Tracking Faults Using Prime Network Events

The following topics describe how to use Cisco Prime Network Events (Prime Network Events) to view and manage faults:

User Roles Required to Work with Prime Network Events

This topic identifies the roles that are required to work with Prime Network Events. Prime Network determines whether you are authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect elements), authorization is based on the default permission that is assigned to your user account. Only users with the Administrator role can log into Prime Network Events.
- For element-based tasks (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

For more information on user authorization, see the topic on device scopes in the *Cisco Prime Network 4.0 Administrator Guide*.

Launching Prime Network Events

To launch Prime Network Events, choose **Start > Programs > Cisco Prime Network >** ***gateway IP address*** **>** Cisco Prime Network Events, and enter your username and password. If any client updates are available, Prime Network automatically installs them.

Note If Prime Network is integrated with the suite, launch Prime Network Events from Prime Central. Choose **Assure > Prime Network > Events** in the menu bar. The Prime Network Events application is opened in a separate window.

Setting Up Your Events View

The Prime Network Events Options dialog box enables you to change various aspects of the event display in Prime Network Events. To set up your events view, choose **Tools > Options** from the main menu. Table 8-1 lists the available options.

Table 8-1 Options for Changing Prime Network Events GUI Client

Option	Description
Save last filter	Saves the filter criteria defined per event type in the Filter Events dialog box. The filter criteria are available the next time you log into Prime Network Events. **Note** Events are not filtered automatically when you next log into Prime Network Events unless the *Open Events with saved filter* option is also selected.
Open Prime Network Events with saved filter	When enabled, applies the previously defined filter to the events as soon as you log into Prime Network Events. The events are continuously filtered according to the defined settings, even after you close the application.
Display *n* records per page	Specifies the number of events to be displayed per page.
Export *n* records in total	Sets the maximum number of events to be exported to a file.
Run auto refresh every *n* secs	Automatically refreshes the Prime Network Events display after the specified number of seconds. **Note** This option uses rapid refresh from the database, which can affect the performance of other vital database options.
Display data for the last *n* hours	Displays past events from the specified number of hours. Values range from 1 to 336 hours (14 days), with a default of 2 hours. If you increase the number of hours, it can take longer for the events to be displayed.
Find mode (No automatic data retrieval)	Operates the Prime Network Events window in Find mode. In this mode, no events will be retrieved from the database when you open the application or switch between tabs. You can click the Find button in the toolbar to search for the events you need. When in Find mode, the status bar in the Prime Network Events window shows "Find Mode (no automatic data retrieval)."

Viewing Events and Tickets in Cisco Prime Network Events

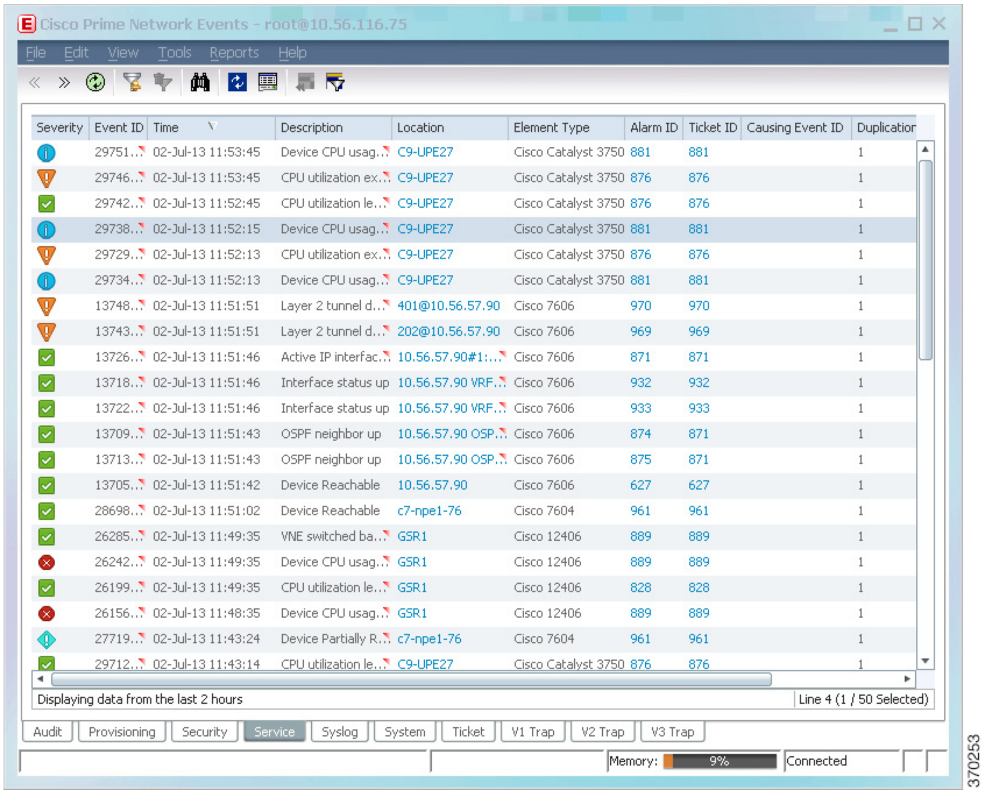
Events are displayed according to event categories, which are represented by tabs in the Cisco Prime Network Events window. Each tab displays an events list log that provides event information for the specific event category. Events can be of system type or network type. The Ticket tab displays the tickets that have been generated for correlated events. Events and tickets are sorted by date, with the latest item displayed first and the oldest item displayed last.

