

Advanced Insight Manager (AIM) Frequently Asked Questions

November 2009
Revision 1

This document provides answers to frequently asked questions about the Advanced Insight Manager (AIM), a basic component of Advanced Insight Solutions (AIS). AIS is a Juniper Networks product used to enable automatic detection and packaging of reactive events and proactive intelligence information. It supports Juniper Networks E Series, J Series, M Series, MX Series, T Series, EX Series, Netscreen Firewall/VPN, SSG Series, WX Series, and SRX Series devices and routing platforms to ensure maximum uptime.

The AIM application provides a gateway between JUNOS device archive locations and Juniper Support Systems (JSS). It 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 Juniper Technical Assistance Center (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 detailed information about AIM, see the *AIS User Guide* and the *AIS Release Notes* located at <http://www.juniper.net/support/>.

Contents

AIM Overview	7
Q. What is AIM?	7
Q. How does AIM work?	7
Q. Does AIM operate in different modes?	7
Q. What are the types of AIM licenses?	8

Q. How do I activate AIS, if I am a partner?8

Q. How does AIM operate differently for end customers?9

Q. How do I activate AIS, if I am the end user?9

Q. Can multiple customers share the same J-Care Technical Services agreement through a single partner? 10

Q. Does AIM need JUNOScope?10

Q. When does AIM send notifications?10

Q. What information is sent between AIM and JSS?10

Q. What is in an iJMB?10

Q. What do I do if iJMBs are not being sent to JSS?10

Q. What communication protocols are used in transferring JMBs between JUNOS devices and AIM? 11

Q. How can I check if AIM is running?11

Q. How can I separately manage devices from multiple networks in AIM? 11

Q. Can I use SSH between AIM and a Juniper Device, when I use the export version on JUNOS and have not executed the Encryption Agreement? 11

System Requirements 11

Q. What browsers are supported to connect to the AIM server? 11

Q. What is the maximum number of devices that can be managed by a single AIM installation? 11

Q. What are the minimum installation requirements on Solaris and Linux OS for the AIM server? 12

Q. How much disk space does AIM require, according to the number of devices managed by AIM? 13

Q. Which virtualization products are supported for running AIM? 13

Q. What versions of AIM support a VM? 13

Q. Can I use an external storage medium (not on AIM) to store data collected from network devices? 13

Q. What are optimum bandwidth requirements between the network devices and AIM, and between AIM and JSS? 13

Installation 14

Q. Can I install AI-Scripts after installing AIM? 14

Q. Can the same authorization codes be used if AIM is re-installed on the same or a different server? 14

Q. Approximately how much time does it take to install the AIM server software on each supported platform? 14

Q. Can AIM and JUNOScope installations use the same mySQL port number? 14

Q. How are multiple networks handled in AIM? How do I ensure that only approved personnel have access to information about each network? 14

Q. Do I need any specific server maintenance operations for AIM? 15

Q. How do I uninstall the AIM application? 15

Setting Up AIM	15
Organizations	15
Q. What is an organization?	15
Q. What is a Test Mode?	15
Device Groups	16
Q. What is a device group?	16
Q. What are the types of device groups?	16
Q. What is a Directives Group?	16
Q. What is the best practice to configure archive locations?	16
Q. Which is the recommended protocol that can be used SCP, SFTP, FTP, or anonymous FTP?	16
User Groups	17
Q. Can I group different users in AIM?	17
Q. What AIM user privileges must I have to set up user groups?	17
License Management	17
Q. What does AIM License Manager do?	17
Q. What access privileges are required to use License Manager?	17
Q. Are there operational modes in AIM that require a valid license?	17
Q. How do I activate only particular features that I wish to use?	17
Q. Can I use AIM in Demo Mode? If yes, for how long?	18
Q. How do I activate the features that a license file supports?	18
Q. How can I tell which features are licensed in AIM?	18
Q. What is the purpose of a capacity license in AIM?	19
Q. How will I know when the device/services license capacity exceeds 100 %?	19
Q. How do I view which J-Care Technical Services licenses exist?	19
Q. How do I view the J-Care Technical Services license capacity usage?	19
JUNOS Configuration (Organizations)	20
Q. How do I use a public key instead of a password in the archive location URL?	20
Organization & Device Groups	21
Q. What are the prerequisites to create an AIM organization?	21
Q. How do I add devices to a directives group of AIM?	21
Q. Can I delete a device in AIM?	22
AIM Users	22
Q. What privileges do I need to manage AIM users?	22
Q. What are AIM user requirements?	22
Q. What is the default AIM username and password? How can I change it?	22
Q. What permissions do different levels of ownership have?	22
Q. What are the AIM user privileges?	23
Q. What permissions can I set for AIM users?	23
Troubleshooting	24
Q. Where can we find the explanations of notifications and error messages reported by JSS to AIM?	24
Q. How do I know if AIM is receiving JMBs?	24
Q. How can I suppress a specific AI-Script from executing?	24

Security	25
Q. How does AIM do authentication and authorization?	25
Q. What ports need to be opened on the Firewall and what is the direction of connection initiation between AIM & JSS?	25
Juniper Data Collector	25
Q. What is the Juniper Data Collector (JDC) ?	25
Q. How does the JDC operate?	25
Q. What type of information does the JDC show?	25
Q. How do I configure JUNOS and NS so that AIM can connect to them?	26
Q. Are there different types of JDC Directives?	26
Incident Manager	26
Q. What tasks can I perform using the Incident Manager?	26
Q. How do I submit a case to JSS?	27
Q. How does incident data flow at a partner AIM?	27
Q. How does incident data flow at an end user AIM?	27
Q. How can I manage incidents and cases in AIM?	28
Q. How do I control how I react to incidents?	28
Q. When AIM is configured to connect to a partner proxy AIM, can an end-customer submit Technical Support cases?	28
Q. Can I filter incidents?	28
Q. Can I view incident statistics for reporting?	28
Q. Can I alert other network operators about certain incidents?	29
Q. Can I view incident details?	29
Q. Can I view the JMB from the router?	29
Q. Can I view open incident JSS technical support cases?	29
Q. How do I specify how often I want AIM to scan for incidents?	29
Q. How do I control how often Incident Manager updates incident case status?	29
Intelligence Manager	30
Q. What does the Intelligence Manager do?	30
Q. What privileges do I need to use the Intelligence Manager?	30
Q. What is the intelligence update flow for a partner AIM site?	30
Q. What is the intelligence update flow for an end user site?	31
Q. Can I filter Intelligence updates?	31
Q. How do I determine whether an intelligence update affects devices on my network or not?	31
Q. How do I register for JSS alerts?	31
Q. Can I view the contents of an informational JMB?	32
Q. Can I notify other network operators of Information updates?	32
Q. How do I alter the interval between Information JMB upload to JSS?	32
Q. How do I change the Intelligence Update owner status?	32
Q. How do alerts or Intelligence updates appear in the Intelligence Manager?	32
Q. How often do the network elements report the iJMB (Intelligence-driven mode) to AIM?	33
Inventory Manager	33
Q. What does the Inventory Manager do?	33
Q. What access privileges do I need to use Inventory Manager?	33
Q. What inventory data can I view?	33

