This chapter provides information about Cisco ONS 15454 SDH user security. To provision security, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

Chapter topics include:

- User IDs and Security Levels
- User Privileges and Policies
- Audit Trail
- RADIUS Security

Contents

- 1 User IDs and Security Levels
- 2 User Privileges and Policies
  - 2.1 User Privileges by CTC Task
    - 2.1.1 Table 9-1: ONS 15454 SDH Security Levels-Node View
    - 2.1.2 Table 9-2: ONS 15454 SDH Security Levels-Network View
  - 2.2 Security Policies
    - 2.2.1 Superuser Privileges for Provisioning Users
    - 2.2.2 Idle User Timeout
      - 2.2.2.1 Table 9-3: ONS 15454 SDH Default User Idle Times
    - 2.2.3 User Password, Login, and Access Policies
    - 2.2.4 Secure Access
- 3 Audit Trail
  - 3.1 Audit Trail Log Entries
    - 3.1.1 Table 9-4: Audit Trail Window Columns
  - 3.2 Audit Trail Capacities
- 4 RADIUS Security
  - 4.1 RADIUS Authentication
  - 4.2 Shared Secrets
    - 4.2.1 Table 9-5: Shared Secret Character Groups

User IDs and Security Levels

The CISCO15 user ID is provided with the ONS 15454 SDH system, but this user ID is not prompted when you sign into Cisco Transport Controller (CTC). This ID can be used to set up other ONS 15454 SDH users.

You can have up to 500 user IDs on one ONS 15454 SDH. Each CTC or Transaction Language One (TL1) user 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 15454 SDH 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.

See Table 9-3 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.

User Privileges and Policies

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

User Privileges by CTC Task

Table 9-1 shows the actions that each user privilege level can perform in node view.

Table 9-1: ONS 15454 SDH 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/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
		Multishelf Config: Edit	-	-	-	-
		Power Monitor: Edit	-	-	X	X
	Ether Bridge	Spanning trees: Edit	-	-	X	X
	Network	General: Edit	-	-	-	X
		General: View	X	X	X	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
		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
	MS-SPRing	Create/Edit/Delete/Upgrade	-	-	X	X
		Ring Map/Squelch Table/RIP Table	X	X	X	X

	Protection	Create/Edit/Delete	-	-	X	X
	Security	Users: Create/Delete/Clear Security Intrusion Alarm	-	-	-	X
		Users: Edit	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
		Access: Edit/View	-	-	-	X
		RADIUS Server: Create/Edit/Delete/Move Up/Move Down/View	-	-	-	X
		Legal Disclaimer: Edit	-	-	-	X
	SNMP	Create/Delete/Edit	-	-	X	X
		Browse trap destinations	X	X	X	X
	Comm Channels	RS-DCC: Create/Edit/Delete	-	-	X	X
		MS-DCC: Create/Edit/Delete	-	-	X	X
		GCC: Create/Edit/Delete	-	-	X	X
		OSC: OSC Terminations: Create/Edit/Delete	-	-	X	X
		OSC: DWDM Ring ID: Create/Edit/Delete	-	-	-	X
		PPC: Create/Edit/Delete	-	-	X	X
		LMP: General/TE Links/Data Links	X	X	X	X
		LMP: Control Channels	-	-	-	X
	Timing	General: Edit	-	-	X	X
		BITS Facilities: Edit	-	-	X	X
	Alarm Profiles	Alarm Behavior: Edit	-	-	X	X
		Alarm Profiles Editor: Store/Delete[2]	-	-	X	X
		Alarm Profile Editor: New/Load/Compare/Available/Usage	X	X	X	X
	Cross-Connect	Edit	-	-	X	X
	Defaults	Edit/Import	-	-	-	X
		Reset/Export	X	X	X	X
	WDM-ANS	Provisioning: Edit	-	-	-	X
		Provisioning: Reset	X	X	X	X
		Internal Patchcords: Create/Edit/Delete/Commit/ Default Patchcords	-	-	X	X
		Port Status: Launch ANS	-	-	-	X
		Node Setup	X	X	X	X
		Optical Side: Create/Edit/Delete	X	X	X	X
Inventory	-	Delete	-	-	X	X
		Reset	-	X	X	X

