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:

Access Cisco IOS XE software

Before you begin

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

The following sections describe the main methods of accessing the device:

Access Cisco IOS XE software

Procedure

	Command or Action	Purpose
Step 1	#unique_29	
Step 2	#unique_30	
Step 3	#unique_31	
Step 4	#unique_32	

Console connections

The CON port is an EIA or 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.

This section describes the procedure to access the control interface.

- #unique_34
- #unique_35

Connect to the console port

Use this procedure when you need direct access to device configuration via the console port.

Procedure

Step 1 Configure your terminal emulation software with these settings.

- 9600 bits per second (bps),
- eight data bits,
- no parity, and
- no flow control

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

Your terminal displays the device's console output, allowing direct access to device configuration.

Access the console interface

Use the console interface to directly manage and configure the router.

Follow these steps to access the console interface:

Procedure

Step 1 Enter the following command.

```
Router> enable
```

Step 2 If the enable password has not been configured, proceed to Step 3. Otherwise, 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. Enter the commands to complete your tasks.

Step 3 If you enter the **setup** command, refer to "Using Cisco Setup Command Facility" in the "Initial Configuration" section of the Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platform.

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

```
Router# quit
```

You successfully access and exit the privileged EXEC mode in the console interface.

Access the device console using SSH

Secure Shell is a protocol that provides a secure remote access connection to network devices. To enable SSH support on the device, access the device console using SSH as described in these steps.

Before you begin

Ensure the device is reachable via IP and supports SSH.

Install SSH client software on your management workstation.

Procedure

Step 1 Configure the device host name.

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

Here, *host name* is the device host name 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 for your device.

```
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.

You will establish a secure SSH session to the device console.

Remote CLI access methods

This section provides procedures to access the CLI from a remote console using Telnet.

- Enable console access to the device via Telnet

• Access a console interface using Telnet

Enable console access to the device via Telnet

This section describes the necessary steps and configuration requirements for enabling remote access to a device console using Telnet.

Before you begin

Ensure the device is configured to support remote access using Telnet over a TCP/IP network.

Configure the device's virtual terminal lines with the **line vty** command.

Set the vty lines to require user login and specify a password to secure remote access. For details about the **line vty** command, refer the Cisco IOS Terminal Services Command Reference document.

Use this task to set up remote console access for network management.

Procedure

Step 1 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 on the vty lines.

Step 2 To ensure login is not disabled on the lines when using AAA authentication, configure the list with the **login authentication** command and also define the login list with the **aaa authentication login** 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.

Step 3 Ensure the device has a configured hostname or an IP address before attempting Telnet access.

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

The device is now configured to allow remote console access via Telnet using password or AAA authentication.

Access a console interface using Telnet

Use this procedure when you need to manage a device from your terminal or PC via Telnet.

Follow these steps to access the console interface:

Before you begin

Ensure Telnet is enabled on the device.

Procedure

From your terminal or PC, enter one of the following commands:

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

Here, *host* refers to 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
When you use an access server, specify a valid port number, such as **telnet 198.51.100.2 2004**, in addition to the hostname or IP address.

The following 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
```

You are connected to the console interface of the remote device.

USB serial console ports

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. Refer to the 'Connecting to a Console Terminal or Modem' section for detailed instructions.

- Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platform
- Hardware Installation Guide for Cisco Catalyst 8200 Series Edge Platforms

Keyboard shortcuts

A keyboard shortcut is a key combination or sequence that

- allows commands to be entered without regard to case sensitivity,
- enables the use of abbreviated commands and parameters, and
- requires that abbreviations contain enough unique letters to distinguish them from any other available commands or parameters.

This 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.

History buffer

The history buffer is a CLI feature that:

- stores the last 20 commands you entered,
- enables history substitution so you can access previous commands without retyping them, and
- uses special abbreviated commands to quickly recall and reuse stored entries.

This 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 you are in EXEC mode, lists the last few commands you entered.

