# Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices

**First Published: May 2, 2005**
**Last Updated: March 25, 2011**

Cisco IOS software-based networking devices provide several features that can be used to implement basic security for command-line sessions using only the operating system running on the device. These features include the following:

- Different levels of authorization for CLI sessions to control access to commands that can modify the status of the networking device versus commands that are used to monitor the device
- Assigning passwords to CLI sessions
- Requiring users to log in to a networking device with a username
- Changing the privilege levels of commands to create new authorization levels for CLI sessions

This module is a guide to implementing a baseline level of security for your networking devices. It focuses on the least complex options available for implementing a baseline level of security. If you have networking devices installed in your network with no security options configured, or you are about to install a networking device and you need help understanding how to implement a baseline of security, this document will help you.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices" section on page 38.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Contents



# Restrictions for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Your networking device must not be configured to use any local or remote authentication, authorization, and accounting (AAA) security features. This document describes only the non-AAA security features that can be configured locally on the networking device.

For information on how to configure AAA security features that can be run locally on a networking device, or for information on how to configure remote AAA security using TACACS+ or RADIUS servers, see the *Cisco IOS Security Configuration Guide: Securing User Services, Cisco IOS Release 15.1M&T*.

# Information About Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

# Benefits of Creating a Security Scheme for Your Networking Device

The foundation of a good security scheme in the network is the protection of the user interfaces of the networking devices from unauthorized access. Protecting access to the user interfaces on your networking devices prevents unauthorized users from making configuration changes that can disrupt the stability of your network or compromise your network security.

The features described in this document can be combined in many different ways to create a unique security scheme for each of your networking devices.

You can enable nonadministrative users to run a subset of the administrative commands available on the networking device by lowering the entitlement level for the commands to the nonadministrative privilege level. This can be useful for the following scenarios:

- ISPs that want their first-line technical support staff to perform tasks such as enabling new interfaces for new customers or resetting the connection for a customers whose connection has stopped transmitting traffic. See the "Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to Shut Down and Enable Interfaces" section on page 34 section for an example of how to do this.
- When you want your first-line technical support staff to have the ability to clear console port sessions that were disconnected improperly from a terminal server. See the "Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to Clear Remote CLI Sessions" section on page 32 section for an example of how to do this.
- When you want your first-line technical support staff to have the ability to view, but not change, the configuration of a networking device to facilitate troubleshooting a networking problem. See the "Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to View the Running Configuration Automatically" section on page 33 section for an example of how to do this.

# Cisco IOS CLI Modes

To aid in the configuration of Cisco devices, the Cisco IOS CLI is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of router and network operations. The commands available to you at any given time depending on the mode you are in. Entering a question mark (**?**) at the system prompt (router prompt) allows you to obtain a list of commands available for each command mode.

The use of specific commands allows you to navigate from one command mode to another. The standard order in which a user would access the modes is as follows: user EXEC mode; privileged EXEC mode; global configuration mode; specific configuration modes; configuration submodes; and configuration subsubmodes.

**Note** The default configuration of a Cisco IOS software-based networking device allows you to configure passwords to protect access only to user EXEC mode (for local and remote CLI sessions) and privileged EXEC mode. This document describes how you can provide additional levels of security by protecting access to other modes, and commands, using a combination of usernames, passwords and the **privilege** command.

Most EXEC mode commands are one-time commands, such as **show** or **more** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. EXEC mode commands are not saved across reboots of the router.

From privileged EXEC mode, you can enter global configuration mode. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots.

From global configuration mode you can enter a variety of protocol-specific or feature-specific configuration modes. The CLI hierarchy requires that you enter these specific configuration modes only through global configuration mode. For example, interface configuration mode is a commonly used configuration mode.

From configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode. For example, the subinterface configuration mode is a submode of the interface configuration mode.

ROM monitor mode is a separate mode used when the router cannot boot properly. If your system (router, switch, or access server) does not find a valid system image to load when it is booting, the system will enter ROM monitor mode. ROM monitor (ROMMON) mode can also be accessed by interrupting the boot sequence during startup.

The following sections contain detailed information on these command modes:



## User EXEC Mode

When you start a session on a router, you generally begin in user EXEC mode, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in user EXEC mode. This level of access is reserved for tasks that do not change the configuration of the router, such as determining the router status.

If your device is configured to require users to log in the login process will require a username and a password. If you enter incorrect password three times, the connection attempt is refused.

User EXEC mode is set by default to privilege level 1. Privileged EXEC mode is set by default to privilege level 15. For more information see the "Privileged EXEC Mode" section on page 5. When you are logged in to a networking device in user EXEC mode your session is running at privilege level 1. When you are logged in to a networking device in privileged EXEC mode your session is running at

privilege level 15. You can move commands to any privilege level between 1 and 15 using the **privilege** command. See the "Cisco IOS Privilege Levels" section on page 11 for more information on privilege levels and the **privilege** command.

In general, the user EXEC commands allow you to connect to remote devices, change terminal line settings on a temporary basis, perform basic tests, and list system information.

To list the available user EXEC commands, enter a question mark (**?**). The list of commands will vary depending on the software feature set and router platform you are using.

The user EXEC mode prompt consists of the hostname of the device followed by an angle bracket (>), for example, Router>.

The default hostname is generally Router, unless it has been changed during initial configuration using the **setup** EXEC command. You can also change the hostname using the **hostname** global configuration command.

**Note** Examples in Cisco IOS documentation assume the use of the default name of "Router." Different devices (for example, access servers) may use a different default name. If the routing device (router, access server, or switch) has been named with the **hostname** command, that name will appear as the prompt instead of the default name.

**Note** You can enter commands in uppercase, lowercase, or mixed case. Only passwords are case-sensitive. However, Cisco IOS documentation convention is to always present commands in lowercase.

## Privileged EXEC Mode

In order to have access to all commands, you must enter privileged EXEC mode, which is the second level of access for the EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. In privileged EXEC mode, you can enter any EXEC command, because privileged EXEC mode is a superset of the user EXEC mode commands.

Because many privileged EXEC mode commands set operating parameters, privileged EXEC level access should be password protected to prevent unauthorized use. The privileged EXEC command set includes those commands contained in user EXEC mode. Privileged EXEC mode also provides access to configuration modes through the **configure** command, and includes advanced testing commands, such as **debug**.

Privileged EXEC mode is set by default to privilege level 15. User EXEC mode is set by default to privilege level 1. For more information see the "User EXEC Mode" section on page 4. By default the EXEC commands at privilege level 15 are a superset of those available at privilege level 1. You can move commands to any privilege level between 1 and 15 using the **privilege** command. See the "Cisco IOS Privilege Levels" section on page 11 for more information on privilege levels and the **privilege** command.

The privileged EXEC mode prompt consists of the hostname of the device followed by a pound sign (#), for example, Router#.

To access privileged EXEC mode, use the **enable** command. If a privileged EXEC mode password has been configured the system will prompt you for a password after you issue the **enable** command. Use the **exit** command to leave privileged EXEC mode.

**Note** Privileged EXEC mode is sometimes referred to as "enable mode," because the **enable** command is used to enter the mode.

