

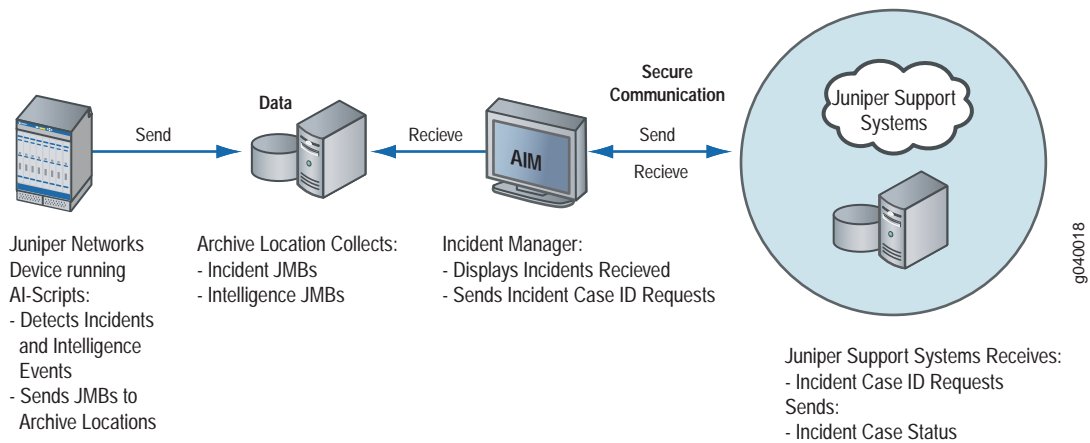
Chapter 13

Using AIM Incident Manager

The Incident Manager provides a view of all incidents received by Advanced Insight Manager. Incidents are problem event Juniper Message Bundles that are detected and deposited in device archive locations. AIM Incident Manager provides a user interface to view incidents alphabetically by organization name and device group.

Figure 14 shows the data flow through which AIM receives incident JMBs and manages them to 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 detailed incident information as described in “Viewing Incident Details (Incident for Device)” on page 135
- Change incident ownership, as described in “Assigning an Incident Owner” on page 138.)
- View and change incident status, as described in “Change Incident Owner Status” on page 138
- Submit and request for a case ID, as described in “Submitting a Case Request” on page 132
- Flag an incident to a user, as described in.
- Clear Flag—Removes the flag from any of the selected Incidents as described in “Clearing a Flag” on page 133.
- 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 JSS. See “Submitting a Case Request” on page 132.
- Create 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. See “Creating Reaction Policies” on page 153
- Delete any selected Incidents. See “Deleting an Incident” on page 139

This chapter includes the following sections:

- Viewing Incident Manager on page 129
- Submitting a Case Request on page 132
- Creating a Policy on page 132
- Clearing a Flag on page 133
- Viewing Incidents by Organization on page 134
- Viewing Incident Details (Incident for Device) on page 135
- Viewing Incident Juniper Message Bundle (JMB) on page 138
- Change Incident Owner Status on page 138
- Deleting an Incident on page 139

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 69.

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

Incidents as of 2008-02-09 01:55:48 (1 - 10 of 40)

<input type="checkbox"/>		Organization/ Device Group	Host ID	Platform	Synopsis	Occurred	Owner	Status	Case ID	Flag
<input type="checkbox"/>	3	ACME Networks/ Northeast	device-01	m10	UL_COMMIT	2008-02-05 20:59:11 PST	NOC-tech-05 (Assigned)	Updated	2008- 0205- 0776	
<input type="checkbox"/>	2	ACME Networks/ Northeast	Prod1- dev-98	m10	Daemon Crash	2008-02-05 20:21:56 PST	admin-Prod-1 (Assigned)	Updated	2008- 0205- 0777	
<input type="checkbox"/>	3	BEST Networks/ Region-075	Net-005- dev-047	m10	UL_COMMIT	2008-01-31 10:26:16 PST	NOC-tech-05 (Assigned)	Updated	2008- 0204- 0772	
<input type="checkbox"/>	3	BEST Networks/ Region-075	device-666	m10	UL_COMMIT	2008-01-31 10:24:15 PST	NOC-tech-07 (Assigned)	Updated	2008- 0205- 0774	

Incident Manager Table Element Descriptions

Table 62 describes the Incident Manager table command buttons.

