

# Advanced Insight Solutions 1.0 Release Notes

Release 1.0R1  
14 February 2008  
Part No. 530-022699-01  
Revision 1

These release notes accompany Release 1.0R1 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, and T-series routing platforms devices.

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

<b>Contents</b>	Release 1.0 Features .....	2
	AIS Major Elements .....	2
	AIS Service Subscriptions .....	4
	AIM Customer/Partner Engagement Models: .....	4
	JUNOScope 9.0 Script Management .....	5
	(Optional) Installing the JUNOScope Software .....	5
	Installing Advanced Insight Scripts (AI-Scripts) .....	5
	Installing the Advanced Insight Manager Software .....	5
	AIM System Requirements .....	6
	Sun Solaris Server System Minimum Requirements .....	6
	Red Hat Linux Server System Minimum Requirements .....	6
	AIM application Client Workstation Requirements .....	6
	Information Requested During Installation .....	6
	DNS Access .....	7
	Install ID and Licensing .....	7
	Downloading the AIM Application .....	8
	Running the AIM Application Installer .....	8
	Running the Graphical Installer .....	8
	Running the Console Installer .....	8
	Configuring the ai_manager.rc file .....	9
	Starting and Stopping AIM Application Services .....	9
	Starting All Services Simultaneously .....	10
	Starting Each Service Individually .....	10
	Stopping All Services Simultaneously .....	10
	Stopping Each Service Individually .....	10
	Using AIM Application Services Scripts .....	10
	mysql .....	11
	jboss .....	11
	aimService .....	11
	allservices .....	12
	Connecting to the AIM Application and Logging In .....	12
	Connecting to the AIM Application .....	12
	Logging In to the AIM Application .....	13
	Changing the AIM Administrator Password .....	13

Uninstalling the AIM Application .....	13
AIM Application Installation Directory Structure .....	14
Related Juniper Networks Documentation .....	14
How To Request Support .....	19
Revision History .....	19

## Release 1.0 Features

Advanced Insight Solutions (AIS), a Juniper Networks product that provides reactive and proactive support for J-series, M-series, MX-series, and T-series routing platforms (devices), has the following features:

- AIS Major Elements on page 2
- AIS Service Subscriptions on page 4
- AIM Customer/Partner Engagement Models: on page 4
- JUNOScope 9.0 Script Management on page 5

### ***AIS Major Elements***

AIS consists of three major elements:

- AI-Scripts on page 2
- The Advanced Insight Manager (AIM) Application on page 3
- Juniper Support Systems (JSS) on page 4

### ***AI-Scripts***

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

- React to specific incident events that occur on devices and provide relevant information about the problems for analysis
- Periodically collect data on events that can be used to predict and prevent risks in the future.
- Package all incident and intelligence event data into a format, called a Juniper Message Bundle (JMB), and send it to a remote archive location so that it can be collected and displayed by Advanced Insight Manager (AIM).

For more information about AI-Scripts, see the *AIS User Guide* and *AI-Scripts Release Notes*.

## The Advanced Insight Manager (AIM) Application

The Advanced Insight Manager (AIM) application provides a gateway between JUNOS device archive locations and JSS to reactively manage incidents and proactively manage intelligence information. AIM provides the following features:

- Installs on a Sun Solaris or Red Hat Enterprise Linux server. Connect to it from a Web browser, such as Microsoft Internet Explorer 6 or Mozilla Firefox.
- Operates in fully functional, demo mode for 60 days with a 5-device management capacity. The user should obtain a license file from Juniper Networks, and load the license file into AIM for activation of the licensed features, such as:
  - Base Product—Required to use AIM beyond a 60-day demo period. Allows operation of Incident Manager and Intelligence Manager and the creation of one Organization.
  - Capacity—Required for controlling the number of devices from each class that AIM will accept incident and intelligence messages from in the archive locations being monitored.
  - Feature Licenses—Feature licenses turn on and off different features available in the product. AIM Multi-Site functionality is an example of a feature which requires a license.



**NOTE:** Having a license for AIM does not automatically mean that the customer has a license to subscribe to the AIS Base or AIS Proactive services needed for full functionality of the Advanced Insight Solutions (AIS).

