

Advanced Insight Solutions 1.1 Release Notes

28 July 2008
Part Number: 530-024288-01
Revision 2

These release notes accompany Release 1.1 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, and EX-series routing platforms (devices).

You can also find these release notes, the *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 1.1 Features	3
New Device Group, Device, Defect Type Filters for Incidents and Intelligence Information	3
New Intelligence Update Received Trigger in Reaction Policies	3
Reaction Policies that Trigger When a Device Group or Organization is Associated	4
New Send Only Configuration Indexes Information JMB Configuration Filter Level	4
New Proactive Case Manager	4
New Statistics Area in Incident Manager	5
New Statistics Area in Intelligence Manager	5
New Inventory Manager	5
Advanced Insight Solutions Overview	5
Installing and Configuring AIS Elements	6
AIS Quick Setup Checklist	7
Installing the Advanced Insight Manager Software	8
AIM System Requirements	8
Information Requested During Installation	9
DNS Access	11

- Install ID and Licensing 11
- Downloading the AIM Application 11
- Running the AIM Application Installer 12
 - Running the Graphical Installer 12
 - Running the Console Installer 12
- Configuring the ai_manager.rc file 12
- Starting and Stopping AIM Services 13
 - Starting AIM Services Sequence Manually 13
 - Starting All Services Simultaneously 13
 - Starting Each Service Individually 14
 - Stopping All Services Simultaneously 14
 - Stopping Each Service Individually 14
- Using AIM Application Services Scripts 14
 - mysql 14
 - jboss 15
 - aimService 15
 - allServices 15
- Connecting to the AIM Application and Logging In 16
 - Connecting to the AIM Application 16
 - Logging In to the AIM Application 17
- Changing the AIM Administrator Password 17
- AIM Application Installation Directory Structure 17
- AIM Log Files 17
 - AIM Install Log 18
 - AIM Messages Exchange Log 18
 - AIM Policy Log 19
 - AIM JMB Log 20
- Uninstalling the AIM Application 21
- Upgrading AIM 21
- List of Technical Publications 21
- Requesting Technical Support 28
- Revision History 29

New Advanced Insight Solutions 1.1 Features

The Advanced Insight Manager has the following new features included in the current release. For more detailed information about Advanced Insight Solutions 1.1 new features, see the *AIS 1.1 User Guide* on the Juniper Networks software download site <http://www.juniper.net/support>.

- New Device Group, Device, Defect Type Filters for Incidents and Intelligence Information on page 3
- New Intelligence Update Received Trigger in Reaction Policies on page 3
- Reaction Policies that Trigger When a Device Group or Organization is Associated on page 4
- New Send Only Configuration Indexes Information JMB Configuration Filter Level on page 4
- New Proactive Case Manager on page 4
- New Statistics Area in Incident Manager on page 5
- New Statistics Area in Intelligence Manager on page 5
- New Inventory Manager on page 5

New Device Group, Device, Defect Type Filters for Incidents and Intelligence Information

In addition to filtering incidents and information JMBs by organization, you can now filter by device group, device, or defect type on a specified option. Filtering by defect type is available for incidents only.

To filter incidents or information JMBs by device group, device, or defect type:

1. In the Incident Manager Incident table or on the Information JMBs tab, select a filter option in Filter By drop-down list box. The available filters include: Nothing, Defect Type, Device, Device Group, and Organization.
2. In the On drop-down list box, select the item on which you want filtered. When Nothing (default) is selected, the associated On drop-down list box is blank. When you select filter by device, device group or organization, the On drop-down list box options include All and the available names. When you select to filter by defect type, the On drop-down list box includes All, Hardware Failure, Resource Exhaustion, and Software Failure.

