



## Managing Traps and Events

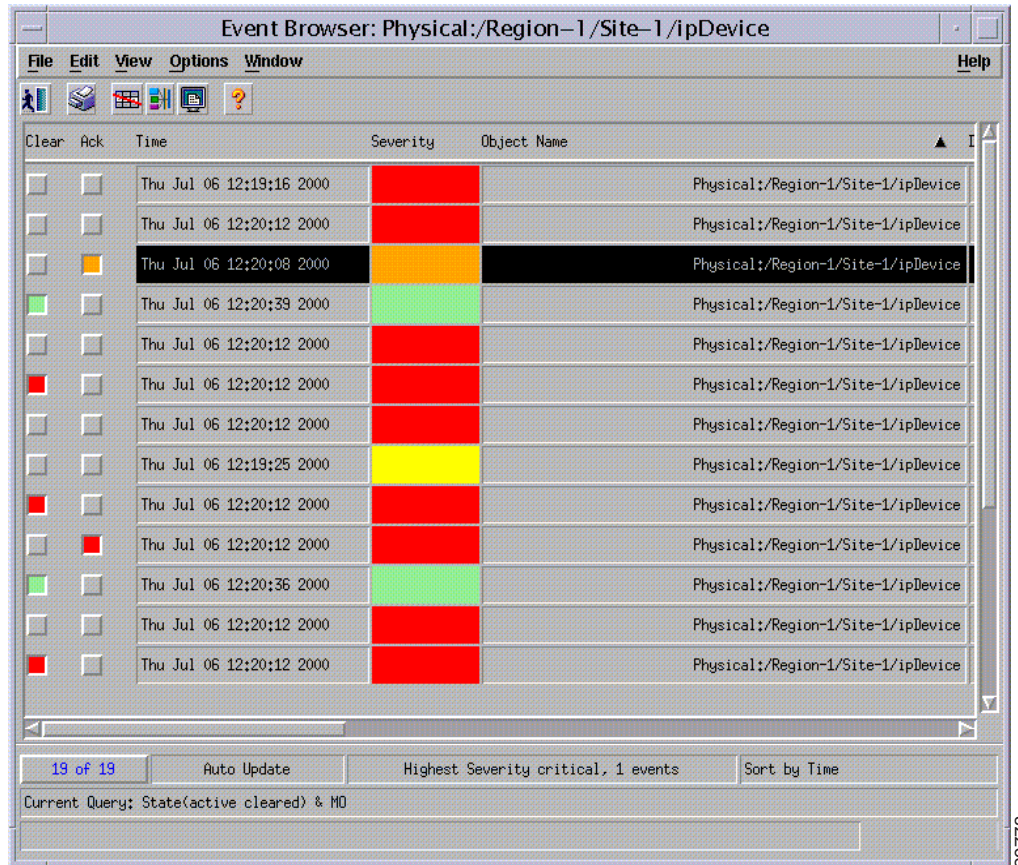
---

### Introduction to Fault Management

One of the most important aspects of network management is the ability to identify events on the system and to take action to resolve them quickly and efficiently. For example, there may be a power supply fault in a chassis that would require an engineer to be sent out to rectify the fault. This fault is critical to the running of the network and would need prompt attention.

In CMNM, when a condition (fault) occurs on a managed object in the network, the system is notified immediately. This notification is shown as an event or alarm and can be viewed with the CEMF Event Browser. The Event Browser is opened from the CEMF Launchpad. A screen similar to Figure 8-1 is displayed.

Figure 8-1 Event Browser Screen



The Event Browser provides a tool to manage the network efficiently; you can list, query, and sort all or some events according to how you want to manage the network. Services can be invoked on events so that faults can be attended to from the screen that shows the event.

**Note**

You can also view events on CEMF maps, however, only the most severe fault on a managed object is shown on the map icon.

You can have more than one Event Browser session open at any one time. Each Event Browser session can have different queries specified. All users can see any event. In the Event Browser window, you can acknowledge that a particular event is one that you are going to deal with, and all other users then see that the event is being handled. When the event is cleared, it is shown in the Event Browser window, so other users know that the event requires no further attention.

When an event is received, it is shown as active and unacknowledged (the two indicators are shown as grey). At this stage, no one has taken responsibility to deal with it. You may not want to view all events on the system, so a query can be set up using the CEMF Query Editor to view specific events.

# How CEMF Models Events

A CEMF event represents a notification from a managed entity that a certain condition has just occurred. These events usually represent error conditions on managed elements.

Each event is associated with the object for which it provides notification. Therefore, an object can have a number of events related to itself at any one time.

## Event Information

The default information stored against all CEMF events includes:

- The object on which the event was raised
- The time the event was raised
- The severity of the event
- A description of the event
- The state of the event.

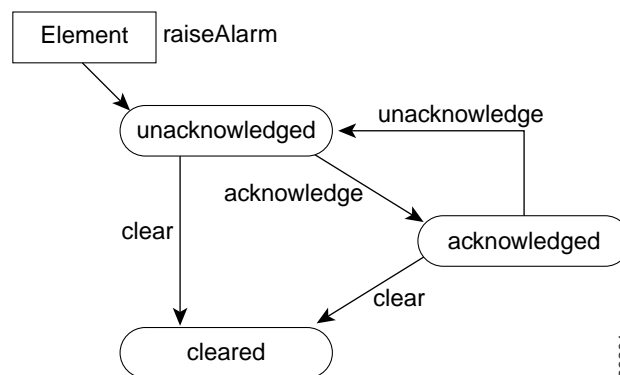
Descriptions of event state and severity are given below.

## Event State

The event state indicates whether the event is acknowledged or unacknowledged and active or cleared. When a new event is received by the system, its state is active/unacknowledged. You may acknowledge the event, which indicates to other users that the event is being handled. Once the event has been dealt with, you may clear the event. When you cannot clear an event due to an existing problem, it can be returned to the unacknowledged state and subsequently acknowledged or cleared by another user.

When an event is in the unacknowledged or acknowledged state, it is counted as being active, and therefore, it is still affecting the state of the object upon which it was raised.

*Figure 8-2 State Diagram for Events*



After events are cleared, they continue to be stored within the system for a configurable amount of time to maintain an event history for an element. These events can be viewed and manipulated in the same way as any other event.

## Colors used to Indicate Severity

Each event has a severity, indicating the importance of the event, and is identified with a corresponding color as shown in Table 8-1.

*Table 8-1 Colors Used to Indicate Severity*

	Color	Severity of Event
	Red	Critical
	Orange	Major
	Yellow	Minor
	Cyan	Warning
	Green	Normal
	White	Informational

## Source Domain

The source domain identifies where an event was generated. In CEMF, the source domain can be one of the following:

- SNMP—Event was generated by the managed network
- Internal—Event is generally generated by CEMF

## Management Domain

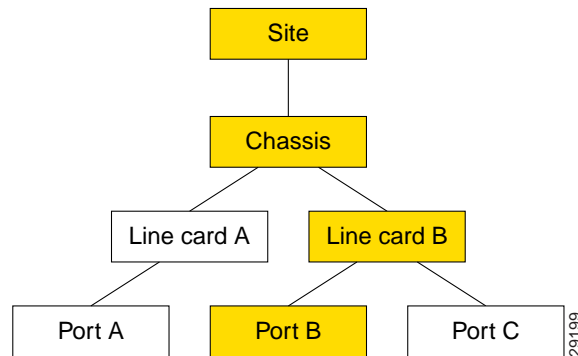
This is the management domain of SNMP trap information. The SNMP MIB specific information typically defines the equipment type generating a trap.

## Event Propagation

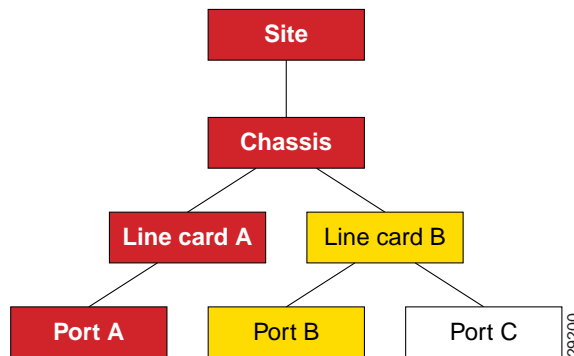
In order to make the identification of potential problems easy, CEMF propagates the alarm state of objects upwards through each object view.

In real terms, this means that if an object receives an event, then not only does it change color to reflect its new state, but all parent objects within a view, also change color, to reflect the most severe alarm on any of the children. The example in the following diagram shows a typical physical view of the network. The line cards are contained within the chassis, the chassis within a bay, the bay within a site, and so on.

If a minor alarm was received on Port B, then it, and all of the objects up to the region, turn yellow to indicate a potential minor problem, as illustrated in Figure 8-3.

*Figure 8-3 Example Minor Event Propagation*

If a critical alarm was then received on Port A, then it, and all of the objects up to the region, turn red to indicate a potential critical problem, as illustrated in Figure 8-4.

*Figure 8-4 Example Critical Event Propagation*

If the critical alarm is then cleared, the icons return to yellow.

## How CMNM Manages Faults

CMNM provides fault management of the Cisco MGC node, including the Cisco MGC host, the Cisco SLT, and the LAN switch. Traps generated by these elements are displayed within the CEMF system. When an alarm is received for an object, a pop-up balloon on Map Viewer shows the number and severity of the alarms for that object. The balloon color indicates the severity of the most severe alarms. The fault management features of the Cisco MGC allow you to view, acknowledge, and clear alarms for a given object.

CMNM handles numerous connectivity traps. CMNM defines the necessary trap mappings and containment trees, allowing CMNM to delegate all traps relating to the connectivity network to the nodes that represent it. You can display these alarms in the Event Browser.

When the Cisco MGC host detects a problem with one of its logical connections, it generates a trap. CMNM receives these traps and maps them to the object that represents that logical connection. For example, if CMNM receives a trap that the link to a media gateway is down, CMNM maps that trap to the object that represents the media gateway link and displays an alarm icon on the Map Viewer.

CMNM maps the incoming traps to alarms. However, not all traps are mapped to alarms. CMNM filters out duplicate traps from a network element. It also filters out traps from network elements that report a problem, and then reports within a few seconds (up to 6) when the problem is resolved. That is, the Cisco MGC automatically clears existing alarms when a network element reports that an alarm condition is no longer present. This reduces the number of unnecessary alarms displayed in the Event Browser. You cannot configure when an alarm should be automatically cleared.

## Presence Polling

CMNM periodically polls each managed object (the Cisco MGC host, Cisco SLT, Cisco MGX 8260, LAN switch, and BAMS) to ensure that the device is still reachable using SNMP. If the device is not reachable, it is indicated by annotation on the map display and an alarm is generated. In addition the object is placed into the CEMF errored state.

After the object loses connectivity, CEMF continues to poll the object until it can be reached. Once connectivity is re-established, the alarm is cleared and the annotation on Map Viewer is removed. In addition the object is returned to the CEMF normal state.

CMNM also displays the status of the Cisco MGC host connectivity network. This includes the logical connections from the active Cisco MGC host to the:

- Interfaces (Ethernet, TDM)
- STPs
- Point codes (SS7 Routes)
- Remote MGCs
- TCAP nodes
- Cisco Media Gateways

The logical connections from the active Cisco MGC host are shown as subnodes under the common Cisco MGC host object. If the standby Cisco MGC host is not processing calls, only the network connectivity of the active Cisco MGC host is shown.

