Managing Security

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

This topic contains the following information:

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 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 NEs 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

Login Advisory Message

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

```
NOTICE: This is a private computer system. Unauthorised access or use may lead to
prosecution.
```

Note The login advisory message is not shown, if you log in to Prime Optical through Prime Central.

You can customize the default advisory message as follows:

Step 1 Log in to the Prime Optical server as the root or optusr user.

Step 2 Use a text editor to edit the OpticalPortalProperties.js file in the /opt/CiscoTransportManagerServer/tomcat/webapps/OpticalPortal/lib/xwt/nls directory. Edit the "advisory: property."

The new advisory message can contain up to 1600 characters.

Step 3 Save the changes.

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

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.

User Profiles and Roles

Every user profile is assigned a transport or security role. The only deviation from this is the SysAdmin user which has both transport and security roles. A user assigned with a transport role has access to operations that are required for EMS and NE administration. A user assigned with a security role has access to all operations required to manage encryption (WSE) cards. You can create a custom user profile

or use one of the default Prime Optical user profiles. To create a custom user profile, follow the procedure described in "Adding a Custom User Profile" section on page 8-37.

You can also grant the user with Provisioner and Operator profiles to modify the system coordinates.

- You need to create a duplicate profile for the provisioner profile or the operator profile.
- You must grant read or write privileges for the created duplicate profile for configure system co-ordinates operation.
- Any user created on the basis of the duplicate profile will be able to save the System co-ordinates in **Network Map**.
- By default, users with operator or provisioner profiles will have read-only privileges for configure system co-ordinates operation. It is possible for the users to still save the custom co-ordinates in network map.

Prime Optical has the following default user profiles:

Table 8-1 Prime Optical Default User Profiles

User Profile	Role	Description
SysAdmin (Administrator)	Transport and Security	Manages Prime Optical access (create, modify, delete, and end sessions) for any profile. SysAdmins are the only users who can enable or disable a profile, and access information about other administrator profiles (SuperUser and SecurityAdmin). **Note** Disabling a user profile also disables all users with that profile. They will no longer be listed in the Cisco Prime Optical User Profiles or in the Cisco Prime Optical **Users** tables. **Caution** SysAdmin users can also disable the SysAdmin profile. If the profile is disabled, you will have to contact Cisco support to enable it again.
SuperUser (Administrator)	Transport	Manages Prime Optical access (create, modify, delete, and end sessions) for profiles with transport roles only. **Note** If WSE cards are provisioned, in addition to creating a SuperUser user, you must also create a SecurityAdmin user.
NetworkAdmin	Transport	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	Transport	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	Transport	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.
SecurityAdmin (Administrator)	Security	Security system administrators who manage Prime Optical access (create, modify, delete, and end sessions) for profiles with Security roles only. **Note** This user profile must be created, in addition to the SuperUser profile, when provisioning WSE cards.

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

User Profile	Role	Description
SecurityProvisioner	Security	Users who perform daily network surveillance, provisioning, and PM activities on specific NEs provisioned WSE cards. SecurityProvisioner users cannot access administrative information.
SecurityOperator	Security	Users who perform daily network surveillance and PM activities on specific NEs provisioned with WSE cards. SecurityOperator users cannot access administrative information.

For specific information on what operations each user profile can perform see Table 8-2.

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.

Performing User Administration

This section describes how to perform user administration, including:

- Viewing the Prime Optical Users Table, page 8-14
- Creating a Prime Optical User, page 8-15
- Modifying a Prime Optical User's Properties, page 8-18
- Deleting a Prime Optical User, page 8-21
- Viewing Logged In Prime Optical Users, page 8-22
- Ending an Active Prime Optical User Session, page 8-22
- Viewing a List of Failed Login Attempts, page 8-23
- Setting User Interface Preferences, page 8-23
- Locked User Account, page 8-24
- Changing Your User Password, page 8-24
- Managing Security Advisory Messages, page 8-26
- Setting User Preferences, page 8-27
- Enabling or Disabling the Continuous Audible Alarm, page 8-30
- Configuring Prime Optical Security Parameters, page 8-30
- Sending Messages to Other Users, page 8-35
- Viewing User Notification Messages, page 8-36

Table 8-2 lists the Prime Optical default user profiles and the privileges associated with each profile. See "User Profiles and Roles" section on page 8-2 for default user profile descriptions.

Note

- The SuperUser profile has access to all operations, except the Change State operation of the User profile.
- The NetworkAdmin profile has access to all NEs and groups. The SysAdmin profile has access to no NEs or groups.

Table 8-2 Prime Optical Default User Profile Access

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
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 > Change State[1]	Allow	Deny	Deny	Deny
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
Edit > User Preferences	Allow	Allow	Allow	Allow
Edit > Change Password	Allow	Allow	Allow	Allow
Fault > Alarm Browser	Allow	Allow	Allow	Allow

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
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 > *NE_Model* > BLSR Table	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Create BLSR	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > MS-SPRing Table	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Create MS-SPRing	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Equipment Inventory Table	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Initialize ML Cards	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > L2 Topology Table	—	Allow	Allow	Allow
Configuration > *NE_Model* > Create L2 Topology	—	Allow	Allow	Deny
Configuration > *NE_Model* > QoS Profile Table	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Create QoS Profile	Deny	Allow	Allow	Deny
Configuration > *NE_Model* > Discover L2 Topologies	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Alarm Profiles Management	Deny	Allow	Allow	Deny
Configuration > *NE_Model* > NE Defaults Management	Deny	Allow	Allow	Deny
Configuration > *NE_Model* > VLAN DB Profile Management	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Circuit Table	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Rolls Table	Deny	Allow	Allow	Allow
Configuration > *NE_Model* > Update Circuit	Deny	Allow	Allow	Deny
Configuration > *NE_Model* > Repair Circuit	Deny	Allow	Allow	Deny
Configuration > *NE_Model* > Configure Node	Deny	Allow	Allow	Allow

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
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
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
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

