

# Advanced Insight Scripts (AI-Scripts) 1.0 Release Notes

**5 April, 2008**  
**Part Number: 530-022700-01**  
**Revision 2**

These release notes accompany Release 1.0 of the Advanced Insight Scripts (AI-Scripts), JUNOS event scripts used to enable Juniper Networks J-series, M-series, MX-series, and T-series routing platforms to:

- React to specific incident events that occur and provide relevant information 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 structured format, such as a Juniper Message Bundle (JMB), and send it to an archive location to be collected and displayed by the Advanced Insight Manager (AIM) application.

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 <http://www.juniper.net/support/>.

## Contents

Release 1.0 Features .....	3
AI-Scripts Operation .....	3
AI-Script Modes .....	3
Events Detected By AI-Scripts .....	3
Current Software Release .....	9
Issues Fixed Since Last Release .....	9
Outstanding Issue .....	9
AI-Scripts Troubleshooting .....	9
Installing an AI-Script Install Bundle Using JUNOScope Software .....	10
Upgrading from AI-Scripts 1.0R1 Install Package to 1.0R2 .....	10

- Installing AI-Scripts ..... 10
  - AI-Script System Requirements ..... 10
  - AI-Script Installation Methods ..... 10
  - Downloading AI-Script Install Packages ..... 11
  - AI-Script Install Package Versioning ..... 11
  - AI-Script Install Locations on Devices ..... 12
  - Automatically Installing AI-Scripts Overview ..... 12
  - Automatically Installing AI-Scripts ..... 12
  - Manually Configuring and Installing AI-Scripts on Devices ..... 13
- AI-Script Installation Commands ..... 15
  - Installing an AI-Script Package ..... 16
  - Deleting an AI-Script Package ..... 16
  - Rolling Back an AI-Script Package ..... 16
  - Not Saving Copies of AI-Scripts Package Files During Installation ..... 16
  - Removing AI-Script Packages After Installation ..... 16
- List of Technical Publications ..... 16
- Requesting Technical Support ..... 23
- Revision History ..... 24

## Release 1.0 Features

---

This section describes key features of the current AI-Scripts release.

- AI-Scripts Operation on page 3
- AI-Script Modes on page 3

### AI-Scripts Operation

AI-Scripts 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 structured format, such as 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).

### AI-Script Modes

AI-Scripts operate in two distinct modes:

- Reactive (incident-driven)—A trigger event occurs and is detected on a device. An AI-Script is executed. An AI-Script builds a Juniper Message Bundle (JMB) with event and router data, and sends it to a designated AIM archive location.

Each AI-Script corresponds to a specific device event. The list of device problem events that can be detected and reported will evolve over time. See Table 1 on page 3.

- Proactive (intelligence-driven)—AI-Scripts monitor device system resources for fluctuations that could signal a future problem. AI-Scripts collect intelligence data for analysis. A tailored AI-Script builds a JMB with intelligence data, and sends it to a designated remote AIM archive location.

## Events Detected By AI-Scripts

---

Table 1 on page 3 lists the events detected by Release 1.0 of the AI-Scripts.

**Table 1: Events Detected by AI-Scripts**

Event ID	Description
ACCT_MALLOC_FAILURE	The accounting statistics process could not allocate memory from the heap.
ASP_L2TP_NO_MEM	The Layer 2 Tunneling Protocol (L2TP) could not allocate the memory it needed to create a flow for the indicated tunnel and session.
CFMD_RTsock_OPEN_FAILURE	The connectivity fault management process (cfmd) could not successfully open a routing socket to the kernel, for the indicated reason.

