



CHAPTER 8

Managing Security

This chapter describes Cisco Prime Optical security and how to manage users. This includes an overview of security domains and a description of the user security and NE security features available in Prime Optical.

This chapter contains the following sections:

- [8.1 Overview, page 8-1](#)
- [8.2 Login Advisory Message, page 8-2](#)
- [8.3 User Security, page 8-2](#)
- [8.4 NE Security Management, page 8-41](#)
- [8.5 Audit Log, page 8-72](#)
- [8.6 Northbound Gateway Security, page 8-76](#)

8.1 Overview

Why create a security policy?

- To create a baseline of your current security posture
- To set the framework for security implementation
- To define allowed and disallowed behaviors
- To help determine necessary tools and procedures
- To communicate consensus and define roles
- To define how to handle security incidents

The following security domains govern Prime Optical networks:

- Prime Optical client—A Prime Optical client must be created with one of the existing default user profiles or with a new custom user profile with appropriate access privileges. This new user profile should be created and assigned to a user.
- Prime Optical Operations Support System (OSS) users—OSS-to-Prime Optical sessions are configured by the Prime Optical GateWay EMS-to-NMS interface architectural component. See [Chapter 12, “Managing Southbound and Northbound Interfaces”](#) for more information about Prime Optical GateWay.

- NE users—An NE user account must be set up so Prime Optical can use it to communicate with the NE. NE user accounts are used to directly access the NE through the NE's craft tool or the command-line interface (CLI).

Prime Optical supports the following security features:

- Login advisory message
- User management and profiles
- NE access control
- Audit Log
- Northbound gateway security

8.2 Login Advisory Message

After logging into the Prime Optical client, a login advisory message is shown. By default, the advisory message reads:

Cisco Prime Optical is a carrier-class, multitechnology management system that integrates the end-to-end management of legacy transport networks and packet optical transport networks. Cisco Prime Optical helps communication service providers (CSPs) deliver the capacity and quality of service (QoS) required to support the delivery of rich-content-based services and high-bandwidth applications.



Note

The login advisory message is not shown if you login to Prime Optical through Prime Central.

You can customize the default advisory message as follows:

- Step 1** Log into the Prime Optical server as the root user.
- Step 2** Use a text editor to edit or create the advisory.txt file in the /opt/CiscoTransportManagerServer/cfg directory.

The new advisory message can contain up to 1600 characters. The advisory.txt file does not exist by default.
- Step 3** Save the changes.

All subsequent users who log into the Prime Optical client will see the new advisory message.



Note

You can also disable the advisory message altogether. See [8.3.3.13 Configuring Prime Optical Security Parameters](#), page 8-29.

8.3 User Security

This section describes user security and management. This includes procedures on how to add a new user, modify a user's properties, delete a user, and end an active user session. It also includes procedures on how to add, modify, and delete custom profiles and how to perform NE user administration.

8.3.1 Restricting User Access

The **Administration > Users** menu launched from the Domain Explorer window, manages user security. Prime Optical administration allows restricted access logins to enable users to perform tasks based on detailed access privileges. For each action, a user is given read-only, read/write, or no access privileges.

8.3.2 User Privilege Profiles

By default, Prime Optical contains the following user profiles:

- SuperUser—Users who have access to all operations.
- SysAdmin—System administrators who manage Prime Optical access.
- NetworkAdmin—Typically, network operations center (NOC) supervisors who perform daily network NE operations. These operations do not include changing the NE username and password in the NE Authentication tab.
- Provisioner—Users who perform daily network surveillance, provisioning, and PM activities on specific NEs. Each provisioner can have only one active session. Provisioners cannot access administrative information.
- Operator—Users who perform daily network surveillance and PM activities on specific NEs. Each operator can have only one active session. Operators cannot access administrative information.

Prime Optical allows SuperUsers and SysAdmins to generate custom user profiles with certain privileges. Custom user profiles are grouped into categories and each category has a set of operations. After the user profiles are generated, they can be assigned to new Prime Optical users.

**Note**

You must select the privileges for all possible operations, even for privileges related to modules that are not currently installed on the server.

8.3.3 Performing User Administration

This section describes how to perform user administration, including:

- [8.3.3.1 Viewing the Prime Optical Users Table, page 8-13](#)
- [8.3.3.2 Creating a Prime Optical User, page 8-15](#)
- [8.3.3.3 Modifying a Prime Optical User's Properties, page 8-18](#)
- [8.3.3.4 Deleting a Prime Optical User, page 8-21](#)
- [8.3.3.5 Viewing Logged In Prime Optical Users, page 8-22](#)
- [8.3.3.6 Ending an Active Prime Optical User Session, page 8-22](#)
- [8.3.3.7 Viewing a List of Failed Login Attempts, page 8-23](#)
- [8.3.3.8 Locked User Account, page 8-23](#)
- [8.3.3.8 Locked User Account, page 8-23](#)
- [8.3.3.9 Changing Your User Password, page 8-23](#)
- [8.3.3.10 Managing Security Advisory Messages, page 8-25](#)

- [8.3.3.11 Setting User Preferences, page 8-26](#)
- [8.3.3.12 Enabling or Disabling the Continuous Audible Alarm, page 8-29](#)
- [8.3.3.13 Configuring Prime Optical Security Parameters, page 8-29](#)
- [8.3.3.14 Sending Messages to Other Users, page 8-34](#)
- [8.3.3.15 Viewing User Notification Messages, page 8-35](#)

The following table lists the Prime Optical default user profiles and the privileges associated with each profile.

**Note**

The SuperUser profile has access to all operations, and is not specifically listed in a separate column.

**Note**

The NetworkAdmin profile has access to all NEs and groups. The SysAdmin profile has access to no NEs or groups.

Table 8-1 **Prime Optical Default User Profiles**

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Domain Explorer				
File > New Group	Deny	Allow	Deny	Deny
File > Add Network Element(s)	Deny	Allow	Deny	Deny
File > Dashboard	Allow	Allow	Allow	Allow
File > Network Map	Deny	Allow	Allow	Allow
File > Subnetwork Explorer	Deny	Allow	Deny	Deny
File > Domain NE Table	Deny	Allow	Allow	Allow
File > TNE Devices	Deny	Allow	Deny	Deny
File > ENE Devices	Deny	Allow	Allow	Allow
File > Notify Users	Allow	Allow	Allow	Allow
File > Refresh Data	Allow	Allow	Allow	Allow
File > Debug Options	Allow	Allow	Allow	Allow
File > Exit	Allow	Allow	Allow	Allow
Edit > Cut	Deny	Allow	Deny	Deny
Edit > Copy	Deny	Allow	Deny	Deny
Edit > Paste	Deny	Allow	Deny	Deny
Edit > Delete	Deny	Allow	Deny	Deny
Edit > Delete All	Deny	Allow	Deny	Deny
Edit > Undelete	Deny	Allow	Deny	Deny
Edit > Expand	Deny	Allow	Allow	Allow
Edit > Collapse	Deny	Allow	Allow	Allow
Edit > Find	Deny	Allow	Allow	Allow
Edit > Find Next	Deny	Allow	Allow	Allow

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Edit > User Preferences	Allow	Allow	Allow	Allow
Edit > Change Password	Allow	Allow	Allow	Allow
Fault > Alarm Browser	Allow	Allow	Allow	Allow
Fault > Alarm Log	Allow	Allow	Allow	Allow
Fault > Event Export Manager	Allow	Allow	Allow	Allow
Fault > Ping NE	Deny	Allow	Allow	Allow
Fault > Test NE Connectivity	Deny	Allow	Allow	Allow
Fault > Stop Continuous Beep	Deny	Allow	Allow	Allow
Fault > SysLog Viewer	Deny	Allow	Allow	Allow
Performance > PM Query by NE Model	Deny	Allow	Allow	Allow
Performance > PM Query by Category	Deny	Allow	Allow	Allow
Performance > PM Collection Settings	Deny	Allow	Allow	Deny
Configuration > NE Explorer	Deny	Allow	Allow	Allow
Configuration > Link Table	Deny	Allow	Allow	Allow
Configuration > Create Circuit	Deny	Allow	Allow	Deny
Configuration > Manage VLANs	Deny	Allow	Allow	Deny
Configuration > Create Link	Deny	Allow	Allow	Deny
Configuration > Create Server Trail	Deny	Allow	Allow	Deny
Configuration > Compare Config Files	Deny	Allow	Deny	Deny
Configuration > <i>NE_Model</i> > BLSR Table	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Create BLSR	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > MS-SPRing Table	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Create MS-SPRing	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Equipment Inventory Table	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Initialize ML Cards	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > L2 Topology Table	—	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Create L2 Topology	—	Allow	Allow	Deny
Configuration > <i>NE_Model</i> > QoS Profile Table	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Create QoS Profile	Deny	Allow	Allow	Deny
Configuration > <i>NE_Model</i> > Discover L2 Topologies	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Alarm Profiles Management	Deny	Allow	Allow	Deny
Configuration > <i>NE_Model</i> > NE Defaults Management	Deny	Allow	Allow	Deny
Configuration > <i>NE_Model</i> > VLAN DB Profile Management	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Circuit Table	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Rolls Table	Deny	Allow	Allow	Allow
Configuration > <i>NE_Model</i> > Update Circuit	Deny	Allow	Allow	Deny

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Configuration > NE_Model > Repair Circuit	Deny	Allow	Allow	Deny
Configuration > NE_Model > Configure Node	Deny	Allow	Allow	Allow
Configuration > NE_Model > Launch Web Interface	Deny	Allow	Allow	Allow
Configuration > NE_Model > Launch CLI	Deny	Allow	Allow	Allow
Configuration > NE_Model > Launch TL1 Interface	Deny	Allow	Allow	Allow
Configuration > NE_Model > Launch Cisco Edge Craft	Deny	Allow	Allow	Allow
Configuration > NE_Model > Launch CTC	Deny	Allow	Allow	Allow
Configuration > NE_Model > APC Domain Management	Deny	Allow	Allow	Allow
Configuration > NE_Model > Create SVLAN	Deny	Allow	Allow	Deny
Configuration > NE_Model > NE Discrepancy Table	Deny	Allow	Allow	Allow
Configuration > NE_Model > Discovery Info Table	Deny	Allow	Allow	Allow
Configuration > NE_Model > Resync with NE	Deny	Allow	Allow	Allow
Configuration > NE_Model > Template Manager	Deny	Allow	Allow	Deny
Configuration > NE_Model > Rediscover	Deny	Allow	Allow	Allow
Configuration > NE_Model > Rediscover All	Deny	Allow	Allow	Allow
Configuration > NE_Model > Launch IOS CLI	Deny	Allow	Allow	Allow
Configuration > NE_Model > Template Configuration	Deny	Allow	Deny	Deny
Configuration > PT System > Provision > Create TP Tunnel	Deny	Allow	Allow	Deny
Configuration > PT System > Provision > Create Pseudowire	Deny	Allow	Allow	Deny
Configuration > PT System > Provision > Create EVC	Deny	Allow	Allow	Deny
Configuration > PT System > Provision > QoS Provisioning	Deny	Allow	Allow	Deny
Configuration > PT System > Provision > QoS Editor	Deny	Allow	Allow	Deny
Configuration > PT System > Display > TP Tunnel Table	Deny	Allow	Allow	Deny
Configuration > PT System > Display > Pseudowire Table	Deny	Allow	Allow	Deny
Configuration > PT System > Display > EVC Table	Deny	Allow	Allow	Deny
Configuration > PT System > Advanced Troubleshooting > TP Tunnel XC Table	Deny	Allow	Deny	Deny
Configuration > PT System > Advanced Troubleshooting > Pseudowire XC Table	Deny	Allow	Deny	Deny
Configuration > PT System > Advanced Troubleshooting > EVC XC Table	Deny	Allow	Deny	Deny
Configuration > PT System > Advanced Troubleshooting > Refresh L2 Service Data Discovery	Deny	Allow	Deny	Deny
Administration > Job Monitor	Deny	Allow	Allow	Deny
Administration > Service Monitor	Allow	Deny	Deny	Deny
Administration > Self Monitor	Deny	Allow	Deny	Deny
Administration > Memory Backup	Deny	Allow	Deny	Deny

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Administration > Memory Restore	Deny	Allow	Deny	Deny
Administration > Memory Backup Upload	Deny	Allow	Deny	Deny
Administration > Image Transfer	Deny	Allow	Deny	Deny
Administration > NE Software Table	Deny	Allow	Deny	Deny
Administration > Bulk Software Activation	Deny	Allow	Allow	Deny
Administration > Software Management > Optical	Deny	Allow	Deny	Deny
Administration > SNTP Configuration	Deny	Allow	Deny	Deny
Administration > Bulk FTP Configuration	Deny	Allow	Allow	Allow
Administration > Users	Allow	Deny	Deny	Deny
Administration > GateWay/SNMP Users	Allow	Deny	Deny	Deny
Administration > Control Panel	Allow	Deny	Deny	Deny
Administration > Audit Log	Allow	Deny	Deny	Deny
Administration > Error Log	Allow	Allow	Deny	Deny
Administration > Supported NE Table	Allow	Allow	Deny	Deny
Administration > CTC Upgrade Table	Allow	Allow	Deny	Deny
Administration > CTC User Profiles	Allow	Allow	Deny	Deny
Administration > <i>NE_Model</i> > NE User Access Administration	Allow	Allow	Deny	Deny
Administration > <i>NE_Model</i> > Audit Trail Table	Allow	Allow	Deny	Deny
Administration > <i>NE_Model</i> > Security Advisory Management	Allow	Allow	Deny	Deny
Administration > <i>NE_Model</i> > NE Authentication	Allow	Allow	Deny	Deny
Administration > <i>NE_Model</i> > IOS Users Table	Deny	Allow	Allow	Deny
Administration > <i>NE_Model</i> > SNMPv3 Users	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 MIB Views	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 Group Access	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 Trap Destinations	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 Notification Filters	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 Proxy Forwarder	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 Proxy Trap Forwarder	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 Remote Users	Allow	Allow	Allow	Allow
Administration > <i>NE_Model</i> > SNMPv3 Configuration	Allow	Allow	Allow	Allow
Administration > ONS 155XX > ONS 155XX SNMP Settings Table	Allow	Allow	Deny	Deny
Administration > ONS 155XX > Flash File Table	Allow	Allow	Deny	Deny
Network Map				
File > Open	Deny	Allow	Allow	Allow
File > Open (New Window)	Deny	Allow	Allow	Allow

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
File > Parent	Deny	Allow	Allow	Allow
File > Save	Deny	Allow	Allow	Allow
File > Save As Default	Deny	Allow	Deny	Deny
File > Revert To Default	Deny	Allow	Allow	Allow
File > Notify Users	Deny	Allow	Allow	Allow
File > Refresh Data	Deny	Allow	Allow	Allow
File > Debug Options	Deny	Allow	Allow	Allow
File > Close	Deny	Allow	Allow	Allow
Edit > Enable Drag	Deny	Allow	Allow	Allow
Edit > Enable Offview	Deny	Allow	Allow	Allow
Edit > Change Map Background	Deny	Allow	Allow	Allow
Edit > Change Node Icon	Deny	Allow	Allow	Allow
Edit > Zoom In	Deny	Allow	Allow	Allow
Edit > Zoom Out	Deny	Allow	Allow	Allow
Edit > Zoom Area	Deny	Allow	Allow	Allow
Edit > Find	Deny	Allow	Allow	Allow
Edit > Find Next	Deny	Allow	Allow	Deny
Edit > Expand All Links	Deny	Allow	Allow	Allow
Edit > Collapse All Links	Deny	Allow	Allow	Allow
Edit > Circular Layout	Deny	Allow	Allow	Allow
Edit > Spring Layout	Deny	Allow	Allow	Allow
Edit > Table Layout	Deny	Allow	Allow	Allow
Edit > Declutter Layout	Deny	Allow	Allow	Allow
Edit > User Preferences	Deny	Allow	Allow	Allow
Edit > Change Password	Deny	Allow	Allow	Allow
Subnetwork Explorer				
File > Add New Network Partition	—	Allow	—	—
File > Add New Subnetwork	—	Allow	—	—
File > Add Network Element(s)	Deny	Deny	Deny	Allow
Alarm Browser				
Fault > Acknowledge Alarms	Allow	Allow	Allow	Allow
Fault > Acknowledge All Alarms	Allow	Allow	Allow	Allow
Fault > Clear Alarm(s)	Allow	Allow	Allow	Allow
Fault > Show Alarm Note	Allow	Allow	Allow	Allow
Fault > Hide Cleared Alarms	Allow	Allow	Allow	Allow
Fault > Hide Acknowledged Alarms	Allow	Allow	Allow	Allow

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Fault > Reset All Alarms	Allow	Allow	Allow	Allow
Fault > Locate Alarm/Event	Allow	Allow	Allow	Allow
TNE Devices				
Edit > Open Tunnel	Deny	Allow	Deny	Deny
Edit > Close Tunnel	Deny	Allow	Deny	Deny
Edit > Modify Tunnel	Deny	Allow	Deny	Deny
Link Table				
Edit > Modify Link	—	Allow	Allow	Deny
Edit > Delete Link	—	Allow	Allow	Deny
Configuration > Circuit Table	Deny	Allow	Allow	Allow
Configuration > Circuit Path Table	—	Allow	Allow	Deny
Configuration > Link Utilization Table	—	Allow	Allow	Deny
BLSR Table				
Edit > Edit BLSR	Deny	Allow	Allow	Deny
Edit > Delete BLSR	Deny	Allow	Allow	Deny
Edit > Upgrade BLSR	Deny	Allow	Allow	Deny
Edit > Switch BLSR	Deny	Allow	Allow	Deny
L2 Topology Table				
Configuration > Circuits	—	Allow	Allow	Allow
Configuration > ML Cards	Deny	Allow	Allow	Deny
Configuration > Create L2 Topology	—	Allow	Allow	Deny
Configuration > Modify L2 Topology	—	Allow	Allow	Deny
Configuration > Delete L2 Topology	—	Allow	Allow	Deny
Configuration > Create L2 Service	—	Allow	Allow	Deny
Configuration > Show L2 Services	—	Allow	Allow	Allow
Configuration > Modify Ports	—	Allow	Allow	Deny
Configuration > Enable L2 Service	Deny	Allow	Allow	Deny
Configuration > Add/Remove Card	Deny	Allow	Allow	Deny
Configuration > Resync L2 Topology	Deny	Allow	Allow	Deny
QoS Profile Table				
Configuration > Create QoS Profile	Deny	Allow	Allow	Deny
Configuration > Modify QoS Profile	Deny	Allow	Allow	Deny
Configuration > Delete QoS Profile	Deny	Allow	Allow	Deny
Configuration > Duplicate QoS Profile	Deny	Allow	Allow	Deny
Configuration > Show QoS Profile	Deny	Allow	Allow	Allow
Circuit Table				

