:(Critical) Does not have the words:(Submitted)	Email to: (myemailaccount@carrier.com)

For information about using the Proactive Case table and creating reaction policies, see “Creating Reaction Policies” on page 237.

Chapter 16

Using the AIM Drafts Folder

This chapter describes how the AIM Drafts folder works. AIM automatically saves every 30 seconds when you create or modify certain objects. This action allows you to navigate away from an object to do another AIM operation, then come back to that object later in the Drafts folder to finish.

Autosave occurs when you create:

- Organizations
- Device Groups in Organizations
- Reaction Policies
- Proactive Cases

When you create any of the objects listed above, AIM automatically saves a draft after the first 30 seconds. Then AIM saves again each 30 seconds after that.

The Drafts folder in the AIM navigation area displays, in parentheses, the number of objects that are waiting for you to finish. Each object is active in AIM (and removed from the Drafts folder) immediately after it is finished.

Autosave also occurs while you modify a filed on the following pages:

- Intelligence Updates
- Proactive

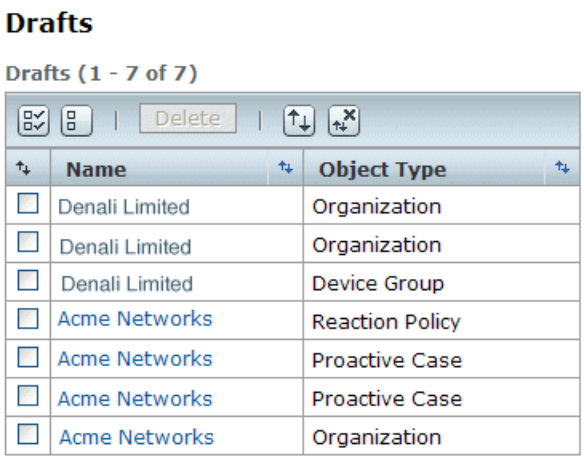
When you navigate to modify a field on these pages, the Save Changes button is disabled. After you modify a field, the Save Changes button is enabled. If after 30 seconds you have not saved a modified field, autosave occurs and the Save Changes button is disabled.

This chapter includes the following information:

Viewing Objects in the Drafts Folder

To view AIM objects that you have created but have not finished, follow these steps:

1. Click Drafts. The Drafts page appears.



2. Click the object name. The name is a link that opens the object creation page. For example, if you were creating a proactive case, the appropriate Proactive Case Manager page appears.
3. Finish creating the AIM object and save the changes. The object is removed from the Drafts folder.

Deleting Objects in the Drafts Folder

You can remove an object from the Drafts folder if you do not want to finish creating it.

To remove an object from the Drafts page, follow these steps:

1. Click Drafts in the AIM navigation area. The Drafts page appears.
2. Select one or more objects. The Delete button is enabled.
3. Click Delete. The selected objects are removed from the Drafts page and from the AIM database.

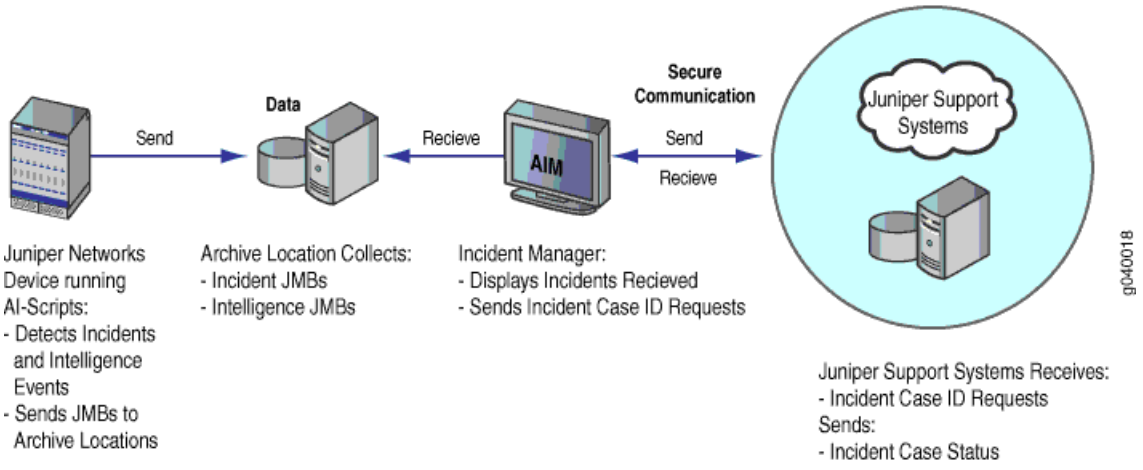
Chapter 17

Using AIM Incident Manager

The Incident Manager provides a view of all incidents received by Advanced Insight Manager. Incidents are problem event Juniper Message Bundles that are detected and deposited in device archive locations. AIM Incident Manager provides a user interface to view incidents alphabetically by organization name and device group. Incident Manager also displays all open JSS Technical Support cases for all Site IDs, The Technical Support user interface is available in both standard and partner controller modes.

Figure 15 on page 163 shows the flow through which AIM receives incident JMBs and manages them to successful case resolution in a direct customer engagement model.

Figure 15: Incident Flow Diagram for Direct Customer Engagement Model



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.

For information about the incident data flow for a partner and end-user engagement model, see“Incident Data Flow for Partner and End-User Engagement Model” on page 165.

To use Incident Manager, you must have AIM admin and AIM ownership privileges.

From Incident Manager, you can:

- Filter the incident data in the data by what you need to view, for example, by defect, device type, device group, or organization
- View statistics that summarize the incident data shown in the table. See “Statistics Dashboard Description” on page 168
- View detailed incident information as described in “Viewing Incident Details (Incident for Device)” on page 180.
- Change incident ownership, as described in “Assigning an Incident Owner” on page 186.
- View and change incident status, as described in “Changing Incident Owner Status” on page 187.
- Submit and request a case ID, as described in “Submitting a Case Request” on page 173.
- Flag an incident to a user, as described in “Flagging An Incident to a User” on page 176.
- Clear Flag—Removes the flag from any of the selected Incidents as described in “Clearing a Flag” on page 201.
- 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 JSS. See “Submitting a Case Request” on page 173.
- Create 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. See “Creating Reaction Policies” on page 237.
- Delete any selected Incidents. See “Changing Incident Owner Status” on page 187“Deleting an Incident” on page 139.
- View all open JSS Technical Support cases. See “Using the Technical Support Tab” on page 188.

This chapter includes the following sections:

Incident Data Flow for Partner and End-User Engagement Model

This section describes the incident flow at the end user and the partner in an AIS partner and end-user engagement model.

Incident Flow at the End User Site

1. An incident JMB is deposited in the end-user AIM database.
2. The incident JMB is detected by the end-user AIM.
3. The end user submits a case for the incident in Incident Manager. (See "Submitting a Case Request" on page 173.
4. The end user AIM service sends a Create Case request to the partner AIM.
5. The partner AIM acknowledges receiving the case with a transaction ID (the partner AIM database ID of the incident).
6. The end-user AIM service begins polling the partner AIM service for the incident case creation ID.
7. The partner AIM service returns the incident case ID and the case link and stores it in the end-user database.
8. The end-user AIM service stops polling for the incident case and starts polling for the incident case update status.

Incident Flow at the Partner Site

1. The partner AIM receives a create incident case request from the end-user AIM.
2. The partner AIM service detects the create incident case and process the incident JMB in the database.
3. The partner AIM sends a response to the end user containing a transaction ID (partner AIM database incident ID).
4. A new incident appears in the partner AIM Incident Manager.
5. A partner user with AIM administrative privileges decides whether to resolve the issue or send it JSS. If the partner decides to send the incident to JSS with the end-user alias and trace route. If the partner sends the incident case request to JSS, including the end-user alias and trace route.
6. The partner decides whether to use the JSS incident case ID and link. If the partner decides not to use the JSS incident case ID, edit the following fields in the AIM Settings > General Settings page:
   - Partner case ID
   - Partner case link
   - Partner case status
7. Save the settings.

Using the Incident Manager Tab

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 “Advanced Insight Solutions Overview” on page 3.

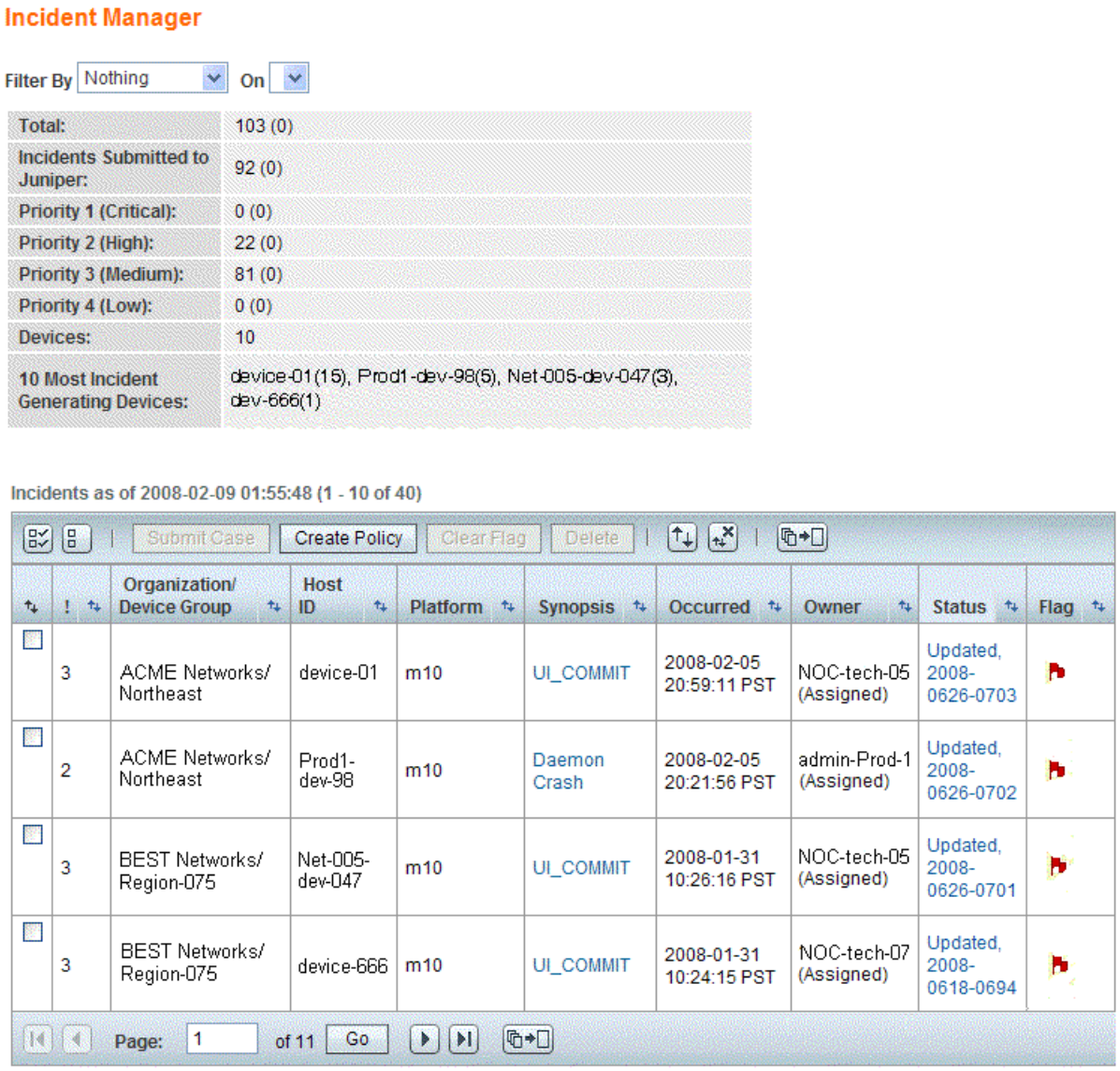
Any incident displayed in bold in Incident Manager indicates that incident has been detected, assigned, or flagged to the user since the last time you logged into AIM.

This section includes the following:

NOTE: If you are running AIM in standalone mode and navigate to the Proactive Case Manager page, the follow message appears: Proactive cases can not be submitted because there are no organizations that either contain devices or have valid credentials. Proactive Case Manager is disabled when AIM is not connected to JSS (Standalone mode).

To view the Incident Manager table, do the following:

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



For more detailed information about the Incident Manager page, see “Incident Manager Page Descriptions” on page 167

Incident Manager Page Descriptions

This section describes the parts of the Incident Manager page.

- Incident Manager Table Button Descriptions on page 169
- Incident Manager Table Column Descriptions on page 170

Filter By and Filter On Drop-Down List Box Description

Table 65 on page 168 describes the operation of the Incident Manager Filter By and On drop-down list boxes.

Table 65: Incident Manager Table Filter By and On Drop-Down List Box Description

Name	Description	Privileges	Enabled/Disabled	Results
Filter By drop-down list box	Displays the items on which you can filter the data in the Incident Manager table: ■ Nothing—(Default) Displays a blank On drop-down list box, and no filtering occurs in the table. ■ Defect—Displays all or the available individual defect types in the On drop-down list box. (This option is only available in Incident Manager.) ■ Device—Displays all or the available individual device names in the On drop-down list box. ■ Device Group—Displays all or the available individual device group names in the On drop-down list box. ■ Organization—Displays all or the available individual organization names in the On drop-down list box.	None, AIM User	Always enabled	Displays the associated available items in the On drop-down list box. See the Description for this list box.
On drop-down list box	Is associated with the Filter By drop-down list box, and displays the items available on which to be filtered: all or the individual item names depending on the Filter By option selected.	None, AIM User	Always enabled	Displays the available items on which to sort based on the Filter By option selected.

Statistics Dashboard Description

Table 66 on page 169 describes the Statistics dashboard at the top of the Incident Manager table that provides a summary of displayed device incident data.

You can show the statistics dashboard by clicking the plus sign. The default is for the statistics dashboard to be hidden.

Table 66: Incident Manager Table Statistics Dashboard

Statistics	Description	Privilege Required to Modify
Total	Based on the current filter, the total number of incidents and number of new incidents since the user was last logged in. Format example: 25 (5)	None; not allowed to modify
Incidents submitted to Juniper	The number of incidents displayed in the table that have been reported to JSS. Format example: 15 (1)	None; not allowed to modify
Priority 1 (Critical)	Based on the current filter, the number of incidents with priority 1 and number of new incidents with priority 1 since the user was last logged in. Format example: 5 (0)	None; not allowed to modify
Priority 2 (High)	Based on the current filter, the number of incidents with priority 2 and number of new incidents with priority 2 since the user was last logged in. Format example: 10 (3)	None; not allowed to modify
Priority 3 (Medium)	Based on the current filter, the number of incidents with priority 3 and number of new incidents with priority 3 since the user was last logged in. Format example: 5 (2)	None; not allowed to modify
Priority 4 (Low)	Based on the current filter, the number of incidents with priority 4 and number of new incidents with priority 4 since the user was last logged in. Format example: 5 (0)	None; not allowed to modify
Devices	The number of devices represented by the incidents displayed in the table. Format example: 8	None; not allowed to modify
10 Most Incident Generating Devices	A list of the top 10 devices that have generated the most incidents in descending order. Format example: deviceA (75), deviceB (72), deviceC (70), deviceD (67), deviceE (64), deviceF (62), deviceG (59), deviceH (56), deviceI (54)	None; not allowed to modify
Show/Hide Statistics	Clicking on the plus or minus image will show or hide the statistics at the top of the page.	None; not allowed to modify

Incident Manager Table Button Descriptions

Table 67 on page 169 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 JSS 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 JSS.	None, AIM User	Enabled when you select an incident.	Case ID submitted message appears.

Table 67: Incident Manager Table Command Button Descriptions *(continued)*

Button Name	Description	Privileges	Enabled/Disabled	Results
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.	AIM User	Always enabled	Displays Reaction Policies page.
Clear Flag	Removes the flag from any of the selected Incidents.	AIM User	Enabled when you select an incident.	Removes flag.
Delete	Removes any selected Incidents	AIM User	Enabled when you select an incident.	Removes incident.

Incident Manager Table Column Descriptions

Table 68 on page 170 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—Critical ■ 2—High ■ 3—Medium ■ 4—Low	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-JMB
Platform	Indicates the platform of the device the incident occurred on.	N/A	Set by the JUNOS System
Synopsis	Text description of the incident. This field is a link and can be used to navigate to the detail screen of the selected incident.	N/A	Set by the JUNOS system
Occurred	Time that the JUNOS device detected the incident.	Date and time	N/A

Table 68: Incident Manager Table Column Descriptions *(continued)*

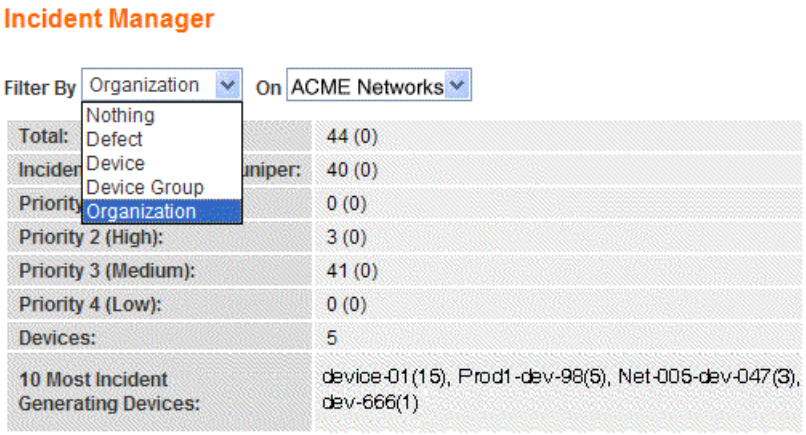
Column	Description	Range/Length	Default
Owner	User that has currently been assigned ownership for this incident, as well as the owner's status regarding the incident. Format: owner (status)	Owner—Any valid user login for AIM Status—assigned, in progress, completed	Unassigned
Status	The JSS case status of this incident.	Initial, Submitted, Created, Updated	Initial
Case ID	The case ID assigned by the JSS Case Management system. This field is a link and can be used to navigate into the JSS Case Management application.	N/A	Empty until case created.
Flag	Indicates whether this entry has been flagged to the user for inspection.	N/A	N/A

Filtering Incident Manager Table Data

The Filter By and On drop-down list boxes at the top of the Incident Manager table allow you to display specific incident data necessary for you to monitor devices on your network. You can filter by defect, device, device group, and organization. Filtered data is displayed in the Statistics dashboard and the Incident Manager table.

To filter Incident Manager table data to show incidents by specific criteria, follow these steps:

1. In the Filter By drop-down list box. select the filter category This action automatically displays the specific filter options in the On drop-down list box. See Table 69 on page 173.