## How Traps Are Managed for Network Devices

The following sections outline the southbound traps that are handled from the network elements. CMNM does not handle every possible trap that can be generated from each of the network elements, only those traps that are used for management of the devices.

### Cisco SLT Traps

*Table 8-2 Cisco SLT Traps*

Trap	MIB
coldStart	SNMPv2-MIB
warmStart	SNMPv2-MIB
linkUp	IF-MIB

*Table 8-2 Cisco SLT Traps*

linkDown	IF-MIB
authenticationFailure	SNMPv2-MIB
syslogAlarm	CISCO-SYSLOG-MIB
configChange	CISCO-CONFIG-MAN-MIB-V1SMI

## LAN Switch 5500 Traps

*Table 8-3 LAN Switch Traps*

Trap	MIB
coldStart	SNMPv2-MIB
warmStart	SNMPv2-MIB
linkUp	IF-MIB
linkDown	IF-MIB
authenticationFailure	SNMPv2-MIB
configChange	CISCO-CONFIG-MAN-MIB-V1SMI
switchModuleUp	CISCO-STACK-MIB
switchModuleDown	CISCO-STACK-MIB

## Catalyst 2900XL Traps

*Table 8-4 2900XL Traps*

Trap	MIB
coldStart	SNMPv2-MIB
warmStart	SNMPv2-MIB
linkUp	IF-MIB
linkDown	IF-MIB
authenticationFailure	SNMPv2-MIB
syslogAlarm	CISCO-SYSLOG-MIB
configChange	CISCO-STACK-MIB

## Catalyst 2900 Traps

*Table 8-5 2900 Traps*

Trap	MIB
coldStart	SNMPv2-MIB
warmStart	SNMPv2-MIB
linkUp	IF-MIB
linkDown	IF-MIB
authenticationFailure	SNMPv2-MIB
authenticationFailure	SNMPv2-MIB
configChange	CISCO-STACK-MIB
switchModuleUp	CISCO-STACK-MIB
switchModuleDown	CISCO-STACK-MIB

## Cisco MGC Host Traps

CMNM handles the traps in Table 8-6 from the Cisco MGC hosts.

*Table 8-6 Cisco MGC Host Traps*

Trap	MIB
qualityOfService	CISCO-TRANSPATH-MIB
processingError	CISCO-TRANSPATH-MIB
equipmentError	CISCO-TRANSPATH-MIB
environmentError	CISCO-TRANSPATH-MIB
commAlarm	CISCO-TRANSPATH-MIB

## Cisco MGX 8260 Traps

*Table 8-7 Cisco MGX 8260 Traps*

Trap	MIB
coldStart	SNMPv2-MIB
warmStart	SNMPv2-MIB
linkUp	IF-MIB
linkDown	IF-MIB
authenticationFailure	SNMPv2-MIB
shelfMajorAlarm	mms1600_trap
shelfMinorAlarm	mms1600_trap
shelfAlarmClear	mms1600_trap



*Table 8-7 Cisco MGX 8260 Traps*

Trap	MIB
shelfSecurityAlert	mms1600_trap
shelfColdStart	mms1600_trap
shelfHistoryChg	mms1600_trap
cardInserted	mms1600_trap
cardRemoved	mms1600_trap
cardFailed	mms1600_trap
cardCoreSwitched	mms1600_trap
cardServiceSwitched	mms1600_trap
cardMajorAlarm	mms1600_trap
cardMinorAlarm	mms1600_trap
cardAlarmCleared	mms1600_trap
cardActive	mms1600_trap
cardCoreRedFailed	mms1600_trap
cardSmRedFailed	mms1600_trap
cardMsmMajorAlarm	mms1600_trap
cardMismatched	mms1600_trap
cardCfgCleared	mms1600_trap
cardInStdbby	mms1600_trap
cardBackInserted	mms1600_trap
cardBackRemoved	mms1600_trap
dsx1LineAdded	mms1600_trap
dsx1LineDeleted	mms1600_trap
dsx1LineModified	mms1600_trap
dsx1MajorAlarm	mms1600_trap
dsx1MinorAlarm	mms1600_trap
dsx1AlarmClear	mms1600_trap
dsx1PerfMajorAlarm	mms1600_trap
dsx1PerfMinorAlarm	mms1600_trap
dsx1PerfAlarmCleared	mms1600_trap
dsx1UpdateThreshold	mms1600_trap
dsx1PayloadLoopup	mms1600_trap
dsx1LineLoopup	mms1600_trap
dsx1OtherLoopup	mms1600_trap
dsx1LineLoopDown	mms1600_trap
dsx1LineBertOn	mms1600_trap
dsx1LineBertOff	mms1600_trap

*Table 8-7 Cisco MGX 8260 Traps*

Trap	MIB
dsx3LineAdded	mms1600_trap
dsx3LineDeleted	mms1600_trap
dsx3LineModified	mms1600_trap
dsx3MajorAlarm	mms1600_trap
dsx3MinorAlarm	mms1600_trap
dsx3AlarmClear	mms1600_trap
dsx3PerfMajorAlarm	mms1600_trap
dsx3PerfMinorAlarm	mms1600_trap
dsx3PerfAlarmCleared	mms1600_trap
dsx3UpdateThreshold	mms1600_trap
dsx3PayloadLoopup	mms1600_trap
dsx3LineLoopup	mms1600_trap
dsx3OtherLoopup	mms1600_trap
dsx3LineLoopDown	mms1600_trap
etherLineAdded	mms1600_trap
etherLinedeleted	mms1600_trap
etherLineConfigChange	mms1600_trap
etherLineActive	mms1600_trap
etherLineInActive	mms1600_trap
etherLineFailed	mms1600_trap
etherLineAlarmCleared	mms1600_trap
voicePortAdded	mms1600_trap
voicePortDeleted	mms1600_trap
voicePortDeleted	mms1600_trap
voicePortModified	mms1600_trap
emmMajorAlarm	mms1600_trap
emmMinorAlarm	mms1600_trap
emmAlarmClear	mms1600_trap
clockMajorAlarm	mms1600_trap
clockMinorAlarm	mms1600_trap
clockAlarmCleared	mms1600_trap
clockSwitched	mms1600_trap
dmcM13MapAdded	mms1600_trap
dmcM13MapDeleted	mms1600_trap
dmcM13MapModified	mms1600_trap

Table 8-7 Cisco MGX 8260 Traps

Trap	MIB
dspMinorAlarm	mms1600_trap
dspMajorAlarm	mms1600_trap

## Trap Receipt Not Guaranteed

CMNM does not provide any guarantee that it received a trap from the southbound systems or network elements. CMNM does not perform any negotiation with the network elements to detect or recover lost traps. However, you can perform presence polling to display trap data that may have been lost.

## Forwarding Traps to Other Systems

CMNM provides forwarding of traps generated by each component of the Cisco MGC node (the Cisco MGC host, Ciso SLT, and LAN switch) to northbound systems.



### Note

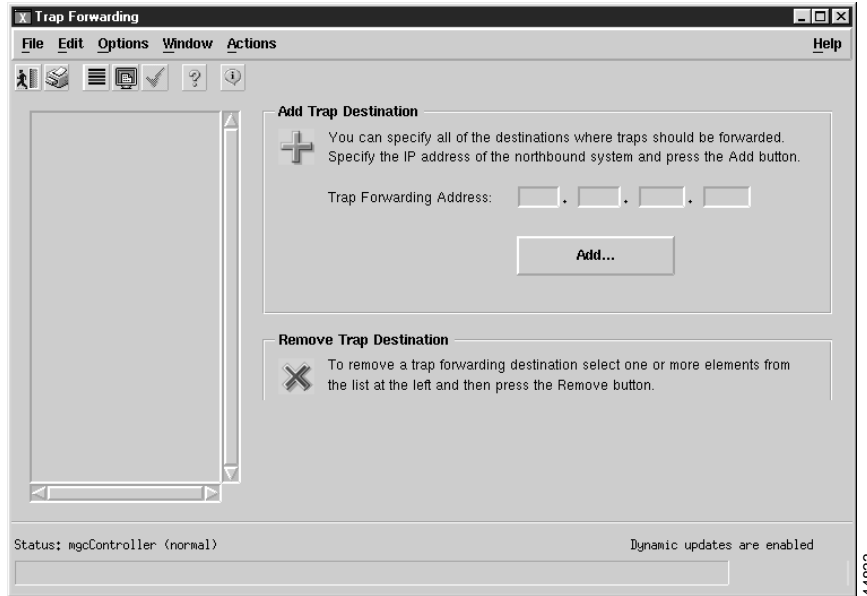
If you plan to configure CMNM to forward traps to northbound systems, you should only configure SNMP Version 1 traps on network devices. CMNM only forwards SNMP Version 1 traps to northbound systems. For more information on configuring SNMP on network devices, see Chapter 3, “Configuring Network Devices for Management.”

Traps are forwarded to the northbound systems using standard SNMP transport. To receive traps, northbound systems must register with CMNM. If the northbound system wants to receive standard SNMP traps, you must manually enter the IP address of the northbound system in CMNM. CMNM either provides a dialog where this information is entered or you must deploy an object that represents the northbound system.

To forward traps to another system:

- 
- Step 1** Select the site icon on the Map Viewer.
  - Step 2** Right-click to display the pull-down menu, select **Tools**, then **Open Trap Forwarding**.  
You see the screen in Figure 8-5.

Figure 8-5 Trap Forwarding Screen



**Step 3** Next to Trap Forwarding Address:, enter the IP address to which you want to forward traps and click **Add**.

You see the screen in Figure 8-6.

Figure 8-6 Action Report Screen



**Step 4** Click **Close**, then close the Trap Forwarding screen shown in Figure 8-5.

**Step 5** Select the site icon on the Map Viewer, right-click to display the pull-down menu, select **Tools**, then **Open Trap Forwarding**.

You see the Trap Forwarding screen shown in Figure 8-5 with the IP address you specified added to the left pane.




---

**Note** To remove an IP address, from the Trap Forwarding screen select the IP address, select **Actions**, then **Remove**. You see a screen confirming your action. Click **OK**.

---

## Opening the Event Browser

The Event Browser application is launched using the  icon in the CEMF Launchpad screen. The Query Editor window is displayed.

Set your query (the Event Browser displays events that match the query criteria). For more information, see the “Filtering Events Using Queries” section on page 8-15.

From the pop-up menu available when you right-click one or more objects in the Map Viewer (the Event Browser displays only the events associated with the selected objects), or from other CEMF applications, select the **Event Browser** option.

## Overview of the Event Browser Screen

The main panel in the Event Browser window, shown in Figure 8-7, displays a list of events including:

- Object name (the managed device’s name)
- Time the event was raised
- Severity of the event (color-coded)
- Description of the event

Two indicators, color-coded to the severity of the event, are available to the left of the object name:

- Clear (an indicator to show if an event is active or cleared)
- Ack (an indicator to show if an event is acknowledged or unacknowledged).

Click **Ack** to indicate to other users that the fault is being worked on. The button changes to the color of the severity, in this case, red. If for any reason you cannot clear the problem, this button can be deselected so the event can be reassigned. Click **Clear** when the fault has been rectified to indicate that the event requires no further attention.

