Chapter 8

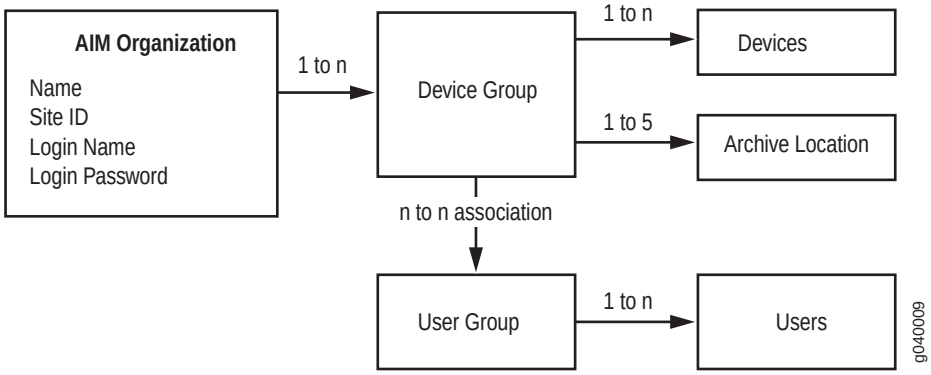
Configuring AIM Organizations and Device Groups

This chapter describes how to set up Advanced Insight Manager (AIM) Organizations and associated settings. An Organization represents a customer site in Juniper Support Systems (JSS). Organizations provide a way to manage multiple sites with one AIM installation by dividing the network into multiple logical customer site.

If you install the AIM Base Product license, you can create one Organization. Install the AIM Multi-Site feature license to create more than one Organization,

An AIM Organization requires a unique name, site ID, login name, and password to communicate with JSS. It also requires that you accept the Click-Through Agreement before proceeding. The site ID is an identifier used to denote the Customer Site field currently used in the JSS Clarify system. You can associate an Organization with one or more device groups providing a way to maintain groups of devices belonging to different customer networks. You can associate one or more devices to each device group. You can also associate a device group with one to five archive locations. You can associate an archive location with one device group at a time. You can associate a device group to one or more user groups. You can associate a user group to one or more AIM users. See Figure 11.

Figure 11: AIM Organization Creation Rules Diagram



Organizations contain device groups which are used to partition devices within one Organization. For more information about setting up a device group, see “Creating Device Groups” on page 72. Device groups are also used in conjunction with user groups to limit the access of users to certain groups of devices. See “Setting Up AIM Users” on page 89.

AIM integrates with Juniper Support Systems alert system by providing a way to register for alerts for each Organization. When alerts are registered through AIM, instead of the customer receiving e-mail messages, the alert messages are received by AIM then displayed in Intelligence Manager, see “Associating Registered Alerts with Organizations” on page 79 and.

(Optional) You can use AIM to install AI-Script bundles (also known as AI-Script install packages) on devices as long as JUNOScope software is installed. 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, see “Automatically Installing AI-Script Bundles” on page 83

You can also manually configure and install AI-Script bundles on each device separately.

Only users with AIM Admin Settings privileges can configure Organizations and device groups.

The chapter includes the following information:

- Organization Prerequisites on page 68
- Organization Configuration Sequence on page 69
- Adding Organization Credentials on page 70
- Creating Device Groups on page 72
- Configuring Archive Locations on page 73
- Associating Devices to a Device Group on page 75
- Associating User Groups to Device Groups on page 77
- Associating Registered Alerts with Organizations on page 79
- Using the Organizations Table on page 81
- Automatically Installing AI-Script Bundles on page 83

Organization Prerequisites

Perform the following before creating an AIM Organization:

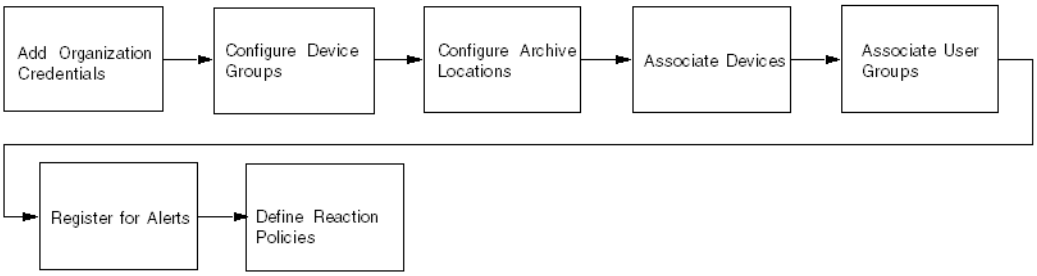
- Obtain a Site ID from Juniper Customer Support
- Obtain the Clarify username and password for the site from Juniper Customer Support.