Table 62: 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 JSS.	AIM User	Enabled when you select an incident.	Case ID submitted message appears.
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.	AIM User	Always enabled	Displays Reaction Policies page.
Clear Flag	Removes the flag from any of the selected Incidents.	AIM User	Enabled when you select an incident.	Removes flag.
Delete	Removes any selected Incidents	AIM User	Enabled when you select an incident.	Removes incident.
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.	AIM User	Always enabled	Displays only incidents from selected organization.

Table 63 describes the columns in the Incident Manager table.

Table 63: Incident Manager Table Column Descriptions (1 of 2)

Column	Description	Range/Length	Default
!	Indicates the priority of the incident received <ul style="list-style-type: none"> ■ 1—Critical ■ 2—High ■ 3—Medium ■ 4—Low 	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	Text 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

Table 63: Incident Manager Table Column Descriptions (2 of 2)

Column	Description	Range/Length	Default
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)	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

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.

Incident Manager

Incidents as of 2008-02-09 01:55:48 (1 - 10 of 40)

		Organization/ Device Group	Host ID	Platform	Synopsis	Occurred	Owner	Status	Case ID	Flag
<input checked="" type="checkbox"/>	3	ACME Networks/ Northeast	device-01	m10	UL_COMMIT	2008-02-05 20:59:11 PST	NOC-tech-05 (Assigned)	Updated		
<input type="checkbox"/>	2	ACME Networks/ Northeast	Prod1- dev-98	m10	Daemon Crash	2008-02-05 20:21:56 PST	admin-Prod-1 (Assigned)	Updated		
<input type="checkbox"/>	3	BEST Networks/ Region-075	Net-005- dev-047	m10	UL_COMMIT	2008-01-31 10:26:16 PST	NOC-tech-05 (Assigned)	Updated		
<input type="checkbox"/>	3	BEST Networks/ Region-075	device-666	m10	UL_COMMIT	2008-01-31 10:24:15 PST	NOC-tech-07 (Assigned)	Updated		

2. 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 detailed information about creating a reaction policy, see “Using AIM Incident Manager” on page 127.

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.

Incident Manager

Incidents as of 2008-02-09 01:55:48 (1 - 10 of 40)

		Submit Case	Create Policy	Clear Flag	Delete	Organization: All				
		Organization/ Device Group	Host ID	Platform	Synopsis	Occurred	Owner	Status	Case ID	Flag
<input type="checkbox"/>	3	ACME Networks/ Northeast	device-01	m10	UL_COMMIT	2008-02-05 20:59:11 PST	NOC-tech-05 (Assigned)	Updated	2008- 0205- 0776	
<input type="checkbox"/>	2	ACME Networks/ Northeast	Prod1- dev-98	m10	Daemon Crash	2008-02-05 20:21:56 PST	admin-Prod-1 (Assigned)	Updated	2008- 0205- 0777	
<input type="checkbox"/>	3	BEST Networks/ Region-075	Net-005- dev-047	m10	UL_COMMIT	2008-01-31 10:26:16 PST	NOC-tech-05 (Assigned)	Updated	2008- 0204- 0772	
<input type="checkbox"/>	3	BEST Networks/ Region-075	device-666	m10	UL_COMMIT	2008-01-31 10:24:15 PST	NOC-tech-07 (Assigned)	Updated	2008- 0205- 0774	

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 drop-down list.

