

Advanced Insight Solutions 1.2 Release Notes

12 December 2008
Part Number: 530-026848-01
Revision 3

These release notes accompany Release 1.2R2 of the Juniper Networks Advanced Insight Solutions (AIS), a Juniper Networks product that provides reactive (incident-driven) and proactive (intelligence-driven) services for Juniper Networks J-series, M-series, MX-series, T-series, E-series, EX-series, and SRX-series routing platforms (devices).

You can also find these release notes, the *Advanced Insight Solutions Release Notes*, and the *AIS User Guide* on the Juniper Networks Technical Publications Web page, which is located at <http://www.juniper.net/support/>.

Contents

New Advanced Insight Solutions 1.2 Features	3
AIM 1.1 to 1.2R2 Automatic Upgrade	3
Juniper Data Collector	3
Juniper Data Collector JUNOS Devices	4
Juniper Data Collector E-series (JUNOSe) Device Support	5
Juniper Data Collector NetScreen (ScreenOS) Device Support	6
AIM Partner Controller and End-User Operational Modes	7
AIM Usability Enhancements	9
Advanced Insight Solutions Overview	10
Resolved Issues	11
Outstanding Issues	12
Installing and Configuring AIS Elements	12
AIS Quick Setup Checklist	13
Installing the Advanced Insight Manager Application	13
AIM System Requirements	14
Information Requested During Installation	15
DNS Access	16
Install ID and Licensing	17

- Downloading the AIM Application 17
- Running the AIM Application Installer 17
 - Running the Graphical Installer 18
 - Running the Console Installer 18
- Configuring the ai_manager.rc file 18
- Starting and Stopping AIM Services 19
 - Starting All Services Simultaneously 19
 - Starting Each Service Individually 19
 - Stopping All Services Simultaneously 20
 - Stopping Each Service Individually 20
- Using AIM Application Services Scripts 20
 - mysql 20
 - jboss 21
 - aimService 21
 - allServices 21
 - aimJDCService 22
- Connecting to the AIM Application and Logging In 22
 - Connecting to the AIM Application 22
 - Logging In to the AIM Application 23
- Changing the AIM Administrator Password 23
 - AIM Application Installation Directory Structure 23
- Uninstalling the AIM Application 24
- Upgrading from AIM 1.0 to AIM 1.2R2 24
- Automatically Upgrading from AIM 1.1 to AIM 1.2R2 24
- List of Technical Publications 25
- Requesting Technical Support 32
- Revision History 34

New Advanced Insight Solutions 1.2 Features

The Advanced Insight Manager has the following new features included in the current release. For more detailed information about new features in AIS 1.2, see the *AIS User Guide* on the Juniper Networks technical publications site, located at <http://www.juniper.net/support>.

- AIM 1.1 to 1.2R2 Automatic Upgrade on page 3
- Juniper Data Collector on page 3
- Juniper Data Collector JUNOS Devices on page 4
- Juniper Data Collector E-series (JUNOSe) Device Support on page 5
- Juniper Data Collector NetScreen (ScreenOS) Device Support on page 6
- AIM Partner Controller and End-User Operational Modes on page 7
- AIM Usability Enhancements on page 9

AIM 1.1 to 1.2R2 Automatic Upgrade

The AIM 1.2R2 installer automatically detects whether AIM 1.1 is installed, then asks the AIS admin whether to upgrade it. If the admin wants to upgrade, AIM 1.2R2 stops AIM 1.1, backs it up, and upgrades it. AIM 1.2R2 does not automatically upgrade AIM 1.0.

Juniper Data Collector

The Juniper Data Collector (JDC) gathers intelligence information from Juniper Networks devices that are not capable of running AI-Scripts, such as M-series, T-series, and J-series devices running versions of JUNOS prior to release 9.0, E-series devices running JUNOSe, and certain NetScreen Firewall/VPN devices running ScreenOS.



NOTE: The JDC supports earlier versions of JUNOS devices running the standard JUNOS operating system. It does not support devices running the JUNOS-EX or JUNOS-ES operating system variants. However, the AI-Scripts support all three variants of the operating system.

See “Juniper Data Collector E-series (JUNOSe) Device Support” on page 5 for specific JUNOSe and “Juniper Data Collector NetScreen (ScreenOS) Device Support” on page 6 for a list of specific NetScreen devices supported by the Juniper Data Collector.

The Juniper Data Collector processes the collected intelligence information and displays it in Advanced Insight Manager (AIM) Intelligence Manager for customer analysis. The AIM Intelligence Manager sends intelligence information (according to the Information JMB Configuration Filter Level option selected in AIM General Settings) to Juniper Support Systems (JSS). JSS processes the intelligence information and sends AIM Intelligence Manager proactive intelligence messages and alerts to maximize device operation on the network.



NOTE: The filter setting is set globally at the application level and applies to all device types. However JMB's for JUNOSe and ScreenOS devices contain no configuration data and are therefore not affected by this setting.

