

# Advanced Insight Solutions (AIS) Frequently Asked Questions

**11 June 2009**  
**Part Number: 530-029753-01**  
**Revision 1**

This document provides answers to frequently asked questions about 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.

AIS provides a comprehensive set of tools and technologies that work with Juniper Networks J-Care Technical Service offerings. AIS makes network operations simpler, more reliable and more cost-effective.

AIS enables faster problem identification, resolution, and avoidance within the customer's own support organization, the Juniper Networks partner's support organization, and the Juniper Technical Assistance Center (JTAC).

For more detailed information, see the *Advanced Insight Solutions Guide* and the *Advanced Insight Solutions Release Notes* located at <http://www.juniper.net/techpubs/software/management/ais/>.

## Contents

AIS Overview .....	3
Q. What is AIS? .....	3
Q. How can I get AIS? .....	3
Q. As a J-Assure customer with an active contract, can I use AIS without migrating to the new J-Care Technical Services? .....	4
Q. What are the major components in AIS? .....	4
Q. What are the basic customer engagement models in AIS? .....	4
Q. What is the AIS Incident (Reactive) Workflow? .....	4
Q. What is the AIS Intelligence (Proactive) Workflow? .....	5

- Q. Which Juniper Networks devices does AIS support? .....5
- Q. Does AIS support non-Juniper Networks devices? .....6
- Q. What are the basic AIS NOC roles? .....6
- Q. What type of incidents are detected by AIS? .....7
- Q. Can I define the incidents detected by AIS? .....7
- Q. How does AIS licensing work? .....7
- Q. How do I plan for AIS? .....8
- Q. Does Juniper Networks provide AIS training? .....9
- AIS System Requirements and Performance .....10
  - Q. What are the AIS system requirements? .....10
  - Q. What browsers and versions are supported by AIS? .....11
  - Q. How many devices can be managed by a single AIM installation? .....11
  - Q. Do I need any special patches on LINUX or Solaris? .....11
- AIS Security .....12
  - Q. How can I ensure that my confidential data is safe? .....12
  - Q. How does AIS ensure data transport security between network devices and AIM, and AIM and JSS? .....13
  - Q. Does Juniper ever access the AIM server on my network? .....13
  - Q. What authentication is used between AIM and network elements? .....13
  - Q. Who at Juniper can access my data? .....13
  - Q. Can I control the amount of information that I send to Juniper or a Juniper partner? .....13
- AIS Configuration .....14
  - Q. How do I activate AIS in a direct-customer engagement model? .....14
  - Q. How do I activate AIS in a partner-deployed engagement model? .....15
  - Q. How do I activate AIS in a partner end-customer engagement model? .....16
  - Q. Is it necessary to install the default Web and database server packages? .....16
  - Q. How do I verify that AIS is working? .....16
- AIS Operation .....18
  - Q. How does AIS work in a direct-customer engagement model deployment? .....18
  - Q. How does AIS work in a partner-deployed engagement model deployment? .....18
  - Q. How does AIS work in a partner end-customer engagement model deployment? .....18
  - Q. How do I report an AIS technical problem to Juniper? .....18
  - Q. Is it possible to submit a direct RMA with AIS? .....18
  - Q. How can other OSS systems be notified when an incident occurs? .....18
  - Q. How does information from network elements wind up in AIM? .....19

## AIS Overview

---

### Q. What is AIS?

Advanced Insight Solutions (AIS) provides tools and processes to automate the delivery of support services for Juniper Networks devices running on your network.

AIS provides reactive and proactive support for these devices operating in service provider and enterprise networks by:

- Automatically detecting events (incidents) and intelligence information
- Managing incidents to quick resolution by Juniper Technical Support using specialized tools.
- Providing intelligence information updates to prevent incidents from occurring.

A full AIS deployment includes the following components:

- The Advanced Insight Scripts, which run on each device running JUNOS software 9.0 or later.
- The Advanced Insight Manager (AIM), which runs at the customer site.
- The Juniper Networks Support Systems, which are located within Juniper Networks premises.

For more information on the components of AIS, see the *Advanced Insight Solutions Guide*.

### Q. How can I get AIS?

You can get AIS by following these steps:

1. Log into the Juniper Networks software download site and download the AIS components to install.

Download the following:

- 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/>
  - (Optional) JUNOScope Software:  
<https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/>
2. (Optional) Install and set up the JUNOScope software.
  3. Install and connect to AIM.
  4. Generate and activate the AIS license key.

