Administration of Controller

Using the Controller Interface

You can use the controller interface in the following two methods:

Using the Controller GUI

A browser-based GUI is built into each controller.

It allows up to five users to simultaneously browse into the controller HTTP or HTTPS (HTTP + SSL) management pages to configure parameters and monitor the operational status for the controller and its associated access points.

For detailed descriptions of the controller GUI, see the Online Help. To access the online help, click **Help** on the controller GUI.

Note We recommend that you enable the HTTPS interface and disable the HTTP interface to ensure more robust security.

The controller GUI is supported on the following web browsers:

- Microsoft Internet Explorer 11 or a later version (Windows)
- Mozilla Firefox, Version 32 or a later version (Windows, Mac)
- Apple Safari, Version 7 or a later version (Mac)

Note We recommend that you use the controller GUI on a browser loaded with webadmin certificate (third-party certificate). We also recommend that you do not use the controller GUI on a browser loaded with self-signed certificate. Some rendering issues have been observed on Google Chrome (73.0.3675.0 or a later version) with self-signed certificates. For more information, see CSCvp80151.

Guidelines and Restrictions on using Controller GUI

Follow these guidelines when using the controller GUI:

- To view the Main Dashboard that is introduced in Release 8.1.102.0, you must enable JavaScript on the web browser.

Note Ensure that the screen resolution is set to 1280x800 or more. Lesser resolutions are not supported.

- You can use either the service port interface or the management interface to access the GUI.
- The controller may intermittently or fail to respond when there is a high volume of packets destined for the controller's management IP address.
- You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.
- Click **Help** at the top of any page in the GUI to access the online help. You might have to disable your browser's pop-up blocker to view the online help.

Logging On to the GUI

Note Do not configure TACACS+ authentication when the controller is set to use local authentication.

Procedure

Step 1 Enter the controller IP address in your browser's address bar. For a secure connection, enter **`https://ip-address`**. For a less secure connection, enter **`https://ip-address`**.

Step 2 When prompted, enter a valid username and password, and click **OK**.

The **Summary** page is displayed.

Note The administrative username and password that you created in the configuration wizard are case sensitive.

Logging out of the GUI

Procedure

Step 1 Click **Logout** in the top right corner of the page.

Step 2 Click **Close** to complete the log out process and prevent unauthorized users from accessing the controller GUI.

Step 3 When prompted to confirm your decision, click **Yes**.

Using the Controller CLI

A Cisco Wireless solution command-line interface (CLI) is built into each controller. The CLI enables you to use a VT-100 terminal emulation program to locally or remotely configure, monitor, and control individual controllers and its associated lightweight access points. The CLI is a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulation programs to access the controller.

Note We recommend that you do not run two simultaneous CLI operations because this might result in incorrect behavior or incorrect output of the CLI.

Note For more information about specific commands, see the *Cisco Wireless Controller Command Reference* for relevant releases at: https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

Logging on to the Controller CLI

You can access the controller CLI using either of the following methods:

- A direct serial connection to the controller console port
- A remote session over the network using Telnet or SSH through the preconfigured service port or the distribution system ports

For more information about ports and console connection options on controllers, see the relevant controller model's installation guide.

Using a Local Serial Connection

Before you begin

You need these items to connect to the serial port:

- A computer that is running a terminal emulation program such as Putty, SecureCRT, or similar
- A standard Cisco console serial cable with an RJ45 connector

To log on to the controller CLI through the serial port, follow these steps:

Procedure

Step 1 Connect console cable; connect one end of a standard Cisco console serial cable with an RJ45 connector to the controller's console port and the other end to your PC's serial port.

Step 2 Configure terminal emulator program with default settings:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Note The controller serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, run the **config serial baudrate** *value* and **config serial timeout** *value* to make your changes. If you set the serial timeout value to 0, serial sessions never time out.

If you change the console speed to a value other than 9600, the console speed used by controller will be 9600 during boot and will only change upon the completion of boot process. Therefore, we recommend that you do not change the console speed, except as a temporary measure on an as-needed basis.

Step 3 Log on to the CLI—When prompted, enter a valid username and password to log on to the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI displays the root level system prompt:

```
(Cisco Controller) >
```

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Using a Remote Telnet or SSH Connection

Before you begin

You need these items to connect to a controller remotely:

- A PC with network connectivity to either the management IP address, the service port address, or if management is enabled on a dynamic interface of the controller in question
- The IP address of the controller
- A VT-100 terminal emulation program or a DOS shell for the Telnet session

Note

- By default, controllers block Telnet sessions. You must use a local connection to the serial port to enable Telnet sessions.
- The **aes-cbc ciphers** are not supported on controller. The SSH client which is used to log in to the controller should have minimum a non-aes-cbc cipher.
- The controller may intermittently or fail to respond when there is a high volume of packets destined for the controller's management IP address.