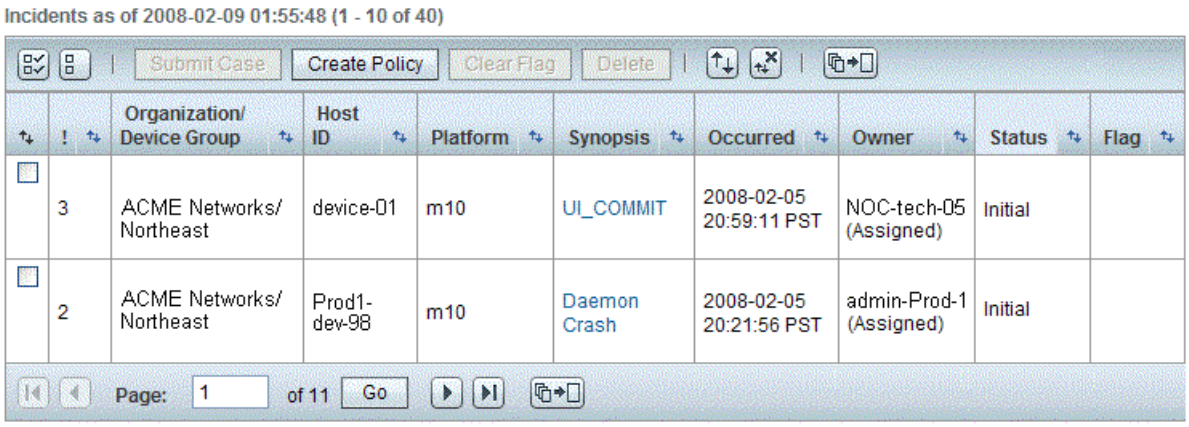


Table 69 on page 173 describes the operation of the Filter By and On drop-down list boxes for filtering Incident Manager table data.

Table 69: Filter By and On Drop-Down List Box Operation

Filter By drop-down list box	On drop-down list box
Nothing	The On drop-down list box is blank, and no filtering occurs.
Defect	Displays the list of all incident defect types on which you can filter.
Device	Displays the list of all devices names managed by AIS on which you can filter incident data.
Device Group	Displays the list of all device group names on which you can filter incident data.
Organization	Displays the list of all organization names on which you can filter incident data.

2. In the On drop-down list box, select the filter option.

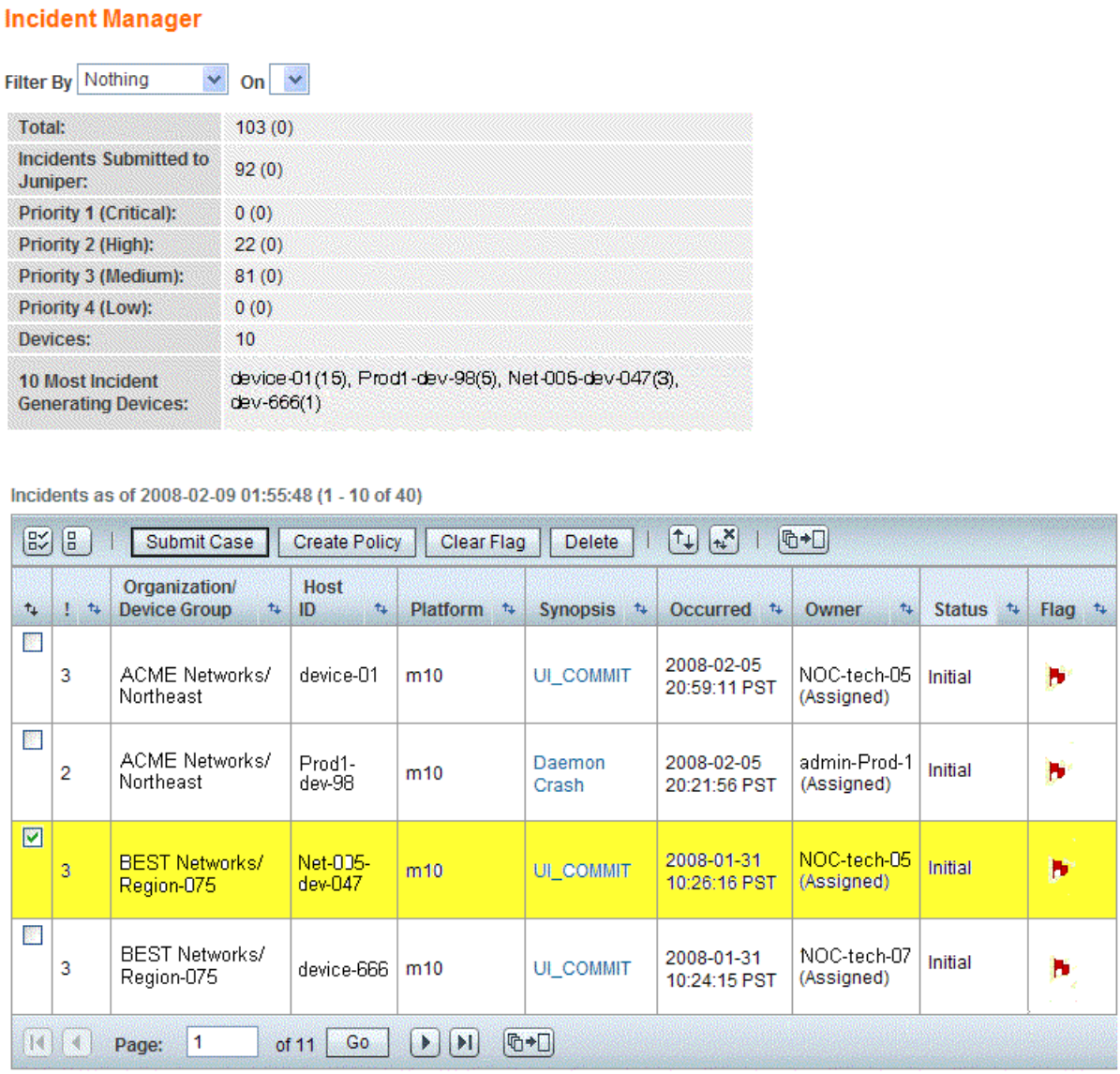
Submitting a Case Request

From the Incident Manager table, you can easily submit a case request to Juniper Support Systems (JSS). After 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 request, follow these steps:

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



2. 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.

   The incident case ID appears in the Status cell.

Creating a Policy

For detailed information about creating a reaction policy, see “Creating Reaction Policies” on page 237.

Flagging An Incident to a User

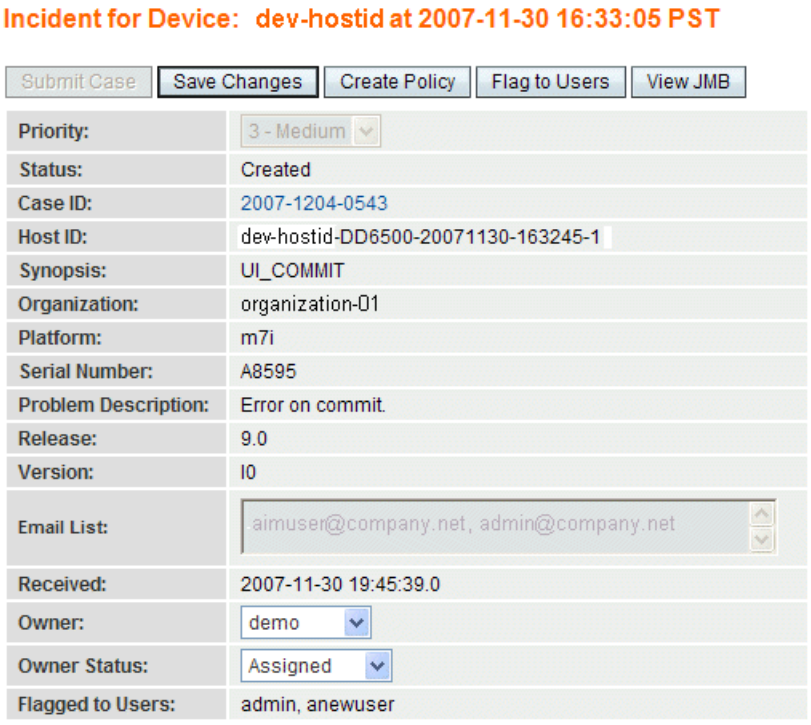
Flagging an incident informs an AIM user who might be impacted or needs to be aware of an incident.

You can flag an incident to a user. Flagging an incident, displays that incident in Incident Manager table.

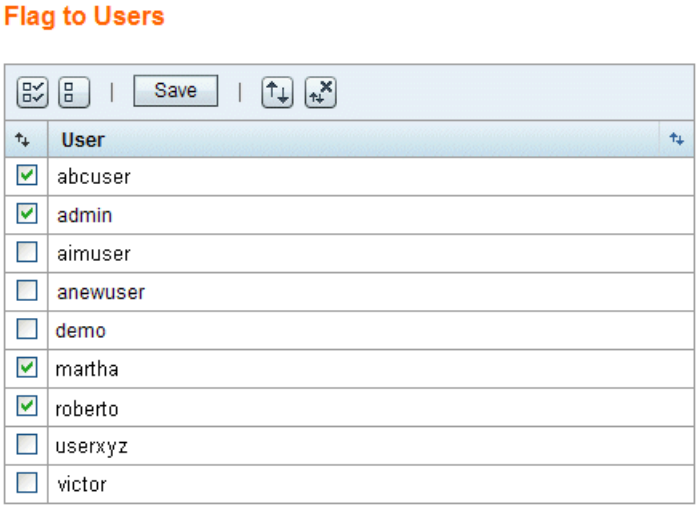
Incidents that are bold indicate that they have been flagged to you since the last time you logged into AIM.

To flag an incident to a user, follow these steps:

1. From the Incident Manager table, click the incident synopsis link. The Incident Details page appears.



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

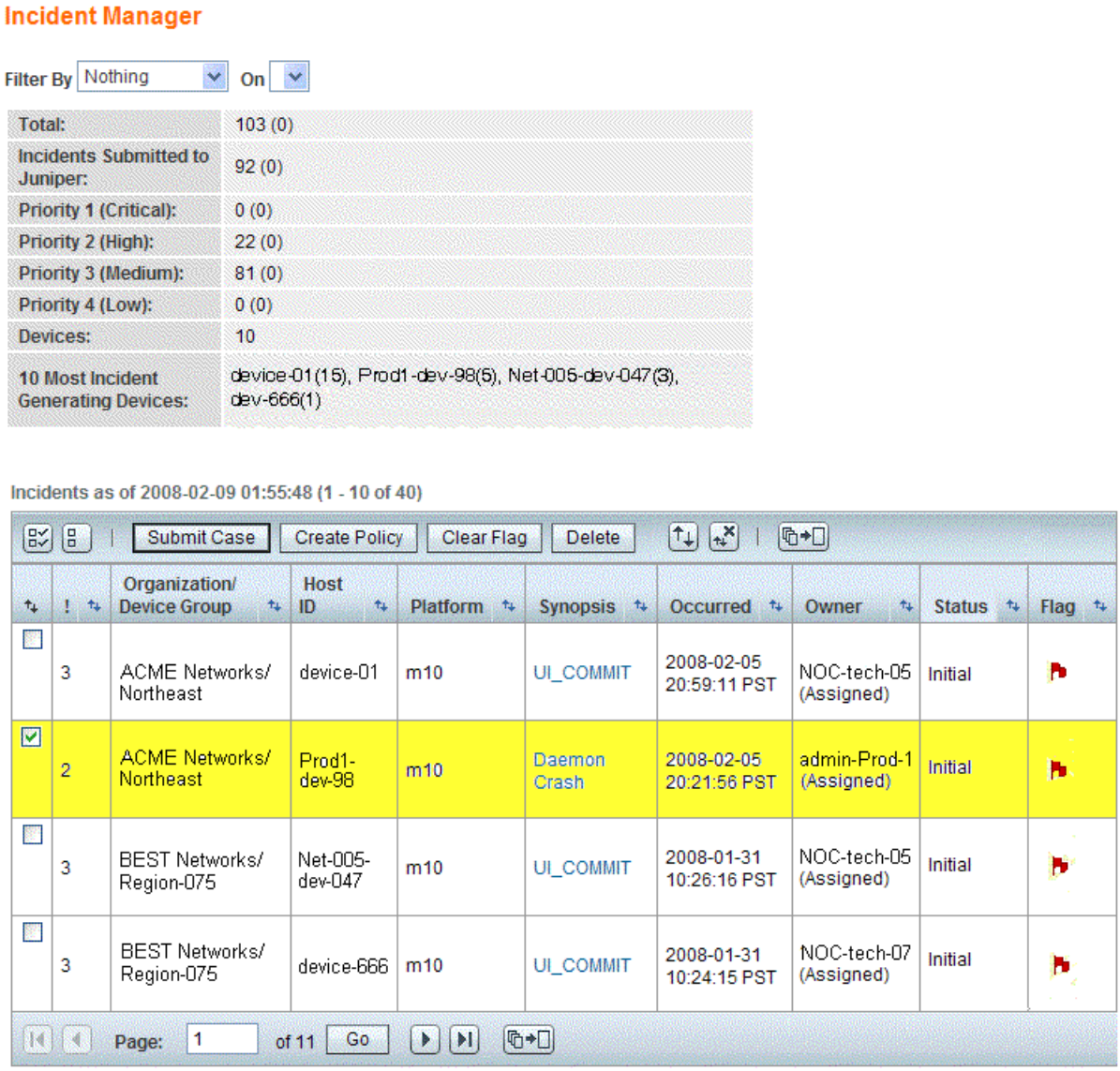


3. On the Flag to Users page, select the users to whom you want to flag the incident.
4. Click Save. The flag appears in the incident Flag column in the Incident Manager table.

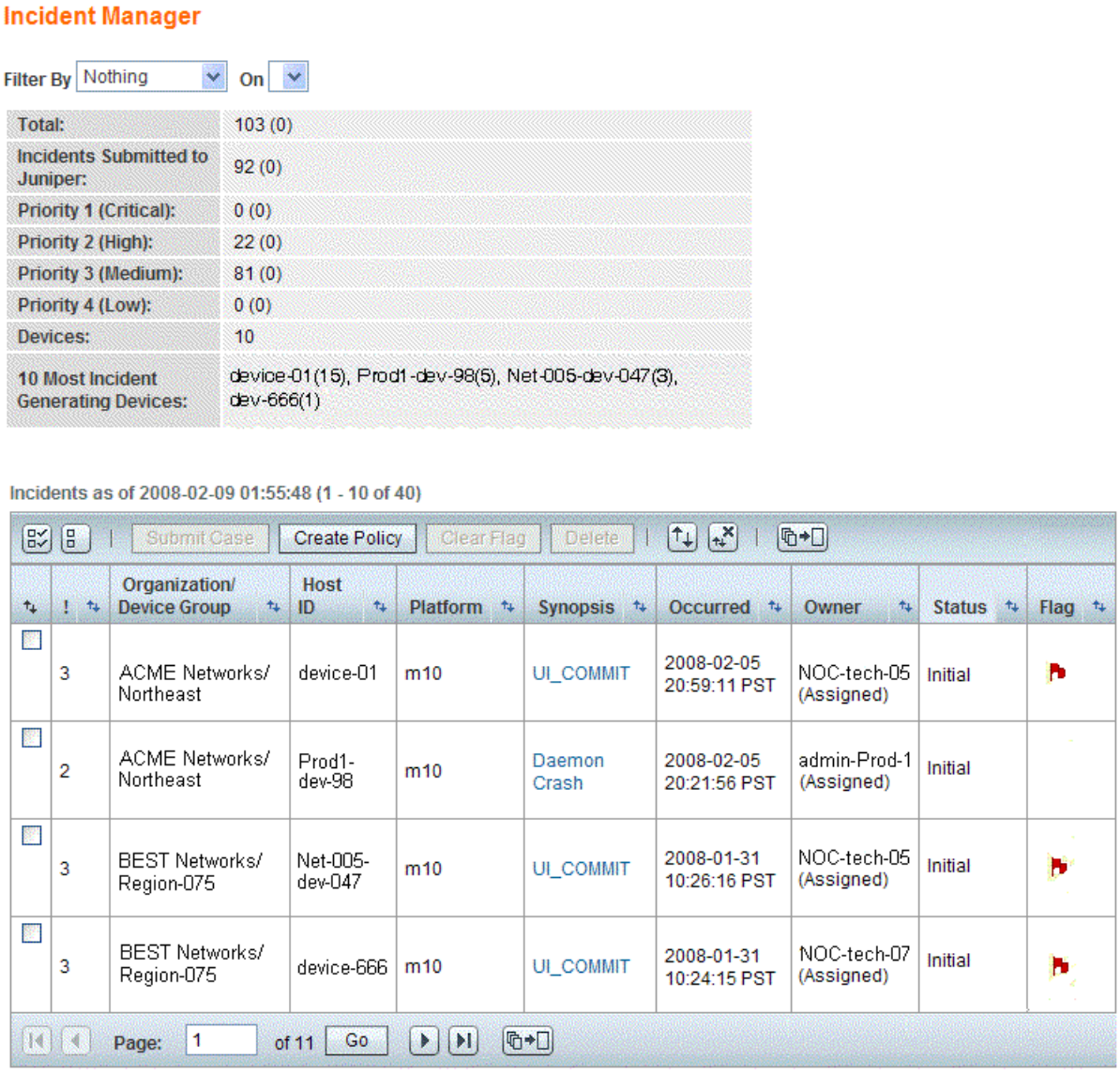
Clearing a Flag

To clear a 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.