- Download AI-Scripts Install Packages from the Juniper Networks Website to the local host file system.
- (Optional) In Setting > General > Script Bundles, select the AI-Script install packages that you want to install on JUNOS devices using the JUNOScope software Script Management.
- Configure the archive locations into which JUNOS devices will deposit JMB files. Verify that the AIM Service can access these locations as local directories (network file system (NFS) mount them if they are not local directories on the system).
- (Optional) In Settings > JUNOScope Settings: Devices Managed by JUNOScope settings, import Devices imported from JUNOScope
- Add AIM users
- Add AIM User groups
- Associate AIM users with user groups

Organization Configuration Sequence

Figure 12 shows the sequence required to create an organization.

Figure 12: AIM Organization Configuration Sequence



- Adding Organization Credentials on page 70
- Creating Device Groups on page 72
- Configuring Archive Locations on page 73
- Associating Devices to a Device Group on page 75
- Associating User Groups to Device Groups on page 77
- Associating Registered Alerts with Organizations on page 79

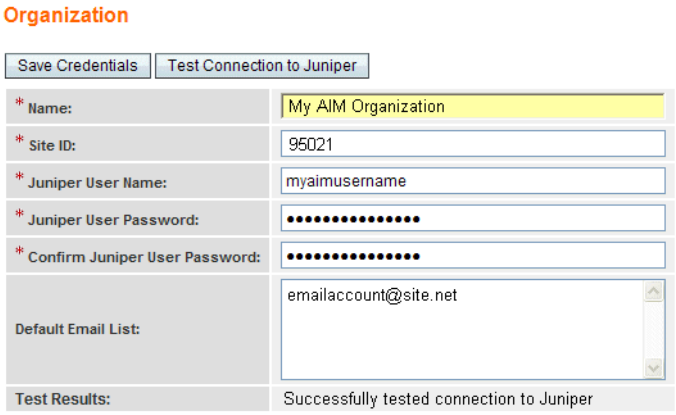
Adding Organization Credentials

To create an AIM Organization, follow these steps:

1. Click the Settings tab, then click > Organizations in the navigation pane. The Organization page appears.

The Organizations table is empty until you create an Organization. Once you've created an organization, AIM Organizations table displays the names of existing Organizations listed alphabetically by name and includes site ID, Juniper user name, and results of the connection test between AIM and JSS.

2. Click Add New. The Organization page appears.



3. Type the Organization credentials in the provided fields. (See "Organization Page Field Descriptions" on page 71.)

4. Click Test Connection to Juniper. This command verifies the Organization Credential settings and displays the connection results. See Table 27.

5. Click Save Credentials. This action verifies and saves the Organization credentials, and displays the Device Groups, and Alert Registration tables. See Table 27.

AIM Organization Page Description

Table 27 defines the Organization page command buttons.

Table 27: Organization Page Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Credentials	Tests connection to JSS, and if successful, then saves organization name and authentication credentials in the database.	AIM Admin	If privileged	Saves the new organization credentials in the AIM database
Test Connection to Juniper	Uses the values in the fields to test the connection to JSS.	None	Always enabled	Displays the result of the test connection to JSS: success or failure.

Table 28 defines the Organization page fields.

