



CHAPTER 9

Managing Faults

This chapter describes the process of fault management (FM), and details the options available in Cisco Prime Optical to locate, diagnose, and report network problems.

This chapter includes the following information:

- [9.1 What Is Fault Management?, page 9-1](#)
- [9.2 Where Can I Get Information on Affected Services and Customers?, page 9-3](#)
- [9.3 What Fault Information Can I See?, page 9-14](#)
- [9.4 Is the Service Working?, page 9-15](#)
- [9.5 Where Is the Fault?, page 9-27](#)
- [9.6 How Can I Find the Root Cause of the Fault?, page 9-32](#)
- [9.7 Who Is Responsible for Managing the Fault?, page 9-41](#)
- [9.8 How Can the Fault Be Fixed?, page 9-42](#)

9.1 What Is Fault Management?

Fault management is the process of locating, diagnosing, and reporting network problems. This is important for increasing network reliability and effectiveness, and for increasing the productivity of network users. Fault management is more than just handling emergencies. It provides functions for managing problems with services and handling customer-facing service problems.

Efficient fault management can:

- Save repair costs through efficient fault detection, location, and correction
- Improve customer care through efficient trouble administration
- Improve service availability and equipment reliability through proactive maintenance and through measurement, review, and corrective action

One responsibility of fault management is to detect faults. A piece of equipment, a transmission medium, a software module, or a database is said to be in a fault state if it cannot perform its intended function and meet all of the requirements placed on that function. The onset of a fault is called a *failure event* and is usually signaled by one or more alarm reports. The termination of a fault state is called a *clear event*.

Fault management is responsible for determining, from a variety of information sources, the root cause of a fault, and for its repair. In certain cases, the root cause of a fault might be in a connecting network. In such cases, fault management is responsible for reporting the problem through appropriate channels.

Service assurance is the overall process of ensuring that the purchased level of service is delivered. The Element Management System (EMS) plays a key role in maintaining the health of both NEs and transmission facilities. This is done in conjunction with other systems, typically at the network management layer and service management layer. The EMS can be the primary repository of detailed history of NE-specific faults and events, technician action, and performance data.

The steps for successful fault management are:

1. Identify a problem by gathering data about the state of the network (polling and trap generation).
2. Restore any services that have been lost.
3. Isolate the cause, and decide if the fault should be managed.
4. Correct the fault if possible.

9.1.1 What the NE Provides

Currently deployed, intelligent NEs provide the management system with the following, which are required for effective fault management:

- Detection of the four main types of failure:
 - Equipment failure—Detected through failure detection mechanisms built into the hardware, and through routine exercises and diagnostics.
 - Software failure—Detected through failure of software checks, and through routine audits.
 - Communication failure—Detected through defects in the incoming signal or outgoing signal characteristics. Defects include line coding errors, framing bit errors, parity errors, cyclic redundancy check errors, and addressing errors. Signal characteristics include optical or electrical power, analog signal-to-noise ratio, and deviation from required voltage or wavelength.
 - Environmental failure.
- Notification of failure—NEs notify a management system when a failure occurs by generating an alarm report. The NE can also report a summary of current fault states, or replay its log of historical failures and clears.
- Notification of changes in operational state of the NE components—If a component of the NE is in a fault state, a management system should not receive further alarms, alerts, or scheduled performance data from that component.



Note

Prime Optical forwards northbound information and integrates with other third-party management systems to give options that are not directly available in Prime Optical.

9.1.2 Fault Notification and Maintenance

Fault notification and maintenance can be proactive or reactive:

- Proactive notification—Where *X* contacts *Y* to query *Y* on potential problems in *Y*'s domain.
- Reactive maintenance—Where *Y* notifies *X* of a problem regarding a service delivered from *Y* to *X*.

9.1.2.1 Proactive Maintenance

Automated detection tests and surveillance software enable rapid initiation of the repair process, sometimes even before customers have noticed a problem. This is called proactive maintenance and promotes customer satisfaction.

Proactive maintenance consists of functions and processes associated with the detection, analysis, isolation, and resolution of problems by means that are independent of customer trouble reports. The problems might be faults or degradations in equipment or transmission media.

The goals of proactive maintenance are to:

- Detect and fix service quality problems before the customer calls to establish a trouble report, or at least to start the repair process before the customer calls, thereby minimizing the time, as perceived by the customer, before service is restored.
- Maintain the transport network at a high level of quality by identifying the facilities that perform relatively poorly and rehabilitating them.

9.1.2.2 Reactive Maintenance

Reactive maintenance is required when a failure occurs. This type of problem can be time-consuming and costly. It requires accurate administration of trouble reports, rapid analysis and repair of service-affecting faults, and notifications to the customer of restoration of service, all of which also promote customer satisfaction.

9.1.3 Root Cause Analysis

The *root cause* is the most basic reason for an undesirable condition or problem that, if eliminated or corrected, would have prevented the problem from occurring. The outcome of the root cause analysis is not a restatement of the most obvious symptom, but is the result of a methodical analysis of the problem situation, leading to the most basic cause.

Root cause analysis captures additional information about defects for the purpose of identifying preventive actions. Prime Optical includes advanced debugging features that capture additional information about defects.

9.2 Where Can I Get Information on Affected Services and Customers?

The first thing to do in fault management is to identify what services and which customers are affected by the fault. Prime Optical provides a number of options for viewing this information. The following table describes where to obtain information on affected services and customers.

Table 9-1 *Obtaining Information on Affected Services and Customers*

Where	Description	For More Information, See
Dashboard	Shows useful alarm and NE information in one easily accessible location.	1.5.1 Dashboard, page 1-9
Tooltips	Visible when you position the cursor over a managed object (domain, group, subnetwork, NE, board, link, and so on). The tooltip displays additional information about the selected object.	—
Domain Explorer	Home window; provides a logical view of the network plus alarm, connectivity, and operational status.	1.5.2 Domain Explorer, page 1-10
Subnetwork Explorer	Similar in appearance and function to the Domain Explorer. A key difference is that the Subnetwork Explorer provides a single-level grouping of NEs based on network partitions and subnetworks.	1.5.3 Subnetwork Explorer, page 1-23
Network Map	Displays a geographical layout of the network.	1.5.6 Network Map, page 1-29
Alarm Browser	Displays standing alarms and conditions in the managed domain that are assigned a severity level of critical, major, minor, or warning. It also shows cleared alarms that are not acknowledged.	9.2.1 Viewing the Alarm Browser, page 9-4
Alarm Log	Contains alarms that have transitioned from the Alarm Browser.	9.2.4 Viewing the Alarm Log, page 9-8

9.2.1 Viewing the Alarm Browser

The Alarm Browser displays standing alarms and conditions in the managed domain that are assigned a severity level of critical, major, minor, or warning. It also shows cleared alarms that are not acknowledged. The Alarm Browser and Alarm Log views provide a robust listing of all current and historical alarms and events. See [9.2.4 Viewing the Alarm Log, page 9-8](#) for information about the Alarm Log.

To display the Alarm Browser, select an NE, group, subnetwork, or domain node from the Domain Explorer, Subnetwork Explorer, Network Map, or NE Explorer; then, choose **Fault > Alarm Browser** (or click the **Open Alarm Browser** tool from the Dashboard).



Note

- No alarms or events are generated in the Alarm Browser if Oracle shuts down.
- Refer to the appropriate NE documentation for a list of alarms supported on each NE. See [1.7.2 Related Cisco NE Documentation, page 1-50](#).
- Use the toolbar icons to manage the alarm display. See [Appendix A, “Icons and Menus Displayed in Prime Optical”](#) for an explanation of each toolbar icon.

The following table describes the fields in the Alarm Browser.

Table 9-2 *Field Descriptions for the Alarm Browser Window*

Field	Description
Alarm ID	Unique number that the system uses to identify a particular alarm.
Perceived Severity	<p>Perceived severity of the selected alarm (critical, major, minor, or warning). The background color also indicates the severity, where:</p> <ul style="list-style-type: none"> Red = Critical Orange = Major Yellow = Minor Blue = Warning Green = Cleared <p>Note For the ONS 15530 and ONS 15540, alarms that are shown in the command-line interface (CLI) as informational are shown in Prime Optical as warnings.</p>
Acknowledged	Whether the selected alarm has been acknowledged by the user. Values are Yes and No.
Note	Any notes that were entered for the selected alarm. If you choose Fault > Show Alarm Note (or click the Show Alarm Note tool), you can see the login name of the user who entered the note and the time when the note was entered.
Alias ID	Alias name of the NE.
Probable Cause	<p>Probable cause of the selected alarm. Some possible values include:</p> <ul style="list-style-type: none"> Not Applicable/Unknown—If no additional information is available Mismatch of equipment and attributes (MEA) alarm—For misconfigured pluggable port modules (PPMs) Link Layer Keep-Alive Failure—When the keepalive frame on the POS port is disabled and the port is shut down Bad Packet Count Exceeds Threshold—When the packets through the front port have CRC errored frames Auto-Negotiation Remote Failure Indication—When a remote Gigabit Ethernet port is shut down from a local port
Condition	Error message or condition name that is associated with the alarm or event.
Affected Object	Name of the object where the selected alarm occurred.
Module Name	Name of the module where the selected alarm occurred.
Physical Location	Physical location of the equipment where the selected alarm occurred, such as chassis, rack, subrack (shelf), slot, and port numbers.
Alarm Time Stamp	Date and time when the alarm occurred on the server.
NE Alarm Time Stamp	Date and time when the alarm occurred on the NE.
Service Affecting	<p>Whether the alarm or event is service affecting (SA). Values are:</p> <ul style="list-style-type: none"> Yes—The alarm is service affecting No—The alarm is not service affecting N/A—No information is provided by the NE
Clear Time Stamp	Date and time when the alarm was cleared on the server.

Table 9-2 *Field Descriptions for the Alarm Browser Window (continued)*

Field	Description
NE Clear Time Stamp	Date and time when the alarm was cleared on the NE.
Acknowledged Time Stamp	Date and time when the user acknowledged the selected alarm.
Acknowledged Username	Login name of the user who acknowledged the selected alarm.
Alarm Status	Status of the selected alarm (active or cleared).
Description	Additional information about the selected alarm. If there is no additional information, this field is blank.
Source ID	Name of the NE where the selected alarm occurred.
TL1 Direction	TL1 direction for RTRV-ALM-ALL and RTRV-COND-ALL TL1 commands and REPT^ALM/COND autonomous messages. Values are Receive or Transmit. This field is blank for non-TL1 alarms.
TL1 Location	TL1 location for RTRV-ALM-ALL and RTRV-COND-ALL TL1 commands and REPT^ALM/COND autonomous messages. Values are Near End or Far End. This field is blank for non-TL1 alarms.

