

Using Cisco IOS XE Software

This chapter describes the basics of using the Cisco IOS XE software in autonomous mode and includes the following section:

- Cisco IOS XE software, on page 1

Cisco IOS XE software

Before you begin

Use the console (CON) port to access the command-line interface (CLI) directly or when using Telnet.

This sections describes the main methods of accessing the device:

Procedure

Step 1 Access the CLI using a directly-connected console, on page 1

Step 2 Use SSH to access console, on page 2

Step 3 Access the CLI from a remote console using Telnet, on page 3

Step 4 Access the CLI from a USB serial console port, on page 5

Access the CLI using a directly-connected console

The CON port is an EIA/TIA-232 asynchronous, serial connection with no-flow control and an RJ-45 connector. The CON port is located on the front panel of the chassis.

These sections describe the procedure to access the control interface:

- Connect to the Console Port, on page 2
- Using the Console Interface, on page 2

Connect to the Console Port

Procedure

Step 1 Configure your terminal emulation software with the following settings:

- 9600 bits per second (bps)
- 8 data bits
- No parity
- No flow control

Step 2 Connect to the CON port using the RJ-45-to-RJ-45 cable and the RJ-45-to-DB-25 DTE adapter or the RJ-45-to-DB-9 DTE adapter (labeled Terminal).

Using the Console Interface

Procedure

Step 1 Enter the following command:

```
Router> enable
```

Step 2 (Go to Step 3 if the enable password has not been configured.) At the password prompt, enter your system password:

```
Password: enablepass
```

When your password is accepted, the privileged EXEC mode prompt is displayed.

```
Router#
```

You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 3 If you enter the **setup** command, see "Using Cisco Setup Command Facility" in the "Initial Configuration" section of the Hardware Installation Guide for Cisco 8300 Series Secure Routers.

Step 4 To exit the console session, enter the **quit** command:

```
Router# quit
```

Use SSH to access console

Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. To enable SSH support on the device:

Procedure

Step 1 Configure the hostname:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Here, *host name* is the device hostname or IP address.

Step 2 Configure the DNS domain of the device:

```
Router(config)# ip domain name cisco.com
```

Step 3 Generate an SSH key to be used with SSH:

```
Router(config)#  crypto key generate rsa
The name for the keys will be: Router.xxx.cisco.com Choose the size of the key modulus in the range

of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few
minutes.
How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Router(config)#
```

Step 4 By default, the vtys? transport is Telnet. In this case, Telnet is disabled and only SSH is supported:

```
Router(config)#line vty 0 4
xxx_lab(config-line)#transport input ssh
```

Step 5 Create a username for SSH authentication and enable login authentication:

```
Router(config)# username jsmith privilege 15 secret 0 p@ss3456
Router(config)#line vty 0 4
Router(config-line)# login local
```

Step 6 Verify remote connection to the device using SSH.

Access the CLI from a remote console using Telnet

These topics describe the procedure to access the CLI from a remote console using Telnet:

- Prepare to connect to the device console using Telnet, on page 3
- Telnet to access a console interface, on page 4

Prepare to connect to the device console using Telnet

To access the device remotely using Telnet from a TCP/IP network, configure the device to support virtual terminal lines using the **line vty** global configuration command. Configure the virtual terminal lines to require users to log in and specify a password.

See the Cisco IOS Terminal Services Command Reference document for more information about the line **vty global** configuration command.

To add a line password to the vty, specify a password with the **password** command when you configure the **login** command.

If you are using authentication, authorization, and accounting (AAA), configure the **login authentication** command. To prevent disabling login on a line for AAA authentication when you configure a list with the login authentication command, you must also configure that list using the **aaa authentication login** global configuration command.

For more information about AAA services, see the Cisco IOS XE Security Configuration Guide: Secure Connectivity and the Cisco IOS Security Command Reference documents. For more information about the **login line-configuration** command, see the Cisco IOS Terminal Services Command Reference document.

In addition, before you make a Telnet connection to the device, you must have a valid hostname for the device or have an IP address configured on the device. For more information about the requirements for connecting to the device using Telnet, information about customizing your Telnet services, and using Telnet key sequences, see the Cisco IOS Configuration Fundamentals Configuration Guide.

Telnet to access a console interface

Procedure

Step 1 From your terminal or PC, enter one of these commands:

- **connect host** [*port*] [*keyword*]
- **telnet host** [*port*] [*keyword*]

Here, *host* is the device hostname or IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information about these commands, see the Cisco IOS Terminal Services Command Reference document.

