Change Node Settings

This chapter explains how to modify node provisioning for the Cisco ONS 15454. To provision a new node, see Chapter 4, "Turn Up Node." To change default network element settings and to view a list of those settings, refer to the *Cisco ONS 15454 Release 4.6 Network Element Defaults* document.

> **Note** The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

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

1. NTP-A81 Change Node Management Information, page 12-2—Complete this procedure as needed to change node name, contact information, latitude, longitude, date, time, and login legal disclaimer.
2. NTP-A201 Change CTC Network Access, page 12-4—Complete this procedure as needed to change the IP address, default router, subnet mask, network configuration settings, and static routes.
3. NTP-A226 Modify DWDM Node Settings, page 12-7—Complete as needed.
4. NTP-A202 Customize the CTC Network View, page 12-10—As needed, complete this procedure to create domains and customize the appearance of the network map, including specifying a different default map, creating domains, selecting your own map or image, and changing the background color.
5. NTP-A203 Modify or Delete Card Protection Settings, page 12-15—Complete as needed.
6. NTP-A255 Delete Communications Channel Terminations, page 12-20—Complete this procedure as needed to delete DCC, LDCC, GCC, and DWDM OSC terminations.
7. NTP-A85 Change Node Timing, page 12-23—Complete as needed.
8. NTP-A205 Modify Users and Change Security, page 12-25—Complete this procedure as needed to make changes to user settings, including security level and security policies, and to delete users.
9. NTP-A87 Change SNMP Settings, page 12-33—Complete as needed.

NTP-A81 Change Node Management Information

Purpose	This procedure changes the node name, date, time, contact information, or the login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-7
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. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 In the node view, click the **Provisioning > General** tabs.

Step 4 Complete the "DLP-A140 Change the Node Name, Date, Time, and Contact Information" task on page 12-2, as needed.

Step 5 Complete the "DLP-A265 Change the Login Legal Disclaimer" task on page 12-3, as needed.

Step 6 After confirming the changes, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A140 Change the Node Name, Date, Time, and Contact Information

Purpose	This procedure changes basic information such as node name, date, time, and contact information.
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

Note Changing the date, time, or time zone might invalidate the node's performance monitoring counters.

Step 1 In node view, click the **Provisioning > General** tabs.

Step 2 Change any of the following:

- General: Node Name
- General: Contact
- Location: Latitude
- Location: Longitude

- Location: Description

Note To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click Reset Node Position.

- Time: Use NTP/SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time
- AIS-V Insertion On STS-1 Signal Degrade - Path: Insert AIS-V on STS-1 SD-P
- AIS-V Insertion On STS-1 Signal Degrade - Path: SD-P BER

See the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-7 for detailed field descriptions.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-A265 Change the Login Legal Disclaimer

Purpose	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
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	Superuser

Step 1 In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.

Step 2 The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. Use the following HTML commands to format the text, as needed:

- <b> Begins boldface font
- </b> Ends boldface font
- <center> Aligns type in the center of the window
- </center> Ends the center alignment
- <font=n, where n = point size> Changes the font to the new size
- </font> Ends the font size command
- <p> Creates a line break

- <sub> Begins subscript
- </sub> Ends subscript
- <sup> Begins superscript
- </sup> Ends superscript
- <u> Starts underline
- </u> Ends underline

Step 3 If you want to preview your changed statement and formatting, click the **Preview** subtab.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A201 Change CTC Network Access

Purpose	This procedure changes essential network information, including IP settings, static routes, and OSPF options.
Tools/Equipment	None
Prerequisite Procedures	NTP-A169 Set Up CTC Network Access, page 4-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional ONS 15454 networking information and procedures, including IP addressing examples, static route scenarios, Open Shortest Path First (OSPF) protocol, and routing information protocol options are provided in the IP Networking section of the *Cisco ONS 15454 Reference Manual*.