9.2.2 Filtering Data in the Alarm Browser

-
- Step 1** In the Alarm Browser window, choose **File > Filter** (or click the **Filter Data** tool). The Filter dialog box opens.
- Step 2** Specify the filter parameters described in the following table.
- Step 3** After making your selections, click **OK** to run the filter.
-

Table 9-3 **Field Descriptions for the Alarm Browser Filter Dialog Box**

Tab	Description
Alarm Time (<i>time zone</i>)	<p>Allows you to filter alarm data for a specified time period, ranging from the past hour to the past 6 months. Additionally, you can click the User Specified radio button to specify exact filter start and end times by date and hour. The time zone can be Greenwich Mean Time (GMT), a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. Use the calendar tool to choose the year, month, and day:</p> <ul style="list-style-type: none"> • Year—Click the year combo box or the double arrow (<<, >>) at the bottom of the calendar. • Month—Click the month combo box or the single arrow (<, >) at the bottom of the calendar. • Day—Click the day number on the calendar. The current date is shown in blue. <p>If you want to filter alarms and the time period is not important, click No Time Specified. Click From Now Onward to set the filter time to start immediately and continue until you change filter parameters.</p>
Source ID	<p>Allows you to move NEs back and forth between the list of available source IDs and selected source IDs and then run the alarm filter. If you have the appropriate user permissions, you can filter Prime Optical EMS alarms by selecting Prime Optical and adding it to the Selected Source ID list.</p> <p>If more than 100 NEs are selected, the Source ID tab dims and all devices are included in the filter criteria you specify.</p> <p>Note Use the scroll bars at the bottom and right side of the lists to display all options in the lists.</p>
Module Name	<p>Allows you to specify which module types you want to include in the alarm filter. The modules displayed depend on the NE selection in the Domain Explorer tree when the Alarm Browser is opened. Use the Add and Remove buttons to filter the display to specific modules. The Alarm Browser displays alarms for modules listed under Selected Module Name.</p> <p>Note Use the scroll bars at the bottom and right side of the lists to display all options in the lists.</p>
Affected Object	<p>Allows you to specify which objects you want to include in the alarm filter. All objects are displayed regardless of the NE selected in the Domain Explorer tree when the Alarm Browser is opened. Use the Add and Remove buttons to filter the display to specific objects. The Alarm Browser displays alarms for objects listed under Selected Affected Object. To filter NE-specific EMS alarms, include Prime Optical in the Selected Affected Object list.</p> <p>Below the Available Affected Object list is a text field where you can enter characters to search quickly for available objects. The text field accepts an asterisk (*) as a wildcard character. Alarms that do not match the search criteria are not displayed. The text field below the Available Affected Object list allows you to select multiple objects and add them to the Selected Affected Object list. To do so, proceed as follows:</p> <ol style="list-style-type: none"> 1. Filter the Available Affected Object list with a wildcard or a regular expression. 2. Choose Ctrl and select the required items from the Available Affected Object list. 3. Repeat steps 1 and 2, if required, to make additional selections. The selections you make are not visible; they are held in memory until you click the Add button. <p>Note You must choose Ctrl before selecting objects from the Available Affected Object list. Objects selected are cleared from memory unless you press Ctrl before making your selection.</p> <ol style="list-style-type: none"> 4. Click Add. The items you selected are now listed in the Selected Affected Object list. <p>Note Use the scroll bars at the bottom and right side of the lists to display all options in the lists.</p>

Table 9-3 Field Descriptions for the Alarm Browser Filter Dialog Box (continued)

Tab	Description
PS	Allows you to filter alarm data based on perceived severity (Critical, Major, Minor, and Warning) and alarm status (Active and Cleared). You can filter on acknowledged alarms, unacknowledged alarms, or both. You can also filter service-affecting alarms, nonservice-affecting alarms, and/or alarms where the service-affecting status is not known.
Physical Location	Allows you to filter alarm data based on the physical location of an NE or its components. To view the tab, an NE must be selected in the Domain Explorer tree. The filters that are available depend on the NE that is selected when the Alarm Browser is opened. For example, if you select a CTC-based NE, you can filter data by shelf, slot, and port.
ID	Allows you to filter alarm data based on a specific starting and ending alarm ID. Check the Disregard All Other Filter Criteria check box to base the filter on only the starting and ending alarm ID.
NE Alarm Time (time zone)	Allows you to filter alarm data for a specified time period, ranging from the past hour to the past 6 months. Additionally, you can click the User Specified radio button to specify exact filter start and end times by date and hour. The time zone can be GMT, a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. If you want to filter alarms and the time period is not important, click No Time Specified . Click From Now Onward to set the filter time to start immediately and continue until you change filter parameters.

9.2.3 Adding Alarm Notes

Use the Alarm Note dialog box to read any comments that have been entered for the selected alarm and to enter additional comments. In the Alarm Browser window, select an alarm and choose **Fault > Show Alarm Note** (or click the **Show Alarm Note** tool). The following table provides descriptions.

Table 9-4 Field Descriptions for the Alarm Note Dialog Box

Field	Description
Note	Provides space to type comments about the selected alarm. You can enter up to 1,900 characters in the Note field. To add your comments to the previous comments, click the Append radio button. To overwrite the previous comments, click Replace . To delete the comments, click Delete . Note You can enable and disable the ability to overwrite or delete alarm notes in the Control Panel > UI Properties pane.
History	Comments that were entered by previous users. This field also shows the login name of the user who entered the note and the time when the note was entered.

9.2.4 Viewing the Alarm Log

The Alarm Log contains alarms that have transitioned from the Alarm Browser. Cleared alarms are transitioned when you acknowledge them or when automatic acknowledgment has been enabled (in the Control Panel > UI Properties pane). In addition, the Alarm Log shows a history of cleared and

acknowledged alarms and all transient conditions (also known as events or autonomous nonalarmed messages). Events are placed directly into the Alarm Log; they do not appear in the Alarm Browser. By default, the Alarm Log shows alarm and event information that occurred during the last 4 hours.

To save a filter, check the **Save Filter** check box, and click **OK** in the Filter dialog box. Upon selecting a saved filter, the Filter tool changes to red.



Note The Alarm Log supports only one saved filter per user.

To delete a filter, choose **File > Delete Saved Filter**. When you delete a saved filter, the Filter tool reverts to blue, indicating that the filter is not saved.

To view the Alarm Log, select a node in the Domain Explorer tree and choose **Fault > Alarm Log** (or click the **Open Alarm Log** tool). The following table provides descriptions.

Table 9-5 *Field Descriptions for the Alarm Log Window*

Field	Description
ID	Unique number that the system uses to identify a particular alarm or event.
Alias ID	Alias name of the NE.
Affected Object	Name of the object where the selected alarm or event occurred. For NE-specific alarms, the affected object field displays “CTM.” For the non-NE specific alarms: <ul style="list-style-type: none"> Maximum number of login attempts exceeded alarm—The affected object field displays the user ID associated with the alarm. Prime Optical self-monitor alarm—The affected object field displays the threshold parameter associated with the alarm.
Module Name	Name of the module where the selected alarm or event occurred.
Physical Location	Physical location of the equipment where the selected alarm or event occurred, such as rack, subrack (shelf), slot, and port numbers.
Probable Cause	Probable cause of the selected alarm or event.
Condition	Error message or condition name that is associated with the alarm or event.
Perceived Severity	Severity of the alarm before it was cleared. Perceived Severity is listed as: <ul style="list-style-type: none"> Critical (CR) Major (MJ) Minor (MN) Warning (WR) Indeterminate (IN) The background color of the column indicates the alarm status, where: <ul style="list-style-type: none"> Green = Cleared alarms Purple = Indeterminate events <p>Note Indeterminate events are transient events that do not have a severity indicated by the source NE. Indeterminate events do not have a cleared condition.</p>

Table 9-5 *Field Descriptions for the Alarm Log Window (continued)*

Field	Description
Service Affecting	Whether the alarm or event is service affecting. Values are: <ul style="list-style-type: none"> • Yes if the alarm is service affecting • No if the alarm is not service affecting • N/A if no information is provided by the NE
Time Stamp (time zone)	Date and time when the alarm or event occurred on the Prime Optical server.
Clear Time (time zone)	Date and time when the alarm was cleared on the Prime Optical server.
Duration	Amount of time required to clear an alarm (Prime Optical clear time – Prime Optical time) in <i>ddd:hh:mm:ss</i> format.
NE Time Stamp (time zone)	Date and time when the alarm or event occurred on the NE.
NE Clear Time (time zone)	Date and time when the alarm or event was cleared on the NE.
Description	Brief description of the selected alarm or event. If no description is entered, this field is blank.
Acknowledged Username	Login name of the user who acknowledged the alarm or event. Note If the alarm acknowledgement is set to Automatic and you can manually acknowledge an alarm, the Acknowledged Username is not overwritten when the alarm clears.
Acknowledged Time	Date and time when the alarm or event was acknowledged. Note If the alarm acknowledgement is set to Automatic and you can manually acknowledge an alarm, the Acknowledged Time is not overwritten when the alarm clears.
Note	Any notes that were entered for the selected alarm or event. This field also shows the login name of the user who entered the note and the time stamp when the note was entered.
Source ID	Name of the NE or EMS where the selected alarm or event occurred.
TL1 Direction	TL1 direction for RTRV-ALM-ALL and RTRV-COND-ALL TL1 commands and REPT^ALM/COND autonomous messages. Values are Receive or Transmit. This field is blank for non-TL1 alarms.
TL1 Location	TL1 location for RTRV-ALM-ALL and RTRV-COND-ALL TL1 commands and REPT^ALM/COND autonomous messages. Values are Near End or Far End. This field is blank for non-TL1 alarms.

9.2.5 Filtering Data in the Alarm Log

By default, the Alarm Log shows alarm and event information that occurred during the last 4 hours. Use the drop-down menu to the right of the time-based Filter Data tool to filter event data for various time periods.

- Step 1** In the Alarm Log window, choose **File > Filter** (or click the **Filter Data** tool). The Filter dialog box opens.

- Step 2** Specify the filter parameters described in the following table.
- Step 3** After making your selections, click **OK** to run the filter.
- Step 4** To save a filter:
- Open the Alarm Log Filter dialog box.
 - Click the **PS** tab.
 - Check the **Save Filter** check box.
 - Click **OK**. In the Alarm Log window, the Filter tool changes to red, indicating that a saved filter is present.



Note The Alarm Log supports only one saved filter per user.

- Step 5** To delete a saved filter, choose **File > Delete Saved Filter** in the Alarm Log window. At the following prompt, click **Yes**:

The saved filter will be deleted. The current filter will remain applied to the table. Are you sure you want proceed?

When you delete a saved filter, the Filter tool reverts to blue in the Alarm Log window.

