Controlling Switch Access with Passwords and Privilege Levels

Restrictions for Controlling Switch Access with Passwords and Privileges

Disabling password recovery will not work if you have set the switch to boot up manually by using the **boot manual** command in global configuration mode. This command produces the boot loader prompt (*switch:*) after the switch is power cycled.

Restrictions and Guidelines for Reversible Password Types

- If the startup configuration has a type 6 password and you downgrade to a version in which type 6 password is not supported, you can/may be locked out of the device.

Restrictions and Guidelines for Irreversible Password Types

- Username secret password type 5 and enable secret password type 5 must be migrated to the stronger password type 8 or 9. For more information, see Protecting Enable and Enable Secret Passwords with Encryption, on page 6.
- Plain text passwords are converted to nonreversible encrypted password type 9.

Note This is supported in Cisco IOS Release 15.2(7)E3 and later releases.

Information About Passwords and Privilege Levels

The following sections provide information on passwords and privilege levels.

Preventing Unauthorized Access

You can prevent unauthorized users from reconfiguring your device and viewing configuration information. Typically, you want network administrators to have access to your device while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your device, you should configure one or more of these security features:

- At a minimum, you should configure passwords and privileges at each device port. These passwords are locally stored on the device. When users attempt to access the device through a port or line, they must enter the password specified for the port or line before they can access the device.
- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the device. These pairs are assigned to lines or ports and authenticate each user before that user can access the device. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.
- If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information.
- You can also enable the login enhancements feature, which logs both failed and unsuccessful login attempts. Login enhancements can also be configured to block future login attempts after a set number of unsuccessful attempts are made. For more information, see the Cisco IOS Login Enhancements documentation.

Default Password and Privilege Level Configuration

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

This table shows the default password and privilege level configuration.

Table 1: Default Password and Privilege Levels

Feature	Default Setting
Enable password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.
Enable secret password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	No password is defined.

Additional Password Security

Unmasked Secret Password

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a TFTP server, you can use either the **enable password** or **enable secret** commands in global configuration mode. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC 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.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and vty passwords.

Masked Secret Password

With **enable secret** command, password is encrypted but is visible on the terminal when you type the password. To mask the password on the terminal, use the **masked-secret** global configuration command. The encryption type for this password is type 9, by default.

You can use this command to configure masked secret password for common criteria policy.

Password Recovery

By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted.

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in Virtual Terminal Protocol (VTP) transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

To re-enable password recovery, use the **service password-recovery** command in global configuration mode.

Terminal Line Telnet Configuration

When you power-up your switch for the first time, an automatic setup program runs to assign IP information and to create a default configuration for continued use. The setup program also prompts you to configure your switch for Telnet access through a password. If you did not configure this password during the setup program, you can configure it when you set a Telnet password for a terminal line.

Username and Password Pairs

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Privilege Levels

Cisco devices use privilege levels to provide password security for different levels of switch operation. By default, the Cisco IOS software operates in two modes (privilege levels) of password security: user EXEC (Level 1) and privileged EXEC (Level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

Privilege Levels on Lines

Users can override the privilege level you set using the **privilege level** command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to a more restricted group of users.

Command Privilege Levels

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip traffic** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

How to Control Switch Access with Passwords and Privilege Levels

The following sections provide various configuration examples on how to control switch access with passwords and privilege levels.

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode.

To set or change a static enable password, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device configure terminal`	Enters global configuration mode.
Step 3	**enable password** *password* **Example:** `Device(config)# enable password secret321`	Defines a new password or changes an existing password for access to privileged EXEC mode. By default, no password is defined. *password*: Specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password abc?123, do this: **a.** Enter **abc**. **b.** Enter **Crtl-v**. **c.** Enter **?123**. When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Protecting Enable and Enable Secret Passwords with Encryption

To establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level, perform this procedure.

Procedure

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

Step 3	Use one of the following:
	• **enable password** [**level** *level*] {*unencrypted-password* | *encryption-type encrypted-password*}
	• **enable secret** [**level** *level*] {*unencrypted-password* | *encryption-type encrypted-password*}
	Example:
	`Device(config)# enable password level 12 example123`
	or
	`Device(config)# enable secret 9 $9$sMLBsTFXLnnHTk$0L82`
		• Defines a new password or changes an existing password for access to privileged EXEC mode.
		• Defines a secret password, which is saved using a nonreversible encryption method.
		• (Optional) For *level*, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).
		• For *unencrypted-password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
		• For *encryption-type*, the available options for **enable password** are type 0 and 7, and type 0, 5, 8, and 9 for **enable secret**. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration. Secret encryption type 9 is more secure, so we recommend that you select type 9 to avoid any issues while upgrading or downgrading.

	Command or Action	Purpose

		Note
		• If you do not specify an encryption type for the secret password, the password is auto converted to type 9.
		• If you specify an encryption type and then enter a clear text password, it will result in an error.
		• You can also configure type 9 encryption for the secret password manually by using the **algorithm-type scrypt** command in global configuration mode. For example:
		`Device(config)# username user1 algorithm-type scrypt secret cisco`
		Or
		`Device(config)# enable algorithm-type scrypt secret cisco`
		Run the **write memory** command in privileged EXEC mode for the type 9 secret to be permanently written into the startup configuration.

	Command or Action	Purpose
Step 4	**service password-encryption** **Example:** `Device(config)# service password-encryption`	(Optional) Encrypts the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Masked Secret Password

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Use one of the following: • **username** *name***masked-secret** • **username** *name***common-criteria-policy** *policy-name* **masked-secret** **Example:** `Device(config)# username cisco masked-secret` or	• Defines a masked secret password, which is saved using a nonreversible encryption method. • Defines a masked secret password for common criteria policy. • The masked secret password must be greater than 4 characters. The maximum length of masked-secret password is 256 characters. By default, no password is defined.