See the “Using AIM Intelligence Manager” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

New Intelligence Update Received Trigger in Reaction Policies

You can create a reaction policy to trigger when a new intelligence message is received and specify that you only want the action to occur if there are devices that are impacted by the new message. All email messages sent based on a reaction policy with the trigger type New Intelligence Update Received, include a list of devices impacted if the Devices Impacted filter is enabled. The email message includes the same information that displays on the Scan for Impact page.

See the “Creating Reaction Policies” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

Reaction Policies that Trigger When a Device Group or Organization is Associated

You can create a reaction policy that will execute the actions specified if the device group or organization is associated. Reaction policies for specific device groups only support incident-based trigger types. You can create a reaction policy from the Organization Details and Device Group Details pages. The Intelligence Message Received trigger is only available if the policy is initiated from an organization and will execute if the organization is associated with the message received.

See the “Configuring AIM Organizations and Device Groups” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

New Send Only Configuration Indexes Information JMB Configuration Filter Level

A new Send Only Configuration Indexes option is available to set the level of information shared with Juniper Networks in information JMBs to send only the configuration indexes that indicate which technologies are present in the device configuration. The Information JMB Config Filter Level is set on the General Settings page.

See the “Configuring AIM General Settings” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

New Proactive Case Manager

The new AIM Proactive Case Manager allows you to create a proactive case requesting Juniper Support Systems to send information about upgrading device to a specific software release. Proactive cases are displayed by organization, synopsis, platform, software version, issue date, due date, owner, and status. To use Proactive Case Manager, you must have an Intelligence feature license and an AIS Proactive Service (Intelligence-Driven Online Service) subscription.

To view proactive cases, you must have access to the organization associated with the case. From Proactive Case Manager, you can: create a proactive case, clear a flag, delete a proactive case, or filter the proactive cases by organization.

To create a proactive case, follow these steps:

1. Click Proactive Case Manager in the AIM navigation pane. The Proactive Case page appears.
2. Click Submit Proactive Case. The Create Proactive Case page appears. Add the necessary case information, including a problem description.
3. Click Next Step. Create Proactive Case – Specify Platforms page appears.
4. Select the platforms that you want.
5. Click Finish. This action saves the proactive case in the AIM database and sends the case to JSS for a case ID.

See the “Using Proactive Case Manager” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

New Statistics Area in Incident Manager

A statistics area has been added to the top of the Incident Manager Incidents table to summarize key data displayed at a glance. Statistics change based on the filter performed on the table data. In Incident Manager, you see the total number of incidents and the number of new incidents since you last logged in, incidents submitted to JSS, the total number of priority level 1 to 4 incidents and the number of priority incidents since you last logged in, the number of devices represented by the total incidents, and a list of the top 10 most incident-generating devices.

See the “Using AIM Incident Manager” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

New Statistics Area in Intelligence Manager

A statistics area has been added to the top of the Intelligence Manager Intelligence Updates tab to summarize key data displayed at a glance. Statistics change based on the filter performed on the table data. On the Intelligence Updates tab, you see the total number of total number of messages and number of new messages received since you last logged in, the total number of alert messages and the number of new alert messages received since you last logged in, and the total number of new information messages received since you last logged in.

See the “Using AIM Intelligence Manager” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

New Inventory Manager

A new AIM Inventory Manager lists all of the devices to which a user has access based on the user’s user group and the device group association to those user groups. To display Inventory Manager, click Inventory Manager in the navigation area. Devices are listed by organization/device group, device name, device platform, serial number, and active software version. Filter inventory data by device group or organization. Device detail information is displayed by clicking the device name in the table. From Inventory Manager, you can export data to a file or in XML format.

See the “Using AIM Inventory Manager” chapter in the *Advanced Insight Solutions 1.1 User Guide*.

Advanced Insight Solutions Overview

Advanced Insight Solutions is available when you order the top 3 levels of Juniper Networks J-Care Technical Services to support Juniper Networks devices running on your network. See Table 1 on page 6.

Table 1: 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)

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.

AIS consists of three major elements:

- AI-Scripts that 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) that 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) that resolves 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 Advanced Insight Solutions User Guide.