Table 9-6 Field Descriptions for the Alarm Log Filter Dialog Box

Tab	Description
Time Stamp (time zone)	<p>Allows you to filter alarm and event data for a specified time period, ranging from the past hour to the past 6 months. Additionally, you can click the User Specified radio button to specify exact filter start and end times by date and hour. The time zone can be GMT, a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. Use the calendar tool to choose the year, month, and day:</p> <ul style="list-style-type: none"> Year—Click the year combo box or the double arrow (<<, >>) at the bottom of the calendar. Month—Click the month combo box or the single arrow (<, >) at the bottom of the calendar. Day—Click the day number on the calendar. The current date is shown in blue. <p>If you want to filter alarms and events and the time period is not important, click No Time Specified. Click From Now Onward to set the filter time to start immediately and continue until you change filter parameters.</p>
Source ID	<p>Allows you to move NEs back and forth between the list of available source IDs and selected source IDs and then run the filter. If you have the appropriate user permission, you can filter Prime Optical EMS alarms and events by selecting Prime Optical and adding it to the Selected Source ID list.</p> <p>If more than 100 NEs are selected, the Source ID tab dims and all devices are included in the filter criteria you specify.</p> <p>Note Use the scroll bars at the bottom and right side of the lists to display all options in the lists.</p>
Module Name	<p>Allows you to specify which modules you want to include in the filter. The modules displayed depend on the NE selection in the Domain Explorer tree when the Alarm Log is opened. Use the Add and Remove buttons to filter the display to specific modules. The Alarm Log displays events for modules listed under Selected Module Name.</p> <p>Note Use the scroll bars at the bottom and right side of the lists to display all options in the lists.</p>

Table 9-6 *Field Descriptions for the Alarm Log Filter Dialog Box (continued)*

Tab	Description
Affected Object	<p>Allows you to specify which objects you want to include in the filter. The objects displayed depend on the NE selection in the Domain Explorer tree when the Alarm Log is opened. Use the Add and Remove buttons to filter the display to specific objects. The Alarm Log displays events for entities listed under Selected Affected Object.</p> <p>To filter NE-specific EMS alarms, select Prime Optical and add it to the Selected Affected Object list.</p> <p>Below the Available Affected Object list is a text field where you can enter characters to search quickly for available objects. The text field accepts an asterisk (*) as a wildcard character. Alarms that do not match the search criteria are not displayed.</p> <p>Note Use the scroll bars at the bottom and right side of the lists to display all options in the lists.</p>
PS	<p>Allows you to filter data based on the perceived severity (PS) of the alarm or event. Additionally, you can filter service-affecting alarms and events, nonservice-affecting alarms and events, and/or alarms and events where the service-affecting status is not known.</p> <p>Follow these steps to save a filter:</p> <ol style="list-style-type: none"> 1. Check the Save Filter check box, and click OK in the Filter dialog box. 2. The saved filter is added to the table. 3. When you choose File > Apply Saved Filter, the table populates with the attributes saved for that filter. <p>Note An “at” symbol (@) in the Filter indicates that you are viewing a saved filter.</p> <p>Follow these steps to delete a filter:</p> <ol style="list-style-type: none"> 1. Choose File > Delete Saved Filter (or click the Delete Saved Filter tool). <p>The following message appears in the Delete Filter dialog box:</p> <p>The saved filter will be deleted. The current filter will remain applied to the table. Are you sure you want proceed?</p> <ol style="list-style-type: none"> 2. Click Yes. 3. When you run two parallel Prime Optical client sessions, deleting a saved filter from one session does not reflect any changes on the other. The Apply and Delete buttons remain enabled in the second session. <p>The following message appears when you click either of the buttons in the Filter dialog box of the second session:</p> <p>The saved filter no longer exists in the system. The current user might have deleted it in a different Prime Optical client session.</p> <ol style="list-style-type: none"> 4. Click OK. <p>The Apply and Delete buttons are disabled. The Filter tool reverts to blue, indicating that the filter is not saved.</p> <p>Note The menu items Apply Saved Filter and Delete Saved Filter and the Delete Saved Filter tool are enabled only if there is a saved filter for that table.</p>
Physical Location	<p>Allows you to filter data based on the physical location of an NE or its components. To view the tab, an NE must be selected in the Domain Explorer tree. The filters that are available depend on the NE selected. For example, if you select a CTC-based NE, you can filter data by shelf, slot, and port.</p>


Table 9-6 Field Descriptions for the Alarm Log Filter Dialog Box (continued)

Tab	Description
ID	Allows you to filter data based on alarm or event ID. Enter a starting ID and an ending ID; then, run the filter to see only the alarms or events that occurred within the specified range of IDs. Check the Disregard All The Other Filter Criteria check box to ignore all other filter specifications. In addition, you can filter the view to only alarms, only events, or both alarms and events.
NE Alarm Time (time zone)	Allows you to filter alarm data for a specified time period, ranging from the past hour to the past 6 months. Additionally, you can click the User Specified radio button to specify exact filter start and end times by date and hour. The time zone can be GMT, a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. If you want to filter alarms and the time period is not important, click No Time Specified . Click From Now Onward to set the filter time to start immediately and continue until you change filter parameters.

9.2.6 Exporting All Data in the Alarm Log or Alarm Browser

You can export the entire contents of the Alarm Browser or Alarm Log to a text file. You can export all of the data in the Alarm Browser or Alarm Log, as long as the window is not in automatic refresh mode. It might take longer to open the Alarm Browser or Alarm Log with the export entire table feature enabled.

The entire-table export writes the data to a user-specified text file and retains the user-selected table customizations. For example, if you customized the table to make a column invisible, that column does not appear in the exported file.

-
- Step 1** Complete the following substeps to enable the export entire table feature:
- In the Domain Explorer window, choose **Edit > User Preferences**.
 - In the User Preferences dialog box, click the **FM Preferences** tab.
 - Check the **Enable Export of the Entire Table** check box.
 - Check the **Save current settings** check box.
 - Click **OK**.
- Step 2** In the Domain Explorer window, choose **Fault > Alarm Browser** or **Alarm Log**.
- Step 3** In the Alarm Browser or Alarm Log window, choose **File > Export**.
- Step 4** In the Export dialog box, click the **Entire table (only if Auto Refresh is disabled)** radio button.
-  **Note** This option is disabled if the window is in Auto Refresh mode.
- Step 5** In the Export Data to File field, specify a location for the exported file. Click **Browse** to change the file location.
- Step 6** Click **OK**. A progress bar tracks the export progress.
-

9.3 What Fault Information Can I See?

An alarm is represented by a notification from a managed NE that a certain condition has just occurred. These alarms usually represent error conditions on NEs. Each alarm is associated with the NE for which it provides notification, and an NE can have a number of alarms related to itself at any time.

Each NE shown in the Domain Explorer tree has a corresponding alarm icon that indicates the highest severity alarm that affects the NE. Management domain nodes and group nodes have alarm icons that reflect the highest alarm condition of the NEs contained in the domain or group.

The user-defined Domain Explorer views have “bubble-up” alarm severity propagation and drill-down capabilities to isolate fault conditions and identify service-delivery impact.

9.3.1 How Are Alarms Displayed?

You can set the Alarm Browser or Alarm Log to display full background color for the entire selected row. The color corresponds to the alarm status and severity. In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box opens. On the FM Preferences tab, check the **Color Entire Row in Table View** check box.

In the Dashboard, Map Viewer, Alarm Browser, and Domain Explorer, the color of the border surrounding a component, or the background color, indicates the operational status of the component. When status changes, the border or the background color changes as indicated in the following table.

Table 9-7 Alarm Severity Colors for the Dashboard, Map Viewer, Alarm Browser, and Domain Explorer

Color	Severity	Meaning	Description
Green	Cleared	Component is active.	The component is operating normally.
Yellow	Minor	Minor failure.	The component is down; both administrative and operational values are down. This does not necessarily indicate a fault condition; the component might be disabled.
Orange	Major	Component is down.	Administrative status is up and operational value is down.
Red	Critical	Component failed.	Physical hardware failure.
Cyan (blue-green)	Warning	Interface is dormant.	The interface cannot pass packets, but is in a pending state waiting for some external event to place it in the up state. The interface might have packets to transmit before establishing a connection to a remote system, or a remote system might be establishing a connection to the interface. When the pending event occurs, the interface changes to the up state.

9.3.1.1 Understanding How Prime Optical Displays the Affected Object Field

Prime Optical displays the Affected Object field in the Alarm Browser and Alarm Log windows in the same way as for the Interface field in PM tables. See [10.4.7 Understanding How Prime Optical Displays the Interface Field, page 10-31](#).

For the ONS 155xx, the Affected Object field can be:

- wavepatch—The alarm is related to the optical client side of the card.
- wave—The alarm is related to the optical connection with the OADM (filter) card.

- The actual interface object, which changes depending on the card. For example, WaveEthernetPhy for a 10 Gb card, EsconPhy for an ESCON card, and so on.

9.3.2 Suppressing Alarms

Alarm suppression is useful when the NE is under maintenance. You can also suppress alarms for a single shelf in an ONS 15454 multishelf NE.



Caution

If multiple CTC or TL1 sessions are open, alarms in all other open sessions are also suppressed.

9.3.2.1 Suppressing Alarms at the Card Level—CTC-Based NEs

-
- | | |
|---------------|---|
| Step 1 | In the Domain Explorer window, select a CTC-based NE and choose Configuration > NE Explorer . |
| Step 2 | In the NE Explorer tree, click the specific card. |
| Step 3 | In the card slot property sheet of the NE Explorer window, click the Identification tab. |
| Step 4 | Check the Suppress Alarms check box. |
| Step 5 | Click Apply . |
-

9.3.2.2 Suppressing Alarms at the Node Level—CTC-Based NEs

-
- | | |
|---------------|---|
| Step 1 | In the Domain Explorer window, select a CTC-based NE and choose Configuration > NE Explorer . |
| Step 2 | In the node property sheet of the NE Explorer window, click the Alarm tab. |
| Step 3 | Click the Alarm Behavior subtab. |
| Step 4 | Check the Suppress Alarms check box. |
| Step 5 | Click Apply . |
-

9.4 Is the Service Working?

Network devices report symptoms of problems by generating events. An event in this context is a message indicating that a device or application in your network has discovered something of note. The network devices generate many types of events automatically. In addition, you can use thresholds to define or modify the conditions under which events are generated. A *threshold* is a trigger, set up on a continuous data stream, that is a point of interest that generates events when that point is satisfied.

The events generated need to be analyzed to determine whether they represent a fault condition or a problem in your network.

It is important to generate events when there is a problem. It is also important to limit the number of events generated to prevent an excessive load on the network. Prime Optical performs a number of self-monitoring tasks where threshold limits can be set. The threshold limits are set in the Self Monitor table. (See [10.3.12 Using the Self Monitor Table, page 10-15](#).) If a threshold is crossed, an EMS alarm is generated.

You can obtain information regarding how the system is performing and how long certain tasks are taking to complete by selecting **Administration > Control Panel**, then **Alarm Configuration > Threshold EMS Alarms** or **Alarm Configuration > Nonthreshold EMS Alarms**. (See [9.4.4 Setting Up and Viewing Alarm Configuration Parameters, page 9-18](#).) By monitoring this data, you can identify potential system problems before they become critical in the operation of the EMS. Associated with each parameter that is monitored are three alarm thresholds. The administrator can set a minor, major, and critical threshold value for each parameter. If any of these thresholds are crossed, then an alarm will be raised to provide notification of the situation.

Threshold alarms are raised when their limit exceeds the value set for critical, major, minor, or warning thresholds. For example, you can set threshold alarms for disk usage for 90%, 80%, 70%, and 60%, meaning a warning alarm is raised when the disk becomes 61% full and a critical alarm is raised when the disk becomes 91% full. The server checks these parameters at every polling interval that is set in the Poll Frequency field.

