CHAPTER 5

Security

This chapter provides information about Cisco ONS 15600 user security. To provision security, refer to the *Cisco ONS 15600 Procedure Guide*.

Chapter topics include:

5.1 Users IDs and Security Levels

When you log in to an ONS 15600 for the first time, you use the CISCO15 user ID, which is provided with every ONS 15600 system. You can use the CISCO15 ID, which has Superuser privileges, to create other ONS 15600 user IDs. For detailed instructions about creating users, refer to the *Cisco ONS 15600 Procedure Guide*.

Each ONS 15600 permits up to 500 Cisco Transport Controller (CTC) or TL1 user IDs. A user ID is assigned one of the following security levels:

- 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.
- Provisioning—Users can access provisioning and maintenance options.
- Maintenance—Users can access only the ONS 15600 maintenance options.
- Retrieve—Users can retrieve and view CTC information but cannot set or modify parameters.

See Table 5-3 on page 5-6 for idle user timeout information for each security level.

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 and prevent concurrent logins for all users.

5.2 User Privileges and Policies

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

5.2.1 User Privileges by Security Level

Table 5-1 shows the actions that each security level allows in node view. An "X" indicates that the action is supported on the associated security levels.

Table 5-1 ONS 15600 Security Levels—Node View

CTC Tab	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 alarms and events	X	X	X	X
Circuits	Circuits	Create/Delete	—	—	X	X
		Edit/Filter/Search	X	X	X	X
	Rolls	Complete/ Force Valid Signal/ Finish	—	—	X	X
Provisioning	General	General: Edit	—	—	Partial[1]	X
	Network	General: Edit	—	—	—	X
		Static Routing: Create/Edit/Delete	—	—	X	X
		OSPF: Create/Edit/Delete	—	—	X	X
		Internal Subnet: Edit/Reset	—	—	X	X
		Proxy: Create/Edit/Delete	—	—	—	X
		Firewall: Create/Edit/Delete	—	—	—	X
	OSI	Main Setup: Edit	—	—	—	X
		TARP: Config: Edit	—	—	—	X
		TARP: Static TDC: Add/Edit/Delete	—	—	X	X
		TARP: MAT: Add/Edit/Remove	—	—	X	X
		Routers: Setup: Edit	—	—	—	X
		Routers: Subnets: Edit/Enable/Disable	—	—	X	X
		Tunnels: Create/Edit/Delete	—	—	X	X
	BLSR	Create/Edit/Delete/Upgrade	—	—	X	X
		Ring Map/Squelch Table/RIP Table	X	X	X	X
	Protection	Create/Delete/Edit	—	—	X	X

Table 5-1 ONS 15600 Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
	Security	Users: Create/Delete/Clear Security Intrusion	—	—	—	X
		Users: Edit	Same user	Same user	Same user	All users
		Active Logins: View/Logout/ Retrieve Last Activity Time	—	—	—	X
		Policy: Edit/View	—	—	—	X
		Access: Edit/View	—	—	—	X
		RADIUS Server: Create/Edit/Delete/Move Up/Move D own/View	—	—	—	X
		Legal Disclaimer: Edit	—	—	—	X
	SNMP	Create/Edit/Delete	—	—	X	X
		Browse trap destinations	X	X	X	X
	Comm Channels	SDCC: Create/Edit/Delete	—	—	X	X
		LDCC: Create/Edit/Delete	—	—	X	X
	Timing	General: Edit	—	—	X	X
		BITS Facilities: Edit	—	—	X	X
	Alarm Profiles	Alarm Behaviour: Edit	—	—	X	X
		Alarm Profile Editor: Store/Delete[2]	—	—	X	X
		Alarm Profile Editor: New/Load/Compare/Available/Usage	X	X	X	X
	Alarm Extenders	External Alarms: Edit	—	—	X	X
		External Controls: Edit	—	—	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
	Routing Table	Retrieve			X	X
	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
	BLSR	Edit/Reset	—	X	X	X

Table 5-1 ONS 15600 Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
	Protection	Switch/Lock out/Lockon/Clear/ Unlock	—	X	X	X
	Software	Download	—	X	X	X
		Activate/Revert/Accept	—	—	—	X
	Diagnostic	Retrieve Diagnostic File	—	—	X	X
		Run Diagnostic Test/Soft-reset	—	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
	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
	Preferred Copy	Edit/Reset	—	—	—	X

1. Provisioner user cannot change node name, contact, location, or alarm indication signal–VT (AIS-V) insertion on STS-1 signal degrade (SD) parameters.
2. 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.

Table 5-2 shows the actions that each user privilege level can perform in network view.

Table 5-2 ONS 15600 Security Levels Network View

CTC Tab	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
Circuits	Circuits	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
	Rolls	Complete, Force Valid Signal, Finish	—	—	X	X

Table 5-2 ONS 15600 Security Levels Network View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning	Security	Users: Create/Delete	—	—	—	X
		Users: Change	Same User	Same User	Same User	All Users
		Active logins: Logout/Retrieve Last Activity Time/View	—	—	—	X
		Policy: Edit/View	—	—	—	X
	Alarm Profiles	Store/Delete[1]	—	—	X	X
		New/Load/Compare/Available/ Usage	X	X	X	X
	BLSR	Create/Edit/Delete/Upgrade	—	—	X	X
	Overhead Circuits	Create/Delete/Edit/Merge	—	—	X	X
		Search	X	X	X	X
	Provisionable Patchcords (PPC)	Create/Delete (not supported for ONS 15600 nodes)	—	—	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
	Diagnostics	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.

