



Manage Alarms

This chapter explains how to view and manage the alarms and conditions on a Cisco ONS 15454.

Cisco Transport Controller (CTC) detects and reports alarms generated by the Cisco ONS 15454 and the ONS network. You can use CTC to monitor and manage alarms at a card, node, or network level. You can also view alarm counts on the LCD front panel.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. [NTP-A195 Document Existing Provisioning, page 9-2](#)—Complete this procedure as needed to print or export node data.
2. [NTP-A196 View Alarms, History, Events, and Conditions, page 9-5](#)—Complete this procedure as needed to see alarms and conditions occurring on the node and a complete history of alarm and condition messages.
3. [NTP-A68 Delete Cleared Alarms from Display, page 9-13](#)—Complete this procedure as needed to delete cleared alarm information.
4. [NTP-A69 View Alarm-Affected Circuits, page 9-14](#)—Complete this procedure as needed to find circuits that are affected by a particular alarm or condition.
5. [NTP-A70 View Alarm Counts on the LCD for a Node, Slot, or Port, page 9-16](#)—Complete this procedure as needed to see a statistical count of alarms that have occurred for a slot or port.
6. [NTP-A71 Create, Download, and Assign Alarm Severity Profiles, page 9-17](#)—Complete this procedure as needed to change the default severity for certain alarms, to assign the new severities to a port, card, or node, and to delete alarm profiles.
7. [NTP-A168 Enable, Modify, or Disable Alarm Severity Filtering, page 9-29](#)—Complete this procedure as needed to enable, disable, or modify alarm severity filtering in the Conditions, Alarms, or History screens at the node or network level.
8. [NTP-A72 Suppress Alarms or Discontinue Alarm Suppression, page 9-33](#)—Use these tasks as needed to suppress reported alarms at the port, card, or node level and to disable the suppress command to resume normal alarm reporting.

NTP-A195 Document Existing Provisioning

Purpose	This procedure prints card, node, or network CTC information in graphical or tabular form on a Windows-provisioned printer. It also exports card, node, or network information as delineated text files to other applications. This procedure is useful for network record keeping and troubleshooting.
Tools/Equipment	A printer connected to the CTC computer by a direct or network connection
Prerequisite Procedures	Chapter 4, “Turn Up Node”
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

-
- Step 1** Complete the [“DLP-A60 Log into CTC” task on page 3-24](#) at the node where you want to record or save data. If you are already logged in, continue with [Step 2](#).
- Step 2** As needed, complete the [“DLP-A515 Print CTC Data” task on page 9-2](#).
- Step 3** As needed, complete the [“DLP-A516 Export CTC Data” task on page 9-4](#).
- Stop. You have completed this procedure.**
-

DLP-A515 Print CTC Data

Purpose	This task prints CTC card, node, or network data in graphical or tabular form on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

-
- Step 1** Click the tab (and subtab, if present) containing the information you want to print. For example, click the **Alarms** tab to print Alarms window data.
- The print operation is available for all network, node, and card view windows.
- Step 2** From the File menu choose **Print**.
- Step 3** In the Print dialog box, click a printing option ([Figure 9-1](#)).
- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.
 - Tabbed View—Prints the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed View, you print only history items appearing in the window. This option is available for all windows.

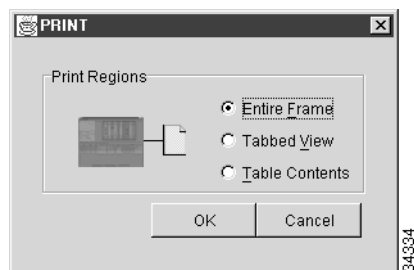
- Table Contents—Prints CTC data in table format without graphical representations of shelves, cards, or tabs. This option applies to all windows except:
 - Provisioning > General > General, Power Monitor windows
 - Provisioning > Network > General, RIP windows
 - Provisioning > Security > Policy, Access, or Legal Disclaimer windows
 - Provisioning > SNMP window
 - Provisioning > Timing window
 - Provisioning > UCP > Node window
 - Provisioning > WDM-ANS> Provisioning window
 - Maintenance > Cross-Connect > Cards window
 - Maintenance > Database window
 - Maintenance > Diagnostic window
 - Maintenance > Protection window
 - Maintenance > Timing > Source window

The Table Contents option prints all the data contained in a table and the table column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

**Tip**

When you print using the Tabbed View option, it can be difficult to distinguish whether the printout applies to the network, node, or card view. To determine the view, compare the tabs on the printout. The network, node, and card views are identical except that network view does not contain an Inventory tab or Performance tab.

Figure 9-1 Selecting CTC Data For Print



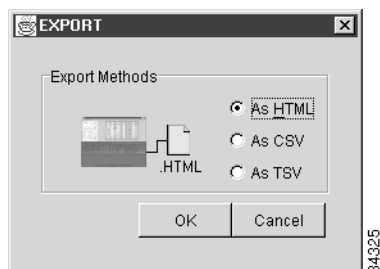
- Step 4** Click **OK**.
- Step 5** In the Windows Print dialog box, click a printer and click **OK**.
- Step 6** Repeat this task for each window that you want to print.
- Step 7** Return to your originating procedure (NTP).

DLP-A516 Export CTC Data

Purpose	This task exports CTC table data as delineated text to view or edit the data in text editor, word processing, spreadsheet, database management, or web browser applications.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

-
- Step 1** Click the tab containing the information you want to export (for example, the Alarms tab or the Circuits tab).
- Step 2** Choose **Export from the File menu**.
- Step 3** In the Export dialog box, click a data format ([Figure 9-2](#)):
- As HTML—Saves data as a simple HTML table file without graphics. The file must be viewed or edited with applications such as Netscape Navigator, Microsoft Internet Explorer, or other applications capable of opening HTML files.
 - As CSV—Saves the CTC table as comma-separated values (CSV). This option does not apply to the Maintenance > Timing > Report window.
 - As TSV—Saves the CTC table as tab-separated values (TSV).

Figure 9-2 Selecting CTC Data For Export



- Step 4** If you want to open a file in a text editor or word processor application, procedures may vary; but typically you can use the File > Open command to view the CTC data, or you can double-click the file name and choose an application such as Notepad.
- Text editor and word processor applications format the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.
- Step 5** If you want to open the file in spreadsheet and database management applications, procedures may vary; but typically you need to open the application and choose File > Import, then choose a delimited file to format the data in cells.

Spreadsheet and database management programs also allow you to manage the exported data.



Note An exported file cannot be opened in CTC.

The export operation applies to all tabular data except:

- Provisioning > General > General, Power Monitor windows
- Provisioning > Network > General, RIP windows
- Provisioning > Security > Policy, Access, or Legal Disclaimer windows
- Provisioning > SNMP window
- Provisioning > Timing window
- Provisioning > UCP > Node window
- Provisioning > WDM-ANS> Provisioning window
- Maintenance > Cross-Connect > Cards window
- Maintenance > Database window
- Maintenance > Diagnostic window
- Maintenance > Protection window
- Maintenance > Timing > Source, Report windows

Step 6 Click **OK**.

Step 7 In the Save dialog box, enter a name in the File name field using one of the following formats:

- [filename].html—for HTML files
- [filename].csv—for CSV files
- [filename].tsv—for TSV files

Step 8 Navigate to a directory where you want to store the file.

Step 9 Click **OK**.

Step 10 Repeat the task for each window that you want to export.

Step 11 Return to your originating procedure (NTP).

NTP-A196 View Alarms, History, Events, and Conditions

Purpose	This procedure is used to view current or historical alarms and conditions for a card, a node, or network. This information is useful for monitoring and troubleshooting hardware and software events.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Complete the “[DLP-A60 Log into CTC](#)” task on page 3-24 at the node that contains the alarms you want to view. If you are already logged in, continue with [Step 2](#).

Step 2 In the card, node, or network view, click the **Alarms** tab to view the alarms for that card, node, or network ([Figure 9-3](#)).

