

Chapter 6

Configuring AIM General Settings

This chapter describes how to configure the Advanced Insight Manager (AIM) general settings, which also include JUNOScope and Script Bundle settings.

General settings within AIM include parameters necessary for AIM to retrieve information from device archive locations for incident and intelligence messages, and from Juniper Support Systems (JSS) for case management and intelligence updates. General settings allows you to set the port, amount, and frequency of information sharing with JSS.

JUNOScope settings allow AIM to integrate with the JUNOScope software Script Management feature to automatically install script bundles on multiple devices at once.

Script Bundle settings provide a central point for managing script bundles (also known as a AI-Script install packages) that have been downloaded from the Juniper Networks software download site. The script bundle must be local to the system running AIM. When configuring Device Groups, you can only associate one script bundle to a Device Group.

You must have AIM administrator privileges to configure general settings.

This chapter includes the following topics:

- Configuring General Settings on page 51
- Configuring JUNOScope Settings on page 53
- Configuring Script Bundle Settings on page 57

Configuring General Settings

AIM General Settings allow the user to do the following:

- Set the interval used by AIM to scan device archive locations for Juniper Message Bundles (JMBs).
- Set the interval used by AIM to poll JSS for case status updates.
- Set the interval used by AIM to poll JSS for intelligence updates specific to your site.

- Set the amount of information sharing included in informational JMBs
- Set the interval used to send newly detected information JMBs to JSS
- Set the port on which the AIM Service listens for requests from the client. The default port number is the value set during the AIM installation.

To configure AIM General settings, follow these steps:

1. In AIM, click the Settings Tab. The General Settings page appears.

General Settings

Save Settings

General Settings:	
* Incident Scan Interval (min):	<input type="text" value="1"/>
* Case Status Update Interval (min):	<input type="text" value="1"/>
* Intelligence Update Scan Interval (min):	<input type="text" value="1"/>
Information JMB Config Filter Level:	<input type="text" value="Send all information"/>
Upload Information JMB Interval:	<input type="text" value="On detection"/>
* Local RMI Port:	<input type="text" value="1022"/>

2. Add the required AIM General settings. See “AIM General Settings Page Description” on page 52.
3. Click Save Settings. This action saves the AIM General settings that you modify and updates the AIM service with these new settings.

AIM General Settings Page Description

Table 11 describes the General Settings page command button.

Table 11: General Settings Command Button

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Settings	Saves any modified AIM general settings and updates the AIM service with these new settings.	AIM Admin Settings	Enabled if admin privileges	Saves settings that were modified.

Table 12 describes the AIM General Settings parameters.

Table 12: General Settings Parameters

Name	Description	Privileges	Range/ Length	Default
Incident Scan Interval (min):	Interval used to scan for new incidents in AIM archive locations.	AIM Admin Settings	0 = Off, 1 - 1440 (60 seconds - 24 hours)	3 minutes
Case Status Update Interval (min)	Interval used to poll for JTAC Case status updates from JSS Case Manager	AIM Admin Settings	1 - 1440 minutes (60 seconds - 24 hours)	4 minutes
Intelligence Update Scan Interval (min)	Interval used to poll for intelligence updates for this site in AIM archive locations.	AIM Admin Settings	1 - 1440 minutes (60 seconds - 24 hours)	3 minutes
Information JMB Config Filter Level	Specifies the amount of device configuration information in Juniper Message Bundles to share with Juniper: <ul style="list-style-type: none"> ■ Do not send ■ Send all information except configuration ■ Send all information with IP Addresses overwritten ■ Send all information 	AIM Admin Settings	N/A	Do not send
Upload Information JMB Interval	Interval used to send any newly detected Intelligence JMBs to JSS: <ul style="list-style-type: none"> ■ On Detection ■ Daily ■ Weekly ■ Monthly 	AIM Admin Settings	N/A	Monthly
Local RMI Port	Port on which the AIM Service listens for requests from the client	AIM Admin Settings	1-65535	1022

Configuring JUNOScope Settings

JUNOScope Settings allow the AIM application to integrate with the JUNOScope software Script Management feature to automatically install a script bundle (also known as an AI-Script install package) on multiple devices at once.

