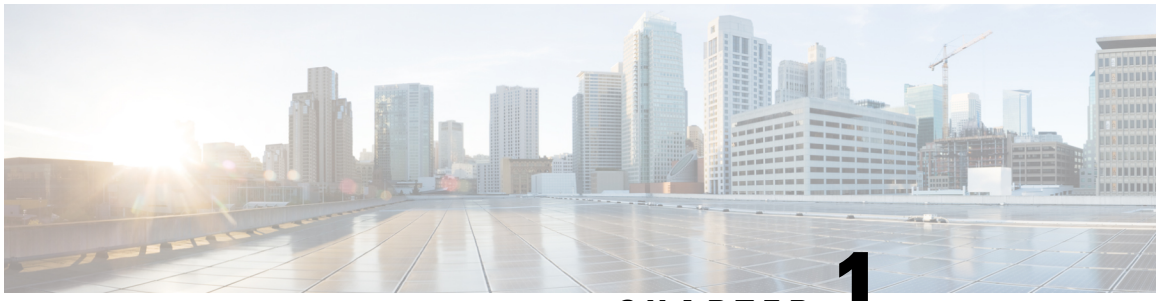
User Security Configuration Guide, Cisco IOS XE Fuji 16.9.x

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

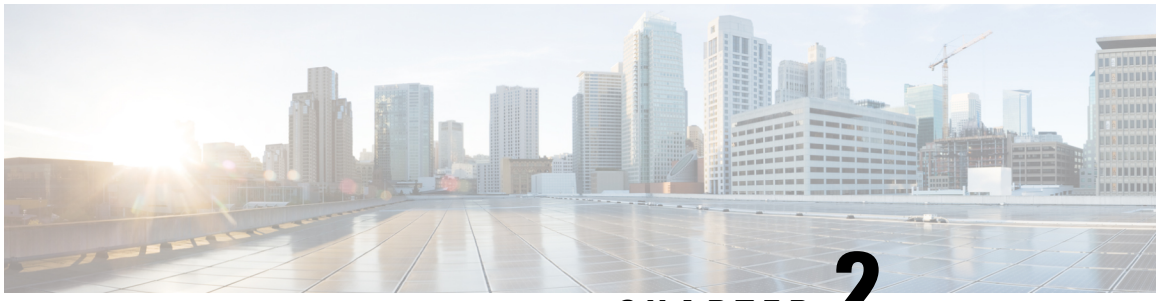
Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the . RSS feeds are a free service.



CHAPTER 2

Cisco IOS Login Enhancements-Login Block

The Cisco IOS Login Enhancements (Login Block) feature allows users to enhance the security of a router by configuring options to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected.

The login block and login delay options introduced by this feature can be configured for Telnet or SSH virtual connections. By enabling this feature, you can slow down “dictionary attacks” by enforcing a “quiet period” if multiple failed connection attempts are detected, thereby protecting the routing device from a type of denial-of-service attack.

Note Whenever you want to use the AAA "quiet-mode" feature, you have to configure the aaa new-model using the **aaa new-model** command.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Information About Cisco IOS Login Enhancements

Protecting Against Denial of Service and Dictionary Login Attacks

Connecting to a routing device for the purposes of administering (managing) the device, at either the User or Executive level, is most frequently performed using Telnet or SSH (secure shell) from a remote console (such as a PC). SSH provides a more secure connection option because communication traffic between the user's device and the managed device are encrypted. The Login Block capability, when enabled, applies to both Telnet connections and SSH connections.

The automated activation and logging of the Login Block and Quiet Period capabilities introduced by this feature are designed to further enhance the security of your devices by specifically addressing two well known methods that individuals use to attempt to disrupt or compromise networked devices.

If the connection address of a device is discovered and is reachable, a malicious user may attempt to interfere with the normal operations of the device by flooding it with connection requests. This type of attack is referred to as an attempted Denial-of-Service, because it is possible that the device may become too busy trying to process the repeated login connection attempts to properly handle normal routing services or will not be able to provide the normal login service to legitimate system administrators.

The primary intention of a dictionary attack, unlike a typical DoS attack, is to actually gain administrative access to the device. A dictionary attack is an automated process to attempt to login by attempting thousands, or even millions, of username/password combinations. (This type of attack is called a "dictionary attack" because it typically uses, as a start, every word found in a typical dictionary as a possible password.) As scripts or programs are used to attempt this access, the profile for such attempts is typically the same as for DoS attempts; multiple login attempts in a short period of time.

By enabling a detection profile, the routing device can be configured to react to repeated failed login attempts by refusing further connection request (login blocking). This block can be configured for a period of time, called a "quiet period". Legitimate connection attempts can still be permitted during a quiet period by configuring an access-list (ACL) with the addresses that you know to be associated with system administrators.

Login Enhancements Functionality Overview

Delays Between Successive Login Attempts

A Cisco device can accept virtual connections as fast as they can be processed. Introducing a delay between login attempts helps to protect the Cisco device against malicious login connections such as dictionary attacks and DoS attacks. Delays can be enabled in one of the following ways:

- Via the **auto secure** command. If you enable the AutoSecure feature, the default login delay time of one second is automatically enforced.
- Via the **login block-for** command. You must enter this command before issuing the **login delay** command. If you enter only the **login block-for** command, the default login delay time of one second is automatically enforced.
- Via the new global configuration mode command, **login delay**, which allows you to specify a the login delay time to be enforced, in seconds.

Login Shutdown If DoS Attacks Are Suspected

If the configured number of connection attempts fail within a specified time period, the Cisco device will not accept any additional connections for a "quiet period." (Hosts that are permitted by a predefined access-control list [ACL] are excluded from the quiet period.)

The number of failed connection attempts that trigger the quiet period can be specified via the new global configuration mode command **login block-for**. The predefined ACL that is excluded from the quiet period can be specified via the new global configuration mode command **login quiet-mode access-class**.

This functionality is disabled by default, and it is not enabled if autosecure if enabled.

How to Configure Cisco IOS Login Enhancements

Configuring Login Parameters

Use this task to configure your Cisco device for login parameters that help detect suspected DoS attacks and slow down dictionary attacks.

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of one second
- All login attempts made via Telnet or SSH are denied during the quiet period; that is, no ACLs are exempt from the login period until the **login quiet-mode access-class** command is issued.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
5. **login quiet-mode access-class** {*acl-name* | *acl-number*}
6. **login delay** *seconds*

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**login block-for** *seconds* **attempts** *tries* **within** *seconds* **Example:** `Router(config)# login block-for 100 attempts 2 within 100`	Configures your Cisco IOS XE device for login parameters that help provide DoS detection. **Note** This command must be issued before any other login command can be used.

Step 5	**login quiet-mode access-class** {*acl-name* | *acl-number*}
	Example:
	`Router(config)# login quiet-mode access-class myacl`
		(Optional) Although this command is optional, it is recommended that it be configured to specify an ACL that is to be applied to the router when the router switches to quiet mode. When the router is in quiet mode, all login requests are deniedand the only available connection is through the console.
		If this command is not configured, then the default ACL **sl_def_acl** is created on the router. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.
		For example:
		`Router#show access-lists sl_def_acl`
		`Extended IP access list sl_def_acl`
		`10 deny tcp any any eq telnet`
		`20 deny tcp any any eq www`
		`30 deny tcp any any eq 22`
		`40 permit ip any any`

Step 6	**login delay** *seconds* **Example:** `Router(config)# login delay 10`	(Optional) Configures a delay between successive login attempts.

What to Do Next

After you have configured login parameters on your router, you may wish to verify the settings. To complete this task, see the following section "Verifying Login Parameters, on page 7."

Verifying Login Parameters

Use this task to verify the applied login configuration and present login status on your router.

SUMMARY STEPS

1. **enable**
2. **show login failures**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show login failures** **Example:** `Router# show login`	Displays login parameters. • **failures** --Displays information related only to failed login attempts.

Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Router# show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for**command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; five login requests have already failed.

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100
 seconds.
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

The following sample output from **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures
Information about login failure's with the device
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Router# show login failures
*** No logged failed login attempts with the device.***
```

Configuration Examples for Login Parameters

Setting Login Parameters Example

The following example shows how to configure your router to enter a 100 second quiet period if 15 failed login attempts is exceeded within 100 seconds; all login requests will be denied during the quiet period except hosts from the ACL “myacl.”

```
Router(config)# aaa new-model
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class myacl
```

Additional References

Related Documents

Related Topic	Document Title
Configuring autosecure	AutoSecure feature module.
Security commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*
Secure Management/Administrative Access	Role-Based CLI Access feature module.

Standards

Standards	Title
None.	--

MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

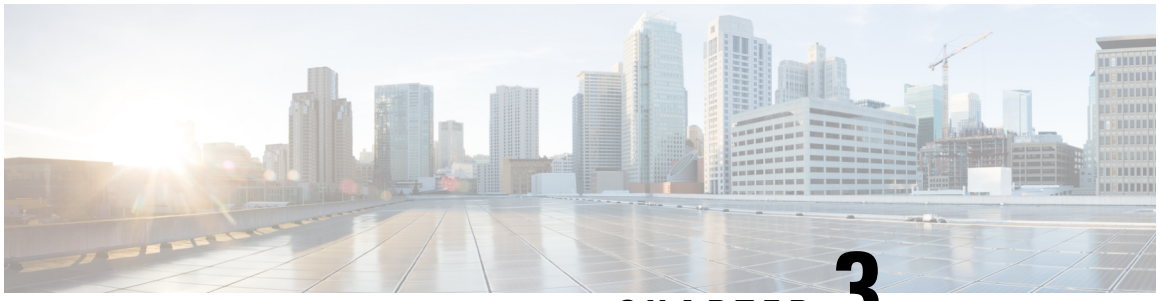
Feature Information for Cisco IOS Login Enhancements-Login Block

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 1: Feature Information for Cisco IOS Login Enhancements (Login Block)

Feature Name	Releases	Feature Configuration Information
Cisco IOS Login Enhancements	Cisco IOS XE Release 2.1	The Cisco IOS Login Enhancements (Login Block) feature allows users to enhance the security of a router by configuring options to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Service Aggregation Routers. The following commands were modified by this feature: **login block-for**, **login delay**, **login quiet-mode access-class**, **show login**.



CHAPTER 3

Configuring Security with Passwords, Privileges, and Logins

Cisco IOS based networking devices provide several features that can be used to implement basic security for CLI 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 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 the 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 caveats and feature information, see Bug Search Tool and 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 table.

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

Restrictions for Configuring Security with Passwords, Privileges, and Logins

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 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 *Securing User Services Configuration Guide Library*.

Restrictions and Guidelines for Reversible Password Types

- 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.

Restrictions and Guidelines for Irreversible Password Types

- Password type 5 is deprecated. Password type 5 must be migrated to stronger password type 8 or type 9.
- For username secret password type 5 and for enable secret password type 5, migrate to type 8 or type 9.

Information About Configuring Security with Passwords, Privileges, and Logins

Benefits of Creating a Security Scheme

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 Cisco IOS XE features described in this document can be combined in many different ways to create a unique security scheme for each of your networking devices. Here are some possible examples that you can configure:

- You can enable non administrative users to run a subset of the administrative commands available on the networking device by lowering the entitlement level for the commands to the non administrative 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 customer whose connection has stopped passing traffic. See the Example: Configuring a Device to Allow Users to Shutdown and Enable Interfaces, on page 46 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 a Device to Allow Users to Clear Remote Sessions, on page 44 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 a Device to Allow Users to View the Running Configuration, on page 45 section for an example of how to do this.

Cisco IOS XE CLI Modes

To aid in the configuration of Cisco devices, the Cisco IOS XE command-line interface 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 depend on the mode you are in. Entering a question mark(**?**) at the system prompt (device 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 XE software based networking device only allows you to configure passwords to protect access 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. As an example, this chapter describes the *subinterface configuration mode* , 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. ROMMON is not covered in this document because it does not have any security features available in it.

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 log-in process will require a username and a password. You may try three times to enter a password before 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. When you are logged into a networking device in user EXEC mode your session is running at privilege level 1. By default the EXEC commands at privilege level 1 are a subset of those available at privilege level 15. When you are logged into 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.

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, use the following command:

Command	Purpose
`Device(config)#` **?**	Lists the user EXEC mode commands

The user EXEC mode prompt consists of the host name of the device followed by an angle bracket (>), as shown in the following example:

```
Device>
```

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

Note Examples in Cisco IOS XE documentation assume the use of the default name of "Device." Different devices (for example, access servers) may use a different default name. If the 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.

To list the commands available in user EXEC mode, enter a question mark (**?**) as shown in the following example:

```
Device> ?

Exec commands:
 <1-99>           Session number to resume
 connect          Open a terminal connection
 disconnect       Disconnect an existing telnet session
 enable           Turn on privileged commands
```

```
exit             Exit from Exec mode
help             Description of the interactive help system
lat              Open a lat connection
lock             Lock the terminal
login            Log in as a particular user
logout           Exit from Exec mode and log out
menu             Start a menu-based user interface
mbranch          Trace multicast route for branch of tree
mrbranch         Trace reverse multicast route to branch of tree
mtrace           Trace multicast route to group
name-connection  Name an existing telnet connection
pad              Open a X.29 PAD connection
ping             Send echo messages
resume           Resume an active telnet connection
show             Show running system information
systat           Display information about terminal lines
telnet           Open a telnet connection
terminal         Set terminal line parameters
tn3270           Open a tn3270 connection
trace            Trace route to destination
where            List active telnet connections
x3               Set X.3 parameters on PAD
```

The list of commands will vary depending on the software feature set and platform you are using.

Note You can enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive. However, Cisco IOS XE 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, on page 14. When you are logged into a networking device in privileged EXEC mode your session is running at privilege level 15. When you are logged into a networking device in user EXEC mode your session is running at privilege level 1. 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 XE Privilege Levels, on page 22 for more information on privilege levels and the **privilege** command.

The privileged EXEC mode prompt consists of the host name of the device followed by a pound sign(#), as shown in the following example:

```
Device#
```

To access privileged EXEC mode, use the following command:

Command	Purpose

`Device> enable`
`Password`
`Device# exit`
`Device>`
	Enables privileged EXEC mode.
	• 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 a telnet 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, on page 19. The system administrator uses the **enable secret** or **enable password**global configuration commands 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, on page 28.

To return to user EXEC mode, use the following command:

Command	Purpose
`Device# disable`	Exits from privileged EXEC mode to user EXEC mode.

The following example shows the process of accessing privileged EXEC mode:

```
Device> enable
Password:<letmein>
Device#
```

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 the **?** command 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 XE 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 following command in privileged EXEC mode:

Command	Purpose
`Device# configure terminal`	From privileged EXEC mode, enters global configuration mode.

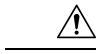
The following example shows the process of entering global configuration mode from privileged EXEC mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
```

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 host-name of the device followed by (config) and the pound sign (#). To list the commands available in privileged EXEC mode, issue the **?** command 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. This behavior is explained in more detail later in this document.

As shown in the example above, the system dialogue 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, 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 one of the following commands:

Command	Purpose

`Device(config)# end`
or
`Device(config)# ^Z`
	Ends the current configuration session and returns to privileged EXEC mode.

`Device(config)# exit`	Exits the current command mode and returns to the preceding mode. For example, exits from global configuration mode to privileged EXEC mode.

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 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 Release 12.2 *Cisco IOS Interface Configuration Guide* . For protocol-specific commands, refer to the appropriate Cisco IOS XE software command reference.

To access and list the interface configuration commands, use the following command:

Command	Purpose
`Device(config)# interface type number`	Specifies the interface to be configured, and enters interface configuration mode.

In the following example, the user enters interface configuration mode for serial interface 0. The new prompt, *hostname* (config-if)#, indicates interface configuration mode.

```
Device(config)# interface serial 0
Device(config-if)#
```

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 XE software documentation set.

To access subinterface configuration mode, use the following command in interface configuration mode:

Command	Purpose
`Device(config-if)# interface type number`	Specifies the virtual interface to be configured and enters subinterface configuration mode.