Figure 9-3 CTC Node View

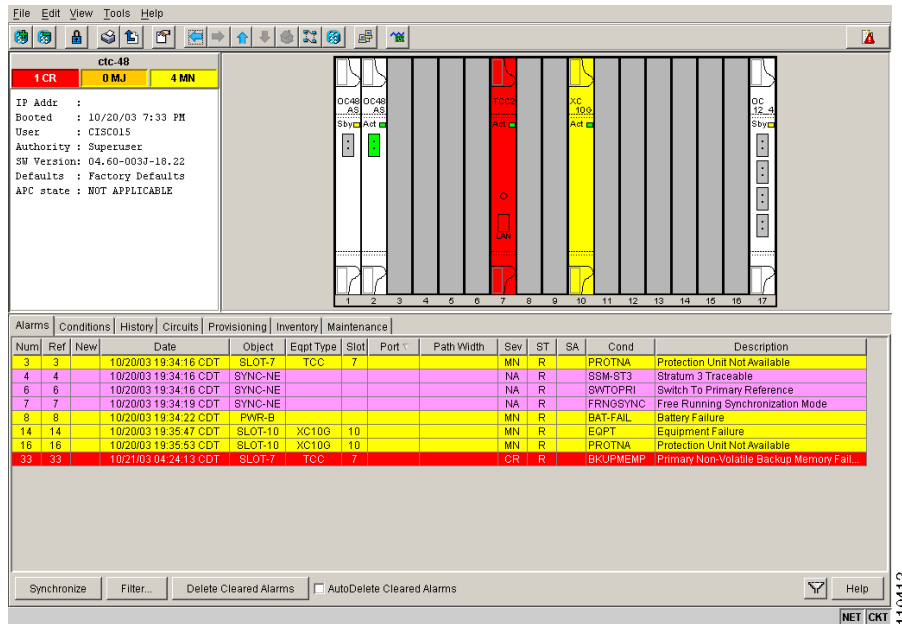


Table 9-1 lists the columns in the Alarms window and their descriptions.

Table 9-1 Alarm Column Descriptions

Column	Information Recorded
New	Indicates a new alarm; to change this status, click either the Synchronize button or the Delete Cleared Alarms button
Date	Date and time of the alarm
Node	Node where the alarm occurred (appears only in network view)
Object	TL1 access identifier (AID) for the alarmed object; for an STSmon or VTmon, this is the monitored STS or VT
Eqpt Type	If an alarm is raised on a card, the card type in this slot
Slot	If an alarm is raised on a card, the slot where the alarm occurred (appears only in network and node view)
Port	If an alarm is raised on a card, the port where the alarm is raised; for STSTerm and VTTerm, the port refers to the upstream card it is partnered with
Path Width	Indicates how many STSs are contained in the alarmed path. This information compliments the alarm object notation, which is explained in Table 9-3.
Sev	Severity level: CR (critical), MJ (major), MN (minor), NA (not-alarmed), NR (not-reported)
ST	Status: R (raised), C (clear)
SA	When checked, indicates a service-affecting alarm
Cond	The error message/alarm name; these names are alphabetically defined in the <i>Cisco ONS 15454 Troubleshooting Guide</i>
Description	Description of the alarm

Table 9-1 Alarm Column Descriptions (continued)

Column	Information Recorded
Num	An incrementing count of alarm messages
Ref	The reference number assigned to the alarm

Table 9-2 lists the color codes for alarm and condition severities. In addition to the severities listed in the table, CTC alarm profiles list inherited (I) and unset (U) severities. These are only listed in the network view Provisioning > Alarm Profiles tab and are not currently implemented.

Table 9-2 Color Codes for Alarms and Condition Severities

Color	Description
Red	Raised Critical (CR) alarm
Orange	Raised Major (MJ) alarm
Yellow	Raised Minor (MN) alarm
Magenta (pink)	Raised Not-Alarmed (NA) condition
Blue	Raised Not-Reported (NR) condition
White	Cleared (C) alarm or condition

In network view, CTC identifies STS and VT alarm objects using a TL1-type access identifier (AID).

Table 9-3 lists these AIDs.

Table 9-3 Network View STS and Alarm Object Identification

STS and VT Alarm Numbering		
MON object	STS-<Slot>-<Port>-<STS> For example, STS-6-1-6 VT1-<Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-1-6-1-1	Port=1
TERM object	<Upstream Slot>-<Port>-<STS> For example, STS-6-3-6 <Upstream Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-3-6-1-1	Port=1

Step 3 If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide* for information and troubleshooting procedures.

Step 4 Complete the “DLP-A517 View Alarm or Event History” task on page 9-8, the “DLP-A113 Synchronize Alarms” task on page 9-11, or the “DLP-A114 View Conditions” task on page 9-11 as needed.

Stop. You have completed this procedure.

DLP-A517 View Alarm or Event History

Purpose	This task is used to view past cleared and uncleared ONS 15454 alarm messages at the card, node, or network level. This task is useful for troubleshooting configuration, traffic, or connectivity issues that are indicated by alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Decide whether you want to view the alarm message history at the node, network, or card level.

Step 2 To view node alarm history:

- a. Click the **History > Session** tabs to view the alarms and conditions (events) raised during the current session.
- b. Click the **History > Node** tabs to view the alarm and condition history for the node.
If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.
- c. Click **Retrieve** to view all available messages for the History > Node tabs.



Note

Alarms can be unreported when they are filtered out of the display using the Filter button in either tab. See the [“DLP-A225 Enable Alarm Filtering” task on page 9-29](#) for information.



Tip

Double-click an alarm in the alarm table or an event (condition) message in the history table to display the view that corresponds to the alarm message. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Step 3 To view network alarm history, from node view:

- a. From the **View** menu choose **Go to Network View**.
- b. Click the **History** tab.
Alarms and conditions (events) raised during the current session appear.

Step 4 To view card alarm history from node view:

- a. From the View menu choose **Go to Previous View**.
- b. Double-click a card on the shelf graphic to open the card-level view.



Note

TCC2 cards and cross-connect (XC or XC10G) cards do not have a card view.

- c. Click the **History > Session** tab to view the alarm messages raised during the current session.

- d. Click the **History > Card** tab to retrieve all available alarm messages for the card and click **Retrieve**.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.



Note The ONS 15454 can store up to 640 critical alarm messages, 640 major alarm messages, 640 minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15454 discards the oldest events in that category.

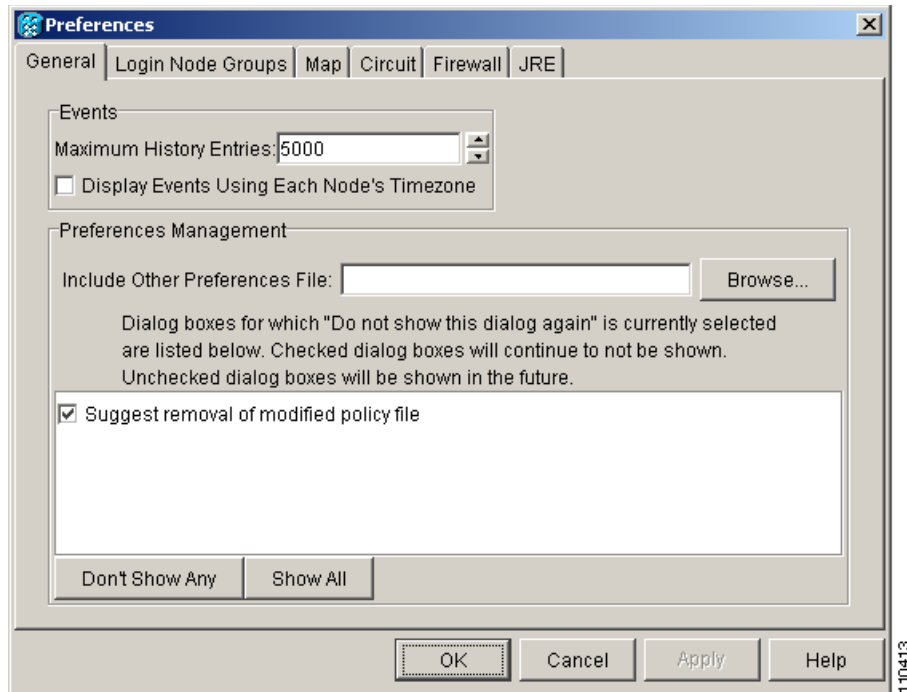
Raised and cleared alarm messages (and events, if selected) appear.

- Step 5** Return to your originating procedure (NTP).

DLP-A111 Changing the Maximum Number of Session Entries for Alarm History

Purpose	This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

- Step 1** From the Edit menu, choose **Preferences**.
The CTC Preferences dialog box appears ([Figure 9-4](#)).