**Table 1: Events Detected by AI-Scripts** (continued)

CHASSISD_BUS_DEVICE_OPEN_FAILURE	The chassis process (chassisd) could not open the indicated bus device for the indicated reason.
CHASSISD_CLOCK_FAILURE	The chassis process (chassisd) determined that the indicated clock source failed in the indicated way.
CHASSISD_CMB_READBACK_ERROR	The chassis process (chassisd) could not read back information from the Chassis Management Bus (CMB) about the indicated component (field-replaceable unit, or FRU).
CHASSISD_FAN_FAILURE	The indicated fan or impeller failed. The chassis process (chassisd) raised an alarm and increased the speed of the remaining fans (and impellers, if applicable) to full speed.
CHASSISD_FASIC_FTOKEN_ERROR	The chassis process (chassisd) detected an underflow or overflow error on the indicated F chip on the indicated Control Board (CB).
CHASSISD_FASIC_HSL_LINK_ERROR	The chassis process (chassisd) detected an error for the indicated high-speed link (HSL) for the indicated F chip on the indicated Control Board (CB).
CHASSISD_FASIC_INPUT_DROP	The Packet Forwarding Engine divides packets into smaller units called cells for more efficient processing. As the indicated F chip on the indicated Control Board (CB) processed data that was received from the indicated Packet Forwarding Engine on the indicated Flexible PIC Concentrator (FPC), it dropped the indicated number of cells per second.
CHASSISD_FASIC_OUTPUT_DROP	The Packet Forwarding Engine divides packets into smaller units called cells for more efficient processing. As the indicated F chip on the indicated Control Board (CB) processed data before sending it to the indicated Packet Forwarding Engine on the indicated Flexible Port Concentrator (FPC) for outgoing transmission, it dropped the indicated number of cells per second.
CHASSISD_FASIC_PIO_READ_ERROR	The indicated routine failed with a read error at the indicated address and register for the indicated F chip and link on the indicated Control Board (CB).
CHASSISD_FASIC_PIO_WRITE_ERROR	The indicated routine failed with a write error at the indicated address and register for the indicated F chip and link on the indicated Control Board (CB).
CHASSISD_FASIC_SRAM_ERROR	The chassis process (chassisd) detected that SRAM failed to initialize for the indicated F chip on the indicated Control Board (CB).
CHASSISD_FCHIP_HSR_ERROR	The chassis process (chassisd) detected an error in the high-speed receiver (HSR) subsystem for the F chip with the indicated characteristics.
CHASSISD_FCHIP_HST_ERROR	The chassis process (chassisd) detected an error in the high-speed transmitter (HST) subsystem for the F chip with the indicated characteristics.
CHASSISD_FCHIP_LINK_ERROR	The chassis process (chassisd) detected an error for the indicated high-speed receiver (HSR) or high-speed transmitter (HST) link for an F chip on the indicated Switch Interface Board (SIB).
CHASSISD_FCHIP_PIO_READ_ERROR	The indicated routine failed with a read error at the indicated address and register for the indicated F chip and link.
CHASSISD_FCHIP_PIO_WRITE_ERROR	The indicated routine failed with a write error at the indicated address and register for the indicated F chip and link.

**Table 1: Events Detected by AI-Scripts (continued)**

CHASSISD_FHSR_READ_REG_ERROR	The high-speed receiver (HSR) read routine failed at the indicated address on an F-chip register.
CHASSISD_FHSR_WRITE_REG_ERROR	The high-speed receiver (HSR) write routine could not record the indicated value at the indicated address on an F-chip register.
CHASSISD_FHST_READ_REG_ERROR	The high-speed transmitter (HST) read routine failed at the indicated address on an F-chip register.
CHASSISD_FHST_WRITE_REG_ERROR	The high-speed transmitter (HST) write routine could not record the indicated value at the indicated address on an F-chip register.
CHASSISD_FILE_OPEN	The chassis process (chassisd) could not open the indicated file for the indicated reason.
CHASSISD_FM_ERROR	During execution of the indicated fabric management routine, the indicated error occurred between the indicated Switch Interface Board (SIB) and the indicated Packet Forwarding Engine on the indicated Flexible PIC Concentrator (FPC).
CHASSISD_FM_ERROR_SIB_L_FB_HSR	In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the T640 routing nodes (called SIB-Ls) and the SIBs in the TX Matrix platform (called SIB-Ss). The chassis process (chassisd) on the routing node that houses the indicated SIB-L detected an error in the electrical path between the indicated ports on the SIB-L and the corresponding SIB-S.
CHASSISD_FM_ERROR_SIB_L_FB_SMF	In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the TX Matrix platform (the switch-card chassis, or SCC) and the SIBs in the T640 routing nodes (called SIB-Ls). The chassis process (chassisd) on the routing node that houses the indicated SIB-L detected the indicated error as packets that were traveling in the indicated direction were translated between electrical and optical media.
CHASSISD_FM_ERROR_SIB_S_FB_HSR	In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the TX Matrix platform (called SIB-Ss) and the SIBs in the T640 routing nodes (called SIB-Ls). The chassis process (chassisd) on the TX Matrix platform detected an error in the electrical path between the indicated port on the indicated SIB-S and the indicated port on a SIB-L installed in the indicated routing node (line-card chassis, or LCC).
CHASSISD_FM_ERROR_SIB_S_FB_SMF	In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the TX Matrix platform (called SIB-Ss) and the SIBs in the T640 routing nodes (line-card chassis, or LCCs). The chassis process (chassisd) on the TX Matrix platform detected the indicated error as packets that were traveling to or from the indicated LCC were translated between electrical and optical media.
CHASSISD_FM_SIB_ERROR	The chassis process (chassisd) detected the indicated type of error on the indicated Switch Interface Board (SIB) and performed the indicated action.
CHASSISD_HSR_FIFO_ERROR	A first-in, first-out (FIFO) read error occurred during execution of the indicated routine on the indicated high-speed receiver (HSR).
CHASSISD_IPC_MSG_DROPPED	The chassis process (chassisd) dropped an interprocess communication (IPC) message because the message queue had already reached maximum capacity.