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Configuration > Open Circuit Span	—	Allow	Allow	Allow
Configuration > Create Circuit	—	Allow	Allow	Deny
Configuration > Modify Circuit	—	Allow	Allow	Deny
Configuration > Delete Circuit	—	Allow	Allow	Deny
Configuration > High Level Trace Circuit	Deny	Allow	Allow	Deny
Configuration > Trace Circuit	—	Allow	Allow	Allow
Configuration > VLAN Table	—	Allow	Allow	Allow
Configuration > Show Circuit Note	—	Allow	Allow	Allow
Configuration > Roll Circuit	—	Allow	Allow	Deny
Configuration > Member Circuits	Allow	Allow	Allow	Allow
Configuration > Merge Table	—	Allow	Allow	Deny
Configuration > Reconfigure Circuit(s)	—	Allow	Allow	Deny
MS-SPRing Table				
Edit > Edit MS-SPRing	Deny	Allow	Allow	Allow
Edit > Delete MS-SPRing	Deny	Allow	Allow	Allow
Edit > Upgrade MS-SPRing	Deny	Allow	Allow	Allow
Edit > Switch MS-SPRing	Deny	Allow	Allow	Allow
Rolls Table				
Configuration > Complete Roll	—	Allow	Allow	Deny
Configuration > Finish Roll	—	Allow	Allow	Deny
Configuration > Cancel Roll	—	Allow	Allow	Deny
Configuration > Delete Roll	—	Allow	Allow	Deny
Configuration > Force Valid Signal	—	Allow	Allow	Deny
APC Domain				
Edit > Run APC	Deny	Allow	Allow	Deny
Edit > APC Results	Deny	Allow	Allow	Deny
Edit > Enable APC	Deny	Allow	Allow	Deny
Edit > Disable APC	Deny	Allow	Allow	Deny
Edit > Discover APC Domain	Deny	Allow	Allow	Deny
SVLAN Table				
Edit > Modify SVLAN	Deny	Allow	Allow	Deny
Edit > Delete SVLAN	Deny	Allow	Allow	Deny
Configuration > Create SVLAN	Deny	Allow	Allow	Deny
Configuration > Trace SVLAN	Deny	Allow	Allow	Deny
Configuration > Add Drop	Deny	Allow	Allow	Deny
Configuration > Delete Drop	Deny	Allow	Allow	Deny

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Job Monitor Table				
Edit > Cancel Task	—	Allow	—	—
Edit > Cancel Job	—	Allow	—	—
Edit > User Note	—	Allow	—	—
Edit > NE Software Table	—	Allow	—	—
NE Software Table				
Edit > Commit	—	Allow	—	—
Edit > Revert/Switch	—	Allow	—	—
Edit > Accept	—	Allow	—	—
Edit > Reset ML Cards	Deny	Deny	Deny	Deny
TP Tunnel Service Table				
Edit > Delete	Deny	Allow	Allow	Deny
Edit > View/Modify	Deny	Allow	Allow	View—Allow
				Modify—Deny
Configuration > Trace	Deny	Allow	Allow	Allow
Configuration > Pseudowire Table	Deny	Allow	Allow	Deny
PW Service Table				
Edit > Delete	Deny	Allow	Allow	Deny
Edit > View/Modify	Deny	Allow	Allow	View—Allow
				Modify—Deny
Configuration > Trace	Deny	Allow	Allow	Allow
EVC Service Table				
Edit > Delete	Deny	Allow	Allow	Deny
Edit > View/Modify	Deny	Allow	Allow	View—Allow
				Modify—Deny
Configuration > Trace	Deny	Allow	Allow	Allow
TP Tunnel XC Table				
Edit > Delete	Deny	Allow	Deny	Deny
Edit > TP Circuit Table	Deny	Allow	Deny	Deny
Configuration > Rediscover	Deny	Allow	Deny	Deny
Configuration > Refresh	Deny	Allow	Deny	Deny
Pseudowire XC Table				
Edit > Delete	Deny	Allow	Deny	Deny
Edit > Pseudowire Table	Deny	Allow	Deny	Deny
Configuration > Rediscover	Deny	Allow	Deny	Deny
Configuration > Refresh	Deny	Allow	Deny	Deny
EVC XC Table				

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Edit > Delete	Deny	Allow	Deny	Deny
Edit > EVC Table	Deny	Allow	Deny	Deny
Configuration > Rediscover	Deny	Allow	Deny	Deny
Configuration > Refresh	Deny	Allow	Deny	Deny
Prime Optical Users				
Edit > Create	Allow	—	—	—
Edit > Modify	Allow	—	—	—
Edit > Delete	Allow	—	—	—
Edit > Unlock	Allow	Deny	Deny	Deny
Administration > User Profiles	Allow	Deny	Deny	Deny
Administration > Logged In Users	Allow	Deny	Deny	Deny
Administration > Failed Login Attempts	Allow	Deny	Deny	Deny
Prime Optical User Profiles				
Edit > Create	Allow	Deny	Deny	Deny
Edit > View/Modify	Allow	Deny	Deny	Deny
Edit > Delete	Allow	Deny	Deny	Deny
Edit > Duplicate	Allow	Deny	Deny	Deny
Logged In Users Table				
Administration > Log Out User	Allow	Deny	Deny	Deny
OSS SNMPv3 Users Table				
Edit > Add	Deny	Deny	Deny	Deny
Edit > Modify	Deny	Deny	Deny	Deny
Edit > Delete	Deny	Deny	Deny	Deny
GateWay/CORBA Users Table				
Edit > Add	Deny	Deny	Deny	Deny
Edit > Modify	Deny	Deny	Deny	Deny
Edit > Delete	Deny	Deny	Deny	Deny
Administration > Logged In GateWay CORBA Users	Deny	Deny	Deny	Deny
Supported NE Table				
Edit > Add	Allow	Allow	—	—
Edit > Delete	Allow	Allow	—	—
CTC Upgrade Table				
Edit > Add	Allow	Allow	—	—
Edit > Activate	Allow	Allow	—	—
Edit > Delete	Allow	Allow	—	—
CTC User Profiles Table				
Edit > Create	Allow	Allow	—	—

Table 8-1 Prime Optical Default User Profiles (continued)

Operation	SysAdmin	NetworkAdmin	Provisioner	Operator
Edit > Modify	Allow	Allow	—	—
Edit > Delete	Allow	Allow	—	—
NE User Access Administration				
Edit > Add	Allow	Allow	—	—
Edit > Add Predefined Users	Allow	Allow	—	—
Edit > Modify	Allow	Allow	—	—
Edit > Delete	Allow	Allow	—	—
Edit > NE Active Users	Allow	Allow	—	—
NE Active Users Table				
Administration > Retrieve Last Activity Time	Deny	Allow	Deny	Deny
Administration > Log Out User	Deny	Allow	Deny	Deny
IOS Users Table				
Edit > Create	Deny	Allow	Allow	Deny
Edit > Modify	Deny	Allow	Allow	Deny
Edit > Delete	Deny	Allow	Allow	Deny
SNMP Community String				
Edit > Add	Allow	Allow	—	—
Edit > Delete	Allow	Allow	—	—
Edit > Modify	Allow	Allow	—	—
Flash File Table				
Edit > Verify	Allow	Allow	—	—
Edit > Delete	Allow	Allow	—	—
Edit > Undelete	Allow	Allow	—	—
Edit > Squeeze	Allow	Allow	—	—
Edit > Activate	Allow	Allow	—	—
SNMPv3 Users Table				
Edit > Add	Deny	Deny	Deny	Deny
Edit > View/Modify	Deny	Deny	Deny	Deny
Edit > Delete	Deny	Deny	Deny	Deny

8.3.3.1 Viewing the Prime Optical Users Table

The Prime Optical Users table displays basic information about Prime Optical users. The table menu options allow you to create new users, modify users, delete users, and unlock user accounts.

To view the Prime Optical Users table, choose **Administration > Users** in the Domain Explorer window. The following table provides descriptions.

**Tip**

You can click any cell or row in the Prime Optical Users table and then type an alphanumeric character on your keyboard. The selection context jumps to the next username row that starts with that letter or number.

If there are multiple usernames that begin with the same letter or number, the selection context cycles through them. For example, if the Prime Optical Users table contains SuperUser and SysAdmin users, and you press the s key multiple times, the selected row toggles between SuperUser and SysAdmin.

Table 8-2 **Field Descriptions for the Prime Optical Users Table**

Field	Description
Username	Username of the selected Prime Optical user.
CTC Username	CTC username of the selected user. This name is used to launch CTC from Prime Optical.
User Privilege Level	User privilege level (SuperUser, SysAdmin, NetworkAdmin, Provisioner, Operator, or a custom profile).
User Domain Name	Name of the management domain where the username belongs.
Password Set Time (<i>time zone</i>)	Last time the password was set.
Locked State	Whether the user's account is locked or unlocked. If the user repeatedly tries unsuccessfully to log into the Prime Optical client (the default maximum is five attempts), the user's account is locked automatically. You can set the maximum number of login attempts a user is allowed before being locked out in the Control Panel > Security Properties pane.
Last Login Time (<i>time zone</i>)	Last time the user logged in.
Login Failed Attempts	Number of times the user tried to log in, but failed.
Login State	Administrative state (Enabled or Disabled) of the user.
User Description	Description of the user.
Password Change Enabled	Current state (Enabled or Disabled) of the password change option.
Multiple Login Enabled	Whether this user is allowed to perform multiple logins simultaneously.
Auto Disable Account	Number of days of nonuse that will prompt the account to be disabled automatically. The range is from 0 to 365 days, in 1-day increments. The Cisco default is 0 days, meaning the account will not be disabled automatically as a result of inactivity.

8.3.3.2 Creating a Prime Optical User


Note

This functionality is disabled when Prime Optical is installed as part of Prime Central.

Use the Create New Prime Optical User wizard to add new Prime Optical users to the domain. [Table 8-3](#) provides descriptions.

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Prime Optical Users table, choose **Edit > Create** (or click the **Create a New User** tool).
- Step 3** In the Create New User wizard, fill in the following fields:
- Username
 - User Password (and confirm password)
 - User Privilege
 - Domain Name
 - Login State
 - Password Change
 - Description
 - Auto Disable Account (days)
 - Require Password Change on Next Login check box
 - Use Global Settings check box
 - Enable check box
 - Period
- Step 4** Click **Next**. When you are finished adding a new SuperUser, NetworkAdmin, or SysAdmin, click **Finish**.
- Step 5** When adding a new Provisioner, Operator, or custom user profile, select the groups and NEs that the Provisioner or Operator will monitor. Selected groups and NEs appear in the Assigned Objects list. (SuperUsers and NetworkAdmins monitor the entire management domain, so there is no need to select groups or NEs when adding one of these users. SysAdmin users do not access any of the NEs.)
- a. To assign groups, click the **Groups** radio button. In the Available Objects list, select the groups that will be assigned to the new user and click **Add**.
 - b. To assign NEs, click the **Network Elements** radio button. In the Available Objects list, select the NEs that will be assigned to the new user and click **Add**.


Note

When individual NEs are assigned, these NEs will appear directly under the top level domain for the user in the Domain Explorer. It is possible that a given NE may have already been assigned as part of a group assignment to the user. In such a case, the same NE will appear directly under the top level domain and also within the assigned group. This behavior is consistent with the Domain Explorer's ability to represent the same group or NE within multiple locations of the hierarchy.

- c. To remove groups or NEs from the Assigned Objects list, select the group or NE from the Assigned Objects list and click **Remove**.
- d. Click **Next** (or **Finish**).

- Step 6** When adding a new Provisioner, you can restrict the set of SONET or SDH circuit sizes that the user can provision. The selected SONET or SDH circuit sizes appear in the Assigned Circuit Sizes list.
- To assign SONET circuits, click the **SONET** radio button. In the Available Circuit Sizes list, select the circuits that will be assigned to the user and click **Add**.
 - To assign SDH circuits, click the **SDH** radio button. In the Available Circuit Sizes list, select the circuits that will be assigned to the user and click **Add**.
 - To remove SONET or SDH circuits from the Assigned Circuit Sizes list, select the circuit size from the Assigned Circuit Sizes list and click **Remove**.
 - Click **Next** (or **Finish**).

- Step 7** (Optional) In the CTC/Craft User Properties area, enter the username and password for accessing CTC-based NEs or NEs that support a TL1 interface. Then, confirm the password.



Note If the CTC/Craft User username and password have been defined for a given user, when that user launches a TL1 session to an NE that supports a TL1 interface, Prime Optical logs the user in automatically with the **ACT-USER** command, using the defined craft username and password.

- Step 8** Click **Finish**.

The new user is listed in the Prime Optical Users table. For CTC-based NEs, the new user will be mapped to a CTC user but the CTC user will not be created in the NE database. To create a CTC user on the NE database, see [8.4.3 Managing NE User Access, page 8-48](#).

Table 8-3 Field Descriptions for the Create New Prime Optical User Wizard

Field	Description
User Properties Pane	
Username	Name that the user will use to access the system. The username must contain from three to twelve alphanumeric characters (A–Z, a–z, 0–9). Alphabetic characters are case-sensitive. The username must be unique and cannot contain spaces or special characters.
	Note After the username is set, it cannot be changed without deleting the user.

Table 8-3 Field Descriptions for the Create New Prime Optical User Wizard (continued)

Field	Description
User Password	<p>Login password that the user will use to access the system. The password complexity is configurable in the Control Panel > Security Properties pane. By default, the user password must:</p> <ul style="list-style-type: none"> Contain at least six characters, but not more than 15 characters. Contain at least two alphabetic characters (A–Z, a–z). Of the alphabetic characters, at least one must be uppercase and one must be lowercase. Contain at least one numeric character (0–9). Contain at least one special character (+ # % , . ; & !). The default special character set is TL1+UNIX. Allow a special character as the first or last character. Allow a numeric character as the first or last character. Not contain the username or any circular shift of the username. An uppercase letter and its corresponding lowercase letter are considered equivalent. For example, if the username is Arthur, the password cannot contain the string arthur, rthura, thurar, hurart, urarth, or rarthu. Differ from the old password by at least three characters. For example, if the old password is MikeBrady5!, the new password cannot be mikebrady5% because only the last character is different. However, the new password MikeBrady2!99 is acceptable because it differs from MikeBrady5! by three characters. <p>Note By default, the minimum time between password changes is 20 days. The new password must differ from the previous password by 3 characters, and the new password is compared against the previous 10 passwords.</p>
Confirm Password	Retype the password to confirm it.
User Privilege	User privilege level.
Domain Name	Domain name. When the user logs into the system, he or she sees all of the devices contained within this domain.
Login State	Permit (enable) or prevent (disable) the user from logging into the system.
Password Change	Permit (enable) or prevent (disable) the user from changing his or her password.
Description	Description of the new user.
Auto Disable Account (days)	Number of days of nonuse that will prompt the account to be disabled automatically. The range is from 0 to 365 days, in 1-day increments. The Cisco default is 0 days, meaning the account will not be disabled automatically as a result of inactivity.
Require Password Change on Next Login	<p>If checked, the user is prompted to change his or her password upon next login to the Prime Optical client.</p> <p>If unchecked, the user is not required to change his or her password upon next login. By default, this option is checked.</p>
Logout	Prime Optical automatically logs the user out of the Prime Optical session after the period in the Period field. Click Use Global Settings to use the settings from the Security window. If you do not select Use Global Settings, click Enable to activate logout for the selected user. Enter a logout length in the Period field.
User Login Sessions	Select whether to allow single or multiple user logins.

Assign Objects to User Pane*(for Provisioner and Operator users only)*

Table 8-3 Field Descriptions for the Create New Prime Optical User Wizard (continued)

Field	Description
Select Object Type	Assign groups or NEs to the new user. Note The Discovered NEs and Deleted NEs groups cannot be assigned to a Provisioner, Operator, or custom user profile.
Select Objects	Select from the list of available objects that can be assigned to the new user. By clicking the Add and Remove buttons, you can move objects back and forth between the Available Objects list and the Assigned Objects list.
Assign Circuit Sizes to User Pane (for Provisioner users only)	
Select Circuit Size Type	Select the circuit types that are relevant, SONET or SDH.
Select Circuit Sizes	Select valid circuit sizes from the list of available circuit sizes. By clicking the Add and Remove buttons, you can move objects back and forth between the Available Circuit Sizes list and the Assigned Circuit Sizes list.
CTC/Craft User Properties Pane	
Username	Active username for accessing CTC-based NEs or NEs that support a TL1 interface. The username must contain at least six alphanumeric characters, but not more than 20 characters.
User Password	Login password for accessing CTC-based NEs or NEs that support a TL1 interface. The new password must: <ul style="list-style-type: none"> • Contain at least 6 alphanumeric characters, but not more than 10. • Contain at least two alphabetic characters (A–Z, a–z). • Contain at least one numeric character (0–9). • Contain at least one special character (+, #, or %).
Confirm Password	Retype the password to confirm it.

8.3.3.3 Modifying a Prime Optical User's Properties

Use the Modify Prime Optical User Properties wizard to modify the properties of an existing Prime Optical user. [Table 8-4](#) provides descriptions.