5. Install and verify AI-Scripts.
6. Set up AIM.

For detailed information on these steps, see the “Setting Up Advanced Insight Solutions” chapter in the *Advanced Insight Solutions Guide*.

**Q. As a J-Assure customer with an active contract, can I use AIS without migrating to the new J-Care Technical Services?**

Yes, current J-Assure customers can use AIS as long as they have a valid J-Assure contract.

**Q. What are the major components in AIS?**

The major components of AIS are:

- AI-Scripts package
- Advanced Insight Manager (AIM)
- Juniper Networks Support Systems (JSS)
- JUNOScope Software (Optional)

**Q. What are the basic customer engagement models in AIS?**

The AIS basic customer engagement models are:

- Direct-Customer AIS Engagement Model
- Partner-Deployed AIS Engagement Model
- Partner and End-Customer Deployed AIS Engagement Model

For more information on these models, see the “Advanced Insight Solutions Overview” chapter in the *Advanced Insight Solutions Guide*

**Q. What is the AIS Incident (Reactive) Workflow?**

The AIS incident-driven workflow occurs as follows:

1. A trigger event occurs and is detected on a device configured for and running AI-Scripts. The appropriate operational script is executed.
2. An operational 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 incident appears in the Incident Manager, where it can be assigned or flagged to an AIM user. Once flagged or assigned, the incident appears in My AIM Home.
4. If desired, an AIM user submits the incident to JSS.

5. JSS connects to clarify and systematically creates a case and returns a case ID to AIM.
6. JTAC engineers work on the case. Case status updates are sent to AIM.

### **Q. What is the AIS Intelligence (Proactive) Workflow?**

JSS receives intelligence information from devices on the network that are AIS-enabled. Juniper Networks engineers use this information with customized tools to perform preventive analysis. JSS sends case statuses, intelligence updates, and alerts back to AIM. AIM periodically polls JSS for informational messages (created by Advanced Services engineers specifically for the customer) or alert messages (based on the alerts for which the customer registered). The intelligence-driven workflow occurs as follows:

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. You 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** tab.
5. AIM periodically queries JSS for intelligence updates. Intelligence Updates consist of alerts (based on the AIM alert subscriptions) or intelligence updates created by Advanced Services engineers specifically for the customer.
6. JSS stages 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.

### **Q. Which Juniper Networks devices does AIS support?**

Table 1 on page 5 shows the devices supported in AIS 1.3.

**Table 1: AIS Supported Devices**

<b>Device Category</b>	<b>Hardware Version</b>
EX Series Devices	EX320024P, EX320024T, EX320048P, EX320048T, EX420024F, EX420024P, EX420024T, EX420048P, EX420048T
J Series Devices	J20, J2300, J2320, J2350, J4300, J4350, J6300, J6350
M Series Devices	M5, M7i, M10, M10i, M20, M40, M40E, M120, M160, M320

**Table 1: AIS Supported Devices** (continued)

Device Category	Hardware Version
Netscreen (ScreenOS) Devices	NETSCREEN204, NETSCREEN208, NETSCREEN500, NETSCREEN5000MGT1, NETSCREEN5200, NETSCREEN520024FE, NETSCREEN52008G, NETSCREEN5200M1, NETSCREEN5200M2, NETSCREEN5200M210G, NETSCREEN5200M28G2, NETSCREENISG1000, NETSCREENISG2000, SSG140SB, SSG140SH, SSG320MSB, SSG320MSH, SSG350MSB, SSG350MSBNTAA, SSG350MSH, SSG350MSHDCNTAA, SSG350MSHNTAA, SSG520, SSG520B, SSG520M, SSG550, SSG550B, SSG550M, NETSCREEN540024FE, NETSCREEN54008G, NETSCREEN5400M1, NETSCREEN5400M2, NETSCREEN5400M210G, NETSCREEN5400M28G2
E Series (JUNOSe) Devices	E120, E320, ERX310, ERX700, ERX705, ERX1400, ERX1440
MX Series Devices	MX240, MX480, MX960
SRX Series	SRX5600, SRX5800
T Series Devices	T320, T640, T1600, TX Matrix

For a more detailed description on the supported devices see *AIS Release Notes*.

### Q. Does AIS support non-Juniper Networks devices?

No, AIS does not support other vendors' platforms.