Table 9-1: ONS 15454 SDH Security Levels-Node View

Maintenance	Database	Backup	-	X	X	X
		Restore	-	-	-	X
	EtherBridge	Spanning Trees:View	X	X	X	X
		MAC Table: Retrieve	X	X	X	X
		MAC Table: Clear/Clear All	-	X	X	X
		Trunk Utilization: Refresh	X	X	X	X
		Circuits: Refresh	X	X	X	X
	Network	Routing Table: Retrieve	X	X	X	X
		RIP Routing Table: Retrieve	X	X	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
	MS-SPRing	Edit/Reset	-	X	X	X
	Protection	Switch/Lock out/Lockon/Clear/ Unlock	-	X	X	X
	Software	Download/Cancel	-	X	X	X
		Activate/Revert	-	-	-	X
	Cross-Connect	Cards: Switch/Lock/Unlock	-	X	X	X
		Resource Usage: Delete	-	-	X	X
	Overhead XConnect	View	X	X	X	X
	Diagnostic	Retrieve Tech Support Log	-	-	X	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
	DWDM	APC: Run/Disable/Refresh	-	X	X	X
		WDM Span Check: Edit/Retrieve Span Loss values/Reset	X	X	X	X
		ROADM Power Monitoring: Refresh	X	X	X	X
		PP-MESH Internal Patchcord: Refresh	X	X	X	X
		Install Without Metro Planner: Retrieve Installation values	X	X	X	X
		All Facilities: Mark/Refresh	X	X	X	X

1. Provisioner user cannot change node name, contact, and location 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 9-2 shows the actions that each user privilege level can perform in network view.

Table 9-1: ONS 15454 SDH Security Levels-Node View

Table 9-2: ONS 15454 SDH 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
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	-	-	-	X
		Users: Edit	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
	MS-SPRing	Create/Delete/Edit/Upgrade	-	-	X	X
	Overhead Circuits	Create/Delete/Edit/Merge	-	-	X	X
		Search	X	X	X	X
	Provisionable Patchcords (PPC)	Create/ Delete	-	-	X	X
	Server Trails	Create/Edit/Delete	-	-	X	X
	VLAN DB Profile	Load/Store/Merge/Circuits	X	X	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.

Security Policies

Users with Superuser security privilege can provision security policies on the ONS 15454 SDH. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters. In addition, a Superuser can prevent users from accessing the ONS 15454 SDH through the TCC2/TCC2P RJ-45 port, the MIC-C/T/P LAN connection, or both. If enabled in the NE defaults, superusers can be configured to override the inactive user timeout interval.

Superuser Privileges for Provisioning Users

Superusers can grant permission to Provisioning users to retrieve audit logs, restore databases, clear performance monitoring (PM) parameters, activate software loads, and revert software loads. 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 on setting up

Superuser privileges, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

Idle User Timeout

Each ONS 15454 SDH 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. The lockouts prevent 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 9-3. The user idle period can be modified by a Superuser; refer to the *Cisco ONS 15454 SDH Procedure Guide* for instructions.

Table 9-3: ONS 15454 SDH Default User Idle Times

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

User Password, Login, and Access Policies

Superusers can view real-time lists of users who are logged into CTC or TL1 by node. Superusers can also provision the following password, login, and node access policies.

- Password length, expiration and reuse-Superusers can configure the password length by 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 and when they can reuse their passwords.
- Locking out and disabling users-Superusers can provision the number of invalid logins that are allowed before locking out users and the length of time before inactive users 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 15454 SDH using the LAN or MIC-C/T/P connections.

  In addition, a Superuser can select secure shell (SSH) instead of Telnet at the CTC Provisioning > Security > Access tabs. SSH is a terminal-remote host Internet protocol that uses encrypted links. It provides authentication and secure communication over unsecure channels. Port 22 is the default port and cannot be changed.

Note: The superuser cannot modify the privilege level of an active user. The CTC displays a warning message when the superuser attempts to modify the privilege level of an active user.

Secure Access

Secure access is based on SSH and SSL protocols. Secure access can be enabled for EMS (applicable to CTC). When access is set to secure, CTC provides enhanced SFTP and SSH security when communicating with the node.

For more information on how to enable EMS secure access, refer *Cisco ONS 15454 SDH Procedure Guide* for instructions.

Audit Trail

The ONS 15454 SDH maintains an audit trail log that resides on the TCC2/TCC2P. This record shows who has accessed the system and what operations were performed during a given time period. The log includes authorized Cisco logins and logouts using the operating system command line interface, Cisco Transport Controller (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 by associating a process or action with a specific user. To view the audit trail log, refer to the *Cisco ONS 15454 SDH Procedure Guide*. to view the audit trail record. Any management interface (CTC, CTM, TL1) can access the audit trail logs.

The audit trail is stored in persistent memory and is not corrupted by processor switches, resets or upgrades. However, if the TCC2/TCC2Ps are removed, the audit trail log is lost.

Audit Trail Log Entries

Table 9-4 contains the columns listed in Audit Trail window.

Table 9-4: Audit Trail Window Columns

Heading	Explanation
Date	Date when the action occurred
Num	Incrementing count of actions
User	User ID that initiated the action
P/F	Pass/Fail (whether or not the action was executed)
Operation	Action that was taken

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

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 15454 SDH Procedure Guide*.

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 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 15454 SDH 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 15454 SDH Procedure Guide* for detailed instructions for implementing RADIUS authentication.

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 9-5.

Table 9-5: 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#mPqAa72(.