**Table 1: Events Detected by AI-Scripts (continued)**

CHASSISD_IPC_MSG_UNHANDLED	The chassis process (chassisd) received an interprocess communication (IPC) message about the indicated FRU. The message had the indicated characteristics. The chassisd process could not handle the message.
CHASSISD_MALLOC_FAILURE	The chassis process (chassisd) could not allocate memory. The chassisd process tried to continue functioning, but the lack of memory usually causes the process to fail. An administrator needs to restart.
CHASSISD_MBE_DETECTED	A multi-bit ECC parity error was detected in Routing Engine DRAM.
CHASSISD_PEM_OVERLOAD	The indicated power entry module (PEM) reported an output voltage overload condition.
CHASSISD_PEM_VOLTAGE	The indicated power entry module (PEM) reported a problem with its output voltage.
CHASSISD_SBE_DETECTED	Too many single-bit correctable ECC parity errors were detected in Routing Engine DRAM.
CHASSISD_SMB_IOCTL_FAILURE	The indicated ioctl() operation failed at the indicated address on the system management bus (SMB).
CHASSISD_SMB_READ_FAILURE	A read() operation failed at the indicated address on the system management bus (SMB).
CHASSISD_TEMP_SENSOR_FAILURE	The temperature sensor for the indicated component (field-replaceable unit, or FRU) either did not respond to a request from the chassis process (chassisd) for a temperature reading or sent a value that is outside the normal operating range.
CHASSISD_UNEXPECTED_EXIT	The chassis process (chassisd) exited unexpectedly and reported the indicated error.
COSD_MALLOC_FAILED	The class-of-service (CoS) process (cosd) could not dynamically allocate memory, for the indicated reason.
COSD_UNEXPECTED_EXIT	COSD waits for the event notifications and processes the events that it is registered for. There was an error during event-handling initialization.
Daemon Crash	A JUNOS daemon crash occurred with a core dump.
DCD_PARSE_STATE_EMERGENCY	The interface process (dcd) encountered an unhandled internal state during interface parsing.
DCD_TRASHED_RED_ZONE	When DCD is allocating heap memory, it uses a private memory allocator that writes a special pattern at the end of each allocated segment of heap memory. Later, when de-allocating this memory, DCD checks for the pattern. If it does not find the previously written pattern, it means the memory was overwritten, which indicates a wild-write in DCD.
DFWD_MALLOC_FAILED	DFWD must dynamically malloc memory for its needs. This allocation request failed. The specific data structure that was being allocated is listed in the message.
DFWD_PARSE_STATE_EMERGENCY	The firewall process (dfwd) encountered an unhandled internal state while parsing an interface.