Juniper Data Collector JUNOS Devices

The Juniper Data Collector (JDC) supports the JUNOS devices listed in Table 1 on page 4. AI-Scripts supports all of the devices in this table.



NOTE: The JDC is currently supported in JUNOS releases 8.1, 8.4, and 8.5.

The JDC supports all of the devices in this table except where noted.

Table 1: Juniper Data Collector JUNOS Device Support

JUNOS Devices	Product Class
M-series Devices	
M5	Class 1
M7i	Class 1
M10	Class 1
M10i	Class 1
M20	Class 1
M40	Class 2
M40e	Class 2
M120	Class 1
M160	Class 2
M320	Class 2
T-series Devices	
T320	Class 3
T640	Class 3
TX	Class 3
Supported by AI-Scripts but not by JDC.	

Table 1: Juniper Data Collector JUNOS Device Support (continued)

JUNOS Devices	Product Class
TXP Supported by AI-Scripts but not by JDC.	Class 3
T1600 Supported by AI-Scripts but not by JDC.	Class 3
J-series Devices	
J2300	Class 1
J2320	Class 1
J2350	Class 1
J4300	Class 1
J4320	Class 1
J4350	Class 1
J6300	Class 1
J6350	Class 1
MX-series Devices	
MX960	Class 2
MX480	Class 2
MX240	Class 2

Juniper Data Collector E-series (JUNOSe) Device Support

The Juniper Data Collector (JDC) gathers intelligence information from the E-series devices. The JDC processes the intelligence information and displays it in the AIM Intelligence Manager for proactive analysis. In this release, the JDC is supported for JUNOSe release versions 8.0, 8.1, 8.2, and 9.0.



NOTE: The JDC only collects intelligence information. It does not collect device configuration information.

The JDC supports the E-series devices listed in Table 2 on page 6.

Table 2: E-series (JUNOSe) Devices

E-series (JUNOSe) Devices	Product Class
E120	Class 2
E320	Class 2
ERX 310	Class 2
ERX 700	Class 2
ERX 705	Class 2
ERX 1400	Class 2
ERX 1440	Class 2

Juniper Data Collector NetScreen (ScreenOS) Device Support

The Juniper Data Collector gathers intelligence information from the NetScreen devices listed in Table 3 on page 6. The Juniper Data Collector processes the intelligence information and displays it in AIM Intelligence Manager for proactive analysis.



NOTE: The JDC only collects intelligence information. It does not collect device configuration information.

Table 3: Netscreen (ScreenOS) Devices

Netscreen (ScreenOS) Devices	Product Class
NetScreen 204	Class 1
NetScreen 208	Class 1
NetScreen 5000 M GT1	Class 1
NetScreen 5200	Class 1
NetScreen 5200 24FE	Class 1
NetScreen 5200 8G	Class 1
NetScreen 5200 M1	Class 1
NetScreen 5200 M2	Class 1
NetScreen 5200 M2 10G	Class 1
NetScreen 5200 M2 8G2	Class 1

Table 3: Netscreen (ScreenOS) Devices *(continued)*

Netscreen (ScreenOS) Devices	Product Class
NetScreen ISG-1000	Class 1
NetScreen ISG-2000	Class 1
SSG 520	Class 1
SSG 520B	Class 1
SSG 520M	Class 1
SSG 550	Class 1
SSG 550B	Class 1
SSG 550M	Class 1
SSG-140-SB	Class 1
SSG-140-SH	Class 1
SSG-320M-SB	Class 1
SSG-320M-SH	Class 1
SSG-350M-SB	Class 1
SSG-350M-SB-N-TAA	Class 1
SSG-350M-SH	Class 1
SSG-350M-SH-DC-N-TAA	Class 1
SSG-350M-SH-N-TAA	Class 1
NetScreen 5400 24 FE	Class 2
NetScreen 5400 8G	Class 2
NetScreen 5400 M1	Class 2
NetScreen 5400 M2	Class 2
NetScreen 5400 M2 10G	Class 2
NetScreen 5400 M2 8G2	Class 2

AIM Partner Controller and End-User Operational Modes

You can run AIM in a cascaded Partner Controller and End Customer engagement method. Juniper Networks partners and their end customers can use AIM with the same or similar functionality as a direct customer. The interaction between the AIS components in an AIM partner and end user installation is as follows:

- The partner installs AIM and connects it to JSS.
- The partner requests a license from Juniper Networks to enable AIM Partner Controller functionality.
- The partner's end users install AIM and configure it to connect to the partner's AIM. End users connect to the partner using the HTTPS communication protocol. The URL used for connection between the end user and the partner is configured on the AIM Settings > General Settings page in the end user's installation.
- The partner creates a proxy device group for each end user and activates the groups with JSS. This can be done through the AIM Settings > Organizations page.
- The partner administrator controls which AIM users have access to each end user by associating user groups to the proxy device group.
- The partner creates reaction policies directed to a proxy device group. This allows the partner to react to certain events (such as a New Incident Detected) specific to a particular end user.
- The end user installs AI-Scripts on devices on the network and sets up AIM to detect device event and informational JMBs.
- The end user operates AIM the same way as an AIM direct customer. However, instead of communicating directly with JSS, the end user communicates with the partner.
- The partner manages communication to and from the end users. For example, cases submitted by the partner's end users can be handled directly by the partner or forwarded to JSS for resolution by Juniper Networks JTAC engineers.
- When partners use their own case management system to track problems, they can integrate with AIM by providing the case link, status, and ID references for each incident reported. AIM forwards the case link and ID to the end user, thus providing the end user with access to the partner's case management system.
- Partners forward any intelligence messages received from JSS to their end users at their discretion. The intelligence message can be customized by the partner before it is sent to the end user.
- The partner's AIM filters end-user items can be based on a specific proxy device group, enabling the partner to view all incidents for a particular end user.

New partner and end user AIM user interface changes appear in AIM as follows:

- License Manager—A new license is required for AIM Partner Controller mode.
- General Settings—Includes a new field for adding the URL used to connect to JSS or a partner. If AIM is run in standard or partner modes, this URL is always the current JSS URL: <https://services.juniper.net>. If AIM is run in end user mode, the URL can be changed to the partner's URL.
- Proxy Organizations—When AIM is run in Partner Controller mode, the partner can create a proxy organization which is a sub-organization representing a end user in the partner's AIM. Proxy organizations allow a partner to view the alerts and informational message sent to a specific end user.
- Organization Device Groups—A device can belong to only one AIM Organization Device group. The Device group is for administrative operation that can lead to

the overwriting of settings on a device. Device groups are visible in all three AIM modes of operation. In the current AIM release, Directives groups are for devices not capable of running AI-Scripts and that use the Juniper Data Collector to gather operational data. Devices can belong to more than one Directives group.

Directives groups are visible in all three AIM modes of operation.

- Incident Manager—An addition to the Organization/Device Group column shows the proxy organization alias. A partner can create a case on behalf of an end user. The Filter by list box name has been changed to Show and includes proxy organizations. The On drop-down list box dynamically changes to show the available proxy organizations. The partner only sees incidents for devices to which they are associated through the user groups to which they belong.
- Incident Details—The Incident Manager Incidents Details page includes new fields for incidents when run in Partner Controller mode so that the partner can resolve an incident themselves instead of JSS by creating a non-Juniper Networks case link, case ID, and case status. If these fields are left unmodified, JSS resolves the case using the JSS attributes.
- Reaction Policies—All reaction policy types now also apply to a proxy organization. Two new reaction policy types (only available in AIM Partner Controller mode) have been added: Incident Reported by End Customer and New Approval Required.
- Intelligence Manager—The Intelligence Updates tab allows filtering by proxy organization to allow the partner to view the alerts and informational messages that have been sent to a specific end user. The Intelligence Updates tab includes a new column for proxy organizations to which an alert or intelligence message has been sent. A new Associate Proxy Organizations button on the Information Entry and Alert Entry pages allows the partner to associate the end users to whom to send alerts and informational messages. A new row in the Intelligence Manager table shows the proxy organizations to which an alert or informational message has been sent. The Scan for Impact page displays a table of all the proxy organizations that the alert or informational message affects. The Scan for Impact page also lets the partner decide to which proxy organizations to send an intelligence update.

AIM Usability Enhancements

The following revisions have been made to the AIM user interface:

- Reaction Policies Page—You can create reaction policies, all attributes, and edit them from a single page instead of a 3-page wizard. Different filters are dynamically available for incident trigger and intelligence trigger types.
- Show/Hide Statistics Dashboard in Incident Manager and Intelligence Manager—You can hide the statistics dashboard on both the Incident Manager and Intelligence Updates to conserve page real estate. You can toggle the statistics dashboard by clicking Show/Hide Statistics. The Filter by and Organizations drop-down list box names have changed to Show.
- Two Incident Manager Tabs: Incidents and Technical Support Cases—The Incidents tab displays all incidents that have been collected from devices. The new Technical Support Cases tab displays all open JSS cases for all site IDs for an AIM installation. The Technical Support Cases tab is available for AIM

Direct-Customer (Standard) and Partner Controller modes. A Refresh button updates retrieves the current open cases.