Figure 9-4 CTC Preferences Dialog Box

Step 2 Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.

Step 3 Click **Apply** and **OK**.



Note Setting the Maximum History Entries value to the high end of the range uses more CTC memory and could impair CTC performance.



Note This task changes the maximum history entries recorded for CTC sessions. It does not affect the maximum number of history entries viewable for a network, node, or card.

Step 4 Return to your originating procedure (NTP).

DLP-A112 Display Alarms and Conditions Using Time Zone

Purpose	This task changes the timestamp for events to the timezone of the ONS node reporting the alarm. By default, the events timestamp is set to the timezone for the CTC workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

-
- Step 1** From the Edit menu, choose **Preferences**.
The CTC Preferences dialog box appears ([Figure 9-4 on page 9-10](#)).
- Step 2** Check the **Display Events Using Each Node's Timezone** check box. The Apply button is enabled.
- Step 3** Click **Apply** and **OK**.
- Step 4** Return to your originating procedure (NTP).
-

DLP-A113 Synchronize Alarms

Purpose	This task is used to view ONS 15454 events at the card, node, or network level and to refresh the alarm listing so that you can check for new and cleared alarms and conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

- Step 1** At the card, node, or network view, click the **Alarms** tab.

- Step 2** Click **Synchronize**.

This button causes CTC to retrieve a current alarm summary for the card, node, or network. This step is optional because CTC updates the Alarms window automatically as raise/clear messages arrive from the node.



Note Alarms that have been raised during the session will have a check mark in the Alarms window New column. When you click Synchronize, the check mark disappears.

- Step 3** Return to your originating procedure (NTP).
-

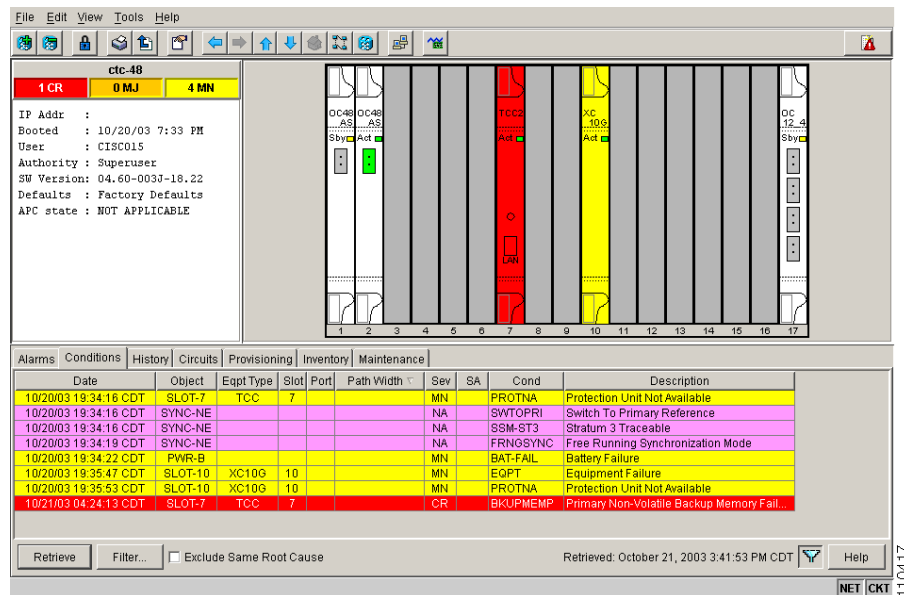
DLP-A114 View Conditions

Purpose	This task is used to view conditions [events with a Not-Reported (NR) severity] at the card, node, or network level. Conditions give you a clear record of changes or events that do not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

- Step 1** From the card, node, or network view, click the **Conditions** tab.
- Step 2** Click **Retrieve** (Figure 9-5).

The Retrieve button requests the current set of fault conditions from the node, card, or network. The window is not updated when events change on the node. You must click Retrieve to see any changes.

Figure 9-5 Node View Conditions Window



Conditions include all fault conditions raised on the node, whether or not they are reported.



Note Alarms can be unreported when they are filtered out of the display. See the [“DLP-A225 Enable Alarm Filtering” task on page 9-29](#) for information.

Events that are reported as Major (MJ), Minor (MN), or Critical (CR) severities are alarms. Events that are reported as Not-Alarmed (NA) are conditions. Conditions that are not reported at all are marked Not-Reported (NR) in the Conditions window severity column.

Conditions that have a default severity of Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA) but are not reported due to exclusion or suppression are shown as NR in the Conditions window.



Note For more information about alarm suppression, see the [“DLP-A522 Suppress Alarm Reporting” task on page 9-33](#).

Current conditions are shown with the severity chosen in the alarm profile, if used. For more information about alarm profiles, see the [“NTP-A71 Create, Download, and Assign Alarm Severity Profiles” procedure on page 9-17](#).



Note When a port is placed in the out of service for maintenance (OOS-MT) state, it raises an Alarms Suppressed for Maintenance (AS-MT) condition. For information about alarm and condition troubleshooting, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

**Note**

When a port is placed in out of service/auto in-service state but is not connected to a valid signal, it generates a loss of signal (LOS) alarm.

- Step 3** If you want to apply exclusion rules, check the **Exclude Same Root Cause** check box at the node or network view, but do not check the Exclude Same Root Cause check box in card view.
- An exclusion rule eliminates all lower-level alarms or conditions that originate from the same cause. For example, a fiber break may cause an LOS alarm, an AIS condition, and an SF condition. If you check the Exclude Same Root Cause check box, only the LOS alarm will appear. According to Telcordia, exclusion rules apply to a query of “all conditions from a node.”
- Step 4** Return to your originating procedure (NTP).

NTP-A68 Delete Cleared Alarms from Display

Purpose	This procedure deletes Cleared (C) status alarms from the alarms window. The procedure can be used to delete transient messages from the CTC History window.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 3-24 at a node where you want to delete alarms. If you are already logged in, go to [Step 2](#).
- Step 2** To delete cleared node-level alarms:
- In the node view, click the **Alarms** tab.
 - Click **Delete Cleared Alarms**, referring to the rules in [Step 5](#).
- This action removes any cleared ONS 15454 alarms from the Alarms tab. The rows of cleared alarms turn white and have a C in their status (ST) column ([Figure 9-5 on page 9-12](#)).
- Step 3** To delete cleared card-level alarms:
- In the node view, double-click the card graphic for the card you want to open.
 - Click the **Alarms** tab and then click **Delete Cleared Alarms**, referring to the rules in [Step 5](#).
- Step 4** To delete cleared network-level alarms:
- In the node view click **View > Go to Network View**.
 - Click the **Alarms** tab and then click **Delete Cleared Alarms**, referring to the rules in [Step 5](#).

- Step 5** Consult the following rules when deleting cleared alarms:
- If the Autodelete Cleared Alarms check box is checked, an alarm disappears from the window when it is cleared.
 - If the Autodelete Cleared Alarms check box is not checked, an alarm remains in the window when it is cleared. The alarm appears white in the window and has a Clear (CL) severity. The alarm can be removed by clicking the Delete Cleared Alarms button.
- Step 6** To remove the transient messages from the History window, click **Delete Cleared Alarms**. Transient messages are single messages, not raise-and-clear pairs (that is, they do not have companion messages stating they are cleared).
- Stop. You have completed this procedure.**
-

NTP-A69 View Alarm-Affected Circuits

Purpose	This procedure is used to view all circuits, if any, affected by an alarm or condition.
Tools/Equipment	None
Prerequisite Procedures	NTP-A196 View Alarms, History, Events, and Conditions, page 9-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