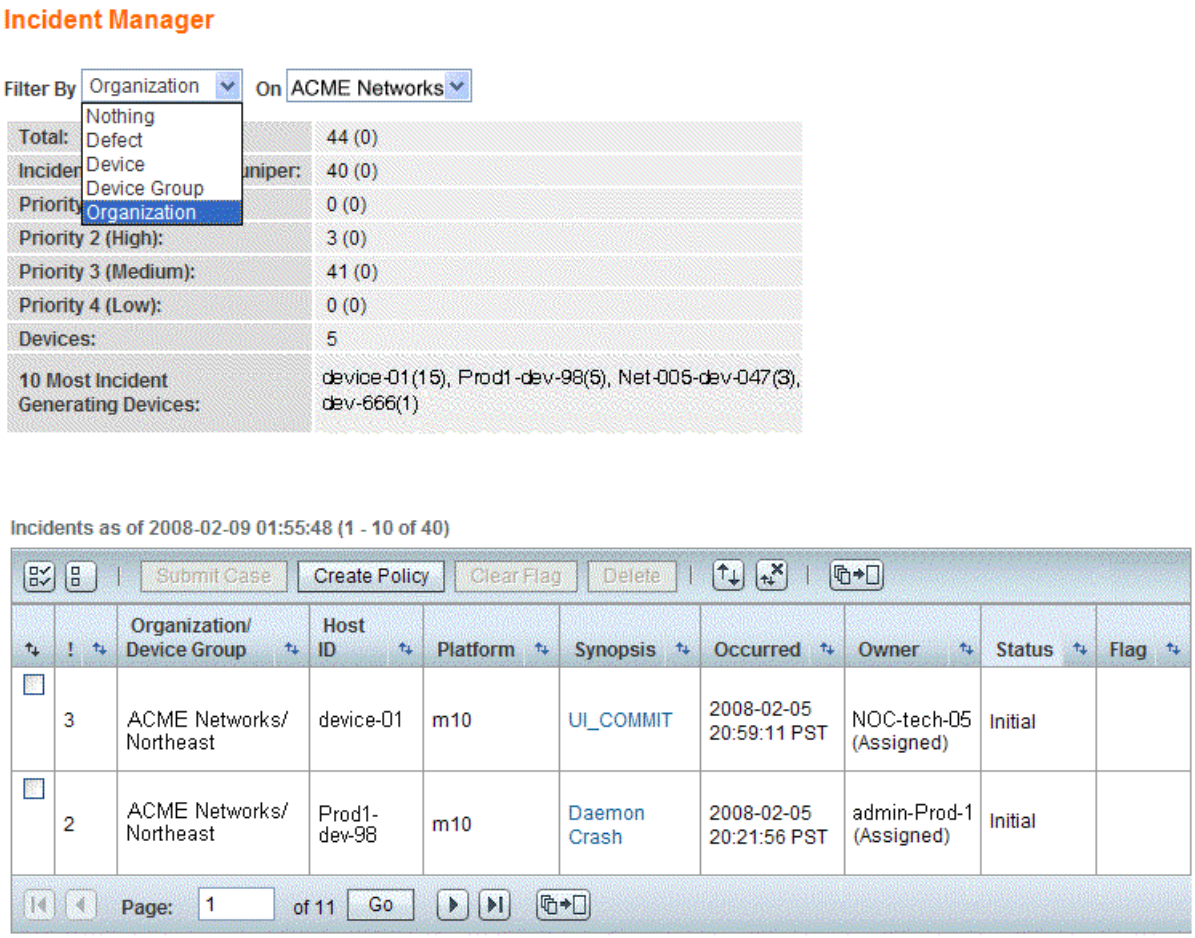


Viewing Incidents by Organization

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

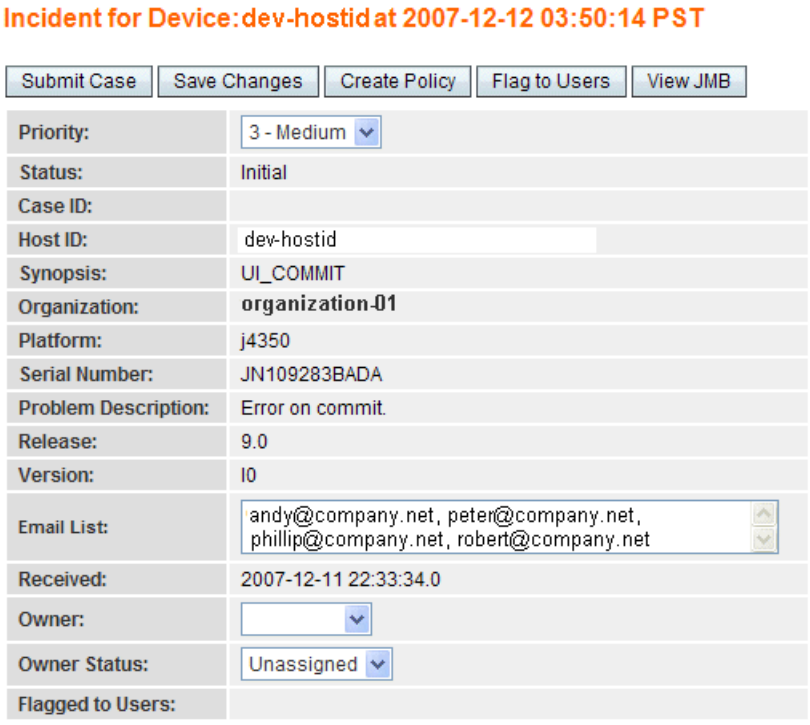
To view incidents by AIM organization, do the following:

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



Viewing Incident Details (Incident for Device)

To view incident details, click the incident Synopsis link in the Incidents table. The Incident for Device page appears.



The Incident for Details page lets you perform the following AIM actions:

- Submit a case, as described in "Submitting a Case Request" on page 173.
- Create an incident reaction policy, as described in "Creating a Policy" on page 175.
- Flag an incident to a user, as described in "Flagging An Incident to a User" on page 176.
- View an incident Juniper Message Bundle (JMB), as described in "Viewing Incident Juniper Message Bundle (JMB)" on page 184.
- Change Incident owner status, as described in "Changing Incident Owner Status" on page 187.

For more information about the Incident Detail (Incident for Device), see "Incident Details (Incident for Device) Page Description" on page 181

Incident Details (Incident for Device) Page Description

Table 70 on page 182 describes the fields on the Incident for Device page.

Table 70: Incident Details (Incident for Device) 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 JSS.	AIM User	Enabled when you select an incident.	Case ID submitted message appears.
Save Changes	Saves changes of any modified fields. Priority and E-mail List cannot be modified if the incident has already been submitted to JSS.	AIM User	Always enabled	Saves changes to AIM database.
Create Policy	Initiates creation of a Reaction Policy. If any Incidents are selected, the policy created will be limited to just those incidents specified. If no Incidents are selected, then the policy will be applied to all the Incidents in the system.	AIM User	Always enabled	Displays Reaction Policies page.
Flag to Users	Sets which user the incident is flagged to for attention and review.	AIM User	Enabled when you select an incident.	Removes the flag.
View JMB	Displays detailed information about the selected incident.	AIM User	Enabled when you select an incident.	Displays the View JMB page

Table 71 on page 182 describes the columns in the Incident Manager table.

Table 71: Incident Details (Incident for Device) Table Column Descriptions

Column	Description	Range/Length	Default
(AIM Partner Controller) Partner Customization	Allows a partner Controller AIM User to specify whether or not they wish to use their case links, Case IDs, and Case Status. The case status String provided is not displayed to the end customer, but is used for updating the AIM status in the Incident View.	N/A	Use Home Base

Table 71: Incident Details (Incident for Device) Table Column Descriptions *(continued)*

Column	Description	Range/Length	Default
Priority	Indicates the priority of the selected incident: ■ 1—Critical ■ 2—High ■ 3—Medium ■ 4—Low	1-4	Set by the device. The priority can be overridden by a reaction policy.
(AIM Partner Controller) Partner Case Link	The URL to the partner's case resolution system.	Enabled/Disabled	Disabled
(AIM Partner Controller) Home Base Status	The JSS case status of resolving this incident.	Initial, Submitted, Created, and Updated	Empty until a case is created.
(AIM Partner Controller) Partner Status	The partner's case status of resolving this incident.	0 – 255 Characters	Empty until a case is created.
(AIM Partner Controller) Home Base Case ID	The case ID used by JSS that provides a link to the JSS Case Management page.	N/A	Empty until a case is created.
(AIM Partner Controller) Partner Case ID	The case ID used by JSS that provides a link to the JSS Case Management page.	0 – 255 Characters	Empty
Host ID	Unique identifier representing the specific incident.	N/A	Set by the JUNOS system or AIM if multiple JMBs
Synopsis	Text description of the incident	N/A	Set by the JUNOS system
Platform	Indicates the device platform on which the incident occurred	N/A	Set by the JUNOS system
(AIM Partner Controller) Serial Number	Serial Number of the Device.	N/A	The Serial Number of the device.
Problem Description	A description of the incident specified by the device	N/A	Set by the JUNOS system
Release	Release of JUNOS software running on the device	N/A	Set by the JUNOS system
Version	Version of JUNOS software running on the device	N/A	Set by the JUNOS system
Email List	List of Partner Controller E-mail addresses for an incident.	0 – 65535 characters	Default E-mail Address list (Set in the Organization Page)
(AIM Partner Controller) Customer EMail List	List of end customer e-mail addresses to be sent a message when a case is submitted to the partner.	N/A	List of E-mail Addresses sent from the end customer for the incident.

Table 71: Incident Details (Incident for Device) Table Column Descriptions *(continued)*

Column	Description	Range/Length	Default
Received	Time that the incident was detected by AIM	Date and time	N/A
Owner	User that has currently been assigned ownership of this incident	Any valid user login for AIM	Bland
Owner Status	Incident owner's status regarding the resolution of the incident	Unassigned, Assigned, In progress, and Completed	Unassigned
Flagged to Users	List of users to which the current incident has been flagged or notified	N/A	Blank
(AIM Partner Controller) Partner Communication	Displays whether information has been sent to the End Customer AIM, and whether it has been received.	Initial, Sent to Customer, Received by Customer	Initial

Viewing Incident Juniper Message Bundle (JMB)

The Juniper Message Bundle (JMB) contains the information that JSS needs to analyze and resolve cases and to prevent the incident from reccurring. For more information about the JMB, see "JMB Contents" on page 49.

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: dev-hostid _PvS_prob_20071201_003445.xml

(Information as received by Router)

MANIFEST

Host Event ID:	dev-hostid-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:	

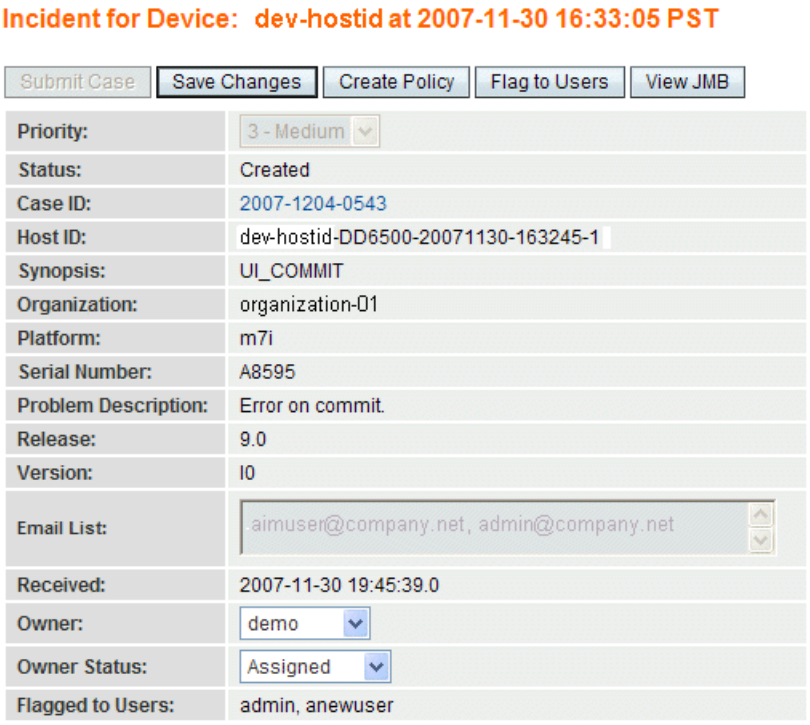
Router Information	
Product Name:	m7i
Host Name:	pvs-m1-re0
OS Platform:	junos

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

Assigning an Incident Owner

To assign an incident to an AIM user, follow these steps:

1. From the Incident Manager table, click an incident Synopsis link. The Incident Detail page appears.

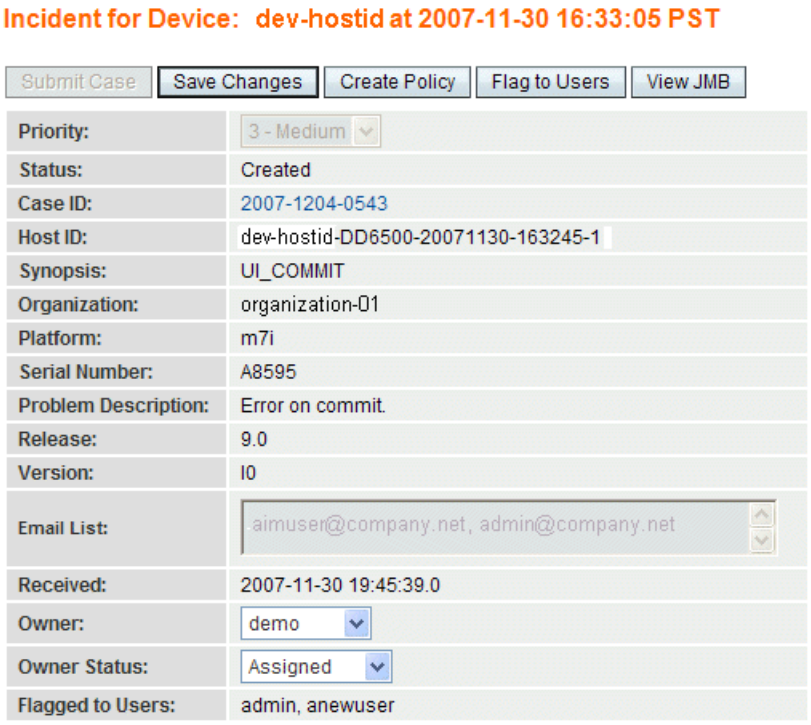


2. From the Owner drop-down list box select an AIM user.
3. Click Save Changes. The incident appears in the Incidents table in My AIM Home for the incident owner.

Changing Incident Owner Status

To change incident owner status, follow these steps:

1. From the Incident Manager table, click an incident Synopsis link. The Incident Detail page appears.



2. From the Owner Status drop-down list box select a status option—Unassigned, Assigned, In Progress, or Completed.
3. Click Save Changes. The incident appears in the Incidents table in My AIM Home for the incident owner.

Deleting an Incident

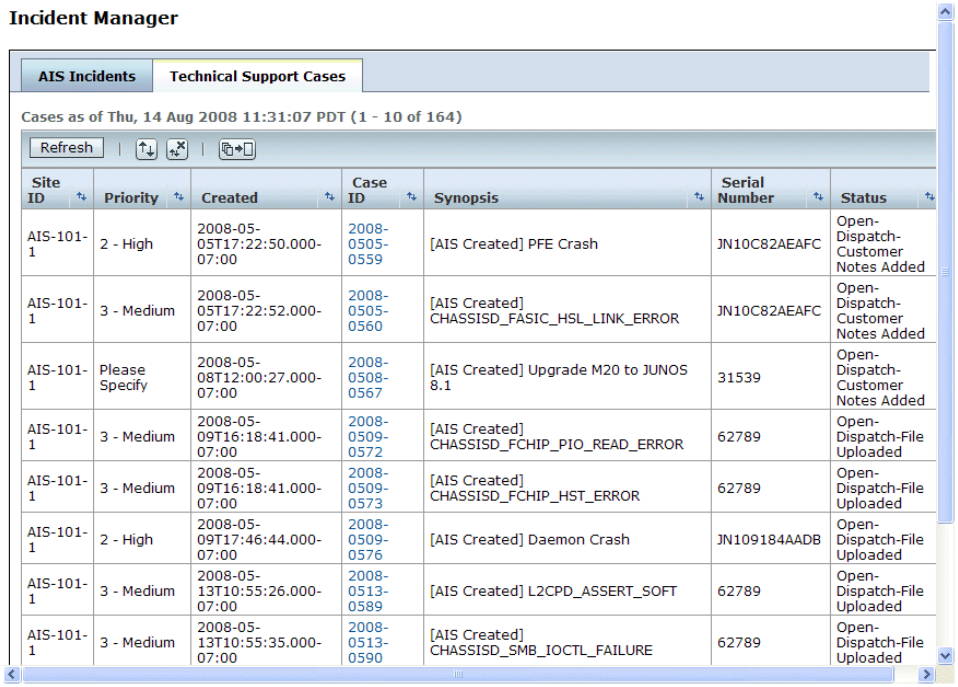
To delete an incident from the Incidents table, follow these steps:

1. In the Incident Manager table, select the incident(s) you want to delete. This action enables the Delete button.
2. Click Delete. The selected incidents are removed from the AIS database.

Using the Technical Support Tab

This section includes the following:

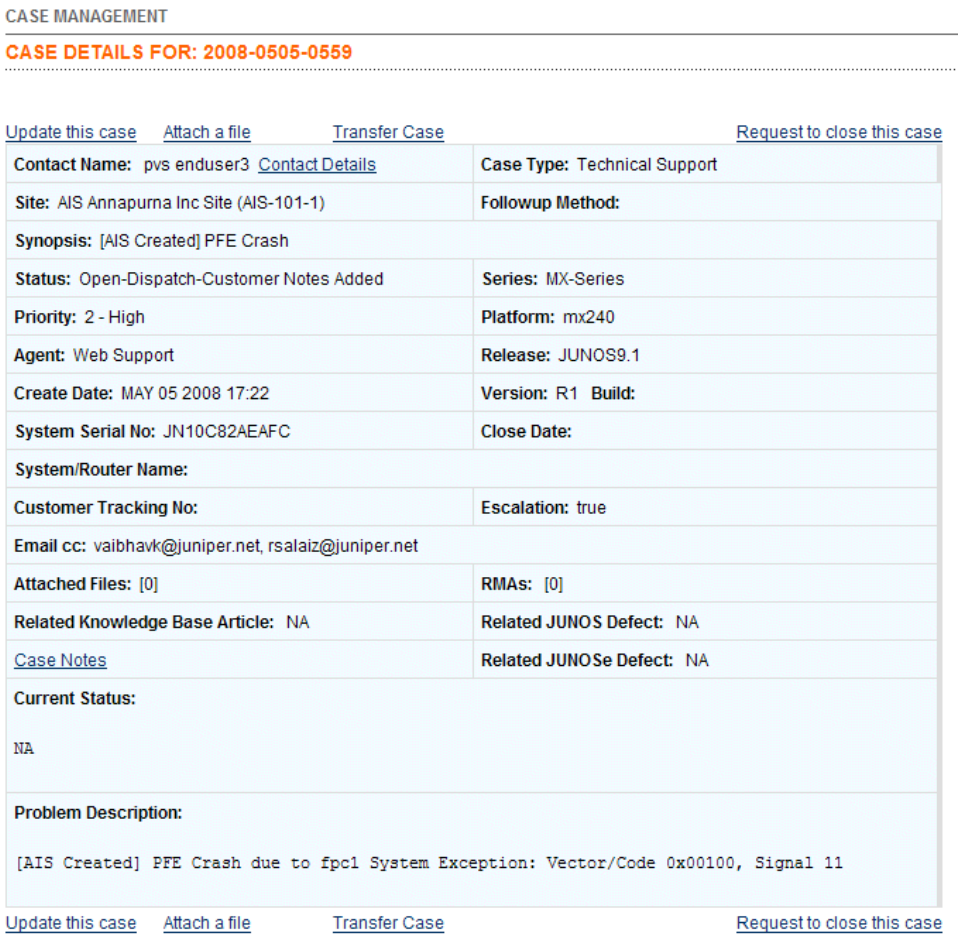
1. In Incident Manager, click the Technical Support Cases tab. The page appears:



Site ID	Priority	Created	Case ID	Synopsis	Serial Number	Status
AIS-101-1	2 - High	2008-05-05T17:22:50.000-07:00	2008-0505-0559	[AIS Created] PFE Crash	JN10C82AEAFC	Open-Dispatch-Customer Notes Added
AIS-101-1	3 - Medium	2008-05-05T17:22:52.000-07:00	2008-0505-0560	[AIS Created] CHASSISD_FASIC_HSL_LINK_ERROR	JN10C82AEAFC	Open-Dispatch-Customer Notes Added
AIS-101-1	Please Specify	2008-05-08T12:00:27.000-07:00	2008-0508-0567	[AIS Created] Upgrade M20 to JUNOS 8.1	31539	Open-Dispatch-Customer Notes Added
AIS-101-1	3 - Medium	2008-05-09T16:18:41.000-07:00	2008-0509-0572	[AIS Created] CHASSISD_FCHIP_PIO_READ_ERROR	62789	Open-Dispatch-File Uploaded
AIS-101-1	3 - Medium	2008-05-09T16:18:41.000-07:00	2008-0509-0573	[AIS Created] CHASSISD_FCHIP_HST_ERROR	62789	Open-Dispatch-File Uploaded
AIS-101-1	2 - High	2008-05-09T17:46:44.000-07:00	2008-0509-0576	[AIS Created] Daemon Crash	JN109184AADB	Open-Dispatch-File Uploaded
AIS-101-1	3 - Medium	2008-05-13T10:55:26.000-07:00	2008-0513-0589	[AIS Created] L2CPD_ASSERT_SOFT	62789	Open-Dispatch-File Uploaded
AIS-101-1	3 - Medium	2008-05-13T10:55:35.000-07:00	2008-0513-0590	[AIS Created] CHASSISD_SMB_IOCTL_FAILURE	62789	Open-Dispatch-File Uploaded

2. Click the Refresh button to view the latest cases.

3. Click the Case ID link to view the case details on the Juniper Networks Case Management page.



CASE MANAGEMENT

CASE DETAILS FOR: 2008-0505-0559

Update this case | Attach a file | Transfer Case | Request to close this case

Contact Name: pvs enduser3 Contact Details	**Case Type:** Technical Support
Site: AIS Annapurna Inc Site (AIS-101-1)	**Followup Method:**
Synopsis: [AIS Created] PFE Crash	
Status: Open-Dispatch-Customer Notes Added	**Series:** MX-Series
Priority: 2 - High	**Platform:** mx240
Agent: Web Support	**Release:** JUNOS9.1
Create Date: MAY 05 2008 17:22	**Version:** R1 **Build:**
System Serial No: JN10C82AEAFC	**Close Date:**
System/Router Name:	
Customer Tracking No:	**Escalation:** true
Email cc: vaibhavk@juniper.net, rsalaiz@juniper.net	
Attached Files: [0]	**RMAs:** [0]
Related Knowledge Base Article: NA	**Related JUNOS Defect:** NA
Case Notes	**Related JUNOSe Defect:** NA
Current Status: NA	
Problem Description: [AIS Created] PFE Crash due to fpc1 System Exception: Vector/Code 0x00100, Signal 11	

Update this case | Attach a file | Transfer Case | Request to close this case

Technical Support Tab Buttons

Table 72 on page 189 describes the fields on the Technical Support Tab.

Table 72: Technical Support Tab Command Button Descriptions

Button Name	Description	Privileges	Enabled/Disabled	Results
Refresh	Allows the user to perform an on demand update of JSS Technical Support cases.	AIM User	N/A	Retrieves latest information on cases.

Viewing the Technical Support Table

Table 73 on page 190 describes the columns in the Technical Support table.

Table 73: Technical Support Table Column Descriptions

Column	Description	Range/Length	Default
Site ID	End-user Site ID.	N/A	
Priority	Indicates the priority of the incident received ■ 1—Critical ■ 2—High ■ 3—Medium ■ 4—Low	1-4	Set by the JUNOS device. May be overridden by a Reaction Policy
Created	Shows information for when the case was created.	Date and time	N/A
Case ID	The case ID used by the JSS system. This field provides a link to navigate to the JSS Case Management page.	N/A	Empty until a case is created
Synopsis	Text description of the case.	Date and time	Set by the JUNOS system
Serial Number			
Status	The status of this case with regards to AIM.	Initial, Submitted, Created, Updated	Sent by JSS

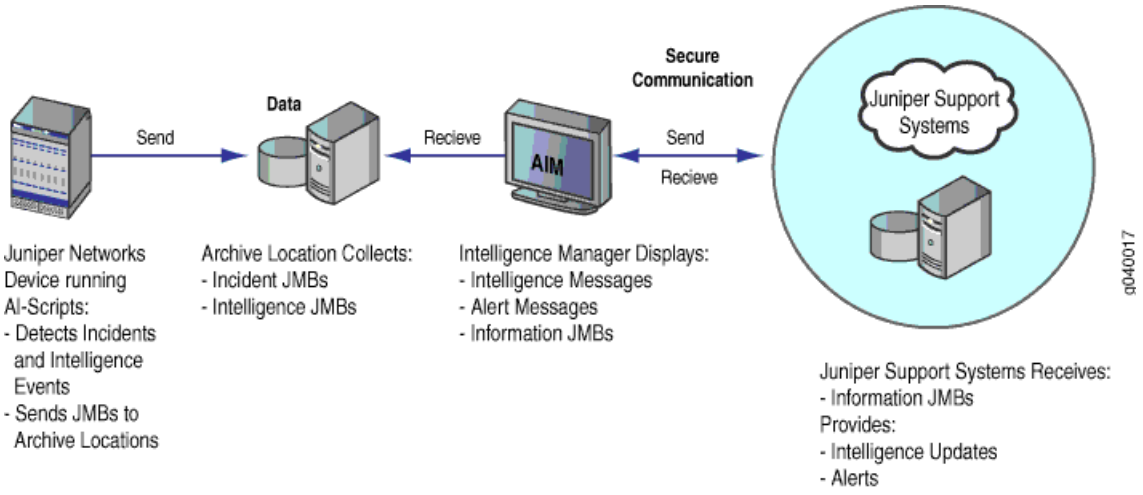
Chapter 18

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 16 on page 191 shows the flow through which Intelligence Manager gets the intelligence information that is displayed on the Intelligence Updates and Information JMBs tabs.

Figure 16: Intelligence Manager Data Flow Diagram



Juniper Networks devices, configured with specialized AI-Scripts, periodically send incident and intelligence 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. JSS 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.

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 "Advanced Insight Solutions Overview" on page 3.

This chapter includes the following sections:

Intelligence Update Partner Controller and End-User Data Flow

This section describes the intelligence information flow at the end user and the partner in an AIS partner and end-user engagement model.

Intelligence Update Flow at the End User Site

1. The end user sets up the information JMBs settings in AIM Settings > General Settings. The end user specifies the Information JMB Config Filter Level and Upload Information JMB Interval options.
2. The end user devices start sending information JMBs to the archive location.
3. The end user's AIM detects new information JMBs and processes them in the database.
4. The end user's AIM sends the information JMBs to the partner's AIM based upon the options selected in Step 1.
5. The end user receives a response from the partner's AIM and stores a transaction ID in the database.

Intelligence Update Flow at the Partner Site

1. The partner has AIM Pro installed with no filtering or blocking of information JMBs.
2. The partner's AIM checks for and receives information JMBs

3. The partner's AIM process the information JMBs and sends a response message with a transaction ID to the end user.
4. The partner send the information JMB to JSS with an alias and trace route.

Viewing Intelligence Updates

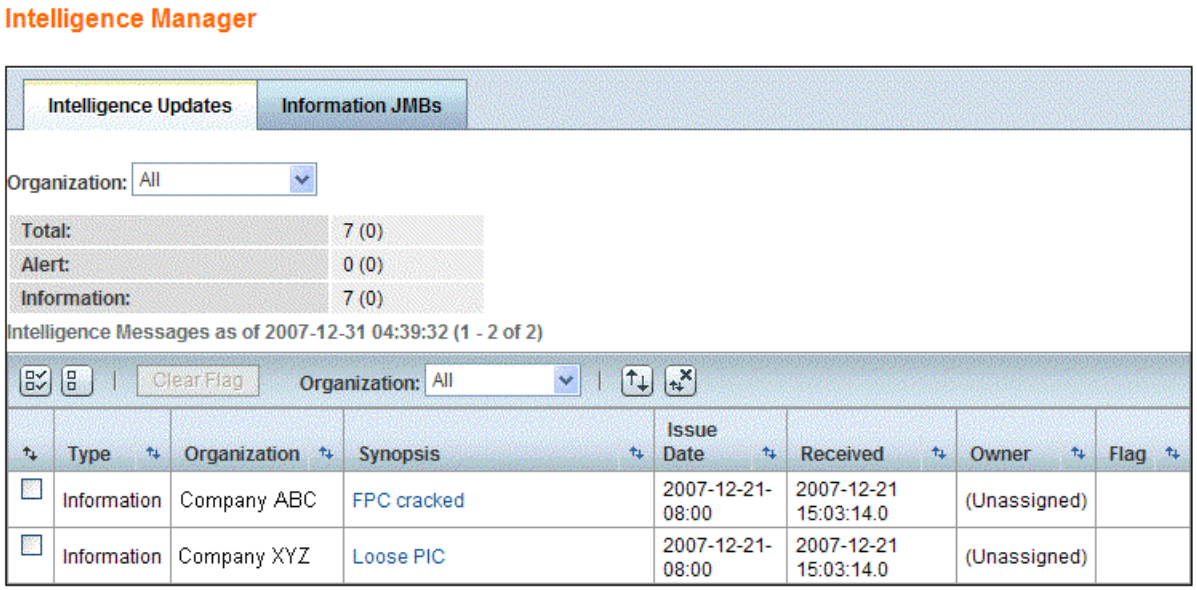
Intelligence Manager—Intelligence Updates displays all intelligence update messages received by AIM from JSS.

Intelligence Manager—Intelligence Updates lets you do the following:

- View all intelligence messages and alerts received from JSS
- View intelligence messages by organization name
- 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.



You can show the statistics dashboard that shows a summary of intelligence messages by clicking the plus image. The default is for the statistics dashboard to be hidden.

For more information on the Intelligence Updates tab description, see “Intelligence Updates Tab Description” on page 194.

Intelligence Updates Tab Description

Table 74 on page 194 describes the Intelligence Updates tab elements.

Table 74: Intelligence Updates Tab 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 the selected organization.

Table 74: Intelligence Updates Tab Element Descriptions *(continued)*

Element Name	Description	Privileges	Enabled/Disabled	Results
Statistics Dashboard	The Statistics Dashboard includes the following display items: ■ Total—Based on the current filter, the total number of messages and number of new messages received since you last logged in shown in parenthesis, for example: 25 (8) ■ Alert—Based on the current filter, the total number of Alert messages and the number of new Alert messages received since you last logged in shown in parenthesis, for example: 15 (5) ■ Information—Based on the current filter, the total number of Information messages and the number of new Information messages received since you last logged in shown in parenthesis, for example: 10 (3)	None; display only field and not allowed to modify	N/A	N/A
Show/Hide Statistics	Clicking on the plus or minus image will show or hide the statistics at the top of the page.	None	Always enabled	The statistics will either be shown if they are not displayed or hidden if they are already displayed.
Clear Flag button	Removes the flag from any selected Intelligence Messages.	AIM Admin	Enabled when you select an intelligence update.	Clears flag

Table 75 on page 195 describes the columns in the Incident Manager table.

Table 75: Intelligence Updates Table Column Description

Column	Description	Default
Type	Indicates the type of Intelligence Message received from JSS: ■ 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

Table 75: Intelligence Updates Table Column Description *(continued)*

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
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 is enabled). 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.

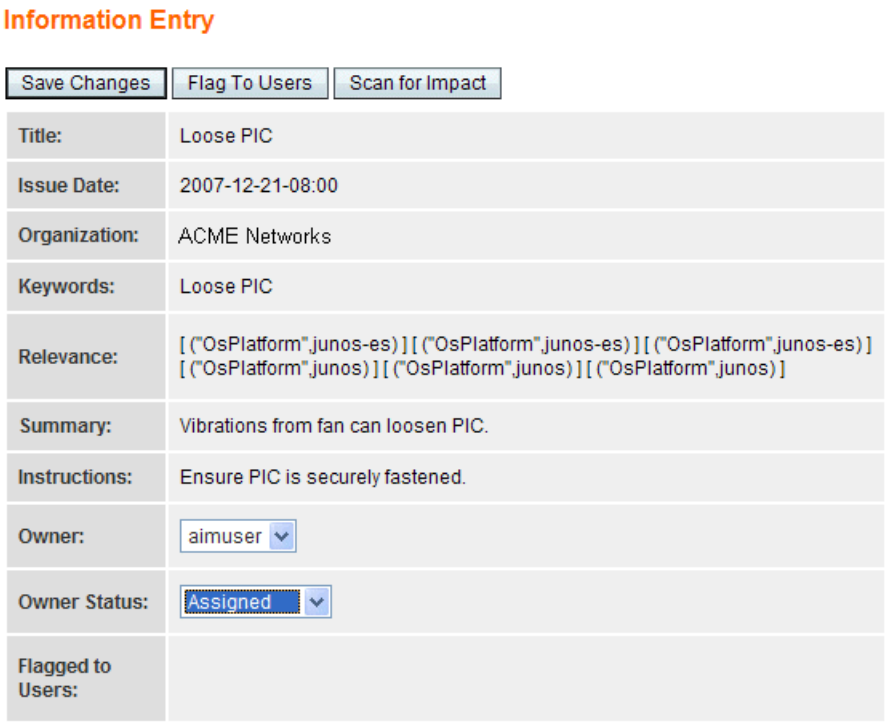
Viewing Intelligence Update Synopsis

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 197.

Information Entry Page Field Descriptions

Table 76 on page 197 describes the fields in the Information Entry page.

Table 76: 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	Text 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.

Table 76: Information Entry Field Descriptions *(continued)*

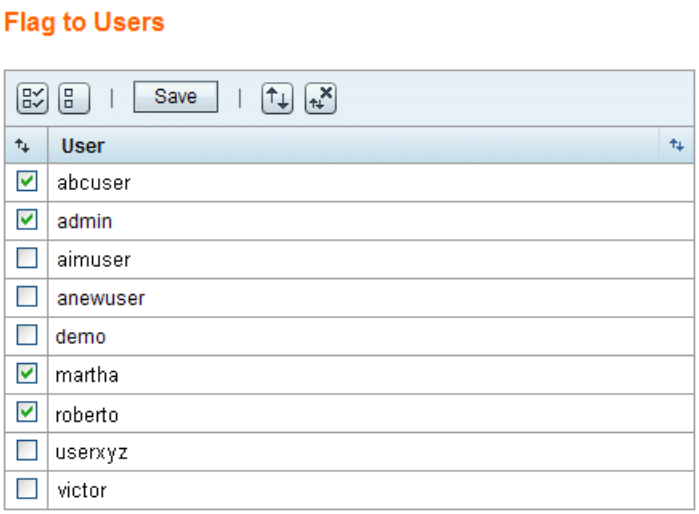
Keywords	List of words specified by JTAC engineer that describe the key components this Information Entry is regarding.
Relevance	Set of one or more relevance entries. Each entry contains some combination of one or more of each of the following: serial numbers, platforms, hardware versions, software versions, general comments.
Source	Indicates the source of the alert message
Products Affected	Specifies one or more of the products affected by the alert message
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 Networks Support Web page for this specific alert

Flagging an Intelligence Update To a User

Flagging the incident is used to inform other users who might be impacted or need to be aware of the incident.

To flag an incident to a user from the 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 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.

Scan for Impact

Devices (2)

Back to Intelligence Update

Device	Platform	Serial Number	Software Version	Date of latest JMB
device-004	m7i	HB6845	9.010	2007-12-14 00:29:07 PST
device-010	m10i	HC8269	9.010	2007-12-12 01:15:25 PST

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

3. Click Back to Intelligence Update.

"Scan for Impact Table Description" on page 199 describes the columns in the Scan for Impact table.

Scan for Impact Table Description

Table 77 on page 199 describes the elements in the Scan for Impact table.

Table 77: Scan for Impact Table Column Descriptions

Element/Column	Description
Back to Intelligence Update	Takes the user from the Scan for Impact page back to the Intelligence Update page.
Device	Name of the device that the intelligence update may impact.
Platform	Type of device.

Table 77: Scan for Impact Table Column Descriptions *(continued)*

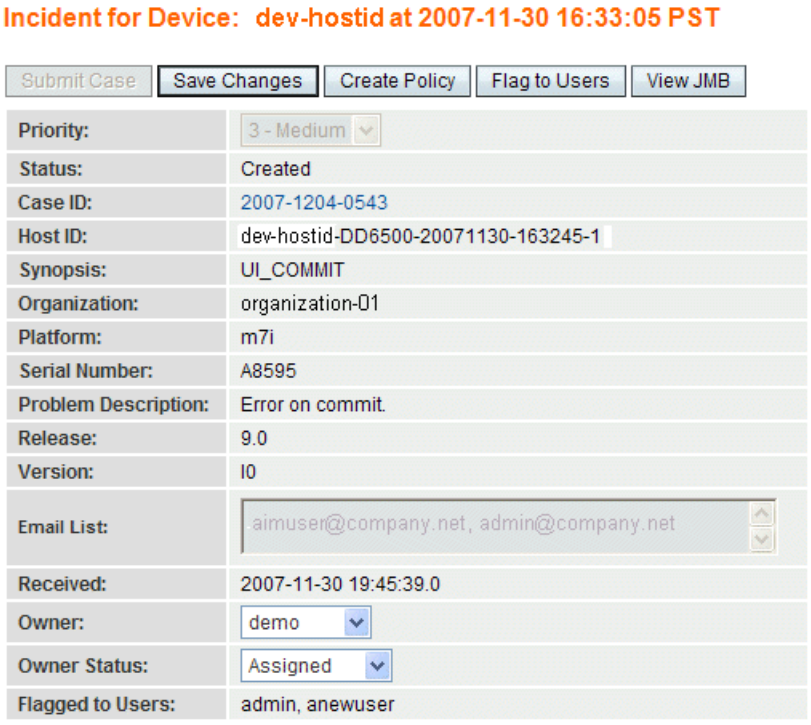
Element/Column	Description
Serial Number	Serial number on the device.
Software Version	Software version running on the device.
Date of Last JMB	Date and time that the last JMB was received that applies to the intelligence message

Assigning an Intelligence Update Owner

The user can have responsibility for following the incident resolution process to completion, including editing the status. See "Understanding AIM Ownership" on page 136. See also "AIM User Privileges" on page 137.

To assign ownership 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.