Table 28: Organization Page Field Descriptions

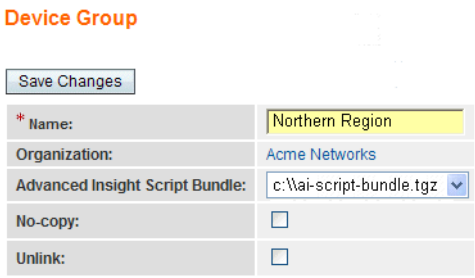
Name	Description	Privileges	Range/ Length	Default
Name	Name of the organization	AIM Admin	64 characters	Blank
Site ID	An identifier used to denote the Customer Site field currently used in the JTAC Clarify system	AIM Admin	80 characters	Blank
Juniper Username	Login to use for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases	AIM Admin	32 characters	Blank
Juniper User Password	Password to use with the username	AIM Admin	32 characters	Blank
Confirm Juniper User Password	Password must be typed in again and must match value in password field	AIM Admin	32 characters	Blank
Default email list	List of e-mail addresses to be used as the default e-mail list when a new case is submitted to Juniper. E-mail addresses should be separated by commas.	AIM Admin	65535 characters	Blank
Test Results	Displays results from the Test Connection to Juniper command: Success or failure	N/A	N/A	Blank

Creating Device Groups

Once the Organization credentials are verified and saved by clicking Save Credentials, the page expands and the Device Group and Registered Alerts tables appear below. The Device Group and Archive Locations tables are empty until you create device groups.

To create a device group, follow these steps:

1. In the Organization Device Group table, click Add New. The Device Group page appears.



2. Type the device group information in the fields and check boxes. (See "Organization Device Group Page Description" on page 72.

   The Organization to which the device group belongs displays in the Organization field. You can not modify the Organization name.

Organization Device Group Page Description

Table 29 defines the Organization page Device Group command buttons.

Table 29: Organization Device Group Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Saves device group parameters and archive locations. If an AI-Script bundle is specified, that bundle is installed on all the devices in the device group.	AIM Admin	If privileged	An error message is displayed if the device group and archive locations settings are not saved.

Table 30 defines the Organization page Device Group fields.

Table 30: Organization Device Group Field Descriptions

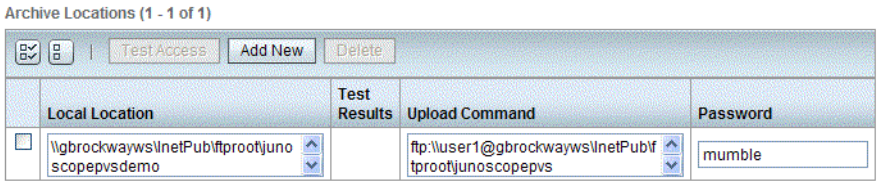
Name	Description	Privileges	Range/ Length	Default
Name	Name of the device group	AIM Admin	32 characters	Blank
Organization	Name of the organization to which this device group belongs. The Organization to which the device group belongs displays in the Organization field. The organization name provides a link to the Organization detail screen. See "AIM Organization Page Description" on page 71.	You can not modify the Organization name.	N/A	Blank
Advanced Insight Script Bundle	Provides a drop-down list of all the AI-Script bundles managed by AIM.	AIM Admin	N/A	Blank
No-copy	Indicates the command to not save a copy of the AI-Script bundle file during installation on the device.	AIM Admin	Checked or unchecked	Blank
Unlink	Indicates the command to remove the AI-Script bundle after successful installation on the device.	AIM Admin	Checked or unchecked	Blank

Configuring Archive Locations

You can create up to five archive locations for a device group.

To configure a new archive location, follow these steps:

1. On the Device Group page, click Add New in the Archive Locations table. A new row appears in the Archive Locations table. The Archive Locations table is empty until you add archive locations.



2. Type the required information in the Archive Locations table column fields. See "Archive Locations Table Description" on page 74.

3. Click Test Access. The test results appear in the Test Results field. The test results are either Success or Failure.

4. Click Save Changes at the top of the Device Groups page. This command saves the device group parameters and the archive locations.

If you specify an AI-Script install package, that package is automatically installed on all the device in the group that were imported from JUNOScope,

Archive Locations Table Description

Table 31 defines the Archive Locations table command columns.

Table 31: Archive Locations Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Test Access	Tests access to the selected device archive local location pathname specified in the Local Location field.	AIM Admin	Enabled when you select an archive location in the Archive Location table.	The Test Access results are either: ■ Successfully accessed location. ■ Failure to access location.
Add New	Adds a new row in the Archive Location table	AIM Admin	Always enabled	
Delete	Removes the selected archive location	AIM Admin	Enabled when you select an archive location row in the Archive Location table.	

