CHAPTER 9

Tracking Faults Using Prime Network Events

The following topics describe how to use Cisco Prime Network Events (Prime Network Events) to track 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.
- 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 3.10 Administrator Guide*.

Only users with the Administrator role can log into Cisco Prime Network Events, as shown in Table 9-1.

Table 9-1 Default Permission/Security Level Required for Cisco Prime Network Events

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing events and tickets	—	—	—	—	X
Viewing events and ticket properties	—	—	—	—	X
Refreshing information displayed in tables	—	—	—	—	X

Table 9-1 Default Permission/Security Level Required for Cisco Prime Network Events (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Filtering events and tickets	—	—	—	—	X
Exporting displayed data	—	—	—	—	X

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.

Note Cisco Prime Network Events shows events only from the fault database and not from the event archive. Use Report Manager to view events from the event archive. For more information, see Chapter 11, "Working with Reports."

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 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.

By using the Cisco Prime Network Events Options dialog box, you can define a filter to be used or the number of items to be displayed in the list. Each tab displays the specified number of entries per page as defined in the Cisco Prime Network Events Options dialog box.

For more information, see Adjusting the Prime Network Events GUI Client Settings, page 8-8.

Because the lists of events and tickets can be lengthy, you can use the left and right arrows on the navigation to move through the records. You can also use the submenus that are available from **View > Go To** in the main menu.

All Tab

The All tab displays information about all events. Additional information specific to the event category can be viewed in the Event Properties window or individual category tabs.

When you launch Cisco Prime Network Events, the All tab is not displayed. You can view this tab by choosing **File > Open All Tab**.

Note When you open the All tab, it might take some time to retrieve information from the Prime Network database for all category events.

You can disable the All tab by following the instructions provided in the *Cisco Prime Network 3.10 Installation Guide*.

Table 9-2 describes the information that is displayed in the All tab.

Table 9-2 All 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 Status Indicators, page 8-4.
Event ID	Event identifier, assigned sequentially.
Time	Date and time when the event occurred and was logged and recorded.
Description	Description of the event.
Location	Entity that triggered the event.
Event Type	Type of event: Audit, Provisioning, Security, Service, Syslog, System, V1 Trap, V2 Trap, or V3 Trap.

System Event Tabs

The following tabs in the Cisco Prime Network Events window display the system events:

- Audit Tab, page 9-3
- Provisioning Tab, page 9-5
- Security Tab, page 9-6
- System Tab, page 9-6

Audit Tab

The Audit tab displays all events generated for each command or request in Prime Network; for example, opening Cisco Prime Network Events displays the **Get** command as shown in Figure 9-1.