Nonthreshold alarms do not have an alarm threshold. Instead, nonthreshold alarms occur when a condition occurs, such as loss of connectivity to an NE. Use the Nonthreshold EMS Alarms tab to set the severity level (critical, major, minor, or warning) for which a nonthreshold alarm should be raised when that condition occurs.

**Caution**

Changing the EMS alarm severities can affect the alarm status seen by listeners on the EMS's OSS interfaces.

The following sections provide information on NEs:

- [9.4.1 Locating Alarms, page 9-16](#)
- [9.4.4 Setting Up and Viewing Alarm Configuration Parameters, page 9-18](#)

These tasks allow you to manage the alarm profiles features:

- [9.4.5 Creating Alarm Profiles—CTC-Based NEs, page 9-22](#)
- [9.4.6 Applying Alarm Profiles—CTC-Based NEs, page 9-23](#)
- [9.4.7 Managing Alarm Profiles—CTC-Based NEs, page 9-24](#)

This task allows you to mark a service as critical for process monitoring purposes:

- [9.4.9 Using the Recovery Properties Pane, page 9-27](#)

9.4.1 Locating Alarms

The Alarm Browser has a specific selection context, which means that it displays alarm information that corresponds to the view where it was launched. If you launch the Alarm Browser from the management domain node, the browser shows all NE alarms and all EMS alarms (if you have permission to see EMS alarms). If you launch the Alarm Browser from a group or NE node, the browser shows only NE alarms for that group or NE node. If you launch the Alarm Browser from the Dashboard, the browser shows all NE alarms for the domain.

You can locate the equipment for an existing alarm from the Alarm Browser.

-
- Step 1** In the Domain Explorer, choose **Fault > Alarm Browser** (or click the **Open Alarm Browser** tool).
- Step 2** In the Alarm Browser, click an alarm condition and choose **Fault > Locate Alarm/Event** (or click the **Locate Alarm/Event Through NE Explorer** tool). The NE Explorer opens and displays the property sheet of the alarmed equipment.
-



Note

Refer to the appropriate NE documentation for a list of alarms supported on each NE. See [1.7.2 Related Cisco NE Documentation, page 1-50](#).

9.4.2 Locating Affected Layer 2 Services

You can locate which Layer 2 services are affected by an existing Layer 2 service alarm.

-
- Step 1** In the Domain Explorer, choose **Fault > Alarm Browser** (or click the **Open Alarm Browser** tool).
- Step 2** In the Alarm Browser, click a Layer 2 service alarm and choose **Fault > Affected L2 Services**. The Affected L2 Services dialog box opens, listing the Layer 2 services that are affected by the selected alarm.
- To retrieve the affected Layer 2 services on the PT System, go to [Step 3](#).
 - To retrieve the affected Layer 2 services on a specific port, go to [Step 4](#).
 - To retrieve the affected Layer 2 services on a channel group, go to [Step 5](#).
- Step 3** To retrieve the affected Layer 2 services on the PT System:
- a. Click the **Packet Transport System** radio button.
 - b. Select the service type (Carrier Ethernet, Pseudowire, or MPLS TP tunnel) from the Service Type drop-down list.
 - c. Select the alarm type from the Alarm Type drop-down list. See [Table 13-28 on page 13-91](#) for the list of alarm types.
 - d. Click **Show**. The affected Layer 2 services on the PT System are displayed in the table.
 - e. (Optional) Click **Reset** to reset the Service Type and Alarm Type drop-down lists.
- Step 4** To retrieve the affected Layer 2 services on a specific port:
- a. Click the **Port** radio button.
 - b. Select the slot from the Slot drop-down list.
 - c. Select the port from the Port drop-down list.
 - d. Select the service type (Carrier Ethernet, Pseudowire, or MPLS TP tunnel) from the Service Type drop-down list.
 - e. Select the alarm type from the Alarm Type drop-down list. See [Table 13-28 on page 13-91](#) for the list of alarm types.
 - f. Click **Show**. The affected Layer 2 services on the port you selected are displayed in the table.

- g.** (Optional) Click **Reset** to reset the Service Type and Alarm Type drop-down lists.
- Step 5** To retrieve the affected Layer 2 services on a channel group:
- Click the **Channel Group** radio button.
 - Select the service type (Carrier Ethernet, Pseudowire, or MPLS TP tunnel) from the Service Type drop-down list.
 - Select the alarm type from the Alarm Type drop-down list. See [Table 13-28 on page 13-91](#) for the list of alarm types.
 - Click **Show**. The affected Layer 2 services on the channel group you selected are displayed in the table.
 - (Optional) Click **Reset** to reset the Service Type and Alarm Type drop-down lists.
- Step 6** (Optional) To cross-launch the service table from the Affected L2 Services dialog box, click **Service Table** to launch the corresponding service table. For example, if you selected Pseudowire as the service type, the Pseudowire Service table opens.
- Step 7** (Optional) To filter the affected Layer 2 services displayed in the table, click the **Filter** button. You can filter by:
- Service ID
 - Name
 - Description
- Step 8** (Optional) To clear the results and run a new query, click **Clear Table**.
-

9.4.3 Viewing Affected Circuits

You can view the circuits affected by a given alarm.

- Step 1** In the Domain Explorer, choose **Fault > Alarm Browser** (or click the **Open Alarm Browser** tool).
- Step 2** Select the alarm for which to view affected circuits, and choose **Fault > Affected Circuits**.
- The Circuit Table appears, displaying all the circuits affected by the selected alarm.
-

9.4.4 Setting Up and Viewing Alarm Configuration Parameters

Use the Alarm Configuration pane to configure and view alarm severities for system parameters.



Caution

Changing the EMS alarm severities can affect the alarm status seen by users on the EMS's OSS interfaces.

Complete the following steps to set up and view alarm configuration parameters:

- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** Click **Alarm Configuration** to open the Alarm Configuration pane. [Table 9-8](#) provides descriptions.
- Step 3** In the Nonthreshold EMS Alarms tab, you can select the severity level that will be assigned to the nonthreshold alarm parameter.



Note Nonthreshold alarms do not have an alarm threshold. These types of alarms occur when an error condition occurs, such as loss of connectivity to an NE. Use the Nonthreshold EMS Alarms tab to set the severity level for which a nonthreshold alarm should be raised when that condition occurs.

- Step 4** After making your selections, click **Save**.



- Note**
- If an alarm is outstanding when you disable it, the system clears the alarm.
 - If an alarm has been manually cleared in the Alarm Browser and a clear alarm is sent, the request will still be processed but it will not have any impact on the alarm.
 - To recover from an alarm condition, see [Appendix G, “Troubleshooting”](#) for information.
 - All alarms on an NE are cleared when the NE is marked as Out of Service.

Table 9-8 *Field Descriptions for the Alarm Configuration Pane*

Field	Description
Threshold EMS Alarms Tab	
Poll Frequency	<p>Threshold alarms are raised when their limit exceeds the value set for critical, major, minor, or warning thresholds. For example, you can set threshold alarms for disk usage for 90%, 80%, 70%, and 60%, meaning a warning alarm is raised when the disk becomes 61% full and a critical alarm is raised when the disk becomes 91% full. The server checks these parameters at every polling interval that is set in the Poll Frequency field. The Poll Frequency value affects only the following parameters:</p> <ul style="list-style-type: none"> • CPU Usage • Memory Usage RAM • Memory Usage SWAP • Disk Usage

Table 9-8 *Field Descriptions for the Alarm Configuration Pane (continued)*

Field	Description
Parameter Name	<ul style="list-style-type: none"> Base Circuit Creation Time (seconds)—Time it takes to create a base circuit. CPU Usage (%)—Percentage of CPU time used for executing user, system, and I/O tasks. Circuit Creation Time Per Hop (seconds)—Time it takes for Prime Optical to create an end-to-end circuit. Config Resynch Time (seconds)—Time it takes for Prime Optical to collect alarm and inventory information from the NE. Disk Usage (%)—Percentage of disk space used in a particular partition. Prime Optical database and partitions are monitored separately. Memory Usage RAM (%)—Percentage of RAM memory used for all system processes. Memory Usage SWAP (%)—Percentage of SWAP memory used for all system processes. NE Synch Time (seconds)—Time it takes to synchronize the Prime Optical server with the NEs. Prune Time 15 min PM (seconds)—Time it takes to prune 15-minute PM data. Prune Time 1 day PM (seconds)—Time it takes to prune 1-day PM data. Prune Time Audit Log (seconds)—Time it takes to prune Audit Log data. Prune Time Audit Trail Log (seconds)—Time it takes to prune Audit Trail Log data. Prune Time Error Log (seconds)—Time it takes to prune Error Log data. Prune Time FM (seconds)—Time it takes to prune FM data. Prune Time Job Monitor (seconds)—Time it takes to prune job monitor data. Prune Time Purge NE (seconds)—Time it takes to prune NE purge data. Prune Time Server Monitor (seconds)—Time it takes to prune server monitor data.
Enable	Whether or not the corresponding parameter in the Parameter Name column is enabled (checked) or disabled (unchecked). When checked, it enables monitoring for the selected parameter. If an EMS threshold alarm is outstanding when you disable monitoring, Prime Optical clears the alarm.
Critical	Amount of time, in minutes, that must elapse before triggering a critical alarm.
Major	Amount of time, in minutes, that must elapse before triggering a major alarm.
Minor	Amount of time, in minutes, that must elapse before triggering a minor alarm.

Table 9-8 *Field Descriptions for the Alarm Configuration Pane (continued)*

Field	Description
Nonthreshold EMS Alarms Tab	
Parameter Name	<ul style="list-style-type: none"> • A critical process is hanging; server will be shut down in 5 minutes. • A process is hanging or terminated. • Alarm resync unsuccessful—The alarm resynchronization could not be completed on the node. • Communication through secondary IP address. • Config resync unsuccessful—Prime Optical could not synchronize with the node. • Failed authentication by NE—This is a major alarm. An incorrect username or password was provided for login. This alarm applies to CTC-based NEs and is cleared when you provide the correct username or password and mark the NE as Out of Service, then as In Service. • Loss of communication—This is a critical alarm. Prime Optical cannot communicate with the node, possibly because the node was disconnected from the network. This alarm applies to all NEs and is cleared when Prime Optical regains connectivity to the NE. • Maximum login attempts exceeded—Prime Optical raises this alarm when you try to connect to the Prime Optical server several times with the wrong username and password. • Memory auto or manual backup failure—This is a minor alarm. Memory backup on the node failed. This alarm applies to CTC-based NEs and is cleared when a subsequent memory backup succeeds. • NE out of Sync—Prime Optical raises this EMS alarm when the health poll of an NE fails because the server is no longer registered on the node to receive event notifications. This alarm is cleared once the initial poll is executed successfully. • PM fail EMS alarm—This is a warning alarm. Prime Optical cannot retrieve performance statistics from the node even though robust PM data collection is enabled and the node has PM buckets that were not retrieved. This alarm applies to CTC-based NEs and is cleared when a subsequent PM collection cycle succeeds. If PM collection is unsuccessful after subsequent retries, the FAIL alarm is cleared and the PM lost EMS alarm is generated. • PM lost EMS alarm—This is a major alarm. Prime Optical cannot retrieve performance statistics from the node when robust PM data collection is not enabled or when robust PM data collection is enabled but the node has overwritten the PM buckets that were not retrieved. This alarm applies to CTC-based NEs and is cleared when the user clears it manually from the Alarm Browser. • PoS port shut down; L2 topology in wrapped state—This alarm is generated when one or more PoS ports related to an L2 topology are shut down. This alarm is cleared when all the PoS ports related to the topology are enabled. • Template manager event. • Unable to change database password—This alarm is generated after a failed attempt to change the database password in the Control Panel > Database Properties pane.
Enable	Whether or not the corresponding parameter in the Parameter Name column is enabled (checked) or disabled (unchecked). When checked, it enables monitoring for the selected parameter. If an EMS nonthreshold alarm is outstanding when you disable monitoring, Prime Optical clears the alarm.
Severity	<p>Click the appropriate cell and select the alarm severity level from the available options (Critical, Major, Minor, or Warning) for each of the parameters listed in the Parameter Name column.</p> <p>Note If an EMS alarm is outstanding when you change its severity level, the outstanding alarm's severity level remains the same and the new severity level takes effect the next time the alarm is raised.</p>

9.4.5 Creating Alarm Profiles—CTC-Based NEs

Use the Create Alarm Profile dialog box to create new alarm profiles for CTC-based NEs.