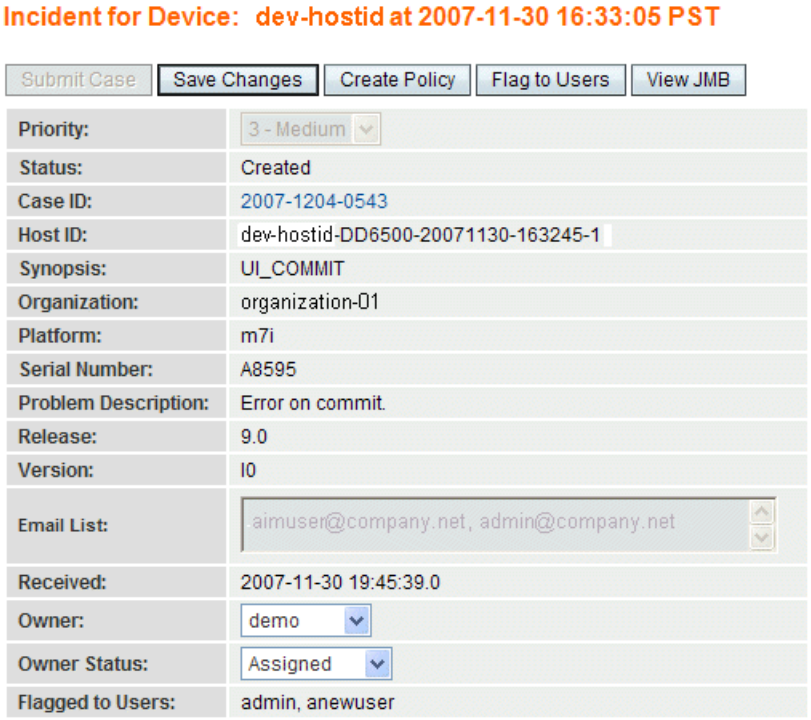
Changing Intelligence Update Owner Status

The incident owner can specify the incident status:

- 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 Owner Status drop-down list.
3. Click Save Changes.

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.

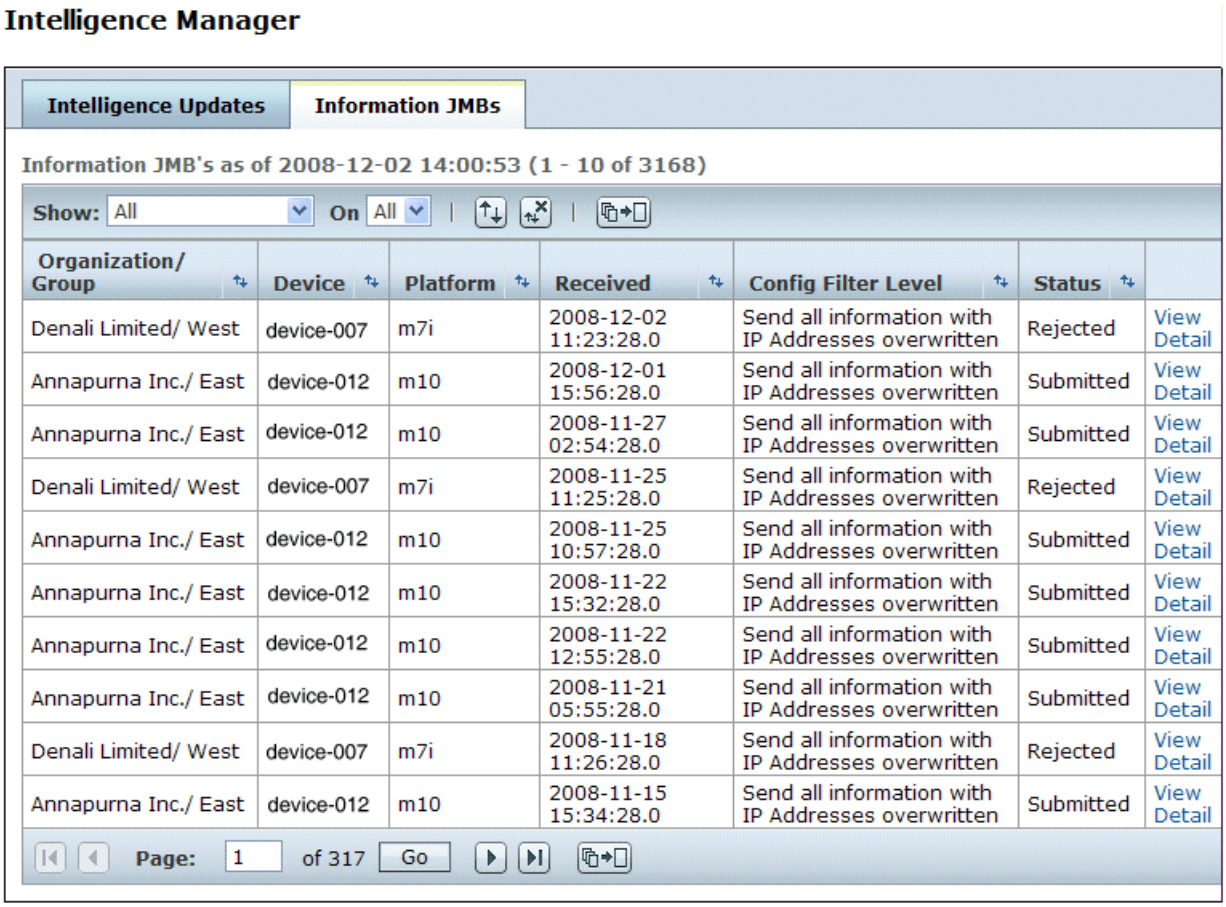
Viewing Information JMBs

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 JMB 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 203.

Information JMBs Table Description

Table 78 on page 203 describes the Intelligence Updates table button and drop-down list box elements.

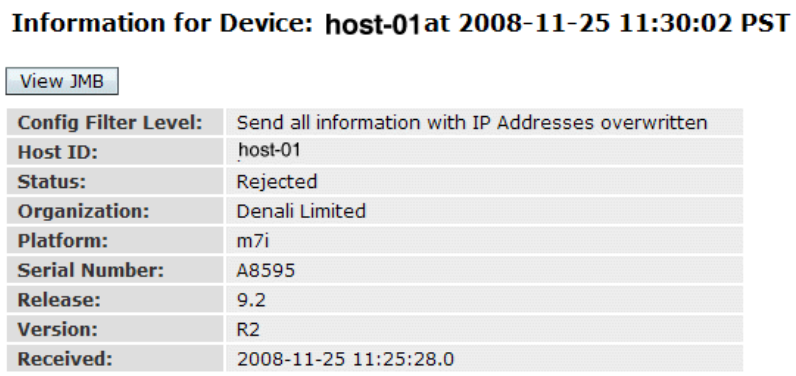
Table 78: Intelligence Updates Table Element Descriptions

Element Name	Description	Privileges	Enabled/Disabled	Results
Show/On drop-down list box	■ The Show drop-down list box displays information JMBs by all, device, device group, directives group, or organization. ■ The On drop-down list box is affected by the Show drop-down list box by displaying the names of the option selected.	AIM Admin Settings	Always enabled	Displays intelligence updates for selected organization.
Organization/Group	Name of the organization and device group in which the JMB belongs.	AIM Admin Settings	N/A	N/A
Device	Name of device that the Information JMB is from.	AIM Admin Settings	N/A	N/A
Platform	Platform of device	AIM Admin Settings	N/A	N/A
Received	Date and time this Information JMB was detected by AIM	AIM Admin Settings	N/A	N/A
Config Filter Level	Displays the device configuration level selected in AIM Settings when the information JMB was uploaded to JSS. For more information see "AIM General Settings Page Description" on page 68.	AIM Admin Settings	N/A	N/A
Status	Indicates whether this Information JMB was sent to JSS. Status is either: Initial Submitted or Rejected.	AIM Admin Settings	N/A	N/A
View Detail link	Displays the Information Detail page for an information JMB entry.	AIM Admin Settings	N/A	Displays the Information JMB Details page.

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 Page Descriptions” on page 204.

Information for Device Page Descriptions

Table 79 on page 204 describes the Information for Device page button description.

Table 79: Information for Device Button Description

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

Table 80 on page 204 describes the fields in the Information JMBs table.

Table 80: Information JMBs Field Descriptions

Column	Description
Config Filter Level	Displays the device configuration level selected in AIM General Settings when the information JMB was submitted. For more information see “AIM General Settings Page Description” on page 68.
Host ID	The name of the device from which an information JMB exists
Organization	The organization within which the information JMB exists
Status	Indicates whether this Information JMB was sent to JSS. Status is either: Initial Submitted or Rejected.
Platform	The routing platform for the information JMB

Table 80: Information JMBs Field Descriptions *(continued)*

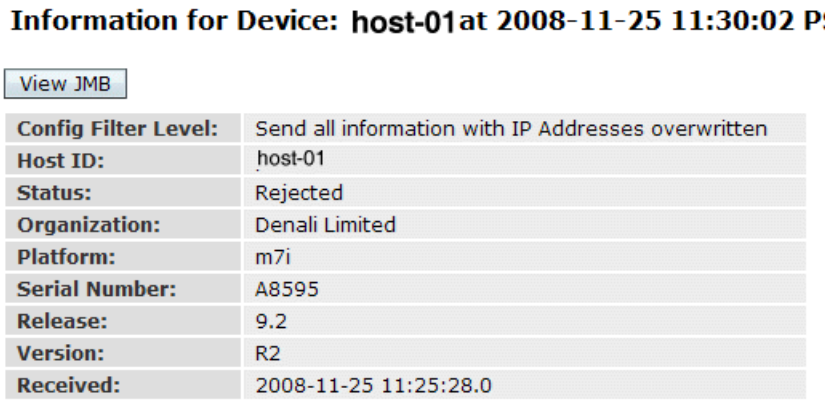
Column	Description
Serial Number	Serial number on the device
Release	JUNOS software release level
Version	JUNOS software version
Received	Time and date the information JMB was received by AIM

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:

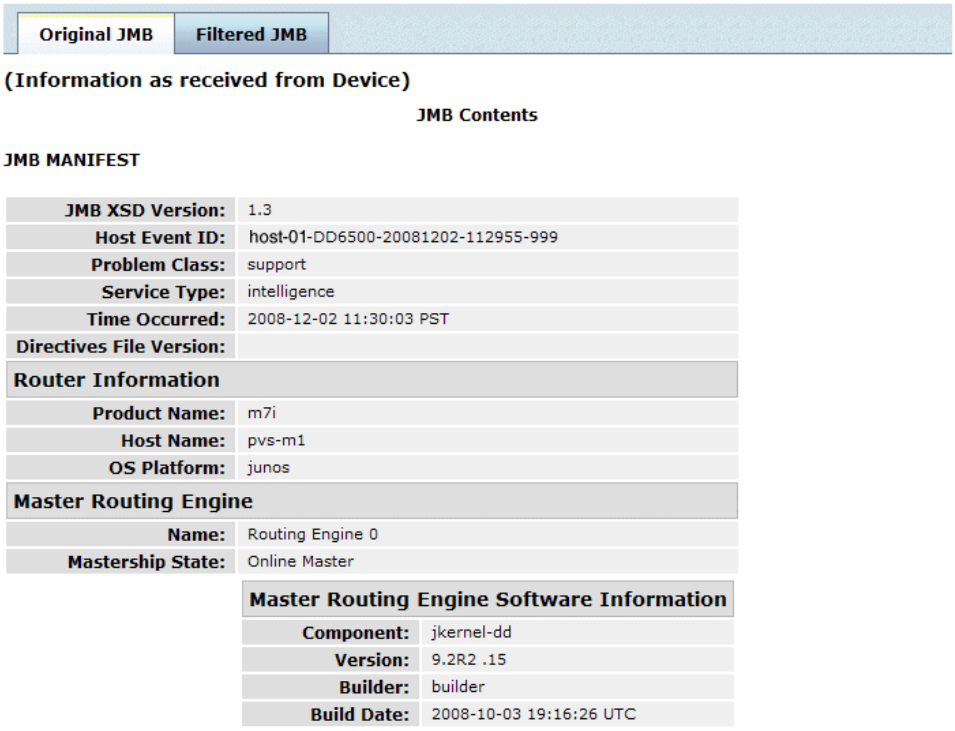
1. In Intelligence Manager, click the Information JMB tab. The Information JMBs table appears.
2. In the Information JMBs table, click the View JMB linking in the Information JMBs table. The Information for the Device page appears.



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

   The Information JMB includes the following information based upon how much shared 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.



- The Original JMB tab displays the information JMB contents unfiltered.

- The Filtered JMB tab displays the information JMB contents filtered according to the setting selected in the AIM General Settings Information JMBs Config Filter level option at the time of upload to JSS.

View JMB: baldy-re0_ais_intel_20081203_200140.xml

Original JMB | Filtered JMB

Sent to Home Base with filter level: Send all information with IP Addresses overwritten

JMB Contents

```
</root-authentication>
<name-server>
   <name>*.*.*.*</name>
</name-server>
<radius-server>
   <name>*.*.*.*</name>
   <secret>$9$n0taC0IyrvLX-yl87Nd4o</secret>
</radius-server>
<scripts>
   <commit>
      <allow-transients/>
      <file>
         <name>jais-activate-scripts.slax</name>
         <optional/>
      </file>
   </commit>
   <op>
      <traceoptions>
         <file>
            <filename>trace</filename>
         </file>
         <flag>
            <name>all</name>
         </flag>
      </traceoptions>
      <file>
         <name>attach-m5_m10.slax</name>
      </file>
      <file>
         <name>dual-re-sw.slax</name>
      </file>
      <file>
         <name>td-fpc-mseries.slax</name>
      </file>
      <file>
         <name>td_fpc_mseries_ppb.slax</name>
      </file>
   </op>
</scripts>
<login>
   <class>
```

Here, the information JMB is filtered with IP addresses overwritten with asterisks (*.*.*.*). For more information, see “AIM General Settings Page Description” on page 68.

Chapter 19

Using AIM Inventory Manager

This chapter describes how to use Inventory Manager, which lists all AIM devices in a table by organization, device group, device name, Juniper Networks routing platform type, serial number, and software version number running on the device.

The Inventory Manager table is populated with devices that are associated to AIM organizations and device groups. For more information about creating organizations and device groups, see "Configuring AIM Organizations and Device Groups" on page 91.

The devices shown in the Inventory Manager table are ones to which the user has access based on the User Groups the user belongs to and the Device Group associations to those User Groups.

From Inventory Manager, you can:

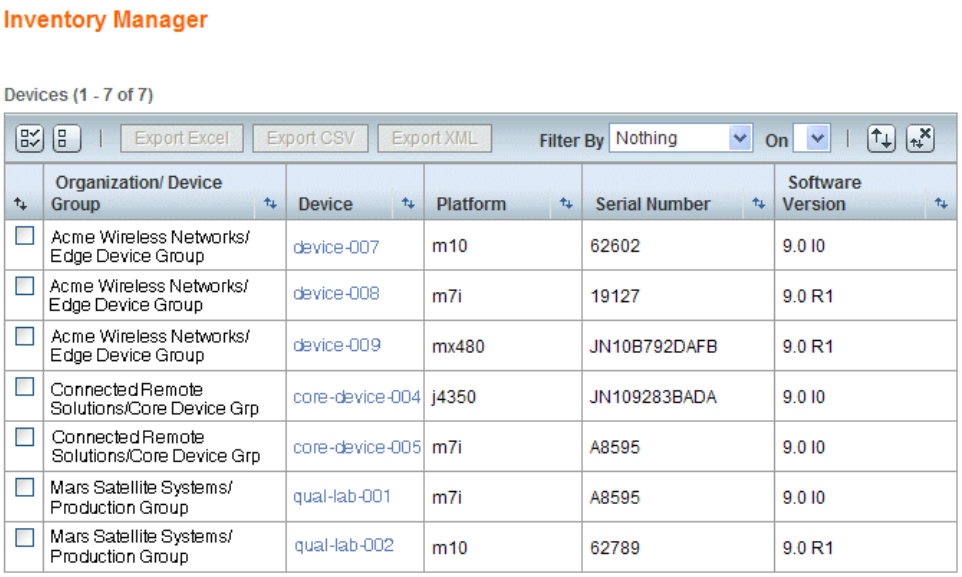
- Filter the Inventory Manager data by organization or device group to show only the data that you are interested in viewing. See "Filtering Inventory Data" on page 213.
- View device detail information showing all the components installed in the device chassis. See "Viewing Device Chassis Detail" on page 214.
- Export Inventory Manager table data in Microsoft Excel, comma-separated value, or XML format. See "Exporting Inventory Data in Microsoft Excel Format" on page 215, "Exporting Inventory Data in CSV Format" on page 215, "Exporting Inventory Data in XML Format" on page 216.

Inventory Manager is part of the AIM Base product.

Viewing Inventory Manager

To view Inventory Manager, do the following:

- Select Inventory Mgr in the AIM navigation area. The Inventory Manager page appears.



Device inventory data is displayed in the table by organization and device group. If you do not have access to or have not created organizations or device groups, the Inventory Manager table is empty. For more information about creating organizations and device groups, see “Configuring AIM Organizations and Device Groups” on page 91.

For more information about the device inventory information that appears in the Inventory Manager table, see “Inventory Manager Table Descriptions” on page 210.

Inventory Manager Table Descriptions

This section describes the Inventory Manager table.

Inventory Manager Table Element Descriptions

Table 81 on page 211 describes the Inventory Manager table element descriptions.

Table 81: Inventory Manager Table Element Decriptions

Event Name	Description	Privileges	Enabled/ Disabled	Results
Export Excel	Inventory Manger generates a Microsoft Excel XLS file containing all data in the Inventory Manager table (including hierarchy info).	None	Enabled if one or more devices are selected	Inventory Manager data appears in Microsoft Excel in XLS file format.
Export CSV	Inventory Manager generates a Microsoft Excel CSV file The data in the file is comma-separated so that it can be imported into a spreadsheet.	None	Enabled if one or more devices are selected	Inventory Manager data appears in Microsoft Excel in CSV file format.
Export XML	Inventory Manager generates a file containing the XML output of the hardware components that are installed in the device chassis for the devices specified. This inventory information is the same as the output for the JUNOS Operational mode show chassis hardware CLI command. You can use the data in the file in the Juniper Networks Hardware Configuration Validation Tool online at http://tools.juniper.net/microcode/	None	Enabled if at least one device is selected	Inventory Manager data for the selected device(s) appears in XML format in a text window.
Filter By drop-down list box	Lists the available Inventory Manager table filter options: ■ Nothing ■ Organization ■ Device Group The default option is Nothing. For more information about filtering Inventory Manager data, see “Filtering Inventory Data” on page 213.	None	Always enabled	The Filter By drop-down list box causes the following actions in the On drop-down list box: ■ The On drop-down is blank if the Nothing option is selected. ■ The names of the available organizations to which the user has access appear in the On drop-down list box if the Organization option is selected. ■ The names of the available device groups to which the user has access appear in the On drop-down list box if the Device Groups option is selected.

Table 81: Inventory Manager Table Element Decriptions *(continued)*

Event Name	Description	Privileges	Enabled/ Disabled	Results
On drop-down list box	Lists the names of the available organizations or device groups to which the user has access. The On drop-down list box is associated and responds to the option you select in the Filter By drop-down list box. If the Nothing option is selected in the Filter By drop-down list box, this drop-down list box is blank. For more information about filtering Inventory Manager data, see "Filtering Inventory Data" on page 93.	None	Always enabled	The On drop-down list box operates as follows: ■ If the Nothing option is selected, the On drop-down is blank. ■ If the Organizations option is selected in the Filter By drop-down list box, the On drop-down list box displays the names of the available organizations to which the user has access. ■ If the Device Groups option is selected in the Filter By drop-down list box, the On drop-down list box displays the names of the available device groups to which the user has access. ■ If the Organizations or Device Group option is selected, the On drop-down list box defaults to All.