**Table 1: Events Detected by AI-Scripts (continued)**

DFWD_TRASHED_RED_ZONE	When DFWD is allocating heap memory, it uses a private memory allocator that writes a special pattern at the end of each allocated segment of heap memory. Later, when de-allocating this memory, DFWD checks for the pattern. If it does not find the previously written pattern, it means the memory was overwritten, which indicates a wild-write in DFWD.
DH_SVC_RTsock_OPEN_FAILURE	The Dynamic Host Configuration Protocol (DHCP) services process (dhcp-service) could not successfully open a routing socket to the kernel. The error string accompanying this log entry indicates the specific error.
DH_SVC_RTsock_REGISTER_FAILURE	The Dynamic Host Configuration Protocol (DHCP) services process (dhcp-service) could not successfully register a callback function with a routing socket. The error string accompanying this log entry indicates the specific error.
DH_SVC_SETSOCKOPT_FAILURE	The Dynamic Host Configuration Protocol (DHCP) services process (dhcp-service) could not set the indicated socket option.
DH_SVC_SOCKET_FAILURE	The Dynamic Host Configuration Protocol (DHCP) services process (dhcp-service) could not create a socket.
EVENTD_EVENT_SEND_FAILED	JUNOS processes can request that the event processing process (eventd) notify them when a specific event occurs. The eventd process could not send an event notification for the indicated reason.
EVENTD_FORK_ERR	The event processing process (eventd) could not create a child process for executing policies.
EVENTD_PIPE_ERR	The event processing process (eventd) could not create a pipe for interprocess communication.
FSAD_ERROR	The File System Access process (fsad) internal error message.
FUD_MEMORY_ALLOCATION_FAILURE	The UDP forwarding process (fud) could not allocate the indicated amount of memory from the heap.
FUD_RTsock_WRITE_FAILURE	The UDP Forwarding process (fud) could not write to its routing socket for the indicated reason.
FUD_SENDMSG_FAILURE	The UDP Forwarding process (fud) could not send data to the indicated destination port and address using the indicated interface and routing instance, which it needs to do during normal operation.
FUD_SENDMSG_NOINT_FAILURE	The UDP Forwarding process (fud) could not send data to the indicated destination port and address using the indicated routing instance, which it needs to do during normal operation.
FUD_SETSOCKOPT_FAILURE	The UDP Forwarding process (fud) could not set the indicated socket option.
FUD_SOCKET_FAILURE	The UDP Forwarding process (fud) could not create a socket.
GRAPH_NO_MEMORY	The graphing process could not allocate memory while trying to create a graph.
L2CPD_ABORT	The Layer 2 Control Protocol process (l2cpd) terminated because of an internal error.