Note

Some fields are read-only when Prime Optical is installed as part of Prime Central.

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Prime Optical Users table, select the Prime Optical user whose user properties will be modified.
- Step 3** Choose **Edit > View/Modify** (or click the **Modify User Properties** tool). The Modify User Properties wizard opens.
- Step 4** Modify the following fields, as needed; then, click **Next**:
- User Password (and confirm password)



Note Regardless of the actual size of the old password, the Password and Confirm Password fields display only a fixed-length string. The fixed-length string contains 15 asterisks (*).

- User Privilege
- Domain Name
- Login State
- Password Change
- Description
- Auto Disable Account
- Require Password Change on Next Login check box
- Use Global Settings check box
- Enable check box
- Period
- User Login Sessions

Step 5 (Optional) For Provisioner, Operator, and custom user profiles, modify the list of assigned objects by adding groups or NEs to the Assigned Objects list or removing groups or NEs from the list. Click **Next**.

Step 6 (Optional) For Provisioners, modify the list of assigned circuit sizes by adding or removing SONET or SDH circuit sizes from the list. Click **Next**.

Step 7 (Optional) Modify the user's CTC/craft username and password for accessing CTC-based NEs or NEs that support a TL1 interface. For username and password constraints, see [Table 8-4](#).

Step 8 Click **Finish**. The user whose properties were modified is listed in the Prime Optical Users table.



- Note**
- After you change the user privilege level, you receive a message that tells you that the selected user will be logged out. Click **OK**. This activity is reported in the Audit Log.
 - The user whose privilege has been changed receives the message "A user with administration privileges has changed the privileges of this user. The application will be closed." The user is then logged out.
 - You cannot change the user privilege of the last instance of a SysAdmin user. You must create another SysAdmin user before changing the user privilege level of the other SysAdmin user.

Table 8-4 Field Descriptions for the Modify User Properties Wizard

Field	Description
Cisco Prime Optical User Properties Pane	
Username	<p><i>Display only.</i> Active username for accessing the system. The username must contain from three to twelve alphanumeric characters (A–Z, a–z, 0–9). Alphabetic characters are case-sensitive. The username must be unique and cannot contain spaces or special characters.</p> <p>Note After the username is set, it cannot be changed without deleting the user.</p>

Table 8-4 Field Descriptions for the Modify User Properties Wizard (continued)

Field	Description
User Password	<p>Login password used to access the system. The password complexity is configurable in the Control Panel > Security Properties pane. By default, the user password must:</p> <ul style="list-style-type: none"> Contain at least six characters, but not more than 15 characters. Contain at least two alphabetic characters (A–Z, a–z). Of the alphabetic characters, at least one must be uppercase and one must be lowercase. Contain at least one numeric character (0–9). Contain at least one special character (+ # % , . ; & !). The default special character set is TL1+UNIX. Allow a special character as the first or last character. Allow a numeric character as the first or last character. Not contain the username or any circular shift of the username. An uppercase letter and its corresponding lowercase letter are considered equivalent. For example, if the username is Arthur, the password cannot contain the string arthur, rthura, thurar, hurart, urarth, or rarthu. Differ from the old password by at least three characters. For example, if the old password is MikeBrady5!, the new password cannot be mikebrady5% because only the last character is different. However, the new password MikeBrady2!99 is acceptable because it differs from MikeBrady5! by three characters. <p>Note By default, the minimum time between password changes is 20 days. The new password must differ from the previous password by three characters, and the new password is compared against the previous 10 passwords.</p>
Confirm Password	Retype the password to confirm it.
User Privilege	User's privilege level.
Domain Name	Domain name. When the user logs into the system, he or she sees all the devices contained within this domain.
Login State	Permit (enable) or prevent (disable) the user from logging into the system.
Password Change	Permit (enable) or prevent (disable) the user from changing his or her password.
Description	User description.
Auto Disable Account	Number of days of nonuse that will prompt the account to be disabled automatically. The range is from 0 to 365 days, in 1-day increments. The Cisco default is 0 days, meaning the account will not be disabled automatically as a result of nonuse.
Require Password Change on Next Login	<p>If checked, the user is prompted to change his or her password upon next login to the Prime Optical client.</p> <p>If unchecked, the user is not required to change his or her password upon next login. By default, this option is checked.</p>
Lockout	Prime Optical automatically locks the current session after the number of minutes in the Period field. Click Use Global Settings to use the settings from the Security window. If you do not select Use Global Settings, click Enable to activate lockout for the selected user. Enter a lockout length in the Period field.
Logout	Prime Optical automatically logs the user out of the Prime Optical session after the number of minutes in the Period field. Click Use Global Settings to use the settings from the Security window. If you do not select Use Global Settings, click Enable to activate logout for the selected user. Enter a logout length in the Period field.

Table 8-4 Field Descriptions for the Modify User Properties Wizard (continued)

Field	Description
User Login Sessions	Whether to allow single or multiple user login.
Assign Objects to User Pane (for Provisioner and Operator users only)	
Select Object Type	Assign specific groups and NEs to operator and provisioner users.
Select Objects	Modify the objects that are assigned to operators and provisioners. Click Add and Remove to move objects back and forth between the Available Objects list and the Assigned Objects list.
Assign Circuit Sizes to User Pane (for Provisioner users only)	
Select Circuit Size Type	Select the circuit types that are relevant, SONET or SDH.
Select Circuit Sizes	Modify the circuit sizes that are assigned to the user. Click Add and Remove to move circuit sizes back and forth between the Available Circuit Sizes list and the Assigned Circuit Sizes list.
CTC/Craft User Properties Pane	
Username	Modify the active username for accessing CTC-based NEs or NEs that support a TL1 interface. The username must contain at least six alphanumeric characters, but not more than 20 characters.
User Password	Modify the user's login password. The user password must: <ul style="list-style-type: none"> • Contain at least 6 alphanumeric characters, but not more than 10. • Contain at least two alphabetic characters (A–Z, a–z). • Contain at least one numeric character (0–9). • Contain at least one special character (+, #, or %).
Confirm Password	Confirm the newly modified password by retyping it.

8.3.3.4 Deleting a Prime Optical User

**Note**

This functionality is disabled when Prime Optical is installed as part of Prime Central.

Step 1 In the Domain Explorer window, choose **Administration > Users**.

Step 2 In the Prime Optical Users table, select the user to be deleted.

**Note**

A user cannot be deleted from the database until that user logs out. However, an active user session can be ended. See [8.3.3.6 Ending an Active Prime Optical User Session, page 8-22](#).

Step 3 Choose **Edit > Delete** (or click the **Delete User** tool).

Step 4 Click **OK** to remove the user from the database.

8.3.3.5 Viewing Logged In Prime Optical Users

The Logged In Prime Optical Users table lists the Prime Optical users who are currently logged into the Prime Optical application.

- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Prime Optical Users table, choose **Administration > Logged In Users** (or click the **Show Logged In Users** tool). The following table provides descriptions.

Table 8-5 *Field Descriptions for the Logged In Users Table*

Field	Description
Username	Name of the user who is currently logged in.
Logged In At	Date and time when the user logged in.
IP Address	User's IP address.
Session ID	Unique session ID number that the Prime Optical server assigns to each Prime Optical user during login.

8.3.3.6 Ending an Active Prime Optical User Session



Note

If you are accessing Prime Optical through Prime Central, the Administration > Users option is disabled.

- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Prime Optical Users table, choose **Administration > Logged In Users** (or click the **Show Logged In Users** tool).
- Step 3** In the Logged In Users table, select the user whose session will be ended and choose **Administration > Log Out User** (or click the **Log Out User** tool).



Note

If you are logged in as an Operator, you cannot log out a SuperUser.

- Step 4** Click **Yes** at the following prompt:

This operation will log out the selected Prime Optical user. The process will take approximately 1 minute and this Prime Optical client will be unusable until then. Do you want to continue?

Wait while the Prime Optical server logs out the selected Prime Optical client. The Prime Optical GUI is frozen for approximately 1 minute until the request is complete.

8.3.3.7 Viewing a List of Failed Login Attempts

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Prime Optical Users table, choose **Administration > Failed Login Attempts** (or click the **Show Failed Login Attempts** tool). The Failed Login Attempts table opens. The following table provides descriptions.
- Step 3** To unlock a locked IP address, select the IP address and choose **Administration > Unlock** (or click the **Unlock User** tool). This re-enables login attempts for the selected IP address. When an IP address is unlocked, the Login Failed Attempts value is reset to zero and the Last Login Failed Time value is set to N/A.
-

Table 8-6 Field Descriptions for the Failed Login Attempts Table

Field	Description
USERNAME	User name of the user who attempted to log in.
CLIENT ADDRESS	IP address of the user who attempted to log in.
TIMESTAMP	Time at which the user attempted to log into the Prime Optical client and failed.

8.3.3.8 Locked User Account

By default, Prime Optical allows users a maximum of five login attempts from the same IP address within a minute. The user account is locked after the fifth unsuccessful login attempt. The lockout duration is one minute, after which the account is automatically unlocked.

When the Prime Optical Server is shut down, it is possible to configure maximum login attempts and the time interval by modifying the settings in the throttlingContext.xml file located at the following path: PrimeOpticalServer/tomcat/webapps/SSO/WEB-INF/spring-configuration/

8.3.3.9 Changing Your User Password



Note

This functionality is disabled when Prime Optical is installed as part of Prime Central.

Prime Optical users can use the Change Password dialog box to change their Prime Optical passwords. The password change applies to the Prime Optical user who is currently logged in. There is an enforced password change request when the default user logs in for the first time. If the user does not change the password, the Prime Optical session is canceled.



Note

- The password complexity is configurable in the **Control Panel > Security Properties** pane.
- It is possible to set up the user account such that the change password function is disabled. See the description of the Password Change field in [8.3.3.2 Creating a Prime Optical User, page 8-15](#).

Complete the following steps to change your user password:

-
- Step 1** In the Prime Optical web client window, choose **Administration > Change Password**.
- Step 2** To change the Prime Optical password:
- In the Change Password dialog box, enter the current password in the Current Password field.
 - Enter the new password in the New Password field. For password constraints, see [Table 8-7](#).
 - Confirm the new password.
-

Table 8-7 Field Descriptions for the Change Password Dialog Box

Field	Description
Password	
Current Password	Enter the old user password.
New Password	<p>Enter the new login password. The password complexity is configurable in the Control Panel > Security Properties pane. By default, the new password must:</p> <ul style="list-style-type: none"> Contain at least six characters, but not more than 15 characters. Contain at least two alphabetic characters (A–Z, a–z). Of the alphabetic characters, at least one must be uppercase and one must be lowercase. Contain at least one numeric character (0–9). Contain at least one special character (+ # % , . ; & !). The default special character set is TL1+UNIX. Allow a special character as the first or last character. Allow a numeric character as the first or last character. Not contain the username or any circular shift of the username. An uppercase letter and its corresponding lowercase letter are considered equivalent. For example, if the username is Arthur, the password cannot contain the string arthur, rthura, thurar, hurart, urarth, or rarthu. Differ from the old password by at least three characters. For example, if the old password is MikeBrady5!, the new password cannot be mikebrady5% because only the last character is different. However, the new password MikeBrady2!99 is acceptable because it differs from MikeBrady5! by three characters. <p>Note By default, the minimum time between password changes is 20 days. The new password must differ from the previous password by 3 characters, and the new password is compared against the previous 10 passwords.</p>
Confirm Password	Retype the password to confirm it.

8.3.3.10 Managing Security Advisory Messages

Use the Security Advisory Message Management wizard to choose a CTC-based NE from which a security advisory message can be loaded. The wizard then provides you with a list of NEs where the user can download this security message. When you click **Finish**, Prime Optical schedules a job for this action, and the security message downloaded to each selected NE is tracked as a separate task on the Job Monitor table.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs > Security Advisory Management**. The Security Advisory Message Management wizard opens. The following table provides descriptions.
- Step 2** Select the NE where the security advisory message exists.
- Step 3** Click the **Text** tab to view the existing security advisory message on the selected NE. If no message exists, you can use this field to enter a new message.
- Step 4** Click **Next**.
- Step 5** Use the **Add** and **Remove** buttons to move NEs to or from the Selected NE(s) list.
- Step 6** Click **Finish**.
-



Note

You can also use the NE Explorer node view to set the security advisory message for CTC-based NEs. In the node properties pane, click the **Security** tab. In the **Legal Disclaimer** subtab, there is a default advisory message that is noncustomer-specific. Change the text if you want the disclaimer to be specific for your company. In the **Preview** subtab, you can view the advisory message before saving it. Click **Apply**.

Table 8-8 Field Descriptions for the Security Advisory Message Management Wizard

Field	Description
Select an NE to View the Security Advisory Message Pane	
Select NE	NE where the security advisory message exists.
	Note If you opened the Security Advisory Message Management wizard after selecting an NE, only that NE will appear in this list.

Table 8-8 Field Descriptions for the Security Advisory Message Management Wizard (continued)

Field	Description
Text	<p>Security advisory message present on the selected NE. If no message exists, you can use this tab to enter a new message.</p> <p>You can use the following HTML commands to format the text:</p> <p><code></code> Begins boldface font</p> <p><code></code> Ends boldface font</p> <p><code><center></code> Aligns type in the center of the window</p> <p><code></center></code> Ends the center alignment</p> <p><code><font=n, where n = point size></code> Changes the font to the new size</p> <p><code></code> Ends the font size command</p> <p><code><p></code> Creates a line break</p> <p><code><sub></code> Begins subscript</p> <p><code></sub></code> Ends subscript</p> <p><code><sup></code> Begins superscript</p> <p><code></sup></code> Ends superscript</p> <p><code><u></code> Starts underline</p> <p><code></u></code> Ends underline</p>
Preview	View the advisory message before saving it.
Save the Security Advisory Message Pane	
Available NE(s)	Select one or more NEs in the Available NE(s) list and click Add to move them to the Selected NE(s) list. The advisory message is saved for the NEs in the Selected NE(s) list.
Selected NE(s)	Select one or more NEs in the Selected NE(s) list and click Remove to move them to the Available NE(s) list.

8.3.3.11 Setting User Preferences

Use the User Preferences dialog box to configure the Prime Optical user interface.

-
- Step 1** In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box opens. The following table provides descriptions.
- Step 2** After specifying the settings, check the **Save Current Settings** check box to preserve the current settings even after logging out. Users with the appropriate privileges can check the **Save as Default User Template** check box to save the current settings as the default for new users who are added in the future. Current users who have not altered their default settings adopt the new default settings when they log out.
- Step 3** Click **OK** to save the settings. After you save the selections, all subsequent views use the saved preferences.
-

Table 8-9 *Field Descriptions for the User Preferences Dialog Box*

Field	Description
Event Notification Tab	
Show Notification Dialog For	<p>Select whether an alert popup displays when a specific alarm or event occurs on NEs in your management domain or on the EMS. You can specify the alarm severity that will generate an alert popup, and whether to include cleared alarms.</p> <p>Note Selections that apply to NEs are allowed only if you have NEs assigned to you. Selections that apply to the EMS are allowed only if you have the appropriate user privilege.</p>
Play Audible Notification For	<p>Select whether an audible alert sounds when a specific alarm or event occurs on an NE or on the Prime Optical application. You can specify the alarm severity that will generate an audible alert, and whether to include cleared alarms. Check the Continuous Alarm for Dashboard Notifications check box to enable continuous audible notification whenever a new update occurs in the Dashboard window. Uncheck this check box to disable continuous audible notifications.</p> <p>Note Selections that apply to NEs are allowed only if you have NEs assigned to you. Selections that apply to the EMS are allowed only if you have the appropriate user privilege.</p>
Miscellaneous Tab	
Display Log/15-Min PM Data For	<p>Change the time period used to display time-sensitive data in 15-minute increments.</p> <p>Note This field is visible only if you have read permission for the Performance Monitor operation.</p> <p>Note If you change the time setting from a shorter time period to a longer time period (for example, from Past 4 Hours to Past 30 Days), you must click Refresh Data in the log window to retrieve the data, even if the Auto Refresh feature is enabled. This behavior is by design, because if there are thousands of nodes under management, it takes a long time to retrieve the data. Prime Optical does not begin retrieving the data until you click Refresh Data manually.</p>
Display 1-Day PM Data For	<p>Change the time period used to display time-sensitive data in 24-hour increments.</p> <p>Note This field is visible only if you have read permission for the Performance Monitor operation.</p>
Table Export Encoding	<p>Change the encoding to use when you export a table to a text file. Options are:</p> <ul style="list-style-type: none"> • Default—The encoding (that is, the translation from a character to the sequence of 0s and 1s that represent it in byte format) used by default. Default encoding depends on various factors, including the locale and the region of the Operating System (OS) running on the machine. Default encoding can only write characters belonging to that specific locale and region. Default encoding has the advantage that all OS applications can correctly read the text file generated by this encoding. • UTF-8—Unicode Transformation Format-8 (UTF-8) is an octet (8-bit) lossless encoding of unicode characters. It encodes each character as a variable number of 1 to 4 octets, where the number of octets depends on the integer value assigned to the unicode character. UTF-8 is the default encoding for XML. UTF-8 is an encoding independent from OS, locale, and region; is standardized by the Unicode consortium; and can write any unicode character in 1, 2, or 3 bytes, depending on the character itself.

Table 8-9 Field Descriptions for the User Preferences Dialog Box (continued)

Field	Description
Enable Refresh Data Timer	<p>The automatic Refresh Data feature automatically refreshes all data being displayed by Prime Optical. You receive the following prompt:</p> <p>Refresh Data action suggested. This action will result in closing all windows and might take some time. Do you want to continue? {Yes No}</p> <p>In an unstable environment where NEs are synchronizing or NEs change their operational state frequently, you might receive the preceding prompt continuously. To disable the prompt, uncheck the Enable Refresh Data Timer check box.</p>
Do Not Display User Profile Creation Warning Messages	<p>Enable or disable the warning dialog box that pops up when you click Finish after creating or modifying a user profile. The warnings are still visible in the User Profile table.</p>
Enable NE Aliases	<p>When checked, it allows you to view the alias names for the following attributes:</p> <ul style="list-style-type: none"> • Node ID • Link name • Circuit name <p>The alias name can be displayed instead of the NE ID in the following windows:</p> <ul style="list-style-type: none"> • Domain Explorer—Tree and Identification tab of the Network Element Properties pane • Subnetwork Explorer—Tree and Identification tab of the Network Element Properties pane • Network Map

Time Preferences Tab

Note This functionality is disabled when Prime Optical is installed as part of Prime Central.