Note
If you are using an access server, specify a valid port number, such as **telnet 198.51.100.2 2004**, in addition to the hostname or IP address.

This example shows how to use the **telnet** command to connect to a device named **router**:

```
unix_host% telnet router
Trying 198.51.100.2...
Connected to 198.51.100.2.
Escape character is '^]'.
unix_host% connect
```

Step 2 Enter your login password:

```
User Access Verification
Password: mypassword
```

Note
If no password has been configured, press **Return**.

Step 3 From user EXEC mode, enter the **enable** command:

```
Router> enable
```

Step 4 At the password prompt, enter your system password:

```
Password: enablepass
```

Step 5 When the **enable** password is accepted, the privileged EXEC mode prompt is displayed:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the Telnet session, use the **exit** or **logout** command.

```
Router# logout
```

Access the CLI from a USB serial console port

The router provides an additional mechanism for configuring the system: a type B miniport USB serial console that supports remote administration of the router using a type B USB-compliant cable. See the "Connecting to a Console Terminal or Modem" section in the Hardware Installation Guide for Cisco 8300 Series Secure Routers.

Use keyboard shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

The table lists the keyboard shortcuts for entering and editing commands.

Table 1: Keyboard shortcuts

Key Name	Purpose
Ctrl-B or the **Left Arrow** key[1]	Move the cursor back one character.
Ctrl-F or the **Right Arrow** key[1]	Move the cursor forward one character.
Ctrl-A	Move the cursor to the beginning of the command line.
Ctrl-E	Move the cursor to the end of the command line.
Esc B	Move the cursor back one word.
Esc F	Move the cursor forward one word.

Use the history buffer to recall commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands.

The table lists the history substitution commands.

Table 2: History substitution commands

Command	Purpose
Ctrl-P or the **Up Arrow** key[1]	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the **Down Arrow** key[1]	Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the **Up Arrow** key.
Router# show history	While in EXEC mode, lists the last few commands you entered.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Understand command modes

The command modes available in Cisco IOS XE are the same as those available in traditional Cisco IOS. This is supported only on the autonomous mode. Use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

The table describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

Table 3: Accessing and exiting command modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** command.	`Router#`	To return to user EXEC mode, use the **disable** command.

Command Mode	Access Method	Prompt	Exit Method
Global configuration	From privileged EXEC mode, use the **configure terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
Diagnostic	The device boots up or accesses diagnostic mode in the following scenarios: • In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the device will reload. • A user-configured access policy is configured using the **transport-map** command that directs a user into diagnostic mode. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) is entered and the device is configured to go to diagnostic mode when the break signal is received.	`Router(diag)#`	If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the device rebooted to get out of diagnostic mode. If the device is in diagnostic mode because of a transport-map configuration, access the device through another port or by using a method that is configured to connect to the Cisco IOS CLI.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon#>`	To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded.

Understand diagnostic mode

The device boots up or accesses diagnostic mode in these scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into the diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the device, and the device was configured to enter diagnostic mode when a break signal was sent.

In the diagnostic mode, a subset of the commands that are available in user EXEC mode are made available to the users. Among other things, these commands can be used to:

- Inspect various states on the device, including the IOS state.
- Replace or roll back the configuration.
- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire device, a module, or possibly other hardware components.
- Transfer files into or off of the device using remote access methods such as FTP, TFTP, and SCP.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous devices, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the device when the device is working normally.

Get help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help that is specific to a command mode, a command, a keyword, or an argument, use one of these commands.

Command	Purpose
`help`	Provides a brief description of the help system in any command mode.
`abbreviated-command-entry?`	Provides a list of commands that begin with a particular character string. **Note** There is no space between the command and the question mark.
`abbreviated-command-entry<Tab>`	Completes a partial command name.

Command	Purpose
`?`	Lists all the commands that are available for a particular command mode.
`command ?`	Lists the keywords or arguments that you must enter next on the command line. **Note** There is a space between the command and the question mark.

Find command options: example

This section provides information about how to display the syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering a part of a command followed by a space. The Cisco IOS XE software displays a list and brief descriptions of the available keywords and arguments. For example, if you are in global configuration mode and want to see all the keywords and arguments for the **arap** command, you should type **arap ?**.

The <cr> symbol in command help output stands for carriage return. On older keyboards, the carriage return key is the **Return** key. On most modern keyboards, the carriage return key is the **Enter** key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available, and that you must press **Enter** to complete the command.

The table shows examples of using the question mark (**?**) to assist you in entering commands.