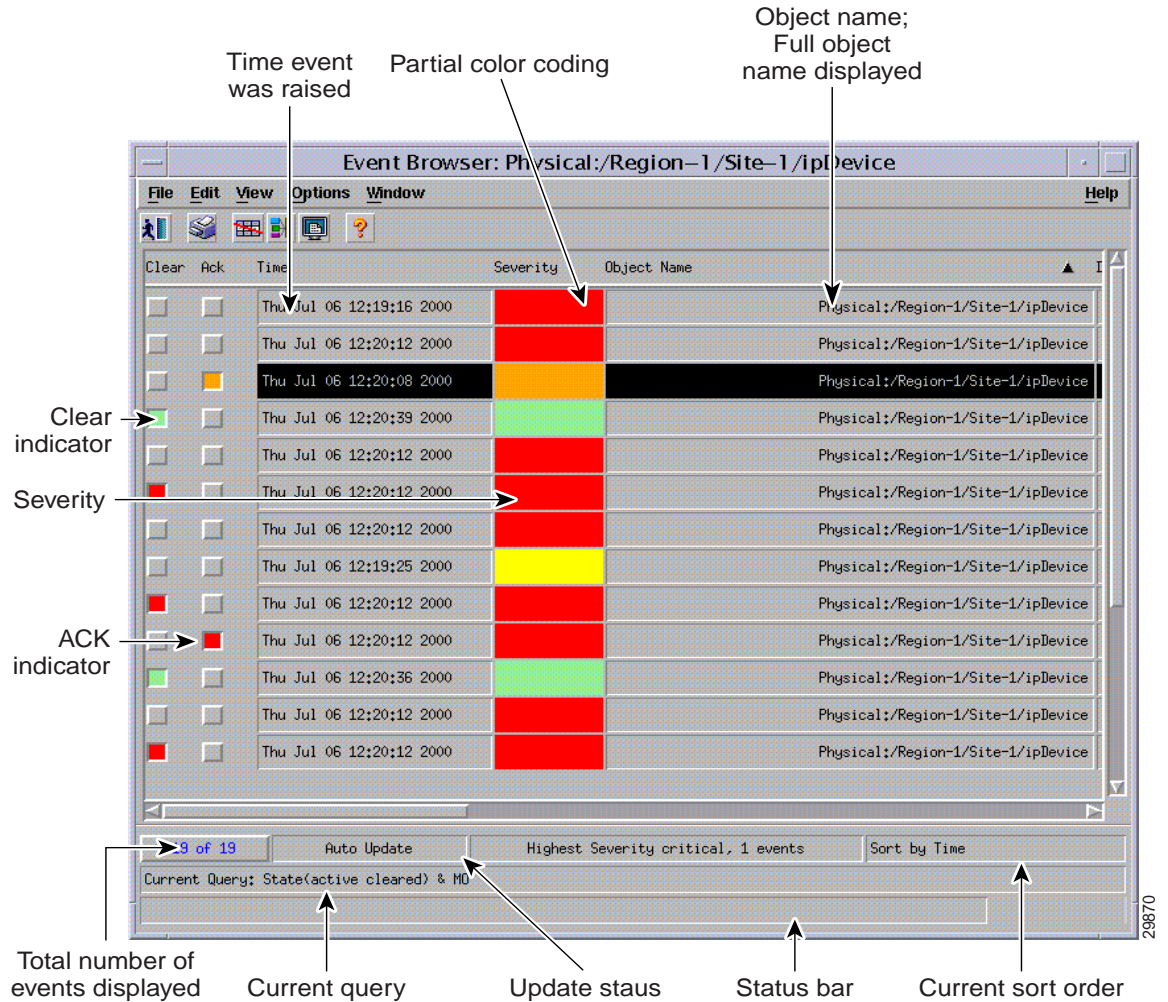


---

**Note** The option to unacknowledge an event is available only to an administrator or to the user who acknowledged the event initially.

---

Figure 8-7 Event Browser Screen



Menus are available that provide you options for modifying the way the information is displayed. From the Edit menu, you can:

- Set up the Event State (Clear Events, Acknowledge, or Unacknowledge Events)
- Set up queries to specify the events you want to see
- Set up sort options to present the events in the order you want

From the View menu you have the following options to manage the way events are viewed on each object:

- Use Auto or Manual Update
- Set the Color Coding
- View the Event History window
- Refresh the Event Browser window
- Display the Full Object Name
- Select Full Name Options

The Full Event Description window allows you to view the status of a selected event. For more information, refer to the “Viewing a Full Description of an Event” section on page 8-28.

Clicking an event severity, name, time, or description selects that event. One or more events can be selected; this gives the opportunity to perform bulk operations. With one or more events selected, clicking the right mouse button displays a pop-up menu that shows the common services available on those events.

The Event Browser window also displays other information in the status bar:

- Progress bar (indicates that events are being added to the display)
- Current Update status (this can be auto or manual)
- Current query
- Current sort order, for example, sort by time
- Total number of events displayed (this number is shown in blue until it is acknowledged by the user by clicking the number)



**Note** The Event Browser can display a maximum of 10,000 entries. If there are more events on the system, this is indicated in the status bar.

In the Event Browser, you can use Print to save the contents of all or part of the browser to a file or to print a paper copy.

## Filtering Events Using Queries

The Event Browser monitors all events on all devices. To work efficiently, you may want to specify the objects on the network with which you are concerned. The Event Browser gives you the option to do this through queries that can be configured to match your requirements. With queries you can choose to include or exclude devices or criteria. For example, you could choose to monitor a particular device, specify a time period, and choose to look only at events that are warnings or are critical. You define a query so that the Event Browser displays only the events that meet the criteria you defined.




**Note** Any changes made to the queries are not stored after exiting the Event Browser.

## Opening the Query Editor

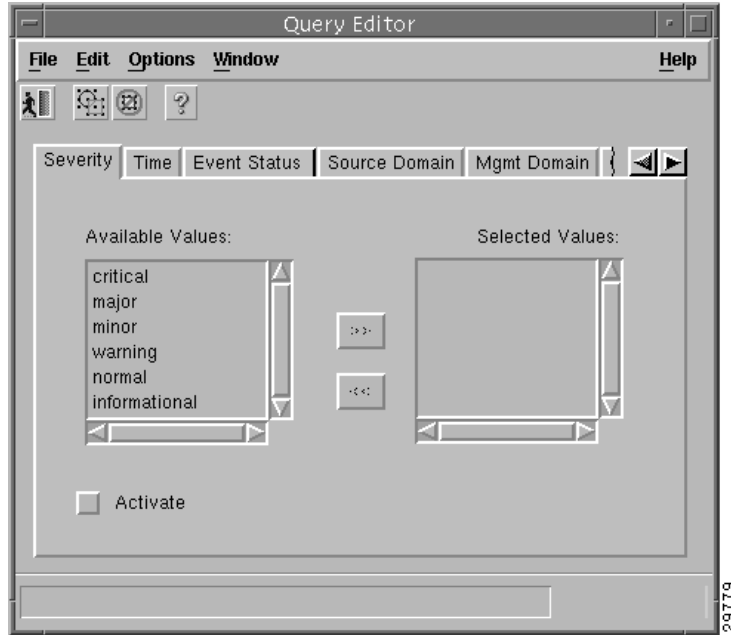
To define a query, click the  icon in the CEMF Launchpad window, or

in the Event Browser, select the **Edit** menu's **Query Setup** option, or

click the Query Filter icon  from the Toolbar.

The Query Editor window, similar to Figure 8-8, is displayed. The criteria that can be used to specify a query are available on individual tabs. Values or criteria can be selected on each tab. A dark gray tab is active (On); its query is used in the Event Browser. A light gray tab is inactive (Off); its query is not used.

Figure 8-8 Query Editor Screen



The Query Editor is split into the following tabbed sections (see the next section, “Setting Filtering Criteria,” for more information):

- Severity
- Time
- Event Status
- Source Domain
- Mgmt Domain
- User
- Event Class
- Object Scope
- Object Class
- Object Attribute Presence
- Object Attribute Value

The Event Browser is updated with events that match the query criteria. A progress bar indicates that CEMF is querying for events and the window is being updated. The total number of events displayed is shown in blue until you acknowledge it by clicking on the number.

## Setting Filtering Criteria

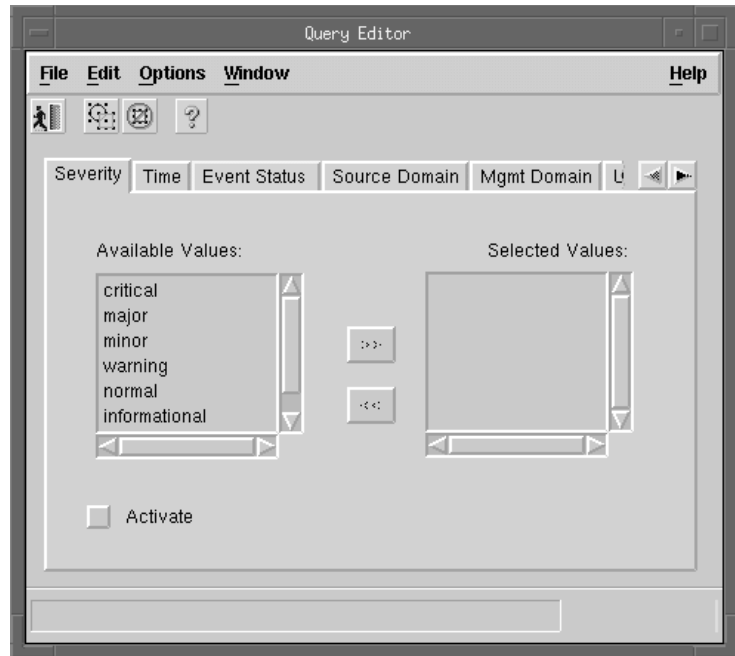
To set filtering (query) criteria:

- 
- Step 1 From the Query Editor screen, click the **Severity** tab.

You see the screen in Figure 8-9.

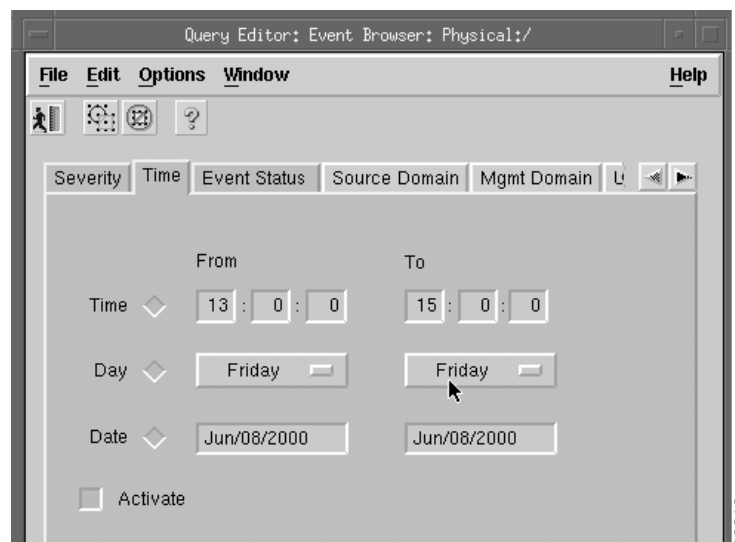


Figure 8-9 Query Editor Screen—Severity Tab



- Step 2** From the Available Values list, select the desired alarm level.
- Step 3** Click the right arrows to transfer the alarm level to the Selected Value list.
- Step 4** Click the **Time** tab.
- You see the screen in Figure 8-10.