Figure 9-1 Audit Tab

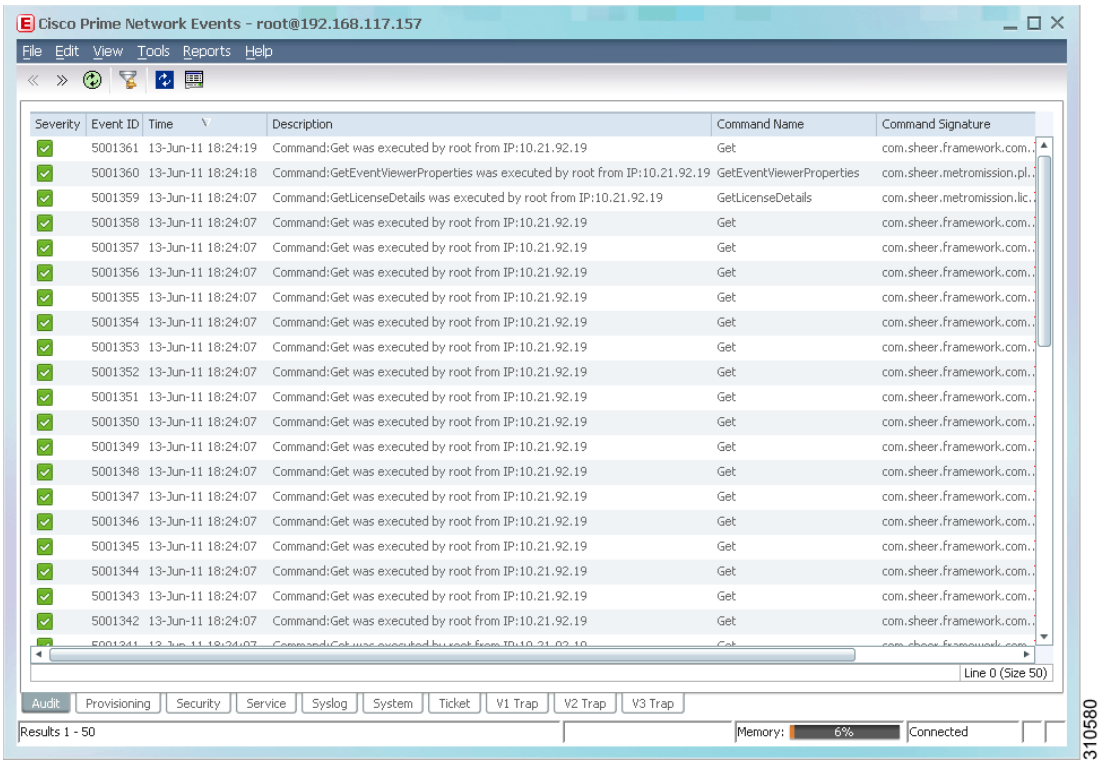


Table 9-3 describes the information that is displayed in the Audit tab.

Table 9-3 Audit 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 Status Indicators, page 8-4.
Event ID	Identifier of the event, assign sequentially.
Time	Date and time when the event happened and was logged and recorded.
Description	Aggregation of portions of the same fields in the Audit Command fields.
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.

The audit service enables you to audit all the commands executed in the system; for example, the **Get** command can be audited. The Audit tab then displays this information.

Provisioning Tab

Events displayed in the Provisioning tab are events triggered during the configuration of a device. Prime Network sends an event explaining the configuration operation, such as configuring the cross-connect table in a device. The Provisioning tab displays detailed information specific to this event category. It contains events from Prime Network Command Builder, Prime Network Activation, and Prime Network Workflow Editor[1].

Additional information specific to this event category can be viewed in the Event Properties window.

If a provisioning event is the result of an activation script, the provisioning event can include an extremely long description. This description is displayed in the Event Properties window in the Details field. If the description exceeds the size of the Details field, Prime Network truncates the description in the database and Details field, and displays the following line to indicate that the description has been truncated:

```
=====CONTENT TRUNCATED BY CISCO PRIME NETWORK=====
```

Table 9-4 describes the information that is displayed in the Provisioning tab.

Table 9-4 Provisioning 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 Status Indicators, page 8-4.
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 “Script Show has failed.”
Location	Entity that triggered the event.
Prime Login Username	Username of the logged in user.
VNE Login Username	Username, which was used to access the device. This field is updated only for events generated by command scripts in Prime Network. For all other commands, this field shows ‘From VNE Login.’
Status	Status, such as Success or Fail.

1. The Workflow Editor is based on LiquidBPM by Autonomy, Inc.

Security Tab

The Security tab displays detailed information specific to this event category. Security events are related to client login and user activity when managing the system and the environment. Additional information specific to this event category can be viewed in the Event Properties window.

Table 9-5 describes the information that is displayed in the Security tab.

Table 9-5 Security 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 Status Indicators, page 8-4.
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 “Invalid password. Couldn’t authenticate user root.”
Location	Entity that triggered the event.
Username	Name of the user who triggered the event.
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 3.10 Supported Service Events*.

System Tab

The System tab displays all the system events related to the everyday working of the internal system and its components. These events can be related to Prime Network and Prime Network gateway resources, representing the system log. Additional information specific to this event category can be viewed in the Event Properties window.

Table 9-6 describes the information that is displayed in the System tab.

Table 9-6 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 Status Indicators, page 8-4.
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 3.10 Supported Service Events*.

Network Event Tabs

The following topics describe the information displayed in Prime Network Events for network events:

Service Tab

The Service tab displays all the events generated by Prime Network, such as Link Down. Service events are related to the alarms that are generated by the Prime Network system. Additional information specific to this event category can be viewed in the Event Properties window.

Table 9-7 describes the information that is displayed in the Service tab.

Table 9-7 Service 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 Status Indicators, page 8-4.
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 “Port down due to oper.”
Location	Hyperlink to the entity that triggered the event.
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 3.10 Supported Service Alarms*.

Syslog Tab

The Syslog tab displays all the syslog events. These events are related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events. Additional information specific to this event category can be viewed in the Event Properties window.

Table 9-8 describes the information that is displayed in the Syslog tab.

Table 9-8 Syslog 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 Status Indicators, page 8-4.
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 “Device configuration changed.”
Location	Hyperlink to the entity that triggered the event.
Alarm ID	Identifier of the alarm associated with the event.
Ticket ID	Identifier of the ticket associated with the event.
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.