> **Note** Cisco Prime Network Events displays active events only. It does not display events that have been archived. To see archived events, use Prime Network's reporting functionality. For more information, see the Cisco Prime Network Operations Reports User Guide.

Prime Network Events displays events for the last two hours by default. To modify the default number of hours for which events are displayed, see Setting Up Your Events View, page 8-2. Increasing the number of hours can affect how long it takes for the events to be displayed.

Figure 8-1 shows an example of the Prime Network Events window.

Figure 8-1 Prime Network Events Window



Severity	Event ID	Time	Description	Location	Element Type	Alarm ID	Ticket ID	Causing Event ID	Duplication
ⓘ	29751...	02-Jul-13 11:53:45	Device CPU usag...	C9-UPE27	Cisco Catalyst 3750	881	881		1
▼	29746...	02-Jul-13 11:53:45	CPU utilization ex...	C9-UPE27	Cisco Catalyst 3750	876	876		1
✓	29742...	02-Jul-13 11:52:45	CPU utilization le...	C9-UPE27	Cisco Catalyst 3750	876	876		1
ⓘ	29738...	02-Jul-13 11:52:15	Device CPU usag...	C9-UPE27	Cisco Catalyst 3750	881	881		1
▼	29729...	02-Jul-13 11:52:13	CPU utilization ex...	C9-UPE27	Cisco Catalyst 3750	876	876		1
ⓘ	29734...	02-Jul-13 11:52:13	Device CPU usag...	C9-UPE27	Cisco Catalyst 3750	881	881		1
▼	13748...	02-Jul-13 11:51:51	Layer 2 tunnel d...	401@10.56.57.90	Cisco 7606	970	970		1
▼	13743...	02-Jul-13 11:51:51	Layer 2 tunnel d...	202@10.56.57.90	Cisco 7606	969	969		1
✓	13726...	02-Jul-13 11:51:46	Active IP interfac...	10.56.57.90#1:...	Cisco 7606	871	871		1
✓	13718...	02-Jul-13 11:51:46	Interface status up	10.56.57.90 VRF...	Cisco 7606	932	932		1
✓	13722...	02-Jul-13 11:51:46	Interface status up	10.56.57.90 VRF...	Cisco 7606	933	933		1
✓	13709...	02-Jul-13 11:51:43	OSPF neighbor up	10.56.57.90 OSP...	Cisco 7606	874	871		1
✓	13713...	02-Jul-13 11:51:43	OSPF neighbor up	10.56.57.90 OSP...	Cisco 7606	875	871		1
✓	13705...	02-Jul-13 11:51:42	Device Reachable	10.56.57.90	Cisco 7606	627	627		1
✓	28698...	02-Jul-13 11:51:02	Device Reachable	c7-npe1-76	Cisco 7604	961	961		1
✓	26285...	02-Jul-13 11:49:35	VNE switched ba...	GSR1	Cisco 12406	889	889		1
⊗	26242...	02-Jul-13 11:49:35	Device CPU usag...	GSR1	Cisco 12406	889	889		1
✓	26199...	02-Jul-13 11:49:35	CPU utilization le...	GSR1	Cisco 12406	828	828		1
⊗	26156...	02-Jul-13 11:48:35	Device CPU usag...	GSR1	Cisco 12406	889	889		1
◆	27719...	02-Jul-13 11:43:24	Device Partially R...	c7-npe1-76	Cisco 7604	961	961		1
✓	29712...	02-Jul-13 11:43:14	CPU utilization le...	C9-UPE27	Cisco Catalyst 3750	876	876		1

Displaying data from the last 2 hours

Line 4 (1 / 50 Selected)

Event Severity Indicators

The Severity column contains color-coded icons that reflect the severity of the event. An icon appears for each ticket or event in the Prime Network Events tabs (based on its severity) as shown in Table 8-2.

Table 8-2 Severity Indicators

Icon	Color	Severity	Icon	Color	Severity
⊗	Red	Critical	◆	Light Blue	Warning
▼	Orange	Major	ⓘ	Medium Blue	Information

Table 8-2 Severity Indicators (continued)

Icon	Color	Severity	Icon	Color	Severity
⚠	Yellow	Minor	?	Dark blue	Indeterminate
✓	Green	Cleared, Normal, or OK			

Event Types and Categories

Events are grouped in tabs according to type. Each tab displays basic information about the events, including severity, event ID, time, and description. In addition, most event tabs show the Location parameter, which indicates the entity that triggered the event and is a hyperlink that can be clicked to access the entity’s properties.

Note Prime Network stores events in the database in Greenwich Mean Time (GMT) format. The Prime Network client converts events to the time zone that is configured on the client workstation. The times displayed in the Cisco Prime Network Events GUI reflect the time according to the client workstation.

