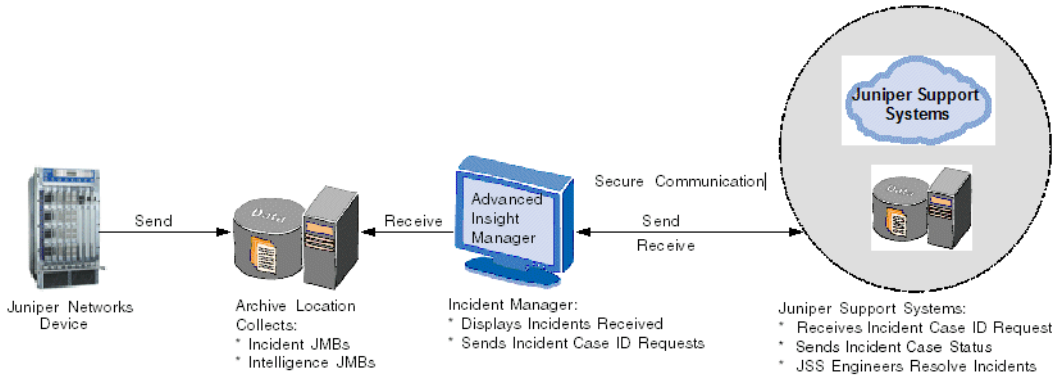
Chapter 13

Using AIM Incident Manager

The Incident Manager provides a view of all incidents received by Advanced Insight Manager. Incidents are displayed alphabetically by organization name and device group.

Figure ___ shows the data flow through which AIM receives incident JMBs and manages them through successful case resolution.

Figure 14: Incident Manager Data Flow Diagram



Juniper Networks devices, configured with specialized AI-Scripts, periodically send incident and intelligence Juniper Message Bundles (JMBs) to a configured archive location. AIM connects to the archive location and periodically receives the incident and intelligence JMBs. Incident Manager displays all of the incident JMBs received. The incident owner sends an incident case ID request to JSS. JSS sends a case ID and opens a case for Juniper engineers to work on a resolution and to send case status back to Intelligence Manager.

To use Incident Manager, you must have AIM admin and AIM ownership privileges. You must also have the AIS Base (Incident-Driven Online Service subscription.

From Incident Manager, you can:

- View an incident detail
- View incident owner
- View incident status

- View case ID
- View whether an incident has been flagged to a user. Clear Flag—Removes the flag from any of the selected Incidents.
- View whether an incident has been submitted to Juniper Support Systems (JSS) for a case to be opened to receive a case ID. Submit Case—submits the selected Incident to JSS so that a case will be created. Submitting a case is only valid if only one incident is selected and if that incident has not already been submitted to the Juniper Homebase.
- Create Policy—Initiates creation of a Reaction Policy. If any Incidents are selected, the policy created will be scoped to just those incidents specified. If no Incidents are selected, then the policy will be applied to all the Incidents in the system.
- Delete any selected Incidents

This chapter includes the following sections:

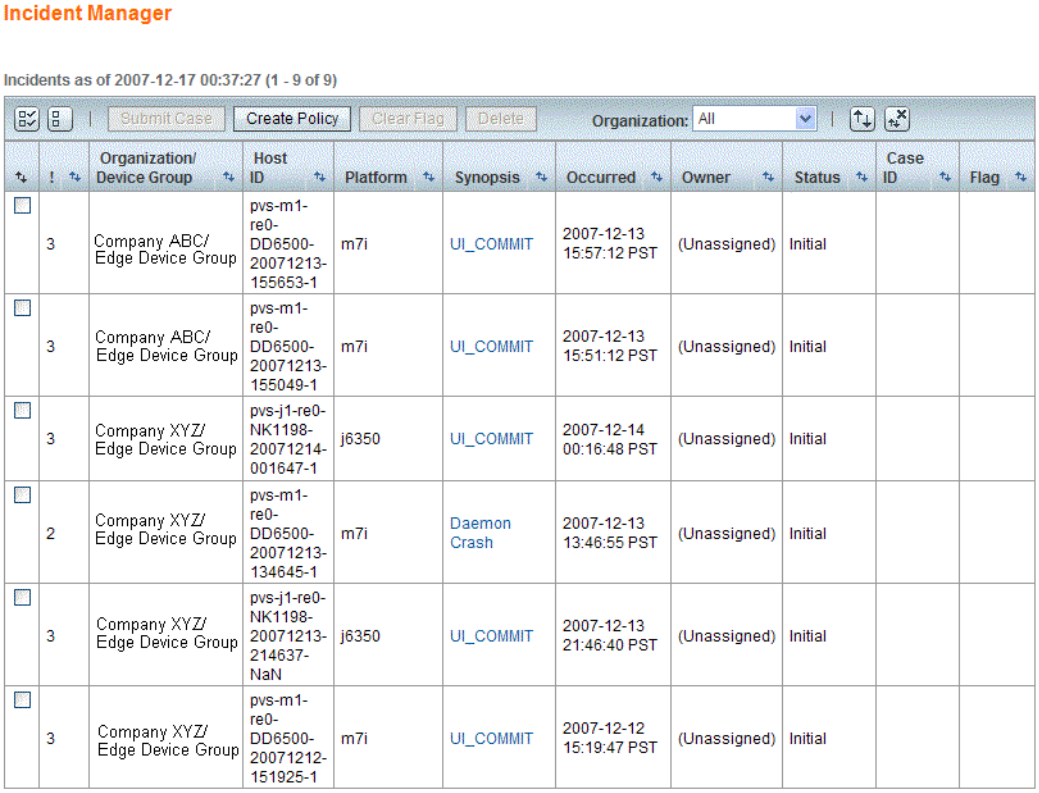
Viewing Incident Manager

You can select to display incidents by all AIM organizations or by ones that you have created. For more information about creating AIM organizations, see "Configuring AIM Organizations and Device Groups" on page 67.

Any incident displayed in bold in Incident Manager indicates that incident has been detected, assigned, or flagged to the user since the last time the user was logged into AIM.

To view the Incident Manager table, do the following:

- Click Incident Manager in the AIM navigation area. The Incident Manager table appears.



Incident Manager Table Element Descriptions

Table 67 describes the Incident Manager table command buttons.

Table 67: Incident Manager Table Command Button Descriptions

Button Name	Description	Privileges	Enabled/ Disabled	Results
Submit Case	Submits the selected Incident to Juniper so that a JTAC case will be created. Note that this action is only valid if only one incident is selected and if that incident has not already been submitted to the Juniper Homebase.			
Create Policy	Initiates creation of a Reaction Policy. If any Incidents are selected, the policy created will be scoped to just those incidents specified. If no Incidents are selected, then the policy will be applied to all the Incidents in the system.			
Clear Flag	Removes the flag from any of the selected Incidents.			

Button Name	Description	Privileges	Enabled/ Disabled	Results
Delete	Removes any selected Incidents			
Organization drop-down list	Lets you select to view incidents for all organizations or by ones that you select that have been created in AIM.			

Table 68 describes the columns in the Incident Manager table.

Table 68: Incident Manager Table Column Descriptions

Column	Description	Range/Length	Default
!	Indicates the priority of the incident received	1-4	Set by the JUNOS device, may be overridden by a Reaction Policy
Host ID	Unique identifier representing the specific incident occurrence.	N/A	Set by the JUNOS system or JUNOScope application if multi-PRB
Platform	Indicates the platform of the device the incident occurred on.	N/A	Set by the JUNOS System
Synopsis	Textual description of the incident. This field is a link and can be used to navigate to the detail screen of the selected Incident. Figure 10 Incident Detail	N/A	Set by the JUNOS system
Occurred	Time that the JUNOS device detected the incident	Date and time	N/A
Owner	User that has currently been assigned ownership for this incident, as well as the owner's status regarding the incident Format: owner (status) See 2.5 Incident Detail for how to assign an owner to an incident	Owner—Any valid user login for AIM Status—assigned, in progress, completed	Unassigned
Status	The status of this incident with regards to AIM. It relates to the interactions between the AIM and the JSS case status.	Initial, Submitted, Created, Updated	Initial
Case ID	The case ID assigned by the Juniper Case Management system. This field is a link and can be used to navigate into the JSS Case Management application. Figure 11 JTAC Case ID - Link to Juniper Case Management	N/A	Empty until case created.
Flag	Indicates if this entry has been flagged to the user for inspection.	N/A	N/A