**Table 1: Events Detected by AI-Scripts (continued)**

L2CPD_ASSERT	The source code for the Layer 2 Control Protocol process (l2cpd) includes internal self-consistency tests. The l2cpd process with the indicated executable name and process ID (PID) terminated because the indicated test failed at the indicated line number in the indicated source file. The process created a diagnostic core file for analysis by technical support personnel.
L2CPD_ASSERT_SOFT	The source code for the Layer 2 Control Protocol process (l2cpd) includes internal self-consistency tests. The l2cpd process with the indicated executable name and process ID (PID) terminated because the indicated type of check failed at the indicated line number in the indicated source file. The process continued to run, but created a diagnostic core file for analysis by technical support personnel.
L2TPD_EVLIB_CREATE_FAILED	The Layer 2 Tunneling Protocol process (l2tpd) could not create a context for handling asynchronous events.
L2TPD_SERVER_START_FAILED	The Layer 2 Tunneling Protocol (L2TP) server did not start.
LACPD_DAEMONIZE_FAILED	The Link Aggregation Control Protocol process (lacpd) could not create a version of itself to run in the background as a daemon.
LIBJNX_DEFAULT_IP_ADDR_NOT_SET	A JUNOS process could not retrieve the system default IP address from the kernel, because the address is not defined there.
PFE Crash	Any PFE board crash that occurs in conjunction with a system exception message.
PPMD_ASSERT_SOFT	The source code for the periodic package management process (ppmd) includes internal self-consistency checks. As the ppmd process with the indicated process ID (PID) executed the binary compiled from the indicated source file, a check failed at the indicated line number in the file. The ppmd process created a diagnostic core file for analysis by technical support personnel and continued to run.
RDD_EVLIB_CREATE_FAILURE	The redundant interfaces process (rdd) could not create a context used for handling all asynchronous events (such as timers and message availability).
RPD_ABORT	The routing protocol process (rpd) terminated because of an internal error.
RPD_ACTIVE_TERMINATE	After receiving multiple termination requests, the routing protocol process (rpd) exited without performing the indicated cleanup tasks.
RPD_ASSERT	The source code for the routing protocol process (rpd) includes internal self-consistency checks. A check failed at the indicated line number in the indicated source file, causing the instance of rpd that was using the indicated binary and had the indicated process ID (PID) to terminate. The process created a diagnostic core dump for analysis by technical support personnel.
RPD_ASSERT_SOFT	The source code for the routing protocol process (rpd) includes internal self-consistency checks. A check failed at the indicated line number in the indicated source file, but the instance of rpd that was using the indicated binary and had the indicated process ID (PID) continued running. The process created a diagnostic core dump for analysis by technical support personnel.
RPD_ISIS_LSPCKSUM	The indicated IS-IS informational link-state PDU (LSP) failed an internal checksum validity test, implying that it was corrupted.
RPD_ISIS_OVERLOAD	The IS-IS link-state database is full and no additional memory can be allocated for it.

**Table 1: Events Detected by AI-Scripts** (continued)

RPD_LMP_UNEXPECTED_OPCODE	The routing protocol process (rpd) received the indicated type of message, which had the indicated invalid operation code.
RPD_RT_ERROR	A route in the routing table was found to be in an unrecoverable error state.
RPD_TASK_FORK	The routing protocol process failed to create the indicated child process.
SPD_DAEMONIZE_FAILED	The adaptive services process (spd) could not create a version of itself to run in the background as a daemon.
SPD_EVLIB_CREATE_FAILURE	The adaptive services process (spd) could not create a context used for handling all asynchronous events (such as timers and message availability).

## Current Software Release

---

The current AI-Scripts release is Release 1.0B2. For information about installing the software release, see “AI-Script Installation Methods” on page 10.

## Issues Fixed Since Last Release

---

The following issues have been fixed since the last AI-Scripts release:

- The destination archive-site name was changed from juniper-junoscope to juniper-aim. (PR 273382)
- The daemon crash event script now captures core file information. (PR 276860)
- The trend data now shows all FPC and backup Routing Engine details. (PR 279650)

## Outstanding Issue

---

The following issue exists in the current AI-Scripts release:

- The AI-Scripts do not include **chassis-re-disk-module** media information on the Routing Engine, such as compact-flash and hard drive, in the Juniper Message Bundle (JMB). (PR 279109)

## AI-Scripts Troubleshooting

---

The following items should be noted during AI-Script installation:

- Installing an AI-Script Install Bundle Using JUNOScope Software on page 10
- Upgrading from AI-Scripts 1.0R1 Install Package to 1.0R2 on page 10

## **Installing an AI-Script Install Bundle Using JUNOScope Software**

To install an AI-Script install bundle to multiple devices using the JUNOScope software, do the following:

- Use the JUNOScope 1.0R2 software with the AI-Scripts 1.0R2 install package.

## **Upgrading from AI-Scripts 1.0R1 Install Package to 1.0R2**

To upgrade from the AI-Scripts 1.0R1 install package to 1.0R2, follow these steps:

1. Delete the existing AI-Scripts by using the following CLI command:

```
request system scripts delete
```

2. In CLI edit mode, modify the event-options name in the [groups juniper-ais event-options destinations] hierarchy:

```
[edit groups juniper-ais event-options destinations]  
user@router#rename juniper-junoscope to juniper-aim
```

3. Commit the configuration change.
4. Follow the steps in “Installing AI-Scripts” on page 10

## **Installing AI-Scripts**

---

- AI-Script System Requirements on page 10
- AI-Script Installation Methods on page 10
- Downloading AI-Script Install Packages on page 11
- AI-Script Install Package Versioning on page 11
- AI-Script Install Locations on Devices on page 12
- Automatically Installing AI-Scripts Overview on page 12
- Automatically Installing AI-Scripts on page 12
- Manually Configuring and Installing AI-Scripts on Devices on page 13

## **AI-Script System Requirements**

Ensure that all devices on which you install AI-Scripts are running JUNOS Release 9.0 or later.