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

Command modes

A command mode is a CLI access level that

- determines which IOS XE commands are available,
- secures and isolates different configuration functions, and
- defines the privileges assigned to each user or process within the operating system.

Cisco IOS XE provides the same command modes as traditional Cisco IOS and supports these modes only in autonomous mode. You access Cisco IOS XE software through the CLI, which divides commands into several modes. The commands available to you always depend on your current mode. When you enter a question mark (**?**) at the CLI prompt, you can see a list of commands available in that 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.

This 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>`	Enter the **logout** command.
Privileged EXEC	From user EXEC mode, enter the **enable** command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, enter the **configure terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, enter the **exit** or **end** command.

Command Mode	Access Method	Prompt	Exit Method
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config if)#`	To return to global configuration mode, use the ui command. To return to privileged EXEC mode, enter the **end** command.

Command Mode	Access Method	Prompt	Exit Method
Diagnostic		`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.

Command Mode	Access Method	Prompt	Exit Method
	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		

Command Mode	Access Method	Prompt	Exit Method
	received.		
ROM monitor	From privileged EXEC mode, enter 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.

Diagnostic mode

A diagnostic mode is a device operation state that

- offers a comprehensive user interface for troubleshooting, surpassing the limited access methods of previous devices
- enables diagnosis and troubleshooting of Cisco IOS problems even when the Cisco IOS process is not functioning properly, and
- provides diagnostic commands that are also accessible in privileged EXEC mode when the device is operating normally.

The device enters diagnostic mode in several scenarios. If the IOS process fails, your device might boot into diagnostic mode automatically, or it may reset first based on device configuration. Additionally, if a user-configured access policy uses the **transport-map** command to direct access into diagnostic mode, the device follows this policy. The device also enters diagnostic mode when it receives a break signal (such as **Ctrl-C** or **Ctrl-Shift-6**) during access, provided it is configured to do so in response to the break

Additional reference information

In diagnostic mode, you have have access to a subset of commands from user EXEC mode. These commands allow users 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 to or from the device using remote access methods such as FTP, TFTP, and SCP.

CLI help commands

Use these CLI commands to access help or list available options and arguments.

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. To get help that is specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

Command	Comment
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.
?	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.

Command help options and symbols

The Cisco IOS XE software provides command-line help so you can enter commands accurately.

- Entering a question mark (**?**) at the CLI prompt or after part of a command displays a list of 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 ?**.
- Command help output shows optional or required arguments, along with brief descriptions.
- The **<cr>** symbol indicates that pressing **Enter** will complete the command.
- If **<cr>** appears at the end of help output, all previous options are optional. If **<cr>** is not displayed, further arguments or keywords are required.

- The **<cr>** symbol refers to the carriage return key, which is labeled **Enter** on most modern keyboards. On older keyboards, the carriage return key is the **Return** key.

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 from '>' to '#', for example, 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)#`

`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)#`.

Command	Comment

`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.

Command	Comment

`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.

`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.

Command	Comment

`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.

CLI command forms

A CLI command form is a configuration command variation that:

- typically has a **no** form to disable a function and a standard form to enable or re-enable a function,
- often includes a default form that resets the command to its default setting using the **default** keyword, and
- is fully documented in Cisco IOS Software command reference publications, which explain the syntax and functions of the standard, **no**, and **default** forms.

Additional reference information

The Cisco IOS software command reference publications document the syntax and effects of both the **no** and **default** forms for configuration commands. To see available **default** commands on your system, enter **default ?** in the appropriate command mode.

Note To disable IP routing (which is enabled by default), use the **no ip routing** command.To re-enable IP routing, use the **ip routing** command.

To reset a command to its default setting, use the default command-name syntax.

Save configuration changes

To ensure your configuration changes are retained after a software reload or power outage, you must save the running configuration to the startup configuration. This task writes your current settings to NVRAM, making them persistent across device reboots.

Before you begin

Make sure you have the necessary privileges to execute configuration commands in the CLI.