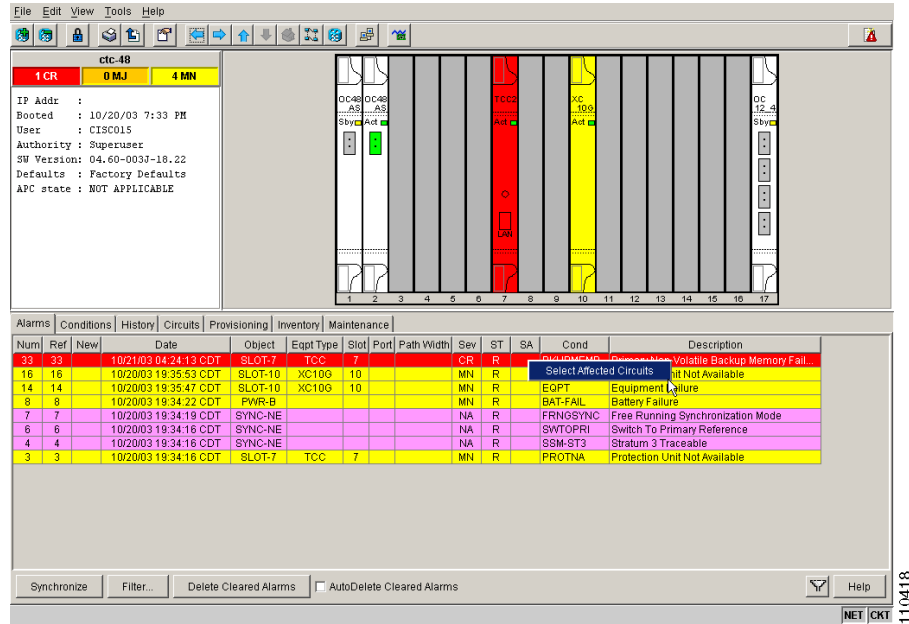
- Step 1** Complete the [“DLP-A60 Log into CTC” task on page 3-24](#). If you are already logged in, continue with [Step 2](#).
- Step 2** In the network, node, or card view, click the **Alarms** tab or **Conditions** tab and then right-click anywhere in the row of an active alarm or condition.



Note The node view is the default, but you can also navigate to the Alarms tab in the network view or card view to perform Step 2.

The Select Affected Circuits option appears on the shortcut menu ([Figure 9-6](#)).

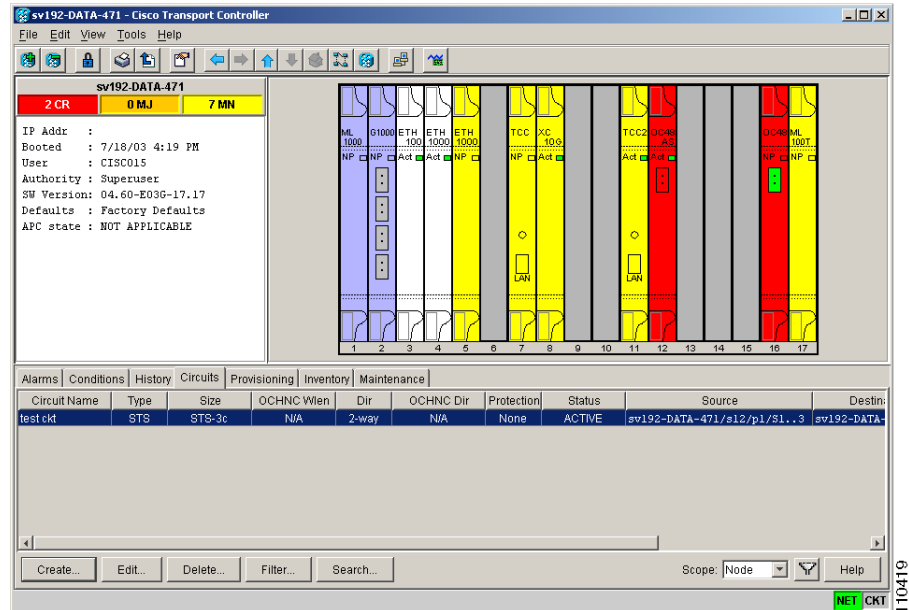
Figure 9-6 Select Affected Circuits Option



Step 3 Left-click or right-click **Select Affected Circuits**.

The **Circuits** window appears with the affected circuits highlighted (Figure 9-7).

Figure 9-7 Viewing Alarm-Affected Circuits



In Release 4.6, Select Affected Circuits behaves differently according to card types, as listed in [Table 9-4](#).

Table 9-4 Select Affected Circuits Behavior by Alarm Type

Alarm Type	Behavior
Transient alarms (such as BLSROSYNC)	CTC displays all circuits on the node.
BITS alarms (such as SWTOSEC) Synchronization alarms (such as SYNCSEC)	CTC displays all circuits on node that the BITS or synchronization alarm reported.
Trunk card path alarms (such as AIS-P, LOP-P, or UNEQ-P)	CTC displays all circuits traversing the trunk card.
OC-N card EQPT alarms (such as IMPROPRMVL)	CTC displays no circuits.
I/O card facility, line, and path alarms (such as LPBKFACILITY, RFI-L, and PLM-P)	CTC displays only the affected circuit.

- Step 4** If you want to search for particular circuits, see the [“DLP-A131 Search for Circuits” task on page 11-6](#).
Stop. You have completed this procedure.

NTP-A70 View Alarm Counts on the LCD for a Node, Slot, or Port

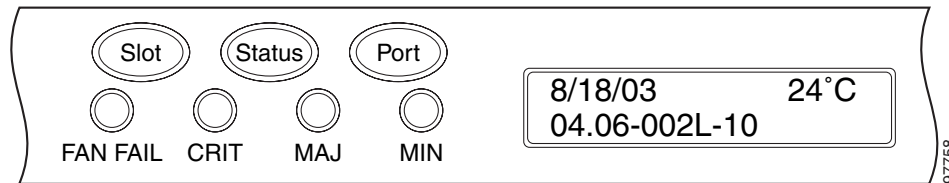
Purpose	This procedure shows how many alarms have occurred on a node, slot, or port without using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

- Step 1** If you want to view the entire alarm summary for the node, press either the **Slot** button or **Port** button on the LCD panel until “Node” appears on the LCD. You will also see the direction, “Status=Alm Ct.” This means that if you press the Status button at this time, as directed in [Step 2](#), you will see an alarm count for the node.
- Step 2** Press the **Status** button. You will see a message similar to, “Alm CT: 2: MJ:2 MN:2,” meaning there are two critical alarms, two major alarms, and two minor alarms.
- Step 3** If you want to see alarm counts for a particular slot, such as the alarms for an OC-3 card in slot 2, press the **Slot** button until you see “Slot-3” on the LCD. You will also see the direction, “Status=Alm Ct.”
- Step 4** Press the **Status** button to see a summary of alarms and severities against the slot. For example, you might see, “Slot-3 Alm CT:0 MJ:1 MN:2,” meaning there are no critical alarms against the slot; there is one major alarm, and there are two minor alarms against it.
- Step 5** If you want to view the alarms against a port on the card, such as Port 3 of the OC-3 card you viewed previously, press Port until you see “Port-3 Status=Alm Ct.”

- Step 6** Press **Status** to view alarm count against the port. You will see a message similar to, “Port-3 Alm CT:0 MJ:1 MN:0.” This means that there is one major alarm against this port.

Figure 9-8 shows the shelf LCD panel.

Figure 9-8 Shelf LCD Panel



To return to the previous view from the Port screen, continue to press **Port** until the display cycles through all the ports on the slot. For instance, on the OC-3 card, press Port until it cycles past Slot 4 and you see “Slot.”

To return to the node menu from the Slot screen, press **Slot** until you cycle through all the slots and see “Node.”

If you do not press any buttons, the LCD will return to its default display with the node name. However, if you did not cycle through the options to return to the node status, you will see the slot or port where you last checked status.



Note A blank LCD results when the fuse on the AIP board has blown. If this occurs, log into <http://www.cisco.com/tac> for more information or log into <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> to obtain a directory of Cisco TAC toll-free numbers for your country.

Stop. You have completed this procedure.

NTP-A71 Create, Download, and Assign Alarm Severity Profiles

Purpose	This procedure creates a customized alarm profile at the network, node, or card level; assigns custom severities individually to port, card, or node, and deletes alarm profiles.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** Complete the “[DLP-A60 Log into CTC](#)” task on page 3-24 at the node where you want to create an alarm profile. If you are already logged in, continue with [Step 2](#) to create, clone or modify an alarm profile, or go to [Step 3](#) to download an alarm profile.

- Step 2** Complete the “[DLP-A518 Create a New or Cloned Alarm Severity Profile](#)” task on page 9-18. This task clones a current alarm profile, renames the profile, and customizes the new profile.
- Step 3** Complete the “[DLP-A524 Download an Alarm Severity Profile](#)” task on page 9-22. This task downloads an alarm severity profile from a CD or a node.



Note After storing a created or downloaded alarm profile, you must go to the node (either by logging into it or clicking on it from the network view) and activate the profile by applying it to the shelf, one or more cards, or one or more ports.