Installing and Configuring AIS Elements

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

- AIS Quick Setup Checklist on page 7
- Installing the Advanced Insight Manager Software on page 8
- Information Requested During Installation on page 9
- DNS Access on page 11
- Install ID and Licensing on page 11
- Downloading the AIM Application on page 11
- Running the AIM Application Installer on page 12
- Configuring the ai_manager.rc file on page 12

- Starting and Stopping AIM Services on page 13
- Using AIM Application Services Scripts on page 14
- Connecting to the AIM Application and Logging In on page 16
- Changing the AIM Administrator Password on page 17
- AIM Application Installation Directory Structure on page 17

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. Manually install the AI-Scripts on Juniper Networks supported devices. You can install AI-Scripts manually at this point or you can 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 Software” on page 8 or the *Advanced Insight Solutions User Guide*.
5. Generate the AIS license key file and activate it. See the “Activating and Loading” section in the *Advanced Insight Solutions User Guide*.
6. Set up AIM and confirm AIS connectivity.
 - Connect to the AIM server in the archive location directory (for example, `ls -l/opt/archivesfor *.xml JMB` files. These files verify successful connectivity.
 - In AIM Intelligence Manager, look for information JMBs by choosing the Advanced Insight Solutions > Intelligence Manager > Information JMBs tab. Click View Detail to see device configuration details.

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

Installing the Advanced Insight Manager Software

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

- AIM System Requirements on page 8

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 2 on page 8. For a Linux server, see Table 3 on page 9.

- Sun Solaris Server System Minimum Requirements on page 8
- Red Hat Linux Server System Minimum Requirements on page 9
- AIM Application Client Workstation Requirements on page 9
- AIM Administrator Requirements on page 9

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 2 on page 8Table 1.

Table 2: 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 archive location and at least 20 GB for AIM application (at least 40 GB if archive location is a local drive on the AIM server) ■ Between 100-1000 devices under management: Allocate at least 50 GB for archive location and at least 50 GB for AIM application (at least 100 GB if archive location is a local drive on the AIM server) ■ More than 1000 devices under management: Contact your Juniper Networks J-Care Technical Service representative

Red Hat Linux Server System Minimum Requirements

Before you install the AIM application software on a Linux server, ensure that the server meets the minimum system requirements shown in Table 3 on page 9.

Table 3: AIM Minimum Linux Server System Requirements

System	Minimum Requirement
Hardware	Red Hat certified hardware platforms
Operating system	Red Hat Enterprise Linux ES version 3 and 4
Processor	Pentium 4 processor
Speed	2.8 GHz or faster
RAM	1 GB
Free disk space	<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 archive location and at least 20 GB for AIM application (at least 40 GB if archive location is a local drive on the AIM server) ■ Between 100-1000 devices under management: Allocate at least 50 GB for archive location and at least 50 GB for AIM application (at least 100 GB if archive location is a local drive on the AIM server) ■ More than 1000 devices under management: Contact your Juniper Networks J-Care Technical Service representative

AIM Application Client Workstation Requirements

Ensure that the client workstation from which you connect to the AIM application is running either 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 or regular user. A non-root user can change the default AIM install directory to any other directory than the default /opt/aim install 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 16.