Table 32 defines the Archive Locations table fields.

Table 32: Archive Location Table Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Local Location	The name of the local path where the Juniper device sends incident and intelligence JMBs. This path is relative to the installation machine.	AIM Admin	128 characters	Blank filed
Test Results	Displays results from the Test Access command for this row. The test results are either: ■ Successfully accessed location. ■ Failure to access location.	Not allowed to modify	N/A	Blank display field
Upload Command	Command that will be specified to set the archive location on the JUNOS devices. This command will be used to transfer the JMB files to the archive location.	AIM Admin	128 characters	Blank field
Password	Password that will be used by the JUNOS devices when they run the upload command to transfer the JMB files to the archive location.	AIM admin	64 characters	Blank field

Associating Devices to a Device Group

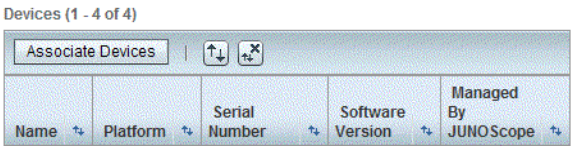
The Devices table displays the devices in the AIM application that are contained in a particular device group.

Devices can be associated to a device group in two ways:

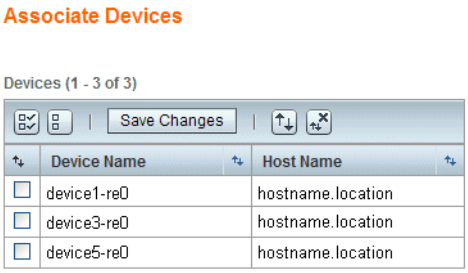
- When a JMB file is detected in any of the archive location of this device group, then the device that generated the JMB file is automatically added to the device group.
- Devices that have been imported from JUNOScope can be associated to the device group manually my the user.

To associate devices, follow these steps:

1. In the Devices table, click Associate Devices. The Devices table is empty until you associate devices to the device group.



The Associate Devices page appears with the available devices.



2. In the Associate Devices table, select the devices you want to associate with the device group. The devices that appear in the table are those that were imported from JUNOScope. See “Configuring JUNOScope Settings” on page 51. See “Associate Devices Table Description” on page 77.

3. Click Save Changes. The newly associated devices now appear in the Device table by device name, routing platform type, serial number, software version, and whether they are managed by the JUNOScope software.

Devices (1 - 4 of 4)

Associate Devices

Name	Platform	Serial Number	Software Version	Managed By JUNOScope
device1-re0	m10	62602	9.0 I0	Yes
device3-re0	j4350	JN109283BADA	9.0 I0	Yes
device5-re0	m7i	A8595	9.0 I0	Yes

See “Devices Table Description” on page 76.

Devices Table Description

Table 33 defines the Device table command buttons.

Table 33: Devices Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled
Associate Devices	Displays the Associate Devices page where you can select device groups to associate with an organization.	AIM Admin	Always is enabled

Table 34 defines the Devices table column descriptions.

Table 34: Devices Table Column Descriptions

Name	Description	Privileges
Name	Name of the device	Not allowed to modify
Platform	Type of device (routing platform)	Not allowed to modify
Serial Number	Serial number of device	Not allowed to modify
Software Version	Operating software release and version running on the device	Not allowed to modify
Managed by JUNOScope	Whether device was imported from the JUNOScope software. Yes appears if the devices is managed by JUNOScope. The column is blank if the devices is not managed by JUNOScope. Indicates that AI-Script bundle will be installed on the device	Not allowed to modify

Associate Devices Table Description

Table 35 describes the command button in the Associate Devices table.

Table 35: Associate Devices Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled
Save Changes	Saves the selected devices to associate with an AIM Device Group as part of AIM Organization creation.	AIM Admin	Always is enabled

Table 36 describes the columns in the Associate Devices table.