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
Administration > *NE_Model* > NE User Access Administration	Allow	Allow	Deny	Deny
Administration > *NE_Model* > Audit Trail Table	Allow	Allow	Deny	Deny
Administration > *NE_Model* > Security Advisory Management	Allow	Allow	Deny	Deny
Administration > *NE_Model* > NE Authentication	Allow	Allow	Deny	Deny
Administration > *NE_Model* > IOS Users Table	Deny	Allow	Allow	Deny
Administration > *NE_Model* > SNMPv3 Users	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 MIB Views	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 Group Access	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 Trap Destinations	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 Notification Filters	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 Proxy Forwarder	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 Proxy Trap Forwarder	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 Remote Users	Allow	Allow	Allow	Allow
Administration > *NE_Model* > SNMPv3 Configuration	Allow	Allow	Allow	Allow
Network Map				
File > Open Child Map	Deny	Allow	Allow	Allow
File > Open Child Map in New Window	Deny	Allow	Allow	Allow
File > Open Parent Map	Deny	Allow	Allow	Allow
File > Save Map	Deny	Allow	Allow	Allow
File > Export	Deny	Allow	Deny	Deny
File > Notify Users	Deny	Allow	Allow	Allow
File > Refresh	Deny	Allow	Allow	Allow
File > Debug Options	Deny	Allow	Allow	Allow
File > Close	Deny	Allow	Allow	Allow
Edit > Filter	Deny	Allow	Allow	Allow
Edit > Copy	Deny	Allow	Allow	Allow
Edit > Select Background	Deny	Allow	Allow	Allow
Edit > Zoom In	Deny	Allow	Allow	Allow
Edit > Zoom Out	Deny	Allow	Allow	Allow
Edit > Zoom To Fit	Deny	Allow	Allow	Allow
Edit > Zoom Area	Deny	Allow	Allow	Allow
Edit > Zoom Magnify	Deny	Allow	Allow	Allow
Edit > Expand/Collapse Group	Deny	Allow	Allow	Deny
Edit > Collapse All Groups	Deny	Allow	Allow	Allow
Edit > Expand All Links	Deny	Allow	Allow	Allow

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
Edit > Collapse All Links	Deny	Allow	Allow	Allow
Edit > Layout	Deny	Allow	Allow	Allow
Edit > User Preferences	Deny	Allow	Allow	Allow
Edit > Global Network Map Configuration	Deny	Deny	Deny	Deny
Fault > Alarm Browser	Deny	Allow	Allow	Allow
Fault > Alarm Log	Deny	Allow	Allow	Allow
Fault > Event Export Manager	Deny	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
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	Deny (Not Displayed)	Deny (Not Displayed)
Configuration > NE Explorer	Deny	Allow	Allow	Allow
Configuration > Link Table	Deny	Allow	Allow	Allow
Configuration > Circuit Report	Deny	Allow	Allow	Allow
Configuration > Create Circuit	Deny	Allow	Allow	Deny (Not Displayed)
Configuration > Manage VLANs	Deny	Allow	Allow	Allow
Configuration > Create Link	Deny	Allow	Allow	Deny (Not Displayed)
Configuration > Create Server Trial	Deny	Allow	Allow	Deny (Not Displayed)
Configuration > Modify Link	Deny	Allow	Allow	Deny (Not Displayed)
Configuration > Delete Link	Deny	Allow	Allow	Deny (Not Displayed)
Configuration > Sonnet/SDH	Deny	Allow	Allow	Allow (Few submenu items are not displayed)
Configuration > Node Management	Deny	Allow	Deny (Not Displayed)	Deny (Not Displayed)
View > Overview	Deny	Allow	Allow	Allow
View > Properties	Deny	Allow	Allow	Allow
View > Explorer	Deny	Allow	Allow	Allow

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
View > Create DWDM Circuit	Deny	Allow	Allow	Deny (Not Displayed)
View > Circuit Search	Deny	Allow	Allow	Deny (Not Displayed)
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 Alarm(s)	Allow	Allow	Allow	Allow
Fault > Unacknowledge Alarm(s)	Allow	Allow	Allow	Allow
Fault > Add/Modify Note	Allow	Allow	Allow	Allow
Fault > Clear Alarm(s)	Allow	Allow	Allow	Allow
Fault > Affected Circuits	Deny	Allow	Allow	Allow
Fault > NE Explorer	Deny	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

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
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				
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

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
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
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
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 > Active User Sessions	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

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
Edit > Delete	Allow	Deny	Deny	Deny
Edit > Duplicate	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	—	—
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

Table 8-2 Prime Optical Default User Profile Access (continued)

Operation	SysAdmin /Security Admin	NetworkAdmin	Provisioner /SecurityProvisioner	Operator/SecurityOperator
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

1. Only SysAdmin profile has access to the Allow operation.

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. Table 8-3 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 8-3 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.

Table 8-3 Field Descriptions for the Prime Optical Users Table (continued)

Field	Description
User Privilege	User privilege level.
User Domain	Name of the management domain where the username belongs.
Password Set Time (*time zone*)	Last time the password was set.
Last Login Time (*time zone*)	Last time the user logged in.
Login State	Administrative state (Enabled or Disabled) of the user.
Description	Description of the user.
Password Change	Current state (Enabled or Disabled) of the password change option.
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. The Cisco default is 0, meaning the account will not be disabled automatically as a result of inactivity.

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 8-4 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 applicable fields. Table 8-4 provides descriptions.

Step 4 Click **Next**. When you are finished adding a new SuperUser, NetworkAdmin, or SysAdmin/SecurityAdmin, click **Finish**.

Step 5 When adding a new Provisioner, Operator, or custom user profile, select the groups and NEs that the Provisioner/SecurityProvisioner or Operator/SecurityOperator 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/SecurityProvisioner, 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.

a. 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**.

b. 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**.

c. 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**.

d. 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 Managing NE User Access, page 8-50.

Table 8-4 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 8-4 Field Descriptions for the Create New Prime Optical User Wizard (continued)

Field	Description
User Password	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: • 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. **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 ten passwords.
Confirm Password	Retype the password to confirm it.
User Privilege	User profile. For more information on default user profiles, see Table 8-1, "Prime Optical Default User Profiles," on page 3. **Note** If WSE cards are provisioned, in addition to creating a SuperUser user, you must also create a SecurityAdmin user.
Domain Name	Domain name. When the user logs in to 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 in to 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. The Cisco default is 0, meaning the account will not be disabled automatically as a result of inactivity.
Require Password Change on Next Login	If checked, the user is prompted to change his or her password upon next login to the Prime Optical client. If unchecked, the user is not required to change his or her password upon next login. By default, this option is checked.
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.

Table 8-4 Field Descriptions for the Create New Prime Optical User Wizard (continued)

Field	Description
User Login Sessions	Select whether to allow single or multiple user logins.
Assign Objects to User Pane	
(*for Provisioner and Operator users only*)	
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: • Contain at least six alphanumeric characters, but not more than ten. • 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.

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 8-5 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**. See Table 8-5 for more information on **Modify User Properties** Wizard field descriptions.

Step 5 (Optional) For Provisioner/SecurityProvisioner, Operator/SecurityOperator, 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 8-5.

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 8-5 Field Descriptions for the Modify User Properties Wizard

Field	Description
Cisco Prime Optical User Properties Pane	
Username	*Display only.* 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. **Note** After the username is set, it cannot be changed without deleting the user.