JUNOScope Settings include the following information:

- URL used to connect AIM to the JUNOScope software
- Username and password of JUNOScope AIM user with read-write privileges
- IP address used by the device to download script bundles from JUNOScope if DNS is disabled on the device

The AIM administrator must set up JUNOScope Settings before devices can be imported from JUNOScope. Devices appear in the Devices table when you click Import JUNOScope devices in the Devices Managed by JUNOScope table.

The AIM administrator can import all devices that are managed by the JUNOScope software. Only devices imported from JUNOScope will have JUNOScope Script Management capabilities, which include:

- Automatically installing a script bundle on one or more devices in a device group.
- Ensuring that AIM archive locations for all devices in the device group are synchronized.

To configure JUNOScope Settings, follow these steps:

1. In the AIM navigation pane, click General > JUNOScope Settings. The JUNOScope Settings page appears. The JUNOScope Settings page has two sections: JUNOScope Settings and Devices Managed by JUNOScope.

JUNOScope Settings

Save JUNOScope Settings		Test Connection to JUNOScope	
JUNOScope Settings:			
JUNOScope URL:	<input type="text" value="https://123.123.123.123:4443"/>		
JUNOScope Username:	<input type="text" value="admin"/>		
JUNOScope Password:	<input type="password" value="....."/>		
Confirm JUNOScope Password:	<input type="password" value="....."/>		
IP Address for Device to JUNOScope FTP connectivity:	<input type="text" value="123.321.23.3"/>		
Test Results:			

Devices Managed by JUNOScope (1 - 3 of 3)

Import JUNOScope Devices			↑↓	✕
Device Name	Host Name	Advanced Insight Manager Device Group		
prod8-device5	prod8-device5.company.net	Northwest Region		
prod9-device6	prod9.dev6.net	Northwest Region		
prod9-device9	prod9.dev9.net	Northwest Region		

2. Add the JUNOScope settings to connect AIM to the JUNOScope software server. See “JUNOScope Settings Table Description” on page 55.
3. Click Save JUNOScope Settings.
4. In the Devices Managed by JUNOScope table, click JUNOScope Devices. This action imports devices managed by JUNOScope into the AIM software. Any devices managed by the JUNOScope software are added. The JUNOScope software can install script bundles automatically to these devices. See “Devices Managed by JUNOScope Table Description” on page 56.

JUNOScope Settings Table Description

Table 13 describes the JUNOScope Settings command buttons.

Table 13: JUNOScope Settings Command Buttons

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Settings	First tests the connection to JUNOScope. If connection is successful, any modified parameters are saved.	AIM Admin Settings	Enabled if admin privileges	Displays the test results of the AIM connection to JUNOScope in the Test Results field: Successfully connected to JUNOScope server or An error message appears if settings are not saved.
Test Connection to JUNOScope	Uses the values in the JUNOScope settings fields to test the AIM connection to JUNOScope.	None	Always enabled	Displays test results of the AIM connection to JUNOScope in the Test Results field.

Table 14 describes the JUNOScope Settings table fields.

Table 14: JUNOScope Settings Table Parameter Descriptions

Name	Description	Privileges	Range/ Length	Default
JUNOScope URL	URL used to communicate with JUNOScope. Required for Script Bundle functionality	AIM Admin Settings	128 characters	Blank
JUNOScope Username	Log in ID to use for AIM communications with JUNOScope. This is the AIM user with read-write privileges created in the JUNOScope software. This setting is required for Script Bundle functionality	AIM Admin Settings	32 characters	Blank
JUNOScope Password	Password to use with the username	AIM Admin Settings	32 characters	Blank
Confirm JUNOScope Password	Password to type again for confirmation. The password must match the one in the password field	AIM Admin Settings	32 characters	Blank
IP Address for Device to JUNOScope FTP Connectivity	IP Address that the JUNOS devices use to transfer the Script Bundle from the JUNOScope server by way of FTP if DNS is not enabled on the device	AIM Admin Settings	32 characters	Blank
Test Results	Displays results from the Test Connection to JUNOScope command	Not allowed to modify	N/A	Blank

Devices Managed by JUNOScope Table Description

Table 15 describes the Devices Managed by JUNOScope table command button.