Table 36: Associate Devices Table Descriptions

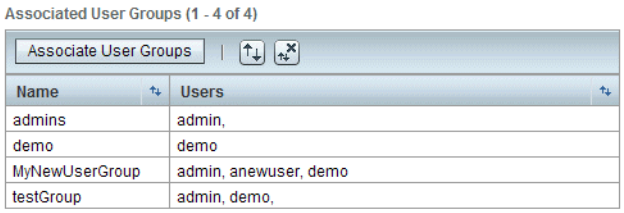
Button Name	Description	Privileges
Device Name	Name of the device to associate with an existing device group	AIM Admin
Host Name	The unique name by which a device is known on a network	AIM Admin

Associating User Groups to Device Groups

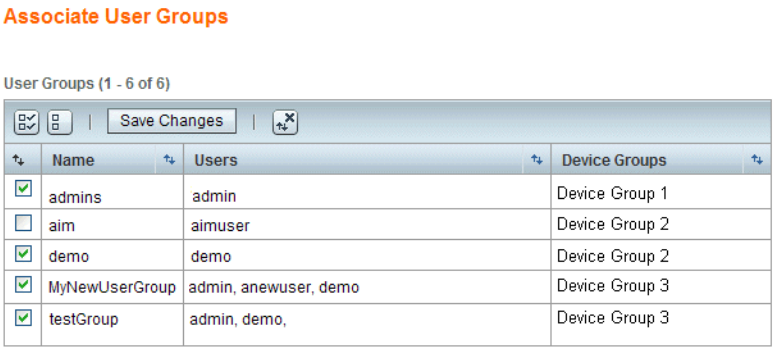
The Associate User Groups table displays the user groups that are currently associated with the device group. The Associate User Groups table displays the user group name and users belonging to it.

To associate users to a device group, follow these steps:

1. In the expanded Device Group page Associated User Groups table, click Associate User Groups.



The Associated User Groups table is empty until you associate user groups to a device group. The Associate User Groups table appears.



2. Select the user groups you want to associate with the device group.

3. Click Save Changes. The selected user group(s) appear on the Associate User Group table. “Associate User Groups Table Description” on page 78.

Associate User Groups Table Description

Table 37 defines the Associate User Groups table command buttons.

Table 37: Associate Users Group Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Sets which user groups are associated with the device group and navigates the user back to the Device Group page	AIM Admin	Disabled until you select a user group.	Saves user groups associated with the device group

Table 38 defines the Archive Location table fields.

Table 38: Associate Users Group Table Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	Name of the user group to associate with the device group	AIM Admin	Not allowed to modify	N/A
Users	Name of users associated to the user group separated by commas	AIM Admin	Not allowed to modify	
Device Groups	Name of the device groups associated with a user group	AIM Admin	Not allowed to modify	

Associating Registered Alerts with Organizations

JSS Alerts that the customer registers for using http://www.juniper.net/alerts/ (scroll to the bottom of the page), can be associated with an Organization. The alerts the customer registers for are selected in the Alert Registration table. The customer can ensure that the requested alerts are selected to associate them with the current organization.

The AIM ties into the Juniper Support Systems (JSS) Alert system which allows customers to go the Juniper support web site and register for specific types of alerts are then be e-mailed to them.