-
- Step 1** In the Domain Explorer tree, select a CTC-based NE and choose **Configuration > NE Explorer**.
- Step 2** In the node properties sheet, click the **Alarm** tab.
- Step 3** In the Profile subtab, click the **Create** button. The Create Alarm Profile dialog box opens. The following table provides descriptions.
- Step 4** After making your selections, click **OK**.
-

Table 9-9 Field Descriptions for the Create Alarm Profile Dialog Box

Field	Description
Enter the Profile Name	Enter the name of the new alarm profile.
Condition	Condition of the alarm.
Severity	<p>Select a severity for the new alarm from the list. Alarm severities include:</p> <ul style="list-style-type: none"> Not Reported (NR)—A raise or clear of the condition is not sent to clients, but is tracked on the NE. You can retrieve a complete list of all raised conditions, including Not Reported as well as Not Alarmed, Critical, Major, and Minor, by using the RTRV COND TL1 command, or its equivalent. Not Alarmed (NA)—A raise or clear of the condition is sent to clients as a nonalarmed TL1 message (REPT EVT). The message has no severity and no service affecting flag. Minor (MN)—The alarm is a minor alarm. Major (MJ)—The alarm is a major alarm. Critical (CR)—The alarm is a critical, traffic-affecting alarm. <p>Note For critical, major, and minor alarms, a raise or clear of the condition is sent to clients as an alarmed message (REPT ALM). This message includes a service affecting flag, which is On or Off. If a normally service affecting condition is raised in a nonservice affecting situation (for example, the nontraffic-bearing side of a protect pair), the condition is sent as minor even if the profile says major or critical.</p> <ul style="list-style-type: none"> UNSET—The value of this alarm corresponds to the value of the default alarm profile on the node. UNSET is useful when transferring alarm profiles between different versions of software. Inherited—The alarm behaves according to its parent object: <ul style="list-style-type: none"> If you set an alarm as Inherited on a port, it uses the card profile. If you set an alarm as Inherited on a card, it uses the node profile. If you sent an alarm as Inherited on a node, it uses the default profile.

9.4.6 Applying Alarm Profiles—CTC-Based NEs

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual CTC-based NEs. A profile can be applied to any node on the network. Alarm profiles must be stored on a node before they can be applied to a node, card, or port.

The two reserved profiles include the Default profile, which sets severities to standard Telcordia GR-253 settings, and the Inherited profile, which sets all alarm severities to inherited. If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm at the next level. For example, a card with an Inherited alarm profile copies the severities used by the node that contains the card. The Inherited profile is not available at the node level.

In the card view, the Alarm Behavior subtab displays the alarm profiles of the selected card. In the node view, the Alarm Behavior subtab displays the alarm profiles for the node. Alarms form a hierarchy. A node-level alarm profile applies to all cards in the node, except those that have their own profiles. A card-level alarm profile applies to all ports on the card, except those that have their own profiles.

At the node level, apply profile changes on a card-by-card basis or set a profile for the entire node. At the card level, apply profile changes on a port-by-port basis or set the profiles for all ports on that card simultaneously.

-
- Step 1** In the Domain Explorer window, click a CTC-based NE and choose **Configuration > NE Explorer**.
 - Step 2** In the node properties sheet, click the **Alarm** tab > **Alarm Behavior** subtab. In the card properties sheet, click the **Alarm Behavior** tab.
 - Step 3** Click **Update** to view the latest Alarm Profile list.
 - Step 4** To apply an alarm profile at the card view, click the appropriate row in the Alarm Profile column for the port desired. To apply an alarm at the node view, click the appropriate row in the Profile column for the card desired.
 - Step 5** Choose the appropriate alarm profile from the drop-down list.
 - Step 6** Repeat these steps for each port that is being assigned a profile.
 - Step 7** Click **Apply**.



Note

- In the Alarm Behavior tab > Alarm Profile drop-down list, you can select any profile and click **Force to all ports** to apply this profile to all ports. But when the profile is saved, the Alarm Profile value returns to Inherited. This is expected behavior, because the drop-down list does not represent a value on the NE. After setting the alarm profile value on the ports, the Alarm Profile field returns to the first selectable value in the drop-down list.
 - The alarm profile is not applied for ONS 15600 SONET or ONS 15600 SDH NEs if the profile was edited outside of the Alarm Profiles Management wizard.
-

9.4.7 Managing Alarm Profiles—CTC-Based NEs

Use the Alarm Profiles Management wizard to download an alarm profile from either an NE or from a local file.



Note

This feature is available for CTC-based NEs with software release 3.4 or later.

- Step 1** In the Domain Explorer window, choose **Configuration > CTC-Based SONET NEs or CTC-Based SDH NEs > Alarm Profiles Management**. The Alarm Profiles Management wizard opens. The following table provides descriptions.
- Step 2** Select an available profile from the NE by clicking the **From NE** radio button or from a file by clicking the **From File** radio button.
- Step 3** Complete one of the following options:
- If you clicked the **From NE** radio button, select the NE and alarm profile from the lists.
 - If you clicked the **From File** radio button, specify the file from a local drive by clicking the **Local** radio button, or from a server by clicking the **Server** radio button.
- Step 4** Click **Next**.
- Step 5** Edit the alarm severity for each alarm condition by clicking a row in the Alarm Severity column.
- Step 6** Click **Next**.
- Step 7** Enter the profile name and save the new alarm profile to the NE by clicking the **Save to NE(s)** radio button, or to a file by clicking the **Save to File** radio button.
- Step 8** Complete one of the following options:
- If you clicked Save to NE(s), select the NE(s) on which to apply the new alarm profile. Check the **Apply to Selected NE(s)** check box if you want to set the alarm profile as the current profile.



Note

If you clicked the **From File** radio button in [Step 2](#), the Available NE(s) list includes all the NEs that Prime Optical currently manages.

- If you clicked Save to File, you can either save the file locally by clicking the **Local** radio button and specifying the directory path, or save it to a server by clicking the **Server** radio button and specifying the server name.

- Step 9** Click **Finish**.

Prime Optical schedules a job for this action. The alarm profile is downloaded to each selected NE and set, if so selected. This is tracked as a separate task in the Job Monitor table.

Table 9-10 Field Descriptions for the Alarm Profiles Management Wizard

Field	Description
Select a Profile	
From NE	Choose From NE if the alarm profile is on an NE. If you select From NE, the From File options are not accessible.

Table 9-10 **Field Descriptions for the Alarm Profiles Management Wizard (continued)**

Field	Description
Select NE	Select the NE where the alarm profile exists.
Select Profile	Select an alarm profile from the list.
From File	Choose From File if the alarm profile file is on your PC or a server. If you select From File, the From NE options are not accessible.
Local	Choose Local if the alarm profile file is on your PC. Enter the path for the file, or click Browse to search for it.
Server	Choose Server if the alarm profile file is located on a server. Use the drop-down list to select a server.
Edit the Profile	
Alarm Condition	List of alarm conditions for the selected alarm profile.
Alarm Severity	<p>Click the field to select a new alarm severity for the alarm condition. Severities are:</p> <ul style="list-style-type: none"> • Not Reported (NR)—A raise or clear of the condition is not sent to clients, but is tracked on the NE. You can retrieve a complete list of all raised conditions, including Not Reported as well as Not Alarmed, Critical, Major, and Minor, by using the RTRV COND TL1 command, or its equivalent. • Not Alarmed (NA)—A raise or clear of the condition is sent to clients as a nonalarmed TL1 message (REPT EVT). The message has no severity and no service affecting flag. • Minor (MN)—The alarm is a minor alarm. • Major (MJ)—The alarm is a major alarm. • Critical (CR)—The alarm is a critical, traffic-affecting alarm. <p>Note For critical, major, and minor alarms, a raise or clear of the condition is sent to clients as an alarmed message (REPT ALM). This message includes a service affecting flag, which is On or Off. If a normally service affecting condition is raised in a nonservice affecting situation (for example, the nontraffic-bearing side of a protect pair), the condition is sent as minor even if the profile says major or critical.</p> <ul style="list-style-type: none"> • Unset—The value of this alarm corresponds to the value of the default alarm profile on the node. Unset is useful when transferring alarm profiles between different versions of software. • Inherited—The alarm behaves according to its parent object: <ul style="list-style-type: none"> – If you set an alarm as Inherited on a port, it uses the card profile. – If you set an alarm as Inherited on a card, it uses the node profile. – If you set an alarm as Inherited on a node, it uses the default profile.
Save the Profile	
Profile Name	Name of the selected alarm profile.
Save to NE(s)	To save the alarm profile to one or more NEs, choose Save to NE(s) . If you choose Save to NE(s), the Save to File options are not accessible.
Available NE(s)	<p>Select one or more NEs in the Available NE(s) list and click Add to move them to the Selected NE(s) list. The contents of the Available NE(s) list depends on the following conditions:</p> <ul style="list-style-type: none"> • If you selected a profile from a file, the Available NE(s) list includes all the NEs that Prime Optical currently manages.
Selected NE(s)	Select one or more NEs in the Selected NE(s) list and click Remove to move them to the Available NE(s) list.

Table 9-10 Field Descriptions for the Alarm Profiles Management Wizard (continued)

Field	Description
Apply to Selected NE(s)	When checked, applies the alarm profile as the node-level alarm profile.
Overwrite the Profile	If a profile of the same name already exists, check this check box to overwrite the profile with the new profile.
Save to File	To save the defaults to a file on your PC or a server, choose Save to File . If you choose Save to File, the Save to NE(s) options are not accessible.
Local	Choose Local to save the file on your PC. Enter the path for the file, or click Browse to search for it.
Server	Choose Server to save the file on a server. Enter a server path in the field.