- The Multi-Site Feature allows the user to create and manage more than one Organization within the AIM application. Each organization represents a different Customer Site.
- User privileges control access to AIM features. Access depends on which user group the user belongs and to which device groups the user group is associated. Each user will only be able to view and perform actions on objects associated to the user groups to which they are assigned.
- Send AIM specific SNMP traps to network management systems
- My AIM Home displays incidents, intelligence messages, and reaction policies owned by or flagged to a user that is logged in.
- Incident Manager displays incidents collected from JUNOS devices that place their JMBs in AIM-monitored archives locations. Incidents can be filtered by Organization (if the Multi-Site feature has been purchased).
- Reaction policies can be created to alert users when incidents occur or when a case is updated. Incidents are reported to JSS and a Case Management ID is assigned.
- Intelligence Manager displays intelligence updates from JSS as well as Information JMBs found in monitored archive locations. Intelligence Information can be filtered by Organization (if the Multi-Site feature has been purchased).

### ***Juniper Support Systems (JSS)***

Juniper Support Systems (JSS) resolves incident cases and proactive analysis information from the customer's network, Juniper Networks internal product knowledge, and Juniper Networks knowledge base to provide intelligence updates.

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

- If the customer enrolls in AIS Base Service (Incident-Driven Online Service), incidents can be reported to Juniper Support Systems to open a case to with all relevant information
- If the customer enrolls in AIS Proactive Service (Intelligence-Driven Online Service), data collected periodically from the routers is sent to JSS. The customer determines how often and the amount of proprietary configuration intelligence information to share with JSS.

### ***AIS Service Subscriptions***

To receive full AIS product functionality, the customer must purchase the following annual subscriptions for the following device classes from Juniper Support Services (JSS). The AIM application displays the annual subscriptions purchased for device classes when it connects to JSS.

- AIS Base Service (Incident-Driven Online Service)—Cases are opened directly from the end-user. Case status and case-ID are returned to the end-user from JSS.
- AIS Proactive Service (Intelligence-Driven Online Service)—Proactive information is reported from the end-user. Proactive analysis information is returned the end-user.

### ***Device Classes:***

AIS device capacity licenses are available for the following device classes:

- Class 1—CPE and branch devices, e.g. J-series, M7i, M10i, M20, M120, EX-3200, EX-4200
- Class 2—Edge and Aggregation devices, e.g. M40e, M320, MX-series
- Class 3—Core devices, e.g. T-series and TX

### ***AIM Customer/Partner Engagement Models:***

- Direct—End-user deploys AIS software elements (AI-Scripts and AIM), and enrolls in AIS services.
- Partner-Deployed—Partner deploys AIM software elements to manage multiple end-users. All connections are through authenticated and encrypted protocols. Secure file transfers occur from multiple device archive locations to partner's AIM. HTTPS connection is made from AIM to JSS.

- Partner End-User-Deployed—End-users deploy AIS software elements. AIM is managed by the partner. Partner connects to AIM installed in end-user site through Web client. A firewall hole or tunnel between end-user and AIM is necessary. The decision to contact Juniper to open a case, request a proactive analysis, etc. are managed by the partner. All connections are through authenticated and encrypted protocols.

## ***JUNOScope 9.0 Script Management***

JUNOScope is an element management tool which provides an integration point to AIM for automatically installing AI-Script Bundles on multiple devices. The Devices managed by JUNOScope can be imported into the AIM system for association with AIM Device Groups. If AIM will be installed on the same system as JUNOScope, JUNOScope should be installed first, however the two applications do not need to be installed on the same system. For more information about the JUNOScope software, see the *JUNOScope 9.0 User Guide* and *JUNOScope 9.0 Software Release Notes*.

## **(Optional) Installing the JUNOScope Software**

For more information about installing the JUNOScope 9.0 or above software, see the *JUNOScope Software Release Notes* and the *JUNOScope Software User Guide* at <http://www.juniper.net/techpubs/software/management/junoscope>.

## **Installing Advanced Insight Scripts (AI-Scripts)**

For more information about installing the AI-Scripts, see the *AI-Scripts Release Notes* at <http://www.juniper.net/techpubs/software/management/ais>.