Q. How can I filter inventory data?	33
Q. Can I export data from the Inventory Manager to external systems/applications?	34
Q. What devices are shown in the Inventory Manager?	34
Q. How can I identify what hardware components are installed in a device?	34
Proactive Case Manager	34
Q. What does the Proactive Case Manager do?	34
Q. What access privileges do I need to use the Proactive Case Manager?	35
Q. What are the types of proactive cases?	35
Q. Can I create or submit a proactive case from an end-customer AIM?	36
Q. How can I submit a case from Proactive Case Manager?	36
Q. Does the Proactive Case Manager work in standalone mode?	36
Q. How can I change ownership or owner status of a proactive case?	36
Q. How can I alert other network operators about a proactive case?	37
Reaction Policies	37
Q. What do reaction policies do?	37
Q. What access privileges do I need to use reaction policies?	37
Q. What does a reaction policy use?	37
Q. What are the reaction policy trigger types?	38
Q. What are the reaction policy filters?	38
Q. What are the reaction policy actions?	38
Q. What are the Intelligence trigger type filters?	39
Q. How do I create a reaction policy?	39
Q. How do you enable or disable a reaction policy?	40
Trap Destinations	40
Q. What do trap destinations do?	40
Q. What are the trap destination settings?	40
Q. How do I add a trap destination?	40
AIM General Settings	41
Q. What privileges do I need to configure AIM general settings?	41
Q. How do I set the intervals at which AIM scans for JMBs, case status updates and intelligence updates?	41
Q. Can I determine how much of the device configuration is viewed by JSS?	41
Q. What is device aware support?	41
Q. How do I enable or disable device aware support?	42
Q. What is the maximum number of concurrent tasks in the JDC? How do I set it?	42
Q. What is the default RMI port setting?	42
Q. How do I test AIM connectivity?	42
Q. Can I modify a script bundle after it has been saved?	42
Q. How can I check how many days are left before the demo mode expires?	43
Q. What is the Home Base URL? How do I set it?	43
AIM Log Viewer	43
Q. What Log Viewer settings can I modify?	43
Q. How do I view AIM log messages?	44

Q. How do I set the priority for log files and the maximum number of backup log files AIM creates?44

Q. Can I control the roll over interval at which a new log is created?44

Q. Where are AIM logs located?44

Q. What are the types of AIM log messages?45

Q. What type of information does the AIM Install log show?45

Q. What type of information does the AIM Messages Exchange log show?45

Q. What type of information does the AIM Policy log show?45

Q. What type of information does the AIM JMB log show?45

MIBs46

Q. In what order do I need to load the AIM MIB using a MIB browser or trap receiver?46

Q. What SNMP traps does the AIM MIB support?46

AIM Overview

Q. What is AIM?

The Advanced Insight Manager (AIM) is a control point for AIS information flow. AIM is a standalone software application that runs on a Solaris or Linux server. It integrates readily with Juniper Networks products such as JUNOScope and third-party network management systems. In AIM, the Intelligence Manager and Incident Manager parse and present the device information that is stored in the database. This is done using an intuitive and user-friendly interface to help you monitor and analyze your devices.

You can also open a secure session with Juniper Networks Support Systems (JSS) so that AIM connects to JSS to create cases, get case updates, receive inform messages with alerts and notices from Juniper. AIM connects to the archive location to retrieve the information JMB. It then displays the information JMB in Incident Manager for reactive services and Intelligence Manager for proactive services. For reactive services, AIM submits a case, to obtain resolution from JSS. For proactive services, JSS analyzes intelligence information, and then sends AIM pertinent information to prevent problem events from occurring in the future

For more information about using AIM, see the “Using Advanced Insight Manager” chapter in the *Advanced Insight Solutions Guide*.

Q. How does AIM work?

AIM works as follows:

- Installs on a Sun Solaris or Red Hat Enterprise Linux server and connects to AIM from a Web browser.
- Processes incident JMBs through detection, case ownership, and case creation to quick resolutions.
- 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.
- Enables different functions based on the license features purchased.

Q. Does AIM operate in different modes?

AIM has three modes of operation:

- 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 partner is able to manage end customer AIMs and determine what information should flow to and from each end customer. This is done with the management of proxy device groups.

- End Customer Connected to Partner—The AIM end customer connects to the partner's AIM, using the partner's secure URL, and sends and receives information from the partner. The partner determines what information flows from the end customers' AIM to JSS. End customers run AIM normally, except that they cannot register for JSS alerts and intelligence messages, connect AIM directly to JSS, view AIM service licenses, or view the Technical Support Cases tab in Intelligence Manager.

Q. What are the types of AIM licenses?

There are two types of licenses available for different AIM engagement models. The engagement models are Direct Customer (Standard) and Partner Controller Engagement Models.

Q. How do I activate AIS, if I am a partner?

To activate AIS in the Direct Customer (Standard) and Partner Controller Engagement Models:

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. Select the **Generate Licenses** tab. The Generate License page appears.
4. From the drop-down list box, select **Advanced Insight Solution (AIS) Family**.
5. Click **GO**. The Generate Licenses — AIS Products page appears.
6. Enter the AIS software serial number, AIM install ID, and AIS authorization code.
7. Click **Generate**. This action generates the AIS license key file. You will receive an e-mail with the AIS license key file attached.
8. Copy the AIS license key file to the root AIM install directory on the AIM operating system.
9. Rename the license file `aim_license`.
10. Log in to AIM as an admin user.
11. Select the **Settings** tab, then click **License Management** in the navigation area. The License Management page appears.
12. Click **Load License File**. The license file is imported into AIM. This action activates the features the license supports.

Q. How does AIM operate differently for end customers?

End customers run AIM in the normal mode, except that they cannot perform the following operations:

- Register for JSS alerts and intelligence messages.
- Connect AIM directly to JSS.
- View the AIM service licenses.
- View the Technical Support Cases tab in the Intelligence Manager.

Q. How do I activate AIS, if I am the end user?

AIS can be activated for the end user by the partner, or by the end user.

- To activate AIS for the end user , the partner must follow these steps:
 1. Send the AIM software package to the end customer. The end customer installs AIM.
 2. When the end customer requests AIS services, provide the AIM install ID.
 3. Request an end user license from Juniper Networks .
 4. Use the install ID and the serial number and authorization codes provided by Juniper, and create a license file for the end customer.
 5. Create a new proxy device group that is contained by a currently defined AIM organization. This can be done using the AIM user interface, under **Settings > Organizations**.
 6. Provide the end customer with name, username, password, and AIS license key file.
- To activate AIS, the end user must follow these steps:
 1. Receive the AIM software package from the partner and install it.
The partner sends the end user the AIM software, partner controller URL for AIM, name, username, user password, and AIS license key file (`aim_license`).
 2. Install and start AIM.
 3. Send the AIM install ID to the partner.
 4. Log in to AIM using the username and password received in step one.
 5. Copy the `aim_license` license file to the root AIM install directory (for example, `/opt/aim`).
 6. In AIM, navigate to **Settings > License Management** and click **Load License File**.
 7. Navigate to **Setting > Organizations** and add a new organization using information from the partner.