5.2.2 Security Policies

Users with Superuser security privileges can provision security policies on the ONS 15600. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters.

5.2.2.1 Superuser Privileges for Provisioning Users

Superusers can grant permission to Provisioning users to perform a set of tasks, including retrieving the audit log, restoring a database, clearing performance monitoring (PM) parameters, activating a software load, and reverting a software load. These privileges can only be set using CTC network element (NE) defaults, except the PM clearing privilege, which can be granted using the CTC Provisioning > Security > Access tabs. For more information about setting up Superuser privileges, refer to the *Cisco ONS 15600 Procedure Guide*.

5.2.2.2 Idle User Timeout

Each ONS 15600 CTC or TL1 user has a specified amount of time to leave the system idle before the CTC window locks. CTC lockouts prevent unauthorized users from making changes. Higher-level users have shorter idle times and lower-level users have longer or unlimited default idle periods, as shown in Table 5-3. Superusers can change user idle times on the Provisioning > Security > Policy tabs.

Table 5-3 ONS 15600 User Idle Times

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

5.2.2.3 Superuser Password and Login Privileges

A Superuser can perform ONS 15600 user creation and management tasks from the network or node (default login) view. In network view, a Superuser can add, edit, or delete users from multiple nodes at one time. In node view, a Superuser can only add, edit, or delete users from that node.

Superuser password and login privilege criteria include:

- Privilege level—A Superuser can change the privilege level (such as Maintenance or Provisioning) of a user ID while the user is logged in. The change will become effective the next time the user logs in and will apply to all nodes within the network.
- Login visibility—Superusers can view real-time lists of users who are logged into a node (both CTC and TL1 logins) by retrieving a list of logins by node. A Superuser can also log out an active user.
- Password length, expiration and reuse—Using NE defaults, Superusers can configure the password length. 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 node view with 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 can be set 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 provision password reuse periods (the number of days before a user can reuse a password) and reuse intervals (the number of passwords a user must generate before reusing a password).
- User lockout settings—A Superuser can manually lock out or unlock a user ID.
- Invalid login attempts—A Superuser sets the number of invalid login attempts a user can make before the user ID is locked out. Additionally, the Superuser sets the time interval the user ID is locked out after the user reaches the login attempt limit.
- Single Session Per User—If the Superuser provisions a user ID to be active for a single occurrence only, concurrent logins with that user ID are not allowed.

5.3 Audit Trail

The ONS 15600 maintains a GR-839-compliant audit trail log that resides on the TSC card. This record shows who has accessed the system and what operations were performed during a given period of time. The log includes authorized Cisco 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 the 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.

Audit trails are useful for maintaining security, recovering lost transactions and enforcing accountability. Accountability is the ability to trace user activities and is done by associating a process or action with a specific user. To view the audit trail log, refer to the "Manage Alarms" chapter in the *Cisco ONS 15600 Procedure Guide*. Users can access the audit trail logs from any management interface (CTC, CTM, TL1).

The audit trail is stored in persistent memory and is not corrupted by processor switches, resets or upgrades. However, if a user pulls both TSC cards, the audit trail log is lost.

5.3.1 Audit Trail Log Entries

Audit trail records capture the following activities:

- 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, apply configuration and so on)
- Connection Mode—Telnet, Console, SNMP
- Category—Type of change; Hardware, Software, Configuration
- Status—Status of the user action (Read, Initial, Successful, Timeout, Failed)
- Time—Time of change
- Message Type—Denotes if the event is Success/Failure type
- Message Details—A description of the change

5.3.2 Audit Trail Capacities

The system 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 (by way of CORBA/CTC).

When the log server reaches a 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 the user off-loads the file, this event occurs once regardless of the amount of entries that are overwritten by the system. To export the audit trail log, refer to the *Cisco ONS 15600 Procedure Guide*.

5.4 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 verifying the identity of, granting access to, 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.

5.4.1 RADIUS Authentication

RADIUS is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises 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 the customer's site, while the clients reside in the dial-up access servers and can be distributed throughout the network.

An ONS 15600 node operates as a client of RADIUS. 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 client and RADIUS 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 eliminates the possibility that someone snooping on an unsecured network could determine a user's password. Refer to the *Cisco ONS 15600 Procedure Guide* for detailed instructions for implementing RADIUS authentication.

5.4.2 Shared Secrets

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

- A RADIUS client and 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 than 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. Shared secrets also verify that the RADIUS message has not been modified in transit (message integrity). The shared secret is also used to 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.
- To ensure a random shared secret, generate a random sequence at least 22 characters long.
- You can use any standard alphanumeric and special characters.
- You can 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 of letters, numbers, and punctuation and change it often to protect your server and your RADIUS clients from dictionary attacks. Shared secrets should contain characters from each of the three groups listed in Table 5-4.

Table 5-4 Shared Secret Character Groups

Group	Examples
Letters (uppercase and lowercase)	A, B, C, D and a, b, c, d
Numerals	0, 1, 2, 3
Symbols (all characters not defined as letters or numerals)	Exclamation point (!), asterisk (*), colon (:)

The stronger your shared secret, the more secure are the attributes (for example, those used for passwords and encryption keys) that are encrypted with it. An example of a strong shared secret is 8d#>9fq4bV)H7%a3-zE13sW$hIa32M#m<PqAa72(.