## **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 6
- AIM application Client Workstation Requirements on page 6
- Information Requested During Installation on page 6
- DNS Access on page 7
- Install ID and Licensing on page 7
- Downloading the AIM Application on page 8
- Running the AIM Application Installer on page 8
- Configuring the ai\_manager.rc file on page 9
- Starting and Stopping AIM Application Services on page 9
- Using AIM Application Services Scripts on page 10

## AIM System Requirements

You can install the AIM application on a Sun Solaris or Red Hat Enterprise Edition Linux server. Ensure that the server on which you install the AIM application meets the minimum system requirements. For a Sun Solaris server, see Table 1. For a Linux server, see Table 2.

### *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 1.

**Table 1: AIM Minimum Sun Solaris Server System Requirements**

System	Minimum Requirement
Operating system	Solaris 9.0 and above. <b>NOTE: GNU Privacy Guard (GPG) is required to be installed on Solaris.</b>
Processor	UltraSPARC III or equivalent
Speed	1.3 GHz or faster
RAM	1 gigabyte (GB)
Free disk space	1 GB

### *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 2.

**Table 2: 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	1 GB

## 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.

## 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 12.
- 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.
- E-mail settings (SMTP Protocol and E-Mail Address)—The settings required for having e-mails sent from an AIM Reaction Policy when you select the Send Email to option.
- AIM Service RMI port number—The port on which the AIM Service will listen for requests from the AIM application. Enter a port number from 1 to 65535. Port number 1122 is the default.
- Username and group for the installation directory—A non-root username and group, for example `aimuser` and `aimgroup` of the user that owns the AIM application installation. The username and group of the user must exist on the workstation.
- `mysql` Port Number—Port number for the locally installed `mysql` database. You can enter a port number from 1 to 65535. Port number 3306 is the default.



**Note**

**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 will generate an Install ID for licensing. The Install ID is displayed at the end of AIM installation on the Installation Complete screen. It can also be viewed on the License Management page under Settings (through the GUI). This ID is needed when contacting Juniper Networks to obtain a license file.

## Downloading the AIM Application

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

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

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

There are two AIM installer files:

- (Red Hat AIM Installer) RH\_AIM1.0R1.tgz
- (Sun Solaris AIM installer) SOL\_AIM1.0R1.tgz

2. Log in to the Juniper Networks authentication system using your username and password supplied by a Juniper Networks representative.
3. Download the AIM application to your local host.
4. Extract the `install.bin` installer file from the downloaded `.tgz` file.

## Running the AIM Application Installer

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

### Running the Graphical Installer

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

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

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

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

2. Follow the onscreen instructions.

### Running the Console Installer

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

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

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

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

2. Follow the console instructions.

## Configuring the ai\_manager.rc file

To receive e-mail from 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 Application Services” on page 9.

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 Application Services



**Note**

**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 10) or start them individually (see “Starting Each Service Individually” on page 10). 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 11.
2. **jboss**—The underlying AIM application server. For more detail about the command options for starting jboss, see “jboss” on page 11.
3. **aimService**—Background service that communicates with Juniper Support Systems. For more detail about the command options for starting aimService, see “aimService” on page 11.

## ***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**

**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 (see page 11)
- jboss (see page 11)
- aimService (see page 11)
- allservices page 12)

## **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 this 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 6.

This section includes the following information:

- Connecting to the AIM Application on page 12
- Logging In to the AIM Application on page 13

### ***Connecting to the AIM Application***

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

1. Start a Web browser.

2. Enter the following URL in the Address text box:

**http://<installmachine>:<jbossport>/AIManagerClient**

Replace *installmachine* with the name or IP address of the server on which the AIM application is installed, and *jbossport* with the port on which the AIM application Web server (JBoss) listens for **HTTP** requests. The default port number is 8080. For example:

**http:// myunixserver:8080/AIManagerClient**

or

**http:// 123.123.123.123:8080/AIManagerClient**

The Advanced Insight Manager Login dialog box appears.

## Logging In to the AIM Application

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

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

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:

To change the AIM administrator password, 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.

## Uninstalling the AIM Application

You can uninstall the AIM application by running the uninstaller, located in the *<installation directory>/AIM\_Uninstaller* directory.