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 "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A266 Change IP Settings, page 12-5
- DLP-A142 Modify a Static Route, page 12-6
- DLP-A143 Delete a Static Route, page 12-6
- DLP-A144 Disable OSPF, page 12-7
- DLP-A250 Set Up or Change Open Shortest Path First Protocol, page 4-16

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A266 Change IP Settings

Purpose	This task changes the IP address, subnet mask, default router, DHCP access, firewall IIOP listener port, LCD IP display, and proxy server settings.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 DLP-A249 Provision IP Settings, page 4-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

⚠ **Caution** Changing the node IP address, subnet mask, or IIOP listener port causes the TCC2s to reboot. If Ethernet circuits using spanning tree protocol originate or terminate on E Series Ethernet cards installed in the node, circuit traffic will be lost for several minutes while the spanning trees reconverge. Other circuits are not affected by TCC2 reboots.

Step 1 In node view, click the **Provisioning** > **Network > General** tabs.

Step 2 Change any of the following:

- IP Address
- Suppress CTC IP Display
- LCD IP Setting
- Default Router
- Forward DHCP Request To
- MAC Address
- Net/Subnet Mask Length
- TCC CORBA (IIOP) Listener Port
- Gateway Settings

See the "DLP-A249 Provision IP Settings" task on page 4-10 for detailed field descriptions.

Step 3 Click **Apply**.

If you changed a network field that will cause the node to reboot, such as the IP address, subnet mask or TCC CORBA Listener Port, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS 15454 TCC2 cards will reboot, one at a time. A TCC2 card reboot causes a temporary loss of connectivity to the node, but traffic is unaffected.

Step 5 Confirm that the changes appear on the Provisioning > Network > General tab. If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

Step 6 Return to your originating procedure (NTP).

DLP-A142 Modify a Static Route

Purpose	This task modifies a static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 DLP-A65 Create a Static Route, page 4-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab.

Step 3 Click the static route you want to edit.

Step 4 Click **Edit.**

Step 5 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-A65 Create a Static Route" task on page 4-15 for detailed field descriptions.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-A143 Delete a Static Route

Purpose	This task deletes an existing static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 DLP-A65 Create a Static Route, page 4-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.

Step 2 Click the static route you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-A144 Disable OSPF

Purpose	This task disables the Open Shortest Path First (OSPF) routing protocol process for an ONS 15454 LAN.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 DLP-A250 Set Up or Change Open Shortest Path First Protocol, page 4-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **OSPF** tabs. The OSPF subtab has several options.

Step 2 In the OSPF on LAN area, uncheck the **OSPF active on LAN?** check box.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

NTP-A226 Modify DWDM Node Settings

Purpose	This procedure sets the network and node settings and provisions the node power levels on ONS 15454s that are provisioned for DWDM.
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	You must use Cisco MetroPlanner or another DWDM network calculation tool to prepare a configuration file for your network. NTP-A268 Install the DWDM or Hybrid Node Cards, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution DWDM settings are normally not changed at the individual node level. Any change to a DWDM node setting usually requires recalculation of power and attenuation levels at other nodes on the DWDM network. Do not change a DWDM node setting unless you are prepared to modify the settings of other DWDM nodes on the network.

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 Perform one of the following tasks as appropriate:

- DLP-A408 Modify DWDM Hub Node Settings, page 12-8.
- DLP-A409 Modify DWDM Terminal Node Settings, page 12-9.
- DLP-A410 Modify DWDM OADM Node Settings, page 12-9.
- DLP-A411 Modify DWDM Line Node Settings, page 12-10.

Step 3 Click the **Connections** tab, then click **Calculate Connections**.

Step 4 Verify that every connection matches the connections specified by the Cisco MetroPlanner design plan. If a connection is not correct:

a. Delete the connection. See the "DLP-A405 Delete a DWDM Connection" task on page 5-9.

b. Uninstall the fibers from the incorrect slot/unit/port.

c. Connect the fiber to the correct slot/unit/port.

d. Create a new connection. See the "DLP-A406 Create a DWDM Connection" task on page 5-8.

Step 5 Click the **Port Status** tab. Click **Launch ANS**.

ANS (Automatic Node Setup) automatically calculates variable optical attenuators (VOAs) set-points to match the expected channel profile at the amplifier input port.

Stop. **You have completed this procedure**.