- Step 4** As necessary, complete the “[DLP-A519 Apply Alarm Profiles to Ports](#)” task on page 9-24 or the “[DLP-A117 Apply Alarm Profiles to Cards and Nodes](#)” task on page 9-26.

Stop. You have completed this procedure.

DLP-A518 Create a New or Cloned Alarm Severity Profile

Purpose	This task creates a custom severity profile or clones and modifies the default severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC , page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs. [Figure 9-8 on page 9-19](#) shows the network view.
- Step 2** To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs. The node view is shown in [Figure 9-3 on page 9-6](#).
- Step 3** To access the profile editor from a card view, click the following tabs:
- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports (“Ether alarming”) or packet over SONET (“POS alarming”). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
 - If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profile Editor** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.

- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 If you want to create a new profile based upon the default profile in use, click **New**. Then go to [Step 10](#).

Step 5 If you want to create a profile using an existing profile located on the node, click **Load** and **From Node** in the Load Profile(s) dialog box.

- Click the node name you are logged into in the Node Names list.
- Click the name of an existing profile in the Profile Names list, such as **Default**. Then go to [Step 7](#).

Step 6 If you want to create a profile using an existing profile located in a file that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

- Click **Browse**.
- Navigate to the file location in the **Open** dialog box.
- Click **Open**.



Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in GR-253-CORE.



Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The alarm severity profile appears in the Alarm Profiles window.



Note The alarm profile list contains a master list of alarms that is used for a mixed node network. Some of these alarms may not be used in all ONS nodes.

Step 8 Right-click anywhere in the profile column to view the profile editing shortcut menu. (Refer to [Step 12](#) for further information about the Default profile.)

Step 9 Click **Clone** in the shortcut menu.



Tip To see the full list of profiles, including those available for loading or cloning, click Available. You must load a profile before you can clone it.

Step 10 In the New Profile or Clone Profile dialog box, enter a name in the New Profile Name field. Profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name. Long file names are supported.

Step 11 Click **OK**.

A new alarm profile (named in [Step 10](#)) is created. This profile duplicates the default profile severities and appears at the right of the previous profile column in the Alarm Profiles window. You can select it and drag it to a different position.



Note Up to 10 profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.

The Default profile sets severities to standard Telcordia GR-253-CORE settings. If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm's severity at the higher level. For example, if you choose the Inherited profile from the network view, the severities at the lower levels (node, card and port) will be copied from this selection. A card with an Inherited alarm profile copies the severities used by the node that contains the card. (If you are creating profiles, you can apply these separately at any level. To do this, refer to the “[DLP-A117 Apply Alarm Profiles to Cards and Nodes](#)” task on page 9-26.)

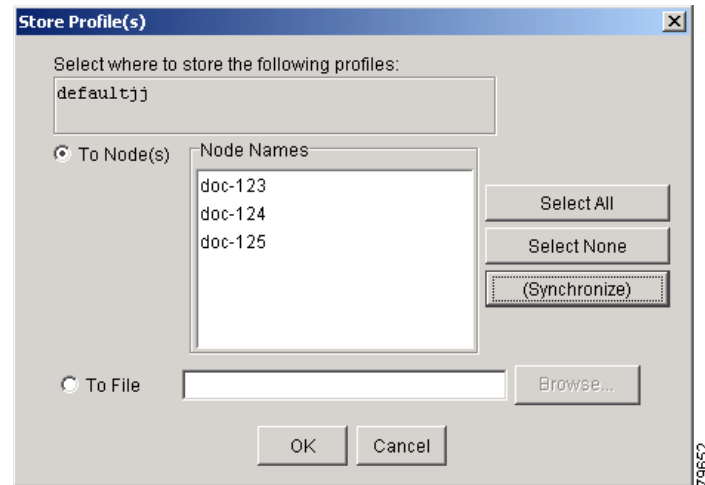
Step 12 Modify (customize) the new alarm profile:

- a. In the new alarm profile column, click the alarm severity you want to change in the custom profile.
- b. Choose a severity from the drop-down menu.
- c. Repeat Steps [a](#) and [b](#) for each severity you want to customize. Refer to the following guidelines when you view the alarms or conditions after making modifications:
 - All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
 - Default severities are used for all alarms and conditions until you create and apply a new profile.
 - Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.

Step 13 After you have customized the new alarm profile, right-click the profile column to highlight it.

Step 14 Click **Store**.

Step 15 In the Store Profile(s) dialog box, click **To Node(s)** and go to Step [a](#) or click **To File** and go to Step [b](#) ([Figure 9-9](#)).

Figure 9-9 Store Profiles Dialog Box

- a. Choose the node(s) where you want to save the profile:
 - If you want to save the profile to only one node, click the node in the Node Names list.
 - If you want to save the profile to all nodes, click **Select All**.
 - If you do not want to save the profile to any nodes, click **Select None**.
 - If you want to update alarm profile information, click **(Synchronize)**.
- b. Save the profile:
 - Click **Browse** and navigate to the profile save location.
 - Enter a name in the File name field.
 - Click **Select** to choose this name and location.



Note Long file names are supported. CTC supplies a suffix of *.pfl to stored files.

- Click **OK** to store the profile.



Note Click the Hide Identical Rows check box to configure the Alarm Profiles window to view rows with dissimilar severities.



Note Click the **Hide Reference Values** check box to configure the Alarm Profiles window to view severities that do not match the Default profile.



Note Click the Only show service-affecting severities check box to configure the Alarm Profiles window not to display Minor and some Major alarms that will not affect service.

Step 16 Return to your originating procedure (NTP).

DLP-A524 Download an Alarm Severity Profile

Purpose	This task downloads a custom alarm severity profile from a network-drive accessible CD-ROM, floppy disk, or hard disk location.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.
- Step 2** To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- Step 3** To access the profile editor from a card view, click the following tabs:
- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports (“Ether alarming”) or packet over SONET (“POS alarming”). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
 - If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profile Editor** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click **Load**.

Step 5 If you want to download a profile that exists on the node, click **From Node** in the Load Profile(s) dialog box.

- a. Click the node name you are logged into in the Node Names list.
- b. Click the name of the profile in the Profile Names list, such as **Default**.

Step 6 If you want to download a profile that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

- a. Click **Browse**.
- b. Navigate to the file location in the **Open** dialog box.
- c. Click **Open**.



Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in GR-253-CORE.



Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The downloaded profile appears at the right side of the Alarm Profiles window.

Step 8 Right-click anywhere in the downloaded profile column to view the profile editing shortcut menu.

Step 9 Click **Store**.

Step 10 In the Store Profile(s) dialog box, click **To Node(s)**.

- a. Choose the node(s) where you want to save the profile:
 - If you want to save the profile to only one node, click the node in the Node Names list.
 - If you want to save the profile to all nodes, click **Select All**.
 - If you do not want to save the profile to any nodes, click **Select None**.
 - If you want to update alarm profile information, click **Synchronize**.
- b. Click **OK**.

Step 11 Return to your originating procedure (NTP).

DLP-A519 Apply Alarm Profiles to Ports

Purpose	This task applies a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile, page 9-18 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click a card to open the card view.



Note You can also apply alarm profiles to cards using the “[DLP-A117 Apply Alarm Profiles to Cards and Nodes](#)” task on page 9-26.



Note The card view is not available for the TCC2 or cross-connect cards.