- My AIM Home User Access Status Message—A system messages notifies an AIM user when they log in on the My AIM Home page if they have been removed from any user group. When a user is removed from an AIM user group, they no longer have access to any incidents, intelligence updates or proactive cases associated with that user group.
- Save Changes On Incident Manager Case Submittal—Any changes made when you submit a case on the Incident Details page will first be saved before the case is sent to JSS for resolution. The Priority, E-Mail List, Owner, and Owner Status fields will be saved.
- Auto-Save During the Creation and Modification of AIM Items—AIM automatically saves a draft every 30 seconds when you create an organization, device groups, reaction policies, and proactive cases. This action lets you navigate away from an item creation without losing any of the attributes. To return to an item in creation, click Drafts in the AIM navigation area. Clicking the draft item name displays the items detail page. When you save the item, it becomes active in AIM and is removed from Drafts. AIM automatically saves when you modify intelligence updates and proactive cases. When the item is modified, the Save Changes button is enabled. If after 30 seconds changes have not been saved by the user, AIM saves the item and the Save Changes button is disabled.
- Device Aware Support General Setting—Enabling device aware support causes intelligence JMBs to flow through AIM to JSS filtered to the Information JMB Configuration Filter Level option selected. Disabling device aware support allows intelligence JMBs to flow based on the whether the AIM Pro functionality exists. JSS accepts intelligence JMBs regardless of whether AIM Base or Pro is enabled. Systems that send information JMBs continue to be counted against the License Management System device counts at AIM installation.

Advanced Insight Solutions Overview

Juniper Networks Advanced Insight Solutions (AIS) provides reactive (incident-driven) and proactive (intelligence-driven) services for Juniper Networks devices. AIS is available when you purchase one of the top three levels J-Care Support Services to support and maintain devices on the network. See Table 4 on page 10.

Table 4: 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, AIM Reports, AIM Inventory Management
J-Care Continuity	AI-Scripts, AIM Case Submission, AIM Reports, AIM Inventory Management, JSS (Insight JTAC)
J-Care Agility	AI-Scripts, AIM Case Submission, AIM Reports, AIM Inventory Management, JSS (Insight JTAC), AIM Proactive Product Reports (Intelligence)

AIS consists of three major elements:

- AI-Scripts run on devices to automatically detect incidents and intelligence information and sends data in Juniper Message Bundles (JMBs) to archive locations.
- Advanced Insight Manager (AIM) collects incident and intelligence data from archive locations and displays it so you can resolve incidents and receive proactive intelligence information to prevent incidents from reoccurring.
- Juniper Support Systems (JSS) resolve incidents and provides preventive intelligence information that is displayed for the user in AIM.

For more overview information about AIS, see the “Advanced Insight Solutions Overview” chapter in the User Guide.

Resolved Issues

The following issues have been resolved in the AIS 1.2R2 application release:

- AIM Install**
- When using the `allservicescript`, there is no 3-minute pause between starting the `jboss` service and starting the `aimService`. (PR 389082)

AIM Upgrade

- A progress indicator now appears when the `jboss` service is started when AIM is upgraded to release 1.2R2.1. (PR 39082)

Juniper Message Bundles

- When the partner controller creates a case on behalf of an end customer, the file upload process now uses the credentials of the partner controller so that JSS will not reject the JMBs. Previously AIM used the end-customer credentials, which are only stored in the AIM database, not by JSS. (PR 394458)
- AIM no longer invalidates JMBs with long file transfers. (PR 398009)

AIM Incident and Intelligence Managers

- Performance issues have been resolved when accessing Intelligence and Incident Managers. (PR 313249)

AIM Juniper Data Collector

- The JDC ScreenOS device type NS-5200 M2 is now supported. (PR 398899)
- The JDC log `AIMJDC.log` file has been enhanced to include more relevant information. (PR 402797)
- The JDC Test Connection button now provides the credentials for verification of the device connection. (PR 302007)

- ScreenOS Device information now contains all valid information when exporting to a file. (PR 311976)
- AIM now supports J6350 Services Routers that are Network Equipment Building Systems (NEBS) compliant. (PR 388311)

AIM Reaction Policies

- The case ID is now included in the JTAC Case Created e-mail alert sent by AIM Reaction Policies to the AIM user. (PR 392811)

Outstanding Issues

The following issues are outstanding in the AIS 1.2R2 application release:

- When installing or uninstalling the AIM 1.2R2 application on a server running Red Hat Linux version 5, the following warning message is appears: `awk: cmd. line:6: warning: escape sequence '\.'` treated as plain ```. Ignored this warning message, because it does not mean any issues with installation. (PR 310505)
- ScreenOS device information has been updated to contain all valid information when exporting to CSV or Microsoft Excel file format. Each export format shows the relevant information with all fields populated correctly. (PR 311975)
- You can not disassociate or delete a device from a Device Group once it has been added through the discovery of a JMB. (PR 262620)
- Commit times can increase when AI-Scripts are installed on a JUNOS device. (PR 294131)

Installing and Configuring AIS Elements

This section describes how to install and configure the AIS elements: JUNOScope software (optional), AI-Scripts, AIM, and JSS.

- AIS Quick Setup Checklist on page 13
- Installing the Advanced Insight Manager Application on page 13
- Information Requested During Installation on page 15
- DNS Access on page 16
- Install ID and Licensing on page 17
- Downloading the AIM Application on page 17
- Running the AIM Application Installer on page 17
- Configuring the ai_manager.rc file on page 18
- Starting and Stopping AIM Services on page 19
- Using AIM Application Services Scripts on page 20
- Connecting to the AIM Application and Logging In on page 22
- Changing the AIM Administrator Password on page 23
- AIM Application Installation Directory Structure on page 23

AIS Quick Setup Checklist

Follow these key steps to setup the AIS components. For more detailed information about how to set up the AIS components, see the “AIS Quick Setup Checklist” chapter in the *AIS User Guide*.