	Command or Action	Purpose
	`Device(config)# username common-criteria-policy test-policy masked-secret`	
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Setting a Telnet Password for a Terminal Line

To set a Telnet password for the connected terminal line, perform this procedure.

Before you begin

- Attach a PC or workstation with emulation software to the switch console port, or attach a PC to the Ethernet management port.
- The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device configure terminal`	Enters global configuration mode.
Step 3	**line vty 0 15** **Example:** `Device(config)# line vty 0 15`	Configures the number of Telnet sessions (lines), and enters line configuration mode. There are 16 possible sessions on a command-capable device. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.
Step 4	**password** *password* **Example:** `Device(config-line)# password abcxyz543`	Sets a Telnet password for the line or lines. *password*: Specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-line)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Username and Password Pairs

To configure username and password pairs, perform this procedure.

Procedure

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

Step 3	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}
	Example:
	`Device(config)# username adamsample privilege 1 password secret456`
	`Device(config)# username 111111111111 mac attribute`
		Sets the username, privilege level, and password for each user.
		• *name*: Specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed.
		• You can configure a maximum of 12000 clients each, for both username and MAC filter.
		• *level*: (Optional) Specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access.
		• *encryption-type*: Enter 0 to specify that an unencrypted password will follow. Enter

	Command or Action	Purpose
		7 to specify that a hidden password will follow. • *password*: Specify the password the user must enter to gain access to the device. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.

Step 4	Use one of the following:
	• **line console 0**
	• **line vty 0 15**
	Example:
	`Device(config)# line console 0`
	or
	`Device(config)# line vty 15`
		Enters line configuration mode, and configures the console port (line 0) or the vty lines (line 0 to 15).

Step 5	**login local** **Example:** `Device(config-line)# login local`	Enables local password checking at login time. Authentication is based on the username specified in Step 3.
Step 6	**end** **Example:** `Device(config-line)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Setting the Privilege Level for a Command

To set the privilege level for a command, follow this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device configure terminal`	Enters global configuration mode.
Step 3	**privilege** *mode* **level** *level command* **Example:** `Device(config)# privilege exec level 14 configure`	Sets the privilege level for a command. • *mode*: Enter **configure** for global configuration mode, **exec** for EXEC mode, **interface** for interface configuration mode, or **line** for line configuration mode. • *level*: Range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password. • *command*: Specify the command to which you want to restrict access.
Step 4	**enable password level** *level password* **Example:** `Device(config)# enable password level 14 SecretPswd14`	Specifies the password to enable the privilege level. • *level*: Range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • *password*: Specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the Default Privilege Level for Lines

Users can override the privilege level you set using the **privilege level** command by logging in to the line and enabling a different privilege level. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

To change the default privilege level for the specified line, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device configure terminal`	Enters global configuration mode.
Step 3	**line vty** *line* **Example:** `Device(config)# line vty 10`	Selects the vty on which to restrict access.
Step 4	**privilege level** *level* **Example:** `Device(config)# privilege level 15`	Changes the default privilege level for the line. *level*: Range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Logging into and Exiting a Privilege Level

Users can lower the privilege level by using the **disable** command.

To log into a specified privilege level and exit a specified privilege level, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** *level* **Example:** `Device> enable 15`	Logs in to a specified privilege level. Following the example, Level 15 is privileged EXEC mode. *level*: Range is 0 to 15.
Step 2	**disable** *level* **Example:**	Exits to a specified privilege level.

	Command or Action	Purpose
	`Device# disable 1`	Following the example, Level 1 is user EXEC mode. *level*: Range is 0 to 15.

Configuration Examples for Controlling Switch Access with Passwords and Privilege Levels

The following section provides configuration examples for controlling switch access with passwords and privilege levels.

Example: Setting or Changing a Static Enable Password

The following example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Device> enable
Device# configure terminal
Device(config)# enable password l1u2c3k4y5
```

Example: Protecting Enable and Enable Secret Passwords with Encryption

The following example shows how to configure the encrypted password *1FaD0$Xyti5Rkls3LoyxzS8* for privilege level 2:

```
Device> enable
Device# configure terminal
Device(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Example: Configuring Masked Secret Password

The following example shows how to configure the masked secret password:

```
Device> enable
Device# configure terminal
Device(config)# username cisco masked-secret
Enter secret: ******
Confirm secret: ******
```

The following example shows how to configure the masked secret password forfor common criteria policy:

```
Device> enable
Device# configure terminal
Device(config)# username cisco common-criteria-policy test-policy masked-secret
Enter secret: ******
Confirm secret: ******
```

Example: Setting a Telnet Password for a Terminal Line

The following example shows how to set the Telnet password to *let45me67in89*:

```
Device> enable
Device# configure terminal
Device(config)# line vty 10
Device(config-line)# password let45me67in89
```

Example: Setting the Privilege Level for a Command

The following example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
Device> enable
Device# configure terminal
Device(config)# line vty 10
Device(config)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
```

Monitoring Switch Access

Table 2: Commands for Displaying DHCP Information

Command	Purpose
show privilege	Displays the privilege level configuration.
show running | **secret username**	Verifies that the username is created and encypted to type9 by default.
show running | **secret enable**	Verifies that the secret password is encypted to type9 by default.

Feature History for Controlling Switch Access with Passwords and Privilege Levels

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS Release 15.2(7)E3k	Controlling Switch Access with Passwords and Privilege Levels	Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.