Incident Manager

Incidents as of 2008-02-09 01:55:48 (1 - 10 of 40)

<input type="checkbox"/> <input type="checkbox"/> <input type="button" value="Submit Case"/> <input type="button" value="Create Policy"/> <input type="button" value="Clear Flag"/> <input type="button" value="Delete"/> Organization: All <input type="button" value="↑↓"/> <input type="button" value="✕"/> <input type="button" value="🔍"/>										
<input type="checkbox"/>	<input type="checkbox"/>	Organization/ Device Group	Host ID	Platform	Synopsis	Occurred	Owner	Status	Case ID	Flag
<input type="checkbox"/>	3	ACME Networks/ Northeast	device-01	m10	UL_COMMIT	2008-02-05 20:59:11 PST	NOC-tech-05 (Assigned)	Updated	2008- 0205- 0776	
<input type="checkbox"/>	2	ACME Networks/ Northeast	Prod1- dev-98	m10	Daemon Crash	2008-02-05 20:21:56 PST	admin-Prod-1 (Assigned)	Updated	2008- 0205- 0777	
<input type="checkbox"/>	3	BEST Networks/ Region-075	Net-005- dev-047	m10	UL_COMMIT	2008-01-31 10:26:16 PST	NOC-tech-05 (Assigned)	Updated	2008- 0204- 0772	
<input type="checkbox"/>	3	BEST Networks/ Region-075	device-666	m10	UL_COMMIT	2008-01-31 10:24:15 PST	NOC-tech-07 (Assigned)	Updated	2008- 0205- 0774	

Viewing Incident Details (Incident for Device)

To view incident details, click the incident Synopsis link in the Incidents table. The Incident for Device page appears. For more information about viewing incident details, see “Viewing Incident Detail” on page 112.

Incident for Device: dev-hostid at 2007-12-12 03:50:14 PST

<input type="button" value="Submit Case"/> <input type="button" value="Save Changes"/> <input type="button" value="Create Policy"/> <input type="button" value="Flag to Users"/> <input type="button" value="View JMB"/>	
Priority:	3 - Medium
Status:	Initial
Case ID:	
Host ID:	dev-hostid
Synopsis:	UL_COMMIT
Organization:	organization-01
Platform:	j4350
Serial Number:	JN109283BADA
Problem Description:	Error on commit.
Release:	9.0
Version:	10
Email List:	andy@company.net, peter@company.net, phillip@company.net, robert@company.net
Received:	2007-12-11 22:33:34.0
Owner:	
Owner Status:	Unassigned
Flagged to Users:	

For more information about the Incident Detail (Incident for Device), see “Incident Details (Incident for Device) Page Description” on page 135

Incident Details (Incident for Device) Page Description

Table 64 describes the fields on the Incident for Device page.

Table 64: Incident for Device Command Button Descriptions (1 of 2)

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 JSS.	AIM User	Enabled when you select an incident.	Case ID submitted message appears.
Save Changes	Saves changes of any modified fields. Priority and Email List cannot be modified if the incident has already been submitted to JSS.	AIM User	Always enabled	Saves changes to AIM database.
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.	AIM User	Always enabled	Displays Reaction Policies page.

Table 64: Incident for Device Command Button Descriptions (2 of 2)

Button Name	Description	Privileges	Enabled/Disabled	Results
Flag to Users	Sets which user the incident is flagged for attention and review.	AIM User	Enabled when you select an incident.	Removes the flag.
View JMB	Displays detailed information about the selected incident.	AIM User	Enabled when you select an incident.	Displays the View JMB page

Table 65 describes the columns in the Incident Manager table.

Table 65: Incident Manager Table Column Descriptions (1 of 2)

Column	Description	Range/Length	Default
Priority	Indicates the priority of the selected incident <ul style="list-style-type: none"> ■ 1—Critical ■ 2—High ■ 3—Medium ■ 4—Low 	1-4	Set by the device. The priority can be overridden by a reaction policy
Status	The status of this incident with regards AIM. It relates to the interaction between AIM and JSS case status	Initial, Submitted, Created, and Updated	Sent by JSS.
Case ID	The case ID used by the JSS system. This field provides a link to navigate to the JSS Case Management page.	N/A	Empty until a case is created.
Host ID	Unique identifier representing the specific incident.	N/A	Set by the JUNOS system or AIM if multiple JMBs
Synopsis	Text description of the incident	N/A	Set by the JUNOS system
Platform	Indicates the device platform on which the incident occurred	N/A	Set by the JUNOS system
Problem Description	A description of the incident specified by the device	N/A	Set by the JUNOS system
Release	Release of JUNOS software running on the device	N/A	Set by the JUNOS system
Version	Version of JUNOS software running on the device	N/A	Set by the JUNOS system
Email List	List of e-mail addresses to be sent a message when a case is submitted to JSS	65535 characters	You set the e-mail list in AIM general settings
Received	Time that the incident was detected by AIM	Date and time	N/A
Owner	User that has currently been assigned ownership of this incident	Any valid user login for AIM	Bland