- Database JNDI port number—The Java Naming and Directory Interface (JNDI) port on which the database listens for requests from the AIM Service. The port is checked for current use. If the port is in use, a warning is displayed and you must enter a new port number. Enter a port number from 1 to 65535.
- 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 name is defaulted to 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 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, for example `aimuser` and `aimgroup` of the user that owns the AIM application installation. 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 up and 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 contacting 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 *Advanced Insight Solutions 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_AIM1.0R1.tgz
 - (Red Hat AIM Installer) RH_AIM1.0R1.tgz
4. Extract the AIM install.bininstaller files from the appropriate AIM package following one of these procedures:
 - For Sun Solaris, follow these steps:
 - a. **gunzip SOL_AIM1.1R1.tgz** This command extracts the results in SOL_AIM1.1R1.tar file.
 - b. **tar -xvf SOL_AIM1.1R1.tar** (This command extracts the install.bin file.
 - For Red Hat Linux, do the following:

```
tar -xvzf RH_AIM1.0R1.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 12
- Running the Console Installer on page 12

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

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

You are prompted for the E-mail settings (SMTP Protocol and E-Mail Address) during the AIM installation. This setting is necessary to receive e-mail from the AIM application when you set a Reaction Policy and select the Send Email to action. If you left the fields blank during the AIM installation process, you can add the values by modifying the ai_manager.rc file and adding the smtp_protocol_value and sender values as required. For the changes to take effect, you must restart the aimService. See “Starting and Stopping AIM Services” on page 13.

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 13) or start them individually (see “Starting Each Service Individually” on page 14).

- Starting AIM Services Sequence Manually on page 13
- Starting All Services Simultaneously on page 13
- Starting Each Service Individually on page 14
- Stopping All Services Simultaneously on page 14
- Stopping Each Service Individually on page 14

Starting AIM Services Sequence Manually

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 14.
2. **jboss**—The underlying AIM application server. For more detail about the command options for starting **jboss**, see “jboss” on page 15.
3. **aimService**—Background service that communicates with Juniper Support Systems. For more detail about the command options for starting **aimService**, see “aimService” on page 15.

Starting All Services Simultaneously

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

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

Starting Each Service Individually

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

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



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

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

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/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 14
- jboss on page 15
- aimService on page 15
- allServices on page 15

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 is required to be running prior to starting the aimService.

Command Usage

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

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

jboss

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

Command Usage

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

- start—Starts the jboss Service as a background process.
- start console—Starts the jboss Service in a new window.
- stop—Stops the jboss Service.
- restart—Stops the jboss Service, and starts it again.
- restart console—Stops the jboss Service, and starts it again in a new console window.
- check—States whether or not 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.

Command Usage

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

- start—Starts the AIM application service as a background process.
- start console—Starts the AIM application service in a new window.
- stop—Stops the AIM application service.
- restart—Stops the AIM application service if it's running, and starts it again.
- restart console—Stops the AIM application service currently running and starts it again in a new console window.
- check—States whether 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 sequence required for the successful use of the AIM application.

Command Usage

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

- **start**—Starts mySQL, Jboss Service, and the AIM application service as background processes.
- **start console**—Starts mysql in the background, then starts the JBoss Service and the AIM application service in new windows.
- **stop**—Stops mysql, JBoss Service, and the AIM application service.
- **restart**—Stops mysql, JBoss Service, and the AIM application service if they're running, and starts them again.
- **restart console**—Stops mysql, JBoss Service, and AIM application service if they're running, then starts mysql in the background, and JBoss and aimService in new windows.
- **check**—States whether or not mysql, JBoss Service, and AIM application services (on this workstation) are currently running.
- **help**—Displays a help 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 8.

This section includes the following information:

- Connecting to the AIM Application on page 16
- Logging In to the AIM Application on page 17

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

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)
|-rc.d (directory used for startup shell scripts)
```