Inventory Manager Table Column Descriptions

Table 82 on page 212 describes the Inventory Manager table column descriptions.

Table 82: Inventory Manager Table Column Descriptions

Name	Description	Privileges
Organization/Device Group	The Organization and Device Group to which the device belongs.	Not allowed to modify
Device	Name of the device. This field is a link to the Chassis Detail page, which displays all the hardware components installed in the device chassis. For more information about the Chassis Detail page, see "Viewing Device Chassis Detail" on page 214.	Not allowed to modify
Platform	Juniper Networks device type—for example M20, MX480, or J4300.	Not allowed to modify
Serial Number	Serial number	Not allowed to modify
Software Version	JUNOS software version currently running on the device, for example 9.1R1.	Not allowed to modify

Filtering Inventory Data

You can filter Inventory Manager data to which the user has access by organization or device group.

To filter inventory data, follow these steps:

1. In the AIM Navigation area, select Inventory Manager. The Inventory Manager page appears.
2. In the Inventory Manager table Filter By drop-down list box, select an organization or device group within which you want to view device inventory.

When you select an organization or device group, the On drop-down list box is populated with the names of the organization or device groups that exist in AIM to which the user has access.

Table 83 on page 213 describes the operation of the associated Filter By and On drop-down list boxes.

Table 83: Associated Filter By and On Drop-Down List Box Operation

Filter By Drop-Down List Box Option	On Drop-Down List Box Results
Nothing	Blank
Organization	List names of available organizations.
Device Groups	Lists names of the available device groups

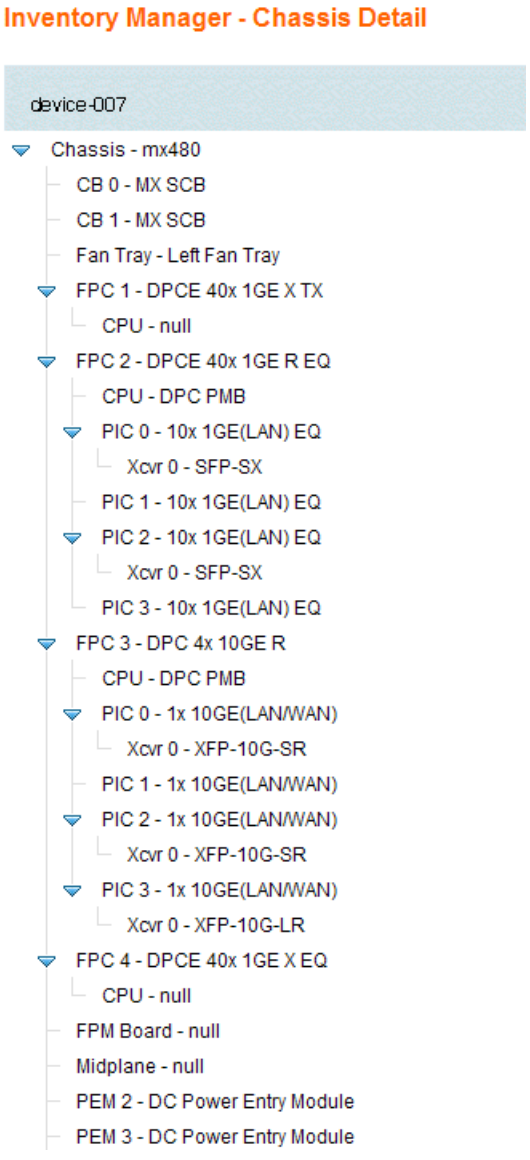
3. In the On drop-down list box, select an organization or device group. Only the devices in the organization or device group that you select are displayed in the Inventory Manager table.

Viewing Device Chassis Detail

The Inventory Manager Chassis Detail page displays all the hardware components that are installed in a device.

To view a device chassis detail, follow these steps:

1. Select Inventory Mgr in the AIM navigation area. The Inventory Manager page appears.
2. In the Inventory Manager table, click a device name in the Device column. The Chassis Detail page appears.



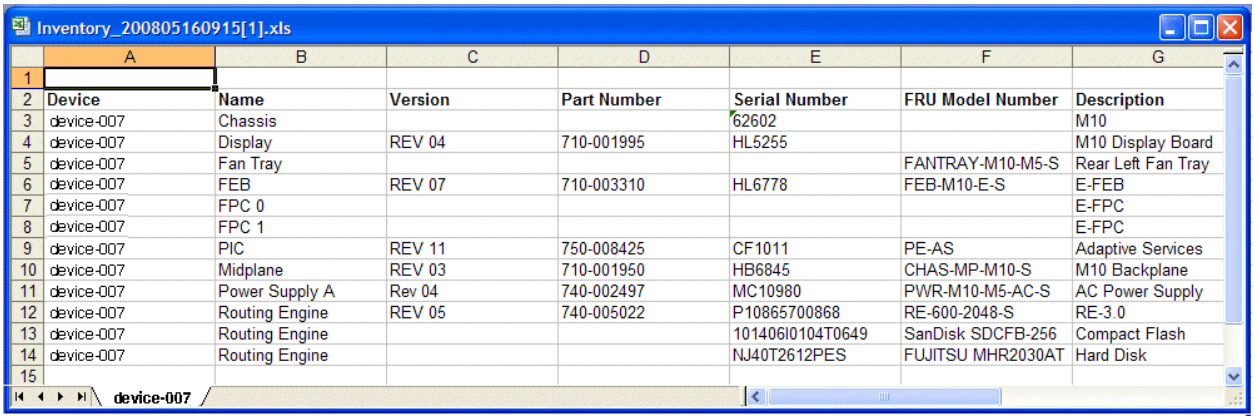
The Chassis Detail hardware components are displayed in an expandable/collapsible tree. To expand component submodules, click the right arrow. To collapse components, click the down arrow.

Exporting Inventory Data in Microsoft Excel Format

You can export Inventory Manager data in Microsoft Excel spreadsheet format to use in reports.

To export Inventory Manager data in Microsoft Excel format, follow these steps:

1. Select Inventory Mgr in the AIM navigation area. The Inventory Manager page appears.
2. In the Inventory Manager table, select the device for which to export inventory data.
3. Click Export Excel. Inventory Manager generates an XLS file that opens in Microsoft Excel.



Inventory_200805160915[1].xls

	A	B	C	D	E	F	G
1							
2	**Device**	**Name**	**Version**	**Part Number**	**Serial Number**	**FRU Model Number**	**Description**
3	device-007	Chassis			62602		M10
4	device-007	Display	REV 04	710-001995	HL5255		M10 Display Board
5	device-007	Fan Tray				FANTRAY-M10-M5-S	Rear Left Fan Tray
6	device-007	FEB	REV 07	710-003310	HL6778	FEB-M10-E-S	E-FEB
7	device-007	FPC 0					E-FPC
8	device-007	FPC 1					E-FPC
9	device-007	PIC	REV 11	750-008425	CF1011	PE-AS	Adaptive Services
10	device-007	Midplane	REV 03	710-001950	HB6845	CHAS-MP-M10-S	M10 Backplane
11	device-007	Power Supply A	Rev 04	740-002497	MC10980	PWR-M10-M5-AC-S	AC Power Supply
12	device-007	Routing Engine	REV 05	740-005022	P10865700868	RE-600-2048-S	RE-3.0
13	device-007	Routing Engine			101406I0104T0649	SanDisk SDCFB-256	Compact Flash
14	device-007	Routing Engine			NJ40T2612PES	FUJITSU MHR2030AT	Hard Disk
15							

device-007

Exporting Inventory Data in CSV Format

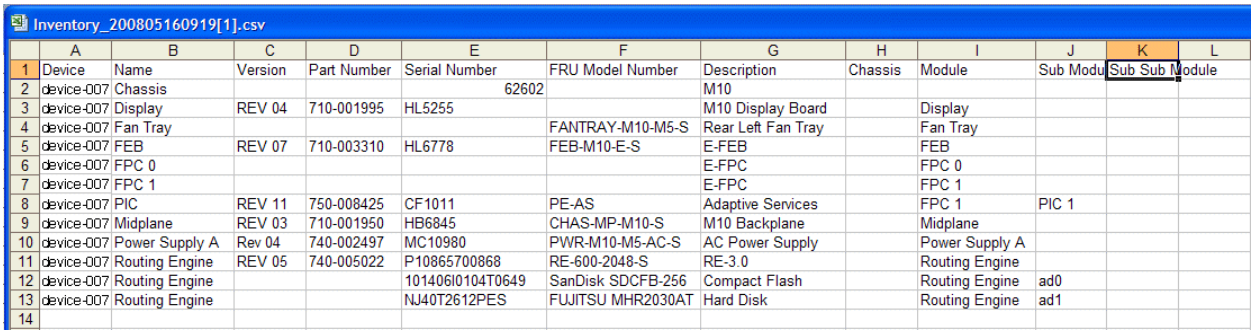
You can export Inventory Manager data in CSV file format. A CSV file is a plain text file which stores each data record separated by a comma.

You can use Inventory Manager CSV files to transfer data between programs, without considering file types.

To transfer Inventory data to CSV file format, follow these steps:

1. Select Inventory Mgr in the AIM navigation area. The Inventory Manager page appears.
2. In the Inventory Manager table, select the device for which to export inventory data.

3. Click Export CSV. Inventory Manager generates a CSV file containing the Inventory Manager table data that displays in Microsoft Excel.



Inventory_200805160919[1].csv

	A	B	C	D	E	F	G	H	I	J	K	L
1	Device	Name	Version	Part Number	Serial Number	FRU Model Number	Description	Chassis	Module	Sub Modu	Sub Sub Module	
2	device-007	Chassis			62602		M10					
3	device-007	Display	REV 04	710-001995	HL5255		M10 Display Board		Display			
4	device-007	Fan Tray				FANTRAY-M10-M5-S	Rear Left Fan Tray		Fan Tray			
5	device-007	FEB	REV 07	710-003310	HL6778	FEB-M10-E-S	E-FEB		FEB			
6	device-007	FPC 0					E-FPC		FPC 0			
7	device-007	FPC 1					E-FPC		FPC 1			
8	device-007	PIC	REV 11	750-008425	CF1011	PE-AS	Adaptive Services		FPC 1	PIC 1		
9	device-007	Midplane	REV 03	710-001950	HB6845	CHAS-MP-M10-S	M10 Backplane		Midplane			
10	device-007	Power Supply A	Rev 04	740-002497	MC10980	PWR-M10-M5-AC-S	AC Power Supply		Power Supply A			
11	device-007	Routing Engine	REV 05	740-005022	P10865700868	RE-600-2048-S	RE-3.0		Routing Engine			
12	device-007	Routing Engine			101406I0104T0649	SanDisk SDCFB-256	Compact Flash		Routing Engine	ad0		
13	device-007	Routing Engine			NJ40T2612PES	FUJITSU MHR2030AT	Hard Disk		Routing Engine	ad1		
14												

Exporting Inventory Data in XML Format

Inventory Manager generates an XML file containing all the hardware components installed in a selected device. You can use the data in the file in the Hardware Configuration Validation Tool online at:

http://tools.juniper.net/microcode/

To export Inventory Manager data in XML file format, follow these steps:

1. Select Inventory Mgr in the AIM navigation area. The Inventory Manager page appears.
2. In the Inventory Manager table, select the device for which to export inventory data.

3. In the Inventory Manager table, click Export XML. Inventory Manager generates an XML file displayed in a text window.

```
- <InventoryExport timestamp="05/16/2008 09:20">
  - <rpc-reply xmlns:junos="http://xml.juniper.net/junos/9.0R1/junos">
    - <chassis-inventory xmlns="http://xml.juniper.net/junos/9.0R1/junos/junos-chassis">
      - <chassis junos:style="inventory">
          <name>baldy-re0</name>
          <serial-number>62602</serial-number>
          <description>m10</description>
        - <chassis-module>
            <name>Display</name>
            <version>REV 04</version>
            <part-number>710-001995</part-number>
            <serial-number>HL5255</serial-number>
            <description>M10 Display Board</description>
          </chassis-module>
        - <chassis-module>
            <name>Fan Tray</name>
            <description>Rear Left Fan Tray</description>
            <model-number>FANTRAY-M10-M5-S</model-number>
          </chassis-module>
        - <chassis-module>
            <name>FEB</name>
            <version>REV 07</version>
            <part-number>710-003310</part-number>
            <serial-number>HL6778</serial-number>
            <description>E-FEB</description>
            <model-number>FEB-M10-E-S</model-number>
          </chassis-module>
        - <chassis-module>
            <name>FPC 0</name>
            <description>E-FPC</description>
          </chassis-module>
        - <chassis-module>
            <name>FPC 1</name>
            <description>E-FPC</description>
          - <chassis-sub-module>
              <name>PIC 1</name>
              <version>REV 11</version>
              <part-number>750-008425</part-number>
              <serial-number>CF1011</serial-number>
              <description>Adaptive Services</description>
            </chassis-sub-module>
          </chassis-module>
```

Chapter 20

Using AIM Proactive Case Manager

This chapter describes how to use Proactive Case Manager, an Advanced Insight Manager (AIM) application, used to submit a case to Juniper Support Systems (JSS). You use Proactive Case Manager to request upgrade information for upgrading one or more Juniper Networks devices to a specified software release, or to obtain other network services provided by JSS. JSS personnel analyze proactive cases and provide recommended feedback.

Proactive Case Manager requires appropriate licensing.

You can view Proactive Case Manager cases at a glance from My AIM Home or directly from the Proactive Case Manager user interface.

Proactive Case Manager lists all proactive cases for an organization. You must have access to the organization associated with the case. Access is determined by the user group you belong to and the device group associated to the user group.

The Juniper Networks partner is responsible for alerting end customers to the results of proactive cases.

NOTE: Creating a proactive case from an end-customer AIM is not yet supported.

This chapter includes the following information:

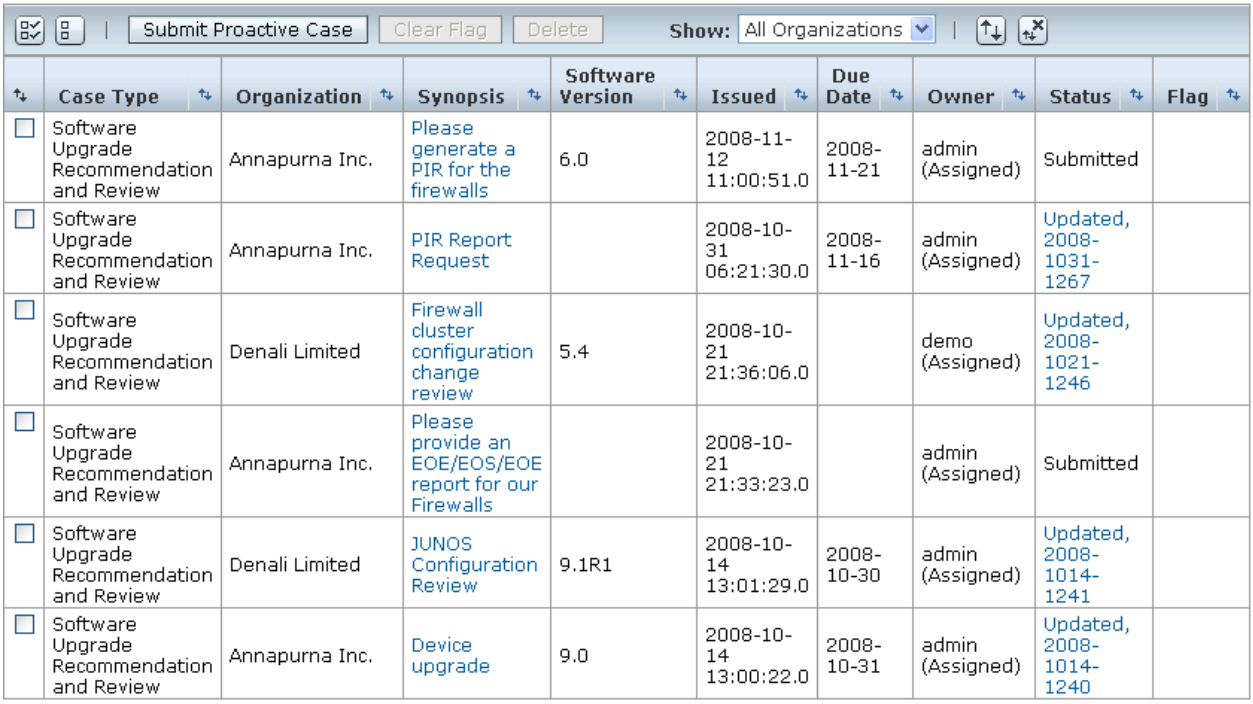
Viewing Proactive Case Manager

You can view Proactive Case Manager cases at a glance from My AIM Home or from the Proactive Case Manager user interface.

The Proactive Case Manager table is blank unless you have submitted proactive cases. Proactive case in bold indicates that a new case has been submitted, assigned, or flagged to you since the last time you were logged into AIM.

To view Proactive Case Manager, do one of the following:

- Log in to Advanced Insight Manager. My AIM Home page appears. If you have submitted proactive cases, you will see them in the Proactive Cases table.
- Select Proactive Case Manager in the AIM navigation area. The Proactive Case Manager table appears.



Case Type	Organization	Synopsis	Software Version	Issued	Due Date	Owner	Status	Flag
Software Upgrade Recommendation and Review	Annapurna Inc.	Please generate a PIR for the firewalls	6.0	2008-11-12 11:00:51.0	2008-11-21	admin (Assigned)	Submitted	
Software Upgrade Recommendation and Review	Annapurna Inc.	PIR Report Request		2008-10-31 06:21:30.0	2008-11-16	admin (Assigned)	Updated, 2008-1031-1267	
Software Upgrade Recommendation and Review	Denali Limited	Firewall cluster configuration change review	5.4	2008-10-21 21:36:06.0		demo (Assigned)	Updated, 2008-1021-1246	
Software Upgrade Recommendation and Review	Annapurna Inc.	Please provide an EOE/EOS/EOE report for our Firewalls		2008-10-21 21:33:23.0		admin (Assigned)	Submitted	
Software Upgrade Recommendation and Review	Denali Limited	JUNOS Configuration Review	9.1R1	2008-10-14 13:01:29.0	2008-10-30	admin (Assigned)	Updated, 2008-1014-1241	
Software Upgrade Recommendation and Review	Annapurna Inc.	Device upgrade	9.0	2008-10-14 13:00:22.0	2008-10-31	admin (Assigned)	Updated, 2008-1014-1240	

For details about the information in the Proactive Case Manager table, see “Proactive Case Manager Table Description” on page 220.