Table 8-5 Field Descriptions for the Modify User Properties Wizard (continued)

Field	Description
User Password	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: • 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. **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 ten passwords.
Confirm Password	Retype the password to confirm it. **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	User's privilege level.
Domain Name	Domain name. When the user logs in to the system, he or she sees all the devices contained within this domain.
Login State	Permit (enable) or prevent (disable) the user from logging in to 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. The Cisco default is 0, meaning the account will not be disabled automatically as a result of nonuse.
Require Password Change on Next Login	If checked, the user is prompted to change his or her password upon next login to the Prime Optical client. If unchecked, the user is not required to change his or her password upon next login. By default, this option is checked.
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 8-5 Field Descriptions for the Modify User Properties Wizard (continued)

Field	Description
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: • Contain at least six alphanumeric characters, but not more than ten. • 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.

Deleting a Prime Optical User

Note
- This functionality is disabled when Prime Optical is installed as part of Prime Central.
- Only Administrator user profiles can delete certain users. For more information, see Table 8-1, "Prime Optical Default User Profiles," on page 3.

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 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.

Viewing Logged In Prime Optical Users

The **Active User Sessions** table lists the Prime Optical users who are currently logged in to the Prime Optical application. Users with SysAdmin and SuperUser user profile privileges can only view this table. For more information on user profiles, see Table 8-1.

In the **Cisco Prime Optical Portal** window, choose **Administration > Active User Sessions**. Table 8-6 provides descriptions.

Table 8-6 Field Descriptions for the Active User Sessions Table

Field	Description
Username	Name of the user who is currently logged in.
Application	Type of application. Options are: • Domain Explorer • Prime Optical Web Portal
Host IP Address	IP Address of the machine where the client session started.
Hostname	(Optional) Name of the host where the client session started.
Date/Time Logged In	(Optional) Login session start date and time, with time zone.
Date/Time Launched	Application (web client or client) session start date and time, with time zone.
Last keepalive	(Optional) Last hello invocation date and time, with time zone.

Ending an Active Prime Optical User Session

Users with proper user profile and/or privileges can terminate (force logout) another user's session of the Cisco Prime Optical Portal and/or of the Prime Optical client. For more information on user profiles, see Table 8-1.

Step 1 In the **Cisco Prime Optical Portal** window, choose **Administration > Active User Sessions**.

Step 2 In the **Active User Sessions** table, select the user whose session will be ended and click the **Log Out** button.

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

Step 3 Click the **Log Out** button. The following prompt occurs:

```
This operation will logout the selected session.
Do you wish to continue?
```

If the closing session is a client, a warning dialog will open at the closing client, displaying the following message:

```
EID-411: This session has been logged out. The client will be closed.
```

If a user tries to log out from a Prime Optical Web Client session, the following error message is displayed:

```
Cannot logout the current session!
```

Viewing a List of Failed Login Attempts

A user with the proper user profile privileges can view a list of failed login attempts. For more information on user profiles, see Table 8-1, “Prime Optical Default User Profiles,” on page 3.

In the **Prime Optical Web Client** window, choose **Administration > Failed Login Attempts**.

Table 8-7 Field Descriptions for the Failed Login Attempts Table

Field	Description
USERNAME	Username 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 in to the Prime Optical client and failed.

Note Attempts made using usernames that do not exist are reported as "UNKNOWN" in the User Name column.

Setting User Interface Preferences

Prime Optical UI has been enhanced to make it compliant with accessibility recommendations. Accessibility is the degree to which a product, device, service, or environment is available to as many users as possible. Accessibility can be viewed as the ability to access and benefit from some system or entity.

The concept often focuses on users with disabilities or special needs.

The **User Interface Preferences** page consists of **Text Size** and **Contrast Level** settings. For more information on UI preferences, see Table 8-8.

Table 8-8 Field Descriptions for the UI Preferences

Field	Description
Text Size	Choose the text size from the following options: • Small (8 points) • Medium (11 points) • Large (16 points)
Contrast Level	Choose the contrast level from the following options: • Medium • High
Activate Simplified UI	Check the **Activate Simplified UI** check box to activate all the UI pages. The UI pages displays the non-focusable elements having an additional control of describing the entire access to the UI page.

In the **Prime Optical Web Client** window, choose **Administration > UI Preferences**.

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/

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 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:

a. In the **Change Password** dialog box, enter the current password in the **Current Password** field.

b. Enter the new password in the **New Password** field. For password constraints, see Table 8-9.

c. Confirm the new password.

Table 8-9 Field Descriptions for the Change Password Dialog Box

Field	Description
Password	
Current Password	Enter the old user password.
New Password	Enter the new login password. The password complexity is configurable in the **Control Panel > Security Properties** pane. By default, the new password must: • 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. **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 ten passwords.
Confirm Password	Retype the password to confirm it.

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.

Note Prime Optical schedules a job for CTC-based NEs.The event status are updated in 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. Table 8-10 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** tab, 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** tab, you can view the advisory message before saving it. Click **Apply**.

Table 8-10 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 8-10 Field Descriptions for the Security Advisory Message Management Wizard (continued)

Field	Description
Text	Security advisory message present on the selected NE. If no message exists, you can use this tab to enter a new message. You can use the following HTML commands to format the text: Begins boldface font Ends boldface font Aligns type in the center of the window Ends the center alignment <font=*n*, where *n* = point size> Changes the font to the new size Ends the font size command <p> Creates a line break _{Begins subscript } Ends subscript ^{Begins superscript } Ends superscript <u> Starts underline </u> Ends underline
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.

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. Table 8-11 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 8-11 Field Descriptions for the User Preferences Dialog Box

Field	Description
Event Notification Tab	
Show Notification Dialog For	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. **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.
Play Audible Notification For	Select an audible alert sound when a specific alarm or event occurs on an NE or on the Prime Optical application. You can specify the alarm severity that generates an audible alert and can also specify the 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. You can also choose the other sound file using **Browse** button to play the customized sound rather than the default sound. Uncheck this check box to disable continuous audible notifications. **Note** Selections that apply to NEs are allowed only if you have NEs assigned to you. Selections that apply to EMS are allowed only if you have the appropriate user privileges. You can choose *.wav, *.aif, *.au file formats only with the following encoding: • ALAW • PCM_FLOAT • PCM_SIGNED • PCM_UNSIGNED • ULAW **Note** The encoding must be supported by a sound card (hardware). Maximum duration for the sound file is 5 seconds.
Miscellaneous Tab	
Display Log/15-Min PM Data For	Change the time period used to display time-sensitive data in 15-minute increments. **Note** This field is visible only if you have read permission for the Performance Monitor operation. **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.
Display 1-Day PM Data For	Change the time period used to display time-sensitive data in 24-hour increments. **Note** This field is visible only if you have read permission for the Performance Monitor operation.

Table 8-11 Field Descriptions for the User Preferences Dialog Box (continued)

Field	Description
Table Export Encoding	Change the encoding to use when you export a table to a text file. Options are: • 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.
Enable Refresh Data Timer	The automatic **Refresh Data** feature automatically refreshes all data being displayed by Prime Optical. You receive the following prompt: `Refresh Data action suggested. This action will result in closing all windows and might take some time. Do you want to continue? {Yes | No}` 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.
Do Not Display User Profile Creation Warning Messages	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.
Enable NE Aliases	When checked, it allows you to view the alias names for the following attributes: • Node ID • Link name • Circuit name The alias name can be displayed instead of the NE ID in the following windows: • 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.	

