CHAPTER 6

Security

This chapter provides information about Cisco ONS 15310-CL and Cisco ONS 15310-MA user security. To provision security, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Chapter topics include:

6.1 Users IDs and Security Levels

A CISCO15 user ID is provided with the ONS 15310-CL and ONS 15310-MA for use with initial login. Use this ID to set up other ONS 15310-CL and ONS 15310-MA user IDs. (For instructions, see the "Turn Up a Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.)

Note Cisco Transport Controller (CTC) does not display the CISCO15 user ID when you log in.

An ONS 15310-CL and ONS 15310-MA node can support up to 500 user IDs. Each CTC or Transaction Language 1 (TL1) user ID can be assigned one of the following security levels:

- Retrieve—Users can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance—Users can access only the ONS 15310-CL and ONS 15310-MA maintenance options.
- Provisioning—Users can access provisioning and maintenance options.
- Superuser—Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.

By default, multiple concurrent user ID sessions are permitted on the node; that is, multiple users can log into a node using the same user ID. However, you can provision the node to allow only a single login per user ID and prevent concurrent logins for all users.

See Table 6-3 on page 6-6 for idle user timeout information for each security level.

6.2 User Privileges and Policies

This section lists user privileges for each CTC action and describes the security policies available to Superusers.

6.2.1 User Privileges by CTC Action

Table 6-1 shows the actions that each user privilege level can perform in node view.

Table 6-1 ONS 15310-CL and ONS 15310-MA Security Levels—Node View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/Filter/Delete Cleared Alarms	X	X	X	X
Conditions	—	Retrieve/Filter	X	X	X	X
History	Session	Filter	X	X	X	X
	Shelf	Retrieve/Filter	X	X	X	X
Circuits	Circuits	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
	Rolls	Complete/Force Valid Signal/Finish	—	—	X	X
Provisioning	General	Edit	—	—	Partial[1]	X
	Network	General: Edit	—	—	—	X
		Static Routing: Create/Edit/ Delete	—	—	X	X
		OSPF: Create/Edit/Delete	—	—	X	X
		RIP: Create/Edit/Delete	—	—	X	X
		Proxy: Create/Edit/Delete	—	—	—	X
		Firewall: Create/Edit/Delete	—	—	—	X
	OSI	Main Setup: Edit	—	—	—	X
		TARP: Config: Edit	—	—	X	X
		TARP: Static TDC: Add/Edit/Delete	—	—	X	X
		TARP: MAT: Add/Edit/Delete	—	—	X	X
		Routers: Setup: Edit	—	—	—	X
		Routers: Subnets: Edit/Enable/Disable	—	—	X	X
		Tunnels: Create/Edit/Delete	—	—	X	X
	Protection	Create/Delete/Edit	—	—	X	X

Table 6-1 ONS 15310-CL and ONS 15310-MA Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning (continued)	Security	Users: Create/Delete/Clear Security Intrusion Alarm	—	—	—	X
		Users: Change	Same user	Same user	Same user	All users
		Active Logins: View/Logout/ Retrieve Last Activity Time	—	—	—	X
		Policy: Edit/View (Prevent superuser disable - NE Default)	—	—	—	X
		Data Comm: Edit/View	—	—	—	X
		Access: Edit/View	—	—	—	X
		RADIUS Server: Create/Edit/Delete/Move Up/ Move Down/View	—	—	—	X
		Legal Disclaimer: Edit	—	—	—	X
	SNMP	Create/Edit/Delete	—	—	X[2]	X
		Browse trap destinations	X	X	X	X
	Comm Channels	SDCC: Create/Edit/Delete	—	—	X	X
		LDCC: Create/Edit/Delete	—	—	X	X
		PPC: Create/Edit/Delete	—	—	X	X
	Timing	General/BITS Facilities: Edit	—	—	X	X
	Orderwire	Enable Buzzer	—	—	X	X
	Alarm Extenders	External Alarms: Edit	—	—	X	X
		External Controls: Edit	—	—	X	X
	Alarm Profiles	Alarm Behavior: Edit	—	—	X	X
		Alarm Profile Editor: Store/Delete[3]	—	—	X	X
		Alarm Profile Editor: New/Load/Compare/Available/ Usage	X	X	X	X
	Defaults	Edit/Import	—	—	—	X
		Reset/Export	X	X	X	X
Inventory	—	Delete	—	—	X	X
		Hard Reset/Soft Reset	—	X	X	X
Maintenance	Database	Backup	—	X	X	X
		Restore	—	—	—	X
	Network	Routing Table: Retrieve	X	X	X	X
		RIP Routing Table: Retrieve	X	X	X	X

