Configure Authentication

This chapter describes the procedures to create users and configure authentication.

Understand Authentication

Authentication is a way of identifying a user before permitting access to the network and network services. When Authentication is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it. Cisco NCS 4000 series uses the RADIUS/TACACS+ server for authenticating remote users.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS is a client/server protocol that runs in the application layer that uses User Datagram Protocol (UDP) for transport.

The RADIUS server process runs in background on a UNIX or Microsoft Windows server and client would be the Cisco network element (NE). RADIUS clients run on Cisco routers and sends the authentication requests to a central RADIUS server that contains all the user authentication and network service access information.

TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is a new protocol developed by Cisco and released as an open standard. TACACS+ uses TCP for transport. TACACS+ protocol is a security application that provides centralized validation of users attempting to gain access to a network element. Since, TCP is connection oriented protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout and others, as it rides on UDP that is connectionless. RADIUS encrypts only the user password as it travels from the RADIUS client to RADIUS server. All other information, for example, username, authorization, and accounting are transmitted in clear text. Therefore, it is vulnerable to various types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.

Create a Local User on a Single Node Using CTC

Purpose	This procedure enables you to create a local user on a single or multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view or network view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 In the Users window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name - Type the user name. The user name must be a maximum of 40 characters (only up to 39 characters for the TACACS and RADIUS authentication). It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot). For TL1 compatibility, the user name must be of 6 to 10 characters.
- Password—Type the user password.

  Note The password change of root user is not supported from CTC.

  The minimum password length for CTC is six and maximum of 20 characters. . The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%,~,!,@,$,+,^,&,*,(),<>,{},[],-._,=) characters, where at least two characters are not alphabetic and at least one character is a special character; or the password can contain any character. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: **RETRIEVE**, **MAINTENANCE**, **PROVISIONING**, or **SUPERUSER**.

- 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 the 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.

Step 4 Click **OK**.

Stop. You have completed this procedure.

Viewing and Retrieving Active Logins

Purpose	This procedure enables you to view active CTC logins, retrieve the last activity time.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	All users

Procedure

Step 1 In node view or network view, click the **Provisioning** > **Security** > **Active Logins** tabs. The Active Logins tab displays the following information:

- Node
- User
- Source IP address
- Session Type (EMS, TL1, FTP, Telnet, or SSH)
- Login time
- Last activity time

Note Active Login tab always display the two telnet sessions for a single CTC session, open by a user using a single IP address.

Step 2 Click **Retrieve Last Activity Time** to display the most recent activity date and time for users in the Last Activity Time field.

Stop. You have completed this procedure.

Configure Authentication Server Order

Purpose	This procedure enables you to configure the order of the servers for DUO Two-Factor authentication.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Important Before you configure the server authentication order, log in to the node using the local username and password.

Procedure

Step 1 In node view or network view, click the **Provisioning** > **Security** > **Radius / Tacacs+** tabs.

The Radius / Tacacs+ tab displays the Authentication Mode and Server in Order of Authentication panes.

Step 2 In the Authentication Mode pane, choose: **Radius**, **Tacacs+**, or **Local**.

(Optional) Check the **Node As Final Authentication When No Server Is Found** check box.

Step 3 In the **Server in Order of Authentication** pane, click **Add** and enter the following.

- Server Type—Displays the selected server type.
- Node Address—IPv4 address of the current node
- Shared Secret—Secret key shared between the client node and the cloud server
- Encrypted—Encrypts and decrypts the authentication data.
- Authentication Port—Authentication port value of the selected server type
- Accounting Port—Accounting port value of the selected server type

Alternatively, you can add the server profile by executing the following CLI command:

```
radius-server host 10.xx.xx.xxx auth-port 1812 acct-port 1813 key ravk@1234
```

Note If more than one server profile is created, the profile at the top is used for authenticating first. Use the following buttons to change the order of the authentication servers:

- Delete—Deletes the created server type.
- Move Up—Moves the server profile up the order.
- Move Down—Moves the server profile down the order.

Step 4 Click **Apply**.

What to do next

Log in using the new username and password stored in the cloud server from the next session.