DLP-A408 Modify DWDM Hub Node Settings

Purpose	This task modifies the node and network types and sets the channel power levels for a DWDM hub node.
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	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-2 on page 5-16.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A409 Modify DWDM Terminal Node Settings

Purpose	This task provisions the node and network types and power levels for a DWDM terminal node.
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	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-4 on page 5-18.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A410 Modify DWDM OADM Node Settings

Purpose	This task provisions the node and network types and power levels for a DWDM optical add/drop module (OADM) node.
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	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-5 on page 5-19.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A411 Modify DWDM Line Node Settings

Purpose	This task modifies the node and network types for a DWDM line node.
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	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-7 on page 5-22.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

NTP-A202 Customize the CTC Network View

Purpose	This procedure modifies the CTC network view, including grouping nodes into domains for a less-cluttered display, changing the network view background color, and using a custom image for the network view background.
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. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks, as needed:

- DLP-A145 Change the Network View Background Color, page 12-11
- DLP-A528 Change the Default Network View Background Map, page 12-11
- DLP-A268 Apply a Custom Network View Background Map, page 12-12
- DLP-A148 Create Domain Icons, page 12-13
- DLP-A149 Manage Domain Icons, page 12-14
- DLP-A269 Enable Dialog Box Do-Not-Display Option, page 12-15
- DLP-A498 Switch Between TDM and DWDM Network Views, page 12-13

Stop. You have completed this procedure.

DLP-A145 Change the Network View Background Color

Purpose	This task changes the network view background color or the domain view background color (the area displayed when you open a domain).
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 or higher

Note If you modify background colors, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the View menu choose **Go to Network View**.

Step 2 If you want to change a domain background, double-click the domain. If not, continue with Step 3.

Step 3 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 4 In the Choose Color dialog box, select a background color.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-A528 Change the Default Network View Background Map

Purpose	This task changes the default map of the CTC network view.
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	Superuser

Note If you modify the background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu choose **Preferences > Map** and check the **Use Default Map** check box.

Step 2 In the node view, click the **Provisioning > Defaults** tabs.

Step 3 In the Defaults Selector area, choose **CTC** and then **network**.

Step 4 Click the **Default Value** field and choose a default map from the drop-down menu. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 5 Click **Apply**. The new network map appears.

Step 6 Click **OK**.

Step 7 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15454 icons are visible. (You can also choose **Fit Graph to Window**.)

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-A268 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map of the CTC network view.
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 or higher

Note You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you apply a custom background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu choose **Preferences > Map** and uncheck the **Use Default Map** check box

Step 2 From the View menu choose **Go to Network View**.

Step 3 Right-click the network or domain map and choose **Set Background Image**.

Step 4 Click **Browse**. Navigate to the graphic file you want to use as a background.

Step 5 Select the file. Click **Open**.

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

Step 7 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15454 icons are visible.

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-A498 Switch Between TDM and DWDM Network Views

Purpose	Use this task to switch between TDM (Time Division Multiplexing) and DWDM (Dense Wavelength Division Multiplexing) network views. This task applies only to Release 4.6 or later.
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 or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 From the Network Scope drop-down menu on the toolbar, choose one of the following:

- All—displays both TDM and DWDM nodes
- TDM—displays only ONS 15454s with SONET or SDH cards including the transponder and muxponder cards.
- DWDM—displays only ONS 15454s with DWDM cards, including the transponder and muxponder cards.

Step 3 Return to your originating procedure (NTP).

DLP-A148 Create Domain Icons

Purpose	This task creates a domain, which is an icon that groups ONS 15454 icons in CTC network view.
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

Note Domains created by one user are visible to all users who log into the network.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Right-click the network map and choose **Create New Domain** from the shortcut menu.

Step 3 When the domain icon appears on the map, click the map name and type the domain name.

Step 4 Press **Enter**.

Step 5 Return to your originating procedure (NTP).

DLP-A149 Manage Domain Icons

Purpose	This task manages CTC network view domain icons.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24 DLP-A148 Create Domain Icons, page 12-13
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All domain changes, such as added or removed nodes, are visible to all users who log into the network.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Locate the domain action you want in Table 12-1 and complete the appropriate steps.

Table 12-1 Managing Domains

Domain action	Steps
Move a domain	Press Ctrl and drag and drop the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag and drop the node icon to the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Choose **Move Node Back to Parent View**.
Open a domain	• Double-click the domain icon. • Right-click the domain and choose **Open Domain**.
Return to network view	Right-click the domain view area and choose **Go to Parent View** from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select **Show Domain Overview**.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

DLP-A269 Enable Dialog Box Do-Not-Display Option

Purpose	This task ensures that a user-selected “Do not display” dialog box preference is enabled for subsequent sessions or it disables the do not display option.
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

Note If any user who has rights to perform an operation (for example, creating a circuit) selects the “Do not show this dialog again” check box in a dialog box, the dialog box is not displayed for any other users who perform that operation on the network from the same computer unless the command is overridden using the following task. (The preference is stored on the computer, not in the node database.)