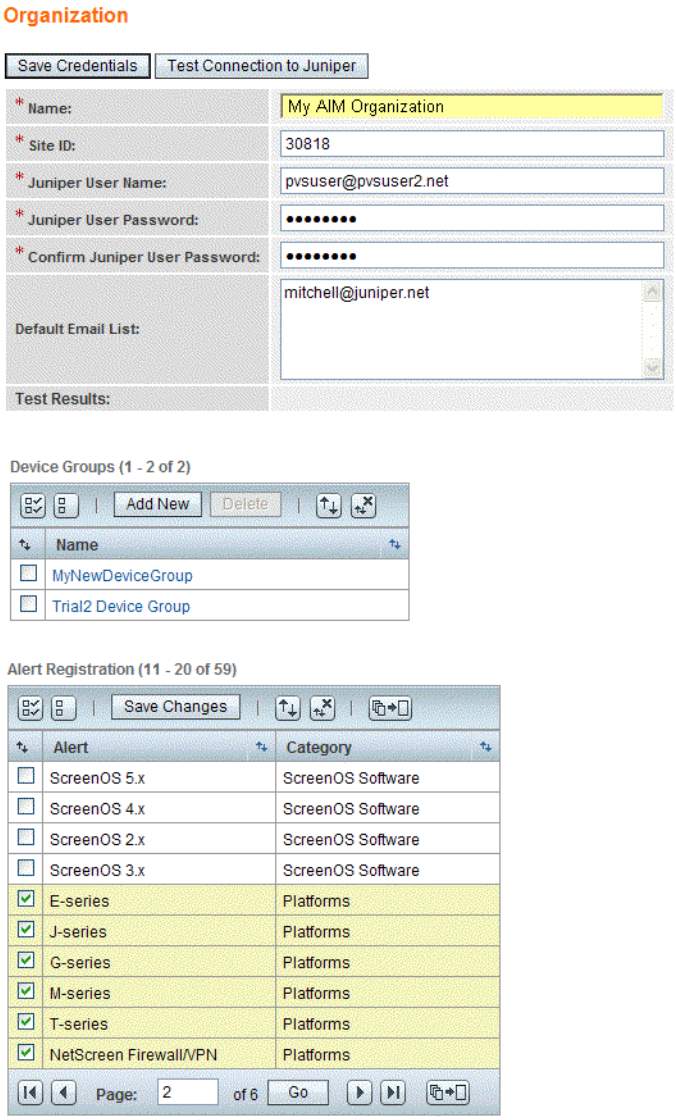
When you register for alerts in AIM, you receive the same information. The difference is instead of receiving the information in e-mail messages, alert messages are received by AIM and displayed in Intelligence Manager. This action provides the customer one central place to receive alerts, a way to manage who is responsible for following up on alerts by assigning alerts to AIM users.

When you click Scan for Impact on an Alert Detail page, you see which devices in the network are impacted by the information received (See “Scanning Intelligence Messages for Impact” on page 123).

When you navigate to the Organization Detail page (see later in this section), the alerts available to register for are retrieved from JSS and are displayed in the Alert Registration table. Those alerts that are checked in the table indicate the ones the organization is already registered to receive. Once you specify the alerts to register for, the Save Changes button registers those alerts with JSS for that Organization.

To associate registered alerts, follow these steps:

1. Click Settings > Organizations. The Organizations page appears. Click the name of the organization to register alerts. This action displays the Organizations page.



   The Alert Registrations table displays the alerts available to register for that are retrieved from Juniper Support Systems. The alerts that the Organization is already registered to receive are checked in the table. See “Alert Registration Table Description” on page 81.

2. Select the alerts that you want to be registered with the Organization.

3. Click Save Changes to register the specified alerts with Juniper Support Systems.

Alert Registration Table Description

Table 39 defines the Alert Registrations table command buttons.

Table 39: Alert Registration Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Registers the selected alerts with Juniper Support Systems	AIM Admin	Enabled when you select an alert.	Registers the selected alert with JSS.

Table 40 defines the Alert Registration table fields.

Table 40: Alert Registration Table Field Descriptions

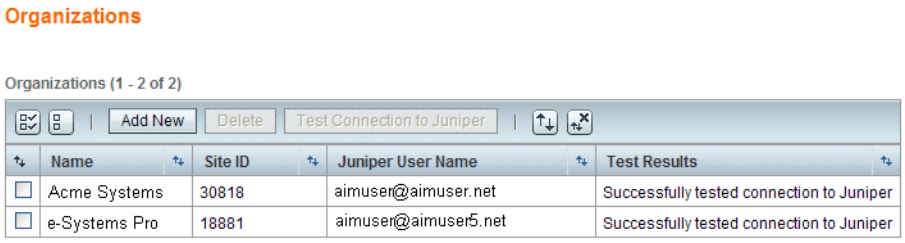
Name	Description	Privileges	Range/ Length	Default
Alert	Type of alert for which to register	Not allowed to modify	N/A	N/A
Category	Category to which the alert belongs	Not allowed to modify	N/A	N/A

Using the Organizations Table

The AIM Organizations table displays an alphabetized listing of organizations by site ID, Juniper user name, and JSSS connection to Juniper test results.

To view the Organizations table, do the following:

1. Click Settings > Organizations. The Organizations table appears with the organizations that have been created.



See “Organization Table Description” on page 82.

Organization Table Description

Table 41 describes the Organizations table command buttons.