## **AI-Script Installation Methods**

There are two ways to install AI-Scripts:

- Automatically, using the JUNOScope Script Management feature to automatically install AI-Scripts to multiple devices at once. For more information about automatically installing AI-Scripts, see “Automatically Installing AI-Scripts” on page 12.

- Manually by installing AI-Scripts on one device at a time. For more information about manually installing AI-Scripts to devices, see “Manually Configuring and Installing AI-Scripts on Devices” on page 13.

## Downloading AI-Script Install Packages

AI-Scripts are released in AI-Script install packages. AI-Script install packages are available for download from the AIS download site. Download also the AI-Scripts Release Notes.

To download an AI-Script install package, follow these steps:

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

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

2. Log in to the Juniper Networks authentication system using the username and password supplied by Juniper Networks.

To download the software, you must have a service contract and an access account. If you do not have an access account, complete the registration form at the Juniper Networks Web site, <https://www.juniper.net/registration/Register.jsp>.

3. Download the AI-Script install package. If you will install an AI-Script install script manually, move the package to the `/var/sw/pkg` directory on the device.

If you do not move the AI-Script install package to the device, you have to use `ftpor scp` in conjunction with the request system scripts `add` command. (Optional) If you will use the JUNOScope software to automatically install an AI-Script package to a group of devices at once. Download the AI-Script install package on the same server as Advanced Insight Manager (AIM).

## AI-Script Install Package Versioning

AI-Script install packages are versioned as follows:

`jais-m.nZx.x-signed.tgz`

or

`jais-1.0R1.5-signed.tgz`

- *m.n* is two integers that represent the software release number; *m* denotes the major release number; *n* the minor.
- *Z* is a capital letter that indicates the type of software release. In most cases, it is an **R**, to indicate that this is released software. If you are involved in testing prereleased software, this letter might be a **B** (for beta-level software).
- *x.x* is the software build number and spin number.

The AI-Script files that in the install package are compressed into a **tgz** tarball file.

Each AI-Script install package supports up to 3 previous years of JUNOS software releases.

The `show version` CLI operational command displays the version of the AI-Script install package that is installed on a device.

The JMB contains the output of the `show version` CLI command to indicate the version of the AI-Script install package installed on a device.

## AI-Script Install Locations on Devices

AI-Scripts are installed on a device hard disk in the following location:

```
/var/db/scripts/
```

AI-Scripts are installed on a device flash drive in the following location:

```
/config/scripts
```



**NOTE:** If you configure the `load-scripts-from-flash` option, the system reads AI-Scripts from the `/config/scripts/` directory; otherwise the system reads AI-Scripts from the `/var/db/scripts/` directory. The `/var/run/scripts` directory will always point to the right scripts directory.

---

## Automatically Installing AI-Scripts Overview

Automatically installing AI-Script install packages to one or more devices involves AIM interaction with JUNOScope software Script Management.

The automated AI-Script installation process requires the following key tasks :

- Install and set up JUNOScope 9.0 or later. See the *JUNOScope Software User Guide*.
- Install AIM. See the *AIS User Guide*.
- Set up AIM settings. See the *AIS User Guide*.
  - General settings.
  - JUNOScope settings (Settings > General > JUNOScope Settings).
  - Set up AI-Script bundles (Settings > General > Script Bundles).
  - Set up organizations.
  - Set up user groups.
  - Set up users.

## Automatically Installing AI-Scripts

You can optionally use AIM to install AI-Script bundles (also known as AI-Script install packages) on devices as long as there is a JUNOScope software installation. AIM

communicates with JUNOScope to install AI-Script bundles on JUNOS devices managed by JUNOScope.