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **General** tab.

The Preferences Management area field lists all dialog boxes where “Do not show this dialog again” is enabled.

Step 3 Choose one of the following options, or uncheck the individual dialog boxes that you want to appear:

- **Don’t Show Any**—Hides all do-not-display check boxes.
- **Show All**—Overrides do-not-display check box selections and displays all dialog boxes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

NTP-A203 Modify or Delete Card Protection Settings

Purpose	This procedure modifies and deletes card protection settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-A170 Create Protection Groups, page 4-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Modifying and deleting protection groups can be service affecting.

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 "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A150 Modify a 1:1 Protection Group, page 12-16
- DLP-A152 Modify a 1:N Protection Group, page 12-17
- DLP-A154 Modify a 1+1 Protection Group, page 12-18
- DLP-A270 Modify a Y Cable Protection Group, page 12-18
- DLP-A499 Modify a Splitter Protection Group, page 12-19
- DLP-A155 Delete a Protection Group, page 12-20

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A150 Modify a 1:1 Protection Group

Purpose	This task modifies a 1:1 protection group for electrical (DS-1, DS-3, EC-1, and DS3XM-6) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A71 Create a 1:1 Protection Group, page 4-28 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** > **Protection** tabs.

Step 2 In the Protection Groups area, click the 1:1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—As needed, type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Note To convert electrical protection groups, see the "NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 13-63.

Step 5 Return to your originating procedure (NTP).

DLP-A152 Modify a 1:N Protection Group

Purpose	This task modifies a 1:N protection group for DS-1 and DS-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A72 Create a 1:N Protection Group, page 4-29 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 Verify that the DS-1 and DS-3 cards are installed according to the 1:N specifications in the "DLP-A72 Create a 1:N Protection Group" task on page 4-29.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

Step 3 In the Protection Groups area, click the 1:N protection group you want to modify.

Step 4 In the Selected Group area, change any of the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Available Entities—If cards are available, they will appear here. Use the arrow buttons to move them into the Working Cards column.
- Working Entities—Use the arrow buttons to move cards out of the Working Cards column.
- Reversion Time—Choose a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A72 Create a 1:N Protection Group" task on page 4-29 for field descriptions.

Step 5 Click **Apply**. The changes are applied. Confirm that the changes appear; if not repeat the task.

Note To convert electrical protection groups, see the "NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 13-63.

Step 6 Return to your originating procedure (NTP).

DLP-A154 Modify a 1+1 Protection Group

Purpose	This task modifies a 1+1 protection group for any optical port (OC-3, OC-12, OC-12 IR, OC-48, OC-48AS, and OC-192).
Tools/Equipment	None
Prerequisite Procedures	DLP-A73 Create a 1+1 Protection Group, page 4-30 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** > **Protection** tabs.

Step 2 In the Protection Groups area, click the 1+1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Bidirectional switching—Check or uncheck
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A73 Create a 1+1 Protection Group" task on page 4-30 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear; if not repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A270 Modify a Y Cable Protection Group

Purpose	This task modifies a Y cable protection group for any client port on a MXP_2.5G_10G, TXP_MR_2.5G, or TXP_MR_10G card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A252 Create a Y-Cable Protection Group, page 4-32 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** > **Protection** tabs.

Step 2 In the Protection Groups area, click the Y Cable protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A252 Create a Y-Cable Protection Group" task on page 4-32 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear; if not repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A499 Modify a Splitter Protection Group

Purpose	This task modifies a Splitter protection group for any client port on a TXPP_MR_2.5G card. Splitter protection is automatically created when the TXPP transponder card is installed.
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 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the Splitter protection group that you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A155 Delete a Protection Group

Purpose	This task deletes a 1:1, 1:N, 1+1, or Y Cable protection group.
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 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box. Confirm that the changes appear; if they do not, repeat Steps 1 through 3.

