



Security

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

Chapter topics include:

- [9.1 User IDs and Security Levels, page 9-1](#)
- [9.2 User Privileges and Policies, page 9-1](#)
- [9.3 Audit Trail, page 9-7](#)
- [9.4 RADIUS Security, page 9-9](#)

9.1 User IDs and Security Levels

The CISCO15 user ID is provided with the ONS 15454 for initial login to the node, but this user ID is not supplied in the prompt when you sign into Cisco Transport Controller (CTC). This ID can be used to set up other ONS 15454 user IDs. (Refer to the *Cisco ONS 15454 Procedure Guide* for instructions.)

You can have up to 500 user IDs on one ONS 15454. 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 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 on page 9-7](#) 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 ID and prevent concurrent logins for all users.

9.2 User Privileges and Policies

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

9.2.1 User Privileges by CTC Action

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

Table 9-1 ONS 15454 Security Levels—Node View

CTC Tab	Subtab	[Subtab]:Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/Filter/Delete Cleared Alarms	X ¹	X	X	X
Conditions	—	Retrieve/Filter	X	X	X	X
History	Session	Filter	X	X	X	X
	Node	Retrieve/Filter	X	X	X	X
Circuits	Circuits	Create/Edit/Delete	— ²	—	X	X
		Filter/Search	X	X	X	X
	Rolls	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X

Table 9-1 ONS 15454 Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]:Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning	General	General: Edit	—	—	Partial ³	X
		Power Monitor: Edit	—	—	X	X
	EtherBridge	Spanning trees: Edit	—	—	X	X
	Network	General: All	—	—	—	X
		Static Routing: Create/Edit/Delete	—	—	X	X
		OSPF: Create/Edit/Delete	—	—	X	X
		RIP: Create/Edit/Delete	—	—	X	X
		Proxy: Create/Delete	—	—	—	X
		Firewall: Create/Delete	—	—	—	X
	OSI	Main Setup	—	—	—	X
		TARP	—	—	—	X
		Routers	—	—	—	X
		GRE Tunnel Routes	—	—	—	X
	BLSR	Create/Edit/Delete	—	—	X	X
		Ring Map/Squelch Table/RIP Table	X	X	X	X
	Protection	Create/Delete/Edit	—	—	X	X
		View	X	X	X	X
	Security	Users: Create/Delete/Clear Security Intrusion	—	—	—	X
		Users: Change password	Same user	Same user	Same user	All users
		Active Logins: View/Logout	—	—	—	X
		Policy: Edit	—	—	—	X
		Access: Edit	—	—	—	X
		RADIUS Server	—	—	—	X
		Legal Disclaimer: Edit	—	—	—	X
	SNMP	Create/Delete/Edit	—	—	X	X
		Browse trap destinations	X	X	X	X
	Comm Channels	SDCC: Create/Edit/Delete	—	—	X	X
		LDCC: 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	X	X
		PPC: Create/Delete	—	—	X	X

Table 9-1 ONS 15454 Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]:Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning	Timing	General: Edit	—	—	X	X
		BITS Facilities: Edit	—	—	X	X
	Alarm Profiles	Alarm Profiles: Edit	—	—	X	X
		Alarm Profiles Editor: Store/Delete ⁴	—	—	X	X
		Alarm Profile Editor: New/Load/Compare/Available/ Usage	X	X	X	X
	Cross-Connect	View	X	X	X	X
	Defaults	Edit/Import	—	—	—	X
		Reset/Export	X	X	X	X
	WDM-ANS	Provisioning: Edit/Import	—	—	—	X
		Provisioning: Reset/Export	X	X	X	X
		Connections: Create/Edit/Delete/Commit/ Calculate	—	—	X	X
		Port Status: Launch	—	—	X	X
	Inventory	—	Delete	—	—	X
Reset			—	X	X	X