Table 8-11 Field Descriptions for the User Preferences Dialog Box (continued)

Field	Description
Time Display	Select 12-hour format or 24-hour format for the display of time information. Options are: • 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	Select the time zone for the date display (*month/day/year* or *day/month/year*). Options are: • 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 (*day/month/year*). • 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.

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.

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 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, NCS 2002 SONET, NCS 2002 SDH, NCS 2006 SONET, and NCS 2006 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 Table 8-12. 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 8-12 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; the Cisco default is 30. 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.
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. A value of 0 disables this feature.
Differ From Previous Password by *n* Characters	Number of characters by which the new password must differ from the previous one. The range is from 1 to 5; the Cisco default is 3.

Table 8-12 Field Descriptions for the Security Properties Pane (continued)

Field	Description
Compare Against Previous *n* Passwords	Number of previously used passwords to compare against the new password. The range is from 0 to 15; the Cisco default is 5. A value of 0 disables this feature.
Password Complexity Rules Area	
Minimum Password Length	Minimum. The range is from 2 to 10; the Cisco default is 6.
Maximum Password Length	Maximum. The range is from 10 to 15; the Cisco default is 12.
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.
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.
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.
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.
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 Set to Use	Special character set to use: • 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 8-12 Field Descriptions for the Security Properties Pane (continued)

Field	Description
Prime Optical Server - FTP Connection Username	Username that the Prime Optical server uses to connect to FTP for software download, memory backup, and memory restore. **Caution** An FTP account must already exist on the server in order for the file transfer to work correctly.
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	Username that the Prime Optical server uses to connect to ONS 15216 OADM NEs. **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.
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	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 CISCO15. The account specified on the NE for Prime Optical to use must be a SuperUser-level account. When ONS 15454 NEs are present, please do the following: • If there are only ONS 15454 NEs with Release 10.6 or later, enter **ROOT15** as the username. • If there are only ONS 15454 NEs prior to Release 10.6, enter **CISCO15**. • If there are a mix of ONS 15454 NEs with Release 10.6 and earlier, you must first enter **ROOT15** as the username and then configure the NE authentication credentials for releases prior to Release 10.6 as CISCO15 using the **NE Authentication** tab. See the "Setting NE Authentication" section on page 8-43. 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. The default username is configured as CISCO15 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 CISCO15.
Password	Password to use for Prime Optical server connections. For the ONS 15454 SDH, this is also the password to use for ML-series card and TL1 tunnel NE connections. **Note** The default password is configured as **CTM123+** for the ML cards specified in the default Cisco IOS configuration file.
Confirm Password	Re-enter the password to confirm it.

Table 8-12 Field Descriptions for the Security Properties Pane (continued)

Field	Description
CTC-Based SONET Tab	
Username	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 **CISCO15**. The account specified on the NE for Prime Optical to use must be a SuperUser-level account. When ONS 15454 NEs are present, please do the following: • If there are only ONS 15454 NEs with Release 10.6 or later, enter **ROOT15** as the username. • If there are only ONS 15454 NEs prior to Release 10.6, enter **CISCO15**. • If there are a mix of ONS 15454 NEs with Release 10.6 and earlier, you must first enter **ROOT15** as the username and then configure the NE authentication credentials for releases prior to Release 10.6 as CISCO15 using the **NE Authentication** tab. See the "Setting NE Authentication" section on page 8-43. 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. 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.
Password	Password to use for Prime Optical server connections. 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. 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.
Confirm Password	Re-enter the password to confirm it.
CTC-Based SDH and CTC-Based SONET Tabs	
Server - SNMP Connection Area **Note** After changing the field values in the Server - SNMP Connection area, mark the NEs as **Out of Service** and then In Service.	
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 SNMPv3user. Values are None, MD5, or SHA.
Authentication Password	Enter the password used to authenticate the SNMPv3 user. The password must contain: • 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) Regardless of the actual length of the password, the Password and Confirm Password fields display only a fixed-length string of 15 asterisks (*).
Confirm Authentication Password	Re-enter the authentication password to confirm it.

Table 8-12 Field Descriptions for the Security Properties Pane (continued)

Field	Description
Privacy Protocol	Select the privacy protocol for the SNMPv3 user. You can choose one of the following: • 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.
CRS Tab	
Username	Username that the Prime Optical server uses to connect to CRS NE.
Password	Password to use for Prime Optical server connections to CRS NE.
Confirm Password	Re-enter the password to confirm it.

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.

Table 8-13 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 Target** area.

- 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 8-13 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.

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. Table 8-14 provides descriptions.

Table 8-14 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.

Managing Prime Optical User Profiles

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

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). Table 8-15 provides descriptions.

Table 8-15 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: • Assign all NEs—SuperUser, NetAdmin • Assign NEs—Operator, Provisioner • Assign No NEs—SysAdmin
Profile Type	Displays the profile type. Values are: • Default • Custom
Description	Description of the user profile.
State	Displays the current profile status. Values are: • Enable • Disable

Adding a Custom User Profile

Use the **Create New User Profile** wizard to add Prime Optical user profiles. Table 8-16 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
- Role
- Visible Alarms (only for admin users)
- Description
- User Profile Privileges

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.
- You must select privileges for all possible operations even if related modules (NEs, GateWay/CORBA, cards, etc.) are not currently installed on the server.
- Only a Super user can view critical alarms. The new user created cannot view the critical alarms.

The **Create New User Profile** Wizard allows you to select a set of Alarm Conditions

For new custom profile alarms in the **Create New User Profile** Wizard, follow these steps:

1. Click the **Set All Read Only** button.
2. Click **Next**.

   A warning message is displayed. Click **Ok**. A dialog box is displayed.
3. Enter the custom alarm profile that you created and select the profile from the **Conditions** area.

   The selected custom profile gets added under the Selected Items area.

Note The **Create New** Wizard for custom profile is displayed only when you select the Select option under Visible Alarms. This feature is not applicable on the **Link** table, network map, and circuit trace.

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 Setting User Preferences, page 8-27 for more information.)

Table 8-16 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 forty 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: • Assign All NEs—SuperUser, NetworkAdmin • Assign NEs—Operator, Provisioner, SecurityOperator, SecurityProvisioner • Assign No NEs—SysAdmin, SecurityAdmin
Role	Transport or Security roles assigned to every user profile. Select **Transport** or **Security** role check box from the Role option. **Note** After a profile is saved, you cannot change the assigned role.
Visible Alarms	Allows you to select the alarms. Available options are: • All—For all alarms. • Select—For specific user profile alarms only.