In the following example, a subinterface is configured for serial line 2, which is configured for Frame Relay encapsulation. The subinterface is identified as "2.1" to indicate that it is subinterface 1 of serial interface 2. The new prompt *hostname* (config-subif)# indicates subinterface configuration mode. The subinterface can be configured to support one or more Frame Relay PVCs.

```
Device(config)# interface serial 2
Device(config-if)# encapsulation frame-relay
Device(config-if)# interface serial 2.1
Device(config-subif)#
```

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 XE CLI Sessions

Local CLI Sessions

Local CLI sessions require direct access to the the console port of the networking device. Local CLI sessions start in user EXEC mode. See the Cisco IOS XE CLI Modes, on page 13 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 are dependant on the type of networking device that you are configuring. See to 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 Secure Shell (SSH). Local CLI sessions start in user EXEC mode. See the Cisco IOS XE CLI Modes, on page 13 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 ROM Monitor Mode.

This document explains how to configure security for remote Telnet sessions. 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 are 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.

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# password password-string
```

Remote CLI sessions use lines that are referred to virtual teletypewriter (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.

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config-line)# password password-string
```

Protect Access to Cisco IOS XE EXEC Modes

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

Protecting 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 protect access to user EXEC mode for local CLI sessions by configuring a password on the console port. See the Configuring and Verifying a Password for Local CLI Sessions, on page 26.

You protect access to user EXEC mode for remote CLI sessions by configuring a password on the virtual terminal lines (VTYs). See the Configuring and Verifying a Password for Remote CLI Sessions, on page 24 for instructions on how to configure passwords for remote CLI sessions.

Protecting 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 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**.

Command	Purpose

enable
 	
`Device> enable`
 	
`Password`
 	
`Device#`
	Enables privileged EXEC mode.
	• Enter your password if prompted. The password will not be shown in the terminal window.
	• The ">" at the end of the prompt string is changed to a "#" to indicate that you are in privileged EXEC mode.

Cisco IOS XE 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 password when it is configured with the **enable password** *password* command
- Authentication key chain passwords used by RIPv2 and EIGRP
- BGP passwords for authenticating BGP neighbors
- OSPF authentication keys for authenticating OSPF neighbors
- ISIS passwords for authenticating ISIS neighbors

This 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 willow
!
interface Ethernet1/0.1
 ip address 172.16.6.1 255.255.255.0
 ip router isis
 ip rip authentication key-chain trees
 ip authentication key-chain eigrp 1 trees
 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 only a minimal level of security because the encryption algorithm used by the **service password-encryption** command to encrypt passwords creates text strings that 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, on page 30 for more information on encrypting clear text passwords in configuration files.

Many of the Cisco IOS XE features that use clear text passwords can also be configured to use the more secure MD5 algorithm. 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. The number 5 in the configuration excerpt below indicates that the enable secret password has been encrypted using the MD5 algorithm.

enable secret 5 1fGCS$rkYbR6.Z8xo4qCl3vghWQ0

The number 7 in the excerpt below indicates that the enable password has been encrypted using the less secure algorithm used by the **service password-encryption** command.

!

enable password 7 00081204

Cisco IOS XE 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:

See the *Cisco IOS Security Command Reference* . (http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html) for more information on how to configure the **username** command.

Cisco IOS XE Privilege Levels

The default configuration for Cisco IOS XE 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 a Device to Allow Users to Shutdown and Enable Interfaces, on page 46 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 will run 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 to help them 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 a Device to Allow Users to View the Running Configuration, on page 45 for an example of how to configure this option.

These command privileges can also be implemented when 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 or not 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 XE Password Configuration

Cisco IOS XE 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 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 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 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 configuring your username password, and the networking device requires that you log into 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 privilege 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 second CLI session technique described above, you can power cycle the networking device so that it returns to the previous passwords that are stored in the startup configuration.

How To Configure Security with Passwords Privileges and Logins

Protecting Access to User Exec Mode

Configuring and Verifying 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 XE 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 doesn't have a password configured for remote CLI sessions you will see a message that a password is required and has not been set. The remote CLI session will be terminated by the remote host.

Before you begin

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.

To perform the verification step (Step 6) for this task, your networking device must have an interface that is in an operational state. The interface must have a valid IP address.

Note 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**line vty** *line-number* [*ending-line-number*] **Example:** `Device(config)# line vty 0 4`	Enters line configuration mode.
Step 4	**password** *password* **Example:** `Device(config-line)# password H7x3U8`	The argument *password* is a character string that specifies the line password. The following rules apply to the *password* argument: • The first character cannot be a number. • The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. • Passwords are case sensitive.
Step 5	**end** **Example:** `Device(config-line)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 6	**telnet** *ip-address* **Example:** `Device# 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). • Enter the password that you configured is step 4 when prompted.

	Command or Action	Purpose
		Note This procedure is often referred to as a starting a recursive Telnet session because you are initiating a remote Telnet session with the networking device from the networking device itself.
Step 7	**exit** **Example:** `Device# exit`	Terminates the remote CLI session (recursive Telnet session) with the networking device.

Troubleshooting Tips

To display information for all users who have access to a lawful intercept view, issue the **show users lawful-intercept** command. (This command is available only to authorized lawful intercept view users.)

What to Do Next

Proceed to the Configuring and Verifying a Password for Local CLI Sessions, on page 26 .

Configuring and Verifying 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 configured the password correctly you should perform this task using a local CLI session using the console port.

Before you begin

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 is 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 0**
4. **password** *password*
5. **end**
6. **exit**
7. Press the Enter key.

DETAILED STEPS

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

What to Do Next

Proceed to the Protecting Access to Privileged EXEC Mode, on page 28.

Protecting Access to Privileged EXEC Mode

Configuring and Verifying 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** commandbecause it encrypts the password that you configure with it with strong encryption . For more information on password encryption issues see the Cisco IOS XE Password Encryption Levels, on page 21. For information on configuring the **enable secret**command see the Configuring and Verifying the Enable Secret Password, on page 31.

Note The networking device must not have a password configured by the **enable secret** command in order to perform this task successfully. If you have already configured a password for privileged EXEC mode using the **enable secret** command, 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** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**enable password** *password*
	Example:
	`Device(config)# enable password t6D77CdKq`
		The argument *password* is a character string that specifies the enable password. The following rules apply to the *password* argument:
		• Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
		• Must not have a number as the first character.
		• Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
		• 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:
		  • Enter abc
		  • Type Crtl-v
		  • Enter ?123

Step 4	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 5	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode.
Step 6	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter the password you configured in step 3.

Troubleshooting Tips

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

What to Do Next

Encrypt the clear text enable password in the configuration file of the networking device using the procedure described in Configuring Password Encryption for Clear Text Passwords, on page 30.

Configuring Password Encryption for Clear Text Passwords

Cisco IOS XE 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 XE Password Encryption Levels, on page 21 for more information.

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

Before you begin

You must have at least one feature that uses clear text passwords configured on your networking device for this 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** **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	**service password-encryption** **Example:** `Device(config)# service password-encryption`	Enables 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 Border Gateway Protocol neighbor passwords.
Step 4	**end** **Example:**	Exits the current configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	

Configuring and Verifying 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.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Perform one of the following steps:
   - **enable secret** *password*
   - **enable secret 5** *previously-encrypted-password*
4. **end**
5. **exit**
6. **enable**

DETAILED STEPS

	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	Perform one of the following steps: • **enable secret** *password* • **enable secret 5** *previously-encrypted-password* **Example:** `Device(config)# enable secret t6D77CdKq` **Example:**	The argument *password* is a character string that specifies the **enable secret** password. The following rules apply to the *password* argument: • Must contain from 1 to 25 uppercase and lowercase alphanumeric characters. • Must not have a number as the first character.

	Command or Action	Purpose

	`Device(config)# enable secret 5 $1$/x6H$RhnDI3yLC4GA01aJnHLQ4/`	• Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
		• 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:
		  • Enter abc
		  • Type Crtl-v
		  • Enter ?123
		or
		Sets a previously encrypted password for privileged EXEC mode by entering the number 5 before the previously encrypted string. 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** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 5	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode.
Step 6	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter the password that you configured in Step 3.

Troubleshooting Tips

If your new password is not accepted proceed to the Configuration Examples for Configuring Security with Passwords Privileges and Logins for instructions on what to do next.

What to Do Next

If you have finished configuring passwords for local and remote CLI sessions and you want to configure additional security features, such as usernames, and privilege levels proceed to the Configuring Security Options to Manage Access to CLI Sessions and Commands, on page 34.

Configuring a Device to Allow Users to View the Running Configuration

To access the running configuration of a device using the **show running-config** command at a privilege level lower than level 15, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **privilege exec all level** *level command-string*
4. **file privilege** *level*
5. **privilege configure all level** *level command-string*
6. **end**
7. **show privilege**
8. **show running-config**

DETAILED STEPS

	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 exec all level** *level command-string* **Example:** `Device(config)# privilege exec all level 5 show running-config`	Changes the privilege level of the specified command from one privilege level to another.
Step 4	**file privilege** *level* **Example:** `Device(config)# file privilege 5`	Allows a user of the privilege level to execute commands that involve the file system on a device.
Step 5	**privilege configure all level** *level command-string* **Example:** `Device(config)# privilege configure all level 5 logging`	Allows a user of a privilege level to see specific configuration commands. For example, allows the user of privilege level 5 to see the logging configuration commands in the running configuration.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**show privilege** **Example:**	Displays the current privilege level.

	Command or Action	Purpose
	`Device# show privilege`	
Step 8	**show running-config** **Example:** `Device# show running-config`	Displays the current running configuration for the specified privilege level.

Example

The following output for the **show running-config** command displays the logging configuration commands in the running configuration. Users with a privilege level below 15 can view the running configuration after configuring the **privilege configure all level** *level command-string* command.

```
Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

Configuring Security Options to Manage Access to CLI Sessions and 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 of the commands 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 of the commands 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

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 XE device permits two types of users to access the CLI. The first type of user is a person who is only allowed to access user EXEC mode. The second type of user is a person who is allowed access to privileged EXEC mode. A user who is only allowed to access 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. On the other hand, 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 in order 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 them 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 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 an additional 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 a Device to Require a Username for the First-Line Technical Support Staff, on page 39.

Note 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 synt steps in this task. See the Cisco IOS command reference book for your Cisco IOS release for further i 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 because it might not return the configuration to the correct default state. Use the **reset** keyword for th command instead to return a command to its default privilege level. For example, to remove the **p exec level** *reload* command from the configuration and return the **reload** command to its default p 15, use the **privilege exec reset** *reload* command.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. Enter the password when prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**enable secret level** *level password* **Example:** `Device(config)# enable secret level 7 Zy72sKj`	Configures a new enable secret password for privilege level 7.
Step 4	**privilege exec level** *level command-string* **Example:**	Changes the privilege level of the **clear counters** command from privilege level 15 to privilege level 7.

	Command or Action	Purpose
	`Device(config)# privilege exec level 7 clear counters`	
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

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.

Before you begin

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 into the networking device at the privilege level specified for the level argument.

Example:

```
Device> enable 7 Zy72sKj
```

Step 2 **show privilege**

Displays the privilege level of the current CLI session

Example:

```
Device# show privilege
```

```
Current privilege level is 7
```

Step 3 **clear counters**

The clear counters command clears the interface counters. This command has been changed from privilege level 15 to privilege level 7.

Example:

```
Device# clear counters

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

Step 4 **clear ip route ***

The *ip route* argument string for the **clear** command should not be allowed because it was not changed from privilege level 15 to privilege level 7.

Example:

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

Step 5 **reload in time**

The reload command causes the networking device to reboot.

Example:

```
Device# reload in

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

Device#

***
*** --- 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** terminates a reload that was previously setup with the the **reload in** *time* command.

Example:

```
Device# 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.

Example:

```
Device# disable
```

Step 8 **show privilege**

Displays the privilege level of the current CLI session

Example:

```
Device> 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.

What to Do Next

If you want to add an additional level of security by requiring that the first level technical staff use a login name, proceed to the Configuring a Device to Require a Username for the First-Line Technical Support Staff, on page 39.

Configuring a 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 login 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 previous task. When a user successfully logs in with the admin username, the CLI session will automatically enter privilege level 7.

Before Cisco IOS XE Release 2.3, 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 XE Release 2.3 and later releases, the new **secret** keyword for the **username** command allows you to configure Message Digest 5 (MD5) encryption for username passwords.

Before you begin

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, on page 34 for instructions on how to change the privilege level for a command.

Note MD5 encryption for the **username** command is not supported in versions of Cisco IOS software prior to Cisco IOS XE Release 2.3.

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 synt steps in this task. Refer to the Cisco IOS command reference book for your Cisco IOS XE release information on the additional arguments and keywords that can be used with these commands.

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**username** *username* **privilege** *level* **secret** *password* **Example:** `Device(config)# username admin privilege 7 secret Kd65xZa`	Creates a username and applies MD5 encryption to the *password* text string.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode.
Step 5	**disable** **Example:** `Device# disable`	Exits the current privilege level and returns to user EXEC mode.
Step 6	**login** *username* **Example:** `Device> login admin`	Logs in the user. Enter the username and password you configured in step 3 when prompted.

Step 7	**show privilege**
	Example:
	`Device# show privilege`
	`Current privilege level is 7`
		The **show privilege** command displays the privilege level of the CLI session.

Step 8	**clear counters**
	Example:
	`Device# clear counters`
	`Clear "show interface" counters on all interfaces [confirm]`
	`Device#`
	`02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console`
		The **clear counters** command clears the interface counters. This command has been changed from privilege level 15 to privilege level 7.

Step 9	**clear** *ip route* ***
	Example:
	`Device# clear ip route *`
	`^`
	`% Invalid input detected at '^' marker.`
		The *ip route* argument string for the **clear** command is not allowed because it was not changed from privilege level 15 to privilege level 7.

Step 10	**reload in** *time* **Example:**	The reload command causes the networking device to reboot.

	Command or Action	Purpose

	`Device# reload in`
	
	`10`
	`Reload scheduled in 10 minutes by console`
	`Proceed with reload? [confirm]`
	`Device#`
	`***`
	`*** --- 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**
	Example:
	
	`Device# reload cancel`
	
	`***`
	`*** --- SHUTDOWN ABORTED ---`
	`***`
	`04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST Sun Mar 27 2005`
		The **reload cancel** command terminates a reload that was previously setup with the the **reload in** *time* command.

Step 12	**disable** **Example:** `Device# disable`	Exits the current privilege level and returns to user EXEC mode.

Step 13	**show privilege**
	Example:
	
	`Device> show privilege`
	
	`Current privilege level is 1`
		Displays the privilege level of the current CLI session

Recovering from a Lost or Misconfigured Password for Local Sessions

There are three methods that can be used to recover from 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.

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 Configuring and Verifying a Password for Local CLI Sessions, on page 26. 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

- 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, to stop. You should only restart a networking device during a period of time that has been allocated for network maintenance.

Recovering from a Lost or Misconfigured Password for Remote Sessions

There are 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

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 Configuring and Verifying a Password for Remote CLI Sessions, on page 24. 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

- 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, to stop. You should only restart a networking device during a period of time that has been allocated for network maintenance.

Recovering from Lost or Misconfigured Passwords for Privileged EXEC Mode

There are two methods that 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

- 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, to stop. You should only restart a networking device during a period of time that has been allocated for network maintenance.

Configuration Examples for Configuring Security with Passwords Privileges and Logins

Example: Configuring a Device to Allow Users to Clear Remote Sessions

The following example shows how to configure a networking device to allow a non administrative user to clear remote CLI session virtual terminal (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:

```
R1> login
Username: admin
Password:
```

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

```
R1# show privilege

Current privilege level is 7
R1#
```

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

```
R1# 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** *2* command terminates the remote CLI session in use by the username root:

```
R1# clear line  2

[confirm]
 [OK]
```

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

```
R1# show user
    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

Example: Configuring a Device to Allow Users to View the Running Configuration

For Users With Privilege Level 15

The following example shows how to configure the networking device to allow a non administrative 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 end of 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
!
```