Table 41: Organizations Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Add New	Initiates creation of a new Organization	AIM Admin Settings	Available if privilege	Displays initial creation screen of Organization
Delete	Deletes specified organizations	AIM Admin Settings	Available if privilege and one or more organizations are selected	Removes all of the selected organizations from the table.
Test Connection to Juniper	Uses the credentials of the selected organizations to test the connection to Juniper.	None	Enabled if one or more organizations are selected	Displays the result of the test connection to JSS (success or failure) for each of the selected Organizations in the Test Results column

Table 42 defines the Organizations table columns.

Table 42: Alert Registration Table Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	Name of the organization This field is a link and can be used to navigate to the detail screen of the organization	Not allowed to modify	N/A	N/A
Site ID	An identifier used to denote the Customer Site field currently used in the JTAC Clarify system	Not allowed to modify	N/A	N/A
Juniper Username	Login to use for communications with the JTAC Clarify system such as creating cases, and checking for updates to existing cases	Not allowed to modify	N/A	N/A
Test Results	Displays results from the Test Connection to Juniper command: Success or failure	Not allowed to modify	N/A	N/A

Viewing Organization Details

To view organization details page, do the following:

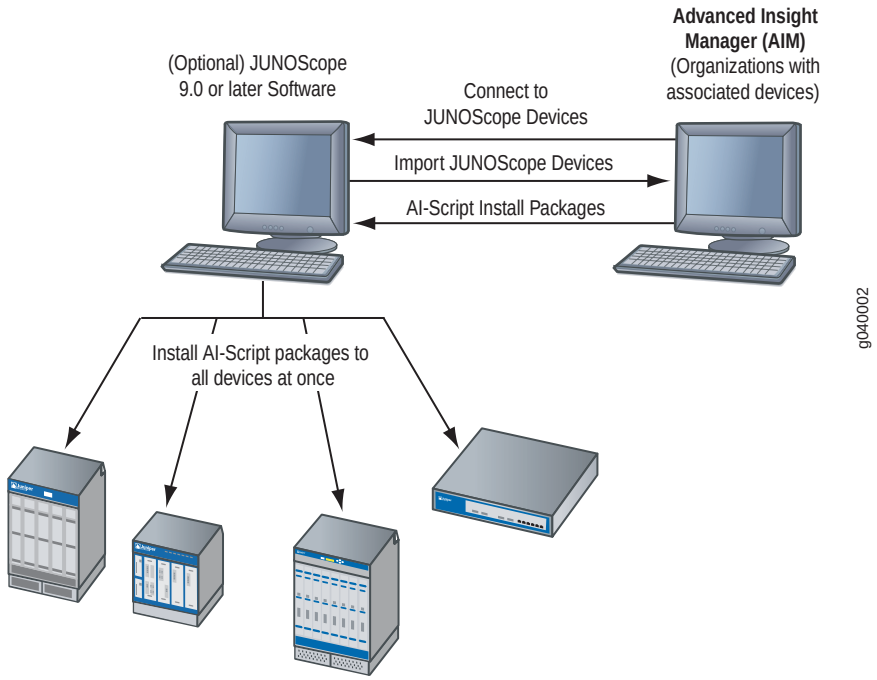
1. Click Settings > Organizations. The Organizations table appears with the organizations that have been created.

2. Click the Organization name link in the table. The to see the setting parameters. The Organization page appears with the credentials and other elements that have been associated, such as device groups and alerts. For more information, see “AIM Organization Page Description” on page 71, “Organization Device Group Page Description” on page 72, and “Alert Registration Table Description” on page 81.

Automatically Installing AI-Script Bundles

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. See Figure 13.

Figure 13: Automatic Installation of AI-Script Install Packages Using JUNOScope



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

1. Configure the credentials used to communicate with JUNOScope, see "Configuring JUNOScope Settings" on page 51.

2. Import devices that are managed by JUNOScope, see "Configuring JUNOScope Settings" on page 51.

3. Configure Script Bundles, see "Configuring Script Bundle Settings" on page 54.

4. Associate imported devices with a device group, see "Creating Device Groups" on page 72.

5. Configure the Script Bundle of the device group and set the No-copy and Unlink installation attributes, see "Creating Device Groups" on page 72

6. Add archive locations specifying the upload command password attributes, see "Configuring Archive Locations" on page 73,

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 41.