Time Display	<p>Select 12-hour format or 24-hour format for the display of time information. Options are:</p> <ul style="list-style-type: none"> • 12 Hour—Displays time information in 12-hour format; for example, 01:30 PM. • 24 Hour—Displays time information in 24-hour format; for example, 13:30. • Use System Locale—Displays time information in 12-hour format or 24-hour format, depending on the default for the system locale.
Time Zone for Date	<p>Select the time zone for the date display (<i>month/day/year</i> or <i>day/month/year</i>). Options are:</p> <ul style="list-style-type: none"> • Local—Displays the date according to the time zone that is configured on the workstation where the Prime Optical client is running. • GMT—Displays the date according to the GMT time zone (<i>day/month/year</i>). • User Defined—Specify a fixed offset from GMT. The offset range is –12 to +13 hours from GMT, in one-hour increments. For offsets other than zero, specify a display string of four characters maximum.

Map Preferences Tab

Open Network Map in New Window	<p>Within network map views, this setting specifies whether to open subsequent frames in the same window, or open a new window for subsequent map views.</p>
Show Off-View Icons	<p>Within map views, this setting enables or disables the display of off-view icons. If an NE has a link defined to an NE on a different map, the off-view NE is represented by an off-view icon. The off-view icon serves as a hyperlink to the map that contains the NE at the opposite end of the link. Off-view icons are used only for links that terminate on an NE; off-view icons are not used for subnetworks or groups.</p>

Table 8-9 Field Descriptions for the User Preferences Dialog Box (continued)

Field	Description
Minimum Icon Size	Specify a fixed and locked pixel size for icons in network maps. Choices are 8x8, 16x16, 24x24, and 32x32. Regardless of the zoom level, the map icon size does not change when it is set to a fixed size. By default, the icon size is variable based on the zoom level. The icon size setting is saved with the other map settings.
FM Preferences Tab	
Color Entire Row in Table View	Set the Alarm Browser or Alarm Log to full background color for the entire selected row. The color corresponds to the alarm status and severity.
Enable Export of Entire Table	Enable or disable the ability to export the entire contents of the Alarm Browser or the Alarm Log. It might take longer to open the Alarm Browser or Alarm Log with the export entire table feature enabled.

8.3.3.12 Enabling or Disabling the Continuous Audible Alarm

-
- Step 1** In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box opens.
- Step 2** In the Event Notification tab > Play Audible Notification For area, check the **Continuous Alarm For Dashboard Notifications** check box.
- Step 3** Click **OK**.
- Step 4** To disable the continuous audible alarm, choose **Fault > Stop Continuous Beep** in the Domain Explorer window.
-

8.3.3.13 Configuring Prime Optical Security Parameters

Use the Security Properties pane to configure Prime Optical security parameters and password complexity rules. You can also specify usernames and passwords for the ONS 15216 EDFA2, ONS 15216 EDFA3, ONS 15216 OADM, ONS 155xx, ONS 15305 CTC, ONS 15310 CL, ONS 15310 MA SONET, ONS 15310 MA SDH, ONS 15327, ONS 15454 SONET, ONS 15454 SDH, ONS 15600 SONET, ONS 15600 SDH, CPT 200, CPT 200 SDH, CPT 600, and CPT 600 SDH.



Note

- Passwords that are already in the system are not affected by modifications to the password complexity rules. The password complexity rules are checked when:
 - A privileged user adds a new user to the system
 - A privileged user modifies an existing user's password
 - A user changes his or her own existing password

- Regardless of the actual length of the password, the Password and Confirm Password fields display only a fixed-length string of 15 asterisks (*).

Complete the following steps to configure Prime Optical security properties:

- Step 1** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 2** Click **Security Properties** and set the parameters described in the following table. Tabs shown depend on the modules that are installed.



Note

If there are many tabs displayed in the properties pane, select the arrow or Show List icons to view all available tabs.

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

Table 8-10 Field Descriptions for the Security Properties Pane

Field	Description
Security Tab	
Note This functionality is disabled when Prime Optical is installed as part of Prime Central.	
Password Aging Area	
Password Aging	Number of days before the password expires. The user is prompted to change the password after the specified number of days. The range is from 0 to 3650 days; the Cisco default is 30 days. A value of 0 disables this feature.
Password Expiration Early Notification	Allows you to configure an early warning period for password expiration. Enter the number of days before the warning in the Password Expiration Early Notification field. Prime Optical supports values of 0 to (password aging - 1), with a maximum of 30. For example, if the password aging is configured for 30 days, the maximum early notification value would be 29 days. A value of 0 disables this feature.
Client Inactivity Timer Settings Area	
Logout Enable	If checked, Prime Optical automatically logs the user out of the Prime Optical session after the period in the Logout Period field.
Logout Period	Number of minutes a user's Prime Optical session is inactive before Prime Optical automatically logs the user out. The range is from 1 to 1440 minutes in 1-minute increments.
Prime Optical Password Rules Tab	
Note This functionality is disabled when Prime Optical is installed as part of Prime Central.	
Password Change Rules Area	
Interval Between Password Change	Number of days a user must wait between password changes. The range is from 0 to 99 days; the Cisco default is 1 day. A value of 0 disables this feature.
Differ From Previous Password by <i>n</i> Characters	Number of characters by which the new password must differ from the previous one. The range is from 1 to 5 characters; the Cisco default is 3 characters.
Compare Against Previous <i>n</i> Passwords	Number of previously used passwords to compare against the new password. The range is from 0 to 15 passwords; the Cisco default is 5 passwords. A value of 0 disables this feature.

Table 8-10 **Field Descriptions for the Security Properties Pane (continued)**

Field	Description
Password Complexity Rules Area	
Minimum Password Length	Minimum password length. The range is from 2 to 10 characters; the Cisco default is 6 characters.
Maximum Password Length	Maximum password length. The range is from 10 to 15 characters; the Cisco default is 12 characters.
Number of Alphabetic Characters	Minimum number of alphabetic characters that the password must include. The range is from 0 to 2; the Cisco default is 2 alphabetic characters.
Number of Lowercase Alphabetic Characters	Minimum number of lowercase alphabetic characters that the password must include. The range is from 0 to 2; the Cisco default is 1 lowercase character.
Number of Uppercase Alphabetic Characters	Minimum number of uppercase alphabetic characters that the password must include. The range is from 0 to 2; the Cisco default is 1 uppercase character.
Number of Numeric Characters	Minimum number of numeric characters that the password must include. The range is from 0 to 2; the Cisco default is 1 numeric character.
Number of Special Characters	Minimum number of special characters that the password must include. The range is from 0 to 2; the Cisco default is 1 special character.
Special Character Set to Use	Special character set to use: <ul style="list-style-type: none"> • TL1—Special characters permitted are + # % • UNIX—Special characters permitted are , . ; % & ! • TL1+ UNIX—(Cisco default) Special characters permitted are , . ; % & ! + # • ASCII—Special characters permitted are @ ` ! " # \$ % & ' () * : + ; [{ , < \ - =] } . > ^ ~ / ? _
Allow Special First or Last Character	If checked, a special character is allowed as the first or last character in the password. If unchecked, the first or last character in the password cannot be a special character.
Allow Numeric First or Last Character	If checked, a numeric character is allowed as the first or last character in the password. If unchecked, the first or last character in the password cannot be a number.
Allow User ID Circular Shift	If checked, the user ID or a circular shift of the ID can be used in the password. If unchecked, the user ID or a circular shift of the ID cannot be used in the password.
ONS 15216 EDFA2 Tab	
Username	Username that the Prime Optical server uses to connect to ONS 15216 EDFA2 NEs.
Password	Password to use for Prime Optical server connections to ONS 15216 EDFA2 NEs.
Confirm Password	Re-enter the password to confirm it.
ONS 15216 EDFA3 Tab	
Server - NE Connection Username	Username that the Prime Optical server uses to connect to ONS 15216 EDFA3 NEs. Note The ONS 15216 EDFA3 has a TL1 interface and multiple usernames can be defined for authentication. Each username can be used for only one active connection. A second connection with the same username is not allowed. The current user must log out before another user can log in with that username.
Password	Password to use for Prime Optical server connections to ONS 15216 EDFA3 NEs.
Confirm Password	Re-enter the password to confirm it.

Table 8-10 Field Descriptions for the Security Properties Pane (continued)


Field	Description
Prime Optical Server - FTP Connection Username	<p>Username that the Prime Optical server uses to connect to FTP for software download, memory backup, and memory restore.</p> <p> Caution An FTP account must already exist on the server in order for the file transfer to work correctly.</p>
Password	Password to use for Prime Optical server connections to FTP.
Confirm Password	Re-enter the password to confirm it.
FTP Directory	Absolute path for the FTP directory, beginning with a forward slash (/).
ONS 15216 OADM Tab	
Server - NE Connection Username	<p>Username that the Prime Optical server uses to connect to ONS 15216 OADM NEs.</p> <p>Note The ONS 15216 OADM has a TL1 interface and multiple usernames can be defined for authentication. Each username can be used for only one active connection. A second connection with the same username is not allowed. The current user must log out before another user can log in with that username.</p>
Password	Password to use for Prime Optical server connections to ONS 15216 OADM NEs.
Confirm Password	Re-enter the password to confirm it.
CTC-Based SDH Tab	
Username	<p>Username that the Prime Optical server uses to connect to ONS 15305 CTC, ONS 15310 MA SDH, ONS 15454 SDH, ONS 15600 SDH, CPT 200 SDH, and CPT 600 SDH NEs. By default, NEs are configured with the username <i>CISCO15</i>.</p> <p>Note The account specified on the NE for Prime Optical to use must be a SuperUser-level account.</p> <p>For the ONS 15310 MA SDH and ONS 15454 SDH, this tab also contains Username fields for Prime Optical server connections to ML-series cards and for Prime Optical server connections to TL1 tunnel NEs.</p> <p>Note The default username is configured as <i>CISCO15</i> for the ML cards specified in the default Cisco IOS configuration file. The Cisco IOS configuration file is included in the Prime Optical server installation CD (misc/bareboneCLI_Security.txt). By default, the username for all connections is configured as <i>CISCO15</i>.</p>
Password	<p>Password to use for Prime Optical server connections.</p> <p>For the ONS 15454 SDH, this is also the password to use for ML-series card and TL1 tunnel NE connections.</p> <p>Note The default password is configured as CTM123+ for the ML cards specified in the default Cisco IOS configuration file.</p>
Confirm Password	Re-enter the password to confirm it.
CTC-Based SONET Tab	

Table 8-10 **Field Descriptions for the Security Properties Pane (continued)**

Field	Description
Username	<p>Username that the Prime Optical server uses to connect to ONS 15310 CL, ONS 15310 MA SONET, ONS 15327, ONS 15454 SONET, ONS 15600 SONET, CPT 200, and CPT 600 NEs. By default, NEs are configured with the username <i>CISCO15</i>.</p> <p>Note The account specified on the NE for Prime Optical to use must be a SuperUser-level account.</p> <p>For the ONS 15310 CL, ONS 15310 MA SONET, and ONS 15454 SONET, this tab also contains a Username field for Prime Optical server connections to ML-series cards.</p> <p>For the ONS 15310 CL, ONS 15310 MA SONET, ONS 15327, and ONS 15454 SONET, this tab also contains a Username field for Prime Optical server connections to TL1 tunnel NEs.</p>
Password	<p>Password to use for Prime Optical server connections.</p> <p>For the ONS 15310 CL, ONS 15310 MA SONET, and ONS 15454 SONET, this tab also contains a Password field for Prime Optical server connections to ML-series cards.</p> <p>For the ONS 15310 CL, ONS 15310 MA SONET, ONS 15327, and ONS 15454 SONET, this tab also contains a Password field for Prime Optical server connections to TL1 tunnel NEs.</p>
Confirm Password	Re-enter the password to confirm it.
CTC-Based SDH and CTC-Based SONET Tabs	
Server - SNMP Connection Area	
<p>Note After changing the field values in the Server - SNMP Connection area, mark the NEs as Out of Service and then In Service.</p>	
SNMPv3	Check this check box to use SNMPv3. If unchecked, Prime Optical uses SNMPv1/v2.
Username	Name of the Prime Optical user who is enabled for SNMPv3 communication.
Authentication Protocol	Select the authentication protocol to use for authenticating the SNMPv3 user. Values are None, MD5, or SHA.
Authentication Password	<p>Enter the password used to authenticate the SNMPv3 user. The password must contain:</p> <ul style="list-style-type: none"> • From 1 to 12 characters • At least one special character other than an apostrophe (') • At least two letters (A-Z, a-z), including at least one uppercase letter • At least one number (0-9) <p>Regardless of the actual length of the password, the Password and Confirm Password fields display only a fixed-length string of 15 asterisks (*).</p>
Confirm Authentication Password	Re-enter the authentication password to confirm it.
Privacy Protocol	<p>Select the privacy protocol for the SNMPv3 user. You can choose one of the following:</p> <ul style="list-style-type: none"> • NONE—No privacy protocol for the user. • DES—Use Data Encryption Standard (DES) for encryption.
Privacy Password	Enter the password used to decrypt the message payload.
Confirm Privacy Password	Re-enter the privacy password to confirm it.

8.3.3.14 Sending Messages to Other Users

Use the Notify Users dialog box to type and send a message to all Prime Optical users, or to all Prime Optical users with the same user privileges. For example, you might want to alert all users before shutting down the Prime Optical server.

The following table provides descriptions.

-
- | | |
|---------------|--|
| Step 1 | In the Domain Explorer window, choose File > Notify Users . The Notify Users dialog box opens. |
| Step 2 | In the Message Targets area, select the recipients of the message. |
| Step 3 | Type the message in the Message area. <ul style="list-style-type: none"> • To send the message to the specified recipients, click Send. • To cancel the message and close the dialog box, click Cancel. • To launch the online help for the Notify Users dialog box, click Help. |
-

Table 8-11 *Field Descriptions for the Notify Users Dialog Box*

Field	Description
Message Targets	Select recipients for your message. This list includes the default NetworkAdmin, Operator, Provisioner, SuperUser, and SysAdmin profiles, as well any custom user profile that has been generated. You can select custom and multiple profiles by using the Shift and Control keys while clicking the profile, or click the All Users radio button to send your message to all users, regardless of user type.
Message	Type your message. The maximum length is 512 characters. If you enter a message that is longer than 512 characters, only the first 512 characters are sent.

8.3.3.15 Viewing User Notification Messages

The User Notification dialog box pops up on your screen when another user sends a message to a certain user profile or to all Prime Optical users, and you belong to one of those groups. The following table provides descriptions.

Table 8-12 *Field Descriptions for the User Notification Dialog Box*

Field	Subfield	Description
Message Received	From	Username of the user who sent you the message.
	Time	Date and time when you received the message.
Message	—	Text of the message. The maximum message length is 512 characters.

8.3.4 Managing Prime Optical User Profiles

The following sections describe how to view, add, modify, delete, and duplicate a Prime Optical user profile.

8.3.4.1 Viewing User Profiles

The Prime Optical User Profiles table displays basic information about Prime Optical user profiles. Use the menu options to manage user profiles.

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Prime Optical Users table, choose **Administration > User Profiles** (or click the **Launch User Profiles Table** tool). The following table provides descriptions.

Table 8-13 *Field Descriptions for the Prime Optical User Profiles Table*

Field	Description
User Profile Name	Name of the existing Prime Optical user profiles.
NE Assignment	NE assignment for the selected user profile. NE assignments are: <ul style="list-style-type: none"> • Assign all NEs—SuperUser, NetAdmin • Assign NEs—Operator, Provisioner • Assign No NEs—SysAdmin
Default Login Sessions	Number of permitted simultaneous logins assigned to the user profile: <ul style="list-style-type: none"> • 1—Only one user with a given profile can log into a specific Prime Optical server at a time. • 2 to 10—The specified number of users (2 to 10) with a given profile can log into a specific Prime Optical server simultaneously. • Unlimited—An unlimited number of users with a given profile can log into a specific Prime Optical server simultaneously.
User Profile Description	Description of the user profile.

8.3.4.2 Adding a Custom User Profile

Use the Create New User Profile wizard to add Prime Optical user profiles. [Table 8-14](#) provides descriptions.

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Cisco Prime Optical Users table, choose **Administration > User Profiles** (or click the **Launch User Profiles Table** tool).
- Step 3** In the Cisco Prime Optical User Profiles table, choose **Edit > Create** (or click the **Create a New User Profile** tool).
- Step 4** In the Create New User Profile wizard, specify the following:
- User profile name
 - NE assignment
 - Max user sessions allowed
 - Description
- Step 5** Click **Next**.
- Step 6** Select a user profile category from the Categories area. Operations for each category are displayed on the right side of the Categories area.
- Step 7** Specify user capabilities by setting permission or privileges for one or all operations. When setting privileges for each operation, select one of the following radio buttons:
- Read Only
 - Read/Write

- No Access

When setting privileges for all operations, select one of the following buttons:

- Set All Read Only
- Set All Read/Write
- Set All No Access



Note

The user profile operations displayed on the right side of the Create New User Profile wizard depend on the category selected. You can select the root node to see all the operations for all categories.

Step 8 Click **Finish**.

Step 9 Click **Yes** in the message box. (The message box will not be displayed if it is disabled in the User Preferences dialog box. See [8.3.3.11 Setting User Preferences, page 8-26](#) for more information.)