Table 6-1 ONS 15310-CL and ONS 15310-MA Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Maintenance (continued)	OSI	IS-IS RIB: Refresh	X	X	X	X
		ES-IS RIB: Refresh	X	X	X	X
		TDC: TID to NSAP/Flush Dynamic Entries	—	X	X	X
		TDC: Refresh	X	X	X	X
	Protection	Switch/Lock out/ Lock-on/Clear/ Unlock	—	X	X	X
	Software	Download	—	X	X	X
		Activate/Revert	—	—	—	X
	Cross-Connect	Resource Usage: Delete	—	—	X	X
		Resource Usage: Refresh	X	X	X	X
	Overhead XConnect	View	X	X	X	X
	Alarm Extenders	External Alarms: View	X	X	X	X
		External Controls: View	X	X	X	X
		Virtual Wires: View/Retrieve	X	X	X	X
		Overhead Termination: View	X	X	X	X
	Diagnostic	Retrieve Tech Support Log Node Diagnostic Logs (Release 9.2)	—	—	X[2]	X
		Lamp Test	—	X	X	X
	Timing	Source: Edit	—	X	X	X
		Report: View/Refresh	X	X	X	X
	Audit	Retrieve	—	—	—	X
		Archive	—	—	X	X
	Test Access	View	X	X	X	X

1. Provisioner user cannot change node name, contact, location, or Virtual Tributary alarm indication signal (AIS-V) insertion on STS-1 signal degrade (SD) parameters.
2. Provisioner user cannot perform this task in secure mode.
3. The action buttons in the subtab are active for all users, but the actions can be completely performed only by the users with the required security levels.

Table 6-2 shows the actions that each user privilege level can perform in network view.

Table 6-2 ONS 15310-CL and ONS 15310-MA Security Levels—Network View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/Filter/Delete cleared alarms	X	X	X	X
Conditions	—	Retrieve/Filter	X	X	X	X
History	—	Filter	X	X	X	X

Table 6-2 ONS 15310-CL and ONS 15310-MA Security Levels—Network View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Circuits	Circuits	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
	Rolls	Complete/ Force Valid Signal/ Finish	—	—	X	X
Provisioning	Security	Users: Create/Delete/Clear Security Intrusion Alarm	—	—	—	X
		Users: Change	Same User	Same User	Same User	All Users
		Active logins: Logout/Retrieve Last Activity Time	—	—	—	X
		Policy: Change	—	—	—	X
	Alarm Profiles	Store/Delete[1]	—	—	X	X
		New/Load/Compare/Available/ Usage	X	X	X	X
	BLSR	Create/Delete/Edit/Upgrade	—	—	X	X
	Overhead Circuits	Create/Delete/Edit/Merge	—	—	X	X
		Search	X	X	X	X
	Provisionable Patchcords (PPC)	Create/Edit/Delete	—	—	X	X
	Server Trails	Create/Edit/Delete	—	—	X	X
	VLAN DB Profile	Load/Store/Merge/Circuits	X	X	X	X
		Add/Remove Rows	—	—	X	X
Maintenance	Software	Download/Cancel	—	X	X	X
	Diagnostic	OSPF Node Information: Retrieve/Clear	X	X	X	X
	APC	Run APC/Disable APC	—	—	—	X
		Refresh	X	X	X	X

1. The action buttons in the subtab are active for all users, but the actions can be completely performed only by the users assigned with the required security levels.