If a password has been configured on the system, you will be prompted to enter it before being allowed access to privileged EXEC mode. The password is not displayed on the screen and is case-sensitive. If an enable password has not been set, privileged EXEC mode can be accessed only by a local CLI session (terminal connected to the console port).

If you attempt to access privileged EXEC mode on a router over a remote connection, such as aTelnet connection, and you have not configured a password for privileged EXEC mode, you will see the **% No password set** error message. For more information on remote connections see the "Remote CLI Sessions" section on page 8. The system administrator uses the **enable secret** or **enable password** global configuration command to set the password that restricts access to privileged EXEC mode. For information on configuring a password for privileged EXEC mode, see the "Protecting Access to Privileged EXEC Mode" section on page 20.

To return to user EXEC mode, use the **disable** command:

Note that the password will not be displayed as you type, but is shown here for illustrational purposes. To list the commands available in privileged EXEC mode, issue question mark (**?**) at the prompt. From privileged EXEC mode you can access global configuration mode, which is described in the following section.

**Note** Because the privileged EXEC command set contains all of the commands available in user EXEC mode, some commands can be entered in either mode. In Cisco IOS documentation, commands that can be entered in either user EXEC mode or privileged EXEC mode are referred to as EXEC mode commands. If user or privileged is not specified in the documentation, assume that you can enter the referenced commands in either mode.

## Global Configuration Mode

The term "global" is used to indicate characteristics or features that affect the system as a whole. Global configuration mode is used to configure your system globally, or to enter specific configuration modes to configure specific elements such as interfaces or protocols. Use the **configure terminal** privileged EXEC command to enter global configuration mode.

To access global configuration mode, use the **configure terminal** command in privileged EXEC mode:

Note that the system prompt changes to indicate that you are now in global configuration mode. The prompt for global configuration mode consists of the hostname of the device followed by (config) and the pound sign (#). To list the commands available in privileged EXEC mode, issue **?** at the prompt.

Commands entered in global configuration mode update the running configuration file as soon as they are entered. In other words, changes to the configuration take effect each time you press the Enter or Return key at the end of a valid command. However, these changes are not saved into the startup configuration file until you issue the **copy running-config startup-config** EXEC mode command.

The system dialog prompts you to end your configuration session (exit configuration mode) by pressing the Control (Ctrl) and "z" keys simultaneously; when you press these keys, **^Z** is printed to the screen. You can actually end your configuration session by entering the Ctrl-Z key combination, using the **end** command, and using the Ctrl-C key combination. The **end** command is the recommended way to indicate to the system that you are done with the current configuration session.

**Caution** If you use Ctrl-Z at the end of a command line in which a valid command has been typed, that command will be added to the running configuration file. In other words, using Ctrl-Z is equivalent to hitting the Enter (Carriage Return) key before exiting. For this reason, it is safer to end your configuration session using the **end** command. Alternatively, you can use the Ctrl-C key combination to end your configuration session without sending a Carriage Return signal.

You can also use the **exit** command to return from global configuration mode to EXEC mode, but this only works in global configuration mode. Pressing Ctrl-Z or entering the **end** command will always take you back to EXEC mode regardless of which configuration mode or configuration submode you are in.

To exit global configuration command mode and return to privileged EXEC mode, use the **end** or **exit** command.

From global configuration mode, you can enter a number of protocol-specific, platform-specific, and feature-specific configuration modes.

Interface configuration mode, described in the following section, is an example of a configuration mode you can enter from global configuration mode.

## Interface Configuration Mode

One example of a specific configuration mode you can enter from global configuration mode is interface configuration mode.

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as an Ethernet, FDDI, or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type.

For details on interface configuration commands that affect general interface parameters, such as bandwidth or clock rate, refer to the *Cisco IOS Interface Configuration Guide*.

To access and list the interface configuration commands, use the interface type number command.

To exit interface configuration mode and return to global configuration mode, enter the **exit** command.

Configuration submodes are configuration modes entered from other configuration modes (besides global configuration mode). Configuration submodes are for the configuration of specific elements within the configuration mode. One example of a configuration submode is subinterface configuration mode, described in the following section.

## Subinterface Configuration Mode

From interface configuration mode, you can enter subinterface configuration mode. Subinterface configuration mode is a submode of interface configuration mode. In subinterface configuration mode you can configure multiple virtual interfaces (called subinterfaces) on a single physical interface. Subinterfaces appear to be distinct physical interfaces to the various protocols.

For detailed information on how to configure subinterfaces, refer to the appropriate documentation module for a specific protocol in the Cisco IOS software documentation set.

To exit subinterface configuration mode and return to interface configuration mode, use the **exit** command. To end your configuration session and return to privileged EXEC mode, press Ctrl-Z or enter the **end** command.

# Cisco IOS CLI Sessions



## Local CLI Sessions

Local CLI sessions require direct access to the console port of the networking device. Local CLI sessions start in user EXEC mode. See the "Cisco IOS CLI Modes" section on page 3 for more information on the different modes that are supported on your networking device. All of the tasks required to configure and manage a networking device can be done using a local CLI session. The most common method for establishing a local CLI session is to connect the serial port on a PC to the console port of the networking device and then to launch a terminal emulation application on the PC. The type of cable and connectors required and the settings for the terminal emulation application on the PC depend on the type of networking device that you are configuring. See the documentation for your networking device for more information on setting it up for a local CLI session.

## Remote CLI Sessions

Remote CLI sessions are created between a host such as a PC and a networking device such as a router over a network using a remote terminal access application such as Telnet and SSH. Local CLI sessions start in user EXEC mode. See the "Cisco IOS CLI Modes" section on page 3 for more information on the different modes that are supported on your networking device. Most of the tasks required to configure and manage a networking device can be done using a remote CLI session. The exceptions are tasks that interact directly with the console port (such as recovering from a corrupted operating system (OS) by uploading a new OS image over the console port) and interacting with the networking device when it is in ROMMON mode.

Telnet is the most common method for accessing a remote CLI session on a networking device.

**Note** SSH is a more secure alternative to Telnet. SSH provides encryption for the session traffic between your local management device such as a PC and the networking device that you are managing. Encrypting the session traffic with SSH prevents hackers that might intercept the traffic from being able to decode it. See *Secure Shell Version 2 Support* feature module for more information on using SSH.

## Terminal Lines Used for Local and Remote CLI Sessions

Cisco networking devices use the word "lines" to refer to the software components that manage local and remote CLI sessions. You use the **line console 0** global configuration command to enter line configuration mode to configure options, such as a password, for the console port.

Remote CLI sessions use lines that are referred to as vty lines. You use the **line vty** *line-number* [*ending-line-number*] global configuration command to enter line configuration mode to configure options, such as a password, for remote CLI sessions.

# Protection of Access to Cisco IOS EXEC Modes

Cisco IOS software provides the ability to configure passwords that protect access to the following:

## Protection of Access to User EXEC Mode

The first step in creating a secure environment for your networking device is protecting access to user EXEC mode by configuring passwords for local and remote CLI sessions.

You can protect access to user EXEC mode for local CLI sessions by configuring a password on the console port. See the "Configuring a Password for Local CLI Sessions" section on page 18.