Table 9-1 ONS 15454 Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]:Actions	Retrieve	Maintenance	Provisioning	Superuser
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
	OSI	IS-IS RIB	—	—	—	X
		ES-IS RIB	—	—	—	X
		TDC	—	—	—	X
	BLSR	Create/Edit/Delete	—	X	X	X
		Ring Map/Squelch Table/ Rip Table	X	X	X	X
	Software	Download	—	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
	Protection	View	X	X	X	X
	Diagnostic	Retrieve/Lamp Test	—	X	X	X
	Timing	Source: Edit	—	X	X	X
		Report: View/Refresh	X	X	X	X
	Audit	Retrieve	—	—	—	X
		Archive	—	—	X	X
	RIP Routing Table	Retrieve	X	X	X	X
	Routing Table	Retrieve	X	X	X	X
	Test Access	View	X	X	X	X
	DWDM	APC: Run/Disable/Refresh	—	X	X	X
WDM Span Check: Retrieve Span Loss values, Reset		X	X	X	X	
ROADM Power Monitoring: Refresh		X	X	X	X	

1. The “X” indicates that the user can perform the actions.
2. The “—” indicates that the privilege to perform an action is not available to the user.
3. Provisioner user cannot change node name, contact, or AIS-V insertion on STS-1 signal degrade (SD) parameters.
4. 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 9-2 shows the actions that each user privilege level can perform in network view.

Table 9-2 ONS 15454 Security Levels—Network View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/Filter/Delete cleared alarms	X ¹	X	X	X
Conditions	—	Retrieve/Filter	X	X	X	X
History	—	Filter	X	X	X	X
Circuits	Circuits	Create/Edit/Delete	— ²	—	X	X
	Rolls	Filter/Search	X	X	X	X
Provisioning	Security	Users: Create/Delete	—	—	—	X
		Users: Change	Same user	Same user	Same user	All users
		Active logins: Logout	—	—	—	X
		Policy: Change	—	—	—	X
	Alarm Profiles	Store/Delete ³	—	—	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/ Delete	—	—	X	X	
Maintenance	Software	Download/Cancel	—	X	—	X

1. The “X” indicates that the user can perform the actions.
2. The “—” indicates that the privilege to perform an action is not available to the user.
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.

9.2.2 Security Policies

Users with Superuser security privileges can provision security policies on the ONS 15454. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters. In addition, a Superuser can access the ONS 15454 through the TCC2/TCC2P RJ-45 port, the backplane LAN connection, or both.

9.2.2.1 Idle User Timeout

Each ONS 15454 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 Procedure Guide* for instructions.

Table 9-3 **ONS 15454 Default User Idle Times**

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

9.2.2.2 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 expirations and reuse—Superusers can specify when users must change and when they can reuse their passwords.
- Login attempts—Superusers can specify the maximum number of times a user is allowed to attempt to log into CTC.
- 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 using the LAN or TCC2/TCC2P RJ-45 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.

9.2.2.3 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 Procedure Guide* for instructions.

9.3 Audit Trail

The Cisco ONS 15454 maintains a Telcordia GR-839-CORE-compliant audit trail log that resides on the TCC2/TCC2P card. Audit trails are useful for maintaining security, recovering lost transactions, and enforcing accountability. Accountability refers to tracing user activities; that is, associating a process or action with a specific user. The audit trail log shows who has accessed the system 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 the change in status of a network element. 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 15454 Procedure Guide*. You 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 you remove both TCC2/TCC2P cards, the audit trail log is lost.

9.3.1 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 box, apply configuration, etc.)
- 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—Whether the event is Success/Failure type
- Message Details—Description of the change

9.3.2 Audit Trail Capacities

The ONS 15454 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 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 15454 Procedure Guide*.

9.4 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.

9.4.1 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 a customer site, while the clients reside in the dial-up access servers and can be distributed throughout the network.

An ONS 15454 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 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 eliminates the possibility that someone monitoring an unsecured network could determine a user's password. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed instructions for implementing RADIUS authentication.

9.4.2 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 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. 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 16 characters long.
- You can use any standard alphanumeric and special characters.
- You can use a shared secret of up to 16 characters in length. To protect your server and your RADIUS clients from brute force attacks, use long shared secrets.
- 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.