The following categories of events can be viewed in Prime Network Events:

- Audit Events, page 8-4
- Provisioning Events, page 8-5
- Security Events, page 8-5
- System Events, page 8-6
- Service Events, page 8-6
- Syslogs, page 8-7
- V1 Traps, page 8-7
- V2 Traps, page 8-8
- V3 Traps, page 8-8

In addition to events, you can also view and manage tickets in Prime Network Events. See Tickets, page 8-9 for more information.

Audit Events

Events related to all login activity and audit of other activities of the system users. The Audit tab displays the following parameters that specifically relate to audit events:

Table 8-3 Audit Events

Column	Description
Command Name	Audit-specific command name, prefaced by, for example, Get, Update, or Find.
Command Signature	Actual command run by Prime Network, such as **GetEventViewerProperties**.
Command Parameters	Command parameters issued with the command identified in the Command Name column.
Originating IP	IP address of the client that issued the command.
User Name	Name of the user who initiated the command.

Provisioning Events

Events displayed in the Provisioning tab are events triggered during the configuration of a device, for example, execution of a configuration script.

The Provisioning tab displays the following parameters that specifically relate to provisioning events:

Table 8-4 Provisioning Events

Column	Description
Prime Login Username	Username of the logged in user.
VNE Login Username	Username that was used to access the device. This field shows “From VNE Login” except in cases where different device access credentials were specified when executing a configuration command. ‘From VNE Login’ means that the username specified when creating the VNE is being used.
Status	Status of the provisioning activity, such as Success or Fail.

Security Events

Security events are related to client login and user activity when managing the system and the environment.

The Security tab displays the following parameters that specifically relate to security events:

Table 8-5 Security Events

Column	Description
Username	Name of the logged in user.
Originating IP	IP address of the client where the event was triggered.

For more information about the system security events displayed in this tab, see *Cisco Prime Network Supported System and Security Events*.

System Events

System events are related to the everyday working of the internal system and its components, such as alarm thresholds, disk space and AVMs.

The System tab displays the following parameters

Table 8-6 System Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Severity Indicators, page 8-3.
Event ID	Identifier of the event, assigned sequentially.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “AVM 77 is shutting down. Unit = 11.22.33.444.”
Location	Entity that triggered the event.

For more information about the system error and event messages displayed in this tab, see *Cisco Prime Network 4.0 Supported System and Security Events*.

Service Events

Service events are network events such as link down events, adaptive polling events, BGP neighbor loss events, and so on.

The Service tab displays the following parameters that specifically relate to service events.

Table 8-7 Service Tab

Column	Description
Element Type	The type of element that triggered the root event, e.g., Cisco 7606.
Alarm ID	Hyperlinked identifier of the alarm associated with the event. Click the link to view the Ticket Properties window.
Ticket ID	Hyperlinked identifier of the ticket associated with the event. Click the link to view the Ticket Properties window.
Causing Event ID	Identifier of the causing event.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

For more information about the service alarms that are displayed in this tab, see *Cisco Prime Network 4.0 Supported Service Alarms*.

Syslogs

Syslogs are received from the devices by the VNEs, and syslog events are generated.

The Syslog tab displays the following parameters that specifically relate to syslog events.

Table 8-8 Syslog Tab

Column	Description
Element Type	The type of element that triggered the root event, e.g., Cisco 7606.
Alarm ID	Hyperlinked identifier of the alarm associated with the event. Click the link to view the Ticket Properties window.
Ticket ID	Hyperlinked identifier of the ticket associated with the event. Click the link to view the Ticket Properties window.
Causing Event ID	Identifier of the causing event.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

V1 Traps

The V1 Trap tab displays the following parameters that relate specifically to V1 traps:

Table 8-9 V1 Trap Tab

Column	Description
Element Type	The type of element that triggered the root event, e.g., Cisco 7606.
Alarm ID	Identifier of the alarm associated with the event, hyperlinked to the Alarm Properties window.
Ticket ID	Hyperlinked sequential identifier of the ticket. Click the link to view the Ticket Properties window.
Causing Event ID	Identifier of the causing event, hyperlinked to the Network Event Properties window.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

For more information about traps, see *Cisco Prime Network Supported Traps*.

V2 Traps

The V2 Trap tab displays the following parameters that relate specifically to V2 traps:

Table 8-10 V2 Trap Tab

Column	Description
Element Type	The type of element that triggered the root event, e.g., Cisco 7606.
Alarm ID	Identifier of the alarm associated with the event, hyperlinked to the Alarm Properties window.
Ticket ID	Sequential identifier of the ticket, hyperlinked to the Ticket Properties window.
Causing Event ID	Identifier of the causing event, hyperlinked to the Network Event Properties window.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

For more information about the Cisco IOS and Cisco IOX traps displayed in this tab, see *Cisco Prime Network Supported Traps*.

V3 Traps

The V3 Trap tab displays the following parameters that relate specifically to V3 traps:

Table 8-11 V3 Trap Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Severity Indicators, page 8-3.
Event ID	Calculated correlation identifier.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Enterprise generic trap.”
Location	Hyperlink to the entity that triggered the trap.
Element Type	The type of element that triggered the root event, e.g., Cisco 7606.
Alarm ID	Identifier of the alarm associated with the event, hyperlinked to the Alarm Properties window.
Ticket ID	Sequential identifier of the ticket, hyperlinked to the Ticket Properties window.
Causing Event ID	Identifier of the causing event, hyperlinked to the Network Event Properties window.