### Q. What are the basic AIS NOC roles?

The roles in the network operations center (NOC) are:

- AIS Administrator
- AIM Administrator
- AIM User
- JUNOScope Software Administrator (Optional)



**NOTE:** The AIS Administrator has a UNIX ID outside AIM and it cannot be amended or deleted.

---

The design, setup, and implementation of the AIS system depends upon the existence of these NOC roles.

Levels of access granted to users can be:

- None — Not allowed to assign any user to any item
- Level I — Take ownership of any unassigned item

- Level II — Take ownership of any item
- Level III — Assign any user ownership of any item

Additional permissions are:

- AIM Admin Setting
- Delete incident
- Reaction Policy
- Submit Case

### **Q. What type of incidents are detected by AIS?**

AIS detects:

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

### **Q. Can I define the incidents detected by AIS?**

No, incident types are defined by Juniper engineers and are included in a single AI-Script bundle.

### **Q. How does AIS licensing work?**

Licensing works differently for various AIS components:

- AI-Scripts are free and require no licensing.
- AIM requires a combination of feature and capacity licenses to achieve full functionality.



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

---

AIM operates in fully functional, demo mode for 60 days. The demo mode allows AIM to support one multi-site organization and monitor five devices. AIM requires Base Product, Feature Licenses, Capacity Licenses, and Maintenance Service licenses.

- JSS validates licensing, receives incident case requests, resolves incidents, analyzes and sends intelligence updates to prevent incidence occurrence. A connection to JSS, for opening cases automatically, requires a valid J-Care technical services contract.

## Q. How do I plan for AIS?

To design and plan the AIS system, consider the tasks mentioned in Table 2 on page 8.

**Table 2: Planning for AIS**

Task	Description/Comment
Read the AIS documentation	<ul style="list-style-type: none"> <li>■ (Optional) <i>JUNOScope Software Release Notes</i> and the <i>JUNOScope Software User Guide</i> (See <a href="https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/">https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/</a>)</li> <li>■ <i>Advanced Insight Scripts (AI-Scripts) Release Notes</i> (See <a href="https://www.juniper.net/support/csc/swdist-encr/swdist-ais/">https://www.juniper.net/support/csc/swdist-encr/swdist-ais/</a>)</li> <li>■ <i>Advanced Insight Solutions Release Notes</i> (See <a href="https://www.juniper.net/support/csc/swdist-encr/swdist-ais/">https://www.juniper.net/support/csc/swdist-encr/swdist-ais/</a>)</li> <li>■ <i>Advanced Insight Solutions Guide</i> (See <a href="https://www.juniper.net/support/csc/swdist-encr/swdist-ais/">https://www.juniper.net/support/csc/swdist-encr/swdist-ais/</a>)</li> </ul>
What you need	<p>Access to the following systems and information is required to complete AIS installation:</p> <ul style="list-style-type: none"> <li>■ (Optional) Dedicated JUNOScope Linux or Solaris software server with appropriate permissions and requirements</li> <li>■ (Optional) JUNOScope software installer file</li> <li>■ (Optional) JUNOScope URL, AIS username and password added to JUNOScope for AIM, IP address for device-to-JUNOScope FTP connectivity, and devices managed</li> <li>■ Dedicated AIM Linux or Solaris server with appropriate permissions and requirements</li> <li>■ (Optional) FTP or file server for device archive locations <ul style="list-style-type: none"> <li>■ NFS mounted to AIM host</li> <li>■ FTP login and password</li> </ul> </li> <li>■ Clarify site ID and credentials</li> <li>■ AIM authorization codes and serial number sent by Juniper Networks</li> <li>■ Juniper Networks software download site URL and credentials</li> <li>■ AIM installer file</li> <li>■ AI-Scripts bundle file</li> <li>■ AI-Scripts installation, configuration, and verification (automatic or manual)</li> <li>■ AIM installation, set up, and verification</li> <li>■ Juniper License Management System (LMS) URL and credentials</li> <li>■ Juniper J-Care Technical Services contact information</li> </ul>
What to install	<ul style="list-style-type: none"> <li>■ (Optional) JUNOScope 9.0 Software or later</li> <li>■ AI-Scripts 1.1 or later</li> <li>■ AIM 1.1 or later</li> <li>■ AIM License File</li> </ul>