Step 5 Return to your originating procedure (NTP).

NTP-A255 Delete Communications Channel Terminations

Purpose	This procedure deletes a DCC, LDCC, GCC, and DWDM OSC terminations on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A354 Provision SONET DCC Terminations, page 6-4 or DLP-A355 Provision SONET LDCC Terminations, page 6-5 or DLP-A343 Provision GCC Terminations, page 7-4 or DLP-A342 Provision OSC Terminations, page 5-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

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 node view, click the **Provisioning > DCC/GCC/OSC** tabs.

Step 3 As needed, complete the following tasks:

- DLP-A156 Delete a SONET DCC Termination, page 12-21
- DLP-A359 Delete a SONET LDCC Termination, page 12-21

- DLP-A360 Delete a GCC Termination, page 12-22
- DLP-A361 Delete a DWDM OSC Termination, page 12-22

Stop. You have completed this procedure.

DLP-A156 Delete a SONET DCC Termination

Purpose	This task deletes a SONET DCC termination on the ONS 15454.
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 Click the **DCC** tab.

Step 2 Click the DCC termination to be deleted and click **Delete**. The Delete SDCC Termination dialog box appears.

Step 3 Check the **Set Port Out of Service** check box if you want to change the port state to out of service (this may be service affecting).

Step 4 Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A359 Delete a SONET LDCC Termination

Purpose	This task deletes a SONET LDCC termination on the ONS 15454.
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

Caution Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Click the **LDCC** tab.

Step 2 Click the LDCC termination to be deleted and click **Delete**. The Delete LDCC Termination dialog box appears.

Step 3 Check the **Set Port Out of Service** check box if you want to change the port state to out of service (this may be service affecting).

Step 4 Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A360 Delete a GCC Termination

Purpose	This task deletes the DWDM GCC terminations required for network setup when using the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards.
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 Click the **GCC** tab.

Step 2 In the GCC Terminations pane, click **Delete.**

Step 3 In the Delete GCC Terminations dialog box, check **Set port OOS** checkbox if you want to place ports out of service.

Step 4 Click **Yes**. GCC-EOC alarms appear until all network GCC terminations are deleted and the ports are out of service.

Step 5 Return to your originating procedure (NTP).

DLP-A361 Delete a DWDM OSC Termination

Purpose	This task deletes a DWDM OSC termination on the ONS 15454.
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

Caution Deleting a OSC termination may cause node isolation and loss of visibility to nodes that do not have other OSCs or network connections to the CTC computer.

Step 1 Click the **OSC** tab.

Step 2 Click the OSC termination you want to delete and click **Delete**.

Step 3 In the Delete OSC Termination confirmation box, click **Yes**. Confirm that the changes appear; of not, repeat the task.

Until all network OSC terminations are deleted, LOS or power failure alarms on the OPT-BST, OSCM, and OSC-CSM might appear.

Step 4 Return to your originating procedure (NTP).

NTP-A85 Change Node Timing

Purpose	This procedure changes the SONET timing settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A28 Set Up Timing, page 4-22
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. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 As needed, complete the "DLP-A157 Change the Node Timing Source" task on page 12-23.

Step 4 If you need to change any internal timing settings, follow the "DLP-A70 Set Up Internal Timing" task on page 4-25 for the settings you need to modify.

Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454s should be timed to a Stratum 2 or better primary reference source.

Step 5 If you need to verify timing after removing a node from a BLSR or path protection, see the "DLP-A195 Verify Timing in a Reduced Ring" task on page 16-11.

Step 6 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A157 Change the Node Timing Source

Purpose	This task changes the SONET timing source for the ONS 15454
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

Caution The following procedure may be service affecting and should be performed during a scheduled maintenance window.

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing section, change any of the following information:

- Timing Mode

Note Because mixed timing can cause timing loops, Cisco does not recommend using the Mixed Timing option. Use this mode with care.

- SSM Message Set
- Quality of RES
- Revertive
- Revertive Time

See the "DLP-A69 Set Up External or Line Timing" task on page 4-23 for field descriptions.

Step 3 In the BITS Facilities section, you can change the following information:

Note The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- BITS In State
- BITS Out State
- State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- LBO

Step 4 In the Reference Lists area, you can change the following information:

Note Reference lists define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference
- BITS 1 Out
- BITS 2 Out

Step 5 Click **Apply**. Confirm that the changes appear; of not, repeat the task.