9.4.8 Managing Custom Alarm Types—CTC-Based NEs

You can add up to 50 custom environmental alarms on the following nodes and cards:

- AIC and AIC-I cards on ONS 15454 SONET and ONS 15454 SDH NEs
- CTX-CL600 cards on ONS 15310 CL NEs
- ONS 15600 SONET NEs
- ONS 15600 SDH NEs
- ONS 15310 MA SONET NEs
- ONS 15310 MA SDH NEs

Custom environmental alarms are reported in the Condition column in the Alarm Log and Alarm Browser windows.

-
- Step 1** In the Domain Explorer window, click one of the CTC-based NEs in the preceding list and choose **Configuration > NE Explorer**.
- Step 2** Do one of the following:
- In the node properties sheet, click the **Alarm Extenders** tab > **User-Defined Alarms** subtab.
 - In the AIC, AIC-I, or CTX-CL600 card properties sheet, click the **Alarm Extenders** tab > **User-Defined Alarms** subtab.
- Step 3** In the Alarm Types area, click **Add**. The Add Alarm Type dialog box opens.
- Step 4** In the New Alarm Type field, enter a unique alarm type name that contains 20 characters or fewer. Only the following characters are valid: 0-9, A-Z, a-z, and hyphen (-).
- Step 5** Click **OK**. The new custom alarm appears in the Alarm Types area.
- Step 6** To delete a custom alarm type, select the alarm in the Alarm Types area and click **Delete**. Click **OK** in the confirmation dialog box.
-

9.4.9 Using the Recovery Properties Pane

You can use the Recovery Properties pane in the Control Panel window to mark a service as critical for process monitoring purposes. If a critical process stops running or fails to poll monitoring services for a long time, the server shuts down and the client generates an alarm.

You can also use the Recovery Properties pane to list the servers that clients will log into if access to the primary server is disrupted.

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** Click **Recovery Properties** to open the Recovery Properties pane. The following table provides descriptions.
- Step 3** Complete the following substeps to set a process as critical:
- Click the **Process Monitoring** tab.
 - Check the **Critical** check box beside each service to indicate that the service is critical.
 - Click **Save**.
-

Field Descriptions for the Recovery Properties Pane

Field	Description
Process Monitoring Tab	
Service Name	Displays the process monitoring service name.
Critical	<p>If checked, the selected service is designated as critical for process monitoring.</p> <p>Note CORBA ImR, Oracle Service, and Service Manager are permanently critical. You cannot uncheck the Critical check boxes for these services.</p> <p>The Prime Optical server may take up to 30 minutes to shut down when a critical process stops running or does not respond to poll monitoring.</p>

9.5 Where Is the Fault?

You need to be able to quickly troubleshoot problems in the network, identify when network capacity is being reached, and provide information to management on the number and types of devices in use. If the network goes down, one of the first things you will need to know is what devices are running on the network. You will want to know the names, addresses, and interfaces associated with each device in order to begin troubleshooting the problem. The more information you have in one central place about all of the devices, the easier it is to locate the necessary information, resolve problems quickly, and provide detailed information to interested parties.

9.5.1 Sources of Information

Fault management receives and processes information from the following sources:

- Autonomous reports of failures from NEs
- Trouble reports from customers and peer systems
- Results of diagnostics, exercises, and audits from NEs
- Impairment indications from performance management
- Network configuration data from configuration management

Prime Optical constantly updates the alarm status of the network based on the alarm and event notifications sent by the monitored NEs and generated by the EMS itself. It performs alarm synchronization with the NE each time the connection to the NE is established or re-established and the NE is in service.

9.5.2 Identifying and Monitoring Alarms

To identify and monitor alarms on groups of NEs:

-
- Step 1** In the Domain Explorer tree, select the management domain node or a group node. If it shows a critical, major, minor, or warning alarm icon, it means that one or more NEs within the management domain or group are experiencing an alarm.
- Step 2** Select the management domain node or group node and choose **Fault > Alarm Browser** (or right-click the node and choose **Alarm Browser** in the popup menu). This opens the Alarm Browser window, which shows all the NEs in the management domain or group that are experiencing an alarm.
-

To identify and monitor alarms on a specific NE:

-
- Step 1** Select an in-service NE in the Domain Explorer tree that shows an alarm icon.
- Step 2** Choose **Fault > Alarm Browser** (or right-click the NE and choose **Alarm Browser** in the popup menu).
- Step 3** For ONS 15216 and CTC-based NEs, you can also choose **Configuration > NE Explorer** to view alarms on the NE or on specific modules. The Module View tab displays a graphic of the module that is installed in the slot. The number of critical, major, minor, and warning alarms for the module is displayed under Alarm Status. (Alarms also display when you move the mouse pointer over the graphic.)
-

9.5.3 Using Visual and Audible Alarm Notifications

-
- Step 1** In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box opens.
- Step 2** In the Event Notification tab, in the Show Notification Dialog For area, select whether or not an alert popup opens when a specific alarm or informational event occurs on NEs in the management domain or in the application.

The Event Notification dialog box opens whenever a new alarm or event occurs. According to your User Preferences selection, you will receive popup notification about alarms by severity and information on events from the NE or from Prime Optical. The Event Notification popup remains open until one of the following occurs:

- You click OK to close the dialog box.
- It is replaced by an Event Notification dialog box with a higher severity.
- You click Disable on the popup window itself to disable additional popups.

The following table describes the fields in the Event Notification dialog box.

- Step 3** In the Play Audible Notification For area, select whether or not an audible alert is sounded when a specific alarm or informational event occurs on the NE or in the application. You can also select whether or not a continuous audible alert is sounded when there is an update in the Dashboard. Check the **Continuous Alarm for Dashboard Notifications** check box.



Note To stop the continuous audible alert, choose **Fault > Stop Continuous Beep** in the Domain Explorer.

- Step 4** Check the **Save current settings** check box and click **OK**.

Table 9-11 *Field Descriptions for the Event Notification Dialog Box*

Field	Description
Source	Name of the source where the alarm or event originated.
Time	Date and time that you received the Event Notification popup.
Category	Category of alarm or event. Alarm categories include Critical, Major, Minor, or Cleared. Event categories include NE event (if the event occurred on an NE) or EMS event (if the event occurred on Prime Optical).
Probable Cause	Probable cause of the alarm or event.
Affected Object	Object that is affected by the alarm or event.
Description	Description of the alarm or event.
Service Affecting	Whether the alarm or event affects service.

9.5.4 Sources of Events

There are two sources of events: EMS-generated alarms and OSS (SNMP, CORBA GateWay, TL1). See [Chapter 12, “Managing Southbound and Northbound Interfaces”](#) for information about OSS events.

9.5.4.1 EMS-Generated Alarms

In addition to reporting NE-generated alarms, the EMS monitors and reports alarms and events on the EMS itself; for example, loss of connectivity to NE, and so on.

The EMS monitors and reports the NE-specific alarms and events (see [Table 9-12](#)) and non-NE-specific alarms and events (see [Table 9-13](#)).

**Note**

NE-specific alarms and events can be viewed and accessed by users who are assigned to the particular NE.

Table 9-12 *NE-Specific Alarms and Events*

NE-Specific Alarms and Events	Description
Loss of communication to an NE	When the system detects loss of connectivity to an NE, an EMS alarm is generated in the Alarm Browser. This EMS alarm is cleared when the system re-establishes connectivity to the NE or when the NE is marked as Out of Service.
Automatic or manual memory backup failure	If an automatic or manual memory backup job fails, an EMS alarm is generated in the Alarm Browser. An individual EMS alarm is generated for each memory backup failure that occurs. All instances of the backup-related EMS alarms are cleared (for that particular NE) when the memory backup succeeds or when the NE is marked as Out of Service.
Prime Optical-to-NE authentication failure	If the system attempts to log into an NE and fails, an alarm is generated. This alarm indicates that the username and password are no longer valid.
Failed PM data retrieval	For CTC-based NEs, an alarm is generated for every PM data retrieval failure. PM 15-minute retrieval fail alarms are generated if the system has not retrieved 15-minute PM data after the number of times to retrieve PM data has been reached. These alarms can be cleared manually or cleared automatically if a PM lost alarm is generated or if PM data is retrieved (PM collection should be set to 15 Min Robust).
Lost PM data	For CTC-based NEs, an alarm is generated for all PM lost data. A lost PM alarm is generated when: <ul style="list-style-type: none"> • The EMS cannot collect PM data for 15 minutes or 1 day and the NE's PM collection is set to either 15 Min or 1 Day. • The EMS cannot collect 15-minute PM data after 8 hours or 1-day PM data after 2 days and the NE's PM collection is set to 15 Min Robust or 1 Day Robust. If there are outstanding PM retrieval fail alarms, these alarms are cleared and the PM lost alarm is generated. These alarms can be cleared manually.

Table 9-13 **Non-NE-Specific Alarms and Events**

Non-NE-Specific Alarms and Events	Description
Maximum number of login attempts exceeded	By default, users have a maximum of five login attempts. The user account is locked after the fifth unsuccessful login attempt and an EMS alarm is generated in the Alarm Browser. The alarm is cleared once the user account is unlocked or the account is deleted.
System self-monitor alarm	<p>Threshold parameters such as CPU usage, memory usage, disk usage, circuit creation time, and resynchronization time are collected and evaluated to monitor the server performance. An alarm is generated if any of these parameters cross their threshold values with their corresponding severity level. The alarms are cleared only after the corresponding parameter value falls below the minor threshold. Subsequent threshold crossings for the same parameter do not generate additional alarms. Only the severity level is changed to indicate the current severity level for the specific parameter.</p> <p>Note Alarms associated with circuit creation, configuration resynchronization, NE synchronization, and PM data collection indicate that the load on the system is high. Reduce the load on the system before proceeding. Alarms associated with pruning times also indicate that the load on the system is high. Reschedule pruning at a time when the system has less activity.</p>

9.5.5 Enabling Fault Synchronization—CTC-Based NEs

Fault synchronization allows the system to collect the alarm history of an NE that has been marked as Out of Service for some time and is marked as In Service again. Alarm history is displayed in the Alarm Browser.

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel** and expand **NE Service**.
- Step 2** Choose **CTC-Based SONET NEs** or **CTC-Based SDH NEs**.
- Step 3** In the Robust Fault Synchronization area, check the appropriate check box:
- Enable ONS 15310 CL
 - Enable ONS 15310 MA
 - Enable ONS 15310 MA SDH
 - Enable ONS 15327
 - Enable ONS 15454
 - Enable ONS 15600
 - Enable ONS 15454 SDH
 - Enable ONS 15600 SDH
 - Enable CPT 200
 - Enable CPT 600
- Step 4** Click **Save**.
-

9.6 How Can I Find the Root Cause of the Fault?

Root cause analysis captures additional information about defects for the purpose of identifying preventive actions.

In some cases, the alarm report or set of alarm reports generated by a fault are sufficient to indicate the root cause. But often, the information in the alarm messages must be supplemented or confirmed by information from customer trouble reports, diagnostics and exercises of equipment, audits of software and databases, and testing of circuits. Tests of equipment are called *diagnostics*, which are designed to identify the root cause of a fault; *exercises*, which isolate a unit or subsystem and verify that it can perform its intended function; and *audits*, which verify the integrity of software.