8. Import the aim_license file.
9. Navigate to **Settings > General Settings** and add the partner's URL.
Click **Save Credentials**. This action will validate the organization credentials at the partner controller.

Q. Can multiple customers share the same J-Care Technical Services agreement through a single partner?

No. Each end-customer must have their own J-Care Technical Services agreement through which they choose their partner. However, the partner may use one AIM installation for multiple customers.

Q. Does AIM need JUNOScope?

No, AIM can run without JUNOScope. However, AIM works with JUNOScope to distribute and install AI-Scripts on JUNOS devices. It also works with JUNOScope to upgrade AI-Scripts.

Q. When does AIM send notifications?

AIM sends notifications when a reaction policy is triggered. Notifications are sent by SNMP traps or by email. See “Q. How do I create a reaction policy?” on page 39

Q. What information is sent between AIM and JSS?

Alerts, information updates, license information, and case status updates are sent between AIM and JSS. JMB's are also transferred between AIM and JSS, and customers have the opportunity to filter the level of configuration details that is shared with Juniper.

Q. What is in an iJMB?

An iJMB contains information about the device like, hardware inventory, software version, configuration details, attachments for various show output commands, trending data, system statistics, and counters representing current conditions for resource utilization and load.

This information is used by JSS to analyze incidents and to provide resolutions. . While incident JMBs are generated when an event occurs on a device, iJMBs contain device information that is sent on a regular basis to archive locations. Juniper uses iJMB's to provide faster case resolution, inform messages, and alerts that help customers prevent issues. They also help in preventing the incidents from recurring

Q. What do I do if iJMBs are not being sent to JSS?

Go to **Settings** and select **General Settings**. Ensure that **Device Aware Support** is enabled and that the **Information JMB Config Filter Level** is not set to **Do Not Send**.

On the Organizations page, make sure that the **Test Mode** is disabled. If it is enabled, iJMBs will remain in the Initial State in the Intelligence Manager.

Q. What communication protocols are used in transferring JMBs between JUNOS devices and AIM?

SCP and SFTP are used between JUNOS devices and AIM. HTTPS is used between the end customer's AIM and the partner's proxy AIM. All communications from the network devices to AIM, and from AIM to the JSS are secure and use authenticated and encrypted protocols. The Juniper Data Collector (JDC) uses SSH and SNMP to collect information from devices not running JUNOS 9.0 or later.

Q. How can I check if AIM is running?

Use the command `./allservices check`. This command will list the services and indicate whether they are running.

Q. How can I separately manage devices from multiple networks in AIM?

Organizations provide a way to manage multiple sites with one AIM installation by dividing the network into multiple logical customer sites. For a partner AIM organizations help manage many customers with a single AIM installation. For direct customers, organizations can be used to manage networks separately, with a single AIM. Every organizations has its own set of isolated devices and users.

Q. Can I use SSH between AIM and a Juniper Device, when I use the export version on JUNOS and have not executed the Encryption Agreement?

No. Without the Crypto license for JUNOS, SSH based protocols will not work. This is not limited to connections to AIM, but to any server where an SSH based protocol is required. If you are unable to use SSH between the Juniper device and AIM, you can use FTP .

System Requirements

Q. What browsers are supported to connect to the AIM server?

Microsoft Internet Explorer 6 and later, and Mozilla Firefox 2.0.0.16 and later are the supported browsers to connect to AIM.

Q. What is the maximum number of devices that can be managed by a single AIM installation?

You can manage up to 3000 devices on a single AIM installation.

Q. What are the minimum installation requirements on Solaris and Linux OS for the AIM server?

The free disk space allocation requirements for both Sun Solaris and Linux servers are:

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

Table 1: Minimum Requirement for Sun Solaris Server

System	Minimum Requirement for Sun Solaris Server
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	2 Gigabyte (GB)

Table 2: Minimum Requirement for Linux Server

System	Minimum Requirement for Linux Server
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	2 GB

Q. How much disk space does AIM require, according to the number of devices managed by AIM?

The free disk space allocation requirements for both Sun Solaris and Linux servers are:

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

Q. Which virtualization products are supported for running AIM?

VMware is the virtual machines that is supported by AIM.

Q. What versions of AIM support a VM?

Any version of AIM may run on a VM.

Q. Can I use an external storage medium (not on AIM) to store data collected from network devices?

An NFS mounted external storage device can be used as a storage medium. This does not require any extra JUNOS device configuration.

Q. What are optimum bandwidth requirements between the network devices and AIM, and between AIM and JSS?

The bandwidth requirements depends on the number of devices and the incidents they generate. As devices increase, the number of incidents increase, and more data will be transferred, thus more bandwidth would be required.

For example, for an M10i with a COSD_RTsock_LIB_ERR event:

- An eJMB was 444700 bytes. The configuration file in XML was 56062 bytes.
- The average eJMB size for this device for the last 27 eJMBs covering a variety of events is 869274 bytes.
- The latest iJMB for an M10i is 138286 bytes. The average for this device over 162 previous iJMBs is 140274 bytes.

Considering the M10i, if there were 500 devices in the network, then there would be $500 * 138286$ bytes (approximately 67MB) of iJMBs generated per week. The number of eJMBs would be on average $n * 869274$ bytes where n is the number of

incidents experienced and recognised by AI-scripts per week and 869274 the average eJMB size. These estimates depend on the number of devices, configuration size, type of incidents, etc.

An estimate of 500KB-1MB per JMB would be a good working number until enough JMBs had been collected in the local environment to more accurately ascertain the traffic impact.

Installation

Q. Can I install AI-Scripts after installing AIM?

The order in which you install AI-Scripts and AIM does not matter. However, it is recommended that you install JUNOScope first. For both AI-Scripts and AIM, 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.

Q. Can the same authorization codes be used if AIM is re-installed on the same or a different server?

Authorization codes are based on the install-id taken from the AIM server. The install-id changes for every AIM installation (even when reinstalling on the same server). Therefore if the AIM is re-installed, the authorization codes are required to be regenerated. To reset the install id for your authorization codes, call Juniper Customer Care.

Q. Approximately how much time does it take to install the AIM server software on each supported platform?

If the operating system pre-requisites are met, the AIM software installs in less than 10 minutes.

Q. Can AIM and JUNOScope installations use the same MySQL port number?

No, the AIM application and the JUNOScope software installations cannot use the same MySQL port number. They are separate installations, each with its 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. It then returns to the port screen to input a different port number.

Q. How are multiple networks handled in AIM? How do I ensure that only approved personnel have access to information about each network?

Organizations in AIM, provide a way to manage multiple sites with one AIM installation. An organization represents a customer site in Juniper Support Systems

(JSS). Device groups are used to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or devices that should otherwise be grouped together. One or more devices can be associated with every device group. Thus the network is divided and handled as multiple logical customer sites.

You can ensure that only approved personnel have access to information about each network by setting limited privileges for each user. Users are able to view only incidents and intelligence messages for which they have appropriate permissions.

Q. Do I need any specific server maintenance operations for AIM?

The disk space for the archive locations should be monitored on a regular basis.