To uninstall the AIM application, follow these steps:

- On the UNIX host where you installed the AIM application, use the following command:

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

## 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)
    
```

## Related Juniper Networks Documentation

Table 3 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 4 lists the books included in the Network Operations Guide series.

Table 5 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 3: Technical Documentation for Supported Routing Platforms (Sheet 1 of 5)**

Document	Description
<b>JUNOS Internet Software Configuration Guides</b>	
<i>Access Privilege</i>	Explains how to configure access privileges in user classes by using permission flags and regular expression. 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.

**Table 3: Technical Documentation for Supported Routing Platforms (Sheet 2 of 5)**

<b>Document</b>	<b>Description</b>
<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 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>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, forwarding options, and cflowd.
<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 Internet 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 routing platform.
<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>System Basics</i>	Describes Juniper Networks routing platforms, and provides information about 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.
<b>JUNOS References</b>	
<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 protocols and policies, 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 CoS, IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.

**Table 3: Technical Documentation for Supported Routing Platforms (Sheet 3 of 5)**

Document	Description
<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.
<b>J-Web User Guide</b>	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web GUI to configure, monitor, and manage Juniper Networks routing platforms.
<b>JUNOS API and Scripting Documentation</b>	
<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>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.
<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.
<b>JUNOScope Documentation</b>	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software 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.
<b>J-series Services Router Documentation</b>	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. 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>Migration Guide</i>	Provides instruction for migrating an SSG 300M-series or SSG 500M-series security device running Screen OS software or a J-series router running JUNOS software to JUNOS software with Enhanced Services.
<i>Interfaces and Routing Guide</i>	Explains how to configure the interfaces on J-series Services Routers running MJUNOS Enhanced Services for basic IP routing with standard routing protocols. ISDN backup, digital subscriber line (DSL) connections and class-of-service (CoS) classification for safer, more efficient routing.
<i>Security Configuration Guide</i>	Explains how to configure J-series Services Routers running JUNOS software with Enhanced Services in virtual private networks (VPNs) and multicast networks; configure firewall NAT and ALGs; apply routing techniques such as zones, policies, stateful firewall filters, and IP Security (IPSec) tunnels; and configure screens and firewall authentication.
<i>Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, change routing and secure contexts, and diagnose common problems on J-series routers running JUNOS software and Enhanced Services.
<i>Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IP Security (IPSec) VPNs, firewalls, and routing on J-series routers running JUNOS software and Enhanced Services.

**Table 3: Technical Documentation for Supported Routing Platforms (Sheet 4 of 5)**

<b>Document</b>	<b>Description</b>
<b>Hardware Documentation</b>	
<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 PICs. Each platform has its own PIC guide.
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
<b>JUNOScope Documentation</b>	
<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.
<b>Advanced Insight Solutions (AIS) Documentation</b>	
<i>Advanced Insight Solutions Guide</i>	Describes the Advanced Insight Solutions (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for incident case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.
<b>J-series Routing Platform Documentation</b>	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series routing platforms. The guide explains how to prepare our site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the Getting Started Guide for your router model.
<i>Basic LAN and WAN Access Configuration Guide</i>	Explains how to configure 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.
<b>Release Notes</b>	
<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 the supported PICs, 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>	Summarizes 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-Script 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.

**Table 3: Technical Documentation for Supported Routing Platforms (Sheet 5 of 5)**

Document	Description
<i>J-series Services Router Release Notes</i>	Briefly describe the J-series Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.
<i>JUNOS Enhanced Services Release Notes</i>	Summarizes new features for a particular release, identify known hardware and software problems, provide information that might have been omitted from the manuals, and provide upgrade and downgrade instructions.

**Table 4: JUNOS Internet 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 routers 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.

**Table 5: 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.

Book	Description
<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 multipotology 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.

## How To Request Support

For technical support, open a support case using the Case Manager link at <http://www.juniper.net/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

For documentation issues, fill out the bug report form located at <https://www.juniper.net/techpubs/docbug/docbugreport.html>.

## Revision History

14 February 2008—Advanced Insight Manager, Release 1.0R1

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

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