- For more information about submitting a case request, see “Submitting a Case Request” on page 135
- For more information about creating a reaction policy when an incident is received, see “Creating a Policy” on page 136

- For more information about clearing a flag to a user, see “Clearing a Flag” on page 136
- For more information about viewing incidents by AIM organizations, see “Viewing Incidents by Organization” on page 136
- For more information about viewing incident detail, see “Viewing Incident Detail” on page 137

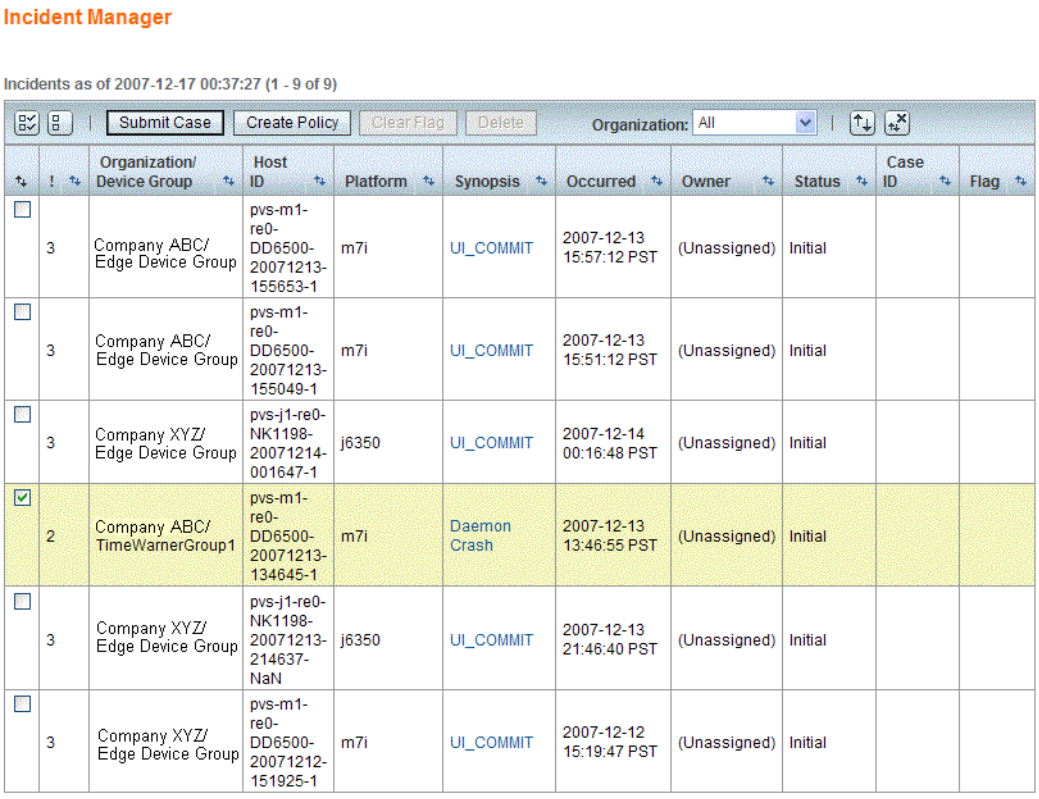
Submitting a Case Request

From the Incident Manager table, you can easily submit a case request from Juniper Support Systems (JSS). Once a case ID is assigned, the Case ID appears in the following places:

- My AIM Home, Incident Manager table
- Incident Manager table
- Incident Detail page

To submit a case ID, follow these steps:

1. From Incident Manager, select an incident for which you want to submit a case ID request. The Submit Case button is enabled.



Click Submit Case. You see the following message:

Successfully submitted case to Juniper: Create Case returned transaction ID

Thereafter, Incident Manager displays the status as Submitted. Then the status changes to Created and the case ID appears in the Case ID column. Finally, the incident is bold.