You can protect access to user EXEC mode for remote CLI sessions by configuring a password on the vtys. See the "Configuring a Password for Remote CLI Sessions" section on page 16 for instructions on how to configure passwords for remote CLI sessions.

## Protection of Access to Privileged EXEC Mode

The second step in creating a secure environment for your networking device is protecting access to privileged EXEC mode with a password. The method for protecting access to privileged EXEC mode is the same for local and remote CLI sessions.

You can protect access to privileged EXEC mode by configuring a password for it. This is sometimes referred to as the enable password because the command to enter privileged EXEC mode is **enable**.

# Cisco IOS Password Encryption Levels

Some of the passwords that you configure on your networking device are saved in the configuration in plain text. This means that if you store a copy of the configuration file on a disk, anybody with access to the disk can discover the passwords by reading the configuration file. The following password types are stored as plain text in the configuration by default:

- Console passwords for local CLI sessions.
- Virtual terminal line passwords for remote CLI sessions.
- Username passwords using the default method for configuring the password.
- Privileged EXEC mode passwords when they are configured with the **enable password** *password* command.
- Authentication key chain passwords used by Routing Information Protocol version 2 (RIPv2) and Enhanced Interior Gateway Routing Protocol (EIGRP).
- BGP passwords for authenticating BGP neighbors.
- Open Shortest Path First (OSPF) authentication keys for authenticating OSPF neighbors.
- Intermediate System-Intermediate System (IS-IS) passwords for authenticating ISIS neighbors.

The following excerpt from a router configuration file shows examples of passwords and authentication keys that are stored as clear text:

```
!
enable password O9Jb6D
!
username username1 password 0 kV9sIj3
!
```

```
key chain trees
 key 1
  key-string key1
!
interface Ethernet1/0.1
 ip address 172.16.6.1 255.255.255.0
 ip router isis
 ip rip authentication key-chain key2
 ip authentication key-chain eigrp 1 key2
 ip ospf authentication-key j7876
 no snmp trap link-status
 isis password u7865k
!
line vty 0 4
 password V9jA5M
!
```

You can encrypt these clear text passwords in the configuration file by using the **service password-encryption** command. This should be considered as a minimal level of security because the encryption algorithm used by the **service password-encryption** command to encrypt passwords creates text strings that can be decrypted using tools that are publicly available. You should still protect access to any electronic or paper copies of your configuration files after you use the **service password-encryption** command.

The **service password-encryption** command does not encrypt the passwords when they are sent to the remote device. Anybody with a network traffic analyzer who has access to you network can capture these passwords from the packets as they are transmitted between the devices. See the "Configuring Password Encryption for Clear Text Passwords" section on page 22 for more information on encrypting clear text passwords in configuration files.

Many of the Cisco IOS features that use clear text passwords can also be configured to use the more secure message digest algorithm 5 (MD5). The MD5 algorithm creates a text string in the configuration file that is much more difficult to decrypt. The MD5 algorithm does not send the password to the remote device. This prevents people using a traffic analyzer to capture traffic on your network from being able to discover your passwords.

You can determine the type of password encryption that has been used by the number that is stored with the password string in the configuration file of the networking device.

# Cisco IOS CLI Session Usernames

After you have protected access to user EXEC mode and privileged EXEC mode by configuring passwords for them you can further increase the level of security on your networking device by configuring usernames to limit access to CLI sessions to your networking device to specific users.

Usernames that are intended to be used for managing a networking device can be modified with additional options such as:

- Automatically starting a CLI session at a specific privilege level. See the "Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff" section on page 29.
- Running a CLI command automatically. See the "Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to View the Running Configuration Automatically" section on page 33.

See the *Cisco IOS Security Command Reference* for more information on how to configure the **username** command.

# Cisco IOS Privilege Levels

The default configuration for Cisco IOS software-based networking devices uses privilege level 1 for user EXEC mode and privilege level 15 for privileged EXEC. The commands that can be run in user EXEC mode at privilege level 1 are a subset of the commands that can be run in privileged EXEC mode at privilege 15.

The **privilege** command is used to move commands from one privilege level to another. For example, some ISPs allow their first level technical support staff to enable and disable interfaces to activate new customer connections or to restart a connection that has stopped transmitting traffic. See the "Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to Shut Down and Enable Interfaces" section on page 34 for an example of how to configure this option.

The **privilege** command can also be used to assign a privilege level to a username so that when a user logs in with the username, the session runs at the privilege level specified by the **privilege** command. For example, if you want your technical support staff to view the configuration on a networking device which will help them to troubleshoot network problems without being able to modify the configuration, you can create a username, configure it with privilege level 15, and configure it to run the **show running-config** command automatically. When a user logs in with the username the running configuration will be displayed automatically. The user's session will be logged out automatically after the user has viewed the last line of the configuration. See the "Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to View the Running Configuration Automatically" section on page 33 for an example of how to configure this option.

These command privileges can also be implemented when you are using AAA with TACACS+ and RADIUS. For example, TACACS+ provides two ways to control the authorization of router commands on a per-user or per-group basis. The first way is to assign privilege levels to commands and have the router verify with the TACACS+ server whether the user is authorized at the specified privilege level. The second way is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the commands that are allowed. For more information about implementing AAA with TACACS+ and RADIUS, see the technical note *How to Assign Privilege Levels with TACACS+ and RADIUS*.

# Cisco IOS Password Configuration

Cisco IOS software does not prompt you to repeat any passwords that you configure to verify that you have entered the passwords exactly as you intended. New passwords, and changes to existing passwords, go into effect immediately after you press the Enter key at the end of a password configuration command string. If you make a mistake when you enter a new password and have saved the configuration on the networking device to its startup configuration file and exited privileged EXEC mode before you realize that you made a mistake, you may find that you are no longer able to manage the device.

The following are common situations that can happen:

- You make a mistake when configuring a password for local CLI sessions on the console port.
  - If you have properly configured access to your networking device for remote CLI sessions, you can Telnet to it and reconfigure the password on the console port.
- You make a mistake when configuring a password for remote Telnet or SSH sessions.
  - If you have properly configured access to your networking device for local CLI sessions, you can connect a terminal to it and reconfigure the password for the remote CLI sessions.
- You make a mistake when configuring a password for privileged EXEC mode (enable password or enable secret password).
  - You will have to perform a lost password recovery procedure.

- You make a mistake when configuring your username password, and the networking device requires that you log in to it with your username.
  - If you do not have access to another account name, you will have to perform a lost password recovery procedure.

To protect yourself from having to perform a lost password recovery procedure open two CLI sessions to the networking device and keep one of them in privileged EXEC mode while you reset the passwords using the other session. You can use the same device (PC or terminal) to run the two CLI sessions or two different devices. You can use a local CLI session and a remote CLI session or two remote CLI sessions for this procedure. The CLI session that you use to configure the password can also be used to verify that the password was changed properly. The other CLI session that you keep in privileged EXEC mode can be used to change the password again if you made a mistake the first time you configured it.

You should not save password changes that you have made in the running configuration to the startup configuration until you have verified that your password was changed successfully. If you discover that you made a mistake configuring a password, and you were not able to correct the problem using the local and remote CLI session technique, you can power cycle the networking device so that it returns to the previous passwords that are stored in the startup configuration.

