Configuring Local Authentication

This chapter describes local authentication. This chapter also describes procedures to configure local authentication and privilege levels.

This chapter includes the following topics:

Understanding Authentication

Access control enables you to restrict access to the network server and its services to a specific group of users. The authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you can set up access control on your router or access server.

Authentication is a way of identifying a user before permitting access to the network and network services. The Carrier Packet Transport (CPT) supports local authentication mechanism to administer its security functions.

NTP-J102 Configure Local Authentication Using Cisco IOS Commands

Purpose	This procedure configures local authentication using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The only supported login authentication method in CPT is local authentication.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** Router(config)# aaa new-model	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**aaa authentication login default** *methodname* **Example:** Router(config-if)# aaa authentication login default local	Creates the default local authentication list.
Step 5	**line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**] **Example:** Router(config)# line vty 0 4	Enters line configuration mode for the lines to which you want to apply the authentication list.
Step 6	**login authentication default** **Example:** Router(config-line)# login authentication default	Applies the authentication list to a line or set of lines.
Step 7	**end** **Example:** Router(config-line)# end	Returns to global configuration mode.

Example: Configure Local Authentication

The following example shows how to configure local authentication using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config-if)# aaa authentication login default local
Router(config)# line vty 0 4
Router(config-line)# login authentication default
Router(config-line)# end
```

NTP-J103 Protect Access to Privileged EXEC Commands Using Cisco IOS Commands

Purpose	This procedure provides a way to control access to the system configuration file and privileged EXEC (enable) commands, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the listed procedures as needed.

- DLP-J291 Set or Change a Static Enable Password Using Cisco IOS Commands, on page 3
- DLP-J292 Protect Passwords with Enable Password and Enable Secret Using Cisco IOS Commands, on page 4
- DLP-J293 Set or Change a Line Password Using Cisco IOS Commands, on page 6
- DLP-J294 Encrypt Passwords Using Cisco IOS Commands, on page 7

Stop. You have completed this procedure.

DLP-J291 Set or Change a Static Enable Password Using Cisco IOS Commands

Purpose	This procedure sets or changes a static password that controls access to privileged EXEC (enable) mode, using Cisco IOS commands.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**username** *user* **password** *password* **Example:** Router(config)# username user1 password pwd	Sets the user name and password.
Step 4	**enable password** *password* **Example:** Router(config)# enable password user1	Enables a new password or changes an existing password for the privileged command level.
Step 5	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J292 Protect Passwords with Enable Password and Enable Secret Using Cisco IOS Commands

Purpose	This procedure configures the router to require an enable password and an enable secret password using Cisco IOS commands.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, you can use either the **enable password** or **enable secret** commands. Both commands accomplish the same thing; that is, they allow you to establish an encrypted password that users must enter to access enable mode (the default), or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

Note If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password serves as the enable password for all VTY sessions.

Use the **enable password** or **enable secret** commands with the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** configuration command to specify the commands accessible at various levels.

You can enable or disable password encryption with the **service password-encryption** command. If you have the **service password-encryption** command enabled, the password you enter is encrypted. When you display it with the **more system:running-config** command, it is displayed in encrypted form.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**username** *user* **password** *password* **Example:** Router(config)# username user1 password pwd	Sets the user name and password.

	Command or Action	Purpose
Step 4	**enable password** [**level** *level-number*] {*password* | *encryption-type encrypted-password*} **Example:** Router(config)# enable password level 2 pswd2	Enables a password for a privilege command mode.
Step 5	**enable secret** [**level** *level-number*] {*password* | *encryption-type encrypted-password*} **Example:** Router(config)# enable secret greentree	Specifies a secret password, saved using a non-reversible encryption method. If both **enable password** and **enable secret** commands are set, the user must enter the **enable secret** password.
Step 6	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

DLP-J293 Set or Change a Line Password Using Cisco IOS Commands

Purpose	This procedure sets or changes a password on a line, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	**password** *password_new* **Example:** Router(config)# password user1	Enables a new password or changes an existing password for the privileged command level.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

DLP-J294 Encrypt Passwords Using Cisco IOS Commands

Purpose	This procedure encrypts passwords using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Encryption prevents the password from being readable in the configuration file.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**service password-encryption**	Encrypts a password.

	Command or Action	Purpose
	Example: Router(config)# service password-encryption	The actual encryption process occurs when the current configuration is written or when a password is configured. The password encryption is applied to all the passwords, including authentication key passwords, privileged command password, and console and virtual terminal line access passwords. The **service password-encryption** command is used to keep unauthorized individuals from viewing your password in your configuration file.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

Understanding Multiple Privilege Levels

CPT supports multiple privilege levels, which provide access to commands. By default, there two levels of access to commands:

- User EXEC mode (level 1)
- Privileged EXEC mode (level 15)

You can configure additional levels of access to commands, called privilege levels, to meet the needs of users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured from level 0, which is the most restricted level, to level 15, which is the least restricted level.

The access to each privilege level is enabled through separate passwords, which you can specify when configuring the privilege level.

For example, if you want a certain set of users to be able to configure only certain interfaces and configuration options, you could create a separate privilege level only for specific interface configuration commands and distribute the password for that level to those users.

NTP-J104 Configure Privilege Levels Using Cisco IOS Commands

Purpose	This procedure configures privilege levels using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the listed procedures as needed.

- DLP-J295 Set the Privilege Level for a Command Using Cisco IOS Commands, on page 9
- DLP-J296 Change the Default Privilege Level for Lines Using Cisco IOS Commands, on page 10
- DLP-J297 Display Current Privilege Levels Using Cisco IOS Commands, on page 11
- DLP-J298 Log In to a Privilege Level Using Cisco IOS Commands, on page 12

Stop. You have completed this procedure.

DLP-J295 Set the Privilege Level for a Command Using Cisco IOS Commands

Purpose	This procedure configures a new privilege level for users, and associate commands with that privilege level, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**privilege** *mode* **level** *level_number command-string* **Example:** Router(config)# privilege exec level 14 configure	Configures the specified privilege level to allow access to the specified command.
Step 4	**enable secret level** *level_number* {**0** | **5**} *password-string* **Example:** Router(config)# end	Sets the password for the specified privilege level. This is the password users will enter after entering the **enable** *level* command to access the specified level. **0** indicates that an unencrypted password string follows; **5** indicates that an encrypted password string follows.
Step 5	**exit** **Example:** Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J296 Change the Default Privilege Level for Lines Using Cisco IOS Commands

Purpose	This procedure changes the default privilege level for a given line or a group of lines, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**] **Example:** Router(config)# line vty 0 4	Enters line configuration mode for the lines.
Step 4	**privilege level** *level_number* **Example:** Router(config-line)# privilege level 10	Specifies a default privilege level for a line.
Step 5	**end** **Example:** Router(config-line)# end	Returns to global configuration mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J297 Display Current Privilege Levels Using Cisco IOS Commands

Purpose	This procedure displays the current privilege levels using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**show privilege** **Example:** Router# show privilege	Displays the current privilege level you can access based on the password you used.
Step 3	Return to your originating procedure (NTP).	—

DLP-J298 Log In to a Privilege Level Using Cisco IOS Commands

Purpose	This procedure logs in to a router at a specified privilege level, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**enable** *level* **Example:** Router# enable 12	Logs in to a specified privilege level.
Step 3	Return to your originating procedure (NTP).	—