Q. How do I uninstall the AIM application?

To uninstall the AIM application, use the following command on the host where you installed the AIM application:

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

Setting Up AIM

Organizations

Q. What is an organization?

An organization represents a customer site in Juniper Support Systems (JSS). Organizations provide a way to manage multiple sites with one AIM installation. This is done by dividing the network into multiple logical customer sites. To create an organization, you require the AIM Base Product license. To create more than one organization, you will need the AIM Multi-Site feature license. To communicate with JSS, an AIM organization requires a unique name, site ID (identifier used in the JSS system), login name, and password. It is also a prerequisite while creating an organization that you accept an agreement allowing sharing of confidential device information with JSS.

Q. What is a Test Mode?

Test mode in AIM prevents the processing of production incidents in JSS. In this mode, the synopsis of any incident sent to JSS is appended with **Test Mode**. When an incident from an organization in test mode is sent to JSS, JSS recognizes the incident as a test case, and does not process it.

Device Groups

Q. What is a device group?

Device groups are used to partition different devices within one organization. By associating an organization with one or more device groups, you can maintain groups of devices belonging to different customer networks. One or more devices can be associated with every device group, and to every device group you can associate an archive location. Further, you can associate a device group to one or more user groups. And every user group to one or more AIM users. To limit the access of users to certain groups of devices, device groups are used in conjunction with user groups.

Q. What are the types of device groups?

The types of device groups are:

- 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 device group for devices supported by the JDC.
- Proxy—A device group that contains a Juniper Networks partner's end customer. A proxy device group provides a way for the partner to control the incident and intelligence information that flows to and from an end customer. For each proxy device group, the partner should create a unique archive location for JMBs.

Q. What is a Directives Group?

A directives group is a group of devices from which the JDC can gather intelligence information. It specifies the archive locations of devices belonging to a group, into which the JDC can deposit JMBs. An organization can contain several directives device groups. Organizations do not share directives device groups. The directives group also has a JDC directives file (directives.rc) which specifies the data collection process that is performed for the devices in that group.

Q. What is the best practice to configure archive locations?

While configuring archive locations you can use `/opt/aimdata/ < siteid > / < device/directive/proxy group > /` . It is recommended that the archive location directory be used exclusively for JMBs and not for other AIM files.

Q. Which is the recommended protocol that can be used SCP, SFTP, FTP, or anonymous FTP?

SCP and SFTP can be used.

User Groups

Q. Can I group different users in AIM?

Yes, AIM allows you to arrange users into user groups. User groups contain a list of selected users. This selection is made from an existing pool of AIM users. The user group a user belongs to and the device group associated to that user group determine that user's access levels for organizations and for performing certain tasks within AIM. The user group name is unique within each AIM installation.

Q. What AIM user privileges must I have to set up user groups?

You need AIM Admin privileges to set up user groups.

License Management

Q. What does AIM License Manager do?

The AIM License Manager allows you to activate device capacity licenses, J-Care Technical Services licenses, and the AIM license file representing all AIM product elements. It also helps you manage different AIM features.

Q. What access privileges are required to use License Manager?

You need AIM Admin privileges to use the License Manager.

Q. Are there operational modes in AIM that require a valid license?

Yes, the three AIM operational modes that require a license are Base (Direct Customer), partner controller and End User.

Q. How do I activate only particular features that I wish to use?

You can use J-Care Technical Services based on the AIM features that you want to activate. Table 3 on page 17 shows the levels of J-Care Technical Services provided, and the associated AI-Scripts and AIM features that are offered.

Table 3: 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)

Table 3: J-Care Technical Services and AIS Functionality (continued)

J-Care Technical Service	AIS Features/Components
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.

Q. Can I use AIM in Demo Mode? If yes, for how long?

Yes, AIM operates in a fully functional demo mode for 60 days. In this mode, it will support one organization and five devices. To use AIM beyond a 60-day demo period, you require Base Product licensing.

Q. How do I activate the features that a license file supports?

To activate the features, you need to load the license file. To load a license file:

1. Log in to the 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. Select the **Generate Licenses** tab, and from the drop-down list box, select **Advanced Insight Solution (AIS) Family**. Click **GO**. The Generate Licenses — AIS Products page appears.
4. Enter the AIS software serial number, AIM install ID, and AIS authorization code.
5. Click **Generate**. This action generates the AIS license key file. You will 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.
9. Click **Settings** in the AIM user interface, then click **License Management**. The License Management page appears.
10. Click **Load License File**. The license file is imported into AIM. This action activates the features the license supports.

Q. How can I tell which features are licensed in AIM?

The AIM License Management page displays the current licenses and services after the license file is imported. To view the License Management page, in the AIM user interface, click **Settings**, then click **License Management**. The License Management page appears.

Q. What is the purpose of a capacity license in AIM?

A capacity license is required to increase the number of devices supported by AIM. The maximum capacity for each AIM installation is 3000 devices.

Q. How will I know when the device/services license capacity exceeds 100%?

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.

To view the Service Licenses page, in the AIM user interface, click **Settings**. Under License Management, click **Service Licenses**.

Q. How do I view which J-Care Technical Services licenses exist?

In the Services Licenses page, the **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, in the AIM user interface, click **Settings**. Under License Management, click **Service Licenses**.

Q. How do I view the J-Care Technical Services license capacity usage?

The total capacity (total number of devices that can be monitored by AIM for a specified device class) and actual usage (The number of devices of this class being monitored by AIM) are displayed on the Service Licenses page. To view the Service Licenses page, in the AIM user interface, click **Settings**. Under License Management, click **Service Licenses**.

JUNOS Configuration (Organizations)

Q. How do I use a public key instead of a password in the archive location URL?

Example of setting up public key authentication:

- The hostname of AIM server is aim-rhel402.
 - The hostname of JUNOS router is tito.
1. Generate a key pair. This can be done in the AIM server, JUNOS router, or a unix system.

```
$ ssh-keygen -t dsa -f aimaccess
Generating public/private dsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in aimaccess.
Your public key has been saved in aimaccess.pub.
The key fingerprint is:
fc:45:2d:ea:f1:9b:5f:cc:df:4e:ca:f4:7a:f3:1c:3d ckim@util1.wftac.jnpr.net
$ ls -l aimaccess*
-rw---- 1 ckim edge8 668 Sep 23 14:44 aimaccess
-rw-r-- 1 ckim edge8 615 Sep 23 14:44 aimaccess.pub
$
```

2. In AIM server, add that public key to the `authorized_keys` of AIMUSER. Ensure that you log in as AIMUSER, and be in the `aimaccess.pub` file in the working directory.
3. As root user shell, set the JUNOS router to use the key.

```
# cp aimaccess /etc/ssh
# vi ~/.ssh/config
...
Host aim-rhel402
  IdentityFile /etc/ssh/aimaccess
...
```

4. You can also set `ssh-known-hosts`, to avoid finger print prompt for the automation script.

```
lab@tito# set security ssh-known-hosts host aim-rhel402,10.3.1.94 rsa-key
AAAA.....zvtyKD8Zf1//U=
```

5. Set the archive-sites without a password.

```
lab@tito# set groups juniper-ais event-options destinations juniper-aim
archive-sites scp://aimuser@aim-rhel402/jmb/dev001
```

Organization & Device Groups

Q. What are the prerequisites to create an AIM organization?

The prerequisites to create an AIM organization:

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

Q. How do I add devices to a directives group of AIM?

To add devices to a directives group of AIM:

1. In the AIM user interface, select **Settings** and 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, from the drop-down list box, select **Add New Directives Group**. The Directives Group page appears.
4. 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 usernames are incorrect or if the network is not available.
5. Click **Save Changes**. The Devices table and the Associate User Groups table appear.
6. Click **Add New Device** in the Devices table to add a new device to the directives group. The Create Device and Add to Directives Group page appears.
7. Enter the new device settings and click **Test Connection**. You can add a JUNOS, JUNOSe, or Screen OS device using appropriate settings.