Table 8-16 Field Descriptions for the Create New User Profile Wizard (continued)

Field	Description
Description	Enter a description of the new user profile.
User Profile Privileges	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. • 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. **Note** Click the **Set All Read Only** button for LOS alarms only. • 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. 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. You can export **User Privileges** specific to a user or all users. **Note** Exporting data can be performed for both HTML and CSV data export. • Click **Generate HTML Report** or **Export Data to File** in **Launch User Profile** Table wizard. A **HTML Report** window is displayed. Following options are available: Export Which Rows? – Selected Rows radio button – All rows in current page radio button – Export Profile Privileges check box Check the **Export Profile Privileges** check box to export the user profile name and the related information, along with the category wise distribution of the operations and the respective permissions. For more information on exporting profile privileges, see Exporting Data.

Modifying a User Profile

Use the **Modify User Profile** wizard to modify Prime Optical user profiles. Table 8-16 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
- Role
- Visible Alarms (only for admin users)
- 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.
- Topology modification is not allowed for custom users.

The **Create New User Profile** Wizard allows you to select a set of **Alarm Conditions**.

For new custom profile alarms in the **Create New User Profile** Wizard, follow these steps:

1. Click the **Set All Read Only** button.
2. Click **Next**.

   A warning message is displayed. Click **Ok**. A dialog box is displayed.
3. Enter the custom alarm profile that you created and select the profile from the **Conditions** area.

   The selected custom profile gets added under the **Selected Items** area.

Note The **Create New** Wizard for custom profile is displayed only when you select the Select option under Visible Alarms. This feature is not applicable on the **Link Table, Network Map**, and **Circuit Trace**.

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 Setting User Preferences, page 8-27 for more information.)

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 Deleting a Prime Optical User, page 8-21.

Duplicating a User Profile

Use the **Domain Explorer** 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 Table 8-17 for name constraints.

Step 5 Click **OK**.

Table 8-17 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 forty 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 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.

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 **Domain Explorer** window.

Step 1 In the **Domain Explorer** window, choose **Administration > CTC-Based NEs**, **ONS 15216 > NE Authentication**. The **NE Authentication** dialog box opens. Table 8-18 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 8-18 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 in to 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**.

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 **Domain Explorer** window, select the NE node.

Step 3 In the node properties pane of the **Domain Explorer** window, click the **Security** tab.

Step 4 Complete the following information in the **Policy** tab:

- 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 in to 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 in days. The range is from 1 to 99; the Cisco default is 45.

Step 5 Complete the following information in the **Password** tab:

- 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 range is from 1 to 5. The default value is 1.
- 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** tab 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—Specify the restore timeout period in minutes. 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; the Cisco default is 5.
- 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** tab 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—Specify the restore timeout period in minutes. 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; the Cisco default is 5.
- 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—Choose 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 **TL1 Access** area:
  - Access State—Choose the TL1 access state from the drop-down list. You can select Disable, Non-secure, or Secure.
- In the **SNMP Access** area:
  - Access State—Choose the SNMP access state from the drop-down. You can select either Disable or Non-secure.
- In the **Other** area:
  - PM Clearing Privilege—Choose the user privilege that allows clearing PM statistics for the NE.
- In the **EMS Access** area:
  - Access State—Choose 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 (SSLIOP) 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 (SSLIOP) listener port is 684.

    Other Constant—When selected, enter the port number that will be used.

Step 8 Complete the following in the **RADIUS Server** tab 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.

  Table 8-19 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 Managing RADIUS Servers, page 8-48 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** tab:

- In the **Advisory Message** tab, 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** tab, you can view the advisory message before saving it.

Step 10 Click **Apply**.

Table 8-19 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.

Managing RADIUS Servers

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 **Domain Explorer** window, select the NE node.

Step 3 In the properties pane of the **Domain Explorer** window, click the **Security** tab > **RADIUS Server** tab.

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.

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** tab.

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.

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** tab.

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.

Managing NE User Access

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

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**. Table 8-20 provides descriptions.

Table 8-20 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 (*CTC-based NEs only*)	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 in to 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.

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**. Table 8-21 provides descriptions.

Table 8-21 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.

Table 8-21 Field Descriptions for the NE User Access Administration Table (continued)

Field	Description
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. • 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.

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 Table 8-22.

Step 3 After making your selections, click **OK** to run the filter.

Table 8-22 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.

Adding an NE User

Use the **Add NE User** wizard to add new users to ONS 15216 EDFA3, or CTC-based NEs. Table 8-23 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 8-23 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	
Username	Username for the new user. • 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 six but not more than ten alphanumeric characters. ONS 15216 EDFA3 NEs support only a single TL1 session for each username.
New Password	User password. • 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 seven but not more than ten ASCII characters, where at least two characters are nonalphabetic and at least one character is a special character (+, #, %). For example, *jpasswd#1* is an acceptable password. The password cannot contain the username. For example, if the username is *CISCO15*, the password cannot be *CISCO15#*. The password is case-sensitive.

Table 8-23 Field Descriptions for the Add NE User Wizard (continued)

Field	Description
Verify/Confirm Password	Re-enter the password to confirm it.
Privilege (*for CTC-based and ONS 15216 EDFA3 NEs*)	Privilege level for the new NE user. • 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. – 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.

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 8-24 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:

a. 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.

b. 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.

c. 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.

d. 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 8-24 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	

Table 8-24 Field Descriptions for the Add Predefined User Wizard (continued)

Field	Description
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.

Modifying an NE User Profile

Use the **Modify NE User** wizard to make changes to existing NE users. Table 8-25 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 NEs 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 8-25 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. • 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 seven but not more than ten ASCII characters, where at least two characters are nonalphabetic and at least one character is a special character (+, #, %). For example, *jpasswd#1* is an acceptable password. The password cannot contain the username. For example, if the username is *CISCO15*, the password cannot be *CISCO15#*. The password is case-sensitive.
Verify/Confirm Password	Re-enter the modified password to confirm it.
Privilege (*for CTC-based and ONS 15216 EDFA3 NEs*)	Modify the privilege level of the user. • 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.

Table 8-25 Field Descriptions for the Modify NE User Wizard (continued)

Field	Description
Timeout (*for ONS 15216 EDFA3 NEs*)	*Display only.* 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. • 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.
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.

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 Ending an Active NE User Session, page 8-60. 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 NEs 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.

Viewing Active NE Users

The **NE Active Users** table displays information about the users who are currently logged in to selected NEs in Prime Optical. Table 8-26 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 8-26 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 (*CTC-based NEs only*)	IP address of the client workstation from which the user has logged in.
Session Type (*CTC-based NEs only*)	Type of active user session (EMS, Telnet, and so on). Prime Optical and CTC sessions are identified as "EMS." This field applies only to the following CTC-based NEs: • 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 8-26 Field Descriptions for the NE Active Users Table (continued)

Field	Description
Last Activity Time (*CTC-based NEs only*)	Date and time when the last activity was performed by the active user on the NE. This field applies only to the following CTC-based NEs: • 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 (*CTC-based NEs only*)	Date and time when the active user logged in to the NE. This field applies only to the following CTC-based NEs: • 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.