1. Download all AIS Components from the Juniper Networks Software Download site.
 - (Optional) JUNOScope Software, release notes, and the user guide at <https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/>.
 - Advanced Insight Scripts (AI-Scripts) and release notes at <https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/>.
 - Advanced Insight Manager (AIM) and the *Advanced Insight Solutions User Guide* at <https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/>.
2. (Optional) Install and set up the JUNOScope 9.0 or later software. For more information, see the *JUNOScope Release Notes* and the *JUNOScope Software User Guide* at <http://www.juniper.net/techpubs/software/management/junoscope>.
3. (Optional) Manually install the AI-Scripts on Juniper Networks supported devices. You can install AI-Scripts manually now or install them automatically later using AIM and JUNOScope script management when you set up the AIM software. For more information, see the *AI-Scripts Release Notes* or the *AIS User Guide*.
4. Install and connect to the AIM software. For more information, see “Installing the Advanced Insight Manager Application” on page 13 or the *AIS User Guide*.
5. Generate the AIS license key file and activate it. See the “Activating and Loading” section in the *AIS User Guide*.
6. Set up AIM and confirm AIS connectivity.
 - Connect to the AIM server in the archive location directory and look for JMB files (for example, `ls -l/opt/archives*.xml`). XML files verify successful connectivity.
 - In AIM Intelligence Manager, look for information JMBs by choosing the Advanced Insight Solutions > Intelligence Manager > Information JMBs tab. Click View Detail to see device configuration details.

See the “Setting Up Advanced Insight Manager” section of the *AIS User Guide*.

Installing the Advanced Insight Manager Application

This section describes how to install the Advanced Insight Manager application. It contains the following information:

- AIM System Requirements on page 14

AIM System Requirements

You can install the AIM on a Sun Solaris or Red Hat Enterprise Edition Linux server. Ensure that the server on which you install the AIM application meets the minimum system requirements. For a Sun Solaris server, see Table 5 on page 14. For a Linux server, see Table 6 on page 14.

- Sun Solaris Server System Minimum Requirements on page 14
- Red Hat Linux Server System Minimum Requirements on page 14
- AIM Application Client Workstation Requirements on page 15
- AIM Administrator Requirements on page 15

Sun Solaris Server System Minimum Requirements

Before you install the AIM application on a Sun Solaris server, ensure that the server meets the minimum system requirements shown in Table 5 on page 14.

Table 5: AIM Minimum Sun Solaris Server System Requirements

System	Minimum Requirement
Operating system	Solaris 9.0 and above. NOTE: GNU Privacy Guard (GPG) is required to be installed on Solaris.
Processor	UltraSPARC III or equivalent
Speed	1.3 GHz or faster
RAM	1 gigabyte (GB)
Free disk space	Follow these guidelines for disk space allocation: <ul style="list-style-type: none"> ■ 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) ■ 100-1000 devices under management: Allocate at least 50 GB for 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 Technical Service representative

Red Hat Linux Server System Minimum Requirements

Before you install the AIM application software on a Linux server, ensure that the server meets the minimum system requirements shown in Table 6 on page 14.

Table 6: AIM Minimum Linux Server System Requirements

System	Minimum Requirement
---------------	----------------------------

Table 6: AIM Minimum Linux Server System Requirements (continued)

Hardware	Red Hat certified hardware platforms
Operating system	Red Hat Enterprise Linux ES version 3, 4, and 5
Processor	Pentium 4 processor
Speed	2.8 GHz or faster
RAM	1 GB
Free disk space	<p>Follow these guidelines for disk space allocation:</p> <ul style="list-style-type: none"> ■ 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) ■ 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 Technical Service representative

AIM Application Client Workstation Requirements

Ensure that the client workstation from which you connect to the AIM application is running either one of the following Web browsers: Microsoft Internet Explorer 6 or Mozilla Firefox 2.0.0.16 or later.

AIM Administrator Requirements

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.

Information Requested During Installation

The AIM application installer prompts you for the following information:

- AIM Software License Agreement—You must accept the agreement.
- Install directory—The directory in which to install the AIM application.
- JBoss server port numbers—The ports (http and https) on which the JBoss server listens for requests to the AIM application. Enter a port number from 1 to 65535. Port number **8080** is the default http port, and port **8443** is the default https port. This is the port number that you must provide when connecting to the AIM application from a Web browser, see “Connecting to the AIM Application and Logging In” on page 22.
- Database JNDI port number—The Java Naming and Directory Interface (JNDI) port on which the database listens for requests from the AIM Service. Enter a port number from 1 to 65535. If the port is in use, a warning is displayed and you must enter a new port number.