Proactive Case Manager Table Description

Proactive Case Manager Table Button and Item Description

Table 84 on page 221 describes the Proactive Case Manager table command buttons.

Table 84: Proactive Case Manager Table Item Descriptions

Button/Item Name	Description	Privileges	Enabled/ Disabled	Results
Submit Proactive Case	Initiates the submission of a Proactive Case	Submit Case	Enabled if user has privilege	Displays the Create Proactive Case page.
Clear Flag	Removes the flag to a user from the selected cases	None	Enabled when one or more items in the table are selected	The flag for all of the selected items in the table are removed.
Delete	Marks any of the selected cases in the table as inactive	Delete	Enabled when one or more items in the table are selected	Deletes the proactive case and removes it from the table.
Organization drop-down list box	Lists the organizations to which the current user has access	None	Always enabled	Filters the cases displayed in the table to show only those associated with the specified organization.

Proactive Case Manager Table Column Description

Table 85 on page 221 describes the columns in the Proactive Case Manager table.

Table 85: Proactive Case Manager Table Column Descriptions

Column	Description	Privilege Required to Modify	Range/Length	Default
Case Type	The type of case selected from the Select Type drop-down list. Table 84 describes the available case types.	Set by user	N/A	N/A
Organization	The organization from which the case was created.	Not allowed to modify	N/A	Set by the user that created the case
Synopsis	Textual description of the proactive case. This field is a link and can be used to navigate to the detail screen of the proactive case.	Not allowed to modify	N/A	Set by the user that created the case
Software Version	Software version running on specified device.	Not allowed to modify	N/A	Set by the user that created the case
Issued	Date and time that the case was created.	Not allowed to modify	Date and time: YYYY-MM-DD 24-hour time	N/A
Due Date	The date by which the customer needs a response from JSS.	Not allowed to modify	N/A	Set by the user that created the case

Table 85: Proactive Case Manager Table Column Descriptions *(continued)*

Column	Description	Privilege Required to Modify	Range/Length	Default
Owner	The user who opened the proactive case.	Not allowed to modify	Owner—Any valid AIM login username. Status: ■ Assigned ■ In progress ■ Completed	User who created the case (Assigned)
Status/Case ID	The JSS status of this proactive case. After the case has been created, the case ID appears. The case ID is assigned by JSS for the proactive case. This field is a link used to navigate to the JSS Case Management page	Not allowed to modify	Status: ■ Submitted ■ Created ■ Updated	Empty until case has been created/submitted
Flag	Indicates if this entry has been flagged to the user for inspection. A flag appears in the Flag column of the Proactive Case Manager table.	Not allowed to modify. You can remove a flag using the Clear Flag action.	N/A	None

Proactive Case Type Descriptions

Table 86 on page 222 describes the proactive case types.

Table 86: Proactive Case Types and Descriptions

Case Type	Description
Configuration Analysis and Change Review	Juniper Networks engineers review and analyze the configuration based on the customer's specified overall requirements to determine whether the current configuration is consistent with best practices for configuring and deploying a specific Juniper Networks product.
Customized Product Issue Report	Juniper Networks provides up to four reports each year about software and hardware defects found in the field that match the customer's deployed network profile.
Design Review	Juniper Networks engineers review the customer's network design, discuss high-level design goals and detailed design plan, assess the design, and analyze benefits and possible areas of improvement.

Table 86: Proactive Case Types and Descriptions *(continued)*

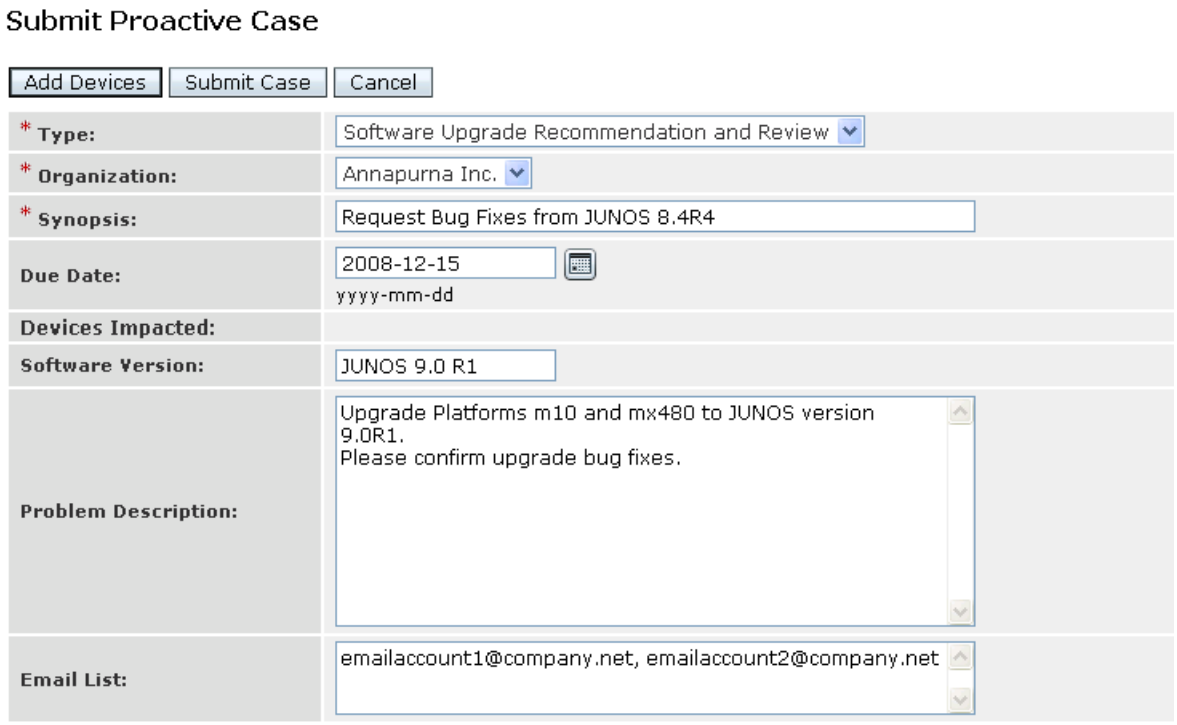
Case Type	Description
EOS/EOL/EOE Report	Juniper Networks provides one End-of-Life, End-of-Support, or End-of-Engineering report specific to customer's deployed Juniper Networks products based on the inventory data provided by the customer or collected through the AI-Script and AIM processes. The report typically includes device, announcement details, most recent software engineering support, most recent hardware engineering support, and replacement product information.
Feature Rollout Plan Review	Juniper Networks engineers review the customer's feature rollout plan, discuss the details of the plan, identify the impact and risks to help minimize service disruption.
Migration and Implementation Review	Juniper Networks engineers review the customer's network change methods and procedures and your acceptance test plan to identify areas of improvement.
Migration Implementation Support	Juniper Networks engineers are available during the network change implementation process to assist the customer with any questions, concerns, or problems during the migration.
Product Impact Issue Review	Juniper Networks engineers evaluate the defects that match the customer's deployed network profile and provide assessment and recommendations regarding the potential network impact and risk based on the customer's specific business and networking needs.
Software Upgrade Recommendation and Review	Juniper Networks engineers review and assess current software, hardware, and feature requirements provided by you, assess your software upgrade risk, analyze potential impact on your network, and recommend a target software release that can best meet your requirements.

Submitting a Proactive Case

You can submit a proactive case only if there are organizations, Proactive Case Manager lists all proactive cases for an organization. You must have access to the organization associated with the case. Access is determined by the user group you belong to and the device group associated to the user group. If there are no organizations, you see the following error message: Proactive cases cannot be submitted because there are no organizations that either contain devices or have valid credentials.

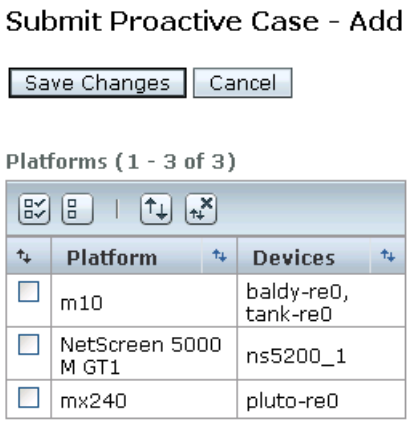
To submit a proactive case to JSS, follow these steps:

1. Select Proactive Case Manager in the AIM navigation area. The Proactive Case Manager table appears.
2. On the Proactive Case Management table, click Submit Proactive Case. The Submit Proactive Case page appears.



3. Provide the necessary information to submit a case to JSS. See “Submit Proactive Case Page Description” on page 225.

4. Click Add Devices to specify a device or devices for which you want to open a case. The Submit Proactive Case Add Devices page appears.



   This table only displays devices associated to the organization selected on the Create Proactive Case page.

5. Select the device platforms that you want to be included in the proactive case. For more information about the Submit Proactive Case–Add Devices page, see “Create Proactive Case–Add Devices Table Descriptions” on page 227.
6. Click Save Changes.
7. Click Submit Case. The proactive case is sent to JSS and saved in the AIM database. The new proactive case appears in bold in the Proactive Case Manager table.

Submit Proactive Case Page Description

Submit Proactive Case Page Button Description

Table 47 describes the Submit Proactive Case page command buttons.

Table 87: Submit Proactive Case Page Command Buttons

Button Name	Description	Privileges	Enabled/ Disabled	Results
Add Devices	Specify one or more devices for which to open a proactive case.	Submit Case	Enabled if user has privilege	Displays the Submit Proactive Case—Add Devices page
Submit Case	Submits a proactive case to Juniper Support Systems (JSS).	Submit Case	Enabled if user has privilege	Proactive case appears in bold in the Proactive Case Manager table.

Table 87: Submit Proactive Case Page Command Buttons *(continued)*

Button Name	Description	Privileges	Enabled/ Disabled	Results
Cancel	Cancels case submission	Submit Case	Enabled if user has privilege	Navigates back to the Proactive Case Manager page (where Submit Proactive Case was selected).

Submit Proactive Case Page Field Descriptions

Table 88 on page 226 describes the Create Proactive Case page fields.

Table 88: Submit Proactive Case Page Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Type	Type of proactive case. Maps to Issue Sub Type in Case Manager.	Submit Case	N/A	Select Type
Organization drop-down list box	The component containing the organizations to which the current user has access. Maps to Choose a Site in Case Manager.	Submit Case	N/A	Blank
Synopsis	Text description of the proactive case. Maps to the Synopsis on the Case Manager page.	Submit Case	200 characters	Blank
Due Date	Date by which the customer needs JSS to respond.	Submit Case	Blank or valid date	Blank
Software Version	Software version the customer wants to find out if the specified platform is compatible with so that the devices of that platform can be upgraded. Maps to Version on the Case Manager page.	Submit Case	Valid release format (for example R1)	Blank
Problem Description	Comments or questions the user wants to convey to the JSS engineer. **Note:**When the case is generated, the application generates information to be included in this field: the platforms specified, the release to which to upgrade, and the devices affected with their current software versions. Maps to Problem Description on the Proactive Case page.	Submit Case	65535 characters	Blank
Email List	List of e-mail addresses, separated by commas, to be notified when the case is submitted to JSS. Maps to Additional Email Recipients on the Proactive Case Manager page.	Submit Case	65535 characters	The e-mail list specified for the selected organization.

Create Proactive Case–Add Devices Table Descriptions

Create Proactive Case–Add Devices Table Descriptions

Table 89 on page 227 describes the Create Proactive Case–Add Devices table command buttons.

Table 89: Create Proactive Case—Add Devices Table Command Button Description

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Goes back to the Submit Proactive Case page.	Submit Case	Enabled if user has privilege	Goes back to the Submit Proactive Case page.
Cancel	Cancels the case submission.	Submit Case	Enabled if user has privilege	Goes back to Proactive Case Manager.

Create Proactive Case - Add Devices Table Description

Table 86 on page 222 describes the Create Proactive Case table columns.

Table 90: Create Proactive Case Page Field Descriptions Clearing a Flag

Name	Description	Privileges
Platform	Platforms to be upgraded. One of the specified platforms maps to "Platform" in Case Manager. The list of platforms will be included in the Problem Description.	Not allowed to modify
Devices	Comma-separated list of devices that are the specified platform and in the specified organization, which the current user has access to.	Not allowed to modify

Viewing Proactive Case Details

To view proactive case details, follow these steps:

1. Use the Proactive Case Manager table in My AIM Home or select Proactive Case Mgr in the AIM navigation area. The Proactive Case Manager table appears.

2. In the Proactive Case Manager table, click the Synopsis link for a case. The Proactive Case page appears.

Proactive Case

Save Changes | Flag to Users

Type:	Software Upgrade Assessment
Organization:	ACME Wireless Networks
Status:	Submitted
Case ID:	
Synopsis:	
Due Date:	2008-05-03
Platforms:	m10, mx480
Devices Impacted:	device001, device005, device007, device008
Release:	9.0
Version:	R1
Problem Description:	AIM Generated: Upgrade platforms m10, mx480 to software version 9.0 R1. Devices Impacted: device001, device005, device007, device008 Customer Specified: "Please confirm upgrade bug fixes"
Email List:	
Issued:	2008-04-01 13:56:59.0
Owner:	admin
Owner Status:	Assigned
Flagged to Users:	

From the Proactive Case page, you can:

- Flag a proactive case to a user; see “Flagging a Proactive Case to a User” on page 233.
- Assign a proactive case owner; see “Assigning a Proactive Case Owner and Changing Status” on page 232.
- Change the proactive case owner status; see “Assigning a Proactive Case Owner and Changing Status” on page 232.

If you assign a proactive case owner or change the case status, click Save Changes.

For more information about using the Proactive Case details page, see “Proactive Case Detail Description” on page 229.

Proactive Case Detail Description

Proactive Case Detail Command Button Description

Table 91 on page 229 describes the Proactive Case Details page command buttons.

Table 91: Proactive Case Detail Page Command Buttons

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Saves the changes you made in the Proactive Case details page	None	Enabled if the user is the owner of the case or if user has ownership privilege Level II or Level III	Changes to the modifiable attributes are saved.
Flag to Users	Lets you select which AIM users to alert about the proactive case	None	Always enabled	Goes to the Flag to User page. See “Assigning a Proactive Case Owner and Changing Status” on page 232.

Proactive Case Detail Field Descriptions

Table 92 on page 229 describes the Proactive Case Details page fields.

Table 92: Proactive Case Detail Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Type	Type of proactive case.	Not allowed to modify	N/A	Software Upgrade Assessment
Organization	Organization from which the case was created.	Not allowed to modify	N/A	Set by the user that created the case
Status	The JSS case status of this proactive case.	Not allowed to modify	Submitted, Created, Updated	Submitted
Case ID	The case ID generated and used by JSS for the proactive case. This field is a link and can be used to navigate into the Juniper Networks Case Management application.	Not allowed to modify	N/A	Empty until the case is created.

Table 92: Proactive Case Detail Field Descriptions *(continued)*

Name	Description	Privileges	Range/ Length	Default
Synopsis	Text description of the proactive case.	Not allowed to modify	N/A	Set by the user that created the case
Due Date	Date by which the customer must receive a response from JSS.	Not allowed to modify	Blank or Valid Date	Set by the user that created the case
Platforms	Device platforms specified to be upgraded	Not allowed to modify	N/A	Set by the user that created the case
Devices Impacted	Comma-separated list of devices that are to be upgraded in the specified organization, which the current user has access to.	Not allowed to modify	N/A	N/A
Release	Software release specified when the case is created (for example, 9.1).	Not allowed to modify	N/A	Set by the user that created the case.
Problem Description	The "AIM Generated" section is generated when the case is created by the application. This section lists the platforms specified, the release to which to upgrade, and the devices impacted with their current software versions. The "Customer Specified" paragraph is the comments or questions the user wanted to convey to the JSS engineer specified during creation of the case.	Not allowed to modify	N/A	Set by the user that created the case.
Email List	List of e-mail addresses, separated by commas, to be sent when the case is submitted to JSS.	Not allowed to modify	65535 characters	Set by the user that created the case
Issued	The date and time that the case was created.	Not allowed to modify	Date and time: YYYY-MMDD 24-hour time	N/A

Table 92: Proactive Case Detail Field Descriptions *(continued)*

Name	Description	Privileges	Range/ Length	Default
Owner	This drop-down list box lists the available AIM users that can be assigned ownership for this proactive case. To change the owner, select a different one in the drop-down list.	User with correct ownership privilege.	Users that have access to this case.	User that created the case
Owner Status	This drop-down list box lists the available status options for the owner.	Only current owner can modify	■ Assigned ■ In Progress ■ Completed	Assigned
Flagged to Users	List of users to which this case has been flagged or alerted	No privilege required	N/A	Blank

Assigning a Proactive Case Owner and Changing Status

To assign a proactive case owner, follow these steps:

1. Use the Proactive Case Manager table in My AIM Home or select Proactive Case Mgr in the AIM navigation area. Proactive Case Manager appears.
2. Click the Synopsis link for a proactive case. The Proactive Case page appears, providing more detailed information. For more information about the Proactive Case details page, see “Proactive Case Detail Description” on page 229.

3. To assign the proactive case, select a user from the Owner drop-down list box.
4. Select the proactive case status for the proactive case owner.

   The owner column in the Proactive Case Manager table displays the case owner with the status in parentheses ( ).
5. Click Save Changes. The proactive case owner user name is saved in the AIM database.
6. Select Proactive Case Mgr to see the new owner in the Proactive Case Manager table.

Flagging a Proactive Case to a User

Flagging a proactive case is used to inform other users who might be affected or need to be aware of an proactive case.

You can flag a proactive case to a user. Flagging a proactive case displays that proactive case in My AIM Home.

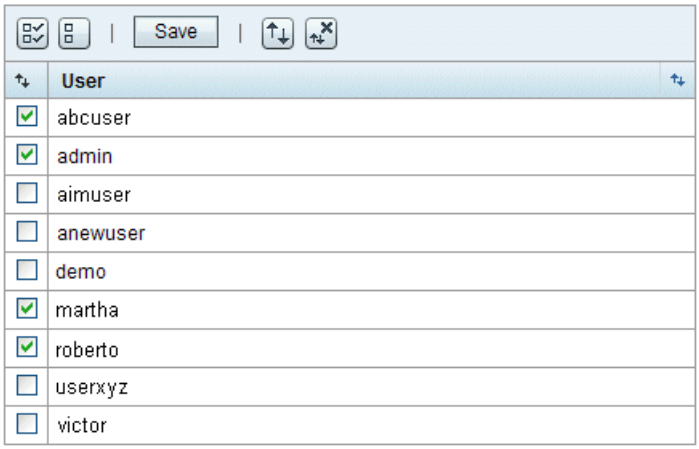
Proactive cases that are bold have been flagged to you since the last time you logged into AIM.

To flag a proactive case to a user from My AIM Home or the Proactive Case Manager user interface, follow these steps:

1. Use the Proactive Case Manager table in My AIM Home or select Proactive Case Mgr in the AIM navigation area. Proactive Case Manager appears.