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 Table 8-27.

Step 3 After making your selections, click **OK** to run the filter.

Table 8-27 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.

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**.

Managing CTC User Profiles

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

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. Table 8-28 provides descriptions.

Table 8-28 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.

Creating a CTC User Profile

Use the **Add New CTC User Profile** dialog box to add new CTC user profiles to the database. Table 8-29 provides descriptions.Table 8-29

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 8-29 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 forty 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.

Modifying a CTC User's Properties

Use the **Modify CTC User Profile** dialog box to make changes to an existing CTC user profile. Table 8-30 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 8-30 Field Descriptions for the Modify CTC User Profile Dialog Box

Field	Description
User ID	*Display only.* Name of the user profile. The profile name must contain from six to forty 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 username is set, it cannot be changed without deleting the user.
User Password	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. **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 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.

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.

Managing Cisco IOS Users

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

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. Table 8-31 provides descriptions.

Table 8-31 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.

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. Table 8-32 provides descriptions.

Step 3 In the **IOS Card Selection** window, complete the following substeps:

a. Select the NE ID on which you want to create a new Cisco IOS user.

b. 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.

c. 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 8-32 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.

Table 8-32 Field Descriptions for the IOS User Creation Wizard (continued)

Field	Description
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.

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. Table 8-33 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 8-33 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	*Display only.* 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.

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.

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 Configuring SNMPv3 Parameters, page 8-66 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 Viewing SNMPv3 Tables, page 8-68 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 Deleting SNMPv3 Users from the SNMPv3 Tables, page 8-72.
4. Provision rows in the **SNMPv3** tables. The **SNMPv3** wizard also allows you to add entries to one or more **SNMPv3** tables. See Configuring SNMPv3 Parameters, page 8-66 for details.

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 Managing SNMPv3—CTC-Based Release 9.6 NEs, page 8-65. 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:

a. Enter the following view information:
   - Name—Name of the MIB view.
   - Subtler 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.

b. 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:

a. Enter the following information in the User area:
   - Username—SNMPv3 username.
   - Group name—Name of the group to which the user belongs.

b. Enter the following information in the Authentication area:
   - Protocol—Protocol used to authenticate the SNMPv3 user.
   - Password—Password used to log in to the Prime Optical server.
   - Confirm Password—Re-enter the password to confirm it.

c. 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**).

Viewing SNMPv3 Tables

The **SNMPv3** tables are grouped according to Table 8-34 types:

- User tables:
  - SNMPv3 NE Users Table, page 8-68
  - SNMPv3 NE MIB Views Table, page 8-69
  - SNMPv3 NE Groups Table, page 8-69
- Trap tables:
  - SNMPv3 NE Trap Destinations Table, page 8-70
  - SNMPv3 NE Notification Filters Table, page 8-70
- Proxy server tables:
  - SNMPv3 NE Proxy Forwarder Table, page 8-71
  - SNMPv3 NE Proxy Trap Forwarder Table, page 8-71
  - SNMPv3 NE Remote Users Table, page 8-72

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. Table 8-34 provides descriptions.

Table 8-34 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.

Table 8-34 Field Descriptions for the SNMPv3 NE Users Table (continued)

Field	Descriptions
Authentication Protocol	Protocol used to authenticate the SNMPv3 user. Valid values are MD5 or SHA.
Privacy Protocol	Protocol used for encryption.

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. Table 8-35 provides descriptions.

Table 8-35 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.

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. Table 8-36 provides descriptions.

Table 8-36 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.

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. Table 8-37 provides descriptions.

Table 8-37 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 SNMPv3 NE Proxy Trap Forwarder Table, page 8-71 for more information.

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. Table 8-38 provides descriptions.

Table 8-38 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.

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. Table 8-39 provides descriptions.

Table 8-39 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.

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. Table 8-40 provides descriptions.

Table 8-40 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.

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. Table 8-41 provides descriptions.

Table 8-41 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.

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.

Adding and Deleting a Static Entry

The adding static entry allows you to view and manage the TARP data cache (TDC). The TDC facilitates Target Identifier Address Resolution Protocol (TARP) processing by storing a list of **TID to NSAP** mappings.

To add a new static entry, do the following:

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **OSI > TARP-TDC** tab.

Step 2 Click **Add Static Entry**.

A **Create New** window opens. Enter the following:

- TID—Enter the TID of the NE. (For ONS nodes, the TID is the Node Name parameter on the node or multishelf view **Provisioning > General** tab.)
- NSAP/NET—Enter the OSI NSAP address in the **NSAP** field. The NSAP that is statistically linked to the TID.

Step 3 Click **OK** to close the **Create New window**.

To delete a static entry, do the following:

Step 1 Click the **OSI > TARP-TDC** tab.

Step 2 Select a static entry that you want to delete.

Step 3 Click **Delete Selected Entry**.

Step 4 Click **Yes** in the confirmation dialog box.

Querying for a NSAP that Matches a TID

Querying for an Network Service Access Point (NSAP) allows you to view and manage the TARP data cache (TDC). The TDC facilitates TARP processing by storing a list of Terminal Identifier (TID) to Network Service Access Point (NSAP) mappings.

Note The TID to NSAP function is not available if the TDC is not enabled on the **TARP-Config** tab.

To query the network for an NSAP that matches a TID, do the following:

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **OSI > TARP-TDC** tab

Step 2 Click **TID to NSAP**.

A **TID to NSAP** window opens.

Step 3 Enter the TID you want to map to an NSAP.

Step 4 Click **OK**, then click **OK** in the information message box.

Step 5 On the **TDC** tab, click **Refresh**.

If TARP finds the TID in its TDC, it returns the matching NSAP. If not, TARP sends protocol data units (PDUs) across the network. Replies returns to the TDC later, and a check TDC later message is displayed.

Creating and Deleting a TARP Manual Area Adjacency

This task adds an entry to the TARP manual adjacency table (MAT). Entries are added to the MAT when the NE must communicate across routers or non-SONET NEs that lack TARP capability.

To create a TARP manual area adjacency, do the following:

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **OSI > TARP-MAT** tab.

Step 2 Click **Add.**

A **Create New** window opens.

- Enter the level for the TARP Type Code that will be sent in the **Level** field. Values are:

  - Level 1—Indicates that the manual area adjacency is within the same area as the node. The entry generates Type 1 PDUs.
  - Level 2—Indicates that the manual area adjacency is in an area different from that of the node. The entry generates Type 2 PDUs.
- Enter the NSAP address of the node at the other end of the TARP manual adjacency in the **NSAP** field.

Step 3 Click **OK** to close the **Create New** window.