- X.509 Certificate settings—Generates an X.509 Certificate required for HTTPS. The following information is requested:
 - Keystore Password—The password should be 6 characters or longer.
 - AIM Server Name—The server on which AIM is being installed.
 - AIM Server Organizational Unit—The organizational unit to which the AIM installation belongs. This information is optional.
 - AIM Installation Organization—The organization to which the AIM installation belongs.
 - AIM Server City or Locality—The city or locality in which the AIM server is located. This information is optional.
 - AIM Server State or Province— The state or province in which the AIM server is located.
 - AIM Server Two-Letter Country Code— The two-letter country code in which the AIM server is located.
- E-mail settings (SMTP Protocol and E-Mail Address)—The settings required for having e-mails sent from an AIM Reaction Policy when you select the Send Email to option.
- AIM Service RMI port number—The port on which the AIM Service will listen for requests from the AIM application. Enter a port number from 1 to 65535. Port number **1122** is the default.
- Username and group for the installation directory—A non-root username and group of the user that owns the AIM application installation, for example, `aimuser` and `aimgroup`. Username and group are only requested if the user installing the application is the root user. The username and group of the user must exist on the workstation.
- MySQL Port Number—Port number for the locally installed MySQL database. You can enter a port number from 1 to 65535. Port number **3306** is the default.



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

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

DNS Access

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

homeBaseURL=https://207.17.137.247

Install ID and Licensing

The AIM installer generates an Install ID for licensing. The Install ID is displayed at the end of AIM installation on the Installation Complete screen. It can also be viewed on the License Management page under Settings (through the GUI). This ID is needed when you contact Juniper Networks to obtain a license file. For more information about generating the AIS license key file, see the “Activating the AIS License” section in the *AIS User Guide*

Downloading the AIM Application

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

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

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

2. Log in to the Juniper Networks authentication system using your username and password supplied by a Juniper Networks representative.
3. Download the AIM application to your local host.

There are two AIM install packages:

- (Sun Solaris AIM installer) SOL_AIM1.2R2.tgz
 - (Red Hat AIM Installer) RH_AIM1.2R2.tgz
4. Extract the AIM install.bin installer files from the appropriate.

For Sun Solaris, enter the following commands:

- a. **gunzip SOL_AIM1.2R2.tgz**

This command extracts the SOL_AIM1.2R2.tar file.

- b. **tar -xvf SOL_AIM1.2R2.tar**

This command extracts the install.bin file.

For Red Hat Linux, enter the following command:

tar -xvzf RH_AIM1.2R2.tgz

Running the AIM Application Installer

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

- Running the Graphical Installer on page 18
- Running the Console Installer on page 18

Running the Graphical Installer

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

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

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

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

2. Follow the onscreen instructions.

Running the Console Installer

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

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

```
user@host> installer location/install.bin -i console
```

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

2. Follow the console instructions.

Configuring the `ai_manager.rc` file

You are prompted for the e-mail settings (SMTP protocol and e-mail address) during the AIM installation. This setting is necessary to receive e-mail from the AIM application when you create a Reaction Policy. If you left the fields blank during the AIM installation process, you can add the values later by modifying the `ai_manager.rc` file and adding the `smtp_protocol_value` and `sender` values as required. The `ai_manager.rc` file is located in the `/opt/aim` directory. For the changes to take effect, you must restart the `aimService`. See “Starting and Stopping AIM Services” on page 19.

The contents of the `ai_manager.rc` file is as follows. Bold text indicates the values to enter.

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

```
smtp_protocol_value=smtp.juniper.net sender=AIM@juniper.net
```

Starting and Stopping AIM Services



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

You must start the following AIM application services before you can use a Web browser to connect and log in to the AIM application. You can start all services at once (see “Starting All Services Simultaneously” on page 19) or start them individually (see “Starting Each Service Individually” on page 19).

- Starting All Services Simultaneously on page 19
- Starting Each Service Individually on page 19
- Stopping All Services Simultaneously on page 20
- Stopping Each Service Individually on page 20

Starting All Services Simultaneously

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

Starting Each Service Individually

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

If you start the services individually, start them in the following order:

1. `mysql`—Open source database that stores information required for AIM application operation. For more detail about the command options for starting `mysql`, see “`mysql`” on page 20.
2. `jboss`—The underlying AIM application server. For more detail about the command options for starting `jboss`, see “`jboss`” on page 21.
3. `aimService`—Background service that communicates with Juniper Support Systems. For more detail about the command options for starting `aimService`, see “`aimService`” on page 21.
4. `aimJDCService`—Background service that starts the Juniper Data Collector. For more detail about the command options for starting `aimJDCService`, see the *AIM User Guide*.

To start each service individually, use the following commands in order:

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



NOTE: The jboss Service and database must be running before you start the aimService.