8. If the connection is successful, click **Create Device**. The new device appears in the Directives Group Devices table.
9. Click **Save Changes**.

Q. Can I delete a device in AIM?

No, you cannot delete a device in AIM.

AIM Users

Q. What privileges do I need to manage AIM users?

You need AIM Admin privileges to manage AIM users.

Q. What are AIM user requirements?

As an AIM user, you must have the following:

- Unique username
- Unique password
- Privileges that determine the operations you can perform

Q. What is the default AIM username and password? How can I change it?

The default AIM user account is:

- Username: admin
- Password: aimadmin

The default AIM user account cannot be deleted, and its privileges cannot be modified.

Q. What permissions do different levels of ownership have?

Table 4 on page 22 describes the permissions assigned to different AIM user ownership levels.

Table 4: AIM Ownership Levels

Ownership Level	Description
None	User is not allowed to own or assign ownership to any AIM user.
Level I	User can voluntarily take ownership of any unassigned incidents or intelligence messages.
Level II	User can voluntarily take ownership of any incidents or intelligence messages whether they are assigned or unassigned.

Table 4: AIM Ownership Levels (continued)

Ownership Level	Description
Level III	User can either give or take away ownership of incidents or intelligence messages to any user.

Q. What are the AIM user privileges?

Table 5 on page 23 describes the AIM user privileges.

Table 5: AIM User Privileges

Privilege	Description
AIM Admin Setting	<p>An AIM administrator can perform the following tasks.</p> <p>A logged-in user without Admin privileges, can only view these settings.</p> <ul style="list-style-type: none"> ■ 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.
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.

Q. What permissions can I set for AIM users?

You can set AIM Admin Setting, Ownership, Delete Incident, Reaction Policy, and Submit Case as the privilege for each user. Permissions for different features will be set based on these privileges. See “Q. What are the AIM user privileges?” on page 23.

Troubleshooting

Q. Where can we find the explanations of notifications and error messages reported by JSS to AIM?

The Synopsis and Problem Description fields explain the error messages reported by JSS to AIM. For a detailed explanation, please see the *AIM User Guide*.

Q. How do I know if AIM is receiving JMBs?

To know if AIM is receiving JMBs you can perform various tests.

Use the **Test Connection to Juniper** button in the AIM user interface (Organizations page) to check your connection status. The result of the test connection to JSS (success or Failure) is displayed for each of the selected organizations in the **Test Results** column.

You can also check if a JMB is being copied successfully to the AIM server, after being processed and copied to the `processedjmb` directory, and is made available in AIM.

To test device and AIM connectivity:

- Connect to the AIM server and in the archive location directory (for example, `ls -l/opt/archives`), look for *.xml JMB files. These files verify successful connectivity.
- In AIM Intelligence Manager, look for information JMBs by clicking the **Information JMBs** tab from the Intelligence Manager. Click **View Detail** to see device configuration details.

Q. How can I suppress a specific AI-Script from executing?

To suppress a specific AI-Script event-script from executing:

1. Find the name of the event-script you want to manually deactivate.
2. Set the policy and event of that event-script to "ignore".

```
set policy < event-script policy name > events < event-ID > then ignore
```



NOTE: By convention, the event-script policy name is the same as the event-script file name.

3. Commit the configuration change.

```
[edit groups juniper-ais event-options]
lab@bones# commit and-quit
[edit event-options]
'policy WEB_MGD_LISTEN_ERROR.slax'
warning: Policy 'WEB_MGD_LISTEN_ERROR.slax' is defined in both JUNOS
```

configuration database and event script, ignoring the one defined in event script
 commit complete
 Exiting configuration mode

Security

Q. How does AIM do authentication and authorization?

AIM does not connect to Juniper devices that are running AI-Scripts. If a directives group is configured on AIM, AIM uses SSH (shared secret) to connect to the devices.

Q. What ports need to be opened on the Firewall and what is the direction of connection initiation between AIM & JSS?

Port 443 needs to be opened on the Firewall. (This may be different for the https proxy)
 The direction of connection initiation is from AIM to JSS.

Juniper Data Collector

Q. What is the Juniper Data Collector (JDC) ?

The Juniper Data Collector (JDC) is an AIM service that collects data from Juniper Networks devices running versions before JUNOS 9.0 in archive locations for proactive monitoring in AIM. It also collects data from non-JUNOS devices, such as E-Series devices and Netscreen Firewall/VPN (ScreenOS) devices. The JDC functions like AI-Scripts. However, it only creates intelligence JMBs, not incidents.

Q. How does the JDC operate?

The JDC operates as follows:

- Collects intelligence data periodically for proactive monitoring.
- Receives configuration information, such as the names of supported devices, from the AIM database.
- Periodically collects data by sending JUNOScript XML commands to a device and receives intelligence information which it packages into a JMB.
- Sends the JMB to an archive location or folder on the AIM serve for AIM to collect and process it.

Q. What type of information does the JDC show?

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

Q. How do I configure JUNOSe and NS so that AIM can connect to them?

Following are configuration examples to connect to AIM:

```

JUNOSe    radius authn server 10.3.1.21
              key radius
              exit
              radius update-source-addr 10.3.222.3

              ip ssh crypto default blowfish-cbc
              ip ssh mac default hmac-md5
              crypto key generate dss
              no ip ssh disable-user-authentication

NS        set ssh version v2
              set ssh enable
  
```

Q. Are there different types of JDC Directives?

There are types of JDC Directives: JUNOS (for versions before 9.0), JUNOSe, and NS.

Incident Manager

Q. What tasks can I perform using the Incident Manager?

The Incident Manager provides a view of all incidents received by AIM. From the 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.
- View detailed incident information.
- Change incident ownership.
- View and change incident status.
- Submit and request a case ID.
- Flag an incident to a user.
- Remove a flag from any incident.
- View whether an incident has been submitted to JSS for a case to be opened to receive a case ID.
- Create a reaction policy.
- Delete any selected incidents.
- View all open JSS Technical Support cases.

Q. How do I submit a case to JSS?

To submit a case request to JSS:

1. From the Incident Manager, select the incident case that you want to submit. The **Submit Case** button is enabled.
2. Click **Submit Case**. You will see the following message if the case submission is successful:

Successfully submitted case to Juniper: Create Case returned transaction ID

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

The incident Case ID appears in the Status cell.