Procedure

Step 1 Verify that your VT-100 terminal emulation program or DOS shell interface is configured with these parameters:

- Ethernet address
- Port 23

Step 2 Use the controller IP address to Telnet to the CLI.

Step 3 When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI shows the root level system prompt.

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Logging Out of the CLI

When you finish using the CLI, navigate to the root level and enter the **logout** command. You are prompted to save any changes that you made to the volatile RAM.

Note The CLI automatically logs you out without saving any changes after 5 minutes of inactivity. You can set the automatic logout from 0 (never log out) to 160 minutes using the **config serial timeout** command.

To prevent SSH or Telnet sessions from timing out, run the **config sessions timeout** *0* command.

Navigating the CLI

- When you log into the CLI, you are at the root level. From the root level, you can enter any full command without first navigating to the correct command level.
- If you enter a top-level keyword such as **config**, **debug**, and so on without arguments, you are taken to the submode of that corresponding keyword.

- **Ctrl + Z** or entering **exit** returns the CLI prompt to the default or root level.
- When navigating to the CLI, enter **?** to see additional options available for any given command at the current level.
- You can also enter the space or tab key to complete the current keyword if unambiguous.
- Enter **help** at the root level to see available command line editing options.

The following table lists commands you use to navigate the CLI and to perform common tasks.

Table 1: Commands for CLI Navigation and Common Tasks

Command	Action
help	At the root level, view system wide navigation commands
?	View commands available at the current level
command ?	View parameters for a specific command
exit	Move down one level
Ctrl + Z	Return from any level to the root level
save config	At the root level, save configuration changes from active working RAM to nonvolatile RAM (NVRAM) so they are retained after reboot
reset system	At the root level, reset the controller without logging out
logout	Logs you out of the CLI

Enabling Web and Secure Web Modes

This section provides instructions to enable the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

You can configure web and secure web mode using the controller GUI or CLI.

Note Due to a limitation in RFC-6797 for the HTTP Strict Transport Security (HSTS), when accessing the controller's GUI using the management IP address, HSTS is not honored and fails to redirect from HTTP to HTTPS protocol in the browser. The redirect fails if the controller's GUI was previously accessed using the HTTPS protocol. For more information, see RFC-6797 document.

This section contains the following subsections:

Enabling Web and Secure Web Modes (GUI)

Procedure

Step 1 Choose **Management** > **HTTP-HTTPS**.

The **HTTP-HTTPS Configuration** page is displayed.

Step 2 To enable web mode, which allows users to access the controller GUI using "http://*ip-address*," choose **Enabled** from the **HTTP Access** drop-down list. Otherwise, choose **Disabled**. The default value is Disabled. Web mode is not a secure connection.

Step 3 To enable secure web mode, which allows users to access the controller GUI using "https://*ip-address*," choose **Enabled** from the **HTTPS Access** drop-down list. Otherwise, choose **Disabled**. The default value is Enabled. Secure web mode is a secure connection.

Step 4 In the **Web Session Timeout** field, enter the amount of time, in minutes, before the web session times out due to inactivity. You can enter a value between 10 and 160 minutes (inclusive). The default value is 30 minutes.

Step 5 Click **Apply**.

Step 6 If you enabled secure web mode in Step 3, the controller generates a local web administration SSL certificate and automatically applies it to the GUI. The details of the current certificate appear in the middle of the **HTTP-HTTPS Configuration** page.

Note If desired, you can delete the current certificate by clicking **Delete Certificate** and have the controller generate a new certificate by clicking **Regenerate Certificate**. You have the option to use server side SSL certificate that you can download to controller. If you are using HTTPS, you can use SSC or MIC certificates.

Step 7 Choose **Controller** > **General** to open the **General** page.

Choose one of the following options from the **Web Color Theme** drop-down list:

- **Default**—Configures the default web color theme for the controller GUI.
- **Red**—Configures the web color theme as red for the controller GUI.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Enabling Web and Secure Web Modes (CLI)

Procedure

Step 1 Enable or disable web mode by entering this command:

config network webmode {**enable** | **disable**}

This command allows users to access the controller GUI using "http://*ip-address*." The default value is disabled. Web mode is not a secure connection.

Step 2 Configure the web color theme for the controller GUI by entering this command:

config network webcolor {**default** | **red**}

The default color theme for the controller GUI is enabled. You can change the default color scheme as red using the **red** option. If you are changing the color theme from the controller CLI, you need to reload the controller GUI screen to apply your changes.

Step 3 Enable or disable secure web mode by entering this command:

config network secureweb {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*." The default value is enabled. Secure web mode is a secure connection.

Step 4 Enable or disable secure web mode with increased security by entering this command:

config network secureweb cipher-option high {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*" but only from browsers that support 128-bit (or larger) ciphers. With Release 8.10, this command is, by default, in enabled state.