Table 8-11 V3 Trap Tab (continued)

Column	Description
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Trap Type OID	Trap object identifier.
Translated Enterprise	Translation of the OID using the MIB. For example, an enterprise OID of .1.3.6.1.2.1.88.2 is displayed in this column as .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIB NotificationPrefix.
Enterprise	Enterprise OID for the trap, representing the company or organization that is associated with the trap.

For more information about the Cisco IOS and Cisco IOX traps displayed in this tab, see *Cisco Prime Network 4.0 Supported Traps*.

Tickets

The Ticket tab displays detailed information specific to tickets. For information about viewing and managing tickets in Prime Network Vision, see Working with Tickets in Prime Network Vision, page 9-1.

Table 8-12 describes the information that is displayed in the Ticket tab.

Table 8-12 Ticket Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the ticket (the color and type of alarm are displayed in the Ticket Properties window Severity field). See Event Severity Indicators, page 8-3.
Ticket ID	Sequentially assigned identifier of the ticket, hyperlinked to the Ticket Properties window.
Notes	An icon in this column indicates that a note has been added for the ticket. Click on the icon to read the note and add your own note, if necessary.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Description	Description of the event, such as “Layer 2 tunnel down.”
Location	Hyperlink to the entity that triggered the event.
Element Type	The type of element that triggered the root event, e.g., Cisco 7606.

Table 8-12 Ticket Tab (continued)

Column	Description
Acknowledged	Whether the ticket is acknowledged or has been modified: Yes, No, or Modified. If a ticket changes after it has been acknowledged, it is marked as Modified. If an acknowledged ticket is deacknowledged, the status changes from Yes to No in this column.
Creation Time	Date and time that the ticket was created.
Event Count	Number of events associated with the ticket.
Affected Devices Count	Number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).
Duplication Count	For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
Reduction Count	Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Ticket Properties window displays one reduction count for each event listed. For more information, see Chapter 9, "Working with Tickets in Prime Network Vision."
Alarm Count	Total number of alarms associated with the ticket, including the root alarm.

For information about viewing ticket properties, see Viewing Ticket Properties, page 8-14.

Working with Cisco Prime Network Events

The following topics describe how to view, filter, and display the properties of specific events and tickets, and how to refresh and export events:

- Viewing Event Properties, page 8-10
- Viewing Ticket Properties, page 8-14
- Refreshing Cisco Prime Network Events Information, page 8-17
- Filtering Events, page 8-18
- Exporting Displayed Data, page 8-21

Viewing Event Properties

Cisco Prime Network Events enables you to view the properties of a specific event type. The Event Properties window displays detailed information about the event; for example, the severity and the number of affected parties.

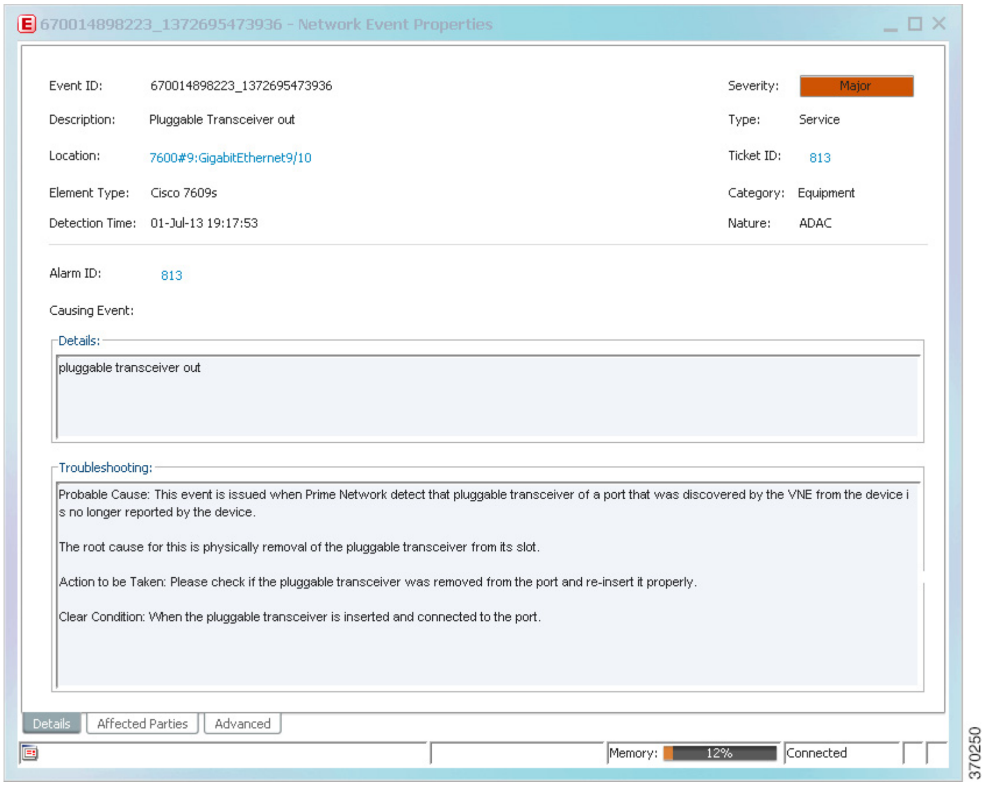
Tip Clicking the **Details** tab on the Event Properties window displays the properties of the selected ticket or event in the Properties pane.