Q. How does incident data flow at a partner AIM?

Incident data at the partner site flows as follows:

1. The partner AIM receives a create incident case request from the end users AIM.
2. The partner AIM service detects the create incident case and processes 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's AIM Incident Manager.
5. The partner user with AIM administrative privileges decides whether to resolve the issue or send it to JSS. If the partner decides to send the incident to JSS, the partner adds the end user alias and trace route.
6. The partner decides whether to use the JSS incident case ID and link. If not, the partner edits the following fields in the AIM > **General Settings** page:
 - Partner case ID
 - Partner case link
 - Partner case status
7. The settings are saved.

Q. How does incident data flow at an end user AIM?

Incident data at the at the end user site, flows as follows:

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.
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.

Q. How can I manage incidents and cases in AIM?

You can manage incidents using the Incident Manager or My AIM Home. See “Q. What tasks can I perform using the Incident Manager?” on page 26.

Q. How do I control how I react to incidents?

You can use a reaction policy to specify what conditions you want AIM to notify you, and how. See “Q. How do I create a reaction policy?” on page 39.

A reaction policy uses:

- Trigger types that cause AIM to react
- Filters to determine which incidents or intelligence messages you want AIM to react to
- Actions to take after the specified incident or intelligence message is triggered

Q. When AIM is configured to connect to a partner proxy AIM, can an end-customer submit Technical Support cases?

No. Technical Support cases must be submitted to Juniper by the partner.

Q. Can I filter incidents?

Yes. 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 incidents by Defect, Device, device group, and organization. Filtered data is displayed in the Statistics Dashboard and the Incident Manager table.

Q. Can I view incident statistics for reporting?

Yes. The Statistics Dashboard at the top of the Incident Manager table provides a summary of displayed device incident data. You can view the statistics dashboard by clicking the + sign in the Incident Manager page. By default, the Statistics Dashboard is hidden.

Q. Can I alert other network operators about certain incidents?

Yes. Flagging an incident informs an AIM user who might be affected, or needs to be aware of an incident. You can flag an incident to a user. Flagging an incident displays that incident in the 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:

1. From the Incident Manager table, click the incident's **Synopsis** link. The Incident Details page appears.
2. Click **Flag to Users**. The Flag to Users page appears.
3. Select the users who should be notified of the incident.
4. Click **Save**. A flag appears in the incident Flag column in the Incident Manager table as a notification to the selected users.

Q. Can I view incident details?

Yes. To view incident details, click the incident **Synopsis** link in the Incidents table. The Incident for Device page appears with the details of the selected incident displayed.

Q. Can I view the JMB from the router?

Yes. You can view the information JMB and its contents collected by AIM from the device archive location.

To view an information JMB, click the **Information JMB** tab in the Intelligence Manager. The Information JMBs table appears.

Q. Can I view open incident JSS technical support cases?

Yes. To view the technical support cases, click the **Technical Support Cases** tab in the Incident Manager.

Q. How do I specify how often I want AIM to scan for incidents?

To determine how often AIM scans for incidents, you can set the **Incident Scan Interval** (min) on the **General Settings** page to the desired limit.

Q. How do I control how often Incident Manager updates incident case status?

To specify how often Incident Case Statuses are updated, you can set the **Case Status Update Interval** (min) on the **AIM General Settings** page to the desired limit.

Intelligence Manager

Q. What does the Intelligence Manager do?

The Intelligence Manager consists of two tabs: Intelligence Updates and Information JMBs.

Intelligence Updates tab provides a list of all Intelligence updates received from JSS. It allows you to 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 an alert flag
- Scan all devices managed by AIM for Intelligence messages or alerts
- Assign an Intelligence message or alert Owner
- Change Owner's Status

The Information JMBs tab provides a list of all intelligence JMBs or messages received from device archive locations. It 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

Q. What privileges do I need to use the Intelligence Manager?

You must have AIM admin and AIM ownership privileges to use Intelligence Manager.

Q. What is the intelligence update flow for a partner AIM site?

Intelligence updates at the partner's site, flows as follows:

1. The partner installs AIM Pro 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 sends the information JMB to JSS with an alias and trace route.

Q. What is the intelligence update flow for an end user site?

Intelligence updates at the end user's site, flows as follows:

1. The end user set 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's 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.

Q. Can I filter Intelligence updates?

Yes. You can filter Intelligence updates using the Organization drop-down list, in the Intelligence Updates tab.

Q. How do I determine whether an intelligence update affects devices on my network or not?

You can view all the contents of each Information Update. Click the Synopsis link in the Intelligence Updates tab.

Q. How do I register for JSS alerts?

You can register for JSS alerts using <http://www.juniper.net/alerts/>. The JSS Alert system allows you to go to the JSS support Web site and register for specific types of alerts that will be sent to you by email. The alerts you register for are selected from the Alert Registration table. You can ensure that the requested alerts are selected, while associating them with the current organization.

To registered for alerts:

1. From the AIM user interface, click Settings > Organizations. The Organizations table appears.
2. Click the name of the organization that you want to register alerts to. The Organization page appears.

The Alert Registrations table displays the alerts available for registration, that are retrieved from JSS. The alerts that the organization is already registered to, will be checked in the table.

3. Select the alerts that you want to register with the organization.
4. Click Save Changes. This registers the specified alerts with JSS.

Q. Can I view the contents of an informational JMB?

Yes. You can view the contents of an informational JMB using **Intelligence Manager** > **Information JMBs** tab, which 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

Q. Can I notify other network operators of Information updates?

Yes. You can flag an information update to users who might be affected or need to be aware of the Update. To flag an intelligence update to a user:

1. From the AIM user interface, click **Intelligence Manager** . The **Intelligence Updates** tab appears by default.
2. Click the **Intelligence message Synopsis** link. The **Information Entry** page appears.
3. Click **Flag to Users**. The **Flag To Users** page appears.
4. Select the users who should be notified of 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 of each flagged user.

Q. How do I alter the interval between Information JMB upload to JSS?

To specify the Information JMB upload interval to JSS, set the **Upload Information JMB Interval** on the **AIM Settings** > **General Settings** page.

Q. How do I change the Intelligence Update owner status?

To specify the intelligence owner status:

1. From **My AIM Home** or **Incident Manager**, click the incident **Synopsis** link. The **Incident Detail** page appears.
2. Select the desired status from the **Owner Status** drop-down list.
3. Click **Save Changes**. This saves the modified status in the AIM database.

Q. How do alerts or Intelligence updates appear in the Intelligence Manager?

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 retrieves 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/alerts to AIM Intelligence Manager, which is displayed on the Intelligence Updates tab. Thus, Intelligence Manager gets the Intelligence information.

Q. How often do the network elements report the iJMB (Intelligence-driven mode) to AIM?

By default, the interval used to poll for iJMBs in AIM archive locations is 3 minutes. You can change this by the setting the Intelligence Update Scan Interval (min) on the AIM General Settings page.