To delete a TARP manual area adjacency, do the following:

Step 1 Click the **OSI** > **TARP-MAT** tab.

Step 2 Select a the TARP manual area adjacency.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the confirmation dialog box.

Modifying a OSI Virtual Router

To view and manage the OSI virtual routers, do the following:

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **OSI** > **Routers-Setup** tab.

Step 2 Chose the router you want provision and click **Edit**.

The **Edit** window opens. Modify the details as in Table 8-42.

Table 8-42 Field Descriptions for Routers-Setup Tab

Field	Description
Router Number	Displays the virtual router number.
System ID	Displays the NSAP system ID of the virtual router. The NSAP system identifier is set to the node's first IEEE 802.3 MAC address + *n*, where *n* = 0 through 6. For the primary router (Router 1), *n* = 0.
Status	Indicates the virtual router status. Choose Enabled or Disabled from the drop-down list. **Note** Router 1 must be enabled before additional routers can be enabled.
Primary Area Address	Indicates the primary manual area address. For Router 1, this is the main NET for the node; that is, the NSAP without the system ID and selector (set to 00) fields.

Table 8-42 Field Descriptions for Routers-Setup Tab (continued)

Field	Description
Manual Area Address 1	Indicates the address of any additional manual areas that are created. **Note** An OSI area allows up to two additional manual areas in addition to the primary manual area.
Manual Area Address 2	Indicates the address of any additional manual areas that are created. **Note** An OSI area allows up to two additional manual areas in addition to the primary manual area.

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

Enabling, Modifying and Deleting a Subnet

To enable a LAN subnet:

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **OSI > Subnets** tab.

Step 2 Click **Enable LAN Subnet**.

The **Enable LAN Subnet** window opens.

Step 3 Enter the details as in Table 8-43.

Table 8-43 Field Descriptions for the Subnets Tab

Field	Description
Router Number	The OSI virtual router where the subnet (SDCC, LDCC, GCC, or OSC) is provisioned.
ISH (sec)	The intermediate system hello (ISH) PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the NETs they serve. The Cisco default is 10 seconds; the range is from 10 to 1000 seconds.
ESH (sec)	The end system hello (ESH) PDU propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs they serve. The Cisco default is 10 seconds; the range is from 10 to 1000 seconds.
IIH (sec)	The intermediate system-to-intermediate system hello (IIH) PDU propagation frequency. The IS-IS hello PDUs establish and maintain adjacencies between ISs. The Cisco default is 3 seconds; the range is from 1 to 600 seconds.
DIS Priority (sec)	The designated intermediate system (DIS) priority. In IS-IS networks, one router is elected as the DIS. For Cisco routers, the DIS priority is 64.
IS-IS Cost (sec)	The cost for sending packets on the subnet. This is used by OSPF routers to calculate the shortest path. The Cisco default value is 20.

Step 4 Click **OK**.

To edit a LAN Subnet:

Step 1 Click the **OSI > Subnet** tab.

Step 2 Click **Edit**.

The **Edit** window opens.

Step 3 Make the necessary modification as in Table 8-43.

Step 4 Click **OK**.

To delete a LAN Subnet:

Step 1 Click the **OSI > Subnet** tab.

Step 2 Select a subnet and click **Delete**.

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

Creating, Editing and Deleting a GRE Tunnel Route

Note The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and the node.

To create a GRE Tunnel Route:

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **OSI > Tunnels** tab.

Step 2 Click **Create**.

The **Create New** window opens. Enter the details as in Table 8-44.

Table 8-44 Field Descriptions for the Tunnels Tab

Field	Description
Tunnel Type	Choose the Tunnel Type between GRE and Cisco.
IP Address	Displays the IP address of the GRE destination Prime Optical or CTC computer.
Netmask Address	Displays the IP address subnet mask of the destination Prime Optical or CTC computer.

Table 8-44 Field Descriptions for the Tunnels Tab (continued)

Field	Description
NSAP Address	The destination NE NSAP address. The NSAP selector (last two NSAP characters) must be 2f (GRE tunnel) or cc (proprietary Cisco tunnel), depending on which tunnel type you want to create. The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add an encapsulation header for each IP packet, while the GRE tunnel adds a small header to the packets. The two tunnel types are incompatible. **Note** Most Cisco routers support the Cisco tunnel, while only a few support both GRE and Cisco IP tunnels.
OSPF Metric	Displays the cost for sending packets across the GRE tunnel. Cost is used by OSPF routers to calculate the shortest path.

Step 3 Click **OK**.

To edit a GRE Tunnel Route:

Step 1 Click the **OSI** > **Tunnels** tab.

Step 2 Click **Edit**.

The **Edit** window opens.

Step 3 Choose the Tunnel Type between **GRE** and **Cisco**.

Step 4 Make the necessary modification as in Table 8-44.

Step 5 Click **OK**.

To delete a GRE Tunnel Route:

Step 1 Click the **OSI** > **Tunnels** tab.

Step 2 Select a the GRE tunnel route and click **Delete**.

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

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

This section describes how to perform audit logs, including:

- Viewing the Audit Log, page 8-79
- Filtering Audit Log Data, page 8-79
- Working With Audit Log Custom Views, page 8-80

- Configuring Audit Log Settings, page 8-84

Viewing the Audit Log

To view the **Audit Log**, choose **Administration > Audit Log** in the **Domain Explorer** window. Table 8-42 provides descriptions.

Table 8-45 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 *Internal*.
Service	Name of the service that generated the **Audit Log** entry.
Time Stamp (*time zone*)	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 *CTM* as the source ID.

Filtering Audit Log Data

To filter **Audit Log** data or create a custom view, do the following:

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

Step 2 From the **Show** drop-down list, choose one of the following options:

Table 8-46 Audit Log Filters

Option	Description
All	Displays all records.
Simple Filter	Displays all records that contain the text you entered.
Custom View	Creates a custom view with selected filter criteria for each column. For more information on creating custom views, see Creating Audit Log Custom Views, page 8-80.
Manage Custom Views	Edits or deletes a custom view. For more information on managing custom views, see Managing Audit Log Custom Views, page 8-84.

Note

- The number of records that is displayed on each page can be configured in the **Audit Log Settings** window. For more information on **Audit Log** settings, see Working With Audit Log Custom Views, page 8-80.
- To only search text within the records of the current page, check the **Quick Filter** check box from the **Audit Log** toolbar and enter search criteria.

Working With Audit Log Custom Views

The following sections describe how to create, filter, and manage custom views:

Creating Audit Log Custom Views

To create a custom view, do the following:

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

Step 2 From the **Show** drop-down list, choose **Custom View.**

Step 3 Set match rules. See "Match Rules" section on page 8-80 for field descriptions.