Step 6 Return to your originating procedure (NTP).

NTP-A205 Modify Users and Change Security

Purpose	This procedure modifies user and security properties for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A30 Create Users and Assign Security, page 4-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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 "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A271 Change Security Policy—Single Node, page 12-25
- DLP-A272 Change Security Policy—Multiple Nodes, page 12-27
- DLP-A511 Change Node Access and PM Clearing Privilege, page 12-28
- DLP-A158 Change User Password and Security Level—Single Node, page 12-29
- DLP-A160 Change User Password and Security Level—Multiple Nodes, page 12-29
- DLP-A159 Delete User—Single Node, page 12-31
- DLP-A161 Delete User—Multiple Nodes, page 12-32

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A271 Change Security Policy—Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
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	Superuser

Step 1 In node view, click the **Provisioning** > **Security** > **Policy** tabs.

Step 2 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 3 In the User Lockout area, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 4 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.

Step 5 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change their password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.

Step 6 In the Other area, you can provision the following:

- Single Session Per User—If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 45 to 90 days.

Step 7 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-A272 Change Security Policy—Multiple Nodes

Purpose	This task changes the security policy for multiple nodes including idle user timeouts, user lockouts, password change, and concurrent login policies.
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	Superuser

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Policy** tabs. A read-only table of nodes and their policies appears.

Step 3 Click a node on the table that you want to modify, then click **Change**.

Step 4 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 5 In the User Lockout area, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 6 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.

Step 7 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number days the user will be warned to change their password for each security level. The range is 2 to 20 days.

Step 8 In the Other area, you can provision the following:

- Single Session Per User—If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 45 to 90 days.

Step 9 In the Select Applicable Nodes area, uncheck any nodes where you do not want to apply the changes.

Step 10 Click **OK**.

Step 11 In the Security Policy Change Results dialog box, confirm that the changes are correct, then click **OK**.

Step 12 Return to your originating procedure (NTP).

DLP-A511 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15454 and sets the user security level that can clear node performance monitoring data.
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	Superuser

Step 1 In node view, click the **Provisioning** > **Security** > **Access** tabs.

Step 2 In the Access area, provision the following:

- LAN access—Sets the access paths to the node:
  - No LAN Access—Allows access to the node only through DCC connections. Access through the TCC2 RJ-45 port and backplane is not permitted.
  - Backplane only—Allows access through DCC connections and the backplane. Access through the TCC2 RJ-45 port is not allowed.
  - Front and Backplane—Allows access through DCC, TCC2 RJ-45 and backplane connections.
- Restore Timeout—Sets a time delay for enabling of front and backplane access when DCC connections are lost and "DCC only" is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.

Step 3 In the Shell Access area, set the shell program used to access the node:

- Telnet—If chosen, allows access to the node using Telnet. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). If chosen, choose the Telnet port. Port 23 is the default.
- SSH—If chosen, allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links. If chosen, Port 22 is the default port. It cannot be changed.

Step 4 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: RETRIEVE, PROVISIONING, MAINTENANCE, or SUPERUSER.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A158 Change User Password and Security Level—Single Node

Purpose	This task changes settings for an existing user at one node.
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	Superuser

Step 1 In node view, click the **Provisioning** > **Security > Users** tabs.

Step 2 Click the user whose settings you want to modify, then click **Change**.

Step 3 In the Change User dialog box, you can:

- Change a user password
- Modify the user security level
- Lock out the user

See the "NTP-A30 Create Users and Assign Security" procedure on page 4-4 for field descriptions.

Step 4 Click **OK**.

Note User settings that you changed during this task will not appear until that user logs off and logs back in.

Step 5 Return to your originating procedure (NTP).

DLP-A160 Change User Password and Security Level—Multiple Nodes

Purpose	This task changes settings for an existing user at multiple 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	Superuser

Note You must add the same user name and password to each node the user will access.

Step 1 From the View menu, choose **Go to Network View**. Verify that you can access all the nodes where you want to add users.

Step 2 Click the **Provisioning** > **Security > Users** tabs. Highlight the user's name whose settings you want to change.

Step 3 Click **Change**. The Change User dialog box appears.