Table 8-14 Field Descriptions for the Create New User Profile Wizard

Field	Description
User Profile Name	Enter the name of the new user profile. The profile name must contain from six to twenty alphanumeric characters (A–Z, a–z, 0–9). Alphabetic characters are case-sensitive. The profile name must be unique in Prime Optical and cannot contain spaces or special characters.
NE Assignment	The NE assignment for the new user profile. Values are: <ul style="list-style-type: none"> • Assign All NEs—SuperUser, NetworkAdmin • Assign NEs—Operator, Provisioner • Assign No NEs—SysAdmin
Max User Sessions Allowed	Select 1 to allow only one user with the selected user profile to log into a specific Prime Optical server. Select a number other than 1 to allow the specified number of users to log into a specific Prime Optical server simultaneously. Select Unlimited if you do not want to restrict the number of users with the selected profile from logging into a specific server simultaneously.

Table 8-14 Field Descriptions for the Create New User Profile Wizard (continued)

Field	Description
Description	Enter a description of the new user profile.
User Profile Privileges	<p>Set user privileges for specific Prime Optical categories. Select a category in the left panel to display that category's available operations. Select an operation from the Operations column; then, select a user privilege for the selected operation from the radio buttons in the Privileges column.</p> <ul style="list-style-type: none"> Set All Read Only—Specifies that the user can only view information related to all the operations with Read Only privilege listed under the specified category. All other operations will be set to No Access. Set All Read/Write—Specifies that the user can view and perform any of the operations with Read/Write privilege listed under the specified category. All other operations will be set to Read Only. Set All No Access—Specifies that the user is not allowed to perform any of the operations with No Access privilege listed under the specified category. All other operations will be set to Read Only. <p>The Warning column lists the dependencies between various operations. After you click Finish to create the new user profile, a warning dialog box lists all of the warning messages. If you check the Don't Display User Profile Creation Warning Messages check box, the warning dialog box does not appear for subsequent user profile creations in the current client session. If you check the Don't Display User Profile Creation Warning Messages check box in the User Preferences dialog box, the warning dialog box is disabled as specified for the current user or as a template for new users.</p>

8.3.4.3 Modifying a User Profile

Use the Modify User Profile wizard to modify Prime Optical user profiles. [Table 8-15](#) provides descriptions.



Note

Users created with a certain profile cannot be changed to another profile. To change profiles, the user must be deleted, then recreated with the new profile.



Note

Modifying a profile will log out all users who are logged in with that profile.

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Cisco Prime Optical Users table, choose **Administration > User Profiles** (or click the **Launch User Profiles Table** tool).
- Step 3** In the Cisco Prime Optical User Profiles table, click the profile to modify; then, choose **Edit > View/Modify** (or click the **View/Modify User Profile Properties** tool).
- Step 4** In the Modify User Profile wizard, modify the following:
- NE assignment
 - Max user sessions allowed
 - Description


- Step 5** Click **Next**.
- Step 6** Select a user profile category from the Categories area. Operations for each category are displayed on the right side of the Categories area.
- Step 7** Specify user capabilities by setting permission or privileges on one or all operations. When setting privileges for each operation, select one of the following radio buttons:
- Read Only
 - Read/Write
 - No Access
- When setting privileges for all operations, select one of the following buttons:
- Set All Read Only
 - Set All Read/Write
 - Set All No Access
-  **Note** The user profile operations displayed on the right side of the Modify User Profile wizard depend on the category selected. You can select the root node to see all the operations for all categories.
- Step 8** Click **Finish**.
- Step 9** Click **Yes** in the message box. (The message box will not be displayed if it is disabled in the User Preferences dialog box. See [8.3.3.11 Setting User Preferences, page 8-26](#) for more information.)

Table 8-15 *Field Descriptions for the Modify User Profile Wizard*

Field	Description
User Profile Name	<i>Display only.</i> Name of the user profile. The profile name must contain from six to twenty alphanumeric characters (A–Z, a–z, 0–9). Alphabetic characters are case-sensitive. The profile name must be unique in Prime Optical and cannot contain spaces or special characters.
NE Assignment	The NE assignment for the user profile. Values are: <ul style="list-style-type: none"> • Assign all NEs—SuperUser, NetAdmin • Assign NEs—Operator, Provisioner • Assign No NEs—SysAdmin Only Assign NEs is available for new profiles, meaning that NEs or groups must always be assigned to the new profile.
Max User Sessions Allowed	Select 1 to allow only one user with the selected user profile to log into a specific Prime Optical server. Select a number other than 1 to allow the specified number of users to log into a specific Prime Optical server simultaneously. Select Unlimited if you do not want to restrict the number of users with the selected profile from logging into a specific server simultaneously.

Table 8-15 Field Descriptions for the Modify User Profile Wizard (continued)

Field	Description
Description	Modify the description of the user profile.
User Profile Privileges	<p>Modify selected user privileges for specific Prime Optical categories. Select a category in the left panel to display that category's available operations. Select an operation from the Operations column, then select a user privilege for the selected operation from the radio buttons in the Privileges column.</p> <ul style="list-style-type: none"> Set All Read Only—Specifies that the user can only view information related to all the operations with Read Only privilege listed under the specified category. All other operations will be set to No Access. Set All Read/Write—Specifies that the user can view and perform any of the operations with Read/Write privilege listed under the specified category. All other operations will be set to Read Only. Set All No Access—Specifies that the user is not allowed to perform any of the operations with No Access privilege listed under the specified category. All other operations will be set to Read Only. <p>The Warning column lists the dependencies between various operations. After you click Finish to modify the user profile, a warning dialog box lists all of the warning messages. If you check the Don't Display User Profile Creation Warning Messages check box, the warning dialog box does not appear for subsequent user profile modifications in the current client session. If you check the Don't Display User Profile Creation Warning Messages check box in the User Preferences dialog box, the warning dialog box is disabled as specified for the current user or as a template for new users.</p> <p>Note Topology modification is not allowed for custom users.</p>

8.3.4.4 Deleting a User Profile

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Cisco Prime Optical Users table, choose **Administration > User Profiles** (or click the **Launch User Profiles Table** tool).
- Step 3** In the Cisco Prime Optical User Profiles table, select the profile you want to delete; then, choose **Edit > Delete** (or click the **Delete User Profile** tool).
- Step 4** In the confirmation dialog box, click **OK**.
-



Note

The default user profiles (SuperUser, SysAdmin, NetworkAdmin, Provisioner, and Operator) cannot be deleted. Custom user profiles cannot be deleted if they are assigned to any user. Delete the user with the custom user profile before deleting the user profile. See [8.3.3.4 Deleting a Prime Optical User, page 8-21](#).

8.3.4.5 Duplicating a User Profile

Use the Create Duplicate Profile window to duplicate an existing Prime Optical user profile.

-
- Step 1** In the Domain Explorer window, choose **Administration > Users**.
- Step 2** In the Cisco Prime Optical Users table, choose **Administration > User Profiles** (or click the **Launch User Profiles Table** tool).
- Step 3** In the Cisco Prime Optical User Profiles table, select the profile you want to duplicate; then, choose **Edit > Duplicate** (or click the **Duplicate User Profile** tool).
- Step 4** In the Create Duplicate Profile dialog box, enter the duplicate profile name. See the following table for name constraints.
- Step 5** Click **OK**.
-

Table 8-16 Field Descriptions for the Create Duplicate Profile Window

Field	Description
Duplicate Profile Name	The name of the duplicate user profile must contain from six to twenty alphanumeric characters (A–Z, a–z, 0–9). Alphabetic characters are case-sensitive. The profile name must be unique in Prime Optical and cannot contain spaces or special characters.

8.4 NE Security Management

This section describes NE security, including setting authentication on an NE, setting up a security policy, using log tables, and managing NE user access.

8.4.1 Setting NE Authentication

Use the NE Authentication dialog box to select the security properties (username and password for each authentication session) for multiple NEs. For each ONS 15000 NE that supports authentication, there is a specific Security tab in the Control Panel window.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs, ONS 15216, ONS 155XX > NE Authentication**. The NE Authentication dialog box opens. The following table provides descriptions. Fields shown depend on the NE that is selected.
- Step 2** Specify the NEs that you will set a username and password authentication for. Click **Add** to add NEs to the Selected NEs list, or click **Remove** to remove NEs from the list.
- Step 3** In the Server - NE Connection area, enter the following information:



Note The username and password that you enter must have Superuser privileges on the node to enable full Prime Optical access to the NE.

- Enable—Check the **Enable** check box to set a username and password that the Prime Optical server will use to establish a connection with the selected NEs.
- Username
- Password (and confirm password)

Step 4 In the Server - TL1 Tunnel GNE Connection area, enter the following information:

- Enable—Check the **Enable** check box to set a GNE TL1 target identifier (TID), username, and password that the Prime Optical server will use to establish a connection with the GNE and reach the selected tunnel NE (TNE).
- GNE TID
- Username
- Password (and confirm password)

Step 5 Click **Save**.

Table 8-17 Field Descriptions for the NE Authentication Dialog Box

Field	Description
Network Elements Area	
Available NEs	List of available NEs.
Selected NEs	List of selected NEs.
Server - NE Connection Area	
Enable	If checked, allows a connection between the Prime Optical server and the NE.
Username	Enter a username for the selected NEs. This field is unavailable if the Enable check box is not checked.
Password	Enter the password for the username. This field is unavailable if the Enable check box is not checked.
Confirm Password	Retype the password. This field is unavailable if the Enable check box is not checked.
Server - TL1 Tunnel GNE Connection Area	
Enable	If checked, specifies a GNE TID, username, and password that the Prime Optical server will use to log into the GNE to set up a TL1 tunnel with the selected TNEs.
GNE TID	Enter the TID of the GNE for the selected TNEs. This field is unavailable if the Enable check box is not checked.
Username	Enter a username for the GNE for the selected TNEs. This field is unavailable if the Enable check box is not checked.
Password	Enter the password for the GNE for the selected TNEs. This field is unavailable if the Enable check box is not checked.
Confirm Password	Retype the password. This field is unavailable if the Enable check box is not checked.



Note

You can also set the NE authentication username and password in the **Domain Explorer > Network Element Properties** pane > **NE Authentication** tab. When changing the username or password of an NE, mark that NE as Out of Service and then In Service.

**Note**

If the username and password fields in the NE Authentication tab are left blank, Prime Optical uses the username and password defined in the Control Panel.

8.4.2 Setting Up a Security Policy

You can set up a security policy for CTC-based NEs.

-
- Step 1** Select a CTC-based NE and choose **Configuration > NE Explorer**.
- Step 2** In the tree view of the NE Explorer window, select the NE node.
- Step 3** In the node properties pane of the NE Explorer window, click the **Security** tab.
- Step 4** Complete the following information in the **Policy** subtab:

- In the Idle User Timeout area:
 - Retrieve—Set the idle user timeout for a CTC Retrieve user.
 - Maintenance—Set the idle user timeout for a CTC Maintenance user.
 - Provisioner—Set the idle user timeout for a CTC Provisioner user.
 - SuperUser—Set the idle user timeout for a CTC SuperUser.

**Note**

Idle time can be from zero to 16 hours, 39 minutes (999 minutes). To deactivate the Idle User Timeout, enter zero as the idle time. A user already logged into the node is not affected by a change to the Idle User Timeout policy.


- In the User Lockout area:
 - Manual Unlock By SuperUser—If checked, the CTC SuperUser user must manually unlock locked out CTC users. If unchecked, locked out CTC users are automatically unlocked after the lockout duration period elapses.
 - Lockout Duration—Set the lockout duration period for locked out CTC users. This field is only enabled if the Manual Unlock by SuperUser check box is unchecked.
 - Failed Logins Allowed—Set the number of failed logins before the CTC user is automatically locked out.
- In the Other area:
 - Single Sessions Per User—If checked, each CTC user can only launch one session at a time.
 - Disable Inactive User—If checked, inactive users will be disabled automatically.
 - Inactive Duration—If Disable Inactive User is checked, specify the inactive duration. The range is from 1 to 99 days; the Cisco default is 45 days.

- Step 5** Complete the following information in the **Password** subtab:

- In the Password Change area:
 - Prevent Reusing Last—Prevents setting a CTC user's current password to one of the most recent passwords. You can set the number of most recent passwords that cannot be reused.

- Disable Password Flipping—If checked, users cannot change passwords for the number of days specified in the Can Change Password After field.
- Can Change Password After—Enter the number of days that must elapse before the user can change the password.
- Force Password Change After Assigned—If checked, during the first successful login, the user is forced to change the password.
- Password Difference—Enter the number of characters by which the new password of a user must differ from the old password, while performing a password change. The default value is 1. The range is from 1 to 5 characters.
- In the Password Aging Area:
 - Enable Password Aging—Check this check box to enable password aging.
 - Aging Period—Enter the aging period, in days, for Retrieve, Maintenance, Provisioner, and SuperUser CTC users. After the aging period expires, CTC users are forced to change their passwords.
 - Warning Period—Enter the warning period, in days, for Retrieve, Maintenance, Provisioner, and SuperUser CTC users. After the warning period expires, CTC users are warned that their passwords will soon expire.

Step 6 Complete the following information in the **Access** subtab for all CTC-based NEs R5.0 or earlier:

- In the Access area:
 - LAN Access—Specify the type of LAN access allowed. Values are Backplane Only, No LAN Access, Front and Backplane, or Front Only.
- 

Note After setting the LAN access to the backplane, the Prime Optical client is unusable for 4 to 5 minutes.

- Restore Timeout—This time period begins if No LAN Access is selected and all DCC connections are lost. If the time expires before a DCC is restored, LAN access is restored so that the node is not isolated. When the DCC comes back, LAN access returns to its specified settings. The range is from 0 (never) to 60 minutes; the Cisco default is 5 minutes.
 - In the Shell Access area:
 - Shell Access On—Specify shell access on Telnet or SSH.
 - Telnet Port—This is enabled if you selected the Telnet radio button. Enter the Telnet port number.
 - SSH Port—*Display only*. Indicates the SSH port number that will be used if the SSH radio button is selected.
 - In the Other area:
 - PM Clearing Privilege—Select the user privilege that allows clearing PM statistics for the NE.

Step 7 Complete the following information in the **Access** subtab for all CTC-based NEs R6.0 or later:

- In the Access area:
 - LAN Access—Specify the type of LAN access allowed. Values are Backplane Only, No LAN Access, Front and Backplane, or Front Only.

**Note**

After setting the LAN access to the backplane, the Prime Optical client is unusable for 4 to 5 minutes.

- Restore Timeout—This time period begins if No LAN Access is selected and all DCC connections are lost. If the time expires before a DCC is restored, LAN access is restored so that the node is not isolated. When the DCC comes back, LAN access returns to its specified settings. The range is from 0 (never) to 60 minutes; the Cisco default is 5 minutes.
- In the Serial Craft Access area:
 - Enable Craft Port—Check this check box to enable the craft port.
- In the Shell Access area:
 - Access State—Select the Shell access state from the drop-down list. You can select Disable, Non-secure, or Secure.
 - SSH Port—*Display only*. Indicates the SSH port number that will be used.
 - SFTP Port—*Display only*. Indicates the SFTP port number that will be used.
 - Telnet Port—This is enabled if you selected the **Non-secure** access state. Enter the Telnet port number that will be used.
 - Use Standard Telnet Port—Check this check box to indicate that the standard Telnet port will be used.
 - Enable Shell Password—*Display only*. Indicates whether the Shell password is enabled. You cannot enable the Shell password in Prime Optical. Enabling and providing a Shell password is currently done in CTC.
- In the EMS Access area:
 - Access State—Select the EMS access state from the drop-down list. You can select either Non-secure or Secure. Then, click **OK** at the following warning message:

When you change the EMS access mode of the NE, Prime Optical resynchronizes the NE connections during the next health poll. If you make provisioning changes to the NE before the resynchronization is complete, the changes might not be saved. Wait for the resynchronization to complete before making any provisioning changes to the NE.

**Note**

When you change the state from Secure to Non-secure or vice versa, the NE might reboot or resynchronize to reflect the changes. During this time, if you try to reapply the other state (Secure to Non-secure or vice versa), the changes might not be saved. The operation requires time to execute successfully.

- CORBA Listener Port—Select the port numbers for the TCC CORBA (IIOP) listener port and the TCC CORBA (SSLIIOP) listener port. Select one of the following radio buttons:
 - Default-Fixed—Assign a default port number.
 - Standard Constant—The port number for the TCC CORBA (IIOP) listener port is 683. The port number for the TCC CORBA (SSLIIOP) listener port is 684.
 - Other Constant—When selected, enter the port number that will be used.
- In the TL1 Access area:
 - Access State—Select the TL1 access state from the drop-down list. You can select Disable, Non-secure, or Secure.

- In the SNMP Access area:
 - Access State—Select the SNMP access state from the drop-down. You can select either Disable or Non-secure.
- In the Other area:
 - PM Clearing Privilege—Select the user privilege that allows clearing PM statistics for the NE.

Step 8 Complete the following in the **RADIUS Server** subtab for all CTC-based NEs R6.0 or later:

- Enable RADIUS Authentication—Check this check box if you want to enable RADIUS authentication.
- Enable RADIUS Accounting—Check this check box if you want to enable RADIUS accounting. This is enabled if the Enable RADIUS Authentication check box is checked.
- Enable the Node as the Final Authenticator When no RADIUS Server is Reachable—Select a row from the RADIUS Servers in Order of Authentication table; then, check this check box. This indicates that the RADIUS server that you selected will be the final authenticator when no other RADIUS servers can be reached.
- Enable Access Challenge—Select a row from the RADIUS Servers in Order of Authentication table; then, check this check box. This indicates that you are enabling access challenge in the RADIUS server that you selected.

The following table describes the fields in the RADIUS Servers in Order of Authentication table.

Click the **Up** and **Down** buttons to reorder the list of RADIUS servers in the table.

See [8.4.2.1 Managing RADIUS Servers, page 8-46](#) for information on how to create, modify, and delete RADIUS servers. You can create a maximum of 10 RADIUS server entries.