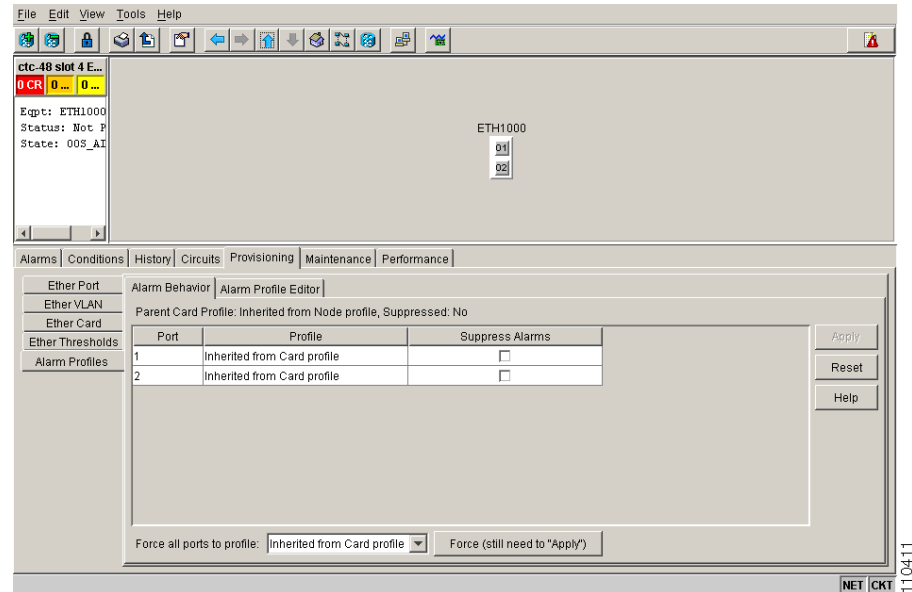
Step 2 Depending on which card you want to apply the profile to, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profiles** tabs or the **Provisioning > POS Alarming > Alarm Profiles** tabs, depending on whether you want to apply the profile to the front physical ports (“Ether alarming”) or packet over SONET (“POS alarming”). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profiles** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.

- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Figure 9-10 shows the alarm profile of Ethernet card ports. CTC shows Parent Card Profile: Inherited.

Figure 9-10 E1000-4 Card Alarm Profile



Go to [Step 3](#) to apply profiles to a port. Go to [Step 4](#) to apply profiles to all ports on a card.

Step 3 To apply profiles on a port basis:

- In card view, click the port row in the Profile column.
- Choose the new profile from the drop-down list.
- Click **Apply**.

Step 4 To apply profiles to all ports on a card:

- In card view, click the **Force all ports to profile** menu arrow at the bottom of the window.
- Choose the new profile from the drop-down list.
- Click **Force (still need to “Apply”)**.
- Click **Apply**.

In node view the Port Level Profiles column indicates port-level profiles with a notation such as “exist (1)” ([Figure 9-11 on page 9-26](#)).

Step 5 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 6 Return to your originating procedure (NTP).

DLP-A117 Apply Alarm Profiles to Cards and Nodes

Purpose	This task applies a custom or default alarm profile to cards or nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile, page 9-18 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tab ([Figure 9-11](#)).

Figure 9-11 Node View Alarm Profile

- Step 2** To apply profiles to a card:
- Click the Profile row for the card.
 - Choose the new profile from the drop-down list.
 - Click **Apply**.
- Step 3** To apply the profile to an entire node:
- Click the **Node Profile** menu arrow at the bottom of the window ([Figure 9-11](#)).
 - Choose the new alarm profile from the drop-down menu.
 - Click **Apply**.
- Step 4** To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 5 Return to your originating procedure (NTP).

DLP-A520 Delete Alarm Severity Profiles

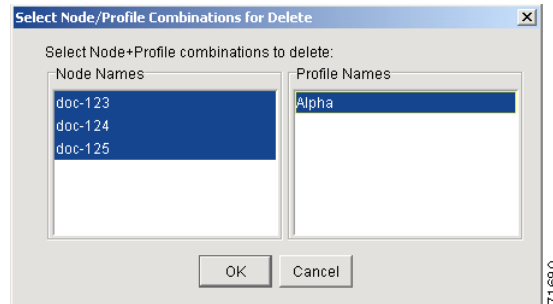
Purpose	This task deletes a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.
- Step 2** To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- Step 3** To access the profile editor from a card view, click the following tabs:
- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports (“Ether alarming”) or packet over SONET (“POS alarming”). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
 - If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profile Editor** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
 - If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- Step 4** Click the profile you are deleting to select it.

Step 5 Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears ([Figure 9-12](#)).

Figure 9-12 Select Node/Profile Combination For Delete Dialog Box



Note You cannot delete the Inherited or Default alarm profiles.



Note A previously created alarm profile cannot be deleted unless it has been stored on the node. If the profile is visible on the Alarm Profiles tab but is not listed in the Select Node/Profile Combinations to Delete dialog box, continue with [Step 9](#).

Step 6 Click the node name(s) in the Node Names list to highlight the profile location.

Tip If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

Step 7 Click the profile name(s) you want to delete in the Profile Names list.**Step 8** Click **OK**.

Click **Yes** in the Delete Alarm Profile dialog box.



Note If you delete a profile from a node, it still appears in the network view Provisioning > Alarm Profile Editor window unless you remove it using the following step.

Step 9 To remove the alarm profile from the window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

Note If a node and profile combination is selected but does not exist, a warning appears: “One or more of the profile(s) selected do not exist on one or more of the node(s) selected.” For example, if node A has only profile 1 stored and the user tries to delete both profile 1 and profile 2 from node A, this warning appears. However, the operation still removes profile 1 from node A.

**Note**

The Default and Inherited special profiles cannot be deleted and do not appear in the Select Node/Profile Combination for Delete Window.

Step 10 Return to your originating procedure (NTP).

NTP-A168 Enable, Modify, or Disable Alarm Severity Filtering

Purpose	This procedure starts, changes, or stops alarm filtering for one or more severities in the Alarms, Conditions, and History windows in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

- Step 1** Complete the [“DLP-A60 Log into CTC” task on page 3-24](#) at the node where you want to enable alarm severity filtering. If you are already logged in, continue with [Step 2](#).
- Step 2** As necessary, complete the [“DLP-A225 Enable Alarm Filtering” task on page 9-29](#). This task enables alarm filtering at the card, node, and network views for all nodes in the network. Alarm filtering can be enabled for alarms, conditions, or events.
- Step 3** As necessary, complete the [“DLP-A521 Modify Alarm, Condition, and History Filtering Parameters” task on page 9-30](#) to modify the alarm filtering for network nodes to show or hide particular alarms or conditions.
- Step 4** As necessary, complete the [“DLP-A227 Disable Alarm Filtering” task on page 9-32](#) to disable alarm profile filtering for all network nodes.
- Stop. You have completed this procedure.**

DLP-A225 Enable Alarm Filtering

Purpose	This task enables alarm filtering for alarms, conditions, or event history in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

-
- Step 1** At the node, network, or card view, click the **Alarms** tab.
- Step 2** Click the **Filter** tool at the lower-right side of the bottom toolbar.
- Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).
- Alarm filtering will be enabled in the card, node, and network views of the Alarms tab at the node and for all other nodes in the network. If, for example, the Alarm Filter tool is enabled in the Alarms tab of the node view at one node, the Alarms tab in the network view and card view of that node will also show the tool enabled. All other nodes in the network will also have the tool enabled.
- If you filter an alarm in card view, the alarm will still be displayed in node view. In this view, the card will display the color of the highest-level alarm. The alarm is also shown for the node in the network view.
- Step 3** If you want alarm filtering enabled when you view conditions, repeat Steps 1 and 2 using the Conditions window.
- Step 4** If you want alarm filtering enabled when you view alarm history, repeat Steps 1 and 2 using the History window.
- Step 5** Return to your originating procedure (NTP).
-

DLP-A521 Modify Alarm, Condition, and History Filtering Parameters

Purpose	This task changes alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering, page 9-29 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

-
- Step 1** At the node, network, or card view, click the **Alarms** tab, Conditions tab, or History tab.
- Step 2** Click the **Filter** button at the lower-left of the bottom toolbar.
- The filter dialog box appears, displaying the General tab. [Figure 9-13](#) shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 9-13 Alarm Filter Dialog Box General Tab

In the General tab Show Severity box, you can choose which alarm severities will show through the alarm filter and provision a time period during which filtered alarms show through the filter. To change the alarm severities shown in the filter, go to [Step 3](#). To change the time period filter for the alarms go to [Step 4](#).

- Step 3** In the Show Severity area, click the check boxes for the severities [Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA)] you want to be reported at the network level. Leave severity check boxes deselected (unchecked) to prevent those severities from appearing.

When alarm filtering is disabled, all alarms show.

- Step 4** In the Time area, click the **Show alarms between time limits** check box to enable it. Click the up and down arrows in the From Date, To Date, and Time fields to modify what period of alarms are shown.
- To modify filter parameters for conditions, continue with [Step 5](#). If you do not need to modify them, continue with [Step 6](#).

- Step 5** Click the filter dialog box **Conditions** tab ([Figure 9-14](#)).

Figure 9-14 Alarm Filter Dialog Box Conditions Tab

When filtering is enabled, conditions in the Show list are visible and conditions in the Hide list are invisible.