For Users With Privilege Level Lower Than Level 15

The following example shows how to configure a networking device to allow a user with privilege level lower than level 15 to view the running configuration.

```
Device> enable
Device# configure terminal
Device(config)# privilege exec all level 5 show running-config
Device(config)# file privilege 5
Device(config)# privilege configure all level 5 logging
Device(config)# end
Device# show privilege

Current privilege level is 5

Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

Example: Configuring a Device to Allow Users to Shutdown and Enable Interfaces

The following example shows how to configure a networking device to allow non administrative users to shutdown and enable interfaces.

The first section is an 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:

```
R1> login
Username: admin
Password:
```

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

```
R1# show privilege
Current privilege level is 7
```

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

```
R1# 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 shutdown and enable an interface:

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface ethernet 1/0
R1(config-if)# shutdown
R1(config-if)# no shutdown
R1(config-if)# exit
R1#
```

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 authentication, authorization and accounting (AAA) features. 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 XE Security Configuration Guide:Securing User Services* , Release 2.

Additional References

The following sections provide references related to Configuring Security with Passwords and, Login Usernames for CLI Sessions on Networking Devices.

Related Documents

Related Topic	Document Title
Managing user access to CLI commands and configuration information	"Role-Based CLI Access" in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
AAA Security Features	*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
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 IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: 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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

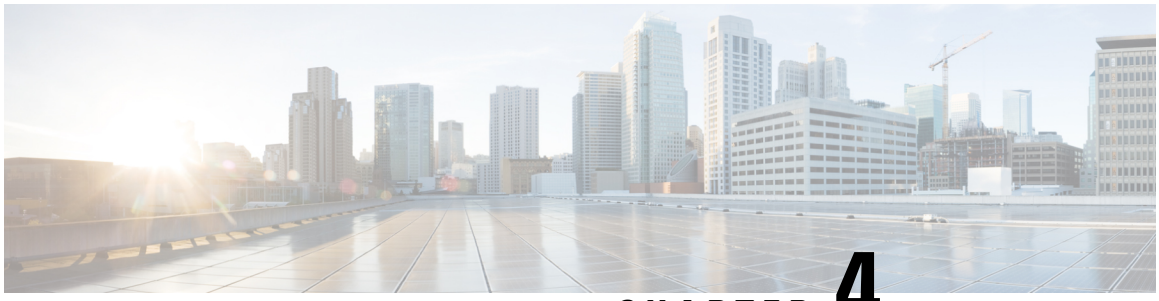
Feature Information for Configuring Security with Passwords Privileges and Logins

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 2: 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		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).



CHAPTER 4

Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define views, which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Prerequisites for Role-Based CLI Access

Your image must support CLI views.

Restrictions for Role-Based CLI Access

Lawful Intercept Images Limitation

CLI views are a part of all platforms and Cisco IOS images because they are a part of the Cisco IOS parser. However, the lawful intercept view is available only in images that contain the lawful intercept subsystem.

Maximum Number of Allowed Views

The maximum number of CLI views and superviews, including one lawful intercept view, that can be configured is 15. (This does not include the root view.)

Parse View Profiles

When you configure Parse View profiles, the 'no' or 'default' commands in combination with any configuration commands are not saved to the startup-configuration file. The configuration is accepted and is persistent until the device is reloaded. Examples of commands which are not saved to the startup-configuration:

- **command configure include all no**
- **command interface include all no**
- **command configure include all default**

Information About Role-Based CLI Access

Benefits of Using CLI Views

Although users can control CLI access via both privilege levels and enable mode passwords, these functions do not provide network administrators with the necessary level of detail needed when working with Cisco IOS devices. CLI views provide a more detailed access control capability for network administrators, thereby, improving the overall security and accountability of Cisco IOS software.

As of Cisco IOS Release 12.3(11)T, network administrators can also specify an interface or a group of interfaces to a view; thereby, allowing access on the basis of specified interfaces.

Root View

When a system is in root view, it has all of the access privileges as a user who has level 15 privileges. If the administrator wishes to configure any view to the system (such as a CLI view, a superview, or a lawful intercept view), the system must be in root view.

The difference between a user who has level 15 privileges and a root view user is that a root view user can configure a new view and add or remove commands from the view. Also, when you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

Lawful Intercept View

Like a CLI view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that store information about calls and users.

Commands available in lawful intercept view belong to one of the these categories:

- Lawful intercept commands that should not be made available to any other view or privilege level
- CLI views that are useful for lawful intercept users but do not have to be excluded from other views or privilege levels

Superview

A superview consists of one or more CLI views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain these characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.
- If a superview is deleted, its associated CLI views are not deleted.

View Authentication via a New AAA Attribute

View authentication is performed by an external authentication, authorization, and accounting (AAA) server via the new attribute **cli-view-name**.

AAA authentication associates only one view name to a particular user; that is, only one view name can be configured for a user in an authentication server.

How to Use Role-Based CLI Access

Configuring a CLI View

Perform this task to create a CLI view and add commands or interfaces to the view, as appropriate.

Before you begin

Before you create a view, you must perform the following tasks:

- Enable AAA using the **aaa new-model** command.
- Ensure that your system is in root view-not privilege level 15.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *view-name* [**inclusive**]
4. **secret** [**0** | **5**] *encrypted-password*
5. **commands** *parser-mode* {**exclude** | **include-exclusive** | **include**} [**all**] [**interface** *interface-name* | *command*]
6. **end**
7. **enable** [*privilege-level* | **view** *view-name*]
8. **show parser view all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Device> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**parser view** *view-name* [**inclusive**]
	Example:
	`Device(config)# parser view first inclusive`
	`Device(config-view)#`
		Creates a view including all commands by default. If the **inclusive** keyword option is not selected, it creates a view excluding all commands by default. You are in the view configuration mode.

Step 4	**secret** [**0**	**5**] *encrypted-password* **Example:** `Device(config-view)# secret 5 secret`	Associates a CLI view or superview with a password. **Note** You must issue this command before you can configure additional attributes for the view. **Note** With CSCts50236, the password can be removed or overwritten. Use the **no secret** command to remove the configured password.
Step 5	**commands** *parser-mode* {**exclude**	**include-exclusive**	**include**} [**all**] [**interface** *interface-name*	*command*]	Adds commands or interfaces to a view and specifies the mode in which the specified command exists.

	Command or Action	Purpose
	Example: `Device(config-view)# commands exec include show version`	**Note** While configuring parser view profiles, the following **no** or **default** commands are not saved to the startup configuration. These commands are in use until the device is reloaded. Once the device is reloaded, reapply these commands to get the required results. • **commands configure include all no** • **commands interface include all no** • **commands configure include all default**
Step 6	**end** **Example:** `Device(config-view)# end`	Exits view configuration mode and returns to privileged EXEC mode.
Step 7	**enable** [*privilege-level* | **view** *view-name*] **Example:** `Device# enable view first`	Prompts you for a password to access a configured CLI view, and you can switch from one view to another view. Enter the password to access the CLI view.
Step 8	**show parser view all** **Example:** `Device# show parser view all`	(Optional) Displays information for all views that are configured on the device. **Note** Although this command is available for both root and lawful intercept users, the **all** keyword is available only to root users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

Troubleshooting Tips

You must associate a password with a view. If you do not associate a password, and you attempt to add commands to the view using the **commands** command, a system message such as the following is displayed:

```
%Password not set for view <viewname>.
```

Configuring a Lawful Intercept View

Perform this task to initialize and configure a view for lawful-intercept-specific commands and configuration information.

Before you begin

Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 using the **privilege** command.

Note Only an administrator or a user who has level 15 privileges can initialize a lawful intercept view.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **li-view** *li-password* **user** *username* **password** *password*
4. **username lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
5. **parser view** *view-name*
6. **secret 5** *encrypted-password*
7. **name** *new-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Device> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**li-view** *li-password* **user** *username* **password** *password* **Example:** `Device(config)# li-view lipass user li_admin password li_adminpass`	Initializes a lawful intercept view. After the li-view is initialized, you must specify at least one user via **user** *username* **password** *password* options.
Step 4	**username lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password* **Example:** `Device(config)# username lawful-intercept li-user1 password li-user1pass`	Configures lawful intercept users on a Cisco device.
Step 5	**parser view** *view-name* **Example:** `Device(config)# parser view li view name`	(Optional) Enters view configuration mode, which allows you to change the lawful intercept view password or the lawful intercept view name.
Step 6	**secret 5** *encrypted-password* **Example:**	(Optional) Changes an existing password for a lawful intercept view.

	Command or Action	Purpose
	`Device(config-view)# secret 5 secret`	
Step 7	**name** *new-name* **Example:** `Device(config-view)# name second`	(Optional) Changes the name of a lawful intercept view. If this command is not issued, the default name of the lawful intercept view is "li-view."

Troubleshooting Tips

To display information for all users who have access to a lawful intercept view, issue the **show users lawful-intercept** command. (This command is available only to authorized lawful intercept view users.)

Configuring a Superview

Perform this task to create a superview and add at least one CLI view to the superview.

Before you begin

Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created using the **parser view** command.

Note You can add a view to a superview only after you configure a password for the superview (using the **secret 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *superview-name* **superview**
4. **secret 5** *encrypted-password*
5. **view** *view-name*
6. **end**
7. **show parser view all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Device> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parser view** *superview-name* **superview** **Example:** `Device(config)# parser view su_view1 superview`	Creates a superview and enters view configuration mode.
Step 4	**secret 5** *encrypted-password* **Example:** `Device(config-view)# secret 5 secret`	Associates a CLI view or superview with a password. **Note** You must issue this command before you can configure additional attributes for the view.
Step 5	**view** *view-name* **Example:** `Device(config-view)# view view_three`	Adds a normal CLI view to a superview. Issue this command for each CLI view that is to be added to a given superview.

Step 6	**end**
	Example:
	`Device(config-view)# end`
	`Device#`
		Exits view configuration mode and returns to privileged EXEC mode.

Step 7	**show parser view all** **Example:** `Device# show parser view`	(Optional) Displays information for all views that are configured on the device. **Note** Although this command is available for both root and lawful intercept users, the **all** keyword is available only to root users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

Monitoring Views and View Users

To display debug messages for all views-root, CLI, lawful intercept, and superview-use the **debug parser view** command in privileged EXEC mode.

Configuration Examples for Role-Based CLI Access

Example: Configuring a CLI View

The following example shows how to configure two CLI views, “first” and “second". Thereafter, you can verify the CLI view in the running configuration.

```
Device(config)# parser view first inclusive
Device(config-view)# secret 5 firstpass
Device(config-view)# command exec exclude show version
Device(config-view)# command exec exclude configure terminal
Device(config-view)# command exec exclude all show ip
Device(config-view)# exit
Device(config)# parser view second
Device(config-view)# secret 5 secondpass
Device(config-view)# command exec include-exclusive show ip interface
Device(config-view)# command exec include logout
Device(config-view)# exit
!
!
Device(config-view)# do show running-config | beg view

parser view first inclusive
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec exclude configure terminal
 commands exec exclude configure
 commands exec exclude all show ip
 commands exec exclude show version
 commands exec exclude show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
!
```

Example: Verifying a CLI View

After you have configured the CLI views “first” and “second", you can issue the **enable view**command to verify which commands are available in each view. The following example shows which commands are available inside the CLI view “first” after the user has logged into this view. (Because the **show ip** command is configured with the all option, a complete set of suboptions is shown, except the **show ip interface** command, which is using the **include-exclusive** keyword in the second view.)

```
Device# enable view first
Password:
Device# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
Device# show ?
```

```
  ip       IP information
  parser   Display parser information
  version  System hardware and software status
Device# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Device Discovery Protocol
.
.
.
```

Example: Configuring a Lawful Intercept View

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added:

```
!Initialize the LI-View.
Device(config)# li-view lipass user li_admin password li_adminpass
Device(config)# end
! Enter the LI-View; that is, check to see what commands are available within the view.
Device# enable view li-view
Password:
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parser view li-view

Device(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views
Device(config-view)#
! NOTE:LI View configurations are never shown as part of 'running-configuration'.
! Configure LI Users.
Device(config)# username lawful-intercept li-user1 password li-user1pass

Device(config)# username lawful-intercept li-user2 password li-user2pass
! Displaying LI User information.
Device# show users lawful-intercept
```

```
li_admin
li-user1
li-user2
Device#
```

Note The lawful intercept view is available only on specific images and the view name option is available only in the LI view.

Example: Configuring a Superview

The following sample output from the **show running-config** command shows that “view_one” and “view_two” have been added to superview “su_view1", “view_three”, and “view_four” have been added to superview “su_view2”:

```
Device# show running-config
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Additional References for Role-Based CLI Access

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
SNMP, MIBs, CLI configuration	*Cisco IOS Network Management Configuration Guide* , Release 15.0.
Privilege levels	"Configuring Security with Passwords, Privileges and Logins" module.

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

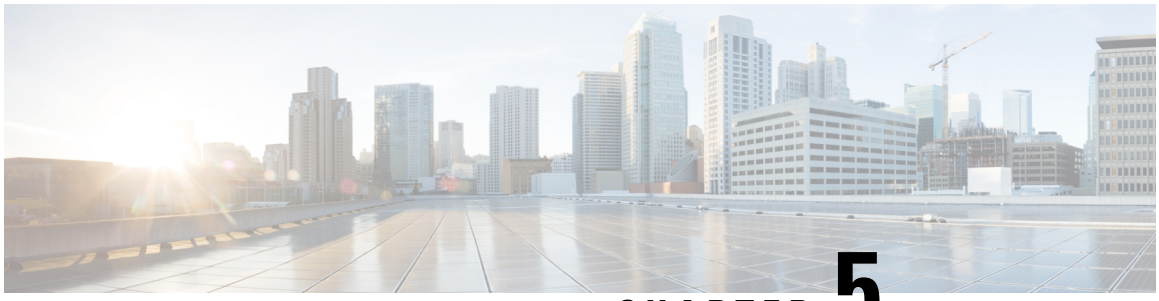
Feature Information for Role-Based CLI Access

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 3: Feature Information for Role-Based CLI Access

Feature Name	Releases	Feature Information
Role-Based CLI Access		The Role-Based CLI Access feature enables network administrators to restrict user access to CLI and configuration information. The CLI view capability was extended to restrict user access on a per-interface level, and additional CLI views were introduced to support the extended view capability. Also, support to group configured CLI views into a superview was introduced. The following commands were introduced or modified: **commands (view)**, **enable**, **li-view**, **name (view)**, **parser view , parser view superview**, **secret**, **show parser view**, **show users**, **username**, and **view**.
Role-Based CLI Inclusive Views		The Role-Based CLI Inclusive Views feature enables a standard CLI view including all commands by default. The following command was modified: **parser view inclusive**.



CHAPTER 5

Information About Secure Storage

Secure Storage feature allows you to secure critical configuration information by encrypting it. It encrypts VPN, IPSec, and other asymmetric key-pairs, pre-shared secrets, the type 6 password encryption key and certain credentials. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised.

By default, this feature is enabled on platforms that come with a hardware trust anchor. This feature is not supported on platforms that do not have hardware trust anchor.