To view event properties:

Step 1 Select the required tab for the specific event type.

Step 2 Select an event and choose **View > Properties** from the main menu. The event properties are displayed for the selected event, either in the lower portion of the Cisco Prime Network Events window or in a separate window as shown in Figure 8-2. The Details tab is displayed by default.

Figure 8-2 Network Event Properties Window - Details Tab



670014898223_1372695473936 - Network Event Properties

Event ID:	670014898223_1372695473936	Severity:	Major
Description:	Pluggable Transceiver out	Type:	Service
Location:	7600#9:GigabitEthernet9/10	Ticket ID:	813
Element Type:	Cisco 7609s	Category:	Equipment
Detection Time:	01-Jul-13 19:17:53	Nature:	ADAC

Alarm ID: 813

Causing Event:

Details:

pluggable transceiver out

Troubleshooting:

Probable Cause: This event is issued when Prime Network detect that pluggable transceiver of a port that was discovered by the VNE from the device i s no longer reported by the device.

The root cause for this is physically removal of the pluggable transceiver from its slot.

Action to be Taken: Please check if the pluggable transceiver was removed from the port and re-insert it properly.

Clear Condition: When the pluggable transceiver is inserted and connected to the port.

Table 8-13 describes the information that is displayed in the Details tab in the Event Properties window.

Table 8-13 Details Tab for Events

Field	Description
Event ID	Unique identifier for the selected event.
Severity	Severity of the event, indicated by color and text label.
Description	Description of the event.
Type	Type of event, such as Security or Service.
Location	Entity that triggered the event, hyperlinked to its entry in inventory.
Element Type	The type of device that triggered the event, e.g., Cisco 7609
Ticket ID	This field is displayed only for network events. Sequential identifier of the ticket, hyperlinked to the Ticket Properties window.
Detection Time	Date and time when the event happened and was logged and recorded.

Table 8-13 Details Tab for Events (continued)

Field	Description
Device Time	The time zone of the device. **Note** This information is available only for Cisco ASR5000 devices.
Category	The category of the fault, which can be any one of the following: • Communications—Associated with procedures and/or processes required to convey information from one point to another. • Quality of Service—Associated with a degradation in the quality of service. • Processing error—Associated with a software or processing fault equipment. • Environmental—Associated with a condition relating to an enclosure in which the equipment resides. • Equipment—Associated with an equipment fault. • Undetermined—Not categorized.
Nature	The nature of the fault, which can be one of the following: • ADAC (Automatically Detected Automatically Cleared)—When the clearing is automatically detected and cleared by Element Management System (EMS). For example, Link Down. • ADMC (Automatically Detected Manually Cleared)—When clearing requires manual intervention. For example, DWDM Fatal Error syslog.
Alarm ID	This field is displayed only for network events. Alarm identifier, hyperlinked to the Ticket Properties window or the Alarm Properties window.
Causing Event	This field is displayed only for network events. The identifier of the causing event.
Details	Detailed description of the event.
Troubleshooting	The probable cause of the event, action to be taken to rectify the problem, and the clearing condition. **Note** This information is available only for service events and Cisco ASR5000 traps.

Step 3 You can view additional properties in the following tabs:

- Advanced tab—See Table 8-14.
- Affected Parties tab—See Table 9-7.
- Audit tab—See Table 8-15.
- Provisioning tab—See Table 8-16.
- Security tab—See Table 8-17.
- Trap tab—See Table 8-18.

The tabs that are displayed depend on the type of event, such as a Service event or a Provisioning event.

Table 8-14 Advanced Tab

Field	Description
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Affected Devices	The number of devices affected by the ticket.
Alarm Count	The total number of alarms associated with the ticket, including the root alarm.

Table 8-15 Audit Tab

Field	Description
User Name	Name of user who initiated the command.
Result	Command result, if available.
Originating IP	IP address of the client that issued the command.
Command Signature	Actual command run by Prime Network, such as **GetEventViewerProperties**.
Command Parameters	Parameters applied to the command.

Table 8-16 Provisioning Tab

Field	Description
User Name	Name of the user who performed the provisioning operation.
Status	Status of the operation: Success or Fail.

Table 8-17 Security Tab

Field	Description
User Name	Name of the user who triggered the event.
Client Type	Client that triggered the event: Cisco Prime Network Vision, Cisco Prime Network Administration, Cisco Prime Network Events, or Unknown.
Originating IP	IP address of the client where the event was triggered.

Table 8-18 Trap Tab

Field	Description
Version	SNMP version: version-1, version-2c, or version-3.
Community String	Community that the device sends in the Protocol Data Unit (PDU).
Error Status	Error status: No Error, Too Big, No Such Name, Bad Value, Read Only, and Gen Err.
Values Table	
Translated OID	String representation of the OID. For example, 1.3.6 is translated into iso.org.dod where: • 1 represents iso. • 3 represents org. • 6 represents dod.
Translated Value	String representation of the OID value. For example, 1.3 is translated to iso(1).org.10, or a specific value, such as “down” or “4 days, 20 hours, 32 minutes, 11 seconds.”
OID	OID that is not translated. It is a dot notation representation of the OID, such as 1.3.6.1.4.1.9.
Value	Value that is not translated.