Table 4: Finding command options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a " # " from the " > ", for example, `Router>` to `Router#`

`Router# configure terminal`
`Enter configuration commands, one per line.`
`End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router (config)#`

Command	Comment

`Router(config)# interface GigabitEthernet ?`
`  <0-1>  GigabitEthernet interface number`
 	
`Router(config)# interface GigabitEthernet 0/?`
`  <0-5>  Port Adapter number`
 	
`Router (config)# interface GigabitEthernet 0/0/?`
 	
`  <0-63>  GigabitEthernet interface number`
 	
`Router (config)# interface GigabitEthernet0/0/1?`
`.  <0-5>`
`Router(config-if)#`
	Enter interface configuration mode by specifying the interface that you want to configure, using the **interface GigabitEthernet** global configuration command.
	
	Enter **?** to display what you must enter next on the command line.
	
	When the <cr> symbol is displayed, you can press **Enter** to complete the command.
	
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  logging  Configure logging for interface`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface MTU`
`  no  Negate a command or set its defaults`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	Enter **?** to display a list of all the interface configuration commands available for the interface. This example shows only some of the available interface configuration commands.

`Router(config-if)# ip ?`
`Interface IP configuration subcommands:`
`  access-group  Specify access control for packets`
`  accounting  Enable IP accounting on this interface`
`  address  Set the IP address of an interface`
`  authentication  authentication subcommands`
`  cgmp  Enable/disable CGMP`
`  dvmrp  DVMRP interface commands`
`  hello-interval  Configures IP-EIGRP hello interval`
`  hold-time  Configures IP-EIGRP hold time`
`  .`
`  .`
`  .`
`Router(config-if)# ip`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	
	Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Command	Comment

Router(config-if)# **ip address ?**
  A.B.C.D IP address
  negotiated IP Address negotiated over PPP
Router(config-if)# **ip address**
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.
	A carriage return (<cr>) is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.

Router(config-if)# ip address 198.51.100.5 ? A.B.C.D IP subnet mask Router(config-if)# **ip address 198.51.100.5**	Enter the keyword or argument that you want to use. This example uses the 198.51.100.5 IP address. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. <cr> is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.
Router(config-if)# **ip address 198.51.100.5 255.255.255.0 ?** secondary Make this IP address a secondary address <cr> Router(config-if)# **ip address 198.51.100.5 255.255.255.0**	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask. Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**. <cr> is displayed. Press **Enter** to complete the command, or enter another keyword.
Router(config-if)# **ip address 198.51.100.5 255.255.255.0** Router(config-if)#	Press **Enter** to complete the command.

How to use the no and default forms of commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Many CLI commands also have a **default** form. By issuing the <*command*> **default** command-name, you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function from a **default** form of the command when the **default** form performs a different function than the plain and **no** forms of the command. To see what default commands are available on your system, enter **default ?** in the appropriate command mode.

Save configuration changes

Use the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It may take a few minutes to save the configuration. After the configuration has been saved, the following output is displayed:

```
[OK]
Router#
```

This task saves the configuration to the NVRAM.

Manage configuration files

The startup configuration file is stored in the nvram: file system and the running configuration files are stored in the system: file system. This configuration file storage setup is also used on several other Cisco router platforms.

As a matter of routine maintenance on any Cisco router, users should back up the startup configuration file by copying the startup configuration file from NVRAM to one of the router's other file systems and, additionally, to a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file if the startup configuration file in NVRAM becomes unusable for any reason.

The **copy** command can be used to back up startup configuration files.

For more detailed information on managing configuration files, see the "Managing Configuration Files" section in the Cisco IOS XE Configuration Fundamentals Configuration Guide.

Filter output from the show and more commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

show *command* | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee**} *regular-expression*

The output matches certain lines of information in the configuration file.

Example

In this example, a modifier of the **show interface** command (**include protocol**) is used to provide only the output lines in which the expression **protocol** is displayed:

Example output for C8375-E-G2:

```
Router# show interface | include protocol
TwoGigabitEthernet0/0/0 is down, line protocol is down
0 unknown protocol drops
TwoGigabitEthernet0/0/1 is up, line protocol is up
0 unknown protocol drops
```

```
TwoGigabitEthernet0/0/2 is down, line protocol is down
0 unknown protocol drops
TwoGigabitEthernet0/0/3 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/4 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/5 is up, line protocol is up
 0 unknown protocol drops
TwoGigabitEthernet0/1/0 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
TwoGigabitEthernet0/1/1 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/2 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/3 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/4 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/5 is down, line protocol is down (notconnect)
 0 unknown protocol drops
TwoGigabitEthernet0/1/6 is up, line protocol is up
0 unknown protocol drops
TwoGigabitEthernet0/1/7 is up, line protocol is up
0 unknown protocol drops
TwoGigabitEthernet0/1/7.10 is up, line protocol is up
GigabitEthernet0 is up, line protocol is up
0 unknown protocol drops
Tunnel0 is up, line protocol is up
Tunnel protocol/transport multi-GRE/IP
0 unknown protocol drops
VirtualPortGroup0 is up, line protocol is up
0 unknown protocol drops
VirtualPortGroup1 is up, line protocol is up
0 unknown protocol drops
VirtualPortGroup10 is up, line protocol is up
0 unknown protocol drops
Vlan1 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
```

Example output for C8355-G2:

```
Router# show interface | include protocol
FiveGigabitEthernet0/0/0 is administratively down, line protocol is down
0 unknown protocol drops
FiveGigabitEthernet0/0/1 is administratively down, line protocol is down
0 unknown protocol drops
FiveGigabitEthernet0/0/2 is administratively down, line protocol is down
0 unknown protocol drops
FiveGigabitEthernet0/0/3 is administratively down, line protocol is down
0 unknown protocol drops
GigabitEthernet0/0/4 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
GigabitEthernet0/0/5 is administratively down, line protocol is down (disabled)
 0 unknown protocol drops
TenGigabitEthernet0/0/6 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
TenGigabitEthernet0/0/7 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
TenGigabitEthernet0/0/8 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/9 is up, line protocol is up
0 unknown protocol drops
GigabitEthernet0 is up, line protocol is up
0 unknown protocol drops
Loopback1 is up, line protocol is up
```

```
0 unknown protocol drops
Loopback2 is up, line protocol is up
0 unknown protocol drops
Loopback3 is up, line protocol is up
0 unknown protocol drops
Tunnel3 is up, line protocol is down
 Tunnel protocol/transport IPSEC/IP
0 unknown protocol drops
Vlan1 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
Vlan10 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
```

Power off a device

The device can be safely turned off at any time by moving the device's power supply switch to the Off position. However, any changes to the running config since the last WRITE of the config to the NVRAM is lost.

Ensure that any configuration needed after startup is saved before powering off the device. The copy running-config startup-config command saves the configuration in NVRAM and after the device is powered up, the device initializes with the saved configuration.

Find support information for platforms and Cisco software images

The Cisco IOS XE software is packaged in feature sets consisting of software images that support specific platforms. The group of feature sets that are available for a specific platform depends on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or see the Release Notes for Cisco 8300 Series Secure Routers.

Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator is a tool that enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To use the navigator tool, an account on Cisco.com is not required.

Software Advisor

Cisco maintains the Software Advisor tool to see if a feature is supported in a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your device. You must be a registered user on Cisco.com to access this tool.

Software Release Notes

See the Release Notes document for Cisco 8300 Series Secure Routers for information about:

- Memory recommendations
- Open and resolved severity 1 and 2 caveats

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in

previous releases. For cumulative feature information, refer to the Cisco Feature Navigator at: https://cfnng.cisco.com/.

CLI session management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that the other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access a router.

- Change the CLI session timeout, on page 15
- Lock a CLI session, on page 15

Information about CLI session management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that each other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access the router.

Change the CLI session timeout

Procedure

Step 1 `configure terminal`

Enters global configuration mode

Step 2 `line console 0`

Step 3 `session-timeout` *`minutes`*

The value of *`minutes`* sets the amount of time that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. Specify a value of 0 for *`minutes`* to disable session timeout.

Step 4 `show line console 0`

Verifies the value to which the session timeout has been set, which is shown as the value for `" Idle Session "`.

Lock a CLI session

Before you begin

To configure a temporary password on a CLI session, use the **lock** command in EXEC mode. Before you can use the **lock** command, you need to configure the line using the **lockable** command. In this example the line is configured as **lockable**, and then the **lock** command is used and a temporary password is assigned.

Procedure

Step 1 `Router# configure terminal`

Enters global configuration mode.

Step 2 Enter the line upon which you want to be able to use the **lock** command.

`Router(config)# line console 0`

Step 3 `Router(config)# lockable`

Enables the line to be locked.

Step 4 `Router(config)# exit`

Step 5 `Router# lock`

The system prompts you for a password, which you must enter twice.

```
Password: <password>
Again: <password>
Locked
```