To configure auto installation of AI-Script bundles to devices, follow these steps:

1. Configure the credentials used to communicate with JUNOScope.
2. Import devices that are managed by JUNOScope.
3. Configure Script Bundles settings.
4. Associate imported devices with a device group.
5. Configure the Script Bundle of the device group and set the No-copy and Unlink installation attributes
6. Add archive locations specifying the upload command password attributes
7. Press the Save Changes button. AIM sends a message to JUNOScope to install the selected script bundle on the associated devices.

If you do not want to use AIM to install AI-Script bundles, you can manually configure and install AI-Script bundles to each device separately. To install AI-Script bundles manually, see “Manually Configuring and Installing AI-Scripts on Devices” on page 13.

## ***Manually Configuring and Installing AI-Scripts on Devices***

Within AIM, devices that are configured for AIS manually are automatically added to the device group that is associated with the AIM archive location to which the JMB was sent. When the AIM detects a JMB for a device that is not managed by JUNOScope Script Management, it will note it.

To manually configure and install AI-Scripts on devices, follow these steps:

1. Download AI-Script install packages. See “Downloading AI-Script Install Packages” on page 11.
2. Configure the device configuration as follows to activate AI Scripts:
  - a. Enter the device CLI configuration mode. Type the `configure` command or the `edit` command from the CLI operation mode. The CLI prompt changes from `user@host>` to `user@host#` and a banner appears to indicate the hierarchy level.
  - b. Configure an AIS destination under group `juniper-aim`:

```
user@host#set groups juniper-ais event-options destination juniper-aim {...}
```

This configuration determines the AIS archive location where JMBs are deposited for a device.

- c. Configure the commit script:

```
user@host#set groups juniper-ais system scripts commit file
jais-activate-scripts.slax optional
```

The AI-Script installer creates this script to activate AI-Scripts on the device.

- d. Configure the allow-transients option to allow transient changes:

```
user@host#set groups juniper-ais system scripts commit allow-transients
```

Transient changes are configuration changes made by commit scripts that do not appear in the configuration (except with a special command).

- e. Apply the juniper-ais group:

```
user@host#set apply-groups juniper-ais
```

- f. (Optional) Configure the load-scripts-from-flash option:

```
user@host#set groups juniper-ais system scripts load-scripts-from-flash
```



**NOTE:** If you configure the load-scripts-from-flash option, the system reads AI-Scripts from the `/config/scripts/` directory; otherwise, the system reads AI-Scripts from the `/var/db/scripts/` directory. The `/var/run/scripts` directory will always point to the right scripts directory.

---

3. Verify that the syntax of a configuration is correct by using the configuration mode `commit check` command:

```
[edit]
user@host# commit check
configuration check succeeds
```

4. Commit the configuration. To save software configuration changes to the configuration database and activate the configuration on the router, use the `commit configuration mode` command. You can issue the `commit` command from any hierarchy level.

```
[edit]
user@host# commit
commit complete
```

5. View the configuration:

```
groups {
  juniper-ais {
    system {
      scripts {
        commit {
          allow-transients;
          file jais-activate-scripts.slax {
            optional;
          }
        }
        load-scripts-from-flash;
      }
    }
  }
  event-options {
    destinations {
      juniper-aim {
```

```

        archive-sites {
            "ftp://anonymous@10.7.0.124/aimdemo";
        }
        . . .

```

6. If you have not moved the AI-Script to the device, do so now. See “Downloading AI-Script Install Packages” on page 11.
7. Install the AI-Script package using the following command (see “AI-Script Installation Commands” on page 15):

```
user@host# request system scripts add <package-name>
```

8. Verify that the AI-Scripts are activated:

```
user@host# show groups juniper-ais | display commit-scripts
```

```

system {
  scripts {
    commit {
      allow-transients;
      file jais-activate-scripts.slax {
        optional;
      }
    }
  }
}
event-options {
  event-script {
    file problem-event-pfcrash.slax;
    file problem-event-dcrash.slax;
    file intelligence-event-main.slax;
    file SPD_EVLIB_CREATE_FAILURE.slax;
    file SPD_DAEMONIZE_FAILED.slax;
    file RPD_TASK_FORK.slax;
    . . .}
  destinations {
    juniper-aim {
      archive-sites {
        "ftp://anonymous@10.7.0.124/aidemo";
      }
    }
  }
}