# Product Security Baseline: Password Encryption and Complexity Restrictions

Product security baseline (PSB) mandates basic security functions and features for all Cisco platforms and products.

There are 12 priority security requirements out of the 110 mandatory requirements in version 2.0 of the product security baseline that must be met to allow the shipping of any product.

The following two sections discuss restrictions that are relevant in AAA technology:

- Password complexity restrictions
- Protection of stored credentials

## Password Complexity Restrictions

The PSB states the following requirements for password complexity restrictions on Cisco products:

- Whenever a user or an administrator wants to create or change a password, the following restrictions apply to the products:
  - The new password contains characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
  - No character in the new password should be repeated more than three times consecutively.
  - The new password should not be the same as the associated username, and should not be the username reversed. The password obtained by capitalization of the username or username reversed also is not accepted.
  - The new password should not be “cisco”, “ocsic”, or any variant obtained by changing the capitalization of letters therein, or by substituting “1”, “|”, or “!” for i, and substituting “0” for “o”, and substituting “$” for “s”.
- It must be possible to individually enable or disable each of these restrictions as part of the product configuration. A user interface should be available for one time to override the restrictions when a password is being set by an administrator.

The first restriction need not be applied to passwords that are expected to be used via a numerical pin pad; in this case, passwords consisting only of digits are permitted. However, such passwords must be used only for access to messaging services, and not for general computer networking services.

For an administrator to enable the restrictions, no particular default setting is required. Restrictions should be enabled by default on products that permit nonadministrative end users to change their own passwords.

AAA enforces these restrictions on creating passwords used in a AAA context which includes passwords created using the **username** command and passwords created to download authorization data.

The complexity restrictions are enabled or disabled using the **aaa password restriction** command. The behavior should be backward-compatible in allowing passwords that were configured before the complexity restrictions were enabled. The CLI should be disabled by default. When the CLI is enabled on a running router, the passwords configured prior to enabling the command should not be subject to the complexity restrictions. The passwords configured following the command should be subject to complexity restrictions. When a router is rebooted using a startup configuration containing the password complexity command enabled, the passwords present in the startup configuration should be allowed without the complexity restrictions; any passwords that are configured after the router has booted should be subject to the complexity restrictions.

### Protection of Stored Credentials

The PSB states the following requirement for password complexity restrictions on Cisco products:

- If the product authenticates remote entities using protocols that do not require the product to possess recoverable copies of the remote entities' credentials, then no recoverable copies of credentials which are used only in this way are to be stored.
- In the specific case where the product authenticates remote entities using the traditional password interchange in which the remote entity discloses its credential to the product for direct comparison against a database, stored credentials must be protected by a method at least as strong as a SHA-1 digest. The use of SHA-256 or SHA-384 instead of SHA-1 is recommended.

To be compliant with the PSB, AAA enforces the protection of stored credentials using SHA-256.

## Recovering from a Lost or Misconfigured Password for Local CLI Sessions

Three methods can be used to recover a lost or misconfigured password for local CLI sessions over console port. The method that you will use depends on the current configuration of your networking device.

The following sections describes the three methods that can be used to recover a lost or misconfigured password:

- Networking Device Is Configured to Allow Remote CLI Sessions, page 14
- Networking Device Is Not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Not Been Saved to the Startup Configuration File, page 14
- Networking Device Is Not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Been Saved to the Startup Configuration File, page 14

### Networking Device Is Configured to Allow Remote CLI Sessions

The fastest method to recover from a lost or misconfigured password for local CLI sessions is to establish a remote CLI session with the networking device and repeat the steps in the "Configuring a Password for Local CLI Sessions" section on page 18. Your networking device must be configured to allow remote CLI sessions and you must know the remote CLI session password to perform this procedure.

### Networking Device Is Not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Not Been Saved to the Startup Configuration File

If you cannot establish a remote session to your networking device, and you have not saved the misconfigured local CLI session password to the startup configuration, you can restart the networking device. When the networking device starts up again it will read the startup configuration file. The previous local CLI session password is restored.

**Caution** Restarting a networking device will cause it to stop forwarding traffic. This will also cause an interruption in any services that are running on the networking device, such as a DHCP server service. You should restart a networking device only during a period of time that has been allocated for network maintenance.

### Networking Device Is Not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Been Saved to the Startup Configuration File

If you cannot establish a remote CLI session with the networking device, and you have saved the misconfigured local CLI session password to the startup configuration, or you have lost the local CLI session password, you must perform a password recovery procedure. Password recovery procedures are device specific. You must locate the document that describes the procedure for your type of networking device. See the "Technical Assistance" section on page 37 for more Cisco support information for your networking device.

## Recovering from a Lost or Misconfigured Password for Remote CLI Sessions

Three methods that can be used to recover from a lost or misconfigured remote CLI session password. The method that you will use depends on the current configuration of your networking device.


- Networking Device Is Configured to Allow Local CLI Sessions, page 14
- Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Not Been Saved to the Startup Configuration File, page 15
- Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Been Saved to the Startup Configuration File, page 15


### Networking Device Is Configured to Allow Local CLI Sessions

The fastest method to recover from a lost or misconfigured password for remote CLI sessions is to establish a local CLI session with the networking device and repeat the steps in the "Configuring a Password for Remote CLI Sessions" section on page 16. Your networking device must be configured to allow local CLI sessions and you must know the local CLI session password to perform this procedure.

### Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Not Been Saved to the Startup Configuration File

If you cannot establish a local CLI session to your networking device, and you have not saved the misconfigured remote CLI session password to the startup configuration, you can restart the networking device. When the networking device starts up again it will read the startup configuration file. The previous remote CLI session password is restored.

**Caution** Restarting a networking device will cause it to stop forwarding traffic. This will also cause an interruption in any services that are running on the networking device, such as a DHCP server service. You should restart a networking device only during a period of time that has been allocated for network maintenance.

### Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Been Saved to the Startup Configuration File

If you cannot establish a local CLI session with the networking device, and you have saved the misconfigured remote CLI session password to the startup configuration, or you have lost the remote CLI session password, you must perform a password recovery procedure. Password recovery procedures are device specific. You must locate the document that describes the procedure for your type of networking device. See the "Technical Assistance" section on page 37 for more Cisco support information for your networking device.

## Recovering from a Lost or Misconfigured Passwords for Privileged EXEC Mode

Two methods can be used to recover from a lost or misconfigured privileged EXEC mode password. The method that you will use depends on the current configuration of your networking device.

- A Misconfigured Privileged EXEC Mode Password Has Not Been Saved to the Startup Configuration File, page 15
- A Misconfigured Privileged EXEC Mode Password Has Been Saved to the Startup Configuration File, or the Privileged EXEC Mode Password Has Been Lost, page 16

### A Misconfigured Privileged EXEC Mode Password Has Not Been Saved to the Startup Configuration File

If you have not saved the misconfigured privileged EXEC mode password to the startup configuration, you can restart the networking device. When the networking device starts up again it will read the startup configuration file. The previous privileged EXEC mode password is restored.

**Caution** Restarting a networking device will cause it to stop forwarding traffic. This will also cause an interruption in any services that are running on the networking device, such as a DHCP server service. You should restart a networking only device during a period of time that has been allocated for network maintenance.