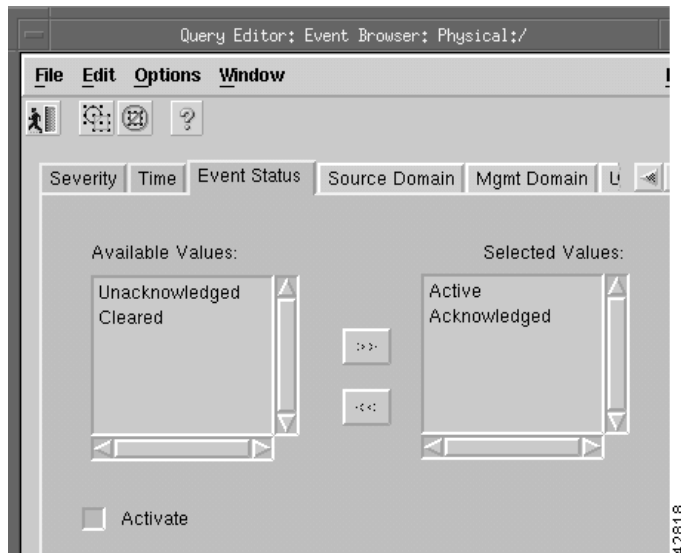
Figure 8-10 Query Editor Screen—Time Tab



- Step 5** Select the time range and the date range for collecting the alarms.
- Step 6** Click the **Event Status** tab.

You see the screen in Figure 8-11.

*Figure 8-11 Query Editor Screen—Event Status Tab*

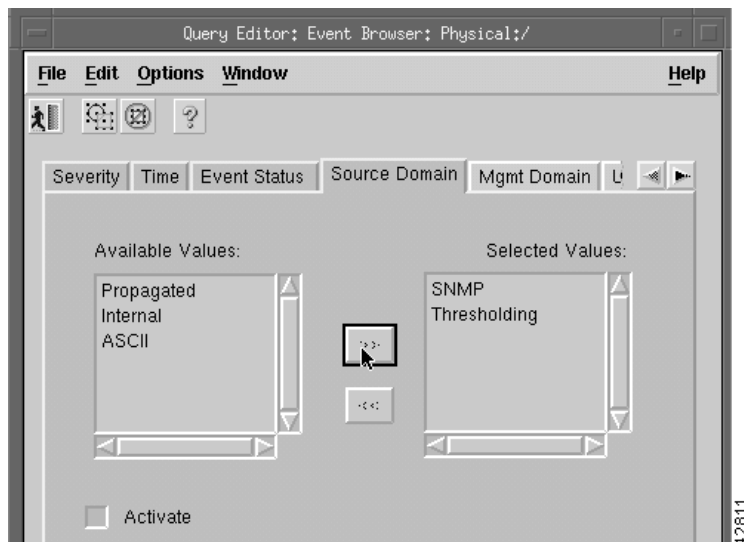


**Step 7** From the Available Values list, select the events and click the right arrows to transfer them to the Selected Values list.

**Step 8** Click the **Source Domain** tab.

You see the screen in Figure 8-12.

*Figure 8-12 Query Editor Screen—Source Domain Tab*

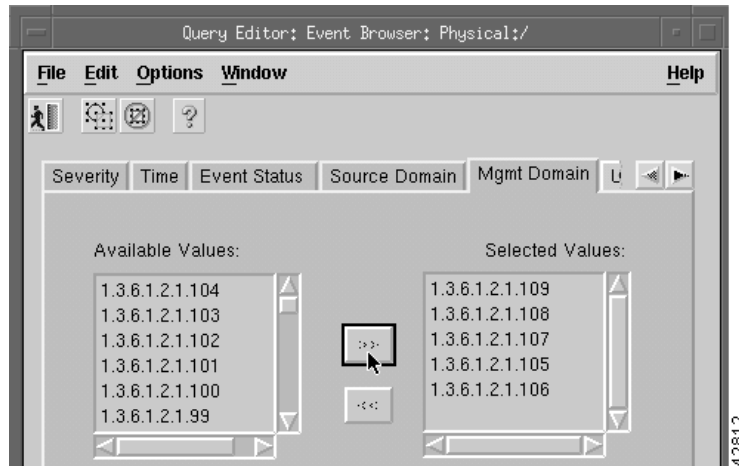


**Step 9** From the Available Values list, select Domain values and click the right arrows to transfer the values to the Selected Values list.

**Step 10** Click the **Mgmt Domain** tab.

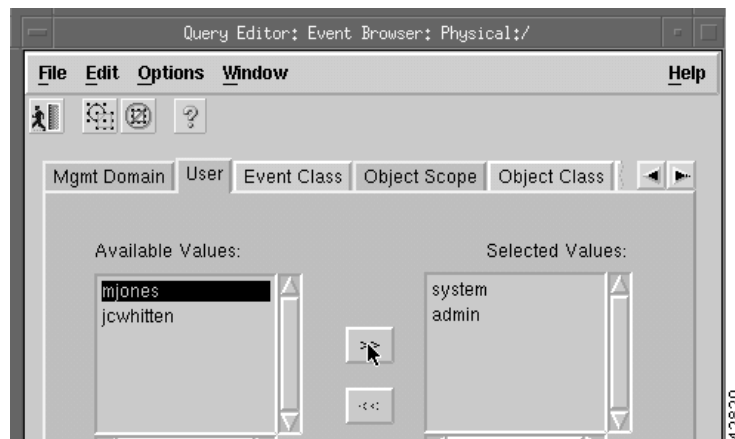
You see the screen in Figure 8-13.

Figure 8-13 Query Editor Screen—Mgmt Domain Tab



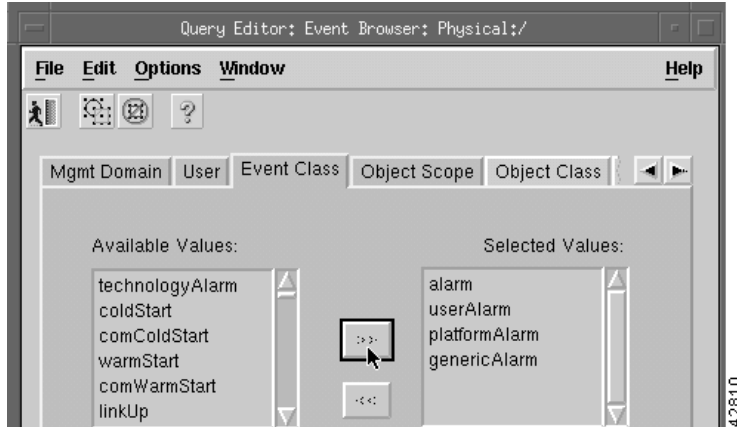
- Step 11** From the Available Values list, select management domains and click the right arrows to transfer the values to the Selected Values list.
- Step 12** Click the arrows on the right side of the tabs to scroll to additional tabs.
- Step 13** Click the **User** tab.  
You see the screen in Figure 8-14.

Figure 8-14 Query Editor Screen—User Tab



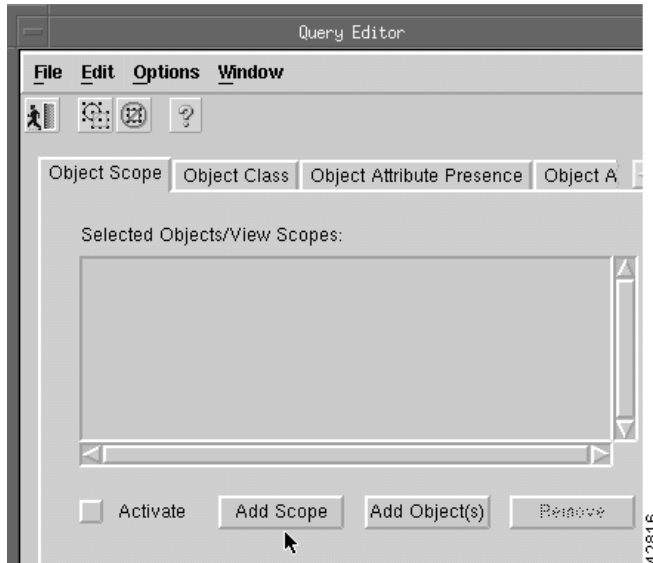
- Step 14** From the Available Values list, select users and click the right arrows to transfer the values to the Selected Values list.
- Step 15** Click the **Event Class** tab.  
You see the screen in Figure 8-15.

Figure 8-15 Query Editor Screen—Event Class Tab



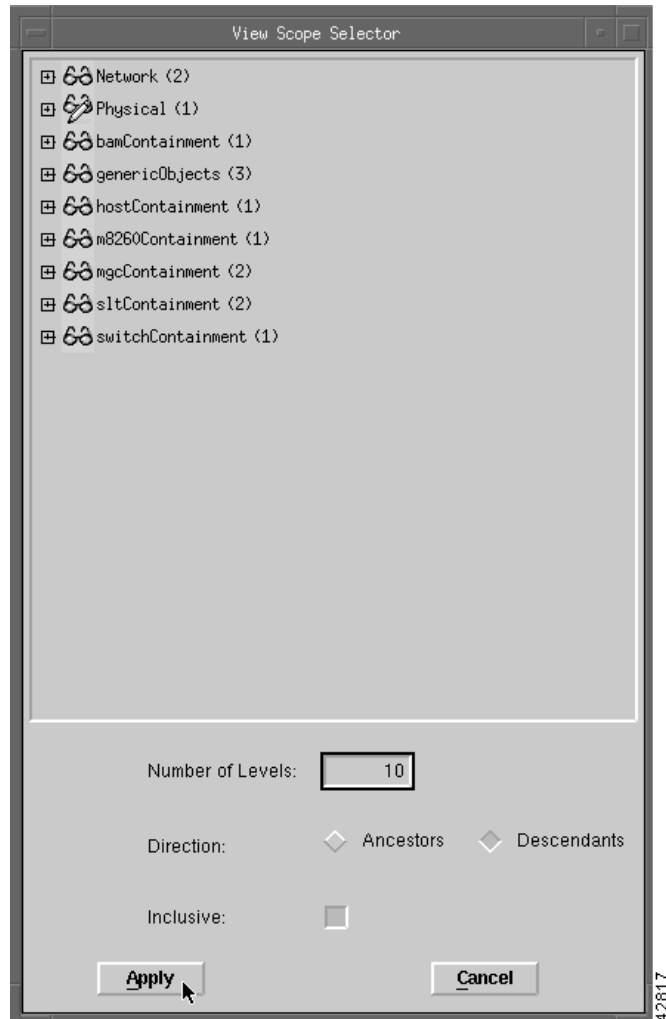
- Step 16 From the Available Values list, select event classes and click the right arrows to transfer the values to the Selected Values list.
- Step 17 Click the **Object Scope** tab to display all the events of a node and all its children.  
You see the screen in Figure 8-16.