```

## AI-Script Installation Commands

---

- Installing an AI-Script Package on page 16
- Deleting an AI-Script Package on page 16
- Rolling Back an AI-Script Package on page 16
- Not Saving Copies of AI-Scripts Package Files During Installation on page 16
- Removing AI-Script Packages After Installation on page 16

## Installing an AI-Script Package

To install an AI-Script install package on a device, use the following command:

```
user@host> request system scripts add <package-name>
```

## Deleting an AI-Script Package

To delete AI-Scripts from a router, use the following command:

```
user@host> request system scripts delete
```

## Rolling Back an AI-Script Package

After the deletion of an AI-Script install package, you can roll back to the last installed package by using the following command:

```
user@host> request system scripts rollback
```

## Not Saving Copies of AI-Scripts Package Files During Installation

To prevent the installer from saving copies of AI-Script package files in the `/var/sw/pkg` directory, use the following command:

```
user@host> request system scripts add no-copy <package-name>
```



**NOTE:** If you use the no-copy option during the jais installation, the jais package cannot be rolled back.

---

You can specify the no-copy option in AIM Device Group settings by selecting the no-copy check box.

## Removing AI-Script Packages After Installation

To remove the AI-Script bundle after successful installation, use the following command:

```
user@host> request system scripts add unlink <package-name>
```

You can specify the unlink option in AIM Device Group settings by selecting the unlink check box.

## List of Technical Publications

---

Table 2 on page 17 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 3 on page 21 lists the books included in the *Network Operations Guide* series. Table 4 on page 22 lists the manuals and

release notes supporting JUNOS software with enhanced services. All documents are available at <http://www.juniper.net/techpubs/>.

Table 5 on page 23 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 2: Technical Documentation for Supported Routing Platforms**

Book	Description
<b>JUNOS Software for Supported Routing Platforms</b>	
<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.

**Table 2: Technical Documentation for Supported Routing Platforms** (continued)

Book	Description
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Protected System Domain</i>	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, 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>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.
<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.

**Table 2: Technical Documentation for Supported Routing Platforms** (continued)

Book	Description
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
<b>J-Web User Guide</b>	
<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.
<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>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>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'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.
<b>JUNOScope Documentation</b>	

**Table 2: Technical Documentation for Supported Routing Platforms** (continued)

Book	Description
<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 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.
<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 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.
<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 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.

**Table 2: Technical Documentation for Supported Routing Platforms (continued)**

Book	Description
<i>AIS AI Script Release Notes</i>	Summarize AI Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

**Table 3: 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 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 4: JUNOS Software with Enhanced Services Documentation**

Book	Description
<i>JUNOS Software with Enhanced Services Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IP Security (IPSec) virtual private networks (VPNs), firewalls, and routing on J-series routers running JUNOS software with enhanced services.
<i>JUNOS Software with Enhanced Services J-series Services Router Quick Start</i>	Explains how to quickly set up a J-series router. This document contains router declarations of conformity.
<i>JUNOS Software with Enhanced Services J-series Services Router Getting Started 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 router running the JUNOS software to JUNOS software with enhanced services.
<i>JUNOS Software with Enhanced Services Interfaces and Routing Configuration Guide</i>	Explains how to configure J-series router interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
<i>JUNOS Software with Enhanced Services Security Configuration Guide</i>	Explains how to configure and manage security services such as stateful firewall policies, IPSec VPNs, firewall screens, Network Address translation (NAT) and Router interface modes, Public Key Cryptography, and Application Layer Gateways (ALGs).
<i>JUNOS Software with Enhanced Services Administration Guide</i>	Shows how to monitor the router 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 with Enhanced Services 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.
<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 router for application acceleration.
<i>JUNOS Software with Enhanced Services Release Notes</i>	Summarize new features and known problems for a particular release of JUNOS software with enhanced services on J-series routers, including J-Web interface features and problems. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software with enhanced services.

**Table 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.
<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

---

5 April 2008—530-022700-01. Advanced Insight Scripts (AI-Scripts) 1.0 Release Notes, Revision 1.

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.