Administration of Cisco WLC

HTTP/HTTPS, SSH/Telnet to Cisco WLC

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.

Restrictions on using Controller GUI

Follow these guidelines when using the controller GUI:

- The controller Web UI is compatible with the following web browsers
    - Microsoft Internet Explorer 11 and later versions
    - Mozilla Firefox 32 and later versions
- 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.
- You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled. The default IP address to connect to the service port interface is 192.168.1.1.
- Click **Help** at the top of any page in the GUI to display online help. You might need 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.

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 **http://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. The default username is admin, and the default password is admin.

Logging out of the GUI

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 controllercontroller GUI.

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

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.

Enabling Web and Secure Web Modes (GUI)

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** text box, 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**.

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)

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. The default value is disabled.

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 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 7 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 8 (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 9 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 10 Reboot the controller by entering this command:
reset system

Using the Controller CLI

A Cisco UWN 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 See the Cisco Wireless Controller Command Reference for information about specific commands.

Note If you want to input any strings from the XML configuration into CLI commands, you must enclose the strings in quotation marks.

Logging on to the Controller CLI

You can access the controller CLI using one of the following two methods:

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

Before you log on to the CLI, configure your connectivity and environment variables based on the type of connection you use.

Guidelines and Limitations

On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller's USB console port and the other end of the cable into the PC's USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

See the Telnet and Secure Shell Sessions section for information on enabling Telnet sessions.

Using a Local Serial Connection

Before You Begin

You need these items to connect to the serial port:

- A PC that is running a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip)
- A null-modem serial cable

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

Step 1 Connect one end of a null-modem serial cable to the controller's console port and the other end to your PC's serial port.

Step 2 Start the PC's VT-100 terminal emulation program. Configure the terminal emulation program for these parameters:

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

Note Minimum serial timeout on Controller is 15 seconds instead of 1 minute.

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, enter **config serial baudrate** *baudrate* and **config serial timeout** *timeout* to make your changes. If you enter config serial timeout 0, serial sessions never time out.

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 displays the root level system prompt:

```
#(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.

Using a Remote Ethernet Connection

Before You Begin

You need these items to connect to a controller remotely:

- A PC with access to the controller over the Ethernet network
- 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.

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 displays 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 logout. The system prompts you to save any changes 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.

Navigating the CLI

The CLI is organized into five levels:

- Root Level
- Level 2
- Level 3
- Level 4
- Level 5

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.

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

Command	Action
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

Telnet and Secure Shell Sessions

Information About Telnet and SSH

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.

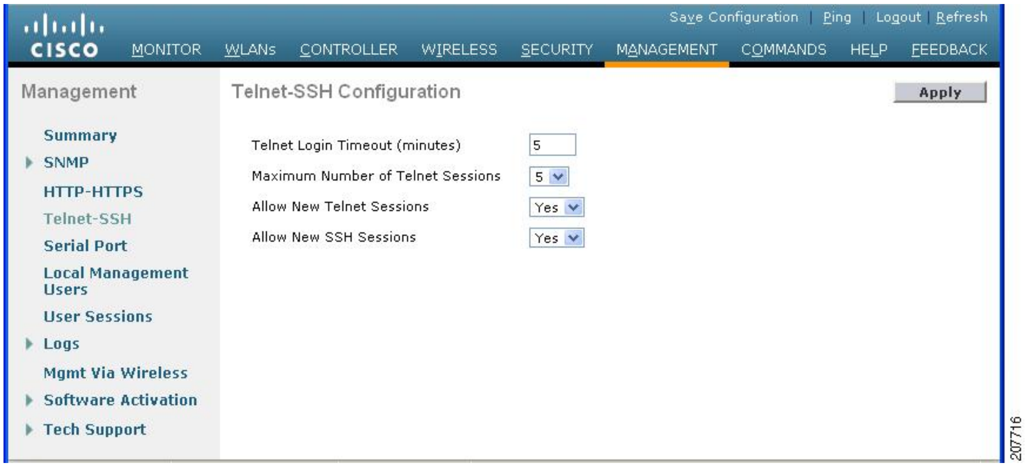
Restrictions on Telnet and SSH

- Only the FIPS approved algorithm aes128-cbc is supported when using SSH to control WLANs.
- The controller does not support raw Telnet mode.

Configuring Telnet and SSH Sessions (GUI)

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

Figure 1: Telnet-SSH Configuration Page



Telnet-SSH Configuration

Telnet Login Timeout (minutes)	5
Maximum Number of Telnet Sessions	5
Allow New Telnet Sessions	Yes
Allow New SSH Sessions	Yes

Step 2 In the **Telnet Login Timeout** text box, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is 0 to 160 minutes (inclusive), and the default value is 5 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 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

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

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.

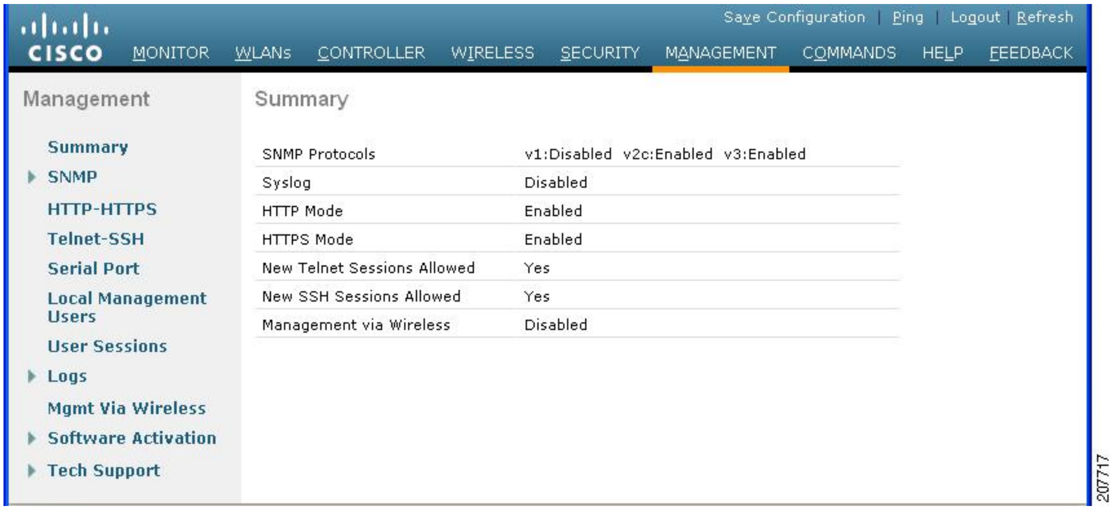
Step 6 From the \ drop-down list, choose **Yes** or **No** to allow or disallow new SSH sessions on the controller. The default value is Yes.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Step 9 To see a summary of the Telnet configuration settings, choose **Management** > **Summary**. The Summary page appears.

Figure 2: Summary Page



Summary

SNMP Protocols	v1:Disabled v2c:Enabled v3:Enabled
Syslog	Disabled
HTTP Mode	Enabled
HTTPS Mode	Enabled
New Telnet Sessions Allowed	Yes
New SSH Sessions Allowed	Yes
Management via Wireless	Disabled

This page shows whether additional Telnet and SSH sessions are permitted.

Note If you are unable to create a new telnet session, close the existing sessions by following the steps:

Configuring Telnet and SSH Sessions (CLI)

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 WLC.

Step 3 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 4 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*

where *timeout* is a value between 0 and 160 minutes (inclusive). The default value is 5 minutes. A value of 0 indicates no timeout.

Step 5 Specify the number of simultaneous Telnet or SSH sessions allowed by entering this command:
config sessions maxsessions *session_num*

where *session_num* is a value between 0 and 5 (inclusive). The default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 6 Save your changes by entering this command:
save config

Step 7 See the Telnet and SSH configuration settings by entering this command:
show network summary

Information similar to the following appears:

```
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 8 See the Telnet session configuration settings by entering this command:
show sessions

Information similar to the following appears:

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

Step 9 See all active Telnet sessions by entering this command:
show login-session

Information similar to the following appears:

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

Step 10 You can clear Telnet or SSH sessions by entering this command:
clear session *session-id*

The *session-id* for the clearing the session should be taken from the **show login-session** command.

Step 11 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.

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.

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

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

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring Telnet Privileges for Selected Management Users (CLI)

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

Management over Wireless

Information About 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.

Restrictions on Management over Wireless

- Management over Wireless can be disabled only if clients are on central switching.

Enabling Management over Wireless (GUI)

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

Step 2 Select 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. The default value is unselected.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Enabling Management over Wireless (CLI)

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 controller-ip-address command

Management by Dynamic Interface

Information About Using Dynamic Interfaces for Management

You can access the controller with one of its dynamic interface IP addresses. Both the wired and wireless clients can access the dynamic interface of the controller using the CLI and GUI. To access the GUI of the controller enter the dynamic interface IP address of the controller in the address field of either Internet Explorer or Mozilla Firefox browser. For wired clients, you must enable management of dynamic interface and must ensure that the wired client is in the VLAN that is mapped to the dynamic interface.

A device, when the management using dynamic interfaces is disabled, can open an SSH connection, if the protocol is enabled. However, you are not prompted to log on. Additionally, the management address remains accessible from a dynamic interface VLAN, unless a CPU ACL is in place. When management using dynamic interface is enabled along with CPU ACL, the CPU ACL has more priority.

The following are some examples of management access and management access using dynamic interfaces, here the management VLAN IP address of the Cisco WLC is 209.165. 201.1 and dynamic VLAN IP address of the Cisco WLC is 209.165. 202.129:

- Source wired client from Cisco WLC's dynamic interface VLAN accesses the management interface VLAN and tries for management access.
- Source wired client from Cisco WLC's management interface VLAN accesses the dynamic interface VLAN and tries for management access.
- Source wired client from Cisco WLC's dynamic interface VLAN accesses the dynamic interface VLAN tries and tries for management access.
- Source wired client from Layer 3 VLAN interface accesses the dynamic interface or the management interface and tries for management access.

Here, management is not the management interface but the configuration access. If the Cisco WLC configuration is accessed from any other IP address on the Cisco WLC other than the management IP, it is management using dynamic interface.

Configuring Management using Dynamic Interfaces (CLI)

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

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