Figure 8-16 Query Editor Screen—Object Scope Tab



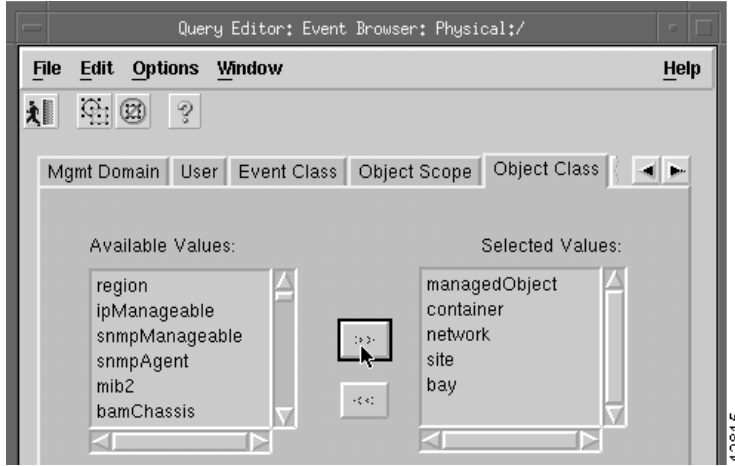
- Step 18 Click **Add Scope**.  
You see the screen in Figure 8-17.

Figure 8-17 View Scope Selector Screen



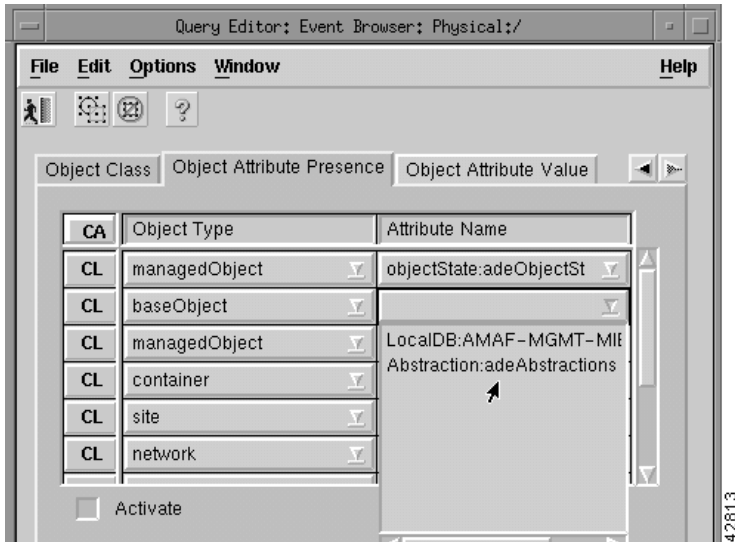
- Step 19** In the View Scope selector, select the node.
- Step 20** Type the number of levels to view. This can be more than needed.
- Step 21** Click the diamond to the left of Descendants and click **Apply**.
- Step 22** On the Query Editor screen, click the **Object Classes** tab.  
You see the screen in Figure 8-18.

Figure 8-18 Query Editor Screen—Object Class Tab



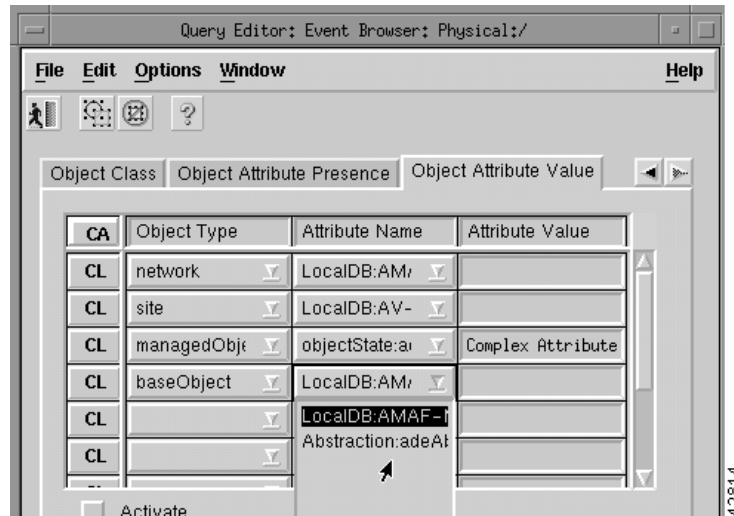
- Step 23 From the Available Values list, select the desired object classes and click the right arrows to transfer the values to the Selected Values list.
- Step 24 Click the **Object Attribute Presence** tab. Click a pull-down menu under Object Type to select a value and click a pull-down menu under Attribute Name to select a value, as shown in Figure 8-19.

Figure 8-19 Query Editor Screen—Object Attribute Presence Tab



- Step 25 Click the **Object Attribute Value** tab. Click a pull-down menu under Object Type to select a value, click a pull-down menu under Attribute Name to select a value, and click a pull-down menu under Attribute Value to select a value, as shown in Figure 8-20.

Figure 8-20 Query Editor Screen—Object Attribute Value Tab



**Step 26** After all values are set, click **Apply** and close the Query Editor.

You see the following message:

Save Query Changes?

**Step 27** Click **Yes**.

The Event Browser begins collecting the data using the criteria you selected and displays it in the Event Browser window.



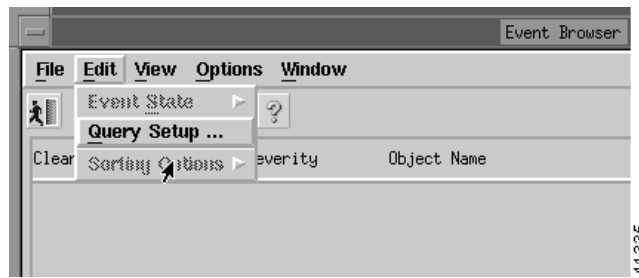
**Note** Query changes are saved for the immediate session only. When you close the Event Browser, the query criteria is reset to the default.

## Modifying Filtering Criteria

You can change the alarm criteria displayed in the Event Browser at any time by launching the Query Editor and changing the values.

**Step 1** To change the criteria, from the Edit menu on the Event Browser, select **Query Setup**, as shown in Figure 8-21.

Figure 8-21 Event Browser—Edit>Query Setup Option



- Step 2 Set up the query by selecting values as described in the “Setting Filtering Criteria” section on page 8-16.
- Step 3 Close the Query Setup screen. The Event Browser displays the data.

## Sorting Events

Query Editor configuration allows you to specify the events you want to see. Sorting gives you options to change the order in which you view the events that match your query criteria.

### Setting Up Sort Options

From the Edit menu, select **Sorting Options**. A pull-down menu is displayed listing the available sorting options. An indicator shows which option is selected. Selecting an option causes the Event Browser display to change to show the appropriate information. The sort option selected is shown in the status bar. You can sort by:

- Time—Shows the most recent event first
- Event Class—Allows you to sort event classes
- Event State—If the query is set up to show all states, this option shows events in the following order:
  - Unacknowledged/Active
  - Acknowledged/Active
  - Cleared/Unacknowledged
  - Cleared/Acknowledged.
- Managed Object—Sorts by the name of the managed object on the network



**Note** Set the option to show full name before sorting by name.

- Severity— If the query was set up to show all severities, this option shows events in the following order:
  - Critical
  - Major
  - Minor
  - Warning
  - Normal



- Decommission
- Informational

## Managing Events

When the Event Browser shows a sorted list of events that match the query criteria set, you can start to manage those events. This is the place to acknowledge an event, which shows that you have taken responsibility for managing that event. If you cannot continue to manage an event, it can be unacknowledged and then becomes available to other users.



Note

---

The option to unacknowledge an event is available only to an administrator or to the user who acknowledged the event initially.

---


When the fault has been rectified and the event requires no further attention, clear the event. It is then removed from the Event Browser.

Three methods are available for managing events:

- Two indicators (Clear and Ack) are available to the left of the object name. Select or deselect the indicator associated with an event in the Event Browser window.
- Use the Edit menu.
- Right-click a selected event to display a pop-up menu of options available on that event.

Clicking an event severity, name, time, or description selects that event. One or more events can be selected; this gives you the opportunity to perform bulk operations.

## Managing an Event from the Window

- 
- Step 1** To clear the event, select the indicator associated with the event or select the object and click the **Clear Events** icon  on the Toolbar.

This displays the Events Clearing window. Enter the reason for clearing the event, then click **Apply** to save or click **Cancel** to exit the window without saving. The indicator changes to the new color of the severity of the event.

- Step 2** Select the **Ack** indicator to Acknowledge an event. The indicator changes to the color of the severity of the event. To Unacknowledge an event, select the **Ack** indicator, which is then shown as deselected.



Note

---

This option is available only to the user who acknowledged the event or to a user with administrative access.

---

## Managing an Event from the Menu Bar

From the Edit menu, you can select the **Edit Event State** option. A pull-down menu is displayed, which provides options to manage the events.

- **Clear Events**—Allows you to clear the event. When you select this option, the Events Clearing window is displayed. Enter a reason then click **Apply** to save the details or click **Cancel** to exit without saving.
- **Acknowledge Events**—Allows you to acknowledge an event.
- **Acknowledge Events with comment**—Allows you to record a reason for acknowledging an event. When you select this option, the Acknowledge Events window is displayed. Enter a reason then click **Apply** to save the details or click **Cancel** to exit without saving.
- **Unacknowledge Events**—Allows you to unacknowledge an event.




### Note

This option is available only to the user who acknowledged the event or to a user with administrative access.

## Enabling Auto or Manual Update

Auto Update is the default state and allows you to view incoming events that are automatically updated in the window.

The status box displays the current update state; either Auto or Manual. If Auto Update is enabled, the status box displays Auto Update.

When the update state is Manual (Auto Update is disabled), you should refresh the window at regular intervals using the View menu's **Refresh** option or the Refresh icon  so that new events are displayed.

To enable auto update:

- Step 1** From the View menu, select **Enable Auto Update**. The message in the status box changes to Auto Update.



### Note

If an indicator is displayed on the pull-down menu, to the left of Enable Auto Update, the Auto Update application is enabled.

To enable manual update:

- Step 1** From the View menu, deselect **Enable Auto Update**.



### Note

The message in the status box changes to Manual Update.

## Setting How Events Are Color-Coded

Three color-coding options are available to you. The color you choose depends on the severity of the event. The options are as follows:

- **Full Color-Coding**—When this option is selected, the severity information displayed has text on a colored background.
- **Partial Color-Coding**—When this option is selected, the Severity column is colored. The color of the column depends on the severity of the event.
- **No Color-Coding**—When this option is selected, text only is displayed in the Severity column.

## Selecting the Type of Color Coding to Be Used

- 
- Step 1** From the View menu, select **Set Color Coding**.
- Step 2** From the menu that appears, select one of the options.  
The selected option is implemented immediately.
- 

## Viewing the Event History

Event history allows you to display any events that match the current query criteria and have had their state changed, either acknowledged, cleared, or unacknowledged. This is disabled by default. To view this information, select the View menu's **Event History** option.