### A Misconfigured Privileged EXEC Mode Password Has Been Saved to the Startup Configuration File, or the Privileged EXEC Mode Password Has Been Lost

If you have saved the misconfigured privileged EXEC mode password to the startup configuration, or you have lost the privileged EXEC mode password, you must perform a password recovery procedure. Password recovery procedures are device specific. You must locate the document that describes the procedure for your type of networking device. See the "Technical Assistance" section on page 37 for more Cisco support information for your networking device.

# How to Configure Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices



## Protecting Access to User EXEC Mode

This section contains the following procedures:



### Configuring a Password for Remote CLI Sessions

This task will assign a password for remote CLI sessions. After you have completed this task the networking device will prompt you for a password the next time that you start a remote CLI session with it.

Cisco IOS software-based networking devices require that you have a password configured for remote CLI sessions. If you attempt to start a remote CLI session with a device that does not have a password configured for remote CLI sessions you will see a message that a password is required and the password is not set. The remote CLI session will be terminated by the remote host.

#### Prerequisites

If you have not previously configured a password for remote CLI sessions, you must perform this task over a local CLI session using a terminal or a PC running a terminal emulation application attached to the console port.

Your terminal, or terminal emulation application, must be configured with the settings that are used by the console port on the networking device. The console ports on most Cisco networking devices require the following settings: 9600 baud, 8 data bits, 1 stop bit, no parity, and flow control is set to "none". See the documentation for your networking device if these settings do not work for your terminal.

### Restrictions

If you have not previously configured a password for remote CLI sessions, you must perform this task over a local CLI session using a terminal attached to the console port.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line vty** *line-number* [*ending-line-number*]
4. **password** *password*
5. **end**
6. **telnet** *ip-address*
7. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **line vty** *line-number* [*ending-line-number*]<br><br>**Example:**<br>`Router(config)# line vty 0 4` | Enters line configuration mode. |
| **Step 4** | **password** *password*<br><br>**Example:**<br>`Router(config-line)# password H7x3U8` | Assigns a password for remote CLI session.<br>• The argument *password* is a character string that specifies the line password. The following rules apply to the *password* argument:<br>– The first character cannot be a number.<br>– The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything.<br>– Passwords are case-sensitive. |
| **Step 5** | **end**<br><br>**Example:**<br>`Router(config-line)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **telnet** *ip-address*<br><br>**Example:**<br>`Router# telnet 172.16.1.1` | Start a remote CLI session with the networking device from your current CLI session using the IP address of an interface in the networking device that is in an operational state (interface up, line protocol up).<br>• Enter the password that you configured is Step 4 when prompted.<br>• To perform this step, your networking device must have an interface that is in an operational state. The interface must have a valid IP address.<br>**Note** This procedure is often referred to as a starting recursive Telnet session because you are initiating a remote Telnet session with the networking device from the networking device itself. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router# exit` | Terminates the remote CLI session (recursive Telnet session) with the networking device. |

### Troubleshooting Tips

Repeat this task if you made a mistake when configuring the remote CLI session password.

## Configuring a Password for Local CLI Sessions

This task will assign a password for local CLI sessions over the console port. After you have completed this task, the networking device will prompt you for a password the next time that you start a local CLI session on the console port.

This task can be performed over a local CLI session using the console port or a remote CLI session. If you want to perform the optional step of verifying that you have configured the password correctly you should perform this task using a local CLI session using the console port.

### Prerequisites

If you want to perform the optional step of verifying the local CLI session password, you must perform this task using a local CLI session. You must have a terminal or a PC running a terminal emulation program connected to the console port of the networking device. Your terminal must be configured with the settings that are used by the console port on the networking device. The console ports on most Cisco networking devices require the following settings: 9600 baud, 8 data bits, 1 stop bit, no parity, and flow control set to “none”. See the documentation for your networking device if these settings do not work for your terminal.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line console** *line-number*
4. **password** *password*

5. **end**
6. **exit**
7. Press the Enter key, and enter the password from Step 4 when prompted.

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **line console** *line-number*<br><br>**Example:**<br>`Router(config)# line console 0` | Enters line configuration mode and selects the console port as the line that you are configuring. |
| **Step 4** | **password** *password*<br><br>**Example:**<br>`Router(config-line)# password Ji8F5Z` | Assigns a password for local CLI session over the console port.<br>• The argument *password* is a character string that specifies the line password. The following rules apply to the *password* argument:<br>– The first character cannot be a number.<br>– The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything.<br>– Passwords are case-sensitive. |
| **Step 5** | **end**<br><br>**Example:**<br>`Router(config-line)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router# exit` | Exits privileged EXEC mode. |
| **Step 7** | Press the Enter key, and enter the password from Step 4 when prompted. | (Optional) Initiates the local CLI session on the console port.<br>• Enter the password that you configured is Step 4 when prompted to verify that it was configured correctly.<br>**Note** This step can be performed only if you are using a local CLI session to perform this task. |

### Troubleshooting Tips

If your new password is not accepted proceed to the "Configuration Examples for Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices" section on page 32 for instructions on what to do next.

# Protecting Access to Privileged EXEC Mode

This section contains the following procedures:

- Configuring the Enable Password, page 20 (optional)
- Configuring Password Encryption for Clear Text Passwords, page 22 (optional)
- Configuring the Enable Secret Password, page 23 (recommended)

## Configuring the Enable Password

Cisco no longer recommends that you use the **enable password** command to configure a password for privileged EXEC mode. The password that you enter with the **enable password** command is stored as plain text in the configuration file of the networking device. You can encrypt the password for the **enable password** command in the configuration file of the networking device using the **service password-encryption** command. However the encryption level used by the **service password-encryption** command can be decrypted using tools available on the Internet.

Instead of using the **enable password** command, Cisco recommends using the **enable secret** command because it encrypts the password that you configure with strong encryption. For more information on password encryption issues see the "Cisco IOS Password Encryption Levels" section on page 9. For information on configuring the **enable secret** command see the "Configuring the Enable Secret Password" section on page 23.

### Restrictions

The networking device must not have a password configured by the **enable secret** command in order for you to perform this task successfully. If you have already configured a password for privileged EXEC mode using the **enable secret** command, that the password configured takes precedences over the password that you configure in this task using the **enable password** command.

You cannot use the same password for the **enable secret** command and the **enable** *password* command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **end**
5. **exit**
6. **enable**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **enable password** *password*<br><br>**Example:**<br>`Router(config)# enable password t6D77CdKq` | Configures a password for privileged EXEC mode.<br>• The argument *password* is a character string that specifies the enable password.<br>• The argument *password* must contain from 1 to 25 uppercase and lowercase alphanumeric characters.<br>• The argument *password* must not have a number as the first character.<br>• The argument *password* can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.<br>• The argument *password* 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 the following:<br>– Enter abc<br>– Type Crtl-v<br>– Enter ?123 |
| **Step 4** | **end**<br><br>**Example:**<br>`Router(config)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router# exit` | Exits privileged EXEC mode. |
| **Step 6** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter the password you configured in Step 3. |

### Troubleshooting Tips

If your new password is not accepted, proceed to the "Recovering from a Lost or Misconfigured Passwords for Privileged EXEC Mode" section on page 15 for instructions on what to do next.