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

Stopping All Services Simultaneously

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

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

Stopping Each Service Individually

To stop each service individually, use the following commands:

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

Using AIM Application Services Scripts

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

- mysql on page 20
- jboss on page 21
- aimService on page 21
- allServices on page 21
- aimJDCService on page 22

mysql

The section provides a reference for the `mysql` command options. MySQL is an open source database used to store information for AIM application operation. The MySQL server must be running before you start the aimService.

`mysql {[start|stop|check]}`

- `start`—Starts the MySQL Server as a background process.
- `stop`—Stops the MySQL Server.
- `check`—States whether the MySQL Server is running.

jboss

This section provides a reference for the **jboss** command options. **jboss** is the underlying server for the AIM application. The **jboss** Service must be running before you start the **aimService**.

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

- **start**—Starts the **jboss** Service as a background process.
- **start console**—Starts the **jboss** Service in a new window.
- **stop**—Stops the **jboss** Service.
- **restart**—Stops the **jboss** Service and starts it again.
- **restart console**—Stops the **jboss** Service and starts it again in a new console window.
- **check**—States whether the **jboss** Service is currently running.
- **help**—Displays a help message.

aimService

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

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

- **start**—Starts the AIM application service as a background process.
- **start console**—Starts the AIM application service in a new window.
- **stop**—Stops the AIM application service.
- **restart**—Stops the AIM application service and starts it again.
- **restart console**—Stops the AIM application service and starts it again in a new console window.
- **check**—States whether the AIM application service is running.
- **help**—Displays a help message.

allServices

This section provides a reference for the **allServices** command options. The **allServices** script starts all services, one at a time, in the required sequence.

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

- **start**—Starts **mySQL**, **jboss** Service, and the AIM application service as background processes.
- **start console**—Starts **mySQL** in the background, then starts the **jboss** Service and the AIM application service in new windows.

- **stop**—Stops mySQL, jboss Service, and the AIM application service.
- **restart**—Stops mySQL, jboss Service, and the AIM application service and starts them again.
- **restart console**—Stops mySQL, jboss Service, and AIM application service, then starts mySQL in the background, and jboss and aimService in new windows.
- **check**—States whether mySQL, jboss Service, and AIM application services (on this workstation) are currently running.
- **help**—Displays a help message.

aimJDCService

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

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

- **start**—Starts the AIM JDC Service as a background process.
- **start**—Starts the AIM JDC Service as a background process.
- **stop**—Stops the AIM Service.
- **restart**—Stops the AIM JDC Service if it's running, and starts it again.
- **restart console**—Stops the AIM JDC Service currently running and starts it again in a new console window.
- **check**—States whether the AIM JDC Service is currently running.
- **help**—Displays a message.

Connecting to the AIM Application and Logging In

You can connect to the AIM application from a UNIX or PC client workstation running a supported Web browser. See “AIM System Requirements” on page 14.

This section includes the following information:

- Connecting to the AIM Application on page 22
- Logging In to the AIM Application on page 23

Connecting to the AIM Application

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

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

`http://installmachine:jbossport/AIManagerClient`

Replace *installmachine* with the name or IP address of the server on which the AIM application is installed, and *jbossport* with the port on which the AIM

application Web server (jboss) listens for HTTP requests. The default port number is 8080. For example:

```
http:// myunixserver:8080/AIManagerClient
```

or

```
http:// 123.123.123.123:8080/AIManagerClient
```

The Advanced Insight Manager Login dialog box appears.

Logging In to the AIM Application

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

1. In the Login page Username text box, type **admin**.
2. In the Password text box, type **aimadmin**.

Click Log In. The My AIM Home page appears.

Changing the AIM Administrator Password

To change the password to a more secure one, follow these steps:

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

AIM Application Installation Directory Structure

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

```
INSTALL_DIR (Default - /opt/aim)
|-aim
|-ai_manager.rc (file used for configuring e-mail services)
|-LICENSE - text file containing the AIM licensing information
|-AIM_Uninstaller (directory containing the uninstaller)
|-bin (directory used for installed utilities and scripts)
|-data (directory used for logs, actual database files, database
configuration sql scripts, etc.)
|-distfiles (directory containing the raw distributions of jboss
and mysql distributions)
|-jboss (directory used for JBoss installation)
|-jre (directory used for the JRE)
```

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

Uninstalling the AIM Application

You must stop all AIM services before you can uninstall the AIM application. The AIM uninstaller is located in the *installation directory*/AIM_Uninstallerdirectory.

To uninstall the AIM application, follow these steps:

1. Stop all AIS services.

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

Shutting down the AIM Service

The AIM Service is not running.

Shutting down the JBoss Service

The JBoss Service is not running.

2. Uninstall AIM using the following command:

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

Upgrading from AIM 1.0 to AIM 1.2R2

Upgrading from AIM 1.0 to 1.2R2 is not supported. You must uninstall AIM 1.0 and then install AIM 1.2R2.

Follow these steps:

1. Stop and uninstall AIM 1.0. See “Uninstalling the AIM Application” on page 24.
2. Install AIM 1.2R2. See “Installing the Advanced Insight Manager Application” on page 13.