Table 65: Incident Manager Table Column Descriptions (2 of 2)

Column	Description	Range/Length	Default
Owner Status	Incident owner's status regarding the resolution of the incident	Unassigned, Assigned, In progress, and Completed	Unassigned
Flagged to Users	List of users to which the current incident has been flagged or notified	N/A	Blank

The Incident for Details page lets you perform the following AIM actions:

- Submit a case, as described in “Submitting a Case Request” on page 132.
- Create an incident reaction policy, as described in “Creating a Policy” on page 132.
- Flag an incident to a user, as described in “Flagging an Incident To a User” on page 137.
- View an incident Juniper Message Bundle (JMB), as described in “Viewing Incident Juniper Message Bundle (JMB)” on page 138
- Change Incident owner status, as described in “Change Incident Owner Status” on page 138

Flagging an Incident To a User

Flagging an incident is used to inform other users who might be impacted or need to be aware of an incident.

To flag an incident to a user, follow these steps:

1. From My AIM Home, click the incident synopsis link. The Incident Detail page appears.
2. On the Incident Detail page, click Flag to Users. The Flag To Users page appears.

Flag to Users

The screenshot shows a web interface for selecting users to flag an incident to. At the top, there are icons for a list, a grid, a 'Save' button, and arrows for sorting. Below this is a table with a header 'User' and a list of user names. Each name has a checkbox to its left. The checked users are abcuser, admin, martha, and roberto. The unchecked users are aimuser, anewuser, demo, userxyz, and victor.

User
<input checked="" type="checkbox"/> abcuser
<input checked="" type="checkbox"/> admin
<input type="checkbox"/> aimuser
<input type="checkbox"/> anewuser
<input type="checkbox"/> demo
<input checked="" type="checkbox"/> martha
<input checked="" type="checkbox"/> roberto
<input type="checkbox"/> userxyz
<input type="checkbox"/> victor

3. On the Flag to Users page, select the user(s) to which you want to flag the incident.

4. Click Save. A flag appears in the incident Flag column in My AIM Home.

Viewing Incident Juniper Message Bundle (JMB)

The Juniper Message Bundle (JMB) contains the information that JSS needs to analyze and resolve cases and to prevent the incident from reoccurring. For more information about the JMB, see “JMB Contents” on page 39.

To view an incident’s Juniper message bundle, follow these steps:

1. From My AIM Home or Incident Manager, click the incident synopsis link. The Incident detail page appears.
2. On the Incident detail page, click View JMB. The JMB detail page appears.

View JMB: dev-hostid_PvS_prob_20071201_003445.xml

(Information as received by Router)

MANIFEST

Host Event ID:	dev-hostid-DD6500-20071130-163245-1
Service Type:	event
Event Time:	2007-11-30 16:33:05 PST
Problem Class:	support
Problem Synopsis:	UI_COMMIT
Problem Description:	Error on commit.
Problem Severity:	3
Problem Priority:	3
Core File Path:	
Serial Number:	

Router Information

Product Name:	m7i
Host Name:	pvs-m1-re0
OS Platform:	junos

Master Routing Engine

Name:	Routing Engine 0
Mastership State:	Online Master

Assigning 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.

Deleting an Incident

To delete an incident from the Incidents table, follow these steps:

1. In the Incident Manager table, select the incident(s) you want to delete. This action enables the Delete button.
2. Click Delete. The selected incidents are removed from the AIS database.