To view the event history:

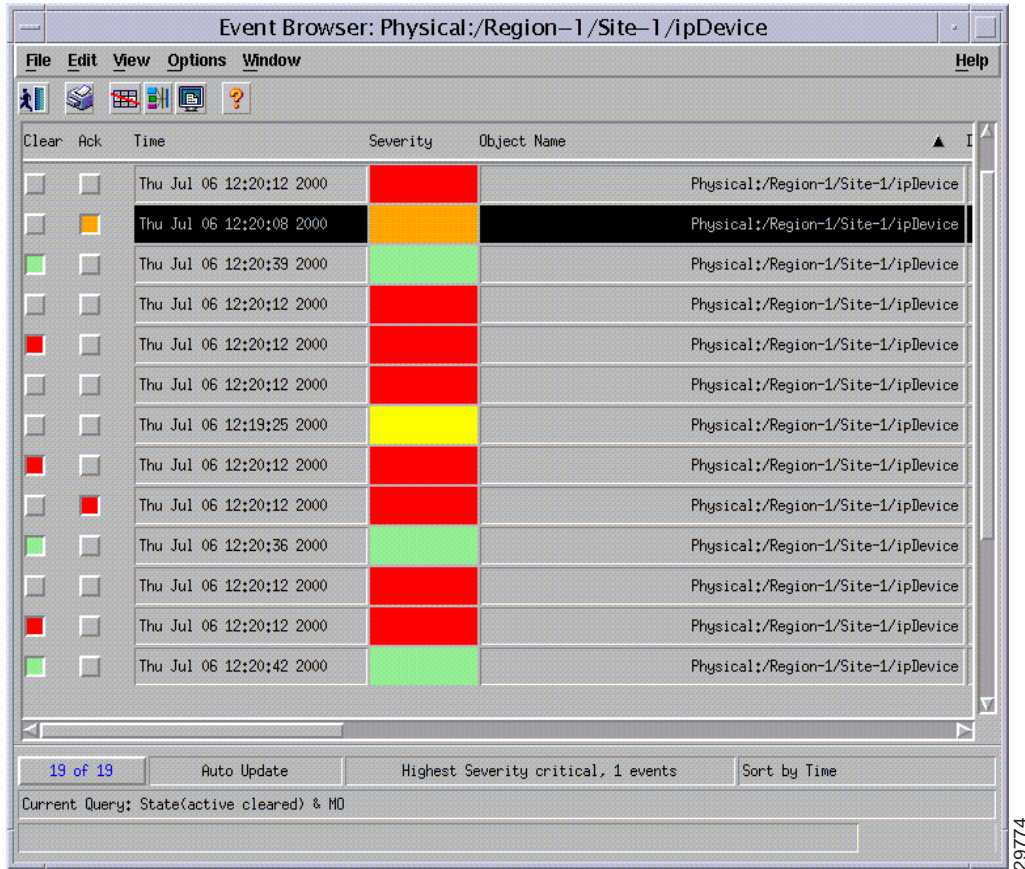
- 
- Step 1** Configure the event query (refer to the “Filtering Events Using Queries” section on page 8-15.)  
The Event Browser displays current events that match the criteria set in the query.
- Step 2** From the View menu, select **Event History**.  
The Event Browser now displays any events that meet that query and have been cleared.



**Note** By default, cleared events are stored by the system for seven days. Therefore, only events that match the current query and have had their state changed in the last seven days, are displayed when the Event History is enabled.


---

Figure 8-22 Event History Enabled Screen



## Refreshing the Event Window

Ensure that Manual Update is selected; this is shown as a current status message. You can then:

- From the View menu, select **Refresh**.
- Click the Refresh icon  on the Toolbar.

The window is refreshed.



### Note

You should refresh the window at regular intervals to show an up-to-date list of events.

## Viewing a Full Description of an Event

Double-clicking an event displays the Full Event Description window. This provides details of the event with Acknowledge and Clearing details.

To view a full description of an event:

Place the cursor over the relevant event in the Event Browser, then double-click the left mouse button or select **Event Description**, then select **Event Information Dialog** from the pop-up menu available on a selected object.

A window similar to Figure 8-23 is displayed.

*Figure 8-23 Full Event Description Screen*



**Note**

If the event has not been cleared, the Event State displays Active and the Clearing Method, User Responsible for Clearing, Clearing Time and Date sections are disabled. The information displayed cannot be altered.

If an event has been cleared, you can view the method used to clear it by clicking **Clearing Event**.

The Full Event description window displays the following information:

- Object name—Name of the CEMF managed object the event was reported against
- Time and Date—The time and date the event was reported
- Severity—The severity of the reported event
- Source Domain—Indicates from which Communications domain the event was reported
- Management Domain—Indicates from which Management domain the event was reported
- Event Description—Provides a brief description of the reported event

- **Event State**—Indicates whether the event is active or cleared. If the event has been cleared, the **Clearing Method**, **User Responsible for Clearing**, and **Clearing Time and Date** sections become active.

## Acknowledge Details

- **Acknowledgement User**—Identifies the user who acknowledged the event
- **Acknowledgement Time and Date**—Identifies when the event was acknowledged

## Clearing Details

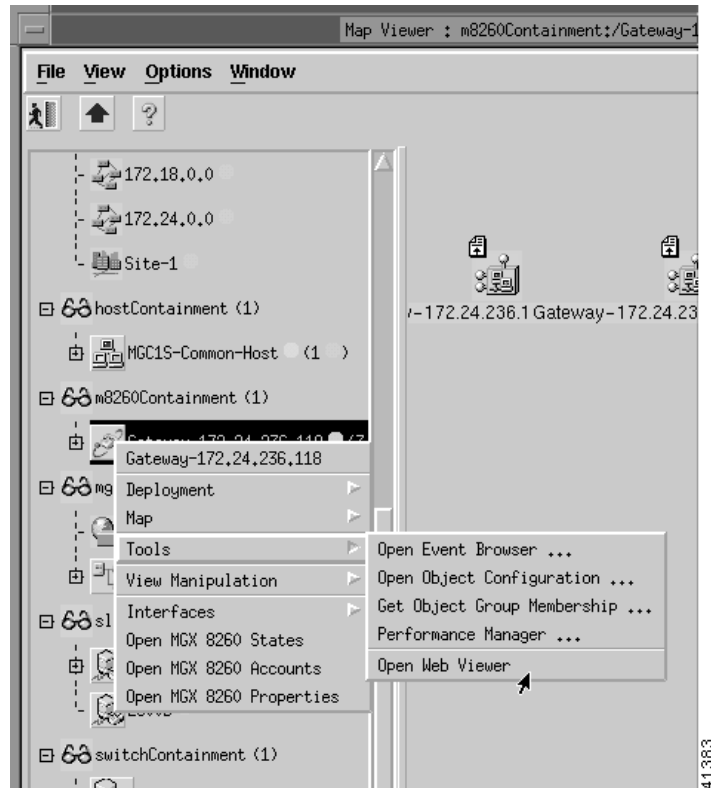
- **Clearing Method**—Indicates if the event was cleared by the network or by a user.
- **User Responsible for Clearing**—Displays the user name responsible for clearing the event.
- **Clearing Time and Date**—Indicates the time and date the event was cleared.
- **Reason for clearing**—The information that was entered in the Events Clearing window, which is completed when the Clear indicator is selected.

# Managing Cisco MGX 8260 Faults

You can view and manage faults on the Cisco MGX 8260 with the Web View tool. To use Web View:

- 
- Step 1** Select the Cisco MGC 8260 icon, right-click to display the pull-down menu, click **Tools**, then **Open Web Viewer**, as shown in Figure 8-24.

Figure 8-24 Map Viewer Screen—Tools&gt;Open Web Viewer Option



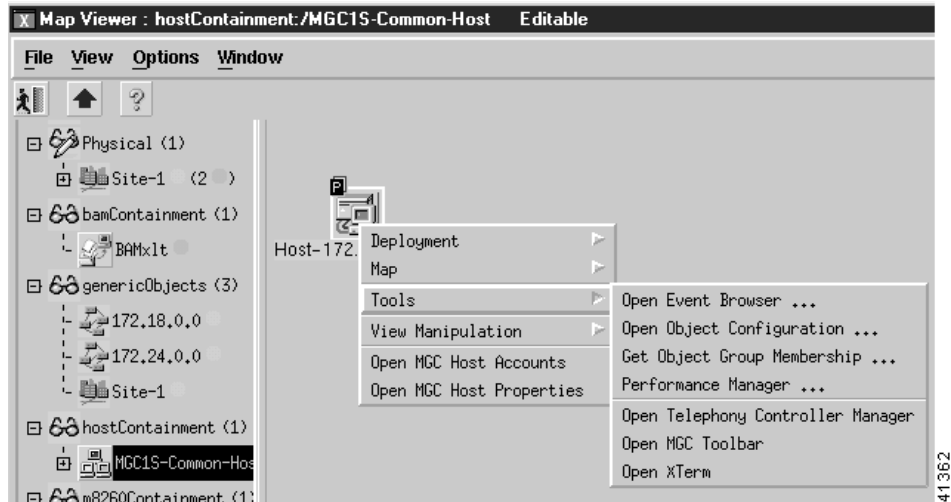
Step 2 When the Web Browser displays, type your user ID and password and click **Login**.

## Using the Cisco MGC Tool Bar

You can manage Cisco MGC host faults and performance from the MGC Toolbar.

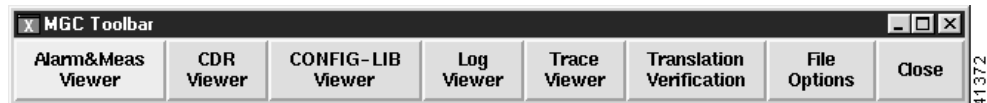
Step 1 Select the Cisco MGC common host, right-click to display the pull-down menu, select **Tools**, then select **Open MGC Toolbar**, as shown in Figure 8-25.

Figure 8-25 Map Viewer Screen—Tools&gt;Open MGC Toolbar Option



You see the screen in Figure 8-26.

Figure 8-26 MGC Toolbar



From the MGC Toolbar you can click the following buttons:

- Alarm&Meas Viewer—View alarms on the Cisco MGC host.
- CDR Viewer—View call detail records (CDRs).
- CONFIG-LIB Viewer—Configure a library.
- Log Viewer—View a log file.
- Trace Viewer—View a trace file.
- Translation Verification—Verify a translation.
- File Options—View a configuration of the files.
- Close—Close the MGC Toolbar.

## Alarm and Measurements Viewer

- Step 1 On the MGC Toolbar, click **Alarm&Meas Viewer** to view alarms on the Cisco MGC host.

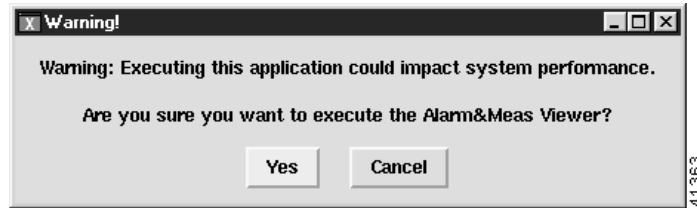


Figure 8-27 MGC Toolbar—Alarm&amp;Meas Viewer Option



You see the screen in Figure 8-28.