Inventory Manager

Q. What does the Inventory Manager do?

The Inventory Manager 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. The Inventory Manager allows you to:

- Filter Inventory Manager data by organization or device group, allowing you to view only the data of your choice.
- View device information details which shows all the components installed in the device chassis.
- Export Inventory Manager table data in Microsoft Excel, Comma-Separated Value (CSV), or XML format.

Q. What access privileges do I need to use Inventory Manager?

You only require AIM User privileges to use the Inventory Manager.

Q. What inventory data can I view?

You can view device inventory data displayed by organization and device group. The organization/Device Group name, Device and Platform details, Serial Number and Software Version are displayed. The Inventory Manager Chassis Detail page displays all the hardware components that are installed in a device. Note that, the Inventory Manager table will be empty if you do not have access to or have not created organizations or device groups.

Q. How can I filter inventory data?

To filter inventory data:

1. In the AIM Navigation area, select **Inventory Manager**. The Inventory Manager page appears.
2. From the **Filter By** drop-down list, 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.

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

Q. Can I export data from the Inventory Manager to external systems/applications?

Yes. You can export Inventory Manager table data in Microsoft Excel, Comma-Separated Value (CSV), and XML formats.

Q. What devices are shown in the Inventory Manager?

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.

Q. How can I identify what hardware components are installed in a device?

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

To view the Device Chassis details:

1. From the AIM user interface, select **Inventory Manager**. The Inventory Manager page appears.
2. Select a **Device Name** from 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.

Proactive Case Manager

Q. What does the Proactive Case Manager do?

The Proactive Case Manager lists all proactive cases of an organization. You can request an information upgrade to upgrading one or more Juniper Networks devices to a specified software release, or obtain other network services provided by JSS. From the Proactive Case page, you can:

- Flag a proactive case to a user.
- Assign a proactive case owner.
- Change the proactive case owner status.

Q. What access privileges do I need to use the Proactive Case Manager?

You only need AIM User privileges to use the Proactive Case Manager.

Q. What are the types of proactive cases?

Table 6 on page 35 describes the types of proactive cases:

Table 6: Proactive Case Types

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 plans, assess the design, and analyze benefits and possible areas of improvement.
EOS/EOL/EOE Report	Juniper Networks provides one End-of-Life, End-of-Support, or End-of-Engineering report specific to the 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, and 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 the customer's 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 the customer's current software, hardware, and feature requirements assess software upgrade risk, analyze potential impact on the network, and recommend a target software release that can best meet the customer's requirements.

Q. Can I create or submit a proactive case from an end-customer AIM?

No. Proactive cases can be created and submitted for the end-customer only by the partner.

Q. How can I submit a case from Proactive Case Manager?

To submit a proactive case to JSS:

1. From the AIM user interface, select **Proactive Case Manager**. The Proactive Case Manager table appears.
2. Click **Submit Proactive Case**. The Submit Proactive Case page appears.
3. Provide the necessary information before you submit the case.
4. Click **Add Devices** to specify a device(s) for which you want to open the 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 included with the proactive case.
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.

Q. Does the Proactive Case Manager work in standalone mode?

No, the Proactive Case Manager does not work in the standalone mode. If you are running AIM in the standalone mode, navigating to the Proactive Case Manager displays an error message.

Q. How can I change ownership or owner status of a proactive case?

To change ownership or owner status of a proactive case:

1. From the AIM user interface, select **Proactive Case Manager**. The Proactive Case Manager page appears. You can also navigate to the Proactive Case table from My AIM Home.
2. Click the **Synopsis** link of a proactive case. The Proactive Case page appears, displaying additional information.
3.
 - To change ownership, select the desired user from the **Owner** drop-down list.
 - To change status of the owner, select a status for the owner, from **Owner Status** drop-down list.

The owner column in the Proactive Case Manager table displays the Case Owner with the Status in parentheses ().

4. Click **Save Changes**. The proactive case owner's username is saved in the AIM database.
5. To see the new owner and owner status in the Proactive Case Manager table, navigate to the Proactive Case Manager.

Q. How can I alert other network operators about a proactive case?

You can alert other network operators about a proactive case by flagging a proactive case. This informs other users who might be affected or need to be aware of an proactive case. When you flag a proactive case to a user, that case is displayed 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:

1. Use the Proactive Case Manager table in My AIM Home or select Proactive Case Manager from the AIM navigation area. Proactive Case Manager page appears.
2. Select the case that you want to flag to the user.
3. Click **Flag to Users**. The Flag To Users page appears.

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

4. Select the users who must be notified of the proactive case.
5. Click **Save**. A flag appears in the Flag column for that case when the flagged user logs into AIM.

Reaction Policies

Q. What do reaction policies do?

Reaction policies specify the circumstances under which you want AIM to send a notification, and who the notification must be sent to.

Q. What access privileges do I need to use reaction policies?

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

Q. What does a reaction policy use?

A reaction policy uses the following:

- Trigger types that cause AIM to react
- Filters to determine which incidents or Intelligence messages you want AIM to react to
- Actions to take after the specified incident or Intelligence message is triggered

Q. What are the reaction policy trigger types?

The reaction policy trigger types are:

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

Q. What are the reaction policy filters?

Table 7 on page 38 describes the reaction policy filters. The maximum length of each of these filters is 256 characters and regular expressions can be used. You need the Reaction Policy user privilege to modify these filters.

Table 7: Reaction Policy Filters

Filter	Description
Priority	Matches priority of incident
Device Name	Matches name of the device the incident occurred on
Serial Number	Matches the serial number of the device the incident occurred on, the serial number specified in the Intelligence message
Has the words	Matches the specified words against any of the fields in the incident or the intelligence update
Doesn't have	Makes sure the specified words are not in any of the fields of the incident or the intelligence update

Q. What are the reaction policy actions?

The reaction policy actions are shown in Table 8 on page 38.

Table 8: Reaction policy Actions

Action	Description
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.
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.
Send Traps to	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.

Q. What are the Intelligence trigger type filters?

Table 9 on page 39 lists the Intelligence trigger type filters and their descriptions:

Table 9: Intelligence Trigger Type Reaction Policy Filters

Filter	Description
Intelligence Update Type	Matches the type of Intelligence message
Products Affected	Matches the products in alert Intelligence messages
Platform Type	Matches the Platforms Affected field in alert Intelligence messages or against the platform type field in information Intelligence messages
Keywords	Matches the Keyword field in information Intelligence messages
Serial Number	Matches the serial number of the device the incident occurred on or the serial number specified in the Intelligence message
Software Version	Matches the software version field in the information Intelligence messages
Hardware Version	Matches the hardware version field in the information Intelligence messages
Devices Impacted	Drop-down component indicating if the filter is enabled or disabled.
Has the words	Matches the specified words in any of the fields in the incident or the intelligence update
Doesn't Have	Makes sure the specified words are not in any of the fields of the incident or the intelligence update

Q. How do I create a reaction policy?

To create a reaction policy:

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. Specify a reaction policy **Name** and select a **Trigger**.
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.
4. Fill in the fields for the action you want AIM to take when the reaction policy criteria are met.
5. Click **Save Settings**. The settings are saved in the database and the newly created reaction policy appears in the Reaction Policies table.