The properties of a selected ticket can be viewed in the Ticket Properties window. For a detailed description of the Ticket tab properties, see Viewing Ticket Properties, page 8-14.

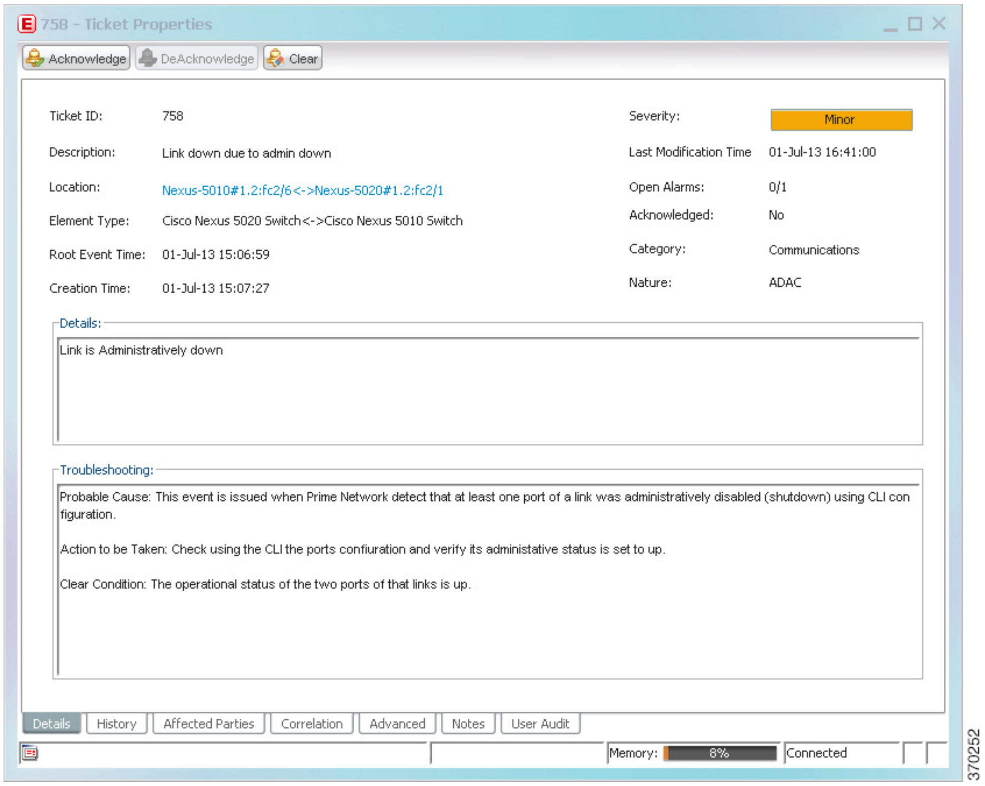
Viewing Ticket Properties

You can view the properties of a selected ticket in Cisco Prime Network Events by displaying the Ticket Properties window. To view ticket properties in Cisco Prime Network Events:

Step 1 In the Ticket tab in the Cisco Prime Network Events window, select the required ticket.

Step 2 Choose **View > Properties** from the main menu. The properties are displayed for the selected ticket, either in the lower portion of the Cisco Prime Network Events window or in a separate window as shown in Figure 8-3.

Figure 8-3 Ticket Properties Window - Details Tab



Ticket ID: 758

Description: Link down due to admin down

Location: Nexus-5010#1.2:fc2/6<->Nexus-5020#1.2:fc2/1

Element Type: Cisco Nexus 5020 Switch<->Cisco Nexus 5010 Switch

Root Event Time: 01-Jul-13 15:06:59

Creation Time: 01-Jul-13 15:07:27

Severity: Minor

Last Modification Time 01-Jul-13 16:41:00

Open Alarms: 0/1

Acknowledged: No

Category: Communications

Nature: ADAC

Details:

Link is Administratively down

Troubleshooting:

Probable Cause: This event is issued when Prime Network detect that at least one port of a link was administratively disabled (shutdown) using CLI con figuration.

Action to be Taken: Check using the CLI the ports confiuration and verify its administative status is set to up.

Clear Condition: The operational status of the two ports of that links is up.

Table 8-19 describes the information that is displayed in the Details tab in the Ticket Properties window.

Table 8-19 Ticket Properties Window - Details Tab

Field	Description
Buttons	
Acknowledge	Acknowledges that the ticket is being handled. For more information, see Acknowledging/Deacknowledging a Ticket, page 9-15. If a ticket is acknowledged, and events are correlated to it after correlation, the ticket is considered to have not been acknowledged. This button is enabled only if the ticket is not acknowledged.
DeAcknowledge	A ticket that has been acknowledged can be deacknowledged, indicating that it still needs to be handled.
Clear	Requests the Prime Network system to remove the faulty network element from the Prime Network networking inventory. In addition, it sets the ticket to Cleared severity or status and automatically changes the acknowledged status of the ticket to Yes. For more information, see Clearing a Ticket, page 9-15. This button is enabled only if the severity of the alarm is higher than Cleared or Normal.
Details Tab	
Ticket ID	Sequentially assigned identifier of the ticket.
Severity	Severity of the ticket, indicated by color and text label.