Supported Platforms

Starting from Cisco IOS Release 15.6(3) M1, the following Cisco 880 Series platforms support Secure Storage:

Table 4: Secure Storage Supported Platforms - Cisco Integrated Services Router 880 PID

C881-K9
C887VA-K9
C886VA-K9
C887VAM-K9
C886VAJ-K9
C888-K9

Starting from Cisco IOS Release 15.6(3) M1, the following Cisco 890 Series platforms support Secure Storage:

Table 5: Secure Storage Supported Platforms - Cisco Integrated Services Router 890 PID

C891FW-E-K9

C891F-K9
C891FW-A-K9
C891-24X-K9

Starting from Cisco IOS Release 15.6(3) M1, the following Cisco 800M Series platforms support Secure Storage:

Table 6: Secure Storage Supported Platforms - Cisco Integrated Services Router 800M PID

C841M-4X/K9
C886VA-K9
C841M-8X/K9

Starting from Cisco IOS XE Release 16.6.1, the following ISR 4000 platforms support Secure Storage:

Table 7: Secure Storage Supported Platforms - Cisco Integrated Services Router 4000 PID

ISR4431
ISR4221
ISR4321
ISR4331
ISR4351
ISR4451-X

Starting from Cisco IOS XE Release 16.6.1, the following ASR 1000 platforms support Secure Storage::

Table 8: Secure Storage Supported Platforms - Cisco ASR 1000 Series Aggregation Services Routers PID

ASR1000-RP3
ASR1001-X
ASR1001-HX
ASR1002-HX

Starting from Cisco IOS XE Release 16.9.1, the following Cisco 1000 Series platforms support Secure Storage::

Table 9: Secure Storage Supported Platforms - Cisco 1000 Series PID

C1101-4P
C1111-8P
C1111-4P

C1112-8P
C1113-8P
C1113-8PM
C1116-4P
C1117-4P
C1117-4PM
C1101-4PLTEP
C1111-8PLTEEA
C1111-8PLTELA
C1111-4PLTEEA
C1111-4PLTELA
C1112-8PLTEEA
C1113-8PLTEEA
C1113-8PLTELA
C1113-8PMLTEEA
C1116-4PLTEEA
C1117-4PLTEEA
C1117-4PLTELA
C1117-4PMLTEEA
C1111-8PWY
C1111-4PWX
C1112-8PWE
C1113-8PWA
C1113-8PWB
C1113-8PWE
C1116-4PWE
C1117-4PWE
C1117-4PWA
C1117-4PWZ

C1117-4PMWE
C1111-8PLTEEAWX
C1111-8PLTELAWY
C1112-8PLTEAWE
C1113-8PLTEEAWA
C1113-8PLTEEAWB
C1113-8PLTEEAWE
C1113-8PLTELAWZ
C1116-4PLTEEAWE
C1117-4PMLTEEA
C1117-4PLTEEAWE
C1117-4PLTEEAWA
C1117-4PLTELAWZ
C1117-4PMLTEEAWE
C1101-4PLTEPWX

Enabling Secure Storage

Before you begin

By default, this feature is enabled on a platform. Use this procedure on a platform where it is disabled.

SUMMARY STEPS

1. Config terminal
2. service private-config-encryption
3. do write memory

DETAILED STEPS

	Command or Action	Purpose
Step 1	Config terminal **Example:** `router#config terminal`	Enters the configuration mode.

	Command or Action	Purpose
Step 2	service private-config-encryption **Example:** `router(config)# service private-config-encryption`	Enables the Secure Storage feature on your platform.
Step 3	do write memory **Example:** `router(config)# do write memory`	Encrypts the private-config file and saves the file in an encrypted format.

Example

The following example shows how to enable Secure Storage:

```
router#config terminal
router(config)# service private-config-encryption
router(config)# do write memory
```

Disabling Secure Storage

Before you begin

To disable Secure Storage feature on a platform, perform this task:

SUMMARY STEPS

1. Config terminal
2. no service private-config-encryption
3. do write memory

DETAILED STEPS

	Command or Action	Purpose
Step 1	Config terminal **Example:** `router#config terminal`	Enters the configuration mode.
Step 2	no service private-config-encryption **Example:** `router(config)# no service private-config-encryption`	Disables the Secure Storage feature on your platform.
Step 3	do write memory **Example:** `router(config)# do write memory`	Decrypts the private-config file and saves the file in plane format.

Example

The following example shows how to disable Secure Storage:

```
router#config terminal
router(config)# no service private-config-encryption
router(config)# do write memory
```

Verifying the Status of Encryption

Use the **show parser encrypt file status** command to verify the status of encryption. The following command output indicates that the feature is available but the file is not encrypted. The file is in 'plain text' format.

```
router#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```

The following command output indicates that the feature is enabled and the file is encrypted. The file is in 'cipher text' format.

```
router#show parser encrypt file status
Feature: Enabled
File Format: Cipher Text
Encryption Version: Ver1
```

Downgrading the Platform Image to an Older Version

Before you downgrade the platform image to an older version where the Secure Storage is not supported, you have to disable the feature in the version where it is supported.

If you do not disable this feature before downgrading to an older image, the private-config file will be in encrypted format. The following Syslog message will be generated to indicate that the file is in encrypted format:

```
%PARSER-4-BADCFG: Unexpected end of configuration file.
```

If the file is in 'plain text', no Syslog message will be generated.

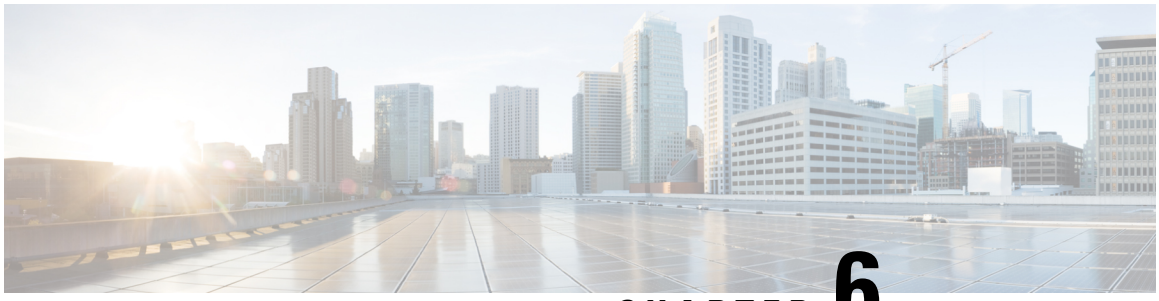
Feature Information for Overview of Secure Storage

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 10: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
Secure Storage	Cisco IOS XE Fuji 16.9.1	The support for Secure Storage is introduced for ASR and ISR platforms.



CHAPTER 6

AutoSecure

The AutoSecure feature secures a router by using a single CLI command to disable common IP services that can be exploited for network attacks, enable IP services and features that can aid in the defense of a network when under attack, and simplify and harden the security configuration of the router.

AutoSecure enhances secure access to the router by configuring a required minimum password length to eliminate common passwords that can be common on many networks, such as “lab” and “company name.” Syslog messages are generated after the number of unsuccessful attempts exceeds the configured threshold.

AutoSecure also allows a router to revert (roll) back to its pre-AutoSecure configuration state if the AutoSecure configuration fails.

When AutoSecure is enabled, a detailed audit trail of system logging messages capture any changes or tampering of the AutoSecure configuration that may have been applied to the running configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Restrictions for AutoSecure

The AutoSecure configuration can be configured at run time or setup time. If any related configuration is modified after AutoSecure has been enabled, the AutoSecure configuration may not be fully effective.

Information About AutoSecure

Securing the Management Plane

The management plane is secured by turning off certain global and interface services that can be potentially exploited for security attacks and turning on global services that help mitigate the threat of attacks. Secure access and secure logging are also configured for the router.

Caution If your device is managed by a network management (NM) application, securing the management plane could turn off some services like the HTTP server and disrupt the NM application support.

The following subsections define how AutoSecure helps to secure the management plane:

Disabling Global Services

After enabling this feature (through the **auto secure** command), the following global services are disabled on the router without prompting the user:

- Finger--Collects information about the system (reconnaissance) before an attack. If enabled, the information can leave your device vulnerable to attacks.
- PAD--Enables all packet assembler and disassembler (PAD) commands and connections between PAD devices and access servers. If enabled, it can leave your device vulnerable to attacks.
- Small Servers--Causes TCP and User Datagram Protocol (UDP) diagnostic port attacks: a sender transmits a volume of fake requests for UDP diagnostic services on the router, consuming all CPU resources.
- Bootp Server--Bootp is an insecure protocol that can be exploited for an attack.
- HTTP Server--Without secure-http or authentication embedded in the HTTP server with an associated ACL, the HTTP server is insecure and can be exploited for an attack. (If you must enable the HTTP server, you are prompted for the proper authentication or access list.)

Note If you are using Cisco Configuration Professional (CCP), you must manually enable the HTTP server through the **ip http server** command.

- Identification Service--An insecure protocol, defined in RFC 1413, that allows one to query a TCP port for identification. An attacker can access private information about the user from the ID server.
- CDP--If a large number of Cisco Discovery Protocol (CDP) packets are sent to the router, the available memory of the router can be consumed, causing the router to crash.

Caution NM applications that use CDP to discover network topology are not able to perform discovery.

- NTP--Without authentication or access-control, Network Time Protocol (NTP) is insecure and can be used by an attacker to send NTP packets to crash or overload the router. (If you want to turn on NTP, you must configure NTP authentication using Message Digest 5 (MD5) and the **ntp access-group** command. If NTP is enabled globally, disable it on all interfaces on which it is not needed.)
- Source Routing--Provided only for debugging purposes, so source routing should be disabled in all other cases. Otherwise, packets may slip away from some of the access control mechanisms that they should have gone through.

Disabling Per Interface Services

After enabling this feature, the following per interface services are disabled on the router without prompting the user:

- ICMP redirects--Disabled on all interfaces. Does not add a useful functionality to a correctly configured to network, but it could be used by attackers to exploit security holes.
- ICMP unreachables--Disabled on all interfaces. Internet Control Management Protocol (ICMP) unreachables are a known cause for some ICMP-based denial of service (DoS) attacks.
- ICMP mask reply messages--Disabled on all interfaces. ICMP mask reply messages can give an attacker the subnet mask for a particular subnetwork in the internetwork.
- Proxy-Arp--Disabled on all interfaces. Proxy-Arp requests are a known cause for DoS attacks because the available bandwidth and resources of the router can be consumed in an attempt to respond to the repeated requests that are sent by an attacker.
- Directed Broadcast--Disabled on all interfaces. Potential cause of SMURF attacks for DoS.
- Maintenance Operations Protocol (MOP) service--Disabled on all interfaces.

Enabling Global Services

After AutoSecure is enabled, the following global services are enabled on the router without prompting the user:

- The **service password-encryption** command--Prevents passwords from being visible in the configuration.
- The **service tcp-keepalives-in** and **service tcp-keepalives-out** commands--Ensures that abnormally terminated TCP sessions are removed.

Securing Access to the Router

Caution If your device is managed by an NM application, securing access to the router could turn off vital services and may disrupt the NM application support.

After enabling this feature, the following options in which to secure access to the router are available to the user:

- If a text banner does not exist, users are prompted to add a banner. This feature provides the following sample banner:

```
Authorized access only
This system is the property of ABC Enterprise
Disconnect IMMEDIATELY if you are not an authorized user!
Contact abc@xyz.com +99 876 543210 for help.
```

- The login and password (preferably a secret password, if supported) are configured on the console, AUX, vty, and tty lines. The **transport input** and **transport output**commandsare also configured on all of these lines. (Telnet and secure shell (SSH) are the only valid transport methods.) The **exec-timeout** command is configured on the console and AUX as 10.
- When the image on the device is a crypto image, AutoSecure enables SSH and secure copy (SCP) for access and file transfer to and from the router. The **timeout** *seconds* and **authentication-retries** *integer* options for the **ip ssh** command are configured to a minimum number. (Telnet and FTP are not affected by this operation and remain operational.)
- If the AutoSecure user specifies that their device does not use Simple Network Management Protocol (SNMP), one of the following functions occur:
  - In interactive mode, the user is asked whether to disable SNMP regardless of the values of the community strings, which act like passwords to regulate access to the agent on the router.
  - In non-interact mode, SNMP is disabled if the community string is “public” or “private.”

Note After AutoSecure has been enabled, tools that use SNMP to monitor or configure a device is unable to communicate with the device through SNMP.

- If authentication, authorization, and accounting (AAA) is not configured, configure local AAA. AutoSecure prompts users to configure a local username and password on the router.

Security Logging

The following logging options are available after AutoSecure is enabled. These options identify security incidents and provide ways to respond to them.

- Sequence numbers and time stamps for all debug and log messages. This option is useful when auditing logging messages.
- Logging messages can be generated for login-related events; for example, the message “Blocking Period when Login Attack Detected” is displayed when a login attack is detected and the router enters “quiet mode.” (Quiet mode means that the router does not allow any login attempts through Telnet, HTTP, or SSH.)

For more information on login system messages, see the Cisco IOS Release 12.3(4)T feature module Cisco IOS Login Enhancements .

- The **logging console critical**command, which sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
- The **logging buffered** command, which copies logging messages to an internal buffer and limits messages logged to the buffer based on severity.
- The **logging trap debugging** command, which allows all commands with a severity higher than debugging to be sent to the logging server.

Securing the Forwarding Plane

To minimize the risk of attacks on the router forward plane, AutoSecure provides the following functions:

- Cisco Express Forwarding (CEF)--AutoSecure enables CEF or distributed CEF (dCEF) on the router whenever possible. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Thus, routers configured for CEF perform better under SYN attacks than routers using the traditional cache.

Note CEF consumes more memory than a traditional cache.

- If the TCP intercept feature is available, it can be configured on the router for connection timeout.
- If strict Unicast Reverse Path Forwarding (uRPF) is available, it can be configured on the router to help mitigate problems that are caused by the introduction of forged (spoofed) IP source addresses. uRPF discards IP packets that lack a verifiable IP source address.
- If the router is being used as a firewall, it can be configured for context-based access control (CBAC) on public interfaces that are facing the Internet.

Note At the beginning of the AutoSecure dialogue, you are prompted for a list of public interfaces.

How to Configure AutoSecure

Configuring AutoSecure

Caution Although the **auto secure**command helps to secure a router, it does not guarantee the complete security of the router.

SUMMARY STEPS

1. **enable**
2. auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	

Step 2	auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]
	Example:
	`Router#`
	`auto secure`
		A semi-interactive dialogue session begins to secure either the management or forwarding planes on the router when the **management** or **forwarding** keyword is selected. If neither option is selected, then the dialogue asks for both planes to be configured. If the **management** keyword is selected, then the management plane is secured only. If the **forwarding keyword is selected, then**the forwarding plane is secured only.
		If the **no-interact** keyword is selected, then the user is not prompted for any interactive configurations.
		If the **full** keyword is selected, then user is prompted for all interactive questions, which is the default.

Configuring Enhanced Security Access to the Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable password** {*password* | [*encryption-type*] *encrypted-password* }
4. **security authentication failure rate** *threshold-rate* **log**
5. **exit** *threshold-rate* **log**
6. **show auto secure config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**enable password** {*password* | [*encryption-type*] *encrypted-password* } **Example:** `Router(config)# enable password elephant`	Sets a local password to control access to various privilege levels.

	Command or Action	Purpose
Step 4	**security authentication failure rate** *threshold-rate* **log** **Example:** `Router(config)# security authentication failure rate 10 log`	Configures the number of allowable unsuccessful login attempts. • *threshold-rate* --Number of allowable unsuccessful login attempts. • **log** --Syslog authentication failures if the rate exceeds the threshold.
Step 5	**exit** *threshold-rate* **log** **Example:** `Router(config)# exit`	Exits configuration mode and enters privileged EXEC mode.
Step 6	**show auto secure config** **Example:** `Router# show auto secure config`	(Optional) Displays all configuration commands that have been added as part of the AutoSecure configuration.

Configuration Example for AutoSecure

The following example is a sample AutoSecure dialogue. After you enable the **auto secure** command, the feature automatically prompts you with a similar dialogue unless you enable the **no-interact** keyword. (For information on which services are disabled and which features are enabled, see the sections, "Securing the Management Plane, on page 72" and "Securing the Forwarding Plane, on page 75" earlier in this document.)

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router but it will not make router
 absolutely secure from all security attacks ***
All the configuration done as part of AutoSecure will be shown here. For more details of
why and how this configuration is useful, and any possible side effects, please refer to
Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:
Interface                  IP-Address OK? Method Status
Protocol
FastEthernet0/1/0          10.1.1.1  YES NVRAM  up down
FastEthernet1/0/0            10.2.2.2  YES NVRAM  up down
FastEthernet1/1/0            10.0.0.1  YES NVRAM  up up
Loopback0                  unassigned YES NVRAM  up up
FastEthernet0/0/0            10.0.0.2  YES NVRAM  up down
Enter the interface name that is facing internet:FastEthernet0/0/0
Securing Management plane services..
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
```

```
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or is same as enable password
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Configure SSH server? [yes]:
Enter the domain-name:example.com
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces
Securing Forwarding plane services..
Enabling CEF (it might have more memory requirements on some low end
platforms)
Enabling unicast rpf on all interfaces connected to internet
Configure CBAC Firewall feature? [yes/no]:yes
This is the configuration generated:
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name example.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
```

```
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
interface FastEthernet0/0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
!
end
Apply this configuration to running-config? [yes]:yes
Applying the config generated to running-config
The name for the keys will be:ios210.example.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
Router#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring SNMP Support	Configuring SNMP Support
Security Commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
PacketCable™ *Control Point Discovery Interface Specification*	*PacketCable™ Control Point Discovery Interface Specification* (PKT-SP-CPD-I02-061013)

MIBs

MIB	MIBs Link
• CISCO-802-TAP-MIB • CISCO-IP-TAP-MIB • CISCO-MOBILITY-TAP-MIB • CISCO-TAP2-MIB • CISCO-USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC-2865	*Remote Authentication Dial In User Service (RADIUS)*
RFC-3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC-3924	*Cisco Architecture for Lawful Intercept in IP Networks*

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

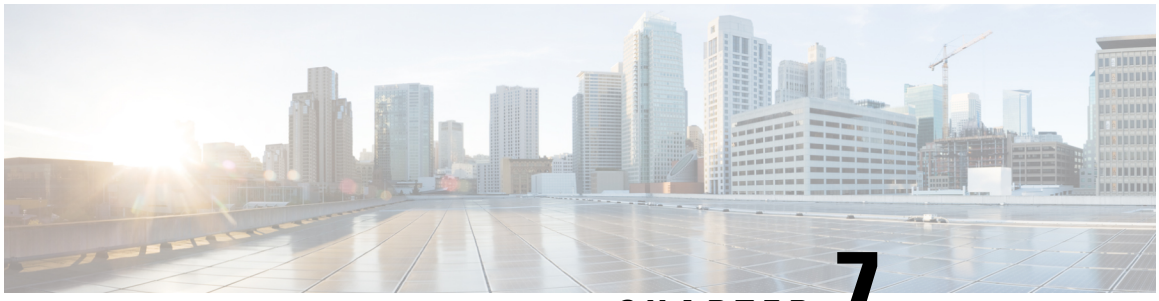
Feature Information for AutoSecure

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 11: Feature Information for AutoSecure

Feature Name	Releases	Feature Information
AutoSecure Manageability	Cisco IOS XE Release 2.3	This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. By using a single command-line interface (CLI), the AutoSecure feature allows a user to perform the following functions: • Disable common IP services that can be exploited for network attacks • Enable IP services and features that can aid in the defense of a network when under attack This feature also simplifies the security configuration of a router and hardens the router configuration. The following commands were introduced or modified: **auto secure** and **show auto secure config**



CHAPTER 7

Configuring Kerberos

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Information About Kerberos

Kerberos is a secret-key network authentication protocol, developed at the Massachusetts Institute of Technology (MIT), that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos, like other secret-key systems, is based on the concept of a trusted third party that performs secure verification of users and services. In the Kerberos protocol, this trusted third party is called the key distribution center (KDC).

The primary use of Kerberos is to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username-and-password authentication mechanism.

The Kerberos credential scheme embodies a concept called "single logon." This process requires authenticating a user once, and then allows secure authentication (without encrypting another password) wherever that user's credential is accepted.

Cisco IOS XE software includes Kerberos 5 support, which allows organizations already deploying Kerberos 5 to use the same Kerberos authentication database on their routers that they are already using on their other network hosts (such as UNIX servers and PCs).

The following network services are supported by the Kerberos authentication capabilities in Cisco IOS XE software:

- Telnet
- rlogin
- rsh
- rcp

Note Cisco Systems' implementation of Kerberos client support is based on code developed by CyberSafe, which was derived from the MIT code. As a result, the Cisco Kerberos implementation has successfully undergone full compatibility testing with the CyberSafe Challenger commercial Kerberos server and MIT's server code, which is freely distributed.

The table below lists common Kerberos-related terms and their definitions.

Table 12: Kerberos Terminology

Term	Definition
authentication	A process by which a user or service identifies itself to another service. For example, a client can authenticate to a router or a router can authenticate to another router.
authorization	A means by which the router determines what privileges you have in a network or on the router and what actions you can perform.
credential	A general term that refers to authentication tickets, such as ticket granting tickets (TGTs) and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of retyping in a username and password. Credentials have a default lifespan of eight hours.
instance	An authorization level label for Kerberos principals. Most Kerberos principals are of the form user@REALM (for example, smith@EXAMPLE.COM). A Kerberos principal with a Kerberos instance has the form user/instance@REALM (for example, smith/admin@EXAMPLE.COM). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. It is up to the server of each network service to implement and enforce the authorization mappings of Kerberos instances. Note that the Kerberos realm name must be in uppercase characters.
Kerberized	Applications and services that have been modified to support the Kerberos credential infrastructure.

Term	Definition
Kerberos realm	A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service. Kerberos realms must always be in uppercase characters.
Kerberos server	A daemon running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.
key distribution center (KDC)	A Kerberos server and database program running on a network host.
principal	Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server.
service credential	A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC, and with the user's TGT.
SRVTAB	A password that a network service shares with the KDC. The network service authenticates an encrypted service credential by using the SRVTAB (also known as a KEYTAB) to decrypt it.
ticket granting ticket (TGT)	A credential that the key distribution center (KDC) issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.

Kerberos Client Support Operation

This section describes how the Kerberos security system works with a Cisco router functioning as the security server. Although (for convenience or technical reasons) you can customize Kerberos in a number of ways, remote users attempting to access network services must pass through three layers of security before they can access network services.

Authenticating to the Boundary Router

This section describes the first layer of security that remote users must pass through when they attempt to access a network. The first step in the Kerberos authentication process is for users to authenticate themselves to the boundary router. The following process describes how users authenticate to a boundary router:

1. The remote user opens a PPP connection to the corporate site router.
2. The router prompts the user for a username and password.
3. The router requests a TGT from the KDC for this particular user.
4. The KDC sends an encrypted TGT to the router that includes (among other things) the user's identity.
5. The router attempts to decrypt the TGT using the password the user entered. If the decryption is successful, the remote user is authenticated to the router.

A remote user who successfully initiates a PPP session and authenticates to the boundary router is inside the firewall but still must authenticate to the KDC directly before being allowed to access network services. This is because the TGT issued by the KDC is stored on the router and is not useful for additional authentication unless the user physically logs on to the router.

Obtaining a TGT from a KDC

This section describes how remote users who are authenticated to the boundary router authenticate themselves to a KDC.

When a remote user authenticates to a boundary router, that user technically becomes part of the network; that is, the network is extended to include the remote user and the user's machine or network. To gain access to network services, however, the remote user must obtain a TGT from the KDC. The following process describes how remote users authenticate to the KDC:

1. The remote user, at a workstation on a remote site, launches the KINIT program (part of the client software provided with the Kerberos protocol).
2. The KINIT program finds the user's identity and requests a TGT from the KDC.
3. The KDC creates a TGT, which contains the identity of the user, the identity of the KDC, and the expiration time of the TGT.
4. Using the user's password as a key, the KDC encrypts the TGT and sends the TGT to the workstation.
5. When the KINIT program receives the encrypted TGT, it prompts the user for a password (this is the password that is defined for the user in the KDC).
6. If the KINIT program can decrypt the TGT with the password the user enters, the user is authenticated to the KDC, and the KINIT program stores the TGT in the user's credential cache.

At this point, the user has a TGT and can communicate securely with the KDC.In turn, the TGT allows the user to authenticate to other network services.

Authenticating to Network Services

The following process describes how a remote user with a TGT authenticates to network services within a given Kerberos realm. Assume the user is on a remote workstation (Host A) and wants to log in to Host B.

1. The user on Host A initiates a Kerberized application (such as Telnet) to Host B.
2. The Kerberized application builds a service credential request and sends it to the KDC. The service credential request includes (among other things) the user's identity and the identity of the desired network service. The TGT is used to encrypt the service credential request.
3. The KDC tries to decrypt the service credential request with the TGT it issued to the user on Host A. If the KDC can decrypt the packet, it is assured that the authenticated user on Host A sent the request.
4. The KDC notes the network service identity in the service credential request.
5. The KDC builds a service credential for the appropriate network service on Host B on behalf of the user on Host A. The service credential contains the client's identity and the desired network service's identity.
6. The KDC then encrypts the service credential twice. It first encrypts the credential with the SRVTAB that it shares with the network service identified in the credential. It then encrypts the resulting packet with the TGT of the user (who, in this case, is on Host A).

7. The KDC sends the twice-encrypted credential to Host A.
8. Host A attempts to decrypt the service credential with the user's TGT. If Host A can decrypt the service credential, it is assured the credential came from the real KDC.
9. Host A sends the service credential to the desired network service. Note that the credential is still encrypted with the SRVTAB shared by the KDC and the network service.
10. The network service attempts to decrypt the service credential using its SRVTAB.
11. If the network service can decrypt the credential, it is assured the credential was in fact issued from the KDC. Note that the network service trusts anything it can decrypt from the KDC, even if it receives it indirectly from a user. This is because the user first authenticated with the KDC.

At this point, the user is authenticated to the network service on Host B. This process is repeated each time a user wants to access a network service in the Kerberos realm.

How to Configure Kerberos

For hosts and the KDC in your Kerberos realm to communicate and mutually authenticate, you must identify them to each other. To do this, you add entries for the hosts to the Kerberos database on the KDC and add SRVTAB files generated by the KDC to all hosts in the Kerberos realm. You also make entries for users in the KDC database.

This section describes how to set up a Kerberos-authenticated server-client system and contains the following topics:

This section assumes that you have installed the Kerberos administrative programs on a UNIX host, known as the KDC, initialized the database, and selected a Kerberos realm name and password. For instructions about completing these tasks, refer to documentation that came with your Kerberos software.

Note Write down the host name or IP address of the KDC, the port number you want the KDC to monitor for queries, and the name of the Kerberos realm it will serve. You need this information to configure the router.

Configuring the KDC Using Kerberos Commands

After you set up a host to function as the KDC in your Kerberos realm, you must make entries to the KDC database for all principals in the realm. Principals can be network services on Cisco routers and hosts or they can be users.

To use Kerberos commands to add services to the KDC database (and to modify existing database information), complete the tasks in the following sections:

Note All Kerberos command examples are based on Kerberos 5 Beta 5 of the original MIT implementation. Later versions use a slightly different interface.

Adding Users to the KDC Database

To add users to the KDC and create privileged instances of those users, use the **su** command to become root on the host running the KDC and use the kdb5_edit program to use the following commands in privileged EXEC mode:

SUMMARY STEPS

1. Router# **ank***username@REALM*
2. Router# **ank***username/instance@REALM*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **ank***username@REALM*	Use the **ank** (add new key) command to add a user to the KDC. This command prompts for a password, which the user must enter to authenticate to the router.
Step 2	Router# **ank***username/instance@REALM*	Use the **ank** command to add a privileged instance of a user.

What to do next

For example, to add user *loki* of Kerberos realm CISCO.COM, enter the following Kerberos command:

```
ank loki@CISCO.COM
```

Note The Kerberos realm name must be in uppercase characters.

You might want to create privileged instances to allow network administrators to connect to the router at the enable level, for example, so that they need not enter a clear text password (and compromise security) to enter enable mode.

To add an instance of *loki* with additional privileges (in this case, enable, although it could be anything) enter the following Kerberos command:

```
ank loki/enable@CISCO.COM
```

In each of these examples, you are prompted to enter a password, which you must give to user *loki* to use at login.

The Enabling Kerberos Instance Mapping, on page 93 describes how to map Kerberos instances to various Cisco IOS XE privilege levels.

Creating SRVTABs on the KDC

All routers that you want to authenticate to use the Kerberos protocol must have an SRVTAB. For more information on extracting SRVTABs, see *Extracting SRVTABs*

To make SRVTAB entries on the KDC, use the following command in privileged EXEC mode:

Command	Purpose
`Router# ark SERVICE/HOSTNAME@REALM`	Use the **ark** (add random key) command to add a network service supported by a host or router to the KDC.

For example, to add a Kerberized authentication service for a Cisco router called *router1* to the Kerberos realm CISCO.COM, enter the following Kerberos command:

```
ark host/router1.cisco.com@CISCO.COM
```

Make entries for all network services on all Kerberized hosts that use this KDC for authentication.

Extracting SRVTABs

SRVTABs contain (among other things) the passwords or randomly generated keys for the service principals you entered into the KDC database. Service principal keys must be shared with the host running that service. To do this, you must save the SRVTAB entries to a file, then copy the file to the router and all hosts in the Kerberos realm. Saving SRVTAB entries to a file is called *extracting* SRVTABs. To extract SRVTABs, use the following command in privileged EXEC mode:

Command	Purpose
`Router# xst router-name host`	Use the kdb5_edit command **xst** to write an SRVTAB entry to a file.

For example, to write the host/router1.cisco.com@CISCO.COM SRVTAB to a file, enter the following Kerberos command:

```
xst router1.cisco.com@CISCO.COM host
```

Use the **quit** command to exit the kdb5_edit program.

Configuring the Router to Use the Kerberos Protocol

Defining a Kerberos Realm

For a router to authenticate a user defined in the Kerberos database, it must know the host name or IP address of the host running the KDC, the name of the Kerberos realm and, optionally, be able to map the host name or Domain Name System (DNS) domain to the Kerberos realm.

To configure the router to authenticate to a specified KDC in a specified Kerberos realm, use the following commands in global configuration mode. Note that DNS domain names must begin with a leading dot (.):

SUMMARY STEPS

1. Router(config)# **kerberos local-realm***kerberos-realm*
2. Router(config)# **kerberos server***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]
3. Router(config)# **kerberos realm** {*dns-domain* | *host* } *kerberos-realm*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **kerberos local-realm***kerberos-realm*	Defines the default realm for the router.
Step 2	Router(config)# **kerberos server***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]	Specifies to the router which KDC to use in a given Kerberos realm and, optionally, the port number that the KDC is monitoring. (The default is 88.)
Step 3	Router(config)# **kerberos realm** {*dns-domain* | *host* } *kerberos-realm*	(Optional) Maps a host name or DNS domain to a Kerberos realm.

What to do next

Note Because the machine running the KDC and all Kerberized hosts must interact within a 5-minute window or authentication fails, all Kerberized machines, and especially the KDC, should be running the Network Time Protocol (NTP).

The **kerberos local-realm**, **kerberos realm**, and **kerberos server** commands are equivalent to the UNIX krb.conf file. The table below identifies mappings from the Cisco IOS XE configuration commands to a Kerberos 5 configuration file (krb5.conf).

Table 13: Kerberos 5 Configuration File and Commands

krb5.conf File	Cisco IOS XE Configuration Command
[libdefaults] `default_realm = DOMAIN.COM`	(in configuration mode) **`kerberos local-realm`** *`DOMAIN.COM`*

[domain_realm]
 	
`.domain.com = DOMAIN.COM`
 	
`domain.com = DOMAIN.COM`
	(in configuration mode)
	
	`kerberos realm`
	`.domain.com`
	`DOMAIN.COM`
	`kerberos realm`
	`domain.com DOMAIN.COM`

[realms]
 	
`kdc = DOMAIN.PIL.COM:750`
 	
`admin_server = DOMAIN.PIL.COM`
 	
`default_domain = DOMAIN.COM`
	(in configuration mode)
	
	`kerberos server`
	`DOMAIN.COM 172.65.44.2`
	`(`*`172.65.44.2`*
	`is the example IP address for`*`DOMAIN.PIL.COM`*
	`)`

For an example of defining a Kerberos realm, see the Defining a Kerberos Realm Examples module.

Copying SRVTAB Files

To make it possible for remote users to authenticate to the router using Kerberos credentials, the router must share a secret key with the KDC. To do this, you must give the router a copy of the SRVTAB you extracted on the KDC.

The most secure method to copy SRVTAB files to the hosts in your Kerberos realm is to copy them onto physical media and go to each host in turn and manually copy the files onto the system. To copy SRVTAB files to the router, which does not have a physical media drive, you must transfer them via the network using TFTP.

To remotely copy SRVTAB files to the router from the KDC, use the following command in global configuration mode:

Command	Purpose
`Router(config)# kerberos srvtab remote {hostname | ip-address} {filename}`	Retrieves an SRVTAB file from the KDC.

When you copy the SRVTAB file from the router to the KDC, the **kerberos srvtab remote** command parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry**format. To ensure that the SRVTAB is available (does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write your running configuration (which contains the parsed SRVTAB file) to NVRAM.

For an example of copying SRVTAB files, see the SRVTAB File Copying Example, on page 94.

Specifying Kerberos Authentication

You have now configured Kerberos on your router. This makes it possible for the router to authenticate using Kerberos. The next step is to tell it to do so. Because Kerberos authentication is facilitated through AAA, you need to enter the **aaa authentication** command, specifying Kerberos as the authentication method. For more information, refer to the chapter "Configuring Authentication".

Enabling Credentials Forwarding

With Kerberos configured thus far, a user authenticated to a Kerberized router has a TGT and can use it to authenticate to a host on the network. However, if the user tries to list credentials after authenticating to a host, the output will show no Kerberos credentials present.

You can optionally configure the router to forward users' TGTs with them as they authenticate from the router to Kerberized remote hosts on the network when using Kerberized Telnet, rcp, rsh, and rlogin (with the appropriate flags).

To force all clients to forward users' credentials as they connect to other hosts in the Kerberos realm, use the following command in global configuration mode:

Command	Purpose
`Router(config)# kerberos credentials forward`	Forces all clients to forward user credentials upon successful Kerberos authentication.

With credentials forwarding enabled, users' TGTs are automatically forwarded to the next host they authenticate to. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time to get a new TGT.

Opening a Telnet Session to the Router

To use Kerberos to authenticate users opening a Telnet session to the router from within the network, use the following command in global configuration mode:

Command	Purpose
`Router(config)# aaa authentication login {default | list-name } krb5_telnet`	Sets login authentication to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.

Although Telnet sessions to the router are authenticated, users must still enter a clear text password if they want to enter enable mode. The **kerberos instance map** command, discussed in a later section, allows them to authenticate to the router at a predefined privilege level.

Establishing an Encrypted Kerberized Telnet Session

Another way for users to open a secure Telnet session is to use Encrypted Kerberized Telnet. With Encrypted Kerberized Telnet, users are authenticated by their Kerberos credentials before a Telnet session is established. The Telnet session is encrypted using 56-bit Data Encryption Standard (DES) encryption with 64-bit Cipher Feedback (CFB). Because data sent or received is encrypted, not clear text, the integrity of the dialed router or access server can be more easily controlled.

Note This feature is available only if you have the 56-bit encryption image. 56-bit DES encryption is subject to U.S. Government export control regulations.

To establish an encrypted Kerberized Telnet session from a router to a remote host, use either of the following commands in EXEC command mode:

Command	Purpose

`Router(config)# connect host [port ] /encrypt kerberos`
 	
or
 	
`Router(config)# telnet host [port ] /encrypt kerberos`
	Establishes an encrypted Telnet session.

When a user opens a Telnet session from a Cisco router to a remote host, the router and remote host negotiate to authenticate the user using Kerberos credentials. If this authentication is successful, the router and remote

host then negotiate whether or not to use encryption. If this negotiation is successful, both inbound and outbound traffic is encrypted using 56-bit DES encryption with 64-bit CFB.

When a user dials in from a remote host to a Cisco router configured for Kerberos authentication, the host and router will attempt to negotiate whether or not to use encryption for the Telnet session. If this negotiation is successful, the router will encrypt all outbound data during the Telnet session.

If encryption is not successfully negotiated, the session will be terminated and the user will receive a message stating that the encrypted Telnet session was not successfully established.

For information about enabling bidirectional encryption from a remote host, refer to the documentation specific to the remote host device.

For an example of using encrypted Kerberized Telnet to open a secure Telnet session, see the Encrypted Telnet Session Example, on page 95.

Enabling Mandatory Kerberos Authentication

As an added layer of security, you can optionally configure the router so that, after remote users authenticate to it, these users can authenticate to other services on the network only with Kerberized Telnet, rlogin, rsh, and rcp. If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service; for example, Telnet and rlogin prompt for a password, and rsh attempts to authenticate using the local rhost file.

To make Kerberos authentication mandatory, use the following command in global configuration mode:

Command	Purpose
`Router(config)# kerberos clients mandatory`	Sets Telnet, rlogin, rsh, and rcp to fail if they cannot negotiate the Kerberos protocol with the remote server.

Enabling Kerberos Instance Mapping

As mentioned in the Creating SRVTABs on the KDC, on page 88, you can create administrative instances of users in the KDC database. The **kerberos instance map** command allows you to map those instances to Cisco IOS XE privilege levels so that users can open secure Telnet sessions to the router at a predefined privilege level, obviating the need to enter a clear text password to enter enable mode.

To map a Kerberos instance to a Cisco IOS XE privilege level, use the following command in global configuration mode:

Command	Purpose
`Router(config)# kerberos instance map` *instance privilege-level*	Maps a Kerberos instance to a Cisco IOS XE privilege level.

If there is a Kerberos instance for user *loki* in the KDC database (for example, *loki/admin*), user *loki* can now open a Telnet session to the router as loki/admin and authenticate automatically at privilege level 15, assuming instance “admin” is mapped to privilege level 15. (See the Opening a Telnet Session to the Router, on page 92.)

Cisco IOS XE commands can be set to various privilege levels using the **privilege level**command.

After you map a Kerberos instance to a Cisco IOS XE privilege level, you must configure the router to check for Kerberos instances each time a user logs in. To run authorization to determine if a user is allowed to run an EXEC shell based on a mapped Kerberos instance, use the **aaa authorization** command with the **krb5-instance** keyword. For more information, refer to the chapter "Configuring Authorization."

Monitoring and Maintaining Kerberos

To display or remove a current user's credentials, use the following commands in EXEC mode:

SUMMARY STEPS

1. Router# **show kerberos creds**
2. Router# **clear kerberos creds**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **show kerberos creds**	Lists the credentials in a current user's credentials cache.
Step 2	Router# **clear kerberos creds**	Destroys all credentials in a current user's credentials cache, including those forwarded.

Kerberos Configuration Examples

Kerberos Realm Definition Examples

To define CISCO.COM as the default Kerberos realm, use the following command:

```
kerberos local-realm CISCO.COM
```

To tell the router that the CISCO.COM KDC is running on host 10.2.3.4 at port number 170, use the following Kerberos command:

```
kerberos server CISCO.COM 10.2.3.4 170
```

To map the DNS domain cisco.com to the Kerberos realm CISCO.COM, use the following command:

```
kerberos realm.cisco.com CISCO.COM
```

SRVTAB File Copying Example

To copy over the SRVTAB file on a host named host123.cisco.com for a router named router1.cisco.com, the command would look like this:

```
kerberos srvtab remote host123.cisco.com router1.cisco.com-new-srvtab
Valid Starting          Expires                 Service Principal
13-May-1996 14:59:44    13-May-1996 23:00:45    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 15
```

```
chet-2500# q
Connection closed by foreign host.
chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.
User Access Verification
Username: chet/restricted
Password:
chet-2500# show kerberos creds
Default Principal:  chet/restricted@CISCO.COM
Valid Starting          Expires                 Service Principal
13-May-1996 15:00:32    13-May-1996 23:01:33    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 3
chet-2500# q
Connection closed by foreign host.
chet-ss20%
```

Encrypted Telnet Session Example

The following example shows how to establish an encrypted Telnet session from a router to a remote host named “host1”:

Router> **telnet host1 /encrypt kerberos**

Additional References

The following sections provide references related to the No Service Password-Recovery feature.

Related Documents

Related Topic	Document Title
Setting, changing, and recovering lost passwords	“ Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices ” feature module
Loading system images and rebooting	“ Using the Cisco IOS Integrated File System ” feature module
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

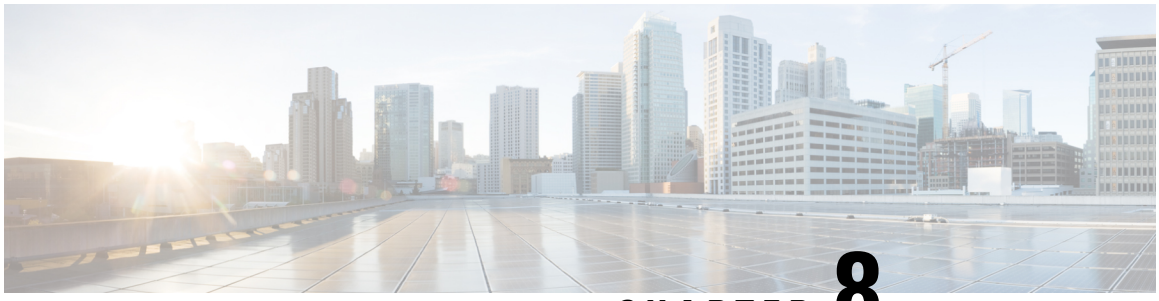
Feature Information for Configuring Kerberos

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 14: Feature Information for Configuring Kerberos

Feature Name	Releases	Feature Information
Encrypted Kerberized Telnet	Cisco IOS XE Release 2.1	With Encrypted Kerberized Telnet, users are authenticated by their Kerberos credentials before a Telnet session is established. The Telnet session is encrypted using 56-bit Data Encryption Standard (DES) encryption with 64-bit Cipher Feedback (CFB). Because data sent or received is encrypted, not clear text, the integrity of the dialed router or access server can be more easily controlled. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **connect**, and **telnet**.
Kerberos V Client Support	Cisco IOS XE Release 2.1	Kerberos 5 support allows organizations already deploying Kerberos 5 to use the same Kerberos authentication database on their routers that they are already using on their other network hosts (such as UNIX servers and PCs). In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 8

Lawful Intercept Architecture

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies (LEA) to provide electronic surveillance as authorized by a judicial or administrative order. The surveillance is performed using wiretaps to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers. The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual using IP sessions.

This document explains LI architecture, including Cisco Service Independent Intercept architecture and PacketCable Lawful Intercept architecture. It also describes the components of the LI feature and provides instructions on how to configure the LI feature in your system.

Before Cisco IOS XE Release 2.5, PPP sessions were tapped based on the accounting session. Circuit-ID based tapping was introduced in Cisco IOS XE Release 2.5.

In Cisco IOS XE Release 2.6, a user session is tapped based on the unique PPP over Ethernet (PPPoE) circuit ID tag. This circuit ID tag serves as a unique parameter for the PPPoE user session on the device. The tapped user session is provisioned through SNMP, and user session data packets and RADIUS authentication data packets are tapped.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Prerequisites for Lawful Intercept

Access to the Cisco LI MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

Communication with Mediation Device

For the router to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:

- The domain name for both the router and the mediation device must be registered in the Domain Name System (DNS).

In DNS, the router IP address is typically the address of the FastEthernet0/0/0 interface on the router.

- The mediation device must have an access function (AF) and an access function provisioning interface (AFPI).
- You must add the mediation device to the Simple Network Management Protocol (SNMP) user group that has access to the CISCO-TAP2-MIB view. Specify the username of the mediation device as the user to add to the group.

When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device's authorization password if you want. The password must be at least eight characters in length.

Restrictions for Lawful Intercept

General Restrictions

There is no command-line interface (CLI) available to configure LI on the router. All error messages are sent to the mediation device as SNMP notifications. All intercepts are provisioned using SNMPv3 only.

Lawful Intercept does not support SUP HA. LI configuration needs to be reapplied after SUP switchover. An SNMP trap will be generated for this event.

Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts are allowed to access the LI MIBs.

Due to its sensitive nature, the Cisco LI MIBs are only available in software images that support the LI feature. These MIBs are not accessible through the Network Management Software MIBs Support page (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml).

SNMP Notifications

SNMP notifications for LI must be sent to User Datagram Protocol (UDP) port 161 on the mediation device, not port 162 (which is the SNMP default).

Information About Lawful Intercept

Introduction to Lawful Intercept

LI is the process by which law enforcement agencies (LEAs) conduct electronic surveillance as authorized by judicial or administrative order. Increasingly, legislation is being adopted and regulations are being enforced that require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance. The types of SPs or ISPs that are subject to LI mandates vary greatly from country to country. LI compliance in the United States is specified by the Commission on Accreditation for Law Enforcement Agencies (CALEA).

Cisco supports two architectures for LI: PacketCable and Service Independent Intercept. The LI components by themselves do not ensure customer compliance with applicable regulations but rather provide tools that can be used by SPs and ISPs to construct an LI-compliant network.

Cisco Service Independent Intercept Architecture

The Cisco Service Independent Intercept Architecture Version 3.0 document describes implementation of LI for VoIP networks using the Cisco BTS 10200 Softswitch call agent, version 5.0, in a non-PacketCable network. Packet Cable Event Message specification version 1.5-I01 is used to deliver the call identifying information along with version 2.0 of the Cisco Tap MIB for call content.

The Cisco Service Independent Intercept Architecture Version 2.0 document describes implementation of LI for VoIP networks using the Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Messages Specification version I08 is still used to deliver call identifying information, along with version 1.0 or version 2.0 of the Cisco Tap MIB for call content. The *Cisco Service Independent Intercept Architecture Version 2.0* document adds additional functionality for doing data intercepts by both IP address and session ID, which are both supported in version 2.0 of the Cisco Tap MIB (CISCO-TAP2-MIB).

The Cisco Service Independent Intercept Architecture Version 1.0 document describes implementation of LI for VoIP networks that are using the Cisco BTS 10200 Softswitch call agent, versions 3.5 and 4.1, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Message Specification version I03 is still used to deliver call identifying information, along with version 1.0 of the Cisco Tap MIB (CISCO-TAP-MIB) for call content. Simple data intercepts by IP address are also discussed.

PacketCable Lawful Intercept Architecture

The P*acketCable Lawful Intercept Architecture for BTS Version 5.0* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, version 5.0, in a PacketCable network that conforms to PacketCable Event Messages Specification version 1.5-I01.

The *PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a PacketCable network that conforms to PacketCable Event Messages Specification version I08.

The PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1 document describes the implementation of LI for voice over IP (VoIP) using Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch call agent, versions 3.5 and 4.1, in a PacketCable network that conforms to PacketCable Event Message Specification version I03.

The *PacketCable Control Point Discovery Interface Specification* document defines an IP-based protocol that can be used to discover a control point for a given IP address. The control point is the place where Quality of Service (QoS) operations, LI content tapping operations, or other operations may be performed.

CISCO ASR 1000 Series Routers

The Cisco ASR 1000 Series Aggregation Services Routers support two types of LI: regular and broadband (per-subscriber). Broadband wiretaps are executed on access subinterfaces and tunnel interfaces. Regular wiretaps are executed on access subinterfaces, tunnel interfaces, and physical interfaces. Wiretaps are not required, and are not executed, on internal interfaces. The router determines which type of wiretap to execute based on the interface that the target's traffic is using.

LI on the Cisco ASR 1000 series routers can intercept traffic based on a combination of one or more of the following fields:

- Destination IP address and mask (IPv4 or IPv6 address)
- Destination port or destination port range
- Source IP address and mask (IPv4 or IPv6 address)
- Source port or source port range
- Protocol ID
- Type of Service (TOS)
- Virtual routing and forwarding (VRF) name, which is translated to a *vrf-tableid* value within the router.
- Subscriber (user) connection ID

The LI implementation on the Cisco ASR 1000 series routers is provisioned using SNMP3 and supports the following functionality:

- RADIUS session intercepts, which can occur in one of the following ways:
  - Interception through Access-Accept packets allows interception to start at the beginning of a session.
  - Interception through CoA-Request packets enables the router to start or stop interception during a session.
- Interception of communication content. The router duplicates each intercepted packet and then places the copy of the packet within a UDP-header encapsulated packet (with a configured CCCid). The router sends the encapsulated packet to the LI mediation device. Even if multiple lawful intercepts are configured on the same data flow, only one copy of the packet is sent to the mediation device. If necessary, the mediation device can duplicate the packet for each LEA.
- Interception of IPv4, IPv4 multicast, IPv6, and IPv6 multicast flows.

VRF Aware LI

VRF Aware LI is the ability to provision a LI wiretap on IPv4 data in a particular Virtual Private Network (VPN). This feature allows a LEA to lawfully intercept targeted data within that VPN. Only IPv4 data within that VPN is subject to the VRF-based LI tap.

VRF Aware LI is available for the following types of traffic:

- ip2ip
- ip2tag (IP to MPLS)
- tag2ip (MPLS to IP)

To provision a VPN-based IPv4 tap, the LI administrative function (running on the mediation device) uses the CISCO-IP-TAP-MIB to identify the name of the VRF table that the targeted VPN uses. The VRF name is used to select the VPN interfaces on which to enable LI in order to execute the tap.

The router determines which traffic to intercept and which mediation device to send the intercepted packets based on the VRF name (along with the source and destination address, source and destination port, and protocol).

Note When using the Cisco-IP-TAP-MIB, if the VRF name is not specified in the stream entry, the global IP routing table is used by default.

Lawful Intercept MIBs

Due to its sensitive nature, the Cisco LI MIBs are only available in software images that support the LI feature. These MIBs are not accessible through the Network Management Software MIBs Support page (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml).

Restricting Access to the Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts should be allowed to access the LI MIBs. To restrict access to these MIBs, you must:

1. Create a view that includes the Cisco LI MIBs.
2. Create an SNMP user group that has read-and-write access to the view. Only users assigned to this user group can access information in the MIBs.
3. Add users to the Cisco LI user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

For more information, see the Creating a Restricted SNMP View of Lawful Intercept MIBs module.

Note Access to the Cisco LI MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

RADIUS-Based Lawful Intercept

A RADIUS-based lawful intercept solution enables intercept requests to be sent (through Access-Accept packets or Change of Authorizationt (CoA)-Request packets) to the network access server (NAS) or to the Layer 2 Tunnel Protocol access concentrator (LAC) from the RADIUS server. All traffic data going to or

from a PPP or L2TP session is passed to a mediation device. Another advantage of RADIUS-based lawful intercept is the synchronicity of the solution—the tap is set with Access-Accept packets so that all target traffic is intercepted.

Intercept requests are initiated by the mediation device via SNMPv3 messages, and all traffic data going to or from a given IP address is passed to a mediation device. Interception based on IP addresses prevents a session from being tapped until an IP address has been assigned to the session.

The RADIUS-based lawful intercept feature provides High Availability (HA) support for LI for the following modes:

- Access-Accept based LI for the new session
- CoA based LI for existing session

The RADIUS-based LI HA supports only the RADIUS based provisioning. The SNMP-based provisioning is not supported.

Intercept Operation

How Intercept Requests Work Within Access-Accept Packets

When an intercept target begins to establish a connection, an Access-Request packet is sent to the RADIUS server. The RADIUS server responds with an Access-Accept packet containing the four RADIUS attributes.

The NAS or the LAC receives the LI-Action attribute with the value 1, allowing the NAS or LAC to duplicate the traffic data at the start of the new session and forward the duplicated data to the mediation device that was specified through the attributes, MD-IP-Address and MD-Port-Number.

Note If the NAS or LAC cannot start intercepting traffic data for a new session, the session does not get established.

If accounting is enabled (through the **aaa accounting network** command and the **aaa accounting send stop-record authentication failure** command), an Accounting-Stop packet must be sent with the Acct-Termination-Cause attribute (49) set to 15, which means that service is not available.

How Intercept Requests Work Within CoA-Request Packets

After a session has been established for the intercept target, CoA-Request packets can be used for the following tasks:

- Starting the interception of an existing session. The LI-Action attribute is set to 1.
- Stopping the interception of an existing session. The LI-Action attribute is set to 0.
- Issuing a dummy intercept request. The LI-Action attribute is set to 2. The NAS or LAC should not perform any session interception; instead, it searches the session on the basis of the Acct-Session-ID attribute value that was specified in the CoA-Request packets. If a session is found, the NAS or LAC sends a CoA acknowledgment (ACK) response to the RADIUS server. If a session is not found, the NAS or LAC issues a “session not found” error message.

In each case, the RADIUS server must send CoA-Request packets with the identified attributes and the Acct-Session-ID attribute. Each of these attributes must be in the packet.

The Acct-Session-ID attribute identifies the session that will be intercepted. The Acct-Session-ID attribute can be obtained from either the Access-Request packet or the Accounting-Stop packet.

When a session is being tapped and the session terminates, the tap stops. The session does not start when the subscriber logs back in unless the Access-Accept indicates a start tap or a CoA-Request is sent to start the session.

Note The frequency of CoA-Request packets should not exceed a rate of one request every 10 minutes.

Service Independent Intercept (SII)

Cisco developed the Service Independent Intercept (SII) architecture in response to requirements that support lawful intercept for service provider customers. The SII architecture offers well-defined, open interfaces between the Cisco equipment acting as the content Intercept Access Point (IAP) and the mediation device. The modular nature of the SII architecture allows the service provider to choose the most appropriate mediation device to meet specific network requirements and regional, standards-based requirements for the interface to the law enforcement collection function.

The mediation device uses SNMPv3 to instruct the call connect (CC) IAP to replicate the CC and send the content to the mediation device. The CC IAP can be either an edge router or a trunking gateway for voice, and either an edge router or an access server for data.

To increase the security and to mitigate any SNMPv3 vulnerability, the following tasks are required:

Restricting Access to Trusted Hosts (without Encryption)

SNMPv3 provides support for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine the security mechanism employed when handling an SNMP packet.

Additionally, the SNMP Support for the Named Access Lists feature adds support for standard named access control lists (ACLs) to several SNMP commands.

To configure a new SNMP group or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in global configuration mode.

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

In this example, the access list named **my-list** allows SNMP traffic only from 10.10.10.1. This access list is then applied to the SNMP group called **my-group**.

Encrypting Lawful Intercept Traffic and Restricting Access to Trusted Hosts

Encryption of intercepted traffic between the router (the content Intercept Access Point (IAP)) and the Mediation Device (MD) is highly recommended.

The following configuration is required:

- Configuring encryption in the router and either an encryption client in the MD or a router associated with the MD to decrypt the traffic.

- Restricting access to trusted hosts.
- Configuring the VPN client.

Configuring encryption in the Router

First configure Authentication, Authorization and Accounting (AAA) parameters. The following example shows how to configure the parameters:

```
aaa authentication login userauthen local
username <username> password 0 <password>
```

The following example uses the internal database; however, external authentication servers can also be specified to perform the authentication.

After configuring the AAA parameters, configure the Internet Security Association and Key Management Protocol (ISAKMP) policy and the crypto map. The following example uses pre-shared keys, Diffie-Hellman (DH) group 2 and AES 256 as the encryption protocol for phase 1 (Internet Key Exchange (IKE)). The crypto map is called dynamic-map and the VPN group is called LI-group. Access-list 108 defines the traffic that is allowed to the router (in this case the ip pool is 10.1.1.1 through 10.1.1.254).

```
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
!
crypto isakmp client configuration group LI-group
key <password>
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
acl 108
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
set transform-set myset
!
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
interface GigabitEthernet0/3
ip address <IP address of LI-enabled router> 255.255.255.0
crypto map clientmap
!
!
ip local pool ippool 10.1.1.1 10.1.1.254
!
!
access-list 108 permit ip  10.1.1.0 0.0.0.255 host 10.0.24.4 <IP address of LI-enabled
router>
```

Restricting Access to Trusted Hosts (with Encryption)

The following example shows how to create an ACL that allows only the IP pool (10.1.1.0/24) for VPN clients, and assign that ACL to the SNMPv3 group.

```
access-list my-list permit ip 10.1.1.0 0.0.0.255
snmp-server group my-group v3 auth access my-list
```

Configuring the VPN Client