The EMS should correlate events and determine the faults that exist in the network. To correlate events means to look for relationships between them.

9.6.1 Setting Up Error Logs

The Error Log tables display server error information that is useful for debugging Prime Optical processes. In most cases, the Error Log is requested by service personnel for debugging a problem on the Prime Optical server. The Error Log captures abnormal and significant events based on severity level. Critical, major, minor, and informational errors are logged to the database; trace and debug information is logged to a log file and does not appear in the Error Log.



Caution

Prime Optical performance will degrade if the trace or debug option is left on. All operations will slow down, and you might lose alarm and event notifications. Use trace or debug only when troubleshooting with a customer support engineer.

The Logging Properties pane allows you to control the volume of messages that is created by the server. To reduce the amount of information logged to the database, turn off entire components (Prime Optical and Prime Optical GateWay/SNMP).

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
 - Step 2** Click **Logging Properties** to open the Logging Properties pane. The Logging Properties pane contains the following tabs: General, SNMP Trap Service Debug, and Basic Service Logging. The following table provides descriptions.
 - Step 3** In the Preferences area of the General tab, choose the logging level that will be included in the Error Log for the Prime Optical server.
 - Step 4** Click **Save**. All changes take effect immediately and do not require restart of the server.
-

Table 9-14 Field Descriptions for the Logging Properties Pane

Field	Description
General Tab - Preferences	
Logging Level	Choose the error level to include in the log files for the Prime Optical server.

Table 9-14 Field Descriptions for the Logging Properties Pane (continued)


Field	Description
Log File Directory	Choose the directory where the log files are saved. The default directory is /opt/CiscoTransportManagerServer/log.
Max. Debug Log File Size	Select the maximum size of the Debug Log file, in megabytes (MB). You can select a default log size for each log file.
Upload Log Files button	Opens the Upload Log Files dialog box, which allows you to view a list of archive log files stored on the server and upload them to a specified directory on the client. See 9.6.1.2 Uploading Log Files, page 9-35 .
Compress File	Compresses the log file, optimizing space.
Enable Initialization Log	Enables the log file that pertains to initialization of a service. With initialization logging, debugging begins well before any service starts.
General Tab - Archiving	
Enable Log File Archiving	If checked, allows you to archive log files to facilitate longer term collection of logging information. When a log file is about to wrap, you can save the regular log file to a separate archive file.
Archive Directory	Specify the directory where archive log files are saved. The name of the archived file incorporates a time stamp (when the file is created) to ensure a unique filename.
Max. No. Archived Log Files	Specify the maximum number of log files to archive on the server. The range is from 1 to 25 files.
Upload Archive button	Opens the Upload Archive dialog box, which allows you to view a list of archive log files stored on the server and upload them to a specified directory on the client. See 9.6.1.1 Uploading Archive Log Files, page 9-34 .
General Tab - Levels of Errors Logged to the Database	
Critical	When this option is checked, Critical severity messages are logged in the Error Log.
Major	When this option is checked, Major severity messages are logged in the Error Log.
Minor	When this option is checked, Minor severity messages are logged in the Error Log.
Informational	When this option is checked, Informational severity messages are logged in the Error Log.
	 Caution Prime Optical performance will degrade if the Informational option is left on. All operations will slow down, and you might lose alarm and event notifications. Use Informational only when troubleshooting with a Cisco customer support engineer.
SNMP Trap Service Debug Tab - Overall Logging	
Enable	Select this radio button to enable overall debugging and to select debug modules for the SNMP trap service.
Disable	Select this radio button to disable overall debugging.
SNMP Trap Service Debug Tab - Debug Modules	
Available	Lists the modules that can be used for debugging. Select a module from the list; then, click the Add button to add the module to the Selected list.
Selected	Lists the modules that will be used for debugging. Select a module from the list; then, click the Remove button to remove the module from the Selected list.
Basic Service Logging Tab - Server Logging	

Table 9-14 Field Descriptions for the Logging Properties Pane (continued)

Field	Description
Enable	Select this radio button to enable Prime Optical server logging without enabling the logging operation on other services.
Disable	Select this radio button to disable Prime Optical server logging without disabling the logging operation on other services.
Basic Service Logging Tab - SM Service Logging	
Enable	Select this radio button to enable overall debugging and to select debug modules for the SM service.
Disable	Select this radio button to disable overall debugging.
Basic Service Logging Tab - SM Service Logging: Debug Modules	
Available	Lists the modules that can be used for debugging. Select a module from the list; then, click the Add button to add the module to the Selected list.
Selected	Lists the modules that will be used for debugging. Select a module from the list; then, click the Remove button to remove the module from the Selected list.

9.6.1.1 Uploading Archive Log Files

Use the Upload Archive dialog box to view a list of archive log files stored on the server and upload them to a specified directory on the client.

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** Click **Logging Properties** to open the Logging Properties pane.
- Step 3** In the General tab > Archiving area, click the **Upload Archive** button. The Upload Archive dialog box opens. The following table provides descriptions.
- Step 4** In the Files area, select log files from the list. To select multiple files, hold down the **Ctrl** key on your keyboard while using your mouse to click files. Click **Select All** to select all files in the list.
- Step 5** In the Upload Location text field, specify where you want to save the log files. Click **Browse** to choose a client location different from the default.
- Step 6** Click **Upload** to upload the selected log files to the specified directory.
-

Table 9-15 Field Descriptions for the Upload Archive Dialog Box

Field	Description
Files	Lists the archive files available on the server location.
Upload Location	Allows you to specify where you want to save the archive files. The default location is <i>client-installation-directory\archive\</i> or <i>client-installation-directory/archive/</i> . Click Browse to choose a different location.
Upload	Uploads the selected log files to the specified location on the client.
Select All	Selects all of the log files in the list.

Table 9-15 Field Descriptions for the Upload Archive Dialog Box (continued)

Field	Description
Cancel	Replaces any changes to user-defined fields with the previous values and closes the dialog box.
Help	Launches the online help for the Upload Archive dialog box.

9.6.1.2 Uploading Log Files

Use the Upload Log Files dialog box to view a list of log files stored on the server and upload them to a specified directory on the client.

-
- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** Click **Logging Properties** to open the Logging Properties pane.
- Step 3** In the General tab > Preferences area, click the **Upload Log Files** button. The Upload Log Files dialog box opens. The following table provides descriptions.
- Step 4** In the Files area, select log files from the list. To select multiple files, hold down the **Ctrl** key on your keyboard while using your mouse to click files. Click **Select All** to select all files in the list.
- Step 5** In the Upload Location text field, specify where you want to save the log files. Click **Browse** to choose a client location different from the default.
- Step 6** Click **Upload** to upload the selected log files to the specified directory.
-

Table 9-16 Field Descriptions for the Upload Log Files Dialog Box

Field	Description
Files	Lists the log files available on the server location.
Upload Location	Allows you to specify where you want to save the log files. The default location is <i>client-installation-directory\log\</i> or <i>client-installation-directory/log/</i> . Click Browse to choose a different location.
Upload	Uploads the selected log files to the specified location on the client.
Select All	Selects all of the log files in the list.
Cancel	Replaces any changes to user-defined fields with the previous values and closes the dialog box.
Help	Launches the online help for the Upload Log Files dialog box.

9.6.2 Viewing the Error Log

The Error Log shows Prime Optical server error information that is useful for debugging purposes. In most cases, the Error Log is requested by service personnel for debugging a problem on the Prime Optical server. The Error Log captures abnormal and significant events based on severity level.

As the default, the Error Log displays information about significant events that occurred during the last four hours. You can change the default time period in the User Preferences dialog box.

To open the Error Log, choose **Administration > Error Log** in the Domain Explorer. The following table describes the fields in the Error Log.

Table 9-17 *Field Descriptions for the Error Log*

Column Name	Description
Time Stamp	Date and time when the error occurred on the Prime Optical server.
Module	Name of the module where the error occurred.
Severity	Severity level of the error: <ul style="list-style-type: none"> Critical, Major, Minor, or Informational—When set to any of these severity levels, all messages corresponding to critical, major, and minor severity levels are logged to the database and all informational messages are stored in the log file. Debug or Trace—When set to debug or trace, all informational and higher messages are logged to the database. All debug and trace messages are logged to the log files.
Submodule	Name of the submodule where the error occurred.
Filename	Name of the file where the error occurred. Cisco technical support engineers use this information for troubleshooting.
Line	Exact line where the error occurred. Cisco technical support engineers use this information for troubleshooting.
Message	Text of the error message.

By default, all messages are logged to the following files in the /opt/CiscoTransportManagerServer/log directory:

- CTMTL1FWDerror.log
- CTMServerError.log
- CTMerror.log
- ONS15216NEService-number-time-stamp.log
- ONS15305NEService-number-time-stamp.log
- ONS1530xPMSERVICE-number-time-stamp.log
- ONS15454NEService-number-time-stamp.log
- ONS15454SDHNEService-number-time-stamp.log
- ONS15454SDHPMSERVICE-number-time-stamp.log
- ONS15454PMSERVICE-number-time-stamp.log
- ONS155xxNEService-number-time-stamp.log
- ONS155xxPMSERVICE-number-time-stamp.log
- ONS15600SDHPMSERVICE-number-time-stamp.log
- ONS15600PMSERVICE-number-time-stamp.log
- UnmanagedNEService-number-time-stamp.log
- SMSERVICE-0-time-stamp.log
- SnmpTrapService-2-time-stamp.log

- CORBAGWService-1-time-stamp.log

By default, all Syslog Service messages are logged to the SyslogService.log file in the /opt/CiscoTransportManagerServer/log directory.

**Note**

The default directory /opt/CiscoTransportManagerServer might have been changed during installation of the Prime Optical server.

After resetting the Error Log level to Critical, Major, Minor, or Informational, remove the log files to free disk space. Each time a new log file is started, a backup of the previous file is kept in the *log-file.bak* file. Remove the backup file at any time.

9.6.3 Filtering Data in the Error Log

- Step 1** In the Error Log, choose **File > Filter** (or click the **Filter Data** tool). The Filter dialog box opens.
- Step 2** Specify the filter parameters described in the following table.
- Step 3** After making your selections, click **OK** to run the filter.

Table 9-18 Field Descriptions for the Error Log Filter Dialog Box

Tab	Description
Time Stamp (time zone)	<p>Allows you to filter Error Log data for a specified time period, ranging from the past hour to the past 6 months. Click the User Specified radio button to specify exact filter start and end times by date and hour. The time zone can be GMT, a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. Use the calendar tool to choose the year, month, and day:</p> <ul style="list-style-type: none"> • Year—Click the year combo box or the double arrow (<<, >>) at the bottom of the calendar. • Month—Click the month combo box or the single arrow (<, >) at the bottom of the calendar. • Day—Click the day number on the calendar. The current date is shown in blue. <p>If you want to filter Error Log data and the time period is not important, click No Time Specified.</p>
Modules	Allows you to filter Error Log data by Prime Optical module.
Submodules	Allows you to select Prime Optical server submodules to filter Error Log data.
Severity	Allows you to filter Error Log data based on severity level: Critical, major, minor, and informational.