- To move conditions individually from the Show list to the Hide list, click the > button.
- To move conditions individually from the Hide list to the Show list, click the < button.
- To move conditions collectively from the Show list to the Hide list, click the >> button.
- To move conditions collectively from the Hide list to the Show list, click the << button.



Note Conditions include alarms.

Step 6 Click **Apply** and **OK**.

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the “[DLP-A225 Enable Alarm Filtering](#)” task on page 9-29), and are not enforced when alarm filtering is disabled (see the “[DLP-A227 Disable Alarm Filtering](#)” task on page 9-32).

Step 7 Return to your originating procedure (NTP).

DLP-A227 Disable Alarm Filtering

Purpose	This task turns off specialized alarm filtering in all network nodes so that all severities are reported in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering , page 9-29 DLP-A60 Log into CTC , page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is indented and disabled if the tool is raised (not selected).

Step 3 If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and click the Filter tool.

Step 4 If you want alarm filtering disabled when you view alarm history, click the **History** tab and click the Filter tool.

Step 5 Return to your originating procedure (NTP).

NTP-A72 Suppress Alarms or Discontinue Alarm Suppression

Purpose	This procedure prevents alarms from being reported for a port, card, or node in circumstances when an alarm or condition is known to exist but you do not want to include it in the display. This procedure also resumes normal alarm reporting by discontinuing the suppression.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Complete the [“DLP-A60 Log into CTC” task on page 3-24](#). If you are already logged in, continue with [Step 2](#).

Step 2 Complete the [“DLP-A522 Suppress Alarm Reporting” task on page 9-33](#) to enable the node to send autonomous messages that clear specific raised alarms and cause suppressed alarms to appear in the Conditions window.



Note Suppressing one or more alarms prevents them from appearing in Alarm or History windows or in any other clients. The suppress command causes CTC to display them in the Conditions window with their severity, their severity color code, and service-affecting status.

Step 3 Complete the [“DLP-A523 Discontinue Alarm Suppression” task on page 9-35](#) to discontinue alarm suppression and resume normal alarm reporting.

Stop. You have completed this procedure.

DLP-A522 Suppress Alarm Reporting

Purpose	This task suppresses the reporting of ONS 15454 alarms at the node, card, or port level.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning



Caution

If multiple CTC/TL1 sessions are open, suppressing alarms in one session suppresses the alarms in all other open sessions.

**Note**

Alarm suppression at the node level does not supersede alarm suppression at the card or port level. Suppression can exist independently for all three entities, and each entity will raise separate alarms suppressed by the user command (AS-CMD) alarm.

Step 1 If you are in node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Step 2 To suppress alarms for the entire node:

- a. Check the **Suppress Alarms** check box.
- b. Click **Apply**.

All raised alarms for the node will change color to white in the Alarms window and their status will change to cleared. After suppressing alarms, clicking **Synchronize** in the Alarms window will remove cleared alarms from the window. However, an AS-CMD alarm will show in node or card view to indicate that node-level alarms were suppressed; this alarm will show System in the Object column.

**Note**

The only way to suppress BITS, power source, or system alarms is to suppress alarms for the entire node. These cannot be suppressed separately, but the shelf backplane can be.

Step 3 To suppress alarms for individual cards:

- a. Locate the card row (using the Location column for the slot number or the Eqpt Type column for the equipment name).
- b. Check the **Suppress Alarms column** check box on that row ([Figure 9-11 on page 9-26](#)).

Alarms that directly apply to this card will change appearance as described in [Step 2](#). For example, if you suppressed raised alarms for an OC-48 card in Slot 16, raised alarms for this card will change in node or card view. The AS-CMD alarm will show the slot number in the Object number. For example, if you suppressed alarms for a Slot 16 OC-48 card, the AS-CMD object will be “SLOT-16.”

Click **Apply**.

Step 4 To suppress alarms for individual card ports double-click the card in node view.

Step 5 Depending on which card ports you want to suppress alarm reporting on, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profiles** tabs or the **Provisioning > POS Alarming > Alarm Profiles** tabs, depending on whether you want to apply the profile to the front physical ports (“Ether alarming”) or packet over SONET (“POS alarming”). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profiles** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.

- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Step 6 Check the **Suppress Alarms** column check box for the port row where you want to suppress alarms (Figure 9-10 on page 9-25).

Step 7 Click **Apply**.

Alarms that apply directly to this port will change appearance as described in [Step 2](#). (However, alarms raised on the entire card will remain raised.) A raised AS-CMD alarm that shows the port as its object will appear in either alarm window. For example, if you suppressed alarms for Port 1 on the Slot 16 OC-48 card, the alarm object will show “FAC-16-1.”

Step 8 Return to your originating procedure (NTP).

DLP-A523 Discontinue Alarm Suppression

Purpose	This task discontinues alarm suppression and reenables alarm reporting on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A522 Suppress Alarm Reporting, page 9-33 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning



Caution

If multiple CTC sessions are open, discontinuing suppression in one session will discontinue suppression in all other open sessions.

Step 1 To discontinue alarm suppression for the entire node:

- In node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tab.
- Uncheck the **Suppress Alarms** check box.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the System object will be cleared in all views.

Step 2 To discontinue alarm suppression for individual cards:

- In the node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- Locate the card that was suppressed in the slot list.

- c. Uncheck the Suppress Alarms column check box for that slot.
- d. Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the slot object (for example, SLOT-16) will be cleared in all views.

Step 3 To discontinue alarm suppression for ports, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profiles** tabs or the **Provisioning > POS Alarming > Alarm Profiles** tabs, depending on whether you want to apply the profile to the front physical ports (“Ether alarming”) or packet over SONET (“POS alarming”). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profiles** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Step 4 Uncheck the **Suppress Alarms** check box for the port(s) you no longer want to suppress.

Step 5 Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the port object (for example, FAC-16-1) will be cleared in all views.

Step 6 Return to your originating procedure (NTP).

NTP-A32 Provision External Alarms and Controls on the Alarm Interface Controller

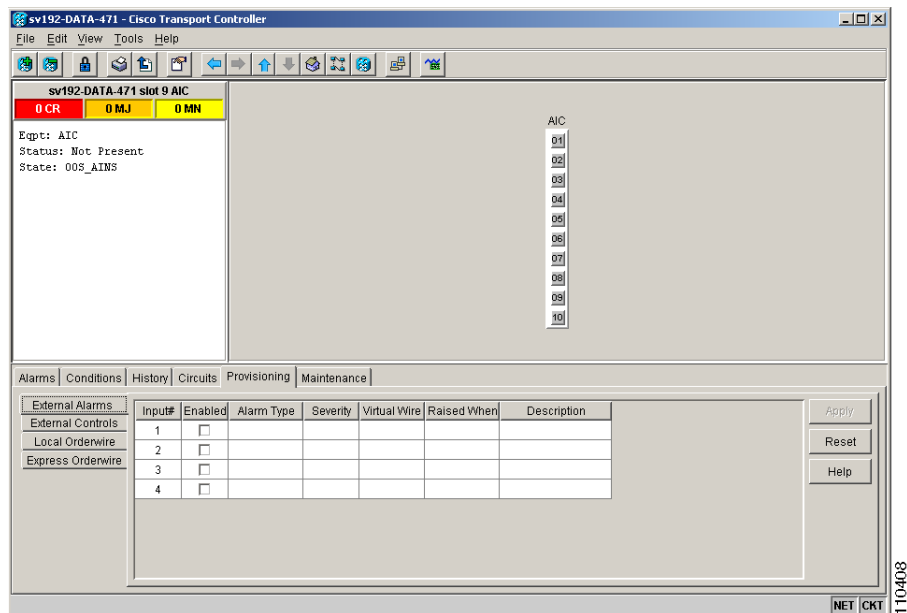
Purpose	This procedure creates external (environmental) alarms and external controls for the Alarm Interface Controller (AIC) card.
Tools/Equipment	An AIC card must be installed in Slot 9.
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher


Note

For information about the AIC external alarms and controls, virtual wire, and orderwire, refer to the *Cisco ONS 15454 Reference Manual*.