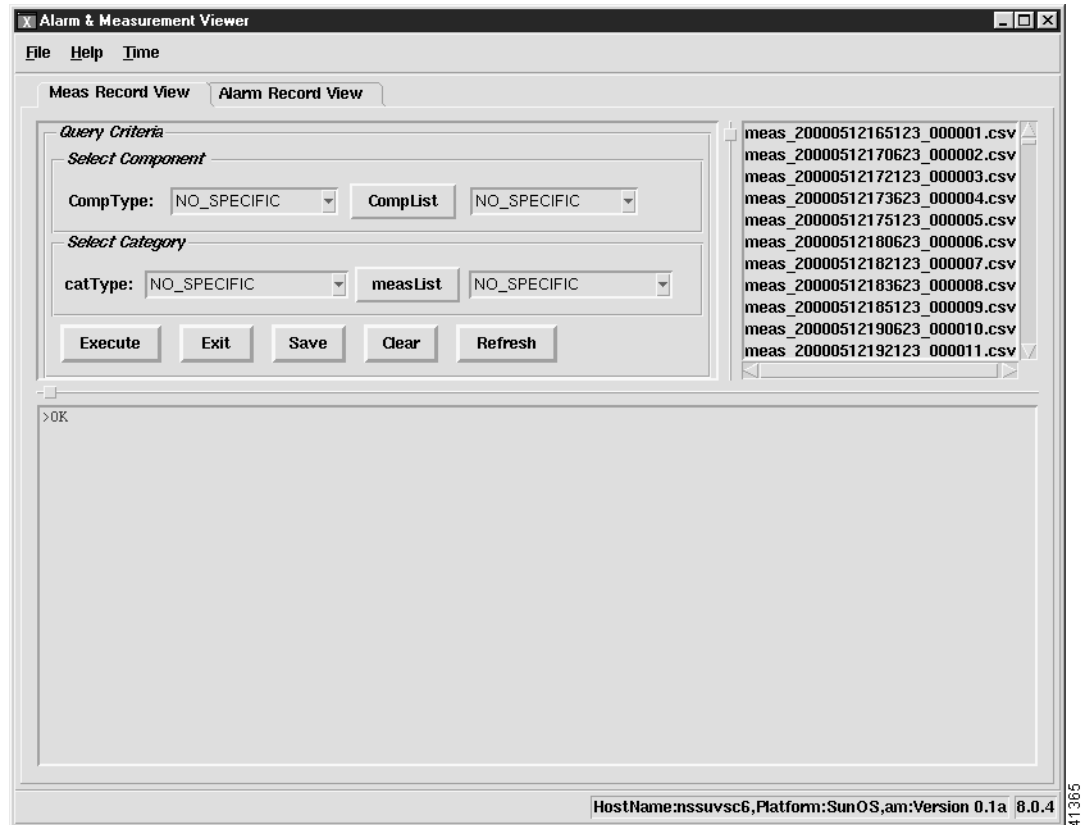
Figure 8-28 Alarm&amp;Meas Viewer Warning Screen



Step 2 Click **Yes**.

You see the screen in Figure 8-29.

Figure 8-29 Alarm &amp; Measurement Viewer Screen—Meas Record View Tab

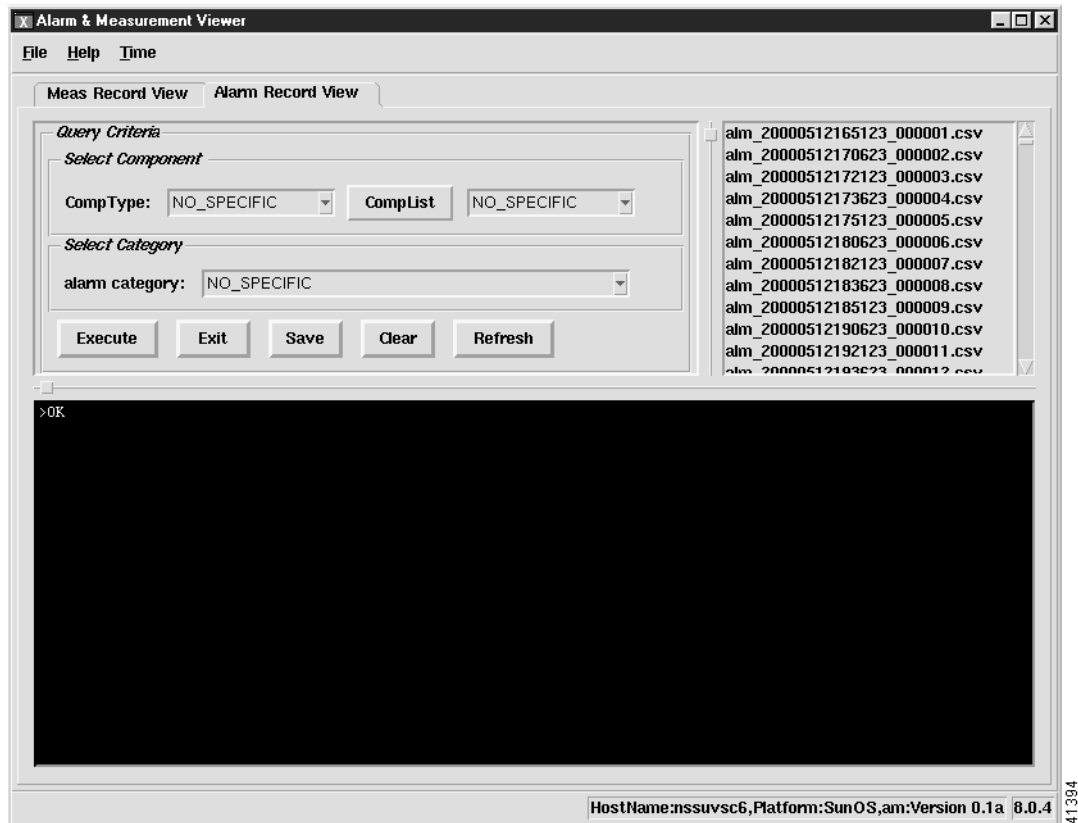


Step 3 In the Select Component box, use the Comp Type and Complist pull-down menus to select values.

Step 4 In the Select Category box, use the catType and measList pull-down menus to select values.

- Step 5** Select a file from the list on the right of the screen.
- Step 6** Click **Execute** to run the query.  
The results appear in the box at the bottom of the screen.
- Step 7** Click the **Alarm Record View** tab to display alarm records.  
You see the screen in Figure 8-30.

*Figure 8-30 Alarm & Measurement Viewer Screen—Alarm Record View Tab*

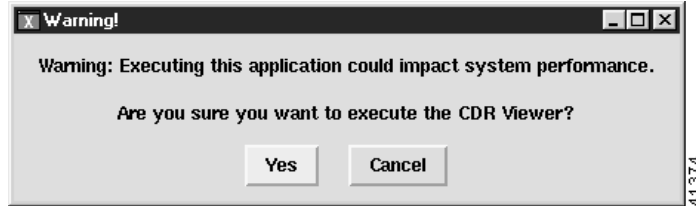


- Step 8** In the Select Component box, use the Comp Type and Complist pull-down menus to select values.
- Step 9** In the Select Category box, use the alarmCategory pull-down menu to select a value.
- Step 10** Select a file from the list on the right of the screen.
- Step 11** Click **Execute** to run the query.  
The results appear in the box at the bottom of the screen.

## CDR Viewer

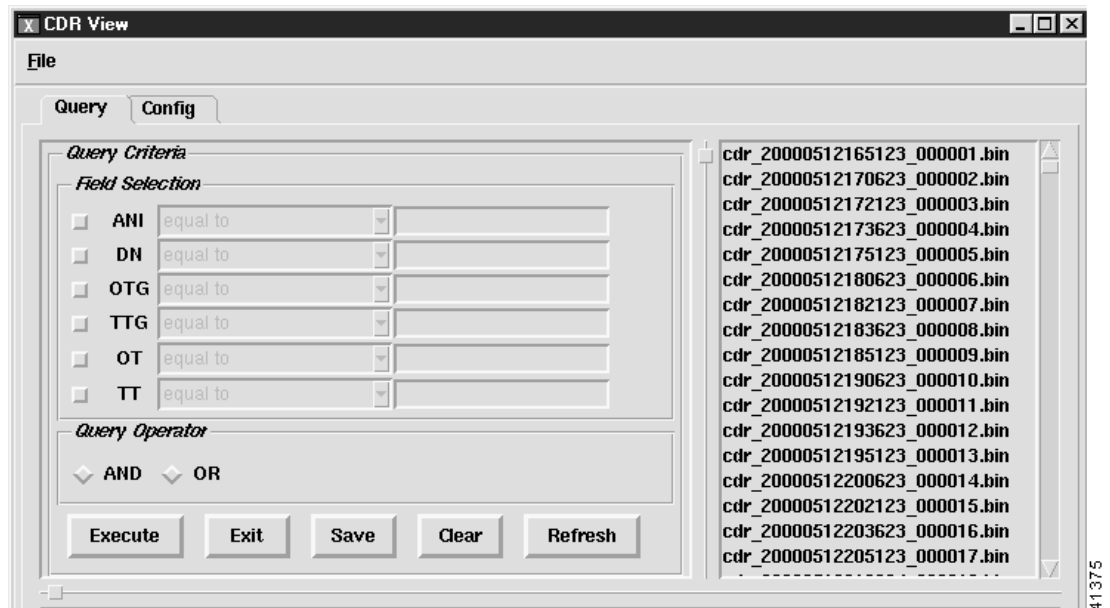
- Step 1** On the MGC Toolbar, click **CDR Viewer** to view CDR records.  
You see the screen in Figure 8-31.

Figure 8-31 CDR Viewer Warning Screen



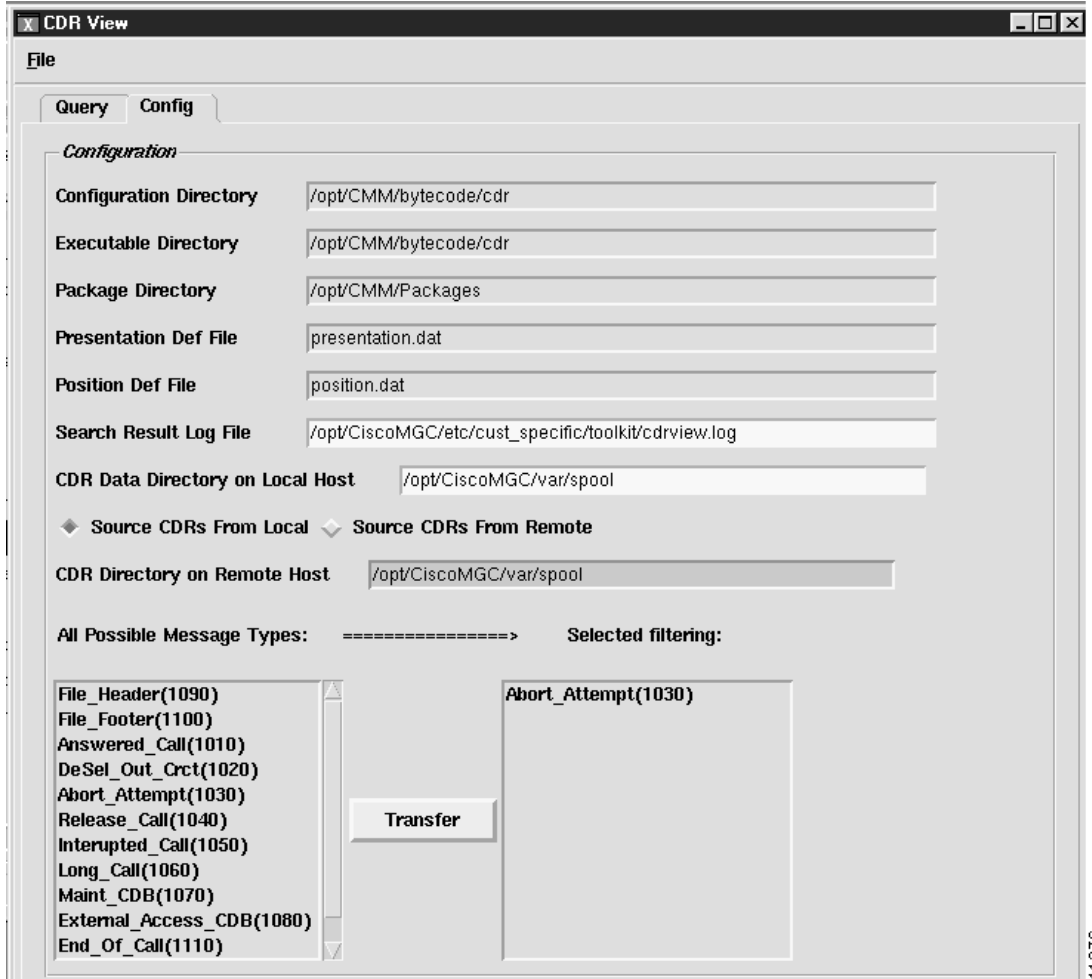
- Step 2** Click **Yes** to proceed.  
 You see the screen in Figure 8-32.