Q. How do you enable or disable a reaction policy?

To enable or disable a reaction policy:

1. Select one or more reaction policies that you wish to enable on the Reaction Policy page.
2. To activate the reaction policy, click **Enable**.
To deactivate the reaction policy, click **Disable**.
3. Click **Save Settings**. The reaction policy will be activated or deactivated based on your selection.

Trap Destinations

Q. What do trap destinations do?

Trap destinations specify a destination for SNMP traps sent when an AIM reaction policy is triggered that has the Send Trap action option enabled.

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, traps that are sent can correspond to the following trigger types:

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

To view all trap destinations, go to **Settings > Trap Destinations**. All trap destinations are listed in the Trap Destinations table.

Q. What are the trap destination settings?

Trap destination settings include trap destination name, IP address, UDP port, community string, and protocol version.

Q. How do I add a trap destination?

To add a new trap destination:

1. From the AIM user interface, click **Settings**, 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 required trap destination information in the row fields.
4. Click **Save Changes**. The new trap destination appears on the Trap Destination page.

AIM General Settings

Q. What privileges do I need to configure AIM general settings?

You must have AIM administrator privileges, to configure AIM general settings.

Q. How do I set the intervals at which AIM scans for JMBs, case status updates and intelligence updates?

You can set these intervals by configuring AIM General settings. To configure AIM General Settings:

1. From the AIM user interface, click **Settings**. The General Settings page appears.
2. Set the required intervals on the AIM General settings page.
3. Click **Save Settings**. This action saves the settings that you modified and updates the AIM service with the intervals that you specified.

Q. Can I determine how much of the device configuration is viewed by JSS?

You can set the **Information JMB Config Filter Level** on the **General Settings** page to specify the amount of device configuration information within JMBs that can be shared with JSS. The filter options are:

- 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.
- Send all information with IP Addresses overwritten—Sends all device information, without IP addresses.
- Send all information—Sends all device information.

Q. What is device aware support?

Device aware support enables intelligence JMBs to flow to JSS, depending on the **Information JMB Config Filter Level** set by the user. By default this is disabled, which allows no intelligence JMBs to be sent to JSS. JSS accepts information JMBs regardless of Base or Pro Service. Information JMBs are counted against the device capacity licenses in AIM.

Q. How do I enable or disable device aware support?

To enable or disable device aware support:

1. From the AIM user interface, click **Settings**. The General Settings page appears.
2. Select the **Device Aware Support** drop-down list and specify the desired option.
3. Click **Save Settings**. This action enables or disables device aware support based on your selection and updates the AIM service with these new settings.

Q. What is the maximum number of concurrent tasks in the JDC? How do I set it?

The JDC maximum concurrent tasks setting, specifies the number of concurrent JDC tasks working in parallel to collect information from devices.

To set the JDC maximum concurrent task number:

1. From the AIM user interface, click **Settings**. The General Settings page appears.
2. Select the JDC maximum concurrent and specify the desired option.
3. Click **Save Settings**. This saves the changes you made and updates the AIM service with these new settings.

Q. What is the default RMI port setting?

The default RMI port setting for AIM service is 1122.

Q. How do I test AIM connectivity?

From the AIM user interface, click **Settings** and then click **Test Connection**. The **Test Results** field displays the results of the connection to JSS or an AIM partner.

The Test Result options are as follows:

- Success— URL is responsive
- No route to host
- Connection refused
- The Home Base server is temporarily unable to service your request

Q. Can I modify a script bundle after it has been saved?

No. A script bundle cannot be modified to remove shipped or add custom scripts. The script bundle will fail to add if it has been altered.

Q. How can I check how many days are left before the demo mode expires?

From the AIM user interface, navigate to **Settings > License Management**. When AIM is running in the demo mode, the following message appears in the License Management page:

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

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

Q. What is the Home Base URL? How do I set it?

The Home Base URL is the location to which information JMBs are sent.

- If you load a Partner Controller license file, the URL will be set to JSS (<https://services.juniper.net>).
- If you run AIM in Direct customer mode, enter <https://services.juniper.net>.
- If you run AIM in End Customer mode, enter the partner's URL (for example, <https://juniperpartner.com:8443>).

To set the Home Base URL, go to **Settings** from the AIM user interface, specify the URL and click **Save Settings**.

AIM Log Viewer

Q. What Log Viewer settings can I modify?

Table 10 on page 43 describes the Log Viewer settings that you can modify.

Table 10: Log viewer Settings

Log Viewer settings	Description
Priority	Sets the priority setting for log files: <ul style="list-style-type: none"> ■ Debug ■ Info ■ Warning ■ Error
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: <ul style="list-style-type: none"> ■ AIManagerJMB.log1 ■ AIManagerJMB.log2
Max File Size (KB)	Sets the maximum size a log file can reach before a new log file is created.

Table 10: Log viewer Settings (continued)

Log Viewer settings	Description
Date Pattern	Sets the interval at which a new log is created.

Q. How do I view AIM log messages?

To view an AIM log file in Log View:

1. From the AIM user interface, click **Settings > General > Logging**. The AIM Log View main page appears with no logs selected.
2. Select the tab for the AIM log file that you want to view. The AIM log message is displayed.

Q. How do I set the priority for log files and the maximum number of backup log files AIM creates?

To change AIM log file settings:

1. From the AIM user interface, 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/modify.
3. Set the **Priority** for log files. The priority options are: Debug, Info, Warning, and Error.

Set the **Backup File Count**. This 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.

4. Click **Save Changes**.

Q. Can I control the roll over interval at which a new log is created?

Yes. The Date Pattern field on the AIM Log Viewer sets the interval at which a new log is created.

To set the interval, from the AIM user interface, click **Settings > General > Logging**. The AIM Log View main page appears with no logs selected. Select the tab for the AIM log file you want to view and set the interval in the Date Pattern field.

Q. Where are AIM logs located?

AIM logs are located in the `/opt/aim/data/logs/` subdirectory where you installed AIM.

Q. What are the types of AIM log messages?

The types of AIM log messages are:

- AIM Messages Exchange Log
- AIM JMB Log
- AIM Policy Log
- Juniper Data Collector Log

Q. What type of information does the AIM Install log show?

The AIM Install log file shows 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.

Q. What type of information does the AIM Messages Exchange log show?

The AIM Messages Exchange log file shows when specific events occurred. For example:

- 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

Q. What type of information does the AIM Policy log show?

The AIM Policy log file contains messages about when a reaction policy was triggered and what action was taken when it occurred. For example, An e-mail was sent, A trap message was sent.

Q. What type of information does the AIM JMB log show?

The AIM JMB log file shows what time a JMB was processed and the reason (if any) why it was rejected.

MIBs

Q. In what order do I need to load the AIM MIB using a MIB browser or trap receiver?

When you use a MIB browser or other SNMP trap receiver, such as HP OpenView, to monitor the devices with SNMP, the following MIB files must be loaded in the order shown.

1. jnx-smi.mib
2. jnx-ai-manager.mib

Q. What SNMP traps does the AIM MIB support?

The AIM MIB supports the SNMP traps shown in Table 11 on page 46. These traps are organized by trap name, SNMP trap OID, and attributes.

Table 11: 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