Table 8-19 Ticket Properties Window - Details Tab (continued)

Field	Description
Description	Description of the ticket.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Location	Hyperlink to the entity that triggered the event. **Note** If the entity that triggered the event is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Open Alarms	Number of open alarms out of all alarms, such as 3/4.
Element Type	The type of device that triggered the root event.
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Acknowledged	Whether or not the ticket has been acknowledged: Yes or No.
Creation Time	Date and time when the ticket was created.
Device Time	The time zone of the device. **Note** This information is available only for Cisco ASR5000 devices.
Category	The category of the fault, which can be any one of the following: • Communications—Associated with procedures and/or processes required to convey information from one point to another. • Quality of Service—Associated with a degradation in the quality of service. • Processing error—Associated with a software or processing fault equipment. • Environmental—Associated with a condition relating to an enclosure in which the equipment resides. • Equipment—Associated with an equipment fault. • Undetermined—Not categorized.
Nature	The nature of the fault, which can be one of the following: • ADAC (Automatically Detected Automatically Cleared)—When the clearing is automatically detected and cleared by Element Management System (EMS). For example, Link Down. • ADMC (Automatically Detected Manually Cleared)—When clearing requires manual intervention. For example, DWDM Fatal Error syslog.
Details	Detailed description of the ticket.
Troubleshooting	The probable cause of the last event in the root alarm, the action to be taken to rectify the problem and the clearing condition. **Note** This information is available only for service events and Cisco ASR5000 traps.

Step 3 As required, review additional properties for the ticket. Table 8-20 identifies the additional tabs that are displayed in the Ticket Properties window and links to the relevant information.

Table 8-20 Ticket Properties Window - Additional Tabs

Tab	Description
History	Contains the history of the ticket, including all the events. For more information, see History Tab, page 9-11.
Affected Parties	The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. For more information, see Affected Parties Tab, page 9-11.
Correlation	Displays all alarms that are correlated to the selected ticket. For more information, see Correlation Tab, page 9-13.
Advanced	The number of affected devices, correlations, duplications, and reductions for the selected ticket. In addition, it provides any other additional information available about the ticket. For more information, see Advanced Tab, page 9-13.
Notes	Enables you to add and save notes for the selected ticket. The Notes tab is not available for tickets that have been archived. For more information, see Notes Tab, page 9-14.
User Audit	Enables you to see which ticket-related actions were carried out by which users, and when the action took place. For more information, see User Audit Tab, page 9-14.

Refreshing Cisco Prime Network Events Information

Cisco Prime Network Events displays current information in lists in each tab. While you view a list, the information is not updated unless you manually refresh the list or activate autorefresh. The default autorefresh setting is 60 seconds and can be adjusted (see Adjusting the Prime Network Vision GUI Client Settings, page 2-40). Your filter settings remain intact.

Table 8-21 shows the refresh buttons.

Table 8-21 Cisco Prime Network Events Refresh Buttons

Button	Name	Function
⟳	Refresh Now	Manually refreshes the events list.
🔄	Auto Refresh	Automatically refreshes the events list. The Auto Refresh icon toggles to indicate whether auto refresh is on or off. This icon indicates auto refresh is on.

To manually refresh a list, choose **View > Refresh** from the main menu. To automatically refresh a list, click **Auto Refresh** in the toolbar.

Filtering Events

The Filter Events dialog box allows you to filter events according to a number of criteria including severity, identifier, time stamp, description, location, and category-specific information.

You may also use the filter to search for information in the database.

The Filter icon toggles to indicate that a filter has been applied.

The following settings in the Cisco Prime Network Events Options dialog box also affect your filters:

- If you check the Keep Last Filter check box, the currently defined filter settings are saved in the registry and are displayed the next time you log in, but are not applied.
- If you check the Open Using Filter check box, the events are continuously filtered according to the defined settings, even when you log out of and back into the application.

For more information, see Adjusting the Prime Network Vision GUI Client Settings, page 2-40.

See the following topics for more information about filtering events:

- Defining Filters, page 8-19
- Removing Filters, page 8-20

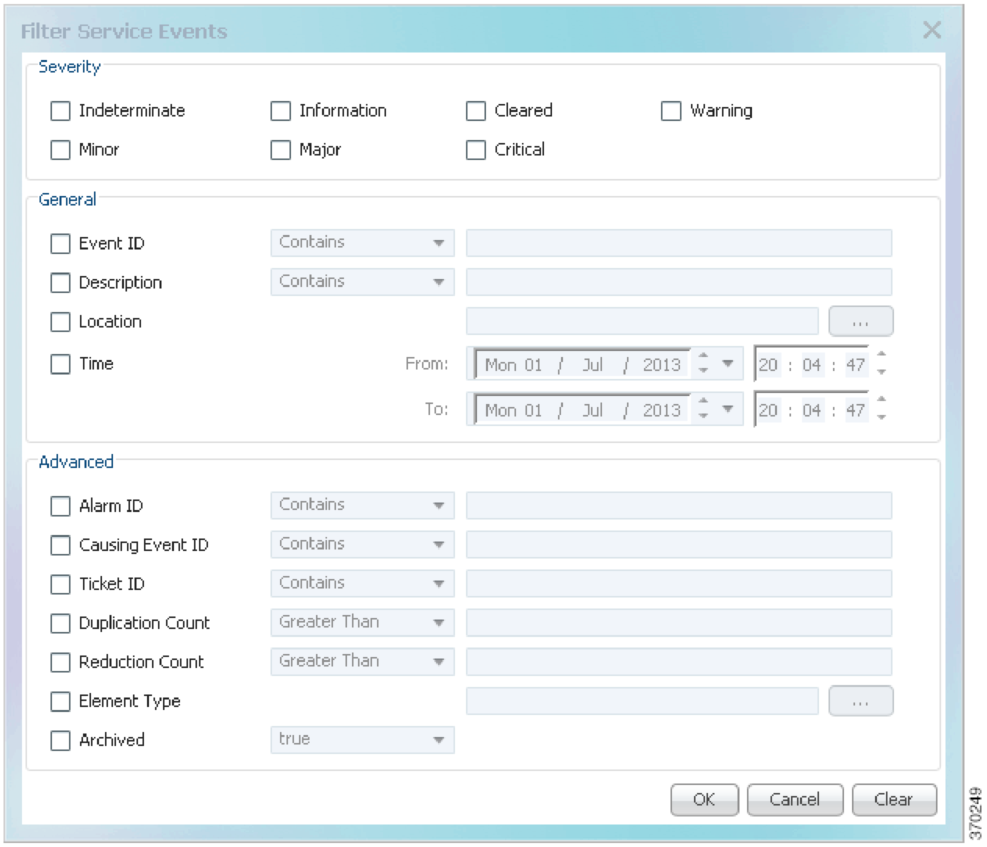
For information about filtering tickets, see Filtering Tickets by Criteria, page 9-7.

Defining Filters

To define a filter:

Step 1 Choose **Edit > Filter** from the main menu. The criteria that you can use for filtering differs for events and tickets. For example, Figure 8-4 shows the Filter Events dialog box for service events. For an example of the Ticket Filter dialog box, see Figure 9-2.

Figure 8-4 Filter Events Dialog Box - Service Events



Filter Service Events

Severity

□ Indeterminate □ Information □ Cleared □ Warning
□ Minor □ Major □ Critical

General

□ Event ID Contains
□ Description Contains
□ Location ...
□ Time From: Mon 01 / Jul / 2013 20 : 04 : 47
To: Mon 01 / Jul / 2013 20 : 04 : 47

Advanced

□ Alarm ID Contains
□ Causing Event ID Contains
□ Ticket ID Contains
□ Duplication Count Greater Than
□ Reduction Count Greater Than
□ Element Type ...
□ Archived true

OK Cancel Clear

Step 2 Specify the filter criteria by using the following steps and the information in Table 8-22:

a. Check the check box for each criterion to use for filtering.

b. As needed, choose the operator for the filter, such as Contains or Does Not Contain.

c. Supply the specific information to apply to the filter, such as the time, a string, or one or more IP addresses.

Table 8-22 Cisco Prime Network Events Filter Events Options

Field	Description
Severity	Severities to be included in the filter.
General	
Event ID	Event identifier to apply to the filter.
Description	String to include or exclude.

Table 8-22 Cisco Prime Network Events Filter Events Options (continued)

Field	Description
Location	Network elements to include. This field is not displayed for Audit events.
Time	Beginning and ending dates and times to apply to the filter.
Network Events Advanced Options	
Alarm ID	Alarm identifier to apply to the filter.
Causing Event ID	Identifier of the causing event to apply to the filter.
Ticket ID	Ticket identifier to apply to the filter.
Duplication Count	Duplication count value to use for filtering.
Reduction Count	Reduction count value to use for filtering.
Element Type	Filter by the type of element that triggered the event.
Archived	Archive status to use for filtering: True or False.
System Events Advanced Options	
Command Name	String in the command name to use for filtering.
Command Signature	String in the command signature to use for filtering.
Command Parameters	String in a command parameter to use for filtering.
Originating IP	Originating IP address to include or exclude from filtering.
Status	Status to use for filtering: Configuring, Fail, Success, or Unknown.
User Name	String in the username to use for filtering.

Step 3 Click **OK** to save your filter settings and apply the filter. The filtered entries are displayed in the list according to the defined criteria.

Removing Filters

To remove a filter:

Step 1 Click **Filter** in the main toolbar.

Step 2 In the Filter Events dialog box, click **Clear**. The selected options in the Filter Events dialog box are cleared.

Step 3 Click **OK**. All events are displayed in the list.

Exporting Displayed Data

Cisco Prime Network Events enables you to export the currently displayed data from the Cisco Prime Network Events table according to the criteria defined in the Cisco Prime Network Events Options dialog box. You can then import and view at a later time.

To export a table to a file:

Step 1 Choose **File > Export**.

Step 2 In the Export Table to File dialog box, browse to the directory where you want to save the list.

Step 3 In the File name field, enter a name for the list.

Step 4 Click **Save**. The displayed events list or rows are saved in the selected directory.