Automatically Upgrading from AIM 1.1 to AIM 1.2R2

The AIM 1.2R2 installer automatically detects whether AIM 1.1 is installed, then asks the AIS admin whether to upgrade it. If the admin wants to upgrade, AIM 1.2 stops AIM 1.1, backs it up, then upgrades it. AIM 1.2 does not automatically upgrade AIM 1.0.

List of Technical Publications

Table 7 on page 25 lists the software and hardware guides and release notes for Juniper Networks , M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 8 on page 29 lists the books included in the *Network Operations Guide* series. Table 9 on page 30 lists the manuals and release notes supporting JUNOS software with enhanced services. All documents are available at <http://www.juniper.net/techpubs/>.

Table 10 on page 31 lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at <http://www.juniper.net/books>.

Table 7: Technical Documentation for Supported Routing Platforms

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

Table 7: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>MX-series Layer 2 Configuration Guide</i>	Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the <i>JUNOS Routing Protocols Configuration Guide</i> .
<i>MX-series Layer 2 Solutions Guide</i>	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Protected System Domain</i>	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing instances, and unicast routing protocols.
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
<i>Software Installation and Upgrade Guide</i>	Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Subscriber Access</i>	Provides an overview of the subscriber access features of the JUNOS software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods.

Table 7: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>System Basics</i>	Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPsec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.

Table 7: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
<i>PIC Guide</i>	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Advanced Insight Solutions (AIS) Documentation	
<i>Advanced Insight Solutions Guide</i>	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.
J-series Routing Platform Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series routing platforms. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the <i>Getting Started Guide</i> for your router model.
<i>Basic LAN and WAN Access Configuration Guide</i>	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
<i>Advanced WAN Access Configuration Guide</i>	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPsec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
<i>Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Release Notes	

Table 7: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Release Notes</i>	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
<i>AIS Release Notes</i>	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
<i>AIS AI-Scripts Release Notes</i>	Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 8: JUNOS Software Network Operations Guides

Book	Description
<i>Baseline</i>	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
<i>Interfaces</i>	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
<i>MPLS</i>	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
<i>MPLS Log Reference</i>	Describes MPLS status and error messages that appear in the output of the <code>show mpls lsp extensive</code> command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.

Table 8: JUNOS Software Network Operations Guides (continued)

Book	Description
<i>MPLS Fast Reroute</i>	Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing.
<i>Hardware</i>	Describes tasks for monitoring M-series and T-series routing platforms.

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

Table 9: JUNOS Software with Enhanced Services Documentation

Book	Description
All Platforms	
<i>JUNOS Software Interfaces and Routing Configuration Guide</i>	Explains how to configure J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
<i>JUNOS Software Security Configuration Guide</i>	Explains how to configure and manage security services such as stateful firewall policies, IP Security (IPsec) virtual private networks (VPNs), firewall screens, Network Address Translation (NAT), Public Key Cryptography, and Application Layer Gateways (ALGs).
<i>JUNOS Software Administration Guide</i>	Shows how to monitor J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
<i>JUNOS Software CLI Reference</i>	Provides the complete JUNOS software with enhanced services configuration hierarchy and describes the configuration statements and operational mode commands not documented in the standard JUNOS manuals.
J-series Only	
<i>JUNOS Software Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software with enhanced services.
<i>JUNOS Software Quick Start</i>	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.

Table 9: JUNOS Software with Enhanced Services Documentation (continued)

Book	Description
<i>JUNOS Software with Enhanced Services J-series Services Router Hardware Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
<i>JUNOS Software Migration Guide</i>	Provides instructions for migrating an SSG device running ScreenOS software or a J-series Services Router running the JUNOS software to JUNOS software with enhanced services.
<i>WXC Integrated Services Module Installation and Configuration Guide</i>	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.
<i>JUNOS Software with Enhanced Services for J-series Services Router Release Notes</i>	Summarizes new features and known problems for a particular release of JUNOS software with enhanced services on J-series Services Routers, including J-Web interface features and problems. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software with enhanced services.

Table 10: Additional Books Available Through <http://www.juniper.net/books>

Book	Description
<i>Interdomain Multicast Routing</i>	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.
<i>JUNOS Cookbook</i>	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
<i>MPLS-Enabled Applications</i>	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.
<i>OSPF and IS-IS: Choosing an IGP for Large-Scale Networks</i>	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks.

Table 10: Additional Books Available Through <http://www.juniper.net/books> (continued)

Book	Description
<i>Routing Policy and Protocols for Multivendor IP Networks</i>	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.
<i>The Complete IS-IS Protocol</i>	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Revision History

15 August 2008—530-026848-01, *Advanced Insight Solutions 1.2 Release Notes*.
Revision 1.

8 October 2008—530-026848-01, *Advanced Insight Solutions 1.2 Release Notes*.
Revision 2.

12 December 2008—530-026848-01, *Advanced Insight Solutions 1.2 Release Notes*.
Revision 3.

Copyright © 2008, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.