```
See the
 Installing the VPN Client
 document to download and configure the Cisco VPN Client for Solaris. See the
Cisco VPN Client installation instructions
 document to download and configure the Cisco VPN Client for other operating systems.
```

How to Configure Lawful Intercept

Although there are no direct user commands to provision lawful intercept on the router, you do need to perform some configuration tasks, such as providing access to LI MIBs, setting up SNMP notifications, and enabling the LI RADIUS session feature. This section describes how to perform the required tasks.

Creating a Restricted SNMP View of Lawful Intercept MIBs

To create and assign users to an SNMP view that includes the Cisco lawful intercept MIBs, perform the steps in this section.

Before you begin

- You must issue the commands in global configuration mode with level-15 access rights.
- SNMPv3 must be configured on the device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **snmp-server view** *view-name MIB-name* **included**
5. **snmp-server view** *view-name MIB-name* **included**
6. **snmp-server view** *view-name MIB-name* **included**
7. **snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name*
8. **snmp-server user** *user-name group-name* **v3 auth md5** *auth-password*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa intercept** **Example:** `Device(config)# aaa intercept`	Enables lawful intercept on the device. • Associate this command with a high administrative security to ensure that unauthorized users cannot stop intercepts if this command is removed. **Note** The **aaa intercept** command is required to set up the wiretap using an IP session.
Step 4	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView ciscoTap2MIB included`	Creates an SNMP view that includes the CISCO-TAP2-MIB (where *exampleView*is the name of the view to create for the MIB). • This MIB is required for both regular and broadband lawful intercept.
Step 5	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	Adds the CISCO-IP-TAP-MIB to the SNMP view.
Step 6	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView cisco802TapMIB included`	Adds the CISCO-802-TAP-MIB to the SNMP view.
Step 7	**snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name* **Example:** `Device(config)# snmp-server group exampleGroup v3 noauth read exampleView write exampleView`	Creates an SNMP user group that has access to the LI MIB view and defines the group's access rights to the view.
Step 8	**snmp-server user** *user-name group-name* **v3 auth md5** *auth-password* **Example:** `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	Adds users to the specified user group.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Where to Go Next

The mediation device can now access the lawful intercept MIBs and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router. To configure the router to send SNMP notification to the mediation device, see the Enabling SNMP Notifications for Lawful Intercept.

Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events. To configure the router to send lawful intercept notifications to the mediation device, perform the steps in this section.

Before you begin

- You must issue the commands in global configuration mode with level-15 access rights.
- SNMPv3 must be configured on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *ip-address* **community-string udp-port** *port notification-type*
4. **snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**
5. **end**

DETAILED STEPS

	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	**snmp-server host** *ip-address* **community-string udp-port** *port notification-type* **Example:**	Specifies the IP address of the mediation device and the password-like community-string that is sent with a notification request.

	Command or Action	Purpose
	`Device(config)# snmp-server 10.2.2.1 community-string udp-port 161 udp`	• For lawful intercept, the **udp-port** must be 161 and not 162 (the SNMP default).
Step 4	**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** **Example:** `Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	Configures the router to send RFC 1157 notifications to the mediation device. • These notifications indicate authentication failures, link status (up or down), and router restarts.
Step 5	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Disabling SNMP Notifications

To disable SNMP notifications on the router, perform the steps in this section.

Note To disable lawful intercept notifications, use SNMPv3 to set the CISCO-TAP2-MIB object cTap2MediationNotificationEnable to false(2). To reenable lawful intercept notifications through SNMPv3, reset the object to true(1).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no snmp-server enable traps**
4. **end**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**no snmp-server enable traps** **Example:** `Device(config)# no snmp-server enable traps`	Disables all SNMP notification types that are available on your system.
Step 4	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Enabling RADIUS Session Intercepts

There are no user CLI commands available to provision the mediation device or taps. However, to enable the intercepts through the CISCO-TAP-MIB you must configure the system to make the account-session-id value available to the mediation device. To enable RADIUS session intercepts on the router, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **aaa authentication ppp default group radius**
5. **aaa accounting delay-start all**
6. **aaa accounting send stop-record authentication failure**
7. **aaa accounting network default start-stop group radius**
8. **radius-server attribute 44 include-in-access-req**
9. **radius-server host** *host-name*
10. **aaa server radius dynamic-author**
11. **client** *ip-address*
12. **domain** {**delimiter** *character*| **stripping [right-to-left]**}
13. **server-key** *word*
14. **port** *port-number*
15. **exit**
16. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa intercept** **Example:** `Device(config)# aaa intercept`	Enables lawful intercept on the router. • Associate this command with a high administrative security to ensure that unauthorized users cannot stop intercepts if this command is removed.
Step 4	**aaa authentication ppp default group radius** **Example:** `Device(config)# aaa authentication ppp default group radius`	Specifies the authentication method to use on the serial interfaces that are running Point-to-Point protocol (PPP). **Note** This command is required because tap information resides only on the RADIUS server. You can authenticate with locally configured information, but you cannot specify a tap with locally configured information.
Step 5	**aaa accounting delay-start all** **Example:** `Device(config)# aaa accounting delay-start all`	Delays the generation of accounting start records until the user IP address is established. Specifying the **all** keyword ensures that the delay applies to all VRF and non-VRF users. **Note** This command is required so that the mediation device can see the IP address assigned to the target.
Step 6	**aaa accounting send stop-record authentication failure** **Example:** `Device(config)# aaa accounting send stop-record authentication failure`	(Optional) Generates accounting stop records for users who fail to authenticate while logging into or during session negotiation. **Note** If a lawful intercept action of 1 does not start the tap, the stop record contains Acct-Termination-Cause, attribute 49, set to 15 (Service Unavailable).
Step 7	**aaa accounting network default start-stop group radius** **Example:** `Device(config)# aaa accounting network default start-stop group radius`	(Optional) Enables accounting for all network-related service requests. **Note** This command is required only to determine the reason why a tap did not start.
Step 8	**radius-server attribute 44 include-in-access-req** **Example:** `Device(config)# radius-server attribute 44 include-in-access-req`	(Optional) Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).

	Command or Action	Purpose
		Note Enter this command to obtain attribute 44 from the Access-Request packet. Otherwise you will have to wait for the accounting packets to be received before you can determine the value of attribute 44.
Step 9	**radius-server host** *host-name* **Example:** `Device(config)# radius-server host host1`	(Optional) Specifies the RADIUS server host.
Step 10	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures a device as an Authentication, Authorization, and Accounting (AAA) server to facilitate interaction with an external policy server and enters dynamic authorization local server configuration mode. **Note** This is an optional command if taps are always started with a session starts. The command is required if CoA-Requests are used to start and stop taps in existing sessions.
Step 11	**client** *ip-address* **Example:** `Device(config-locsvr-da-radius)# client 10.0.0.2`	(Optional) Specifies a RADIUS client from which the device will accept CoA-Request packets.

Step 12	**domain** {**delimiter** *character*| **stripping [right-to-left]**}
	Example:
	`Device(config-locsvr-da-radius)# domain stripping right-to-left`
	Example:
	`Device(config-locsvr-da-radius)# domain delimiter @`
		(Optional) Configures username domain options for the RADIUS application.
		• The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, /, **$**, **%**, \, # or **-**
		• The **stripping** keyword compares the incoming username with the names oriented to the left of the **@** domain delimiter.
		• The **right-to-left** keyword terminates the string at the first delimiter going from right to left.

Step 13	**server-key** *word* **Example:** `Device(config-locsvr-da-radius)# server-key samplekey`	(Optional) Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 14	**port** *port-number* **Example:**	(Optional) Specifies a RADIUS client from which the device will accept CoA-Request packets.

	Command or Action	Purpose
	`Device(config-locsvr-da-radius)# port 1600`	
Step 15	**exit** **Example:** `Device(config-locsvr-da-radius)# exit`	Exits dynamic authorization local server configuration mode and returns to global configuration mode.
Step 16	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Circuit ID Based Tapping

To configure circuit ID based tapping of user session data packets and RADIUS authentication data packets on the router, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber access pppoe unique-key circuit-id**
4. **end**
5. **show pppoe session all**
6. **show idmgr session key circuit-id** *circuit-id*

DETAILED STEPS

	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	**subscriber access pppoe unique-key circuit-id** **Example:** `Device(config)#subscriber access pppoe unique-key circuit-id`	Specifies a unique circuit ID tag for a PPPoE user session to be tapped on the router.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 5	**show pppoe session all** **Example:** `Device# show pppoe session all`	Displays the circuit-id tag in the PPPoE session, which is used in the next step to verify the user session.

Step 6	**show idmgr session key circuit-id** *circuit-id*
	Example:
	`Device# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1`
	Example:
	Example:
	`session-handle = AA000007`
	Example:
	`aaa-unique-id = 0000000E`
	Example:
	`circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1`
	Example:
	`interface = nas-port:0.0.0.0:0/1/1/100`
	Example:
	`authen-status = authen`
	Example:
	`username = user1@cisco.com`
	Example:
	`addr = 106.1.1.3`
	Example:
	`session-guid = 650101020000000E`
	Example:
	`The session hdl AA000007 in the record is valid`
		Verifies the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag.

	Command or Action	Purpose

	Example:
	
	`The session hdl AA000007 in the record is valid`
	Example:
	
	`No service record found`	

Configuration Examples for Lawful Intercept

Example: Enabling Mediation Device Access Lawful Intercept MIBs

The following example shows how to enable the mediation device to access the lawful intercept MIBs. It creates an SNMP view (tapV) that includes four LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```
aaa intercept
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

Example: Enabling RADIUS Session Lawful Intercept

The following example shows the configuration of a RADIUS-Based Lawful Intercept solution on a router acting as a network access server (NAS) device employing an Ethernet PPP connection over Ethernet (PPPoE) link:

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoE-TERMINATE
```

```
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface GigabitEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface GigabitEthernet5/0/0
description To subscriber
no ip address
!
interface GigabitEthernet5/0/0.10
encapsulation dot1q 10
protocol pppoe group PPPoE-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring SNMP Support	*Configuring SNMP Support*
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
PacketCable™ Control Point Discovery Interface Specification	*PacketCable ™ Control Point Discovery Interface Specification* (PKT-SP-CPD-I02-061013)

MIBs

MIB	MIBs Link
• CISCO-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC-2865	*Remote Authentication Dial In User Service (RADIUS)*
RFC-3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC-3924	*Cisco Architecture for Lawful Intercept in IP Networks*

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

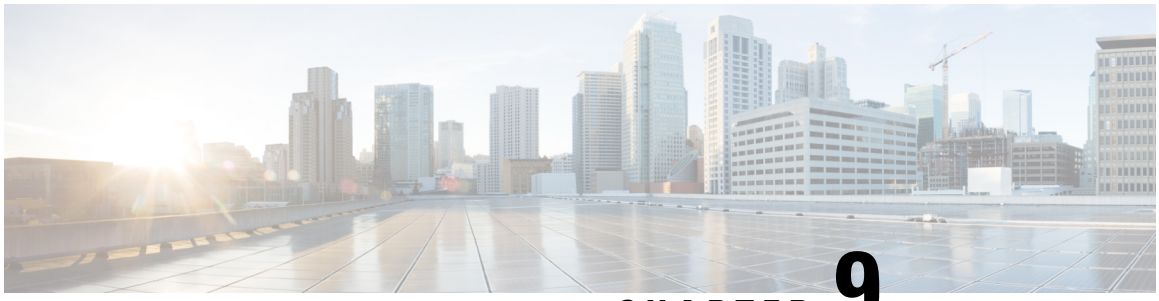
Feature Information for Lawful Intercept

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 15: Feature Information for Lawful Intercept

Feature Name	Releases	Feature Information
Lawful Intercept	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.15S	The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies to provide the ability to intercept VoIP or data traffic going through the edge routers. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. In Cisco IOS XE Release 3.15S, the Lawful Intercept feature was introduced on tunnel interfaces for the Cisco ASR 1000 Series Aggregation Services Routers.
VRF Aware LI (Lawful Intercept)	Cisco IOS XE Release 2.4	VRF Aware LI is the ability to provision a LI wiretap on IPv4 data in a particular Virtual Private Network (VPN). In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
RADIUS-based Lawful Intercept	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.5S	The LI implementation is provisioned using SNMP3 and supports RADIUS session intercepts. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. In Cisco IOS XE Release 3.5, High Availability support was added for RADIUS-Based Lawful Intercept.
Circuit ID based tapping of PPP session for Lawful Intercept.	Cisco IOS XE Release 2.5	In Cisco IOS XE Release 2.5, circuit ID based tapping of a PPP session is introduced. Circuit ID based tapping works only if the tap is provisioned after the user session is active. It is assumed in this instance that the user session is uniquely identified by a circuit ID tag.
Circuit ID based tapping for Lawful Intercept	Cisco IOS XE Release 2.6	In Cisco IOS XE Release 2.6, pre-provisioning of circuit-ID based tapping of a PPP session is introduced. If the tap is provisioned before a user session is active, then the tap is effective whenever the user session becomes active. Also, corresponding RADIUS authentication and accounting packets are tapped. It is assumed in this instance that the user session is uniquely identified by a circuit ID tag.
Non-Lawful Intercept (Non-LI) Images	Cisco IOS XE Release 3.10S	In Cisco IOS XE Release 3.10S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The Non-LI images will be available from Cisco IOS XE Release 3.10S onwards and will not contain the LI subsystems.



CHAPTER 9

LI Support for IPoE Sessions

The LI Support for IPoE Sessions feature extends support for provisioning lawful intercept (LI) to IP over Ethernet (IPoE) sessions in accordance with RFC 2866. This document describes RADIUS-based LI for IPoE. See the "Lawful Intercept Architecture" module for information on LI architecture and components and for configuration tasks and examples.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Restrictions for LI Support for IPoE Sessions

The following restrictions apply to RADIUS-based LI for IPoE sessions:

- You cannot use Access-Accept packets to start TAP for a RADIUS proxy session when the LI parameters are encrypted.
- The **aaa intercept** command must be configured to accept attribute value pairs (AVPs) associated with RADIUS-based LI. The frequency of change of authentication (CoA) requests to start, stop, or no-action, should not exceed a rate of 1 per 10 minutes.
- Intercepted traffic from different users is sent to the same mediation device (MD). You must use a unique stream ID (made up of the first four digits of the eight-digit intercept ID) for each MD.
- The format of intercepted packets captured using RADIUS-based LI include the L2 header; this is different from the format of SNMP-based LI.

- Per-flow tapping is not supported through RADIUS-based LI; it is supported with SNMP-based LI.

Additional References for LI Support for IPoE Sessions

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring SNMP support	*Configuring SNMP Support*
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
PacketCable™ Control Point Discovery Interface Specification	*PacketCable ™ Control Point Discovery Interface Specification* (PKT-SP-CPD-I02-061013)

MIBs

MIB	MIBs Link
• CISCO-IP-TAP-MIB • CISCO-TAP2-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2866	*RADIUS Accounting*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

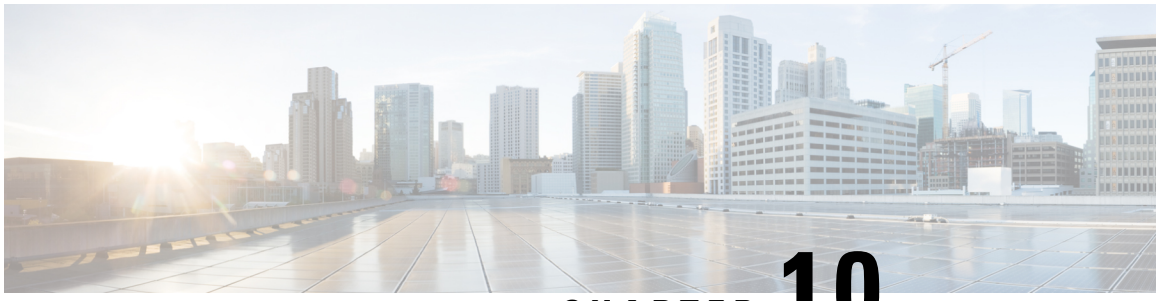
Feature Information for LI Support for IPoE Sessions

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 16: Feature Information for LI Support for IPoE Sessions

Feature Name	Releases	Feature Information
LI Support for IPoE Sessions	Cisco IOS XE Release 3.10S	Extends support for provisioning LI to IPoE sessions in accordance with RFC 2866.



CHAPTER 10

Image Verification

The Image Verification feature allows users to automatically verify the integrity of Cisco IOS XE images and provisioning files. Thus, users can be sure that an image or provisioning file is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Restrictions for Image Verification

Image Verification is applied to and attempted on any file; however, if the file is not an image file or provisioning file, image verification will not occur and you will see the following error, "SIGNATURE-4-NOT_PRESENT."

Note The Image Verification feature can only be used to check the integrity of a Cisco IOS XE software image or provisioning file that is stored on a Cisco IOS XE device. It cannot be used to check the integrity of an image on a remote file system or an image running in memory.

Information About Image Verification

Note Throughout this document, any references to Cisco IOS XE images, also applies to provisioning files.

Benefits of Image Verification

The efficiency of Cisco IOS XE routers is improved because the routers can now automatically detect when the integrity of an image or provisioning file is accidentally corrupted as a result of transmission errors or disk corruption.

How Image Verification Works

Because a production image undergoes a sequence of transfers before it is copied into the memory of a router, the integrity of the image is at risk of accidental corruption every time a transfer occurs. When downloading an image from Cisco.com, a user can run a message-digest5 (MD5) hash on the downloaded image and verify that the MD5 digest posted on Cisco.com is the same as the MD5 digest that is computed on the user's server. However, many users choose not to run an MD5 digest because it is 128-bits long and the verification is manual. Image verification allows the user to automatically validate the integrity of all downloaded images, thereby, significantly reducing user interaction.

How to Use Image Verification

Globally Verifying the Integrity of an Image

The **file verify auto** command enables image verification globally; that is, all images that are to be copied (via the **copy** command) or reloaded (via the **reload** command) are automatically verified. Although both the **copy** and **reload** commands have a **/verify** keyword that enables image verification, you must issue the keyword each time you want to copy or reload an image. The **file verify auto** command enables image verification by default, so you no longer have to specify image verification multiple times.

If you have enabled image verification by default but prefer to disable verification for a specific image copy or reload, the **/noverify** keyword, along with either the **copy** or the **reload** command, will override the **file verify auto** command.

Use this task to enable automatic image verification.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **file verify auto**
4. **exit**

DETAILED STEPS

	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	**file verify auto** **Example:** `Device(config)# file verify auto`	Enables automatic image verification.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode. You must exit global configuration mode if you are going to copy or reload an image.

What to Do Next

After issuing the **file verify auto** command, you do not have to issue the **/verify** keyword with the **copy** or the **reload** command because each image that is copied or reloaded will be automatically verified.

Verifying the Integrity of an Image That Is About to Be Copied

When issuing the **copy** command, you can verify the integrity of the copied file by entering the **/verify** keyword. If the integrity check fails, the copied file will be deleted. If the file that is about to be copied does not have an embedded hash (an old image), you will be prompted whether or not to continue with the copying process. If you choose to continue, the file will be successfully copied; if you choose not to continue, the copied file will be deleted.

Without the **/verify** keyword, the **copy** command could copy a file that is not valid. Thus, after the **copy** command has been successfully executed, you can issue the **verify** command at any time to check the integrity of the files that are in the storage of the router.

Use this task to verify the integrity of an image before it is copied onto a router.

SUMMARY STEPS

1. **enable**
2. **copy** [**/erase**] [**/verify**| **/noverify**] *source-url destination-url*
3. **verify** [**/md5** [*md5-value*]] *filesystem: file-url*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy** [**/erase**] [**/verify**| **/noverify**] *source-url destination-url* **Example:** `Device# copy /verify tftp://10.1.1.1/cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin flash:`	Copies any file from a source to a destination. • **/verify** --Verifies the signature of the destination file. If verification fails, the file will be deleted. • **/noverify** --Does not verify the signature of the destination file before the image is copied. **Note** **/noverify** is often issued if the **file verify auto** command is enabled, which automatically verifies the signature of all images that are copied.
Step 3	**verify** [**/md5** [*md5-value*]] *filesystem: file-url*] **Example:** `Device# flash: tftp://10.1.1.1/cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin flash:`	(Optional) Verifies the integrity of the images in the Device's storage.

Verifying the Integrity of an Image That Is About to Be Reloaded

By issuing the **reload** command with the /**verify** keyword, the image that is about to be loaded onto your system will be checked for integrity. If the /**verify** keyword is specified, image verification will occur before the system initiates the reboot. Thus, if verification fails, the image will not be loaded.

Note Because different platforms obtain the file that is to be loaded in various ways, the file specified in BOOTVAR will be verified. If a file is not specified, the first file on each subsystem will be verified. On certain platforms, because of variables such as the configuration register, the file that is verified may not be the file that is loaded.

Use this task to verify the integrity of an image before it is reloaded onto a router.

SUMMARY STEPS

1. **enable**
2. **reload** [[**warm**] [**/verify**| **/noverify**] *text* | [**warm**] [**/verify**| **/noverify**] **in** [*hh* **:** *mm* [*text*] | [**warm**] [**/verify**| **/noverify**] **at** *hh* **:** *mm* [*month day* | *day month*] [*text*] | [**warm**] [**/verify**| **/noverify**] **cancel**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**reload** [[**warm**] [**/verify**| **/noverify**] *text* | [**warm**] [**/verify**| **/noverify**] **in** [*hh* **:** *mm* [*text*] | [**warm**] [**/verify**| **/noverify**] **at** *hh* **:** *mm* [*month day* | *day month*] [*text*] | [**warm**] [**/verify**| **/noverify**] **cancel**] **Example:** `Device# reload /verify`	Reloads the operating system. • /**verify**--Verifies the signature of the destination file. If verification fails, the file will be deleted. • **/noverify** --Does not verify the signature of the destination file before the image is reloaded. **Note** **/noverify** is often issued if the **file verify auto** command is enabled, which automatically verifies the signature of all images that are copied.

Configuration Examples for Image Verification

Global Image Verification Example

The following example shows how to enable automatic image verification. After enabling this command, image verification will automatically occur for all images that are either copied (via the **copy** command) or reloaded (via the **reload** command).

```
Device(config)# file verify auto
```

Image Verification via the copy Command Example

The following example shows how to specify image verification before copying an image:

```
Device# copy /verify tftp://10.1.1.1/jdoe/c7200-js-mz disk0:
Destination filename [c7200-js-mz]?
Accessing tftp://10.1.1.1/jdoe/c7200-js-mz...
Loading jdoe/c7200-js-mz from 10.1.1.1 (via FastEthernet0/0):!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 19879944 bytes]
19879944 bytes copied in 108.632 secs (183003 bytes/sec)
Verifying file integrity of disk0:/c7200-js-mz
.....................................................................................
.....................................................................................
.....................................................................................
.........................Done!
Embedded Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash       MD5 :CFA258948C4ECE52085DCF428A426DCD
```

```
CCO Hash               MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

Image Verification via the reload Command Example

The following example shows how to specify image verification before reloading an image onto the Device:

```
Device# reload /verify
Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
.....................................................................
.....................................................Done!
Embedded Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash          MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
Proceed with reload? [confirm]n
```

Verify Command Sample Output Example

The following example shows how to specify image verification via the **verify** command:

```
Device# verify disk0:c7200-js-mz
%Filesystem does not support verify operations
Verifying file integrity of disk0:c7200-js-mz.....................................
.....................................................................Done!
Embedded Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash          MD5 :44A7B9BDDD9638128C35528466318183
```

Signature Verified

Additional References

The following sections provide references related to the Image Verification feature.

Related Documents

Related Topic	Document Title
Configuration tasks and information for loading, maintaining, and rebooting system images	Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide
Additional commands for loading, maintaining, and rebooting system images	Cisco IOS Master Command List, All Releases

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	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 IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Image Verification

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 17: Feature Information for Image Verification

Feature Name	Releases	Feature Information
Image Verification		The Image Verification feature allows users to automatically verify the integrity of Cisco IOS XE images. The following commands were introduced or modified: **copy**, **file verify auto**, **reload**, **verify**.