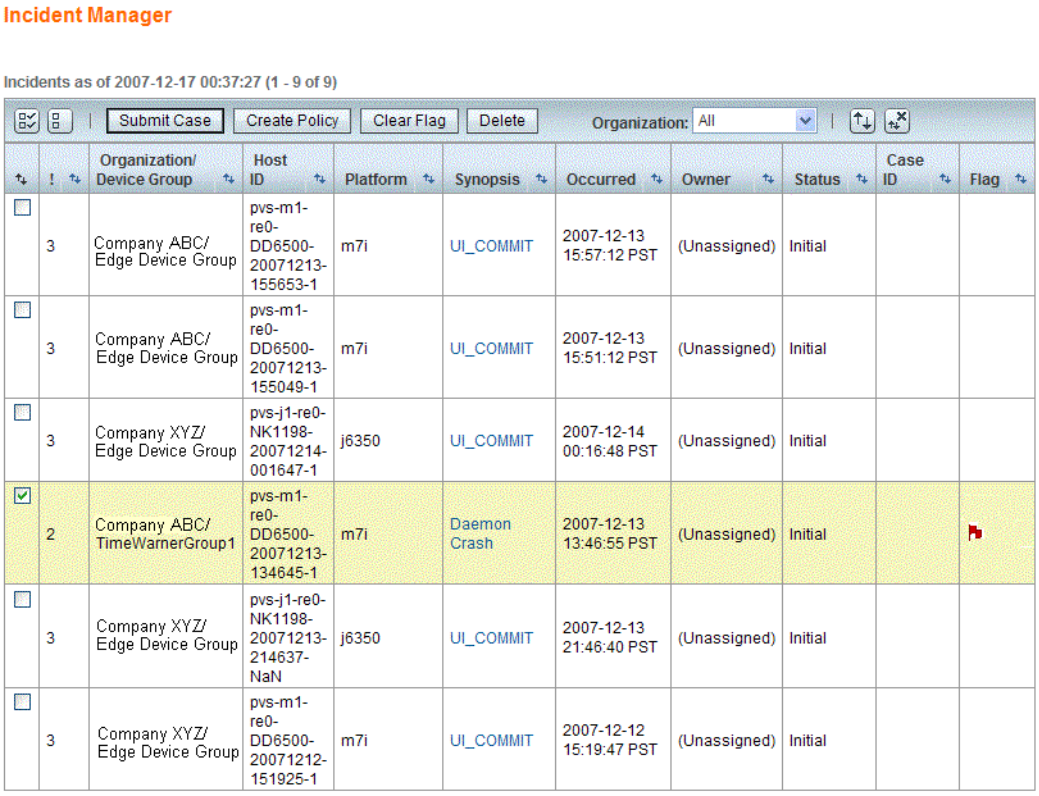
Creating a Policy

For more information about “Creating a Reaction Policy” on page 125.

Clearing a Flag

To clear and flag to a user, follow these steps:

1. In the Incident Manager table, select the incident with the flag that you want to delete. The Clear Flag button is enabled.



