



Controlling Switch Access with Passwords and Privilege Levels

- [Restrictions for Controlling Switch Access with Passwords and Privileges, on page 1](#)
- [Information About Passwords and Privilege Levels, on page 2](#)
- [How to Control Switch Access with Passwords and Privilege Levels, on page 4](#)
- [Monitoring Switch Access, on page 13](#)
- [Configuration Examples for Setting Passwords and Privilege Levels, on page 14](#)
- [Additional References, on page 14](#)
- [Feature History for Controlling Switch Access with Passwords and Privileges, on page 15](#)

Restrictions for Controlling Switch Access with Passwords and Privileges

The following are the 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 global configuration command. This command produces the boot loader prompt (switch:) after the switch is power cycled.
- Password type 0 and type 7 are deprecated. So password type 0 and type 7, used for administrator login to Console, Telnet, SSH, webUI, and NETCONF, must be migrated to password type 8 or type 9.
- No action is required if username and password are type 0 and type 7 for local authentication such as CHAP, EAP and so on for ISG and Dot1x.
- Enable password type 0 and type 7 must be migrated to password type 8 or type 9.
- Password type 5 is deprecated. Password type 5 must be migrated to stronger password type 8 or type 9.

Information About Passwords and Privilege Levels

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

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the enable password or enable secret global configuration commands. 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 virtual terminal line passwords.

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 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 global configuration command.

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 line configuration 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

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Follow these steps to set or change a static enable 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	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. For 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 Ctrl-v when you create the password; for example, to create the password abc?123, do this: a. Enter abc. b. Enter Ctrl-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.

	Command or Action	Purpose
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

Follow these steps to establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Use one of the following: <ul style="list-style-type: none"> • enable password [level level] password encryption-type encrypted-password • enable secret [level level] password encryption-type encrypted-password 	<ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • (Optional) For level, the range is from 0 to 15. Level 1 is normal user EXEC

	Command or Action	Purpose
	<p>Example:</p> <pre>Device(config)# enable password example102</pre> <p>OR</p> <pre>Device(config)# enable secret level 1 password secret123sample</pre>	<p>mode privileges. The default level is 15 (privileged EXEC mode privileges).</p> <ul style="list-style-type: none"> • For 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. • (Optional) For encryption-type, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration. <p>Note If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.</p>
Step 4	<p>service password-encryption</p> <p>Example:</p> <pre>Device(config)# service password-encryption</pre>	<p>(Optional) Encrypts the password when the password is defined or when the configuration is written.</p> <p>Encryption prevents the password from being readable in the configuration file.</p>
Step 5	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>
Step 6	<p>show running-config</p> <p>Example:</p> <pre>Device# show running-config</pre>	<p>Verifies your entries.</p>
Step 7	<p>copy running-config startup-config</p> <p>Example:</p>	<p>(Optional) Saves your entries in the configuration file.</p>

	Command or Action	Purpose
	Device# <code>copy running-config startup-config</code>	

Disabling Password Recovery

Follow these steps to disable password recovery to protect the security of your switch:

Before you begin

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 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.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	system disable password recovery switch {all <1-9>} Example: Device(config)# <code>system disable password recovery switch all</code>	Disables password recovery. <ul style="list-style-type: none">• all - Sets the configuration on switches in stack.• <1-9> - Sets the configuration on the Switch Number selected. <p>This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but it is not part of the file system and is not accessible by any user.</p>
Step 4	end Example: Device(config)# <code>end</code>	Returns to privileged EXEC mode.

What to do next

To remove disable password recovery, use the `no system disable password recovery switch all global` configuration command.

Setting a Telnet Password for a Terminal Line

Beginning in user EXEC mode, follow these steps to set a Telnet password for the connected terminal line:

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> <code>enable</code>	Note If a password is required for access to privileged EXEC mode, you will be prompted for it. Enters privileged EXEC mode.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	line vty 0 15 Example: Device(config)# <code>line vty 0 15</code>	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)# <code>password abcxyz543</code>	Sets a Telnet password for the line or lines. For 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:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-line)# end	
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

Follow these steps to configure username and password pairs:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • For 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. • (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged

	Command or Action	Purpose
		<p>EXEC mode access. Level 1 gives user EXEC mode access.</p> <ul style="list-style-type: none"> • For encryption-type, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow. • For 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	<p>Use one of the following:</p> <ul style="list-style-type: none"> • line console 0 • line vty 0 15 <p>Example:</p> <pre>Device(config)# line console 0</pre> <p>or</p> <pre>Device(config)# line vty 15</pre>	Enters line configuration mode, and configures the console port (line 0) or the VTY lines (line 0 to 15).
Step 5	<p>login local</p> <p>Example:</p> <pre>Device(config-line)# login local</pre>	Enables local password checking at login time. Authentication is based on the username specified in Step 3.
Step 6	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 7	<p>show running-config</p> <p>Example:</p> <pre>Device# show running-config</pre>	Verifies your entries.
Step 8	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Setting the Privilege Level for a Command

Follow these steps to set the privilege level for a command:

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	privilege mode level level command Example: Device(config)# privilege exec level 14 configure	Sets the privilege level for a command. • For mode, enter configure for global configuration mode, exec for EXEC mode, interface for interface configuration mode, or line for line configuration mode. • For level, the 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. • For 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. • For level, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • For 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:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config)# end	
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

Follow these steps to change the default privilege level for the specified line:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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 virtual terminal line on which to restrict access.
Step 4	privilege level level Example: Device(config)# privilege level 15	Changes the default privilege level for the line. For level, the 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.

	Command or Action	Purpose
Step 6	copy running-config startup-config Example: Device# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

What to do next

Users can override the privilege level you set using the privilege level line configuration 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.

Logging into and Exiting a Privilege Level

Beginning in user EXEC mode, follow these steps to log into a specified privilege level and exit a specified privilege level.

Procedure

	Command or Action	Purpose
Step 1	enable level Example: Device> <code>enable 15</code>	Logs in to a specified privilege level. Following the example, Level 15 is privileged EXEC mode. For level, the range is 0 to 15.
Step 2	disable level Example: Device# <code>disable 1</code>	Exits to a specified privilege level. Following the example, Level 1 is user EXEC mode. For level, the range is 0 to 15.

Monitoring Switch Access

Table 2: Commands for Displaying DHCP Information

show privilege	Displays the privilege level configuration.
----------------	---

Configuration Examples for Setting Passwords and Privilege Levels

Example: Setting or Changing a Static Enable Password

This example shows how to change the enable password to 11u2c3k4y5. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Device(config)# enable password 11u2c3k4y5
```

Example: Protecting Enable and Enable Secret Passwords with Encryption

This example shows how to configure the encrypted password \$1\$FaD0\$Xyti5Rkls3LoyxzS8 for privilege level 2:

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

Example: Setting a Telnet Password for a Terminal Line

This example shows how to set the Telnet password to let45me67in89:

```
Device(config)# line vty 10
Device(config-line)# password let45me67in89
```

Example: Setting the Privilege Level for a Command

This 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(config)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
```

Additional References

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Controlling Switch Access with Passwords and Privileges

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 XE Everest 16.5.1a	Controlling Switch Access with Passwords and Privileges	<p>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.</p> <p>Support for this feature was introduced on all the models of the Cisco Catalyst 9500 Series Switches.</p>

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>.