Follow these steps to save configuration changes:

Procedure

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.

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.

Your configuration changes are saved to NVRAM and retained across device reboots or power loss.

Configuration files

A configuration file is a data file that stores and manages the operational settings of a Cisco router. Key details about configuration file storage and maintenance include:

- The startup configuration file resides in the NVRAM: file system.
- The running configuration files are stored in the system: file system.

- Maintains a consistent storage arrangement across different Cisco router platforms.

Additional reference information

Users should routinely back up the startup configuration file on any Cisco router. Copy the startup configuration file from NVRAM to another file system on the router and to a network server to back it up. TA backup makes it easy for you to recover the startup configuration file if the file in NVRAM becomes unusable.

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

To learn more about managing configuration files, refer the "Managing Configuration Files" section in the Cisco IOS XE Configuration Fundamentals Configuration Guide.

Filtering 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 review large amounts of output or if you want to exclude information that is not relevant.

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:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/1 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/2 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/3 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0 is up, line protocol is up
     0 unknown protocol drops
Loopback0 is up, line protocol is up
     0 unknown protocol drops
```

Save configuration changes before powering off

Ensure you save any configuration changes you want to keep by using the **copy running-config startup-config** command before powering off the device.

If you power off the device by switching the power supply to Off without saving, you will lose any changes made to the running configuration since the last save to NVRAM. When you power the device back on, it loads the configuration stored in NVRAM. Only saved settings are retained after startup.

Cisco software images

The Cisco IOS XE Software is packaged in feature sets consisting of software images that provide the following benefits:

- contains a group of feature sets that are available for a specific platform depends on which Cisco software images are included in a release.
- is distributed in multiple feature sets for various deployment needs, and
- supports designated Cisco platforms.

Additional reference information

To identify which software images are available for a particular platform, or whether a feature is present in a given image, use the Cisco Feature Navigator or see the Release Notes for Cisco IOS XE.

Cisco feature navigators

A Cisco feature navigator is an online tool that

- provides details about platform support for Cisco devices,
- enables you to identify which Cisco IOS XE software images support specific features, and
- facilitates software image and feature set searches without requiring a Cisco.com account.

Additional reference information

To find information about platform support details and software image support, refer to the Cisco Feature Navigator.

Software advisor

The Software advisor tool is a Cisco resource that:

- allows you to check if a feature is supported in a specific Cisco IOS XE release,
- helps you locate the software documentation for a given feature, and
- enables you to verify the minimum software requirements of Cisco IOS XE software based on the hardware installed on your device.

Cisco provides the Software Advisor tool, which is available in the Tools and Resources section.

Release notes

The Release Notes document for Cisco Catalyst 8000 Series Edge Platforms is a release-specific resource that:

- provides memory recommendations for the platform,
- lists open and resolved severity 1 and 2 caveats, and
- focuses on the current release without offering cumulative feature information from previous releases

For cumulative feature information, refer to the Cisco Feature Navigator at http://www.cisco.com/go/cfn/.

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.

Best practice for CLI session management

Follow these best practices to ensure secure and effective CLI session management:

- Configure inactivity timeouts to automatically close idle CLI sessions and enhance security.
- Lock your CLI session to prevent others from making configuration changes at the same time.
- Reserve enough system capacity for CLI session access so that you and other administrators can always access the system, even under high load.

Configure 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. Set 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"`.

The device automatically ends the CLI session after the specified period of inactivity, increasing security by preventing unauthorized access to unattended sessions.

Lock a CLI session

Use this task to lock your CLI session when stepping away, requiring a temporary password for re-entry.

Before you begin

To configure a temporary password on a CLI session, first configure the line using the **lockable** command, and then use the **lock** command in EXEC mode. When the line is configured as **lockable**, you can use the **lock** command to assign a temporary password.

Procedure

Step 1 `Router# configure terminal`

Enters global configuration mode.

Step 2 Enter the line where 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
```

Your CLI session is locked. Accessing the session again requires the temporary password you set.