Step 4 In the Change User dialog box, you can:

- Change a user's password
- Modify the user's security level
- Lock out the user

See the "DLP-A75 Create a New User—Multiple Nodes" task on page 4-5 for field descriptions.

Step 5 In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 6 Click **OK**. A Change Results confirmation dialog box appears.

Step 7 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-A315 Log Out a User—Single Node

Purpose	This task logs out a user from a single node.
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	Superuser

Step 1 In node view, click the **Provisioning** > **Security > Active Logins** tabs.

Step 2 Choose the user that you want to log out and click **Logout**.

Step 3 In the Logout User dialog box, check **Lockout before Logout** if you want to lock the user out. This prevents the user from logging in after logout based on parameters provided in the user lockouts in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-A271 Change Security Policy—Single Node" task on page 12-25 for more information.

Step 4 Click **OK**.

Step 5 Click **Yes** to confirm the logout.

Step 6 Return to your originating procedure (NTP).

DLP-A316 Log Out a User—Multiple Nodes

Purpose	This task logs out a user from multiple 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	Superuser

Step 1 From the view menu, chose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Active Logins** tabs.

Step 3 Choose the user you want to log out.

Step 4 Click **Logout**.

Step 5 In the Logout User dialog box, check the nodes where you want to log out the user.

Step 6 Check **Lockout before Logout** if you want to lock the user out prior to logout. This prevents the user from logging in after logout based on user lockout parameters provisioned in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-A271 Change Security Policy—Single Node" task on page 12-25 for more information.

Step 7 In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 8 Click **OK**.

Step 9 Return to your originating procedure (NTP).

DLP-A159 Delete User—Single Node

Purpose	This task deletes an existing user from a single node.
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	Superuser

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-A315 Log Out a User—Single Node" task on page 12-30, or you can choose the "Logout before delete" option in the Delete User dialog box.

Note CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Choose the user you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete User dialog box, verify that the user name displayed is the one you want to delete. Click **Logout before delete? if the user is currently logged in. (You cannot delete users if they are logged in.)**

Step 5 Click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 6 Return to your originating procedure (NTP).

DLP-A161 Delete User—Multiple Nodes

Purpose	This task deletes an existing user from multiple 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	Superuser

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-A316 Log Out a User—Multiple Nodes" task on page 12-31, or you can choose the "Logout before delete" option in the Delete User dialog box.

Note CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security** tabs. Highlight the name of the user you want to delete.

Step 3 Click **Delete**. The Delete User dialog box appears.

Step 4 In the Select Applicable Nodes area, uncheck any nodes where you do not want to delete this user.

Step 5 Click **OK**. A User Deletion Results confirmation dialog box appears.

Step 6 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 7 Return to your originating procedure (NTP).

NTP-A87 Change SNMP Settings

Purpose	This procedure modifies SNMP settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A256 Set Up SNMP, page 4-33
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. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A273 Modify SNMP Trap Destinations, page 12-33
- DLP-A163 Delete SNMP Trap Destinations, page 12-34

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A273 Modify SNMP Trap Destinations

Purpose	This task modifies the SNMP trap destinations on an ONS 15454 including community name, default UDP port, SNMP trap version, and maximum traps per second.
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 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Select a trap from the **Trap Destinations** dialog box.

For a description of SNMP traps, refer to the *Cisco ONS 15454 Reference Manual*.

Step 3 Type the SNMP community name in the Community Name field.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the network management system.

Note The default UDP port for SNMP is 162.

Step 4 Set the Trap Version field for either SNMPv1 or SNMPv2.

Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

Step 5 Set your maximum traps per second in the Max Traps per Second field.

Note The Max Traps per Second is the maximum number of traps per second that will be sent to the SNMP manager. If the field is set to 0, there is no maximum and all traps are sent.

Step 6 If you want to allow the ONS 15454 SNMP agent to accept SNMP SET requests on certain MIBs, check the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 Click **Apply**.

Step 8 SNMP settings are now configured. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations screen. Confirm that the changes appear; if not repeat the task.

Step 9 Return to your originating procedure (NTP).

DLP-A163 Delete SNMP Trap Destinations

Purpose	This task deletes SNMP trap destinations on an ONS 15454.
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 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 In the Trap Destinations area, click the trap you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).