

Chapter 15

Creating Reaction Policies

This chapter describes how to create a reaction policy that lets you specify which incidents you want Advanced Insight Manager (AIM) to react on and what actions you want taken.

A reaction policy is a three-step process that requires:

- Trigger types that cause AIM to react to an incident. See “Create Reaction Policy Page Description” on page 155.
- Filters to specifically determine which incidents or intelligence messages to which you want AIM to react. See “Reaction Policy Set Filter Description” on page 156.
- What actions to take once the specified incident or intelligence message is received. See “Reaction Policy Set Actions Description” on page 156.

You can create a reaction policy from the following locations in AIM:

- My AIM Home
- Incident Manager
- Reaction Policies in the AIM navigation pane

You must have reaction policy user privileges to create an AIM incident reaction policy.

Creating a Reaction Policy

To create a reaction policy, follow these steps:

1. In AIM, do one of the following:
 - From the My AIM Home Reaction Policies table, click Create Policy
 - From Incident Manager, click Create Policy
 - Click Reaction Policies in the AIM navigation pane.

The Create Reaction Policy wizard appears.

Create Reaction Policy

Name:

Trigger:

- New Incident Detected
- Incident Reported to Juniper
- JTAC Case ID Assigned
- JTAC Case Updated
- New Intelligence Update Received

2. Type a reaction policy name, then select a trigger. For more information about the Create Reaction Policy page, see “Create Reaction Policy Page Description” on page 155.
3. Click Next Step. The Create Reaction Policy Set Filter page appears.

Create Reaction Policy - Set Filter

Priority: Has the Words:

Device Name: Doesn't have:

Serial Number:

4. Type the required information in the Create Reaction Policy - Set Filter page. For more information, see “Reaction Policy Set Filter Description” on page 156.
5. Click Next Step. The Create Reaction Policy Set Actions page appears.

Create Reaction Policy - Set Actions

Send Email to:

Send Text Message to:

Send Traps to:

Trap Destinations (0)

Name
No items found.

6. Select the action you want AIM to take when the reaction policy criteria is met. For more information, see “Reaction Policy Set Actions Page Description” on page 156.
7. Click Finish. The Reaction Policies table appears.

Reaction Policies

Policies (1 - 3 of 3)

	Name	Owner	Status	Trigger Type	Filter	Action
<input type="checkbox"/>	Software Policy	aimuser1	Disabled	New Incident Detected	Case ID Assigned: (dev-hostid-FF1234-87654321-123456-5)	Email to: (aimuser@xyz.com)
<input type="checkbox"/>	Hardware Policy	aimuser3	Enabled	JTAC Case ID Associated To Event	Incident ID:(dev-hostid-DD6500-20071130-163245-1)	Email to: (aimuser@xyz.com)
<input type="checkbox"/>	Security Policy	aimuser7	Enabled	New Incident Detected	Priority:(1 - Critical) Device Name:(device 007) Serial Number:(HB6665) Has the words:(Critical) Does not have the words:(Submitted)	Email to: (myemailaccount@carrier.com)

For more information about the Reaction Policies table, see “Reaction Policies Table Description” on page 157.

Create Reaction Policy Page Description

Table 73 describes the Create Reaction Policy page.

Table 73: Create Reaction Policy Page Description

Column	Description	Range/Length	Default
Name field	Name of policy, which must be unique within all the policies owned by the same user.	32 characters	N/A
Trigger Type options	<ul style="list-style-type: none"> ■ Specifies the type of trigger that has to happen for this policy to be applied. ■ New Intelligence Update Received trigger is only available if create policy was initiated from the Reaction Policies page ■ New Event Detected trigger is NOT available if any incidents were specified when create policy was initiated 	<ul style="list-style-type: none"> ■ New Event Detected ■ Event Reported to Juniper ■ JTAC Case ID Assigned, ■ JTAC Case Updated ■ New Intelligence Update Received 	N/A

Reaction Policy Set Filter Description

Table 74 describes the Reaction Policy Set Filter page description.

Table 74: Create Reaction Policy Set Filter Field Descriptions

Column	Description	Range/Length	Default
Priority	Matches the priority of incident of the incident <ul style="list-style-type: none"> ■ 1—Critical ■ 2—High ■ 3—Medium ■ 4—Low 	256 characters	Blank
Has the words	For all trigger types: Matches the specified words against any of the fields in the incident or the intelligence update	256 characters	Blank
Device Name	For incident specific trigger types: Matches the name of the device the incident occurred on.	256 characters	Blank
Doesn't have	For all trigger types: Makes sure the specified words are not in any of the fields of the incident or the intelligence update	256 characters	Blank
Serial Number	For all trigger types: Matches serial number of the device the incident occurred on, OR matches the serial number specified in the relevance of the intelligence message	256 characters	Blank

Reaction Policy Set Actions Description

Table 75 describes the options on the Reaction Policies Set Actions page.

Table 75: Reaction Policy Set Actions Page Description

Column	Description	Range/Length	Default
Send Email to	List of email addresses that will be sent an email message if the policy is triggered and passes the specified filter.	65535 characters	Send Email to
Send Text Message to	List of email addresses that will be sent a text message if the policy is triggered and passes the specified filter.	65535 characters	Send Text Message to
Send Traps to	List of trap destinations that will be sent AIM SNMP traps if the policy is triggered and passes the specified filter. Trap destinations in the table are those created in Settings > Trap Destinations.	N/A	N/A

Reaction Policies Table Description

Table 76 describes the Reaction Policies table command buttons.

Table 76: Reaction Policy Table Command Button Descriptions

Element Name	Description	Privileges	Enabled/Disabled
Create Policy	Displays the Reaction Policies wizard for you to perform all the steps to create reaction policy.	AIM Admin	Enabled
Enable	Activates the selected reaction policies.	AIM Admin	Enabled when you select a reaction policy
Disable	Deactivates a selected reaction policy.	AIM Admin	Enabled when you select a reaction policy
Delete	Removes a selected Reaction Policy	AIM Admin	

Table 77 describes the columns in the Reaction Policies table.

Table 77: Reaction Policies Table Column Descriptions

Column	Description	Range/Length	Default
Name	Name of policy that must be unique within all policies owned by the same user.	32	N/A
Owner	User who created the reaction policy	N/A	N/A
Status	Indicates whether the reaction policy is running or not	Enabled or Disabled	N/A
Trigger	Specifies the type of trigger that has to occur for the reaction policy to be applied.	<ul style="list-style-type: none"> ■ New Event Detected ■ Event Reported to Juniper ■ JTAC Case ID Assigned ■ JTAC Case Updated ■ New Intelligence Update Received 	N/A
Filter	Specifies the filter that must be passed for this reaction policy is triggered and the filter is passed.	See Table 74.	N/A
Action	Specifies the action taken if this reaction policy is triggered and the filter has passed.	Table 75	N/A