Ticket Tab

The Ticket tab displays detailed information specific to tickets. A ticket contains a single root alarm (the root cause alarm can be of any alarm type, such as syslog or service), and all its subsequent correlated alarms. Additional information specific to tickets can be viewed in the Ticket Properties window.

A *Tickets capacity overflow, red threshold reached* system alarm is generated when the maximum number of tickets is exceeded. The alarm severity is defined as critical.

Table 9-9 describes the information that is displayed in the Ticket tab.

Table 9-9 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 Status Indicators, page 8-4.
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.
Acknowledged	Whether the ticket is acknowledged or has been modified: Yes, No, or Modified.
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 10, “Working with Tickets in Cisco 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 9-18.

V1 Trap Tab

This event is triggered when the network element sends a trap message to Prime Network because of a network event, such as Link Down. The V1 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 9-10 describes the information that is displayed in the V1 Trap tab.

Table 9-10 V1 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 Status Indicators, page 8-4.
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.
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 the Cisco IOS and Cisco IOX traps displayed in one of these tabs, see *Cisco Prime Network 3.10 Supported Traps*.

V2 Trap Tab

This event is triggered when the network element sends a trap message to Prime Network because of a network event. The V2 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 9-11 describes the information that is displayed in the V2 Trap tab.

Table 9-11 V2 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 Status Indicators, page 8-4.
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 “SNMP authentication failure.”
Location	Hyperlink to the entity that triggered the trap.
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.
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 3.10 Supported Traps*.

V3 Trap Tab

This event is triggered when the network element sends a trap message to Prime Network because of a network event. The V3 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 9-12 describes the information that is displayed in the V3 Trap tab.

Table 9-12 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 Status Indicators, page 8-4.
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.
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.
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 3.10 Supported Traps*.

Viewing 3.6.x Tabs

If you upgrade to Prime Network 3.10 from Cisco ANA 3.6.x, you can view the following tabs by choosing **File > Open 3.6.x Tabs**:

- 3.6.x Ticket
- 3.6.x Service
- 3.6.x Syslog
- 3.6.x V1 Trap
- 3.6.x V2-V3 Trap

Table 9-13 describes the information that is displayed in each of the 3.6.x tabs.

Table 9-13 3.6.x Tab Contents in Events

Field	Description
3.6.x Ticket Tab	
Severity	Icon of a bell, colored according to the severity of the alarm on the ticket. For more information, see Event Status Indicators, page 8-4.
Ticket ID	Sequentially assigned identifier of the ticket.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Time	Date and time recorded when the first event happened.
Acknowledged	Status of the ticket: Acknowledged, Not Acknowledged, or Modified.
Affected Devices Count	Number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).
Correlation Count	Number of correlated alarms included in the ticket.
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 10, "Working with Tickets in Cisco Prime Network Vision."
Duplication Count	For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
3.6.x Service Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 8-4.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.
3.6.x Syslog Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 8-4.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.

Table 9-13 3.6.x Tab Contents in Events (continued)

Field	Description
3.6.x V1 Trap Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 8-4.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.
Suppress Display	Whether or not the display of the alarm is suppressed.
3.6.x V2-V3 Trap Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 8-4.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.
Suppress Display	Whether or not the display of the alarm is suppressed.

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 9-14
- Viewing Ticket Properties, page 9-18
- Refreshing Cisco Prime Network Events Information, page 9-21
- Filtering Events, page 9-22
- Exporting Displayed Data, page 9-25

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 9-2. The Details tab is displayed by default.