## Configuring Password Encryption for Clear Text Passwords

Cisco IOS software stores passwords in clear text in network device configuration files for several features such as passwords for local and remote CLI sessions, and passwords for neighbor authentication for routing protocols. Clear text passwords are a security risk because anybody with access to archived copies of the configuration files can discover the passwords that are stored as clear text. The **service password-encryption** command can be used to encrypt clear text commands in the configuration files of networking devices. See the "Cisco IOS Password Encryption Levels" section on page 9 for more information.

Complete the following steps to configure password encryption for passwords that are stored as clear text in the configuration files of your networking device.

### Prerequisites

You must have at least one feature that uses clear text passwords configured on your networking device for the **service password-encryption** command to have any immediate effect.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service password-encryption**
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **service password-encryption**<br><br>**Example:**<br>`Router(config)# service password-encryption` | Configures password encryption for all passwords, clear text passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and BGP neighbor passwords. |
| **Step 4** | **end**<br><br>**Example:**<br>`Router(config)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |

## Configuring the Enable Secret Password

Cisco recommends that you use the **enable secret** command, instead of the **enable** *password* command to configure a password for privileged EXEC mode. The password created by the **enable secret** command is encrypted with the more secure MD5 algorithm.

### Restrictions

You cannot use the same password for the **enable secret** command and the **enable** *password* command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable secret** *unencrypted-password*
   or
   **enable secret** *encryption-type encrypted-password*
4. **end**
5. **exit**
6. **enable**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **enable secret** *unencrypted-password*<br>or<br>**enable secret** *encryption-type encrypted-password*<br><br>**Example:**<br>`Router(config)# enable secret t6D77CdKq`<br>or<br>`Router(config)# enable secret 5 $1$/x6H$RhnDI3yLC4GA01aJnHLQ4/` | Configures a password for privileged EXEC mode.<br>• The argument *password* is a character string that specifies the **enable secret** password. The following rules apply to the *password* argument:<br>• The argument *password* must contain from 1 to 25 uppercase and lowercase alphanumeric characters.<br>• The argument *password* must not have a number as the first character.<br>• The argument *password* can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.<br>• The argument *password* 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 the following:<br>– Enter abc<br>– Type Crtl-v<br>– Enter ?123<br>or<br>Sets a previously encrypted password for privileged EXEC mode by entering the number 5 before the previously encrypted string.<br>• You must enter an exact copy of a password from a configuration file that was previously encrypted by the **enable secret** command to use this method. |
| **Step 4** | **end**<br><br>**Example:**<br>`Router(config)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router# exit` | Exits privileged EXEC mode. |
| **Step 6** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter the password that you configured in Step 3. |

## Troubleshooting Tips

If your new password is not accepted proceed to the "Recovering from a Lost or Misconfigured Passwords for Privileged EXEC Mode" section on page 15 for instructions on what to do next.

# Configuring Security Options with Passwords, Privilege Levels, and Usernames to Manage Access to CLI Sessions and CLI Commands

The tasks in this section describe how to configure your networking device to permit the use of a subset of privileged EXEC mode commands by users who should not have access to all of the commands that are available in privileged EXEC mode.

These tasks are beneficial for companies that have multiple levels of network support staff and the company wants the staff at each level to have access to a different subset of the privileged EXEC mode commands.

In this task the users who should not have access to all of the commands that are available in privileged EXEC mode are referred to as the first-line technical support staff.

This section contains the following procedures:


- Configuring the Networking Device for the First-Line Technical Support Staff, page 25
- Verifying the Configuration for the First-Line Technical Support Staff, page 27
- Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff, page 29


## Configuring the Networking Device for the First-Line Technical Support Staff

This task describes how to configure the networking device for first-line technical support users. First-line technical support staff are usually not allowed to run all of the commands available in privileged EXEC mode (privilege level 15) on a networking device. They are prevented from running commands that they are not authorized for by not being granted access to the password assigned to privileged EXEC mode or to other roles that have been configured on the networking device.

The **privilege** command is used to move commands from one privilege level to another in order to create the additional levels of administration of a networking device that is required by companies that have different levels of network support staff with different skill levels.

The default configuration of a Cisco IOS device permits two types of users to access the CLI. The first type of user is allowed to access only user EXEC mode. The second type of user is allowed access to privileged EXEC mode. A user who is allowed to access only user EXEC mode is not allowed to view or change the configuration of the networking device, or to make any changes to the operational status of the networking device. However, a user who is allowed access to privileged EXEC mode can make any change to a networking device that is allowed by the CLI.

In this task the two commands that normally run at privilege level 15 are reset to privilege level 7 using the **privilege** command so that first-line technical support users will be allowed to run the two commands. The two commands for which the privilege levels will be reset are the **clear counters** command and **reload** command.

- The **clear counters** command is used to reset the counter fields on interfaces for statistics such as packets received, packets transmitted, and errors. When a first-line technical support user is troubleshooting an interface-related connectivity issue between networking devices, or with remote users connecting to the network, it is useful to reset the interface statistics to zero and then monitor the interfaces for a period of time to see if the values in the interface statistics counters change.
- The **reload** command is used initiate a reboot sequence for the networking device. One common use of the reload command by the first-line technical support staff is to cause the networking device to reboot during a maintenance window so that it loads a new operating system that was previously copied onto the networking device's file system by a user with a higher level of authority.

Any user that is permitted to know the **enable secret** password that is assigned to the first-line technical support user role privilege level can access the networking device as a first-line technical support user. You can add a level of security by configuring a username on the networking device and requiring that the users know the username and the password. Configuring a username as an additional level of security is described in the "Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff" section on page 29.

Before Cisco IOS Releases 12.0(22)S and 12.2(13)T, each command in a privilege level had to be specified with a separate **privilege** command. In Cisco IOS Releases 12.0(22)S, 12.2(13)T, and later releases, a "wildcard" option specified by the new keyword **all** was introduced that allows you to configure access to multiple commands with only one **privilege** command. By using the new **all** keyword, you can specify a privilege level for all commands which begin with the string you enter. In other words, the **all** keyword allows you to grant access to all command-line options and suboptions for a specified command.

For example, if you wanted to create a privilege level to allow users to configure all commands which begin with **service-module t1** (such as **service-module t1 linecode** or **service-module t1 clock source**) you can use the **privilege interface all level 2 service-module t1** command instead of having to specify each **service-module t1** command separately.

If the command specified in the **privilege** command (used with the **all** keyword) enables a configuration submode, all commands in the submode of that command will also be set to the specified privilege level.

## Restrictions

The **all** "wildcard" keyword option for the **privilege** command is not supported in versions of Cisco IOS software prior to Cisco IOS Releases 12.0(22)S and, 12.2(13)T.

You must not have the **aaa new-model** command enabled on the networking device. You must not have the **login local** command configured for the local CLI sessions over the console port or the remote CLI sessions.

**Note** For clarity, only the arguments and keywords that are relevant for each step are shown in the syntax for the steps in this task. See the Cisco IOS command reference book for your Cisco IOS release for further information on the additional arguments and keywords that can be used with these commands.

