



Security Reference

this chapter contains information related to user IDs and security levels, user privileges and policies, audit trail, and RADIUS security.

- [User IDs and Security Levels, page 1](#)
- [User Privileges and Policies, page 2](#)
- [User Accounts for Encryption and Authentication, page 9](#)
- [Audit Trail, page 10](#)
- [RADIUS Security, page 12](#)
- [Procedure for Users and Security, page 14](#)

User IDs and Security Levels

The Cisco Transport Controller (CTC) ID is provided with the system, but the system does not display the user ID when you sign into CTC. This ID can be used to set up other users.

You can have up to 500 user IDs on one . Each CTC or 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 maintenance options.
- Provisioning-Users can access provisioning and maintenance options.
- Superusers-Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.
- Security Super User-Users can set encryption and card authentication parameters. The security super user creates security users and associates each user with a WSE card. By default, at least one security super user must exist.
- Security User-Users can enable or disable card authentication and payload encryption.
- Root User-Cisco Prime user with all the security and transport privileges. The root user is not supported in CTC or TL1. The security super user can enable the root user through CTC.

See [Idle User Timeout](#), on page 8 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.



Note You must add the same user name and password to each node the user accesses.



Note Maintenance, Provisioning, and Superusers must be properly trained on the hazards of laser safety and be aware of safety-related instructions, labels, and warnings. Refer to the [Cisco Optical Products Safety and Compliance Information](#) document for a current list of safety labels and warnings, including laser warnings. Refer to IEC 60825-2 for international laser safety standards, or to ANSI Z136.1 for U.S. laser safety standards. The explains how users can disable laser safety during maintenance or installation; when following these procedures, adhere to all posted warnings and cautions to avoid unsafe conditions or abnormal exposure to optical radiation.

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

Below table shows the actions that each user privilege level can perform in node view. An X indicates the user is allowed to perform the action. A dash indicates that the user is not allowed to perform the action.

Table 1: Security Levels - Node View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve Security Super User/Security User	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
	Node	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	General: Edit	-	-	PartialA Provisioning user cannot change node name, contact, location and AIS-V insertion on STS-1 signal degrade (SD) parameters.	X
		Multishelf Config: Edit	-	-	X	-
	Network	General: Edit	-	-	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	X
		Firewall: Create/Edit/Delete	-	-	X	X
	OSI	Main Setup: Edit	-	-	X	X
		TARP: Config: Edit	-	-	X	X
		TARP: Static TDC: Add/Edit/Delete	-	-	X	X
		TARP: MAT: Add/Edit/Remove	-	-	X	X
		Routers: Setup: Edit	-	-	X	X
		Routers: Subnets: Edit/Enable/Disable	-	-	X	X
		Tunnels: Create/Edit/Delete	-	-	X	X

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	-	-	-	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	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: Create/Edit/Delete	-	-	X	X
	PPC: Create/Edit/Delete	-	-	X	X
	LMP: General: Edit	X	X	X	X
	LMP: Control Channels: Create/Edit/Delete	-	-	X	X
	LMP: TE Links: Create/Edit/Delete	-	-	X	X
	LMP: Data Links: Create/Edit/Delete	-	-	X	X
Alarm Profiles	Load/Store/Delete 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.	-	-	X	X
	New/Compare/Available/Usage	X	X	X	X
Defaults	Edit/Import	-	-	X	X
	Reset/Export	X	X	X	X
WDMAS	Provisioning: Edit	-	-	X	X

		Provisioning: Reset	X	X	X	X
		Internal Patchcords: Create/Edit/Delete/Commit/ Default Patchcords	-	-	X	X
		Port Status: Launch ANS	-	-	X	X
		Node Setup: Setup/Edit	X	X	X	X
		Optical Side: Create/Edit/Delete	X	X	X	X
Inventory	-	Delete	-	-	X	X
		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
	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
	Software	Download/Cancel	-	X	X	X
		Activate/Revert	-	-	-	X
	Diagnostic	Node Diagnostic Logs	-	-	X	X
	Audit	Retrieve	-	-	-	X
		Archive	-	-	X	X
	DWDWM	APC: Run/Disable/Refresh	-	X	X	X
		WDM Span Check: Retrieve Span Loss values/Edit/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	X	X	X	X
		All Facilities: Mark/Refresh	X	X	X	X

Table 2: Security Levels - Network View, on page 6 shows the actions that each user privilege level can perform in network view. An X indicates the user is allowed to perform the action. A dash indicates that the user is not allowed to perform the action.