Step 9 Complete the following in the **Legal Disclaimer** subtab:

- In the **Advisory Message** subtab, there is a default advisory message that is noncustomer-specific. Change the text if you want the disclaimer to be specific for your company.
- In the **Preview** subtab, you can view the advisory message before saving it.

Step 10 Click **Apply**.

Table 8-18 Field Descriptions for the RADIUS Servers in Order of Authentication Table

Field	Description
IP Address	IP address of the RADIUS server.
Shared Secret	Shared secrets are preshared keys that have been allocated to the communicating parties (the NE and the AAA server) prior to the start of the communication process. Transactions between the NE and the AAA server are authenticated through the use of the shared secret.
Authentication Port	Authentication port number.
Accounting Port	Accounting port number.

8.4.2.1 Managing RADIUS Servers

8.4.2.1.1 Creating a RADIUS Server

Step 1 Select a CTC-based NE R6.0 or later and choose **Configuration > NE Explorer**.

- Step 2** In the tree view of the NE Explorer window, select the NE node.
- Step 3** In the properties pane of the NE Explorer window, click the **Security** tab > **RADIUS Server** subtab.
- Step 4** Click **Create**.
- Step 5** In the Create New RADIUS Server dialog box, enter the following information:
- IP address
 - Shared secret
 - Authentication port
 - Accounting port
- Step 6** Click **OK**. The new RADIUS server is added to the RADIUS Servers in Order of Authentication table. You can create a maximum of 10 RADIUS server entries.
-

8.4.2.1.2 Modifying a RADIUS Server

- Step 1** Select a CTC-based NE R6.0 or later and choose **Configuration > NE Explorer**.
- Step 2** In the tree view of the NE Explorer window, select the NE node.
- Step 3** In the properties pane of the NE Explorer window, click the **Security** tab > **RADIUS Server** subtab.
- Step 4** From the RADIUS Servers in Order of Authentication table, select a RADIUS server to modify; then, click **Edit**.
- Step 5** In the Edit RADIUS Server dialog box, modify the following information:
- IP address
 - Shared secret
 - Authentication port
 - Accounting port
- Step 6** Click **OK**. Changes to the RADIUS server appear in the RADIUS Servers in Order of Authentication table.
-

8.4.2.1.3 Deleting a RADIUS Server

- Step 1** Select a CTC-based NE R6.0 or later and choose **Configuration > NE Explorer**.
- Step 2** In the tree view of the NE Explorer window, select the NE node.
- Step 3** In the properties pane of the NE Explorer window, click the **Security** tab > **RADIUS Server** subtab.
- Step 4** From the RADIUS Servers in Order of Authentication table, select a RADIUS server to delete; then, click **Delete**.
- Step 5** Click **Yes** in the confirmation dialog box.
-

8.4.3 Managing NE User Access

You can view, add, modify, and delete user accounts for CTC-based ONS 15216 EDFA3 NEs.

8.4.3.1 Viewing the CTC-Based NE User Access Administration Table

The NE User Access Administration table displays information about the existing users on the NEs that are selected from the Prime Optical domain.

To view the NE User Access Administration table, choose **Administration > CTC-Based NEs > NE User Access Administration**. The following table provides descriptions.

Table 8-19 *Field Descriptions for the NE User Access Administration Table*

Field	Description
Alias ID	Alias name of the NE.
NE Username	Username of the NE user.
NE User Privilege (<i>CTC-based NEs only</i>)	Privilege level of the user. For CTC-based NEs, user privileges are Retrieve, Maintenance, Provisioning, and Superuser.
Lock Out	Whether the NE user is locked out of the NE.
Last Login Time	Time stamp when the NE user most recently logged in.
Failed Login Count	Number of times the NE user failed to log into the NE successfully.
Disabled	Whether the NE user's access to the NE has been disabled.
Password Change on Next Login	Whether the NE user is required to change his or her password upon the next login to the NE.
NE ID	Unique ID representing the NE.

8.4.3.2 Viewing the NE User Access Administration Table—ONS 15216 EDFA3 NEs

The NE User Access Administration table displays information about the existing users on the NEs that are selected from the Prime Optical domain.

To view the NE User Access Administration table, choose **Administration > ONS 15216 > NE User Access Administration**. The following table provides descriptions.

Table 8-20 Field Descriptions for the NE User Access Administration Table

Field	Description
NE ID	Unique ID representing the NE.
NE Username	Username of the NE user.
NE User Privilege	Privilege level of the user. User privileges are Read Only, Read/Write, and Read/Write/Administrative.
Timeout	Length of the timeout period (in minutes) based on the user privilege. When a timeout occurs, the corresponding session is terminated, because no messages were exchanged for a defined period of time. <ul style="list-style-type: none"> For Read Only users, the Cisco default timeout is 60 minutes. For Read/Write users, the Cisco default timeout is 30 minutes. For Read/Write/Administrative users, the Cisco default timeout is 15 minutes.

8.4.3.3 Filtering NE User Access Administration Table Data

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

Table 8-21 Field Descriptions for the NE User Access Administration Table Filter

Field	Description
NE ID	Move NEs back and forth between the list of available NEs and selected NEs. The filter runs on the NEs in the Selected NE ID list.
User ID	Move users back and forth between the list of available users and selected users. The filter runs on the users in the Selected User ID list.
User Privilege	Select the user privilege levels for filtering.

8.4.3.4 Adding an NE User

Use the Add NE User wizard to add new users to ONS 15216 EDFA3, or CTC-based NEs. [Table 8-22](#) provides descriptions.



Note Only users with Read/Write/Administrative privileges can add a new user to the ONS 15216 EDFA3.

- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs** or **ONS 15216 > NE User Access Administration**. The NE User Access Administration table opens.
- Step 2** Choose **Edit > Add** (or click the **Create a New User** tool) for CTC-based or ONS 15216 EDFA3 NEs. The Add NE User wizard opens.
- Step 3** In the Network Elements area, choose the NEs from the Available NEs list that the new user will have access to and click **Add**. These NEs will appear in the Selected NEs list. If you want to remove NEs that the new user has access to, select the NEs from the Selected NEs list and click **Remove**.
- Step 4** Click **Next**.
- Step 5** Set the new user account:
 - Username
 - Password (and verify password)
 - Privilege (for CTC-based and ONS 15216 EDFA3 NEs)
- Step 6** Click **Add**. Each new user is added in the Selected Users Profile list.
- Step 7** To remove a new user from the Selected Users Profile list, select the user profile and click **Remove**.
- Step 8** Click **Finish**. The result of this activity can be monitored in the Job Monitor table.
- Step 9** In the confirmation dialog box, click **OK**.



Note The addition of an NE user account cannot be scheduled for an NE that is marked as Out of Service. The NE is not available in the list of NEs.

The addition of an NE user account can be scheduled for an NE that is marked as In Service and with a communication state of Unavailable. The job will remain in the Job Monitor table in Waiting status and will be executed once the NE becomes available. This job cannot be canceled while in Waiting status.

Table 8-22 Field Descriptions for the Add NE User Wizard

Field	Description
NE Selection Task	
NE Model	Selected NE model.
Network Elements	List of available and selected NEs. Select one or more NEs from the Available NEs list and click Add to add them to the Selected NEs list. Select one or more NEs from the Selected NEs list and click Remove to remove them from the Selected NEs list.
User Profile Selection Task	

Table 8-22 **Field Descriptions for the Add NE User Wizard (continued)**

Field	Description
Username	<p>Username for the new user.</p> <ul style="list-style-type: none"> For CTC-based NEs, the username must conform with the username rules specified as the NE defaults. To view the username rules, launch the NE Explorer and click the NE Defaults tab. For ONS 15216 EDFA3 NEs, the username must contain at least 6 but not more than 10 alphanumeric characters. ONS 15216 EDFA3 NEs support only a single TL1 session for each username.
New Password	<p>User password.</p> <ul style="list-style-type: none"> For CTC-based NEs, the password must conform with the user password rules specified as the NE defaults. To view the user password rules, launch the NE Explorer and click the NE Defaults tab. For ONS 15216 EDFA3 NEs, the password must contain at least 7 but not more than 10 ASCII characters, where at least two characters are nonalphabetic and at least one character is a special character (+, #, %). For example, <i>jpasswd#1</i> is an acceptable password. The password cannot contain the username. For example, if the username is <i>CISCO15</i>, the password cannot be <i>CISCO15#</i>. The password is case-sensitive.
Verify/Confirm Password	Re-enter the password to confirm it.
Privilege (for CTC-based and ONS 15216 EDFA3 NEs)	<p>Privilege level for the new NE user.</p> <ul style="list-style-type: none"> For CTC-based NEs, privilege levels are Retrieve, Maintenance, Provisioning, and Superuser. For ONS 15216 EDFA3 NEs, privilege levels are Read Only (R), Read/Write (RW), and Read/Write/Administrative (RWA). The timeout period is based on the user privilege. When a timeout occurs, the corresponding session is terminated, because no messages were exchanged for a defined period of time. <ul style="list-style-type: none"> Read Only: The user can monitor the state of an NE, but cannot issue provisioning commands. The Cisco default timeout is 60 minutes. Read/Write: The user can receive notifications, read information, and provision the NE. The user cannot carry out system administrative tasks. The Cisco default timeout is 30 minutes. Read/Write/Administrative: The user can receive notifications, read information, provision the NE, carry out system administrative tasks, and perform user management. The Cisco default timeout is 15 minutes.
Selected Users Profile	List of new NE users. You can click Remove to remove the selected NE user.

8.4.3.5 Adding a Predefined User

Use the Add Predefined User wizard to add a predefined Prime Optical user from an NE or from the NE User Access Administration table. [Table 8-23](#) provides descriptions.


Note

The Add Predefined User wizard is not available for ONS 15216 EDFA3 NEs.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs > NE User Access Administration**. The NE User Access Administration table opens.
- Step 2** For CTC-based NEs, choose **Edit > Add Predefined Users**.
- Step 3** In the Add Predefined User wizard, do the following:
- Select the area from which you will choose the predefined NE user. In the Existing NE User Selection area, click one of the following:
 - From NE**—To choose predefined users of a specific NE.
 - From Prime Optical User Table**—To choose predefined users associated with the Prime Optical user in the Prime Optical User table.
 - From CTC User Profile Table**—To choose predefined users associated with the CTC user in the CTC User Profile table.
 - If you chose to select users from an NE, in the NE Selection area, choose the NE from the **Select NE to pick users from** drop-down list. If you chose to select from the Prime Optical User table, this field is unavailable.
 - If you chose to select users from an NE, specify and verify the password in the Specify User Password area. This password will be applied to all the users selected in the next window. If you chose to select from the Prime Optical User table, you can force a password to the user by checking the **Force Password** check box, then specifying and verifying the password.
 - Specify the user privilege. If you chose to select users from an NE, you can force a privilege to the user by checking the **Force Privilege** check box.
- This privilege will be applied to all the users selected in the next window.
- Step 4** Click **Next**.
- Step 5** Select the predefined users. Use the **Add** and **Remove** buttons to add or remove users in the Selected Users list.
- Step 6** Click **Next**.
- Step 7** Specify the NEs that the new user will have access to. Use the **Add** and **Remove** buttons to add or remove NEs in the Selected NEs list.
- Step 8** Click **Finish**. The result of this activity can be monitored in the Job Monitor table.
- Step 9** In the confirmation dialog box, click **OK**.
-

Table 8-23 *Field Descriptions for the Add Predefined User Wizard*

Field	Description
Predefined User Property Selection Task	
Existing NE User Selection	Choose whether to add the new user from the selected NE, from the Prime Optical User table, or from the CTC User Profile table.
NE Selection	Select the NE from which to choose a user. Note This field is dimmed if you selected From Prime Optical User Table or From CTC User Profile Table in the Existing NE User Selection area.
Force Password	If enabled, forces the predefined user to use a password when logging in. Note This field is dimmed if you selected From NE or From CTC User Profile Table in the Existing NE User Selection area.
Password	Enter the login password that the user will use to access the system. For CTC-based NEs, the password must conform with the password rules specified as the NE defaults. To view the password rules, launch the NE Explorer and click the NE Defaults tab. Note This field is dimmed if you select From CTC User Profile Table in the Existing NE User Selection area.
Confirm Password	Confirm the user password by retyping it.
Force Privilege	If enabled, forces the predefined user to use a specific user privilege level when logging in. Note This field is dimmed if you select From Prime Optical User Table or From CTC User Profile Table in the Existing NE User Selection area.
Privilege	Set the appropriate user privilege level. For CTC-based NEs, privilege levels are Retrieve, Maintenance, Provisioning, and Superuser.
Predefined User Selection Task	
Available Users	Select one or more users from the list and click Add to add them to the Selected Users list. Only the users in the Selected Users list will be added.
Selected Users	Select one or more users from the list and click Remove to remove them from the Selected Users list. Only the users in the Selected Users list will be added.
NE Selection Task	
Available NEs	Select one or more NEs from the list and click Add to add them to the Selected NEs list. Users are added only to the NEs in the Selected NEs list.
Selected NEs	Select one or more NEs from the list and click Remove to remove them from the Selected NEs list. Users are added only to the NEs in the Selected NEs list.

8.4.3.6 Modifying an NE User Profile

Use the Modify NE User wizard to make changes to existing NE users. [Table 8-24](#) provides descriptions.


Note

Only users with Read/Write/Administrative privileges can modify a user's password and privilege level on the ONS 15216 EDFA3.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs** or **ONS 15216 > NE User Access Administration**. The NE User Access Administration table opens.
- Step 2** Select a user from the list. Choose **Edit > View/Modify** (or click the **Modify User Properties** tool) for CTC-based and ONS 15216 EDFA3 NEs.
- Step 3** In the Modify NE User wizard, modify the following information (as needed). Fields shown depend on the NE selected:
- Username
 - Old Password (available only when the selected user is active)
 - New Password (and verify password)
 - Privilege (for CTC-based and ONS 15216 EDFA3 NEs)
 - Lock Out
 - Disabled
 - Change Password on Next Login
 - Modify User on Multiple NEs check box


Note

You cannot modify the Privilege, Lock Out, Disabled, and Change Password on Next Login fields if the selected user is active.

-
- Step 4** Do one of the following:
- a. If you did not check Modify User on Multiple NEs, proceed to the next step.
 - b. If you checked Modify User on Multiple NEs, click **Next**. Select the NEs that the modified user can or cannot access.
- Step 5** Click **Finish**. The result of this activity can be monitored in the Job Monitor table.
- Step 6** In the confirmation dialog box, click **OK**.
- Step 7** If you are modifying the profile of a user who is currently logged in, click **OK** in the warning message. Changes to the NE user profile will take effect on the user's next login attempt.
-

**Note**

- You cannot modify an existing NE user account for an NE that is marked as Out of Service. You can select the NE's records in the NE User Access Administration table, but when you try to modify the account, you will receive an error message telling you that you cannot perform the operation.
- You can schedule modification of an existing NE user account for an NE that is marked as In Service but is unavailable. The job remains in Waiting status in the Job Monitor table and is executed when the NE becomes available. You cannot cancel the job.

Table 8-24 **Field Descriptions for the Modify NE User Wizard**

Field	Description
Username	For the ONS 15216 EDFA3, edit the username. Note For CTC-based NEs, the username is display only; it cannot be modified without deleting the user.
Old Password	Enter the old user password. This field is available only when the selected user is active.
New Password	Modify the user password. <ul style="list-style-type: none"> • For CTC-based NEs, the password must conform with the password rules specified as the NE defaults. To view the password rules, launch the NE Explorer and click the NE Defaults tab. • For ONS 15216 EDFA3 NEs, the password must contain at least 7 but not more than 10 ASCII characters, where at least two characters are nonalphabetic and at least one character is a special character (+, #, %). For example, <i>jpasswd#1</i> is an acceptable password. The password cannot contain the username. For example, if the username is <i>CISCO15</i>, the password cannot be <i>CISCO15#</i>. The password is case-sensitive.
Verify/Confirm Password	Re-enter the modified password to confirm it.
Privilege (<i>for CTC-based and ONS 15216 EDFA3 NEs</i>)	Modify the privilege level of the user. <ul style="list-style-type: none"> • For CTC-based NEs, privilege levels are Retrieve, Maintenance, Provisioning, and Superuser. • For ONS 15216 EDFA3 NEs, privilege levels are Read Only, Read/Write, and Read/Write/Administrative. Note You cannot modify this field if the selected user is active.
Timeout (<i>for ONS 15216 EDFA3 NEs</i>)	<i>Display only.</i> View the length of the timeout period (in minutes) based on the user privilege. When a timeout occurs, the corresponding session is terminated, because no messages were exchanged for a defined period of time. <ul style="list-style-type: none"> • For Read Only users, the Cisco default timeout is 60 minutes. • For Read/Write users, the Cisco default timeout is 30 minutes. • For Read/Write/Administrative users, the Cisco default timeout is 15 minutes.
Lock Out	Check this check box to lock out the NE user. Note You cannot modify this field if the selected user is active.
Disabled	Check this check box to permanently disable the user from logging back into Prime Optical. Note You cannot modify this field if the selected user is active.

Table 8-24 Field Descriptions for the Modify NE User Wizard (continued)

Field	Description
Change Password on Next Login	Check this check box to force the NE user to change his or her password on the next login. Note You cannot modify this field if the selected user is active.
Modify User on Multiple NEs	Check this check box to modify the profile for multiple NEs. The NEs are selected in the next panel.

8.4.3.7 Deleting an NE User

Step 1 In the Domain Explorer window, choose **Administration > CTC-Based NEs** or **ONS 15216 > NE User Access Administration**. The NE User Access Administration table opens.

Step 2 Select a user from the list and choose **Edit > Delete** (or click the **Delete User** tool) for CTC-based and ONS 15216 EDFA3 NEs.

**Note**

You cannot delete a user who is currently logged in. For CTC-based NE users, you must first log out the user from the Active NE Users table. See [8.4.3.10 Ending an Active NE User Session, page 8-59](#). For ONS 15216 EDFA3 NE users, you must wait for the user to log out before deleting that user.