**Table 2: Planning for AIS (continued)**

Task	Description/Comment
Security considerations	<ul style="list-style-type: none"> <li>■ Set up firewall rules to allow outbound connections from the AIM server to JSS on TCP port 443.</li> <li>■ The local DNS should resolve <code>support.net</code> and <code>services.juniper.net</code>.</li> <li>■ Determine the level of device configuration filtering required for JMBs in archive locations.</li> </ul>
Determine AIS engagement model	<ul style="list-style-type: none"> <li>■ Direct-Customer AIS Engagement Model—The AIS direct customer installs AIS software elements (AI-Scripts and AIM).</li> <li>■ 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.</li> <li>■ 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.</li> </ul>
What organizations need AIS	<ul style="list-style-type: none"> <li>■ Customers or sites that need AIS</li> <li>■ Which devices are to be associated with the site ID and Juniper credentials (to define an organization)?</li> <li>■ Number of, and names for, device groups</li> </ul>
What devices need AIS	<ul style="list-style-type: none"> <li>■ Juniper Networks devices meet the AI-Scripts system requirements..</li> <li>■ Where will the archive locations for event and intelligence Juniper Message Bundles (JMBs) for each device be configured?</li> </ul>
What users will use AIS	<p>List the AIM users, including:</p> <ul style="list-style-type: none"> <li>■ Needed permissions</li> <li>■ Needed user groups</li> <li>■ Associations with device groups</li> <li>■ Initial reaction policies</li> <li>■ Initial alert registrations</li> </ul>

### **Q. Does Juniper Networks provide AIS training?**

No, there is no official live training program. However, an AIS online learning course is available to all customers at [http://www.juniper.net/us/en/training/technical\\_education/](http://www.juniper.net/us/en/training/technical_education/). You can also get help and assistance for the product from the AIS team (for a trial) and JTAC (for production).

## AIS System Requirements and Performance

### Q. What are the AIS system requirements?

Ensure that the client workstation from which you connect to the AIM application is running either on Microsoft Internet Explorer 6 or Mozilla Firefox 2.0.0.16 or later.

The AIM installation can be performed by either a root or a non-root (regular) user. A non-root user can change the default AIM install directory to any other directory. The AIM installer will prompt the root user for an existing user and user group, that is not root.

Ensure that you install AIM on a Sun Solaris or Red Hat Enterprise Edition Linux server. The minimum requirements for each of these is shown in Table 3 on page 10 and Table 4 on page 10.

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 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 representative

**Table 3: 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	1 Gigabyte (GB)

**Table 4: 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

**Table 4: Minimum Requirement for Linux Server** (continued)

System	Minimum Requirement for Linux Server
Processor	Pentium 4 processor
Speed	2.8 GHz or faster
RAM	1 GB

**Q. What browsers and versions are supported by AIS?**

AIS supports Microsoft Internet Explorer 6 and Mozilla Firefox 2.0.0.16 or later.



**NOTE:** In AIM 1.0, only Internet Explorer 6.0 and Mozilla are supported. We do not recommend use of any other browser version because it may display some screens incorrectly.

---

**Q. How many devices can be managed by a single AIM installation?**

You can manage up to 3000 devices on a single AIM installation. The number of devices depends on the processing power, storage space and network bandwidth of the AIM.

**Q. Do I need any special patches on LINUX or Solaris?**

Yes. Review the release notes and download relevant updates to your OS. GPG, especially, is required to ensure that license files are read correctly.

To see the AIS Release Notes, go to <http://www.juniper.net/techpubs/software/management/ais/ais13/>.

## AIS Security

---

### **Q. How can I ensure that my confidential data is safe?**

Ensure that these recommended security procedures are followed:

- Design and Planning
  - Carry out a risk assessment for all aspects of the AIS deployment.
  - Document the devices and data that need to be included in the AIS coverage.
  - Assess the level of filtering necessary on the data that AIM forwards to JSS.
  - Create a full security profile for the project, including appropriate design, deployment, and operational information.
- Deployment
  - Carry out hardening according to vendor recommendations.
    - Sun (Solaris): Please refer to <http://www.sun.com/security/index.jsp>.
    - Redhat Linux: Please refer to <https://www.redhat.com/security>.
  - Install AIM on a dedicated server or servers.
  - Ensure that communication between network elements (NEs) and AIM is on dedicated interfaces. Make sure that you use out of band (OOB) management infrastructure wherever possible, or use other segregation mechanisms such as virtual LANS (VLANS) or MPLS VPNs.
  - Create multiple archive locations for each NE to ensure availability.
- Operational
  - Restrict access to the host running AIM to staff with a direct operational requirement.
  - Ensure that all logs from this server are exported from the host and checked regularly.
  - Place AIM in a secure and monitored segment of the out-of-band (OOB) management network.
  - Carry out regular patching of the underlying operating system according to the manufacturer's recommendation.