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

Flag to Users



The Flag to Users page lists the available AIM users that can be assigned to a proactive case.

3. On the Flag to Users page, select the user or users to whom you want to flag the proactive case.
4. Click Save. A flag appears in the Flag column for that case when the flagged user logs into AIM.

Proactive Case Manager

Proactive Cases as of 2008-05-12 16:46:17 (1 - 6 of 6)

Submit Proactive Case | Clear Flag | Delete | Organization: All

Organization	Synopsis	Platforms	Software Version	Issued	Due Date	Owner	Status	Flag
ACME Wireless Networks	Request upgrade info from JUNOS 7.5	mx480	9.0 R1	2008-04-23 16:44:21.0	2008-04-24	admin (Assigned)	Submitted	
ACME Wireless Networks	Request bug fixes from JUNOS 8.4	m10, mx480	9.0 R1	2008-04-01 13:56:59.0	2008-05-03	admin (Assigned)	Submitted	
Connected Remote Solutions	Request security config feature info	m10, mx480, j4350, m7i	9.0 R1	2008-03-28 13:31:45.0	2008-03-29	admin (Assigned)	Submitted	
Connected Remote Solutions	Request upgrade info from JUNOS 8.5	m10	9.0 R1	2008-02-12 00:25:11.0	2008-02-13	admin (Assigned)	Submitted	
Mars Satellite Systems	Request feature fix if upgrade	j4350	9.0 R7	2008-02-05 13:32:54.0	2008-02-29	admin (Assigned)	Submitted	
Mars Satellite Systems	Request difference between 9.0R1	m7i	9.1 R2	2008-01-25 12:03:38.0	2008-02-02	admin (Assigned)	Submitted	

Clearing a Proactive Case Flag

1. Use the Proactive Case Manager table in My AIM Home or select Proactive Case Mgr in the AIM navigation area. The Proactive Case Manager table appears.
2. In the Proactive Case Manager table, select the proactive case. This action enables the Clear Flag button.
3. Click Clear Flag. The flag disappears from the Proactive Case Manager table.

Deleting a Proactive Case

To delete a proactive case, follow these steps:

1. Select Proactive Case Mgr in the AIM navigation area.
2. Select the proactive case you want to delete.
3. Click Delete. The proactive case becomes inactive in the AIM database and is removed from the Proactive Case Manager table.

Chapter 21

Creating Reaction Policies

This chapter describes how to create and edit a reaction policy. Use a reaction policy specify what conditions you want Advanced Insight Manager (AIM) to react to and what actions you want taken.

A reaction policy is a three-step process that requires:

- Trigger types that cause AIM to react. See “Parameters for Creating a Reaction Policy” on page 239.
- Filters to specifically determine which incidents or intelligence messages which you want AIM to react to. See “Parameters for Creating a Reaction Policy” on page 239.
- What actions to take after the specified incident or intelligence message is triggered. See “Parameters for Creating a Reaction Policy” on page 239.

You can create a reaction policy from the following locations in AIM:

- My AIM Home Reaction Policies Table
- Incident Manager from AIM navigation pane
- Reaction Polices from AIM navigation pane
- Organization Credentials page
- Incident Detail page
- Device Group page
- Proxy Device Group page

You must have the reaction policy user privilege to create an AIM reaction policy.

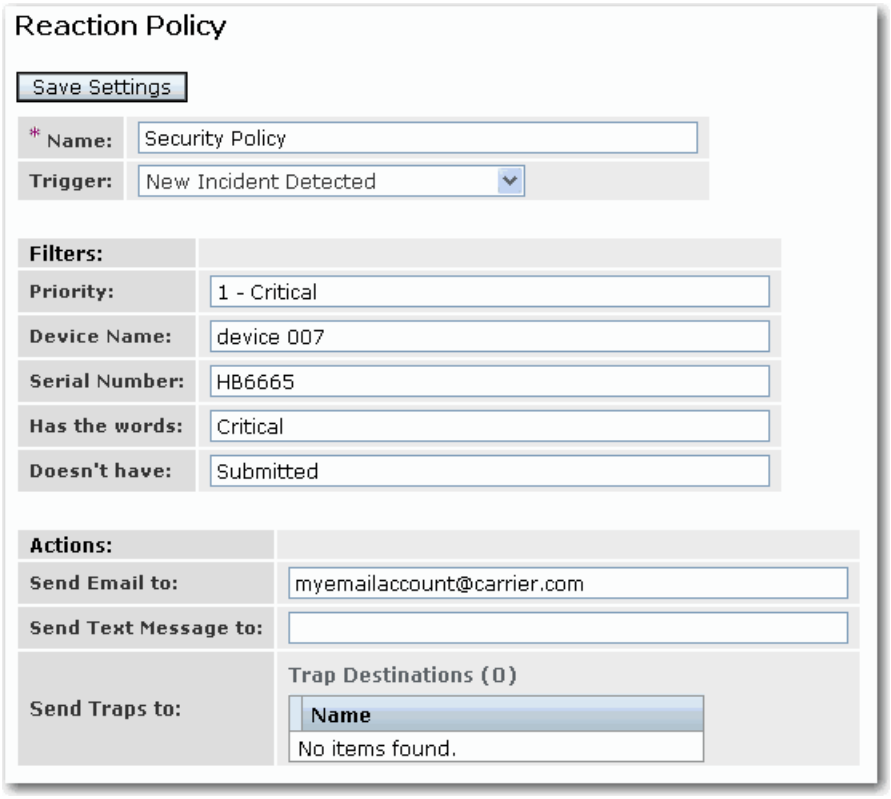
This chapter includes the following sections:

Creating a Reaction Policy

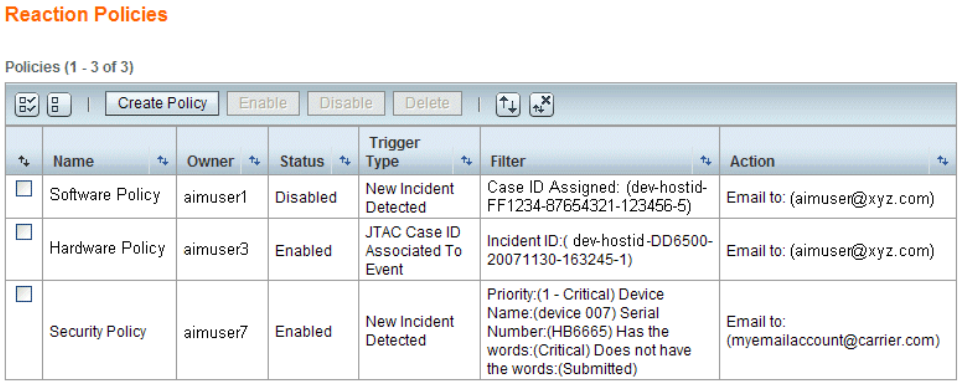
To create a reaction policy, follow these steps:

1. From My AIM Home, Incident Manager, Reaction Policies, Organizations, Incident Detail page, Device Group page, or Proxy Device Group page, click Create Policy.

   The Reaction Policy page appears.



2. Type a reaction policy name, then select a trigger. For more information about the Reaction Policy page, see “Parameters for Creating a Reaction Policy” on page 239.
3. Type in the filter parameters. Different filters are supported for incident and intelligence trigger types. The available filters change when you select the trigger type. If an incident trigger type is selected, see “Parameters for Creating a Reaction Policy” on page 239 for more information. If an intelligence trigger type is selected, see “Intelligence Trigger Type Reaction Policy Filter Parameters” on page 240 for more information.
4. Fill in the fields for the action you want AIM to take when the reaction policy criteria are met. For more information, see “Parameters for Creating a Reaction Policy” on page 239.
5. Click Save Settings at the top of the Reaction Policy page. For more information on the Save Settings command button, see “Actions for Creating a Reaction Policy” on page 239. The Reaction Policies table appears with the new reaction policy.



For more information on the Reaction Policy table, see "Reaction Policies Table Command Button Descriptions" on page 241 and "Reaction Policies Table Column Descriptions" on page 242.

Create Reaction Policy Page Descriptions

Actions for Creating a Reaction Policy

Table 93 on page 239 describes the Reaction Policy page actions.

Table 93: Create Reaction Policy Page Button Descriptions

Name	Description	Privilege Required	Enabled/Disabled	Results
Save Settings	Saves the settings for the policy being created or modified.	Reaction Policy	Always Enabled	Navigates user to the previous page the user was on.

Parameters for Creating a Reaction Policy

Table 94 on page 239 describes the parameters for creating a Reaction Policy.

Table 94: Create Reaction Policy Page Field Descriptions

Column	Description	Privilege Required to Modify	Range/Length	Default
Name	Name of policy, which must be unique within all the policies owned by the same user	Reaction Policy	32 characters	N/A

Table 94: Create Reaction Policy Page Field Descriptions *(continued)*

Column	Description	Privilege Required to Modify	Range/Length	Default
Trigger Type	Specifies the type of trigger required for this policy to be applied. The fields in the filter table dynamically change according to which filters the trigger type selected supports.	Reaction Policy	New Incident Detected, Incident Reported to Juniper, JTAC Case ID Assigned, JTAC Case Updated, New Intelligence Update Received	N/A
Filters:				
Priority	Matches priority of incident	Reaction Policy	256 characters	Blank
Device Name	Matches name of the device the incident occurred on	Reaction Policy	256 characters	Blank
Serial Number	Matches serial number of the device the incident occurred on, the serial number specified in the intelligence message	Reaction Policy	256 characters	Blank
Has the words	Matches the specified words against any of the fields in the incident or the intelligence update	Reaction Policy	256 characters	Blank
Doesn't have	Makes sure the specified words are not in any of the fields of the incident or the intelligence update	Reaction Policy	256 characters	Blank
Actions:				
Send Email to	List of e-mail addresses that receive an e-mail message if the policy is triggered and passes the specified filter. E-mail addresses should be separated by commas.	Reaction Policy	65535 characters	Blank
Send Text Message to	List of e-mail addresses that receive a text message if the policy is triggered and passes the specified filter. E-mail addresses should be separated by commas. (E-mail addresses are used to send the text message.)	Reaction Policy	65535 characters	Blank
Send Traps to	The table contains a list of all the trap destinations defined in the application. An SNMP trap will be sent to the destinations that are selected if the policy is triggered and passes the specified filter.	Reaction Policy	N/A	N/A

Intelligence Trigger Type Reaction Policy Filter Parameters

Table 95 on page 241 describes the parameters for the filters table when Intelligence Trigger Type is selected.

Table 95: Intelligence Trigger Type Reaction Policy Filter Parameters

Column	Description	Privilege Required to Modify	Range/Length	Results
Intelligence Update Type	Matches against type of intelligence message	Reaction Policy	256 characters	Blank
Products Affected	Matches against field in alert intelligence messages	Reaction Policy	256 characters	Blank
Platform Type	Matches against Platforms Affected field in alert intelligence messages or against platform type field in information intelligence messages	Reaction Policy	256 characters	Blank
Keywords	Matches against Keyword field in information intelligence messages	Reaction Policy	256 characters	Blank
Serial Number	Matches serial number of the device the incident occurred on or the serial number specified in the intelligence message	Reaction Policy	256 characters	Blank
Software Version	Matches against software version field in the information intelligence messages	Reaction Policy	256 characters	Blank
Hardware Version	Matches against hardware version field in the information intelligence messages	Reaction Policy	256 characters	Blank
Devices Impacted	Drop-down component indicating if the filter is enabled or disabled.	Reaction Policy	Enabled, Disabled	Disabled
Has the words	Matches the specified words against any of the fields in the incident or the intelligence update	Reaction Policy	256 characters	Blank
Doesn't Have	Makes sure the specified words are not in any of the fields of the incident or the intelligence update	Reaction Policy	256 characters	Blank

Reaction Policies Table Description

Reaction Policies Table Command Button Descriptions

Table 96 on page 241 describes the Reaction Policies table command buttons.

Table 96: Reaction Policy Table Command Button Descriptions

Element Name	Description	Privilege Required	Enabled/Disabled	Results
Create Policy	Creates a new policy	Reaction Policy	Enabled if privilege	Opens create reaction policy page

Table 96: Reaction Policy Table Command Button Descriptions *(continued)*

Element Name	Description	Privilege Required	Enabled/Disabled	Results
Enable	Enables any selected policies	Reaction Policy	Enabled if privilege and one or more products selected	Status of selected policies is changed to Enabled
Disable	Disables any selected policies	Reaction Policy	Enabled if privilege and one or more products selected	Status of selected policies is changed to Disabled
Delete	Deletes the selected policies	Reaction Policy	Enabled if privilege and one or more products selected	Removes the selected policies from the table

Reaction Policies Table Column Descriptions

Table 97 on page 242 describes the columns in the Reaction Policies table.

Table 97: Reaction Policies Table Column Descriptions

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Name	Name of policy that must be unique within all policies owned by the same user.	Hyperlink requires Reaction Policy privilege	32 characters	N/A
Owner	User that created the reaction policy.	N/A	N/A	N/A
Status	Indicates whether the reaction policy is running.	N/A	Enabled or Disabled	N/A
Trigger Type	Specifies the type of trigger required for the reaction policy to be applied.	N/A	New Incident Detected, Incident 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.	N/A	See Table 94 on page 239.	N/A
Action	Specifies the action taken if this reaction policy is triggered and the filter has passed.	N/A	See Table 94 on page 239.	N/A

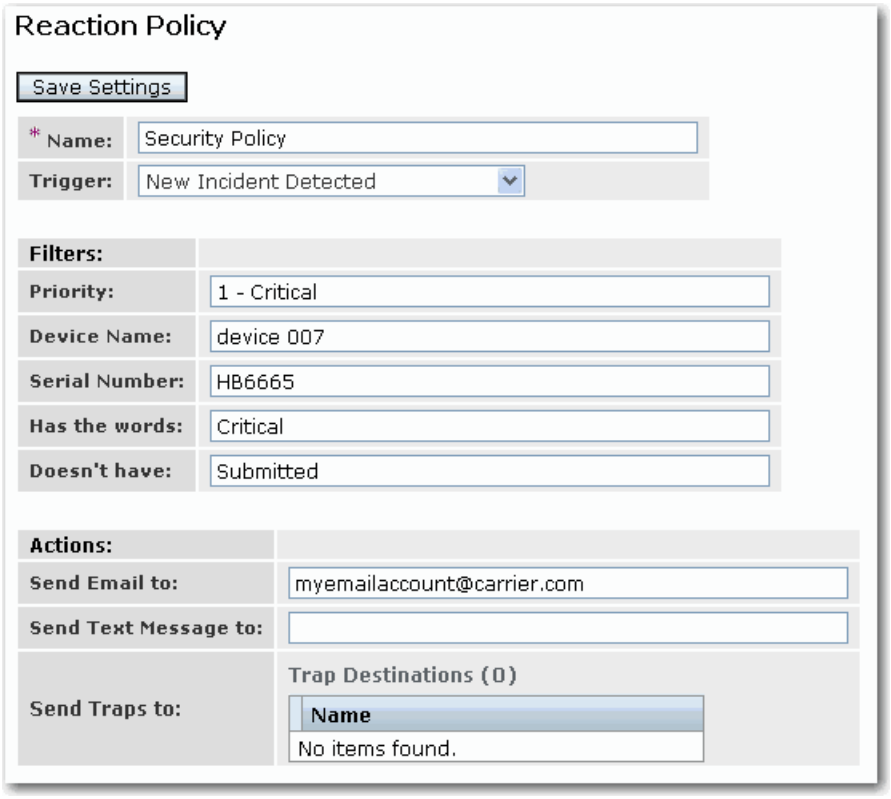
Editing a Reaction Policy

When you edit a reaction policy, the fields are filled with the current values of the policy.

To modify a reaction policy, follow these steps:

1. From the Reaction Policies table in My AIM Home or Reaction Policies, click the name link.

   The Reaction Policy page appears:



2. Edit the desired fields. See “Parameters for Creating a Reaction Policy” on page 239 and “Intelligence Trigger Type Reaction Policy Filter Parameters” on page 240 for more information.
3. Click the Save Settings command button at the top of the Reaction Policy page. The edited Reaction Policy parameters appear in the Reaction Policies table.

Enabling a Reaction Policy

To enable a reaction policy, follow these steps:

1. Select one or more reaction policies that you wish to enable on the Reaction Policy page.
2. Click Enable. This action activates the reaction policies. For more information, see “Reaction Policies Table Command Button Descriptions” on page 241.

Disabling a Reaction Policy

To disable a reaction policy, follow these steps:

1. Select one or more reaction policies that you wish to disable on the Reaction Policy page.
2. Click Disable. This action deactivates the reaction policies. For more information, see “Reaction Policies Table Command Button Descriptions” on page 241.

Deleting a Reaction Policy

To delete a reaction policy, follow these steps:

1. Select Reaction Policy(ies) that you wish to delete on the Reaction Policy page.
2. Click Delete. This action deletes the Reaction Policy(ies). For more information, see “Reaction Policies Table Command Button Descriptions” on page 241.

Part 6

Advanced Insight Manager Management Information Base (MIB)

Chapter 22

Advanced Insight Manager Management Information Base (MIB)

Advanced Insight Manager (AIM) supports the Juniper Networks Advanced Insight Manager enterprise-specific Management Information Bases (MIB). This MIB defines the traps sent by AIM to a remote network management system. See Table 98 on page 250. 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 175.

This chapter includes the following sections:

AIM MIB Contents

The MIB file is named jnx-ai-manager.mib and has 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-ACCESS read-only
STATUS  current
DESCRIPTION
        "Description of Advanced Insight notification."
::= { jnxAIManager 1 }
    jnxAIMHostName OBJECT-TYPE
SYNTAX  DisplayString (SIZE (0..63))
MAX-ACCESS read-only
STATUS  current
DESCRIPTION
"Device associated with Advanced Insight
notification."
::= { jnxAIManager 2 }
    jnxAIMOrganization OBJECT-TYPE
SYNTAX  DisplayString (SIZE (0..63))
MAX-ACCESS read-only
STATUS  current
DESCRIPTION
"Organization associated with Advanced Insight
notification."
::= { jnxAIManager 3 }
    jnxAIMIncidentHostID OBJECT-TYPE
SYNTAX  DisplayString (SIZE (0..63))
MAX-ACCESS read-only
STATUS  current
DESCRIPTION
"HostID of incident associated with Advanced
Insight notification."
::= { jnxAIManager 4 }
    jnxAIMCaseID OBJECT-TYPE
SYNTAX  DisplayString (SIZE (0..63))
MAX-ACCESS read-only
STATUS  current
DESCRIPTION
"CaseID (assigned by Juniper) associated with
Advanced Insight notification."
::= { jnxAIManager 5 }
    jnxAIMIssueDate OBJECT-TYPE
SYNTAX  DisplayString (SIZE (0..63))
MAX-ACCESS read-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 98 on page 250. These traps are organized by trap name, SNMP trap OID, and attributes.

Table 98: 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 7
Index

■ Index on page 253

Index

B

C

D

E

F

H

I

J

W