AIM Log Files

- AIM Install Log on page 18
- AIM Messages Exchange Log on page 18

- AIM Policy Log on page 19
- AIM JMB Log on page 20

AIM Install Log

Filename

Advanced_Insight_Manager_installLog.log

Description

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

Sample

```

Install Begin: Thu Apr 10 19:12:34 PDT 2008
Install End:   Thu Apr 10 19:15:24 PDT 2008
Created with Zero G's InstallAnywhere 7.1 Enterprise Build 2788
Summary
-----
Installation: Successful.
493 SUCCESSES
0 WARNINGS
0 NONFATAL ERRORS
0 FATAL ERRORS
Action Notes: None.
Install Log Detail:
Install Action: InstallAnywhere Variable Status: SUCCESSFUL
Install Action: InstallAnywhere Variable Status: SUCCESSFUL
Install Action: InstallAnywhere Variable Status: SUCCESSFUL
...
Install File: /opt/aim/data/config/Key1.public.asc Status: SUCCESSFUL
Execute Script/Batch file: Install Public Key Status: SUCCESSFUL
Execute Command: su - $USERNAME$ -c "$GPG$ --import
$USER_INSTALL_DIR$/data/$config$/Key1.public.asc"
Status: SUCCESSFUL
Install Directory: /opt/aim/data/db/ Status: SUCCESSFUL
Install File: /opt/aim/data/my.cnf Status: SUCCESSFUL
    
```

AIM Messages Exchange Log

Filename

AIManagerMSG.log

Description

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

- Create Case Request
- Update Intelligence Info
- Validate Login
- Retrieval of Home Base Status

- When Settings on the General Settings Page have been saved, causing updates to the AIM Service
- How many Informational and Alert Messages are retrieved from JSS
- When a Case is created in Clarify
- When a Case has been updated in Clarify

Sample

```

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

```

AIM Policy Log

Filename

AIManagerPOLICY.log

Description

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

Sample

```

2008-06-04 19:08:55,878 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:08:55,884 DEBUG [PolicyEngine] Policy ID :8
2008-06-04 19:09:55,978 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:09:55,986 DEBUG [PolicyEngine] Policy ID :8
2008-06-04 19:10:55,841 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:10:55,846 DEBUG [PolicyEngine] Policy ID :8
2008-06-04 19:11:55,978 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:11:55,983 DEBUG [PolicyEngine] Policy ID :8
2008-06-04 19:12:55,997 DEBUG [PolicyEngine] Policy ID found :[8]
2008-06-04 19:12:56,005 DEBUG [PolicyEngine] Policy ID :8
    
```

AIM JMB Log

Filename

AIManagerJMB.log

Description

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

Sample

```

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

Uninstalling the AIM Application

You must first 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 AIM

Upgrading from AIM 1.0 to 1.1 is not supported. Therefore, you must reinstall AIM.

To upgrade the AIM application, follow these steps:

1. Stop and uninstall AIM. See “Uninstalling the AIM Application” on page 21
2. Install AIM. See “Installing the Advanced Insight Manager Software” on page 8.

List of Technical Publications

Table 4 on page 21 lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 5 on page 26 lists the books included in the *Network Operations Guide* series. Table 6 on page 26 lists the manuals and release notes supporting JUNOS software with enhanced services. All documents are available at <http://www.juniper.net/techpubs/>.

Table 7 on page 28 lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at <http://www.juniper.net/books>.

Table 4: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	

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

Book	Description
<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.
<i>MX-series 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.

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

Book	Description
<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, 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.
<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.

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

Book	Description
<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.
<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.

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

Book	Description
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	
<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.

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

Book	Description
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 5: 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.
<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 or SRX-series services gateway 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 6: 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 and SRX-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.

Table 6: JUNOS Software with Enhanced Services Documentation (continued)

Book	Description
<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 and SRX-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 with Enhanced Services 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 with Enhanced Services Quick Start</i>	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
<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 with Enhanced Services 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 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.
SRX-series Only	

Table 6: JUNOS Software with Enhanced Services Documentation (continued)

Book	Description
<i>JUNOS Software for SRX-series Services Gateway Release Notes</i>	Summarizes new features and known problems for a particular release of JUNOS software with enhanced services on SRX-series services gateways, 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 7: 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.
<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 Manager: <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 Manager 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).

Revision History

29 April 2008—530-024288-01, *Advanced Insight Solutions 1.1 Release Notes*. Revision 1.

28 July 2008—530-024288-01, *Advanced Insight Solutions 1.1 Release Notes*. Revision 2.

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

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe 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.