Ensure that you change the admin password immediately the first time you access AIM.

**Q. How does AIS ensure data transport security between network devices and AIM, and AIM and JSS?**

All communications from the network devices to the AIM, and from the AIM to the JSS are secure. SCP can be used between the network elements and AIM. HTTPS is used between the AIM and JSS. HTTPS is also used between the end customer's AIM and the partner's Proxy AIM.

**Q. Does Juniper ever access the AIM server on my network?**

No. The connection from AIM to towards JSS is always upstream. AIM is not used as a base station host for accessing network elements.

**Q. What authentication is used between AIM and network elements?**

SCP or FTP can be used between AIM and network elements. The JDC however, uses SSH and SNMP to collect information from non-JUNOS 9.0 or later devices.

**Q. Who at Juniper can access my data?**

JTAC engineers, Proactive Engineers and Service Managers at Juniper can access your data.

**Q. Can I control the amount of information that I send to Juniper or a Juniper partner?**

Yes, you can decide what level of information you wish to share. Data is sent from your AIM to JSS over secure HTTP.

## AIS Configuration

---

### Q. How do I activate AIS in a direct-customer engagement model?

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.
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 a more detailed explanation, see the Activating Advanced Insight Solutions chapter from the *Advanced Insight Solutions Guide*.

### **Q. How do I activate AIS in a partner-deployed engagement model?**

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)



**NOTE:** This ID is only relevant for the connectivity between the AIMS. It does not determine your login details on the UNIX host or AIM.

---

- 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

## **Q. How do I activate AIS in a partner end-customer engagement model?**

To activate AIS, you 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. Send the AIM install ID to the partner.
  4. Log in to AIM using the default username and password (`admin/aimadmin`) credentials.
  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. In AIM, navigate 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 add the partner's URL.

On the Organizations page, click **Save Credentials**. This action validates the organization credentials at the partner controller. For more information about creating organizations, see the *Configuring AIM Organizations and Device Groups* chapter in *Advanced Insight Solutions Guide*.

## **Q. Is it necessary to install the default Web and database server packages?**

No, AIS uses its own copy of JBOSS and MYSQL. Hence, there is no need to install other packages.

## **Q. How do I verify that AIS is working?**

You know that AIS is working if:

- All services are running (use the `allservices check` command)
- You can log in to AIM.

- All test connections are successful to JSS, between AIMs, and to test archive locations.
- A JMB is 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 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 **Information JMBs** tab from the Intelligence Manager. Click **View Detail** to see device configuration details.

You can use the **Test Connection to Juniper** button in the AIM UI (Organizations page), to check your connection. The result of the test connection to JSS (success or failure) is displayed for each of the selected Organizations in the **Test Results** column.

## **AIS Operation**

---

### ***Q. How does AIS work in a direct-customer engagement model deployment?***

In a direct-customer engagement model, you install the AIS software elements (AI-Scripts and AIM), and directly subscribe to AIS services.

### ***Q. How does AIS work in a partner-deployed engagement model deployment?***

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 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.

### ***Q. How does AIS work in a partner end-customer engagement model deployment?***

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.

### ***Q. How do I report an AIS technical problem to Juniper?***

To report an AIS technical problem, open a technical support case, and select AIS as the platform with the issue.

### ***Q. Is it possible to submit a direct RMA with AIS?***

No, there is a possibility that a case will be raised based on particular events, and the result of this case may lead to an RMA. However, there is no direct RMA process within the AIM server.

### ***Q. How can other OSS systems be notified when an incident occurs?***

SNMP traps and emails can be sent to other OSS systems from AIM if the OSS systems needs to use these to perform some processing. Considering that many applications

today support XML, AIM can export JMB as an attachment via email and the XML content can be read. If desired, we can share the JMB XML structure, so that necessary mapping can be done to their data structure on the CRM if it supports XML.

**Q. How does information from network elements wind up in AIM?**

Information from network elements is sent to AIM with the help of AI-Scripts and the Juniper Data Collector (JDC).

AI-Scripts are installed on the customer's Juniper Networks JUNOS Software Network Elements (NEs) and these NEs export incident or intelligence data (JMBs) to AIM deployed at their site. AI-Scripts 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 the AIM.

The JDC 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 JDC also collects data from non-JUNOS devices, such as E Series devices and Netscreen Firewall/VPN (ScreenOS) devices. JDC functions like AI-Scripts. However, it only creates intelligence JMBs, not incidents.