**Note**

Only users with Read/Write/Administrative privileges can delete an ONS 15216 EDFA3 user.

Step 3 Click **Yes** in the confirmation dialog box.

Step 4 Click **OK** in the message box.

**Note**

You cannot delete an existing NE user account for an NE that is marked as Out of Service. You can select the NE's records in the NE User Access Administration table, but when you try to delete the account, you will receive an error message telling you that you cannot perform the operation.

**Note**

You can schedule deletion of an existing NE user account for an NE that is marked as In Service but is unavailable. The job remains in Waiting status in the Job Monitor table and is executed when the NE becomes available. You cannot cancel the job.

8.4.3.8 Viewing Active NE Users

The NE Active Users table displays information about the users who are currently logged into selected NEs in Prime Optical. [Table 8-25](#) provides descriptions. Fields shown depend on the NE selected.


Note

The ONS 15216 EDFA3 supports up to 20 user accounts with up to 11 simultaneous Telnet user connections. Each user can open only one connection at a time.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs** or **ONS 15216 > NE User Access Administration**. The NE User Access Administration table opens.
- Step 2** For CTC-based and ONS 15216 EDFA3 NEs, choose **Edit > NE Active Users** (or click the **Show NE Active Users** tool). The NE Active Users table opens.
- Step 3** For CTC-based NEs, choose **Administration > Retrieve Last Activity Time** (or click the **Retrieve Last Activity Time** tool) to refresh the Last Activity Time field for the current list of active users, if the activity time has changed.
-

Table 8-25 **Field Descriptions for the NE Active Users Table**

Field	Description
Alias ID	Alias name of the NE.
NE Username	Name of the user.
Client IP Address (<i>CTC-based NEs only</i>)	IP address of the client workstation from which the user has logged in.
Session Type (<i>CTC-based NEs only</i>)	<p>Type of active user session (EMS, Telnet, and so on). Prime Optical and CTC sessions are identified as “EMS.”</p> <p>This field applies only to the following CTC-based NEs:</p> <ul style="list-style-type: none"> • ONS 15310 CL R6.0 and later • ONS 15310 MA SDH • ONS 15310 MA SONET R7.0 and later • ONS 15327 R6.0 and later • ONS 15454 SDH R6.0 and later • ONS 15454 SONET R6.0 and later • ONS 15600 SONET R6.0 and later

Table 8-25 Field Descriptions for the NE Active Users Table (continued)

Field	Description
Last Activity Time (<i>CTC-based NEs only</i>)	<p>Date and time when the last activity was performed by the active user on the NE.</p> <p>This field applies only to the following CTC-based NEs:</p> <ul style="list-style-type: none"> • ONS 15310 CL R6.0 and later • ONS 15310 MA SDH • ONS 15310 MA SONET R7.0 and later • ONS 15327 R6.0 and later • ONS 15454 SDH R6.0 and later • ONS 15454 SONET R6.0 and later • ONS 15600 SONET R6.0 and later
Login Time (<i>CTC-based NEs only</i>)	<p>Date and time when the active user logged into the NE.</p> <p>This field applies only to the following CTC-based NEs:</p> <ul style="list-style-type: none"> • ONS 15310 CL R6.0 and later • ONS 15310 MA SDH • ONS 15310 MA SONET R7.0 and later • ONS 15327 R6.0 and later • ONS 15454 SDH R6.0 and later • ONS 15454 SONET R6.0 and later • ONS 15600 SONET R6.0 and later
NE ID	Unique ID number of the NE.

8.4.3.9 Filtering NE Active Users Table Data

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

Table 8-26 Field Descriptions for the NE Active Users Table Filter

Field	Description
NE ID	Move NEs back and forth between the list of available NEs and selected NEs. The filter runs on the NEs in the Selected NE ID list.

8.4.3.10 Ending an Active NE User Session

You can use the Log Out User feature to end a user session on CTC-based NEs.

**Note**

The Log Out User feature is not available for ONS 15216 EDFA3 NEs.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs > NE User Access Administration**. The NE User Access Administration table opens.
- Step 2** For CTC-based NEs, choose **Edit > NE Active Users** (or click the **Show NE Active Users** tool). The NE Active Users table opens.
- Step 3** For CTC-based NEs, choose **Administration > Log Out User** (or click the **Log Out User** tool).
- Step 4** Click **Yes**.
-

8.4.4 Managing CTC User Profiles

You can view, create, modify, and delete CTC user profiles in the Prime Optical database.

8.4.4.1 Viewing the CTC User Profiles Table

The CTC User Profiles table contains a list of predefined CTC user profiles that are available in the Prime Optical database. To view the CTC User Profiles table, choose **Administration > CTC User Profiles** in the Domain Explorer window. The following table provides descriptions.

Table 8-27 Field Descriptions for the CTC User Profiles Table

Field	Description
User ID	CTC username.
User Privilege	CTC user privilege.
Description	Description of the CTC user.

8.4.4.2 Creating a CTC User Profile

Use the Add New CTC User Profile dialog box to add new CTC user profiles to the database. The following table provides descriptions.

- Step 1

In the Domain Explorer window, choose **Administration > CTC User Profiles**. The CTC User Profiles table opens.
- Step 2

Choose **Edit > Create** (or click the **Create a New CTC User Profile** tool).
- Step 3

In the Add New CTC User Profile dialog box, enter the following information:
 - User ID
 - User password (and confirm password)
 - User privilege
 - Description
- Step 4

Click **OK**.

Table 8-28 Field Descriptions for the Add New CTC User Profile Dialog Box

Field	Description
User ID	Name of the new user profile. The profile name must contain from six to twenty alphanumeric characters (A–Z, a–z, 0–9). Alphabetic characters are case-sensitive. The user profile name cannot contain spaces or special characters. Note After the user ID is set, it cannot be changed without deleting the user.
User Password	User password. The new password must contain a minimum of six and a maximum of ten alphanumeric (a–z, A–Z, 0–9) and special characters (+, #,%), where at least two characters are alphabetic, at least one character is numeric, and at least one character is a special character. Note Regardless of the actual size of the old password, the Password field displays only a fixed-length string. The fixed-length string contains 15 asterisks (*).
Confirm Password	Retype the password to confirm it.
User Privilege	Access privilege for the new user profile. Privilege levels are Retrieve, Maintenance, Provisioning, and Superuser.
Description	Description of the new user profile.

8.4.4.3 Modifying a CTC User's Properties

Use the Modify CTC User Profile dialog box to make changes to an existing CTC user profile. The following table provides descriptions.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC User Profiles**. The CTC User Profiles table opens.
- Step 2** Choose **Edit > View/Modify** (or click the **Modify CTC User Profile Properties** tool).
- Step 3** In the Modify CTC User Profile dialog box, modify the following information, as needed:
- User password (and confirm password)
 - User privilege
 - Description
- Step 4** Click **OK**.
-

Table 8-29 Field Descriptions for the Modify CTC User Profile Dialog Box

Field	Description
User ID	<p><i>Display only.</i> Name of the user profile. The profile name must contain from six to twenty alphanumeric characters (A–Z, a–z, 0–9). Alphabetic characters are case-sensitive. The user profile name cannot contain spaces or special characters.</p> <p>Note After the username is set, it cannot be changed without deleting the user.</p>
User Password	<p>User password. The password must contain a minimum of six and a maximum of ten alphanumeric (a–z, A–Z, 0–9) and special characters (+, #,%), where at least two characters are alphabetic, at least one character is numeric, and at least one character is a special character.</p> <p>Note Regardless of the actual size of the old password, the Password field displays only a fixed-length string. The fixed-length string contains 15 asterisks (*).</p>
Confirm Password	Retype the modified password to confirm it.
User Privilege	Access privilege for the user profile. Privilege levels are Retrieve, Maintenance, Provisioning, and Superuser.
Description	Description of the user profile.

8.4.4.4 Deleting a CTC User Profile

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC User Profiles**. The CTC User Profiles table opens.
- Step 2** Select the CTC user profile that you want to delete and choose **Edit > Delete** (or click the **Delete CTC User Profile** tool).
- Step 3** Click **OK** in the confirmation dialog box.
-

8.4.5 Managing Cisco IOS Users

You can view, create, modify, and delete Cisco IOS user accounts in the Prime Optical database.

8.4.5.1 Viewing the IOS Users Table

The IOS Users table shows all of the configured Cisco IOS user accounts. You can use the IOS Users table to manage user access to Layer 2 and Layer 3 Cisco IOS cards. Use this table to give users the ability to view or edit the username and password on ML cards in CTC-based NEs.

To view the table, choose **Administration > CTC-Based NEs > IOS Users Table** in the Domain Explorer window. The following table provides descriptions.

Table 8-30 *Field Descriptions for the IOS Users Table*

Field	Description
Alias ID	Alias of the NE.
Module Name	Name of the selected module.
Physical Location	Location of the selected module.
Username	Username that is provisioned on the Cisco IOS card.
Privilege	Privilege level of the selected user.
NE ID	ID number of the NE.

8.4.5.2 Adding an IOS User

Use the IOS User Creation wizard to add new Cisco IOS users to the domain.

-
- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs > IOS Users Table**.
- Step 2** In the IOS Users table, choose **Edit > Create** (or click the **Create a New User** tool). The IOS User Creation wizard opens. The following table provides descriptions.
- Step 3** In the IOS Card Selection window, complete the following substeps:
- Select the NE ID on which you want to create a new Cisco IOS user.
 - In the Available IOS Cards list, select the cards that you want the new user to be able to access. Use the **Add** button to move the cards to the Selected IOS Cards list.
 - Click **Next**.
- Step 4** In the IOS User Information window, enter the following information:
- Username
 - Password (and confirm password)
 - User privilege
- Step 5** Click **Finish**.



Note A progress animator is displayed while the new user is being added to the IOS Users table.

The new user is listed in the IOS Users table.

Table 8-31 *Field Descriptions for the IOS User Creation Wizard*

Field	Description
IOS Card Selection Pane	
NE ID	NE ID on which you want to create a new Cisco IOS user.
Available IOS Cards	Available Cisco IOS data cards that the user can access. Click Add to move the cards to the Selected IOS Cards list.
Selected IOS Cards	Selected Cisco IOS data cards that the user can access. Click Remove to return the cards to the Available IOS Cards list.
IOS User Information Pane	
Username	Name of the Cisco IOS user.
Password	Login password that the Cisco IOS user will use to access ML cards. Note Regardless of the actual size of the old password, the Password and Confirm Password fields display only a fixed-length string. The fixed-length string contains 15 asterisks (*).
Confirm Password	Retype the password to confirm it.
User Privilege	User privilege level. Values are from 0 to 15; the Cisco default is 15.

8.4.5.3 Modifying an IOS User

Use the IOS User Modification wizard to modify the password or privilege level of an existing Cisco IOS user.

- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs > IOS Users Table**.
- Step 2** In the IOS Users table, choose **Edit > Modify** (or click the **Modify User Properties** tool). The IOS User Modification wizard opens. The following table provides descriptions.
- Step 3** In the IOS Card Selection window, complete the following substeps:
 - a. Select the NE ID on which you want to modify the Cisco IOS user password or privilege level.
 - b. In the Available IOS Cards list, select the cards that you want the modified user to be able to access. Use the **Add** button to move the cards to the Selected IOS Cards list.
 - c. Click **Next**.
- Step 4** In the IOS User Information window, enter the following information:
 - Password (and confirm password)
 - User privilege
- Step 5** Click **Finish**.

**Note**

A progress animator is displayed while the user information is modified.

Table 8-32 *Field Descriptions for the IOS User Modification Wizard*

Field	Description
IOS Card Selection Pane	
NE ID	NE ID on which you want to modify the Cisco IOS user.
Available IOS Cards	Available Cisco IOS data cards that the user can access. Click Add to move the cards to the Selected IOS Cards list.
Selected IOS Cards	Selected Cisco IOS data cards that the user can access. Click Remove to return the cards to the Available IOS Cards list.
IOS User Information Pane	
Username	<i>Display only.</i> Name of the Cisco IOS user.
Password	Login password that the Cisco IOS user will use to access ML cards.
Confirm Password	Retype the password to confirm it.
User Privilege	User privilege level. Values are from 0 to 15; the Cisco default is 15.

8.4.5.4 Deleting an IOS User

- Step 1** In the Domain Explorer window, choose **Administration > CTC-Based NEs > IOS Users Table**.
- Step 2** In the IOS Users table, select the user to be deleted.
- Step 3** Choose **Edit > Delete** (or click the **Delete User** tool).
- Step 4** Click **OK** to remove the user from the database.

**Note**

A progress animator is displayed while the delete operation is performed.

8.4.6 Managing SNMPv3—CTC-Based Release 9.6 NEs

**Note**

SNMPv3 is not supported on ONS 15305, ONS 15305 CTC, and ONS 15327 NEs.

The following cases describe how to configure SNMPv3 on CTC-based NEs:

1. Provision a logical SNMPv3 configuration on CTC-based NEs using the SNMPv3 wizard. See [8.4.6.1 Configuring SNMPv3 Parameters, page 8-65](#) for information on the SNMPv3 wizard. To verify the SNMPv3 configuration, see case 2.
2. Check the configured SNMPv3 parameters using the SNMPv3 tables. See [8.4.6.2 Viewing SNMPv3 Tables, page 8-67](#) for instructions on how to open the SNMPv3 tables. The SNMPv3 configuration is correct if the following constraints are verified:
 - The SNMPv3 NE Users table contains the provisioned users for each NE.
 - The SNMPv3 user group is defined in the SNMPv3 NE Groups table for each NE.
 - The SNMPv3 group view is defined in the SNMPv3 NE MIB Views table for each NE.
 - If an NE entry in the SNMPv3 NE Trap Destinations table is associated with a notification filter, the filter is defined in the SNMPv3 NE Notification Filters table for each NE.

If an NE is a proxy NE or ENE, the following additional constraints are verified:

- The target address is the GNE IP address and the port number is 161 in the SNMPv3 NE Trap Destinations table.
- The SNMPv3 NE Proxy Forwarder table of the GNE contains two rows: one for the GET type value and another for the SET type value. Also, the remote NE is the system ID of the ENE, and the remote user is defined in the ENE's SNMPv3 NE Users table.
- The SNMPv3 NE Proxy Trap Forwarder table of the GNE contains a row for the ENE. Also, the tag references the proxy tags in the SNMPv3 NE Trap Destinations table, and the incoming user is defined in the ENE's SNMPv3 NE Users table.

If the SNMPv3 tables contain invalid rows, see case 3. If you need to add rows to one or more SNMPv3 tables, see case 4.



Note

For more information on SNMPv3 for CTC-based NEs, refer to the NE hardware documentation.

3. Delete rows from the SNMPv3 tables. See [8.4.6.3 Deleting SNMPv3 Users from the SNMPv3 Tables, page 8-71](#).
4. Provision rows in the SNMPv3 tables. The SNMPv3 wizard also allows you to add entries to one or more SNMPv3 tables. See [8.4.6.1 Configuring SNMPv3 Parameters, page 8-65](#) for details.

8.4.6.1 Configuring SNMPv3 Parameters

The SNMPv3 wizard allows you to configure parameters in the SNMPv3 tables. You can do one of the following:

- Add entities to one or more SNMPv3 tables. If you choose this option, do not select the Configure Proxy check box in the SNMPv3 wizard.
- Provision the entire SNMPv3 configuration. If you choose this option, select the Configure Proxy check box in the SNMPv3 wizard. The SNMPv3 wizard validates the configuration by verifying that it complies with the constraints listed in [8.4.6 Managing SNMPv3—CTC-Based Release 9.6 NEs, page 8-64](#). Moreover, the SNMPv3 wizard configures the SNMPv3 proxy for proxy NEs.

Complete the following steps to configure the SNMPv3 parameters:

- Step 1** In the Domain Explorer, select a CTC-based NE and choose **Administration > CTC-Based NEs > SNMPv3 Configuration**.

- Step 2** In the SNMPv3 wizard, complete the following substeps:
- Enter the following view information:
 - Name—Name of the MIB view.
 - Subtree OID—Object identifier that designates a subtree element in the MIB hierarchy.
 - Bit Mask—Bit mask that identifies the objects in the subtree.
 - Type—Status of the view. Values are Included or Excluded.
 - Click **Add**. The view information appears in the Table Views area. To remove the view information, select the view information from the Table Views area and click **Delete**.
- Step 3** Click **Next**.
- Step 4** Enter the following group information:
- Group Name—Name of the group.
 - Security Level—Security level of the group. Values are authPriv, authNoPriv, and noAuthNoPriv.
 - Read View Name—The group's view-for-read access name.
 - Notify View Name—The group's view-for-notifications name.
 - Allow SNMP Sets—If checked, users who belong to the group can perform the SNMP SET operation on the NE.
- Step 5** Click **Next**.
- Step 6** Complete the following substeps:
- Enter the following information in the User area:
 - Username—SNMPv3 username.
 - Group name—Name of the group to which the user belongs.
 - Enter the following information in the Authentication area:
 - Protocol—Protocol used to authenticate the SNMPv3 user.
 - Password—Password used to log into the Prime Optical server.
 - Confirm Password—Re-enter the password to confirm it.
 - Enter the following information in the Privacy area:
 - Protocol—Protocol used for encryption.
 - Password—Password used to decrypt the message payload.
 - Confirm Password—Re-enter the password to confirm it.
- Step 7** Click **Next**.
- Step 8** Enter the following notification filter information:
- Profile Name—Filter profile name.
 - Subtree OID—Object identifier that designates a subtree element in the MIB hierarchy.
 - Bit Mask—Bit mask that identifies the objects in the subtree.
 - View Type—Filter type with respect to the subset of the MIB object that is identified by the subtree OID and bitmask fields. Values are Included and Excluded.
- Step 9** Click **Next**.
- Step 10** Enter the following trap destination information:

- Target Address—IP address of the EMS to which the NE forwards the SNMPv3 traps.
- UDP Port—UDP port number to which the NE forwards the SNMPv3 traps.
- Username—SNMPv3 username.
- Security Level—Security level that the SNMPv3 NE uses. Valid values are authPriv, authNoPriv, and noAuthNoPriv.
- Filter Profile—Filter profile name associated with the trap destination.
- Proxy Trap Only—If selected, the NE that acts as the SNMPv3 proxy uses the entries in the SNMPv3 NE Trap Destinations table to forward traps from other NEs to the target address. The SNMPv3 proxy NE does not send its own traps to the target address.
- Proxy Tags—A string used to identify a set of entries in the SNMPv3 NE Trap Destinations table. This is required for SNMPv3 proxy configuration.