Table 15: Devices Managed by JUNOScope Command Button

Button Name	Description	Privileges	Enabled/ Disabled	Results
Import JUNOScope Devices	Request sent to JUNOScope to retrieve all the devices it manages and saves them in the AIM database	AIM Admin Settings	Enabled if you specify JUNOScope settings	Displays the devices imported from JUNOScope in the table.

Table 16 describes the Devices Managed by JUNOScope table fields.

Table 16: Devices Managed by JUNOScope Parameter Descriptions

Name	Description	Privileges	Range/ Length	Default
Device Name	Name JUNOScope user assigned this device.	Not allowed to modify	N/A	N/A
Host Name	Identifier used for network communication between JUNOScope and the JUNOS device. For example it could be a hostname (host-name.juniper.net) or an IP Address	Not allowed to modify	N/A	N/A
Advanced Insight Manager Device Group	The AIM device group to which this device belongs. For information about setting up AIM device groups, see “Creating Device Groups” on page 74.	Not allowed to modify	N/A	N/A

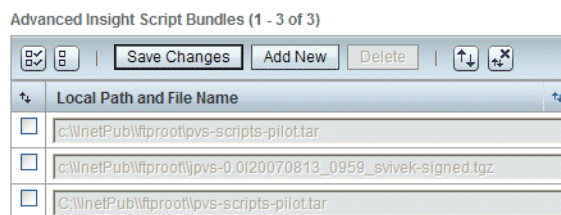
Configuring Script Bundle Settings

Script Bundle settings provide a central point for managing script bundles (also known as AI-Script install packages) that have been downloaded from the Juniper Networks software download site. The script bundle must be located locally to the system running AIM. When configuring Device Groups, you can associate one script bundle to the Device Group that will be downloaded to all devices that belong to the device group. For more information about setting up AIM Device Groups, see “Creating Device Groups” on page 74.

To configure Script Bundle settings, follow these steps:

1. In Settings, click General > Script Bundles. The Script Bundles page appears.

Script Bundles



2. Click Add New. A new row is added to the Script Bundles table. See “Script Bundles Table Description” on page 58.

3. Type the name and path (local to the system running the AIM Service) of the script bundle. The AIM Service verifies that it has access to the file. See “Script Bundles Table Description” on page 58.



NOTE: You cannot modify a script bundle after access to it has been verified and it has been saved in the database.

4. Click Save Changes. The script bundle location is saved to the database.

Script Bundles Table Description

Table 17 describes the command buttons on the Script Bundles page.

Table 17: Script Bundles Table Command Buttons

Button Name	Description	Privileges	Enabled/Disabled	Results
Saves Changes	Saves an added script bundle and verifies that the AIM has access to that file.	AIM Admin Settings	Enabled if admin privileges	Displays an error message if the application could not access the file.
Add New	Adds a new script bundle to AIM.	AIM Admin Settings	Enabled if admin privileges	An empty row is inserted into the bottom of the table so the user can configure the new entry.
Delete	Removes all selected script bundles in the table.	AIM Admin Settings	Enabled if admin privileges	Selected items are removed from the table.

Table 18 describes the Script Bundles location on the local host where AIM is installed.

Table 18: Script Bundles Table Row Description

Name	Description	Privileges	Range/Length	Default
Local Path and File Name	The name of the local path and file name where the script bundle is located on the machine running AIM. Note: A script bundle cannot be modified after access to it has been verified and it's location has been saved in the database.	AIM Admin Settings (only for creation)	128 characters and must be unique	Blank