Figure 8-32 CDR View Screen—Query Tab



- Step 3** Select an action to perform.  
**Step 4** Click the **Config** tab.  
 You see the screen in Figure 8-33.

Figure 8-33 CDR View Screen—Config Tab

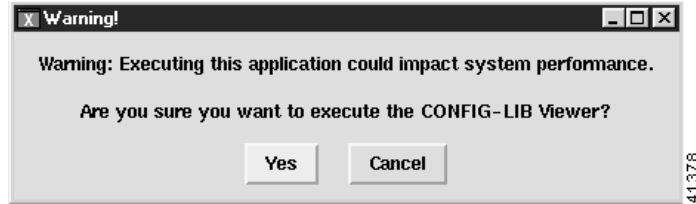


- Step 5 From the All Possible Message Types list, select the messages you want to filter and click **Transfer** to transfer them to the Selected filtering list.

## CONFIG-LIB Viewer

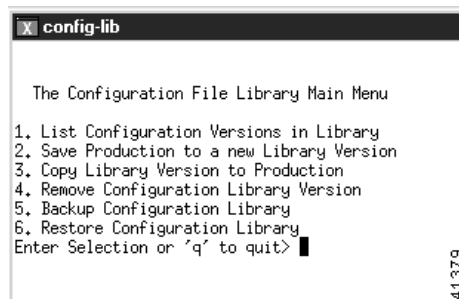
- Step 1 On the MGC Toolbar, click **CONFIG-LIB Viewer** to configure a library.  
You see the screen in Figure 8-34.

Figure 8-34 CONFIG-LIB Viewer Warning Screen



- Step 2 Click **Yes** to continue.  
You see the screen in Figure 8-35.

Figure 8-35 config-lib Screen



- Step 3 Enter the number of the list item to be executed and press **Enter**.

## Log Viewer

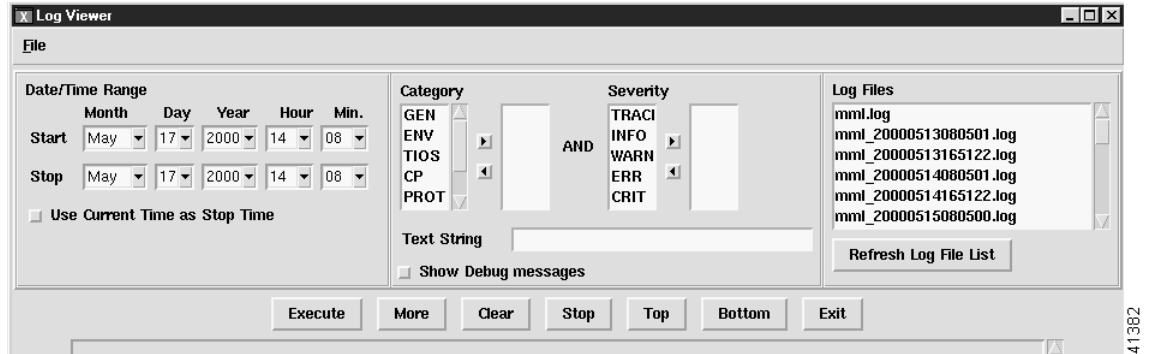
- Step 1 On the MGC Toolbar, click **Log Viewer** to view a log file.  
You see the screen in Figure 8-36.

Figure 8-36 Log Viewer Warning Screen



- Step 2 Click **Yes** to proceed.  
You see the screen in Figure 8-37.

Figure 8-37 Log Viewer Screen

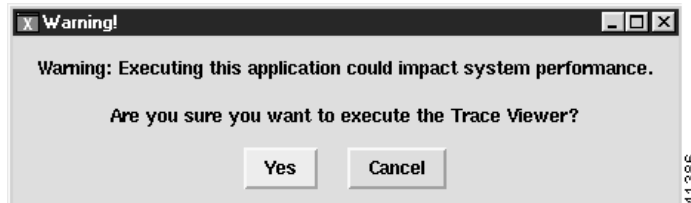


- Step 3 Select categories and severities from the lists, then select a log file.
- Step 4 Select an action to execute.

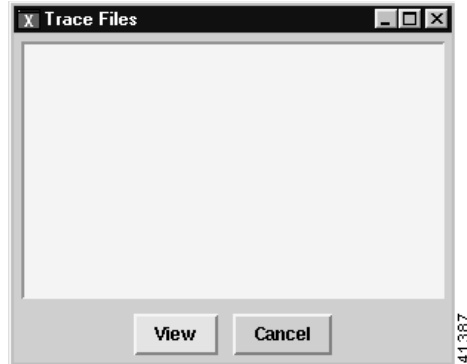
## Trace Viewer

- Step 1 On the MGC Toolbar, click **Trace Viewer** to view a trace file.  
You see the screen in Figure 8-38.

Figure 8-38 Trace Viewer Warning Screen



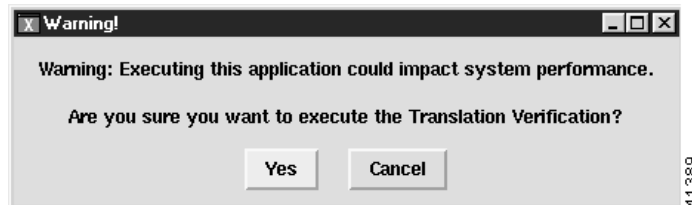
- Step 2 Click **Yes** to continue.  
You see the screen in Figure 8-39.

*Figure 8-39 Trace Files Screen*

- Step 3 Select a trace file to view and click **View**.
- 

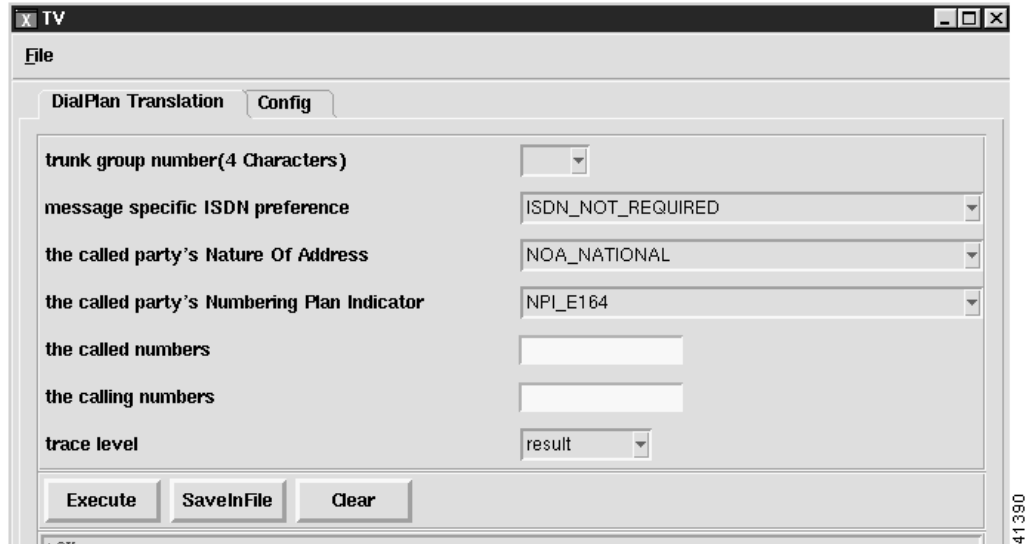
## Translation Verification

- Step 1 On the MGC Toolbar, click **Translation Verification** to verify a translation. You see the screen in Figure 8-40.

*Figure 8-40 Translation Verification Warning Screen*

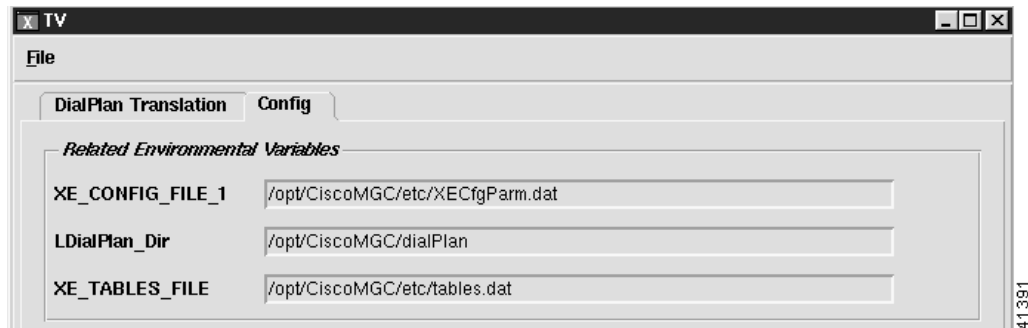
- Step 2 Click **Yes** to continue. You see the screen in Figure 8-41.

Figure 8-41 Translation Verification Screen—DialPlan Translation Tab



- Step 3 Type a four-digit dial plan number in the field provided.
- Step 4 Click **Execute** to finish.
- Step 5 Click **SaveInFile** to save the data in a file for later viewing.
- Step 6 Click the **Config** tab to display related environmental variables.
- Step 7 You see the screen in Figure 8-42.

Figure 8-42 Translation Verification Screen—Config Tab



## File Options

- Step 1 On the MGC Toolbar, click **File Options** to view a configuration of the files.  
You see the screen in Figure 8-43.



Figure 8-43 File Options Screen



Step 2 Click a file, then click an action to execute it.

## Setting How Long Alarms Are Stored

All alarms are automatically stored in the CEMF database. Periodically CEMF purges the alarms from the database to free up room for new alarms.

The alarmDeleter utility controls the deletion of alarms. CEMF does not do any archiving of old alarms, but it can be configured to delete alarms of a specific age and state. Upon installation a cron job is set up to run the Alarm Deleter at midnight every night. At this time, the Deleter queries the alarm database, deleting alarms that meet the specified criteria. The alarmDelete.ini file, shown below, allows you to define these rules. The default is to delete cleared alarms that are seven days old.

```
[logger]
#include "loggercommon.include"
loggingName = alarmDeleter

[AlarmDeleter]
databaseName      = [[OSDBROOT]]/alarm.db
segmentDeletionInterval = 15
ageOfAlarmsInDays= 7
ageOfAlarmsInHours= 0
ageOfAlarmsInMinutes    = 0
deleteAllAlarms= 0

[Database]
#include "databaseCommon.include"
```

The variables used in defining the deletion rules are described in Table 8-8.

*Table 8-8 Alarm Deleter Attributes*

Variable	Description
ageOfAlarmsInDays	The age of the alarm, in days, before it is to be deleted.
ageOfAlarmsInHours	The age of the alarm, in hours, before it is to be deleted.
ageOfAlarmsInMinutes	The age of the alarm, in minutes, before it is to be deleted.
deleteAllAlarms	0 = delete only cleared alarms that match criteria; 1 = delete both active and cleared alarms that match criteria.