Step 11 Do one of the following:

- If you are adding entries to the SNMPv3 tables, uncheck the **Configure Proxy** check box.
- If you choose automatic proxy configuration, check the **Configure Proxy** check box. If checked, Prime Optical identifies the SNMPv3 proxy for each selected ENE. The ENE and SNMPv3 proxy are configured to enable Prime Optical–SNMPv3 NE connectivity using the parameters you defined in steps 2, 4, 6, 8, and 10.

Step 12 Click **Finish**. A job is scheduled on all NEs on which the SNMPv3 NE configuration wizard was started. The job status is listed in the Job Monitor table (**Administration > Job Monitor**).

8.4.6.2 Viewing SNMPv3 Tables

The SNMPv3 tables are grouped according to the following table types:

- User tables:
 - [8.4.6.2.1 SNMPv3 NE Users Table, page 8-67](#)
 - [8.4.6.2.2 SNMPv3 NE MIB Views Table, page 8-68](#)
 - [8.4.6.2.3 SNMPv3 NE Groups Table, page 8-69](#)
- Trap tables:
 - [8.4.6.2.4 SNMPv3 NE Trap Destinations Table, page 8-69](#)
 - [8.4.6.2.5 SNMPv3 NE Notification Filters Table, page 8-70](#)
- Proxy server tables:
 - [8.4.6.2.6 SNMPv3 NE Proxy Forwarder Table, page 8-70](#)
 - [8.4.6.2.7 SNMPv3 NE Proxy Trap Forwarder Table, page 8-71](#)
 - [8.4.6.2.8 SNMPv3 NE Remote Users Table, page 8-71](#)

8.4.6.2.1 SNMPv3 NE Users Table

The SNMPv3 NE Users table displays information on the SNMPv3 users defined on a selected NE. To view the SNMPv3 NE Users table, choose **Administration > CTC-Based NEs > SNMPv3 Users** in the Domain Explorer window. The following table provides descriptions.

Table 8-33 *Field Descriptions for the SNMPv3 NE Users Table*

Field	Descriptions
NE ID	SNMPv3 NE ID.
Username	SNMPv3 username.
Group Name	Name of the group to which the user belongs.
Authentication Protocol	Protocol used to authenticate the SNMPv3 user. Valid values are MD5 or SHA.
Privacy Protocol	Protocol used for encryption.

8.4.6.2.2 SNMPv3 NE MIB Views Table

The SNMPv3 NE MIB Views table displays information on the views defined on a selected NE. A view identifies the subset of an object in the MIB. To view the SNMPv3 NE MIB Views table, choose **Administration > CTC-Based NEs > SNMPv3 MIB Views** in the Domain Explorer window. The following table provides descriptions.

Table 8-34 *Field Descriptions for the SNMPv3 NE MIB Views Table*

Field	Description
NE ID	SNMPv3 NE ID.
View Name	Name of the MIB view.
Subtree OID	Object identifier that designates a subtree element in the MIB hierarchy.
Mask	Bit mask that identifies the objects in the subtree.
Type	Status of the view. Valid values are Included or Excluded.

8.4.6.2.3 SNMPv3 NE Groups Table

The SNMPv3 NE Groups table displays information on the group that is provisioned on a selected NE. To view the SNMPv3 NE Groups table, choose **Administration > CTC-Based NEs > SNMPv3 Group Access** in the Domain Explorer window. The following table provides descriptions.

Table 8-35 *Field Descriptions for the SNMPv3 NE Groups Table*

Field	Description
NE ID	SNMPv3 NE ID.
Group Name	Name of the group.
Security Level	Security level of the group. Valid values are AuthPriv, AuthNoPriv, and NoAuthNoPriv.
Read View	Displays the group's view-for-read access name. The view name must be present in the SNMPv3 NE MIB Views table.
Allow SNMP Sets	If true, users who belong to the group can perform the SNMP SET operation on the NE.
Notify View	Displays the group's notify-for-notifications name. The view name must be present in the SNMPv3 NE MIB Views table.

8.4.6.2.4 SNMPv3 NE Trap Destinations Table

The SNMPv3 NE Trap Destinations table displays information on the trap destinations provisioned on a selected NE. To view the SNMPv3 NE Trap Destinations table, choose **Administration > CTC-Based NEs > SNMPv3 Trap Destinations** in the Domain Explorer window. The following table provides descriptions.

Table 8-36 *Field Descriptions for the SNMPv3 NE Trap Destinations Table*

Field	Description
NE ID	SNMPv3 NE ID.
Target Address	IP address of the EMS to which the NE forwards the SNMPv3 traps.
UDP Port	UDP port number to which the NE forwards the SNMPv3 traps.
Username	SNMPv3 username.
Security Level	Security level that the SNMPv3 NE uses. Valid values are AuthPriv, AuthNoPriv, and NoAuthNoPriv.
Filter Profile Name	Filter profile name associated with the trap destination. The filter profile name must be present in the SNMPv3 NE Notification Filters table.
Proxy Traps Only	If true, the NE that acts as the SNMPv3 proxy uses the entries in the SNMPv3 NE Trap Destinations table to forward traps from other NEs to the target address. The SNMPv3 proxy NE does not send its own traps to the target address.
Proxy Tags	A string used to identify a set of entries in this table. This field is required for SNMPv3 proxy configuration and referenced by the SNMPv3 NE Proxy Trap Forwarder table. See 8.4.6.2.7 SNMPv3 NE Proxy Trap Forwarder Table, page 8-71 for more information.

8.4.6.2.5 SNMPv3 NE Notification Filters Table

The SNMPv3 NE Notification Filters table displays information on the notification filters provisioned on a selected NE. To view the SNMPv3 NE Notification Filters table, choose **Administration > CTC-Based NEs > SNMPv3 Notification Filters** in the Domain Explorer window. The following table provides descriptions.

Table 8-37 *Field Descriptions for the SNMPv3 NE Notification Filters Table*

Field	Description
NE ID	SNMPv3 NE ID.
Filter Profile Name	Filter profile name that identifies the table entry.
Subtree OID	Object identifier that designates a subtree element in the MIB hierarchy.
Bit Mask	Bit mask that identifies the objects in the subtree.
Filter Type	Defines the filter type with respect to the subset of the MIB object that is identified by the subtree OID and bitmask fields. Valid values are Included and Excluded.

8.4.6.2.6 SNMPv3 NE Proxy Forwarder Table

The SNMPv3 NE Proxy Forwarder table displays information on the proxy forwarder entries. The proxy forwarder entries enable SNMPv3 proxying by selected remote NE proxies for GET and SET operations. To view the SNMPv3 NE Proxy Forwarder table, choose **Administration > CTC-Based NEs > SNMPv3 Proxy Forwarder** in the Domain Explorer window. The following table provides descriptions.

Table 8-38 *Field Descriptions for the SNMPv3 NE Proxy Forwarder Table*

Field	Descriptions
NE ID	SNMPv3 NE ID.
Remote NE	Remote SNMPv3 NE ID.
Context Engine ID	Engine ID of the remote NE.
Target Address	Target IP address of the SNMPv3 NE.
Local User	Local SNMPv3 username.
Remote User	Remote SNMPv3 username.
Proxy Type	Identifies the proxy action. Valid values are Read and Write.
Security Level	Security level that the SNMPv3 NE uses. Valid values are AuthPriv, AuthNoPriv, and NoAuthNoPriv.

8.4.6.2.7 SNMPv3 NE Proxy Trap Forwarder Table

The SNMPv3 NE Proxy Trap Forwarder table displays information on trap forwarder entries. The trap forwarder entries enable SNMPv3 proxying by selected remote NE proxies for the TRAP operation. To view the SNMPv3 NE Proxy Trap Forwarder table, choose **Administration > CTC-Based NEs > SNMPv3 Proxy Trap Forwarder** in the Domain Explorer window. The following table provides descriptions.

Table 8-39 Field Descriptions for the SNMPv3 NE Proxy Trap Forwarder Table

Field	Description
NE ID	SNMPv3 NE ID.
Remote NE	Remote SNMPv3 NE ID.
Context Engine ID	Engine ID of the remote NE.
Tag	A string that identifies one or more rows in the SNMPv3 NE Trap Destinations table. The Tag value references the Proxy Tags column in the SNMPv3 NE Trap Destinations table.
Incoming User	Name of the remote NE user.
Security Level	Security level that the SNMPv3 NE uses. Valid values are AuthPriv, AuthNoPriv, and NoAuthNoPriv.

8.4.6.2.8 SNMPv3 NE Remote Users Table

The SNMPv3 NE Remote Users table displays information on the SNMPv3 remote users defined on a selected NE. To view the SNMPv3 NE Remote Users table, choose **Administration > CTC-Based NEs > SNMPv3 Remote Users** in the Domain Explorer window. The following table provides descriptions.

Table 8-40 Field Descriptions for the SNMPv3 NE Remote Users Table

Field	Descriptions
NE ID	SNMPv3 NE ID.
Remote NE	Remote SNMPv3 NE ID.
Context Engine ID	Engine ID of the remote NE.
Group Name	Name of the group.
Authentication Protocol	Protocol used to authenticate the SNMPv3 user. Valid values are MD5 or SHA.
Privacy Protocol	Protocol used for encryption.

8.4.6.3 Deleting SNMPv3 Users from the SNMPv3 Tables

Step 1 In the Domain Explorer, choose **Administration > CTC-Based NEs > SNMPv3 table**. The table opens.

- Step 2** Select the user to delete; then, choose **Edit > Delete User** (or click the **Delete User** tool). A job is scheduled on each NE involved in the delete operation. The job status is listed in the Job Monitor table (**Administration > Job Monitor**).
- Step 3** If the job succeeds, the Refresh button flashes. Click the **Refresh Data** tool.
-

8.5 Audit Log

The Audit Log table contains information about significant events that occurred on the Prime Optical server during a specified time period. By default, the Audit Log displays information about significant events that occurred during the last four hours. You can change the default time period in the User Preferences dialog box.

The Audit Log records the following runtime-affecting operations for monitoring purposes:

- Prime Optical client logins and security violations (including successful/unsuccessful client user logins)
- Prime Optical client logouts, including:
 - User-initiated logout
 - Forced logout by an administrator
 - System-initiated logout due to user inactivity (session timeout expires)
- NE or group location changes in the Domain Explorer tree
- Domain Explorer group operations (add, delete, or modify a group)
- Changes in the Domain Explorer properties of an NE
- Write operations from a native Prime Optical NE Explorer
- Changes in the NE Software table
- NE Service, PM Service, and Prime Optical GateWay Service start or stop operations
- Prime Optical user administration (add, delete, or modify user profiles)
- Changes in:
 - UI properties
 - Security settings
 - Recovery settings
 - Database configuration
 - Error Log configuration
 - NE poller parameters
 - NE autobackup parameters
 - NE service parameters
- Job or task cancellation in the Job Monitor table
- Manual memory backup
- Memory restore
- Software download

- Software activation
- Circuit operations (add, delete, modify, or upgrade circuits)
- Link operations (add, delete, or modify links)
- OSS profile changes (TL1 or CORBA)
- VLAN operations
- Addition or deletion of a GateWay/SNMP trap destination
- Addition or deletion of a CTC binary
- BLSR/MS-SPRing operations
- L2 service operations
- Prime Optical GateWay/CORBA client logins/logouts

8.5.1 Viewing the Audit Log

To view the Audit Log, choose **Administration > Audit Log** in the Domain Explorer window. The following table provides descriptions.

Table 8-41 **Field Descriptions for the Audit Log**

Field	Description
Alias ID	Alias name of the NE.
Username	Name of the user performing the logged event. Events performed by the Prime Optical server are logged under the username <i>Internal</i> .
Service Name	Name of the service that generated the Audit Log entry.
Time Stamp (<i>time zone</i>)	Date and time when the event occurred on the Prime Optical server.
Category	Name of the category in which the event occurred. Events belong to one of the following categories: Prime Optical server administration, Prime Optical server connectivity, Prime Optical server security, Prime Optical server topology, Prime Optical server circuit, Prime Optical server network, NE provisioning, NE connectivity, BLSR/MS-SPRing, or subnetwork management.
Message	Description of the significant event that occurred.
Source ID	Source of the event. Events performed by the Prime Optical server show <i>CTM</i> as the source ID.

8.5.2 Filtering Audit Log Data

- Step 1** In the Domain Explorer window, choose **Administration > Audit Log**.
- Step 2** In the Audit Log window, choose **File > Filter** (or click the **Filter Data** tool). The Filter dialog box opens.
- Step 3** Specify the filter parameters described in the following table.
- Step 4** After making your selections, click **OK** to run the filter.
- Step 5** To save a filter:
- Open the Audit Log Filter dialog box.
 - Click the **Category** or **Service** tab.
 - Check the **Save Filter** check box.
 - Click **OK**. In the Audit Log window, the Filter tool changes to red, indicating that a saved filter is present.



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

- Step 6** To delete a saved filter, choose **File > Delete Saved Filter** in the Audit Log window. At the following prompt, click **Yes**:

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

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

Table 8-42 Field Descriptions for the Audit Log Filter Dialog Box

Tab	Description
Time Stamp (time zone)	<p>Filter Audit Log data for a specified time period, ranging from the past hour to the past 6 months. You can click the User Specified radio button to specify exact filter start and end times by date and hour. The time zone can be GMT, a user-defined offset from GMT, or local time, depending on what is specified in the User Preferences dialog box. Use the calendar tool to choose the year, month, and day:</p> <ul style="list-style-type: none"> Year—Click the year combo box or the double arrow (<<, >>) at the bottom of the calendar. Month—Click the month combo box or the single arrow (<, >) at the bottom of the calendar. Day—Click the day number on the calendar. The current date is shown in blue. <p>If you want to filter Audit Log data and the time period is not important, click No Time Specified.</p>
Source ID	Move NEs back and forth between the list of available NEs and selected NEs and then run the filter.

Table 8-42 **Field Descriptions for the Audit Log Filter Dialog Box (continued)**

Tab	Description
Category	<p>Filter Audit Log data by task.</p> <p>Follow these steps to save a filter:</p> <ol style="list-style-type: none"> 1. Check the Save Filter check box, and click OK on the Filter dialog box. 2. The saved filter is added to the table. 3. When you choose File > Apply Saved Filter, the table populates with the attributes saved for that filter. <p>Note An “at” symbol (@) in the Filter indicates that you are viewing a saved filter.</p> <p>Follow these steps to delete a filter:</p> <ol style="list-style-type: none"> 1. Chose File > Delete Saved Filter (or click the Delete Saved Filter tool). <p>The following message appears in the Delete Filter dialog box:</p> <p>The saved filter will be deleted. The current filter will remain applied to the table. Are you sure you want proceed?</p> <ol style="list-style-type: none"> 2. Click Yes. 3. When you run two parallel Prime Optical client sessions, deleting a saved filter from one session does not reflect any changes on the other. The Apply and Delete buttons remain enabled in the second session. <p>The following message appears when you click either of the buttons in the Filter dialog box of the second session:</p> <p>The saved filter no longer exists in the system. The current user might have deleted it in a different Prime Optical client session.</p> <ol style="list-style-type: none"> 4. Click OK. <p>The Apply and Delete buttons are disabled. The Filter tool reverts to blue, indicating that the filter is not saved.</p> <p>Note The menu items Apply Saved Filter and Delete Saved Filter and the Delete Saved Filter tool are enabled only if there is a saved filter for that table.</p>

Table 8-42 **Field Descriptions for the Audit Log Filter Dialog Box (continued)**

Tab	Description
Username	Move users back and forth between the list of available users and selected users and then run the filter. Events performed by the Prime Optical server are logged under the username <i>Internal</i> .
Service	<p>Move services back and forth between the list of available services and selected services and then run the filter.</p> <p>Follow these steps to save a filter:</p> <ol style="list-style-type: none"> 1. Check the Save Filter check box, and click OK on the Filter dialog box. 2. The saved filter is added to the table. 3. When you choose File > Apply Saved Filter, the table populates with the attributes saved for that filter. <p>Note An “at” symbol (@) in the Filter indicates that you are viewing a saved filter.</p> <p>Follow these steps to delete a filter:</p> <ol style="list-style-type: none"> 1. Choose File > Delete Saved Filter (or click the Delete Saved Filter tool). The following message appears in the Delete Filter dialog box: <pre>The saved filter will be deleted. The current filter will remain applied to the table. Are you sure you want proceed?</pre> 2. Click Yes. 3. When you run two parallel Prime Optical client sessions, deleting a saved filter from one session does not reflect any changes on the other. The Apply and Delete buttons remain enabled in the second session. The following message appears when you click either of the buttons in the Filter dialog box of the second session: <pre>The saved filter no longer exists in the system. The current user might have deleted it in a different Prime Optical client session.</pre> 4. Click OK. The Apply and Delete buttons are disabled. The Filter tool reverts to blue, indicating that the filter is not saved. <p>Note The menu items Apply Saved Filter and Delete Saved Filter and the Delete Saved Filter tool are enabled only if there is a saved filter for that table.</p>

8.6 Northbound Gateway Security

OSS-to-Prime Optical sessions are configured by the Prime Optical GateWay EMS-to-NMS interface architectural component. See [Chapter 12, “Managing Southbound and Northbound Interfaces”](#) for more information about Prime Optical GateWay.