6.2.2 Security Policies

Users with the Superuser security privilege can provision security policies on the ONS 15310-CL and ONS 15310-MA. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters. In addition, a Superuser can access the ONS 15310-CL and ONS 15310-MA through the LAN port on the front of the node. If enabled in the NE defaults, superusers can be configured to override the inactive user timeout interval.

6.2.2.1 Superuser Privileges for Provisioning Users

Superusers can grant permission to Provisioning users to perform a set of tasks. The tasks include retrieving an audit log, restoring a database, clearing performance monitoring (PM) parameters, and activating and reverting software loads. These privileges, except the PM clearing privilege, can only be granted using CTC network element (NE) defaults. See Appendix C, "Network Element Defaults" for more information. To grant the PM clearing privilege using CTC, click the Provisioning > Security > Access tabs. For more information about setting up Superuser privileges, refer to the "Change Node Settings" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

6.2.2.2 Idle User Timeout

Each ONS 15310-CL and ONS 15310-MA CTC or TL1 user can be idle during his or her login session for a specified amount of time before the CTC window is locked. A lockout prevents unauthorized users from making changes. Higher-level users have shorter default idle periods and lower-level users have longer or unlimited default idle periods, as shown in Table 6-3. The user idle period can be modified by a Superuser; refer to the "Change Node Settings" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for instructions.

Table 6-3 Default User Idle Times

Security Level	Idle Time
Superuser	15 minutes
Provisioning	30 minutes
Maintenance	60 minutes
Retrieve	Unlimited

6.2.2.3 User Password, Login, and Access Policies

Superusers can view real-time lists of users who are logged in via CTC or TL1 for each node. Superusers can also provision the following password, login, and node access policies:

- Password length, expiration and reuse—Superusers can configure the password length using NE defaults. The password length, by default, is set to a minimum of six and a maximum of 20 characters. You can configure the default values in CTC node view using the Provisioning > NE Defaults > Node > security > password Complexity tabs. The minimum length can be set to eight, ten, or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are nonalphabetic and at least one character is a special character. Superusers can specify when users must change their passwords and how frequently passwords can be reused.
- Login attempts and locking out users—Superusers can specify the maximum number of times that a user can unsuccessfully attempt to log in before being locked out of CTC. Superusers can also provision the length of time before the lockout is removed.
- Disabling users—Superusers can provision the length of time before inactive user IDs are disabled.
- Node access and user sessions—Superusers can limit the number of CTC sessions one user can have, and they can prohibit access to the ONS 15310-CL and ONS 15310-MA using the LAN connection.

- Secure shell—Superusers can select secure shell (SSH) instead of Telnet at the CTC Provisioning > Security > Access tab. SSH is a terminal-remote host Internet protocol that uses encrypted links. It provides authentication and secure communication over channels that are not secure. Port 22 is the default port and cannot be changed.

6.3 Audit Trail

The ONS 15310-CL and ONS 15310-MA maintain a GR-839-CORE-compliant audit trail log that resides on the 15310-CL-CTX and CTX2500 cards respectively. Audit trails are useful for maintaining security, recovering lost transactions, and tracing user activities. The audit trail log shows who has accessed the node and what operations were performed during a given period of time. The log includes authorized Cisco support logins and logouts using the operating system command line interface (CLI), CTC, and TL1; the log also includes FTP actions, circuit creation/deletion, and user/system generated actions.

Event monitoring is also recorded in the audit log. An event is defined as a change in status of an element within the network. External events, internal events, attribute changes, and software upload/download activities are recorded in the audit trail.

To view the audit trail log, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*. Users can access the audit trail logs from any management interface (CTC, Cisco Transport Manager [CTM], or TL1).

The audit trail is stored in persistent memory and is not corrupted by processor switches or upgrades.