9.6.4 Managing the NE Audit Trail—CTC-Based NEs

The Audit Trail table is a security tool used to investigate unauthorized activities after they occur so that proper remedial action can be taken. It displays audit trail information for CTC-based NEs.

Audit trail entries might be missing from the Audit Trail table because of the following reasons:

- There is heavy provisioning activity on the NE that the local audit trail log on the NE might wrap between polling intervals, and records will be missed for collection.
- The server is down or communications to the NE are unavailable for an extended period. There is a greater likelihood that the log on the NE will wrap before the system can collect the records.


Note

- The audit trail collection interval can be set in the applicable NE Service pane in the Control Panel. See [9.6.4.4 Changing the Audit Trail Collection Interval, page 9-39](#).
- To collect the latest and most reliable audit trail information for a specific NE, the time must be synchronized with the SNTP server. Do not manually set the clock on CTC-based NEs.

9.6.4.1 Viewing the Audit Trail Table

To view the Audit Trail table, choose **Administration > CTC-Based NEs > Audit Trail Table**. The following table provides descriptions.

Table 9-19 *Field Descriptions for the Audit Trail Table*

Field	Description
Alias ID	Alias name of the NE.
Sequence Number	NE-generated record ID.
NE Username	NE user ID.
Time Stamp	Date and time.
Description of Operation	Description of the audit trail operation.
Status of Operation on NE	Status of the audit trail operation. Statuses are Passed, Failed, and Aborted.
NE ID	ID of the selected NE.

9.6.4.2 Filtering Data in the Audit Trail Table

-
- Step 1** In the Audit Trail table, choose **File > Filter** (or click the **Filter Data** tool). The Filter dialog box opens.
- Step 2** Specify the filter parameters described in the following table.
- Step 3** After making your selections, click **OK** to run the filter.
-

Table 9-20 **Field Descriptions for the Audit Trail Table Filter Dialog Box**

Tab	Description
Time Stamp (time zone)	<p>Allows you to filter audit trail data for a specified time period, ranging from the past hour to the past 6 months. Additionally, you can click the User Specified radio button to specify exact filter start and end times by date and hour. The time zone can be GMT, a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. Use the calendar tool to choose the year, month, and day:</p> <ul style="list-style-type: none"> • Year—Click the year combo box or the double arrow (<<, >>) at the bottom of the calendar. • Month—Click the month combo box or the single arrow (<, >) at the bottom of the calendar. • Day—Click the day number on the calendar. The current date is shown in blue. <p>Click No Time Specified if you want to filter audit trail data and the time period is not important.</p>
NE ID	Allows you to move NEs back and forth between the list of available NEs and selected NEs. The filter runs on the NEs in the Selected NE ID list.
Username	Allows you to move users back and forth between the list of available users and selected users. The filter runs on the users in the Selected Users list.
Sequence Number	<p>Allows you to enter a starting and ending sequence number for filtering. Check the Disregard All Other Filter Criteria check box to base the filter on only the starting and ending sequence number.</p> <p>Note If the sequence number reaches 59999, Prime Optical collects audit records starting with 1 in the next collection interval.</p>
Operation Status	Select an operation status for filtering. Operation statuses are Passed, Failed, and Aborted.

9.6.4.3 Enabling or Disabling Audit Trail Collection

- Step 1** In the Domain Explorer tree, select a CTC-Based NE.
- Step 2** In the Network Element Properties pane > Status tab > Audit Trail State field, choose **Enabled** or **Disabled** from the drop-down list.



Note By default, the Audit Trail State field is set to Disabled.

- Step 3** Click **Save**.

9.6.4.4 Changing the Audit Trail Collection Interval

- Step 1** In the Domain Explorer, choose **Administration > Control Panel**.
- Step 2** In the Control Panel, expand **NE Service** and choose **CTC-Based SONET NEs** or **CTC-Based SDH NEs**.
- Step 3** In the Status tab > Audit Trail Collection Interval field, enter the collection interval time. The default is 30 minutes.

Step 4 Click **Save**.

9.6.5 Setting Debug Options

In Prime Optical, the debug option gives you information to investigate, diagnose, and fix a problem. Specifying debug options allows you to choose parameters to display in the Debug Log.

- Step 1** In the Domain Explorer, choose **File > Debug Options**.
- Step 2** Specify the debug options. The following table provides descriptions.
- Step 3** After making your selections, click **Apply**.

Table 9-21 Field Descriptions for the Debug Options Dialog Box



Field	Description
Modules	
Available, Selected	Select modules that will display debug messages. Use the Add and Remove buttons to move modules to the Selected list or remove modules from the list.
Debug Level	
Fatal	Instructs the Debug Log to display messages with a severity level of at least Fatal.
Warning	Instructs the Debug Log to display messages with a severity level of at least Warning.
Info	Instructs the Debug Log to display messages with a severity level of at least Info.
Debug	Instructs the Debug Log to display messages with a severity level of at least Debug.  Caution Prime Optical performance will degrade if the Debug option is left on. All operations will slow down, and you might lose alarm and event notifications. Use Debug only when troubleshooting with a Cisco customer support engineer.
Trace	Instructs the Debug Log to display messages with a severity level of Trace.  Caution Prime Optical performance will degrade if the Trace option is left on. All operations will slow down, and you might lose alarm and event notifications. Use Trace only when troubleshooting with a Cisco customer support engineer.

Table 9-21 Field Descriptions for the Debug Options Dialog Box (continued)

Field	Description
Display Options	
File	<p>Check the File check box to write the Debug Log to a specific file. You can click Browse to browse for a local client directory for the Debug Log. After you specify the filename, the log is stored in <i>filename0.log</i>, and then in <i>filename1.log</i> when <i>filename0.log</i> reaches its maximum size.</p> <p>By default, the Debug Log is saved at C:\Cisco\TransportManagerClient<i>version-number</i>\debug\CTMC-debug0.log or /opt/CiscoTransportManagerClient<i>version-number</i>/debug/CTMC-debug0.log. The dialog box shows the filename without the number 0 or 1, which is appended by default by the Java debugging APIs.</p> <p>Note <i>version-number</i> is replaced by the version number of the installed Prime Optical client.</p>
Max File Size	Enter the maximum file size for the Debug Log, in bytes.
Console	Check the Console check box to write the Debug Log to the console.

9.7 Who Is Responsible for Managing the Fault?

To manage faults effectively, you must know who is taking responsibility for managing each case. Prime Optical offers the following options:

- [9.7.1 Acknowledging and Unacknowledging Alarms, page 9-41](#)
- [9.7.2 Configuring Alarm Acknowledgement and Alarm Notes, page 9-42](#)

9.7.1 Acknowledging and Unacknowledging Alarms

The alarm acknowledgement feature acknowledges selected alarms or all alarms with a single click.

- Step 1** In the Domain Explorer window, select an NE and choose **Fault > Alarm Browser**. This opens the Alarm Browser window for the selected NE.
- The Alarm Browser window lists critical, major, minor, and warning alarms that have not been cleared or cleared alarms that have not been acknowledged.
- Step 2** Select the alarms to be acknowledged and choose **Fault > Acknowledge Alarms** (or click the **Acknowledge Selected Alarm(s)** tool). Click **Yes** in the confirmation dialog box. Click the **Refresh Data** tool to see the changes. A check mark icon provides a visual indication of acknowledged alarms.
- Step 3** Click the **Acknowledge Selected Alarm(s)** tool again to unacknowledge the selected alarms. Click **Yes** in the confirmation dialog box. Click **Refresh Data** to see the changes. The check mark is removed, indicating that the alarm has been unacknowledged.



Note Alarm unacknowledgement is disabled by default. Make sure to enable the alarm unacknowledgement feature in the Control Panel before unacknowledging an alarm. See [9.7.2 Configuring Alarm Acknowledgement and Alarm Notes, page 9-42](#) for more information.

- Step 4** To acknowledge all alarms in the view, choose **Fault > Acknowledge All Alarms** (or click the **Acknowledge All Alarms** tool). Click **Yes** in the confirmation dialog box.

9.7.2 Configuring Alarm Acknowledgement and Alarm Notes

Use the UI Properties pane to configure alarm acknowledgment and enable or disable the alarm note feature.

- Step 1** In the Domain Explorer window, choose **Administration > Control Panel** and click **UI Properties**.

- Step 2** In the Fault Management area, select either Manual or Automatic for alarm acknowledgment.

- If you choose **Manual**, alarms must be acknowledged manually. Cleared alarms move from the Alarm Browser to the Alarm Log once they are acknowledged.
- If you choose **Automatic**, the server automatically acknowledges alarms when they are cleared and moves them from the Alarm Browser to the Alarm Log.



Note

Active alarms are not automatically acknowledged.

If the alarms are initially set to Manual Alarm Acknowledgement, and then you switch to Automatic Alarm Acknowledgement, all the alarms in the Alarm Browser will be cleared and acknowledged automatically. This might take a while, depending on the number of alarms in the database that have not been acknowledged manually.

You can still acknowledge alarms manually even if Automatic Alarm Acknowledgment is set.

- Step 3** Use the Overwrite Alarm Notes option to enable or disable the ability to overwrite alarm notes created by another user.

- Step 4** Choose either Enable or Disable for alarm unacknowledgement.

- If you choose **Enable**, you can unacknowledge alarms in the Alarm Browser.
- If you choose **Disable**, alarms cannot be unacknowledged in the Alarm Browser.

- Step 5** Click **Save**.

9.8 How Can the Fault Be Fixed?

After receiving an alarm, the EMS or the user must take some sort of action on each of the faults. This can include logging the fault, delivering it to an appropriate tracking application, alerting key personnel to a critical fault, or implementing a repair.

9.8.1 Clearing a Security Violation Alarm—ONS 15305 R3.0, ONS 15327, ONS 15454 SONET, ONS 15454 SDH

-
- | | |
|---------------|---|
| Step 1 | In the Domain Explorer tree, select an ONS 15305 R3.0, ONS 15327, ONS 15454 SONET, or ONS 15454 SDH NE and choose Configuration > NE Explorer (or click the Open NE Explorer tool). |
| Step 2 | In the NE Explorer window, choose Fault > Clear Security Violation Alarm . A message appears if there are no security violations or intrusion alarms on the NE or if the operation has been accepted. |
| Step 3 | Click OK in the message box. |
-

9.8.2 Performing a System Reset—ONS 15600 SONET and ONS 15600 SDH

-
- | | |
|---------------|--|
| Step 1 | In the Domain Explorer tree, select the ONS 15600 SONET or ONS 15600 SDH NE for which to view the configuration. |
| Step 2 | Choose Configuration > NE Explorer (or click the Open NE Explorer tool). |
| Step 3 | In the NE Explorer, choose File > System Reset . |
-

9.8.3 Exporting Alarms and Events to a Text File

Use the Event Export Manager to export alarms and events to a text file as they occur. In addition, you can use the Event Export Manager to set various export parameters to refine the export. See [1.6.8 Exporting Alarms and Events, page 1-42](#).