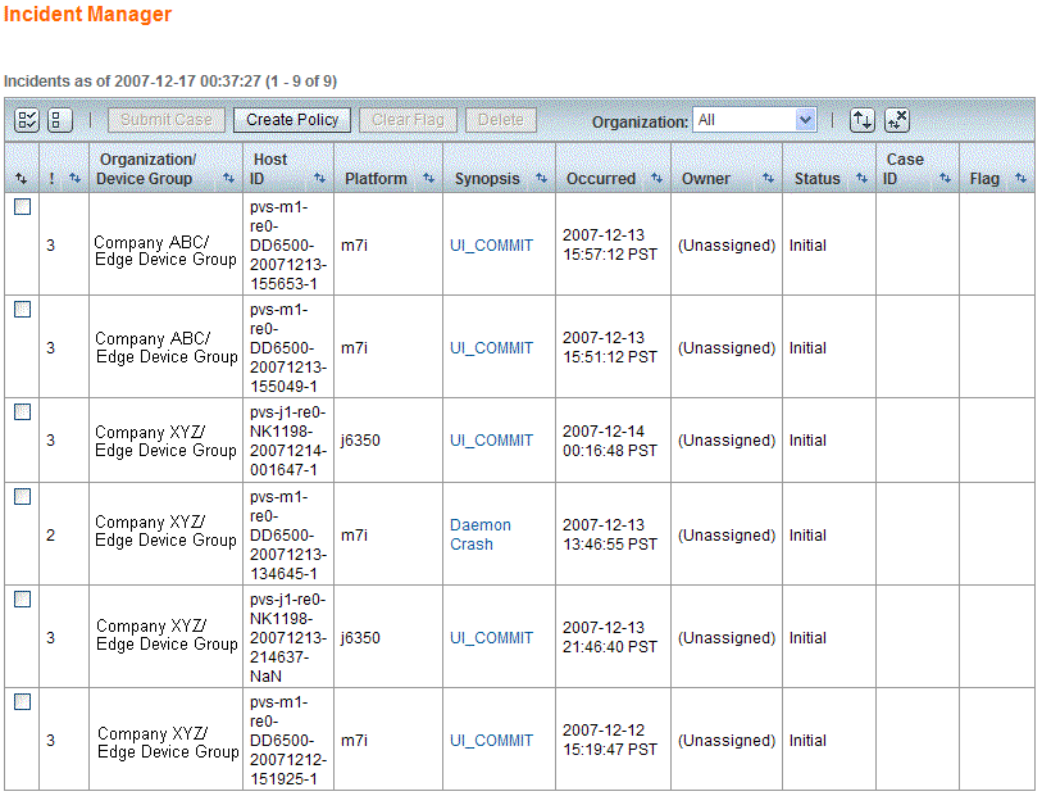
2. Click Clear Flag. The flag is removed, and that incident will no longer appear in the Incidents table in My AIM Home.

Viewing Incidents by Organization

You can view incidents by only the ones that have been collected for a specified AIM organization.

To view incidents by AIM organization, do the following:

- On the Incident Manager table, select the organization that you want from the Organization dro9p down list.



Incident Manager

Incidents as of 2007-12-17 00:37:27 (1 - 9 of 9)

Submit Case | Create Policy | Clear Flag | Delete | Organization: All

	!	Organization/ Device Group	Host ID	Platform	Synopsis	Occurred	Owner	Status	Case ID	Flag
☐	3	Company ABC/ Edge Device Group	pvs-m1-re0-DD6500-20071213-155653-1	m7i	UI_COMMIT	2007-12-13 15:57:12 PST	(Unassigned)	Initial		
☐	3	Company ABC/ Edge Device Group	pvs-m1-re0-DD6500-20071213-155049-1	m7i	UI_COMMIT	2007-12-13 15:51:12 PST	(Unassigned)	Initial		
☐	3	Company XYZ/ Edge Device Group	pvs-j1-re0-NK1198-20071214-001647-1	j6350	UI_COMMIT	2007-12-14 00:16:48 PST	(Unassigned)	Initial		
☐	2	Company XYZ/ Edge Device Group	pvs-m1-re0-DD6500-20071213-134645-1	m7i	Daemon Crash	2007-12-13 13:46:55 PST	(Unassigned)	Initial		
☐	3	Company XYZ/ Edge Device Group	pvs-j1-re0-NK1198-20071213-214637-NaN	j6350	UI_COMMIT	2007-12-13 21:46:40 PST	(Unassigned)	Initial		
☐	3	Company XYZ/ Edge Device Group	pvs-m1-re0-DD6500-20071212-151925-1	m7i	UI_COMMIT	2007-12-12 15:19:47 PST	(Unassigned)	Initial		

Viewing Incident Detail

For more information about viewing incident details, see“Viewing Incident Detail” on page 112.

Viewing Incident Juniper Message Bundle (JMB)

For more information about viewing and incident JMB, see “Viewing a Juniper Message Bundle” on page 114.

Assign an Incident Owner

For more information about assigning an incident owner, see “Assigning an Intelligence Message Owner” on page 120.

Change Incident Owner Status

For more information about changing an incident owner status, see “Changing Incident Owner Status” on page 116.