**Caution** Do not use the **no** form of the **privilege** command to reset the privilege level of a command to its default because it might not return the configuration to the correct default state. Use the **reset** keyword for the **privilege** command instead to return a command to its default privilege level. For example, to remove the **privilege exec level** *reload* command from the configuration and return the **reload** command to its default privilege of 15, use the **privilege exec reset** *reload* command.

## SUMMARY STEPS

1. **enable** *password*
2. **configure terminal**
3. **enable secret level** *level password*
4. **privilege exec level** *level command-string*
5. **privilege exec all level** *level command-string*
6. **end**

### DETAILED STEPS

**Step 1** **enable** *password*

Enters privileged EXEC mode. Enter the password when prompted.

```
Router> enable
```

**Step 2** **configure terminal**

Enters global configuration mode.

```
Router# configure terminal
```

**Step 3** **enable secret level** *level password*

Configures a new enable secret password for privileged EXEC mode.

```
Router(config)# enable secret level 7 Zy72sKj
```

**Step 4** **privilege exec level** *level command-string*

Changes the privilege level of the **clear counters** command from one privilege level to another.

```
Router(config)# privilege exec level 7 clear counters
```

**Step 5** **privilege exec all level** *level command-string*

Changes the privilege level of the **reload** command from one privilege level to another.

```
Router(config)# privilege exec all level 7 reload
```

**Step 6** **end**

Exits global configuration mode.

```
Router(config)# end
```

## Verifying the Configuration for the First-Line Technical Support Staff

This task describes how to verify that the network device is configured correctly for the first-line technical support staff.

### Prerequisites

The following commands must have been modified to run at privilege level 7 for this task:

- **clear counters**
- **reload**

### SUMMARY STEPS

1. **enable** *level password*
2. **show privilege**
3. **clear counters**
4. **clear ip route ***
5. **reload in** *time*
6. **reload cancel**

7. **disable**
8. **show privilege**

## DETAILED STEPS

**Step 1** **enable** *level password*

Logs the user in into the networking device at the privilege level specified for the *level* argument.

```
Router> enable 7 Zy72sKj
```

**Step 2** **show privilege**

Displays the privilege level of the current CLI session.

```
Router# show privilege
Current privilege level is 7
```

**Step 3** **clear counters**

Clears the interface counters.

```
Router# clear counters
Clear "show interface" counters on all interfaces [confirm]
Router#
02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

**Step 4** **clear ip route ***

The **clear ip route** command should not be allowed because it was never changed from the default privilege 15 to the privilege level 7.

```
Router# clear ip route *
          ^
% Invalid input detected at '^' marker.

Router#
```

**Step 5** **reload in** *time*

Causes the networking device to reboot.

```
Router# reload in 10
Reload scheduled in 10 minutes by console
Proceed with reload? [confirm]
Router#


***
*** --- SHUTDOWN in 0:10:00 ---
***

02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20
```

**Step 6** **reload cancel**

The **reload cancel** command terminates a reload that was previously set up with the **reload in** *time* command.

```
Router# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***
```

```
04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED:  Scheduled reload cancelled at 15:38:46 PST
Sun Mar 27 2005
```

**Step 7** **disable**

Exits the current privilege level and returns to privilege level 1.

```
Router# disable
```

**Step 8** **show privilege**

Displays the privilege level of the current CLI session.

```
Router> show privilege

Current privilege level is 1
```

### Troubleshooting Tips

If your configuration does not work the way that you want it to and you want to remove the privilege commands from the configuration, use the **reset** keyword for the **privilege** command to return the commands to their default privilege level. For example, to remove the command **privilege exec level** *reload* command from the configuration and return the **reload** command to its default privilege of 15 use the **privilege exec reset** *reload* command.

## Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff

This task configures the networking device to require that the first-line technical support staff log in to the networking device with a login name of admin. The admin username configured in this task is assigned the privilege level of 7, which will allow users who log in with this name to run the commands that were reassigned to privilege level 7 in the "Configuring the Networking Device for the First-Line Technical Support Staff" task. When a user successfully logs in with the admin username, the CLI session will automatically enter privilege level 7.

Before Cisco IOS Releases 12.0(18)S and 12.2(8)T, two types of passwords were associated with usernames: Type 0, which is a clear text password visible to any user who has access to privileged mode on the router, and type 7, which has a password encrypted by the **service password encryption** command.

In Cisco IOS Releases 12.0(18)S, 12.2(8)T, and later releases, the new **secret** keyword for the **username** command allows you to configure MD5 encryption for username passwords.

### Prerequisites

The following commands must have been modified to run at privilege level 7 for this task:

- **clear counters**
- **reload**

See the "Configuring the Networking Device for the First-Line Technical Support Staff" section on page 25 for instructions on how to change the privilege level for a command.

### Restrictions

MD5 encryption for the **username** command is not supported in versions of Cisco IOS software prior to Cisco IOS Releases 12.0(18)S and 12.2(8)T.

You must not have the **aaa-new model** command enabled on the networking device. You must not have the **login local** command configured for the local CLI sessions over the console port or the remote CLI sessions.

**Note** For clarity, only the arguments and keywords that are relevant for each step are shown in the syntax for the steps in this task. Refer to the Cisco IOS command reference book for your Cisco IOS release for further information on the additional arguments and keywords that can be used with these commands.

### SUMMARY STEPS

1. **enable** *password*
2. **configure terminal**
3. **username** *username* **privilege** *level* **secret** *password*
4. **end**
5. **disable**
6. **login**
7. **show privilege**
8. **clear counters**
9. **clear ip route ***
10. **reload in** *time*
11. **reload cancel**
12. **disable**
13. **show privilege**

### DETAILED STEPS

**Step 1** **enable** *password*

Enters privileged EXEC mode. Enter the password when prompted.

```
Router> enable
```

**Step 2** **configure terminal**

Enters global configuration mode.

```
Router# configure terminal
```

**Step 3** **username** *username* **privilege** *level* **secret** *password*

Creates a username and applies MD5 encryption to the *password* text string.

```
Router(config)# username admin privilege 7 secret Kd65xZa
```

**Step 4** **end**

Exits global configuration mode.

```
Router(config)# end
```

**Step 5** **disable**

Exits the current privilege level and returns to user EXEC mode.

```
Router# disable
```

**Step 6** **login**

Logs in the user. Enter the username and password you configured in Step 3 when prompted.

```
Router# login
```

**Step 7** **show privilege**

The **show privilege** command displays the privilege level of the CLI session.

```
Router# show privilege

Current privilege level is 7
```

**Step 8** **clear counters**

The **clear counters** command clears the interface counters.