When high ciphers is enabled, SHA1, SHA256, SHA384 keys continue to be listed and TLSv1.0 is disabled. This is applicable to webauth and webadmin but not for NMSP.

Step 5 Enable or disable SSLv2 for web administration by entering this command:

config network secureweb cipher-option sslv2 {**enable** | **disable**}

If you disable SSLv2, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is disabled.

Step 6 Enable 256 bit ciphers for a SSH session by entering this command:

config network ssh cipher-option high {**enable** | **disable**}

Step 7 [Optional] Disable telnet by entering this command:

config network telnet{**enable** | **disable**}

Step 8 Enable or disable preference for RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) cipher suites (over CBC cipher suites) for web authentication and web administration by entering this command:

config network secureweb cipher-option rc4-preference {**enable** | **disable**}

Step 9 Verify that the controller has generated a certificate by entering this command:

show certificate summary

Information similar to the following appears:

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

Step 10 (Optional) Generate a new certificate by entering this command:

config certificate generate webadmin

After a few seconds, the controller verifies that the certificate has been generated.

Step 11 Save the SSL certificate, key, and secure web password to nonvolatile RAM (NVRAM) so that your changes are retained across reboots by entering this command:

save config

Step 12 Reboot the controller by entering this command:

reset system

Telnet and Secure Shell Sessions

Telnet is a network protocol used to provide access to the controller's CLI. Secure Shell (SSH) is a more secure version of Telnet that uses data encryption and a secure channel for data transfer. You can use the controller GUI or CLI to configure Telnet and SSH sessions.

In Release 8.10.130.0, Cisco Wave 2 APs support the following cipher suites:

- **HMAC:** hmac-sha2-256,hmac-sha2-512
- **KEX:** diffie-hellman-group18-sha512,diffie-hellman-group14-sha1,ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
- **Host Key:** ecdsa-sha2-nistp256, ssh-rsa
- **Ciphers**: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

This section contains the following subsections:

Guidelines and Restrictions on Telnet and Secure Shell Sessions

- When the controller's config paging is disabled and clients running OpenSSH_8.1p1 OpenSSL 1.1.1 library are connected to the controller, you may experience the output display freezing. You may press any key to unfreeze the display.

  We recommend that you use one of the following methods to avoid this situation:

  - Connect using different version of OpenSSH and Open SSL library
  - Use Putty
  - Use Telnet

- After an AP reboots, you need to enable Telnet if it reverts to its default disabled state.
- When the tool **Putty** is used as an SSH client to connect to the controller running versions 8.6 and above, you may observe disconnects from **Putty** when a large output is requested with paging disabled. This is observed when the controller has many configurations and has a high count of APs and clients, or in either of the cases. We recommend that you use alternate SSH clients in such situations.
- In Release 8.6, controllers are migrated from OpenSSH to libssh, and libssh does not support these key exchange (KEX) algorithms: *ecdh-sha2-nistp384* and *ecdh-sha2-nistp521*. Only *ecdh-sha2-nistp256* is supported.

- In Release 8.10.130.0 and later releases, controllers no longer support legacy cipher suites, weak ciphers, MACs and KEXs.

Configuring Telnet and SSH Sessions (GUI)

Procedure

Step 1 Choose **Management** > **Telnet-SSH** to open the **Telnet-SSH Configuration** page.

Step 2 In the **Idle Timeout(minutes)** field, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is from 0 to 160 minutes. A value of 0 indicates no timeout.

Step 3 From the **Maximum Number of Sessions** drop-down list, choose the number of simultaneous Telnet or SSH sessions allowed. The valid range is from 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet or SSH sessions are disallowed.

Step 4 To forcefully close current login sessions, choose **Management** > **User Sessions** and from the CLI session drop-down list, choose **Close**.

Step 5 From the **Allow New Telnet Sessions** drop-down list, choose **Yes** or **No** to allow or disallow new Telnet sessions on the controller. The default value is **No**.

Step 6 From the **Allow New SSH Sessions** drop-down list, choose **Yes** or **No** to allow or disallow new SSH sessions on the controller. The default value is **Yes**.

Step 7 Save your configuration.

What to do next

To see a summary of the Telnet configuration settings, choose **Management** > **Summary**. The **Summary** page that is displayed shows additional Telnet and SSH sessions are permitted.

Configuring Telnet and SSH Sessions (CLI)

Procedure

Step 1 Allow or disallow new Telnet sessions on the controller by entering this command:

config network telnet {**enable** | **disable**}

The default value is disabled.

Step 2 Allow or disallow new SSH sessions on the controller by entering this command:

config network ssh {**enable** | **disable**}

The default value is enabled.

Note Use the **config network ssh cipher-option high** {**enable** | **disable**} command to enable sha2 which is supported in controller.