Figure 9-2 Network Event Properties Window - Details Tab

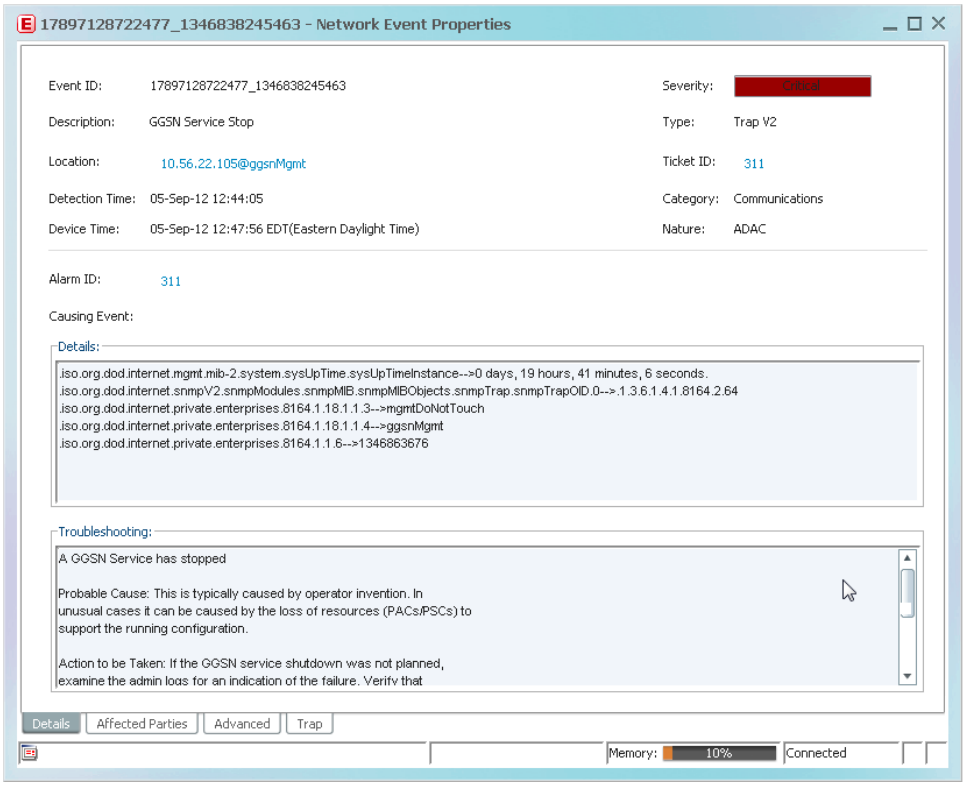


Table 9-14 describes the information that is displayed in the Details tab in the Event Properties window.

Table 9-14 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.
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 9-14 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 Cisco ASR5000 traps.

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

- Advanced tab—See Table 9-15 on page 9-17.
- Affected Parties tab—See Table 10-12 on page 10-15.
- Audit tab—See Table 9-16 on page 9-17.
- Provisioning tab—See Table 9-17 on page 9-17.

- Security tab—See Table 9-18 on page 9-17.
- Trap tab—See Table 9-19 on page 9-18.

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

Table 9-15 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 9-16 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 9-17 Provisioning Tab

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

Table 9-18 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 9-19 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 9-18.

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 9-3.

Figure 9-3 Ticket Properties Window - Details Tab

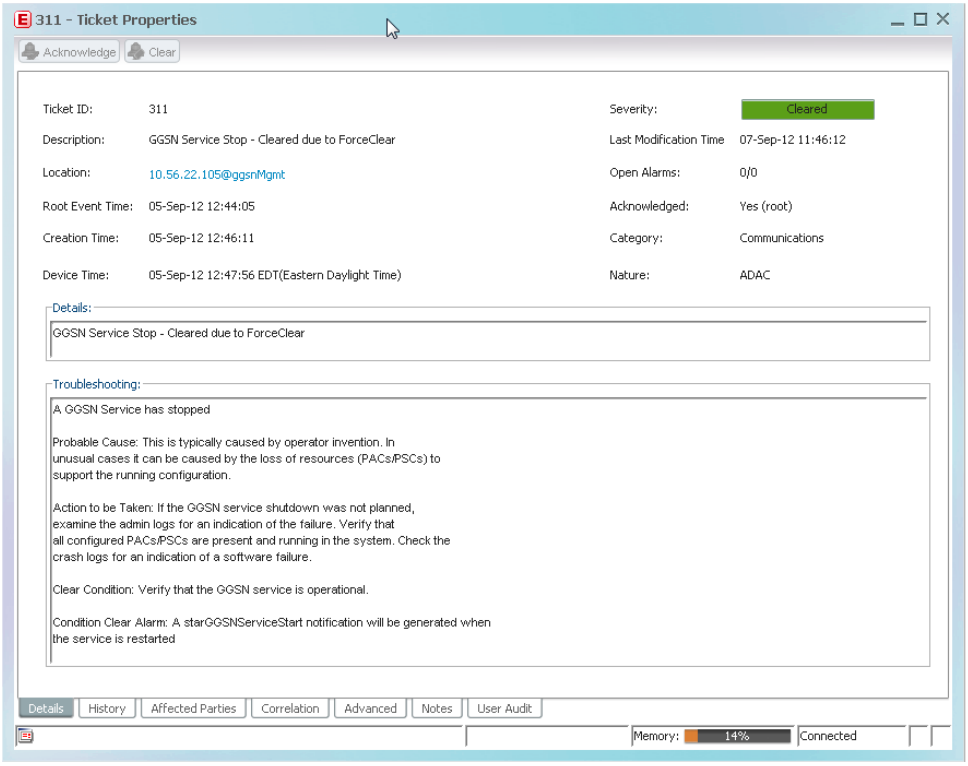


Table 9-20 describes the information that is displayed in the Details tab in the Ticket Properties window.