```
Router# clear counters

Clear "show interface" counters on all interfaces [confirm]
Router#
02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

**Step 9** **clear ip route ***

The **clear ip route** command is not allowed because because it was never changed from the default privilege 15 to the privilege level 7.

```
Router# clear ip route *
         ^
% Invalid input detected at '^' marker.

Router#
```

**Step 10** **reload in** *time*

The reload command causes the networking device to reboot.

```
Router# reload in 10
Reload scheduled in 10 minutes by console
Proceed with reload? [confirm]
Router#


***
*** --- SHUTDOWN in 0:10:00 ---
***

02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20
```

**Step 11** **reload cancel**

Terminates a reload that was previously set up with the **reload in** *time* command.

```
Router# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***
```

```
04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED:  Scheduled reload cancelled at 15:38:46 PST
Sun Mar 27 2005
```

**Step 12** **disable**

Exits the current privilege level and returns to user EXEC mode.

```
Router# disable
```

**Step 13** **show privilege**

Displays the privilege level of the current CLI session.

```
Router> show privilege

Current privilege level is 1
```

# Configuration Examples for Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices



## Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to Clear Remote CLI Sessions

The following example shows how to configure a networking device to allow a nonadministrative user to clear remote CLI session vty lines.

The first section is an excerpt of the running configuration for this example. The following sections show you how this example is used.

The following section is an excerpt of the running configuration:

```
!
privilege exec level 7 clear line
!
no aaa new-model
!
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege exec level 7 clear line
!
! the privilege exec level 7 clear command below is entered automatically
! when you enter the privilege exec level 7 clear line command above, do
! not enter it again
```

```
!
privilege exec level 7 clear
!
```

The following section using the **login** command shows the user logging in to the networking device with the username of admin:

```
Router> login
Username: admin
Password:
```

The following section using the **show privilege** command shows that the current privilege level is 7:

```
Router# show privilege
Current privilege level is 7
Router#
```

The following section using the **show user** command shows that two users (admin and root) are currently logged in to the networking device:

```
Router# show user

    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
   2 vty 0     root       idle                 00:00:17 172.16.6.2

  Interface    User               Mode         Idle     Peer Address
```

The following section using the **clear line** command terminates the remote CLI session in use by the username root:

```
Router# clear line 2
[confirm]
 [OK]
```

The following section using the **show user** command shows that admin is the only user logged in to the networking device:

```
Router# show user

    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
```

# Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to View the Running Configuration Automatically

The following example shows how to configure a networking device to allow a nonadministrative users (no access to privileged EXEC mode) to view the running configuration automatically. This example requires that the username is configured for privilege level 15 because many of the commands in the configuration file can be viewed only by users who have access to privilege level 15.

The solution is to temporarily allow the user access to privilege level 15 while running the **show running-config** command and then terminating the CLI session when the configuration file has been viewed. In this example the networking device will automatically terminate the CLI session when the end of the configuration file has been viewed. No further configuration steps are required.

**Caution** You must include the **noescape** keyword for the **username** command to prevent the user from entering an escape character that will terminate viewing the configuration file and leave the session running at privilege level 15.

```
!
!
username viewconf privilege 15 noescape secret 5 $1$zA9C$TDWD/Q0zwp/5xRwRqdgc/.
username viewconf autocommand show running-config
!
```

# Example: Configuring and Verifying a Networking Device to Allow Nonadministrative Users to Shut Down and Enable Interfaces

The following example shows how to configure a networking device to allow nonadministrative users to shut down and enable interfaces.

The first section is an excerpt of the running configuration for this example. The following sections show you how this example is used.

The following section is an excerpt of the running configuration:

```
!
no aaa new-model
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege interface all level 7 shutdown
privilege interface all level 7 no shutdown
privilege configure level 7 interface
privilege exec level 7 configure terminal
!
! the privilege exec level 7 configure command below is entered automatically
! when you enter the privilege exec level 7 configure terminal command above, do
! not enter it again
!
privilege exec level 7 configure
!
```

The following section using the **login** command shows the user logging in to the networking device with the username of admin:

```
Router> login
Username: admin
Password:
```

The following section using the **show privilege** command shows that the current privilege level is 7:

```
Router# show privilege
Current privilege level is 7
```

The following section using the **show user** command shows that admin is the only user logged in to the networking device:

```
Router# show user
```

```
    Line       User       Host(s)              Idle       Location
*   0 con 0    admin      idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
```

The following section shows that the admin user is permitted to shut down and enable an interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 1/0
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router#
```

# Where to Go Next

Once you have established a baseline of security for your networking devices you can consider more advanced options such as:

- Role-based CLI access—The role-based CLI access feature offers a more comprehensive set of options than the **privilege** command (described in this document) for network managers who want to allow different levels of technical support staff to have different levels of access to CLI commands.
- AAA security—Many Cisco networking devices offer an advanced level of security using AAAfeatures. All of the tasks described in this document, and other—more advanced security features—can be implemented using AAA on the networking device in conjunction with a remote TACACS+ or RADIUS server. For information how to configure AAA security features that can be run locally on a networking device, or for information on how to configure remote AAA security using TACACS+ or RADIUS servers, see the *Cisco IOS Security Configuration Guide: Securing User Services, Cisco IOS Release 15.1M&T*.

# Additional References

## Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | *Cisco IOS Master Commands List, All Releases* |
| Security commands | *Cisco IOS Security Command Reference* |
| Managing user access to CLI commands and configuration information | *Role-Based CLI Access* |
| Configuring MD5 secure neighbor authentication for protocols such as OSPF and BGP | *Neighbor Router Authentication: Overview and Guidelines* |
| Assigning privilege levels with TACACS+ and RADIUS | *How to Assign Privilege Levels with TACACS+ and RADIUS* |

## Standards

| Standard | Title |
|---|---|
| No new or modified RFCs are supported by this functionality, and support for existing RFCs has not been modified. | — |

## MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

## RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported by this functionality, and support for existing RFCs has not been modified. | — |

# Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Note** Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

*Table 1 Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| Enhanced Password Security | 12.0(18)S<br>12.2(8)T | Using the Enhanced Password Security feature, you can configure MD5 encryption for username passwords. MD5 encryption is a one-way hash function that makes reversal of an encrypted password impossible, providing strong encryption protection. Using MD5 encryption, you cannot retrieve clear text passwords. MD5 encrypted passwords cannot be used with protocols that require that the clear text password be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).<br>The following sections provide information about this feature:<br>• Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff, page 29<br>• Configuring the Enable Secret Password, page 23 |

*Table 1 Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices (continued)*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| Privilege Command Enhancement | 12.0(22)S<br>12.2(13)T | The **all** keyword was added to the **privilege** command as a wild card to reduce the number of times that the **privilege** command is entered when you are changing the privilege level of several keywords for the same command.<br>The following sections provide information about this feature:<br>• Before Cisco IOS Releases 12.0(22)S and 12.2(13)T, each command in a privilege level had to be specified with a separate privilege command. In Cisco IOS Releases 12.0(22)S, 12.2(13)T, and later releases, a "wildcard" option specified by the new keyword all was introduced that allows you to configure access to multiple commands with only one privilege command. By using the new all keyword, you can specify a privilege level for all commands which begin with the string you enter. In other words, the all keyword allows you to grant access to all command-line options and suboptions for a specified command., page 26 |
| Product Security Baseline: Password Encryption and Complexity Restrictions | 15.0(1)S | This feature enforces restrictions on creating passwords used in a AAA context that includes passwords created through the **username** command and passwords created to download authorization data.<br>The following sections provides information about this feature:<br>• Product Security Baseline: Password Encryption and Complexity Restrictions, page 12<br>The following commands were introduced or modified: **aaa password restriction**, **enable secret**, **username secret**. |