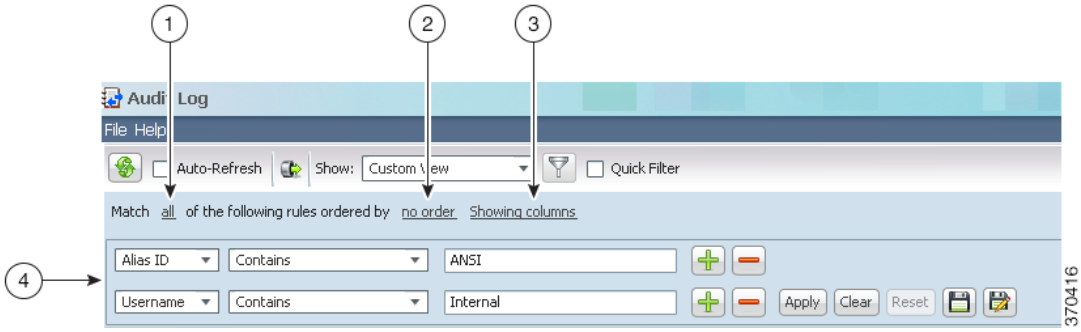
Step 4 Set filter criteria. See "Filtering Audit Log Custom Views" section on page 8-82 for filter criteria.

Step 5 To save this view, see "Saving Audit Log Custom Views" section on page 8-83.

Match Rules

The **Match Rules** area dictates what and how the values in the custom view are displayed.

Figure 8-1 Match Rules



Number	Element	Description
1	Match Rule	Allows you to combine multiple filters.
2	Order Rule	Allows you to order the filtered data.
3	Showing Rule	Allows you to display all or selected column names.
4	Filters	Allows you to filter the data on various criteria.

Table 8-47 describes the Match Rules options.

Table 8-47 Match Rules

Match Rule	Description
All/Any	Enables you to combine multiple filters. The default value displayed is **All**. Click the **All** link to change this option. You can choose one of the following options: • Any—Matches any one of the conditions to filter and display the data. • All—Matches all the conditions.
Order Rule	Enables you to order the filtered data. The default value displayed is **No Order**. Click **No Order** link if you want to view the order rule values in ascending or descending order. To view what columns are sortable, see Table 8-45.
Showing Columns	When the **Showing Column** link is selected, a window with the available and visible columns is displayed. You can choose one of the following options: • Available—Displays all the column names that the **Audit Log** contains. You can move the column name from left to right and vice versa using the navigational buttons. **Note** Double-click the column name to move the column name from Available text box to Visible text box and vice versa. • Visible—Displays the column names that you want to display in the customized configuration view.

Filtering Audit Log Custom Views

To filter **Audit Log** data in a custom view, do the following:

Step 1 Choose the column name and filtering option from the drop-down lists. Different options are available for each column. See Table 8-48 for more information on the available options and search functionality.

Note Filtering options are displayed based on the column selected.

Table 8-48 Filter Criterion

Column Name	Filtering Options	Search Text
• Alias ID • Username • Service • Message • Source ID	• Contains • Does Not Contain • Is Empty • Is not Empty	Enter the search text in the text box to filter the records.
Time Stamp	• Is between • Is before • Is after • Past 1 hour • Past 6 hours • Past 12 hours • Past 1 day • Past 2 day • Past 3 days • Past 4 days	Filter **Audit Log** data for a specified time period, ranging from the past hour to the past 4 days. Use the calendar icon to choose the time, day, month, and year. Click **OK** to choose the time you selected. Click **Now** to select the current time.
Category	• Equals • Does not Equal	Click the **Browse** button. The different options under the category is displayed. Check the check box to pick the desired category. The category selected gets displayed under the selected items. Click **Done**. The selected category details is displayed in the search text box.

Step 2 If necessary, add or delete filter criterion by clicking the + or - icon.

Step 3 Click **Apply**. The next time you open the **Audit Log**, the last custom view you created is displayed.

The **Audit Log** is displayed based on the set conditions. See Action Buttons, page 1-50 for more information.

Saving Audit Log Custom Views

Note All the filter options must be configured correctly before you save a custom view.

To save a custom view, do the following:

Step 1 Click on the **Save** icon.

Step 2 Enter the custom view name in the **Filter Name** text box.

Step 3 From the **Visibility** drop-down list, choose Public or Private.

The custom views are stored in the following two folders:

- Public—Contains the customized view reports that the SuperUser created. Users who have read/write privileges for public filter management operations can edit or remove public custom views. You can make a copy of the other users' custom views using the **Save As** button.
- Private—Contains the customized view details that you created.

Note The custom view name is unique in Public and Private folders. But you can create a custom view name that the SuperUser has created.

Step 4 Click **Save**.

Copying or Renaming Audit Log Custom Views

To copy or rename a custom view, do the following:

Step 1 Select the custom view from the public or private folder.

Step 2 Click the **Save As** icon. The **Save a Custom View** dialog box is displayed.

Tip Enter the custom view name in the **Name** text box.

Step 3 Choose **Visibility** from the drop-down list.

Step 4 Click **Save**. The custom view is saved in a different name.

Note You can make a copy of an existing custom view using the **Save As** button when you do not have Public privileges.

Managing Audit Log Custom Views

Note Users who have read/write privileges for public filter management operations can edit or remove public custom views. However, private custom views can only be managed by the user who created them.

To edit or remove a custom view, do the following:

Step 1 Choose **Manage Custom View** from the drop-down list. The **Manage Custom Views** dialog box is displayed.

Step 2 Choose **Select a Custom View** from the drop-down list.

Step 3 Do one of the following:

- Click **Edit** and modify the **Name** and **Visibility** as required. Click **Save**.
- Click **Remove.** Click **OK** to confirm that you want to delete the custom view. The selected custom view is deleted from the **Manage Custom View** list.

Configuring Audit Log Settings

To configure audit log settings, do the following:

Step 1 Click the **Audit Log Settings** icon in the top-right corner of the window.

The **Audit Log Settings** window is displayed.

Step 2 Make the necessary settings as required. See Table 8-49 for the field descriptions.

Step 3 Click **OK**.

Note Check the **Auto-Refresh** check box to refresh the window.

Table 8-49 Field Descriptions for the Audit Log Settings Dialog Box

Field	Description
Refresh period in minutes	Select the time interval (in minutes) that the data is automatically refreshed. You can select to have the data automatically refresh every 1, 3, 5, or 10 minutes. The default is 1 minute. **Note** Check the **Auto-refresh** check box to refresh the window. The Status bar displays the data from the last time it was updated. If there is any change in the group details of the **Domain Explorer**, it will automatically update the changes in the next refresh.
Records per Page	Displays the number of records shown in a single page.The default record per page is 100. **Note** You can set the minimum of 100 or the maximum of 500 records per page.

Northbound Gateway Security

OSS-to-Prime Optical sessions are configured by the Prime Optical GateWay EMS-to-NMS interface architectural component. See Managing Southbound and Northbound Interfaces for more information about Prime Optical GateWay.