Step 3 (Optional) Specify the number of minutes that a Telnet session is allowed to remain inactive before being terminated by entering this command:

config sessions timeout *timeout*

The valid range for *timeout* is from 0 to 160 minutes, and the default value is 5 minutes. A value of 0 indicates no timeout.

Step 4 (Optional) Specify the number of simultaneous Telnet or SSH sessions allowed by entering this command:

config sessions maxsessions *session_num*

The valid range *session_num* is from 0 to 5, and the default value is 5 sessions. A value of zero indicates that Telnet or SSH sessions are disallowed.

Step 5 Save your changes by entering this command:

save config

Step 6 You can close all the Telnet or SSH sessions by entering this command:

config loginsession close {*session-id* | *all*}

The *session-id* can be taken from the **show login-session** command.

Managing and Monitoring Remote Telnet and SSH Sessions

Procedure

Step 1 Configure SSH access host-key by entering these commands:

- Generate or regenerate SSH host key by entering this command:

  config network ssh host-key generate

  This command generates a 1024-bit key.

- Use device certificate private key as SSH host key by entering this command:

  config network ssh host-key use-device-certificate-key

  This command generates a 2048-bit key.

Step 2 See the Telnet and SSH configuration settings by entering this command:

show network summary

Information similar to the following is displayed:

```
RF-Network Name............................ TestNetwork1
Web Mode................................... Enable
Secure Web Mode............................ Enable
Secure Web Mode Cipher-Option High......... Disable
Secure Web Mode Cipher-Option SSLv2........ Disable
Secure Shell (ssh)......................... Enable
Telnet..................................... Disable
```

...

Step 3 See the Telnet session configuration settings by entering this command:

show sessions

Information similar to the following is displayed:

```
CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

Step 4 See all active Telnet sessions by entering this command:

show login-session

Information similar to the following is displayed:

```
ID    User Name     Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00 admin   EIA-232  00:00:00      00:19:04
```

Step 5 Clear Telnet or SSH sessions by entering this command:

clear session *session-id*

You can identify the *session-id* by using the **show login-session** command.

Configuring Telnet Privileges for Selected Management Users (GUI)

Using the controller, you can configure Telnet privileges to selected management users. To do this, you must have enabled Telnet privileges at the global level. By default, all management users have Telnet privileges enabled.

Note SSH sessions are not affected by this feature.

Procedure

Step 1 Choose **Management** > **Local Management Users**.

Step 2 On the **Local Management Users** page, check or uncheck the **Telnet Capable** check box for a management user.

Step 3 Save the configuration.

Configuring Telnet Privileges for Selected Management Users (CLI)

Procedure

- Configure Telnet privileges for a selected management user by entering this command:
  config mgmtuser telnet *user-name* {**enable** | **disable**}

Management over Wireless

The management over wireless feature allows you to monitor and configure local controllers using a wireless client. This feature is supported for all management tasks except uploads to and downloads from (transfers to and from) the controller.

This feature blocks wireless management access to the same controller that the wireless client device is currently associated with. It does not prevent management access for a wireless client associated with another controller entirely. To completely block management access to wireless clients based on VLAN and so on, we recommend that you use access control lists (ACLs) or similar mechanism.

Restrictions on Management over Wireless

- Management over Wireless can be disabled only if clients are on central switching.
- Management over Wireless is not supported for FlexConnect local switching clients. However, Management over Wireless works for non-web authentication clients if you have a route to the controller from the FlexConnect site.

This section contains the following subsections:

Enabling Management over Wireless (GUI)

Procedure

Step 1 Choose **Management > Mgmt Via Wireless** to open the **Management Via Wireless** page.

Step 2 Check the **Enable Controller Management to be accessible from Wireless Clients** check box to enable management over wireless for the WLAN or unselect it to disable this feature. By default, it is in disabled state.

Step 3 Save the configuration.

Enabling Management over Wireless (CLI)

Procedure

Step 1 Verify whether the management over wireless interface is enabled or disabled by entering this command:

show network summary

- If disabled: Enable management over wireless by entering this command: **config network mgmt-via-wireless** *enable*
- Otherwise, use a wireless client to associate with an access point connected to the controller that you want to manage.

Step 2 Log into the CLI to verify that you can manage the WLAN using a wireless client by entering this command: **telnet** *wlc-ip-addr CLI-command*

Configuring Management using Dynamic Interfaces (CLI)

Dynamic interface is disabled by default and can be enabled if needed to be also accessible for most or all of management functions. Once enabled, all dynamic interfaces are available for management access to controller. You can use access control lists (ACLs) to limit this access as required.

Procedure

- Enable or disable management using dynamic interfaces by entering this command:

  config network mgmt-via-dynamic-interface {**enable** | **disable**}