Table 2: Security Levels - Network View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve Security Super User/Security User	Maintenance	Provisioning	Superuser

Alarms	-	Synchronize/Filter/Delete	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/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	New/Load/Store/DeleteThe 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	-	-	X	X
		Compare/Available/Usage	X	X	X	X
	BLSR (ANSI) MS-SPRing (ETSI)	Create/Edit/Delete/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	X
		Refresh	X	X	X	X

Security Policies

Superusers can provision security policies on the . These security policies include idle user timeouts, password changes, password aging, and user lockout parameters.

Superuser Privileges for Provisioning Users

Superusers can grant permission to Provisioning users to perform a set of tasks. The tasks include retrieving audit logs, restoring databases, clearing PMs, and activating and reverting software loads. These privileges can be set only through CTC network element (NE) defaults, except the PM clearing privilege, which can be granted to Provisioning users using CTC Provisioning > Security > Access tabs. For more information on setting up Superuser privileges, refer to the .

Idle User Timeout

Each 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 3: Default User Idle Times](#), on page 8.

Table 3: 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 user logins 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 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 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 non alphabetic and at least one character is a special character. Superusers can specify when users must change their passwords and when they can reuse them.

- 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. The number of allowed lockout attempts is set to the number of allowed login attempts.

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.

User Accounts for Encryption and Authentication

Users' privileges are determined by these user account types:

- Security Super User- A security super user has privileges to set encryption and card authentication parameters. The security super user creates security users and associates each user with a WSE card. By default, at least one security super user must exist. Therefore, last security super user cannot be deleted and the last user's security level cannot be changed. However, the password can be reset.

The security super user can provision the encryption security feature on a pre-provisioned card. The security super user has these privileges:

- Create, delete, or edit the 'Security User' account
- Enable or disable card authentication
- Enable or disable payload encryption
- Reset the master key on each encrypted stream
- Provision AES secure packet

The security super user needs to authorize the security user after performing each of the following operations:

- Side switch of the controller card (resetting the active card to make the standby card as active)
- NE power cycle (power failure and recovery)
- Software upgrade
- Database restore
- Security Users—Security users are created by a security super user. The security users are associated to a WSE card through its serial number, and have these privileges:
 - Enable or disable card authentication
 - Enable or disable payload encryption
 - Reset the master key on each encrypted stream

- Provision AES secure packet

**Note**

The security user cannot configure encryption on a pre-provisioned card.

- Root User—The root user is Cisco Prime user with all the security and transport privileges mentioned in [Table 1: Security Levels - Node View, on page 2](#) [Table 2: Security Levels - Network View, on page 6](#). The root user is not supported in CTC or TL1. The security super user can enable the root user through CTC.

The following shows the actions that each user privilege level can perform. An X indicates the user is allowed to perform the action. A dash indicates that the user is not allowed to perform the action.

Table 4: Security Super User and Security User Privileges

Actions	Security Super User	Security User
Create Security Users	X	--
Assign security users to individual cards	X	--
Authenticate and authorize cards	X	X
Enable payload encryption and payload authentication	X	X
Configure Encryption on a pre-provisioned card	X	--
Reset session key and change the session key interval	X	X
Filter circuits	X	X
OTN overhead byte selection	X	--
Provision ICV mismatch threshold	X	--
Provision AES secure packet	X	X

Audit Trail

The Cisco maintains a Telcordia GR-839-CORE-compliant audit trail log that resides on the control cards. 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. 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, 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.

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

Audit Trail Log Entries

Table 5: Audit Trail Window Columns, on page 11 contains the columns listed in Audit Trail window.

Table 5: 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, and so on)
- Connection Mode-Telnet, Console, Simple Network Management Protocol (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 whether the event is Success/Failure type
- Message Details-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 Common Object Request Broker Architecture [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 only once regardless of the amount of entries that are overwritten by the system.

RADIUS Security

Superusers can configure nodes to use Remote Authentication Dial In User Service (RADIUS) authentication. RADIUS 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. To configure RADIUS authentication, refer to the .

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

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 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.



Note

In RADIUS authentication, the user can enter up to 39 characters for user name in CTC from R10.5. It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot).

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 6: Shared Secret Character Groups](#), on page 13.

Table 6: 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 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(.

Procedure for Users and Security

This section lists the procedure related to users and security.

- [NTP-G23 Create Users and Assign Security](#). Refer to the chapter "Turn Up a Node" in the .
- [NTP-G88 Modify Users and Change Security](#)