Table 9-20 Ticket Properties Window - Details Tab

Field	Description
Buttons	
Acknowledge	Acknowledges that the ticket is being handled. The status of the ticket is displayed as true in the ticket pane and in the Ticket Properties dialog box. For more information, see Acknowledged Ticket, page 10-7. 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.
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 Cleared Ticket, page 10-7. 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 9-20 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.
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 event, action to be taken to rectify the problem and the clearing condition. **Note** This information is available only for Cisco ASR5000 traps.

Step 3 As required, review additional properties for the ticket.

Table 9-21 identifies the additional tabs that are displayed in the Ticket Properties window and links to the relevant information.

Table 9-21 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 10-13.
Affected Parties	The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. For more information, see Affected Parties Tab, page 10-14.
Correlation	Displays all alarms that are correlated to the selected ticket. For more information, see Correlation Tab, page 10-17.
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 10-18.
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 10-18.
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 10-19.

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 Events GUI Client Settings, page 8-8). Your filter settings remain intact.

Table 9-22 shows the refresh buttons.

Table 9-22 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 Events GUI Client Settings, page 8-8.

See the following topics for more information about filtering events:

- Defining Filters, page 9-23
- Removing Filters, page 9-24

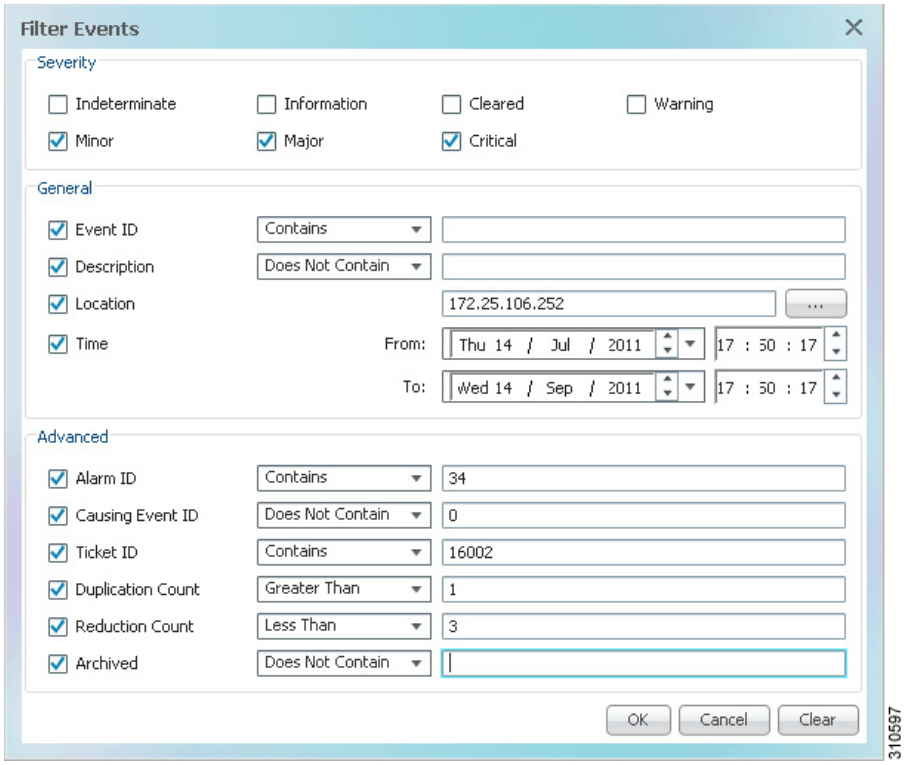
For information about filtering tickets, see Filtering Tickets by Criteria, page 10-8.

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 9-4 shows the Filter Events dialog box for service events. For an example of the Ticket Filter dialog box, see Figure 10-2 on page 10-9.

Figure 9-4 Filter Events Dialog Box - Service Events



Step 2 Specify the filter criteria by using the following steps and the information in Table 9-23:

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 9-23 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 9-23 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.
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.