- Step 1** Verify the backplane wiring. See the “[NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections](#)” procedure on page 1-37 for information about the ONS 15454 backplane pins.
- For external alarms, verify that the external-device relays are wired to the ENVIR ALARMS IN backplane pins.
 - For external controls, verify that the external relays are wired to the ENVIR ALARMS OUT backplane pins.
- Step 2** In the node view, double-click the AIC card on the shelf graphic. The card view appears.
- Step 3** If you are provisioning external alarms, click the **Provisioning > External Alarms** tab ([Figure 9-15](#)). If you are not provisioning external alarms, skip Steps 4 through 6 and go to [Step 7](#).

Figure 9-15 AIC Card External Alarms



Step 4 Complete the following fields for each external device wired to the ONS 15454 backplane:

- **Enabled**—Check the check box to activate the fields for the alarm input number.
- **Alarm Type**—Choose an alarm type from the drop-down list.
- **Severity**—Click a severity in the drop-down list.

The severity you choose determines the external alarm's severity in the Alarms and History tabs and determines whether the LEDs are activated. Critical (CR), Major (MJ), and Minor (MN) alarms activate the LEDs. Not-Alarmed (NA) and Not-Reported (NR) do not activate LEDs, but do report the information in CTC.

- **Virtual Wire**—Choose the virtual wire number in the drop-down list to assign the external device to a virtual wire. Otherwise, do not change the None default. For information about the AIC virtual wire, see the *Cisco ONS 15454 Reference Manual*.
- **Raised When**—From the drop-down list, choose the contact condition (open or closed) that triggers the alarm.
- **Description**—A default description is provided; enter a different description if needed.

Step 5 To provision up to four virtual wire inputs for external devices, complete [Step 4](#) for each additional device.

Step 6 Click **Apply**.

Step 7 If you are provisioning external control outputs for external devices, click the **External Controls** subtab.

Step 8 Complete the following options for each external control wired to the ONS 15454 backplane:

- **Enabled**—Check this check box to activate the fields for the alarm input number.
- **Control Type**—Choose the control type from the drop-down list: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- **Trigger Type**—Choose a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.
- **Description**—Enter a description.

Step 9 To provision additional external controls, complete [Steps 7](#) and [8](#) for each additional device.

Step 10 Click **Apply**.



Note If you provision an external alarm to raise upon an open contact before you physically connect to the ONS equipment, the alarm will raise until you do create the physical connection.



Note When you provision an external alarm, the alarm object is ENV-IN-nn. The variable nn refers to the external alarm's number, regardless of the name you assign.



Note Environmental alarms that you create (and name) should be recorded locally for the NE. Both the Alarm name and resolution are node-specific.

Stop. You have completed this procedure.

NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International

Purpose	This procedure creates external (environmental) alarms and external controls for the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9.
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Note

The AIC-I card alarm provides direct alarm contacts (external alarm inputs and external control outputs) routed through the backplane to wire-wrap pins accessible from the back of the shelf. If you install an Alarm Expansion Panel (AEP), the AIC-I alarm contacts cannot be used. Only the alarm expansion panel (AEP) alarm contacts can be used. For further information about the AEP, see [“NTP-A119 Install the Alarm Expansion Panel” procedure on page 1-34](#) and the [“NTP-A120 Install an External Wire-Wrap Panel to the AEP” procedure on page 1-44](#).

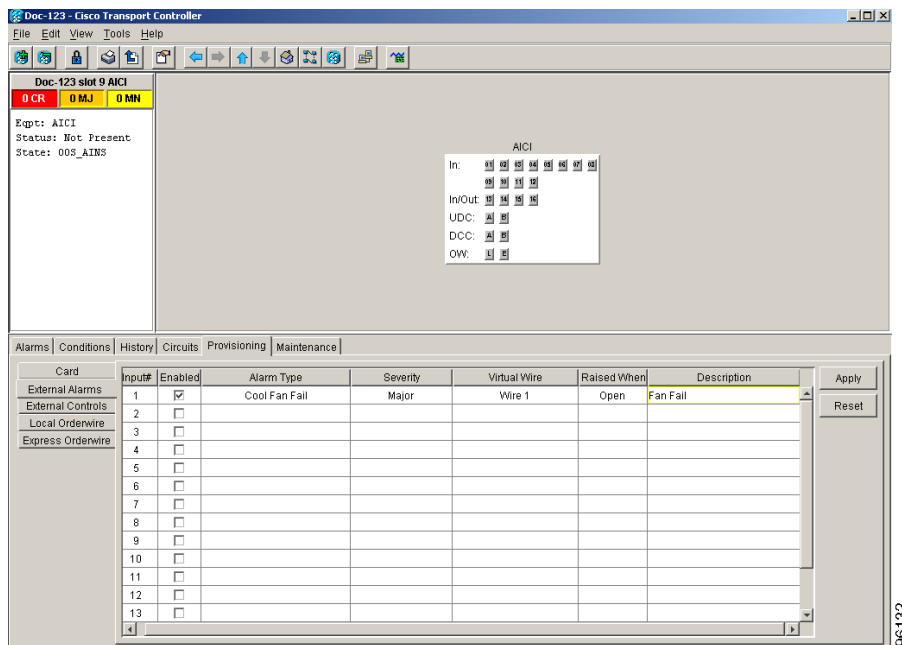


Note

For information about the AIC-I alarms, controls, and virtual wire, refer to the *Cisco ONS 15454 Reference Manual*.

- Step 1** Verify the backplane wiring. If you are using the AEP, see the [“NTP-A119 Install the Alarm Expansion Panel” procedure on page 1-34](#). Otherwise, see the [“NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections” procedure on page 1-37](#) for information about the ONS 15454 backplane pins.
 - a. For external alarms, verify that the external device relays are wired to the ENVIR ALARMS IN backplane pins.
 - b. For external controls, verify that the external device relays are wired to the ENVIR ALARMS OUT backplane pins.
- Step 2** In the node view, double-click the AIC-I card on the shelf graphic. The card view appears.
- Step 3** Click the **Provisioning > Card** tabs.
- Step 4** In the Alarm Contacts area, click the Add Extension radio button if you are using the AEP. Clicking this option will choose the External Alarm input/output type and the AEP extension type; it will give you access to 16 external alarm contacts.
- Step 5** If you did not click Add Extension, in the Input/Output area, choose either External Alarm or External Control. (External Alarm will limit your input/output options as explained in [Step 4](#).) Choosing External Control will enable both external alarms and external controls. This will convert four of the external alarm contacts to external controls, leaving 12 available external control contacts. The extension type for both options is AEP.
- Step 6** Click **Apply**.
- Step 7** If you are provisioning external alarms, click the **External Alarms** tab ([Figure 9-16](#)). If you are not provisioning external alarms, skip Steps [8](#) through [10](#) and go to [Step 11](#).

Figure 9-16 Provisioning External Alarms On The AIC-I Card



Step 8 For external alarms, complete the following fields:

- **Enabled**—Check the check box to activate the fields for the alarm input number.
- **Alarm Type**—Choose an alarm type from the drop-down list.
- **Severity**—Click a severity from the drop-down list.

The severity determines the alarm's severity in the Alarms and History tabs and determines whether the LEDs are activated. Critical (CR), Major (MJ), and Minor (MN) alarms activate the LEDs. Not-Alarmed (NA) and Not-Reported (NR) do not activate LEDs, but do report the information in CTC.

- **Virtual Wire**—Choose the virtual wire number from the drop-down list to assign the external device to a virtual wire. Otherwise, do not change the None default. For information about the AIC-I virtual wire, see the *Cisco ONS 15454 Reference Manual*.
- **Raised When**—From the drop-down, choose the contact condition (open or closed) that triggers the alarm.
- **Description**—A default description is provided; enter a different description if needed.

Step 9 To provision additional devices, complete [Step 8](#) for each additional device.

Step 10 Click **Apply**.

Step 11 For external controls, click the **External Controls** tab and complete the following fields for each control wired to the ONS 15454 backplane:

- **Enabled**—Check this check box to activate the fields for the alarm input number.
- **Control Type**—Choose the control type from the drop-down list: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- **Trigger Type**—Choose a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.
- **Description**—Enter a description.

Step 12 To provision additional external controls, complete [Step 11](#) for each device.

Step 13 Click **Apply**.



Note When you provision an external alarm, the alarm object is ENV-IN-nn. The variable nn refers to the external alarm's number, regardless of the name you assign.



Note Environmental alarms that you create (and name) should be recorded locally for the NE. Both the Alarm name and resolution are node-specific.

Stop. You have completed this procedure.