Note The ONS 15310-CL and ONS 15310-MA do not support a real-time clock with battery backup. Therefore, when you reset 15310-CL-CTX and CTX2500 cards, the audit log is reset to 1970 until you set the date and time again.

6.3.1 Audit Trail Log Entries

Audit trail records capture various types of activities. Individual audit entries contain some or all of the following information:

- User—Name of the user performing the action
- Host—Host from where the activity is logged
- Device ID—IP address of the device involved in the activity
- Application—Name of the application involved in the activity
- Task—Name of the task involved in the activity (view a dialog box, apply configuration, and so on)
- Connection Mode—The service used to connect to the node (for example, Telnet, console, or Simple Network Management Protocol [SNMP])
- Category—Type of change: Hardware, Software, or Configuration
- Status—Status of the user action: Read, Initial, Successful, Timeout, or Failed
- Time—Time of change
- Message Type—Denotes whether the event succeeded or failed
- Message Details—A description of the change

6.3.2 Audit Trail Capacities

The ONS 15310-CL and ONS 15310-MA is able to store 640 log entries.When this limit is reached, the oldest entries are overwritten with new events. When the log server is 80 percent full, an AUD-LOG-LOW condition is raised and logged.

When the log server reaches the maximum capacity of 640 entries and begins overwriting records that were not archived, an AUD-LOG-LOSS condition is raised and logged. This event indicates that audit trail records have been lost. Until you off-load the file, this event will not occur a second time regardless of the amount of entries that are overwritten by incoming data. To export the audit trail log, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

6.4 RADIUS Security

Users with Superuser security privileges can configure nodes to use Remote Authentication Dial In User Service (RADIUS) authentication. Cisco Systems uses a strategy known as authentication, authorization, and accounting (AAA) for enabling, verifying, and tracking the actions of remote users.

RADIUS server supports IPv6 addresses and can process authentication requests from a GNE or an ENE that uses IPv6 addresses.

6.4.1 RADIUS Authentication

RADIUS is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS contains three components:

- A protocol with a frame format that utilizes User Datagram Protocol (UDP)/IP
- A server
- A client

The server runs on a central computer, typically at a customer site, while the clients reside in the dial-up access servers and can be distributed throughout the network.

ONS 15310-CL and ONS 15310-MA nodes operate as clients of the RADIUS server. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and returning all configuration information necessary for the client to deliver service to the user. The RADIUS servers can act as proxy clients to other kinds of authentication servers. Transactions between the RADIUS client and server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server. This prevents someone monitoring an unsecured network from determine a user's password. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* to implement RADIUS authentication.

6.4.2 Shared Secrets

A shared secret is a text string that serves as a password between:

- A RADIUS client and a RADIUS server
- A RADIUS client and a RADIUS proxy

- A RADIUS proxy and a RADIUS server

For a configuration that uses a RADIUS client, a RADIUS proxy, and a RADIUS server, the shared secret that is used between the RADIUS client and the RADIUS proxy can be different from the shared secret used between the RADIUS proxy and the RADIUS server.

Shared secrets are used to:

- Verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared secret.
- Verify that the RADIUS message has not been modified in transit (message integrity).
- Encrypt some RADIUS attributes, such as User-Password and Tunnel-Password.

When creating and using a shared secret:

- Use the same case-sensitive shared secret on both RADIUS devices.
- Use a different shared secret for each RADIUS server-RADIUS client pair.
- Generate a random sequence at least 22 characters long to ensure a random shared secret.
- Use any standard alphanumeric and special characters.
- Use a shared secret of up to 128 characters in length. To protect your server and your RADIUS clients from brute force attacks, use long shared secrets (more than 22 characters).
- Make the shared secret a random sequence from each of the following three categories: letters (upper or lower case), numbers, and punctuation.
- Change the shared secret often to protect your server and your RADIUS clients from dictionary attacks. An example of a strong shared secret is 8d#>9fq4bV)H7%a3-zE13sW$hIa32M#m<PqAa72(.