Controller CLI Commands

Cisco Mobility Express CLI

For features supported in a specific Cisco Mobility Express software release, the Cisco Mobility Express controller software supports most commands that are supported by the Cisco WLC in the same Cisco Unified Wireless Network Software Release version. However, there are several commands and procedures which are specific to, or behave differently on, the Cisco Mobility Express controller. These procedures are given in the following sections.

For a complete listing of the commands supported on the Cisco Mobility Express controller CLI, refer to the Cisco Mobility Express Command Reference for the specific release listed at https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html. Cisco Mobility Express only supports the AireOS commands mentioned in this document.

For information on the commands available on the WLC CLI, refer to the Cisco Wireless Controller Command Reference guides for Cisco Unified Wireless Network Software Releases listed at http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

Using the CLI Initial Configuration Wizard

Before you begin

- Connect to the console port of the access point to perform the following procedure.
- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message, such as “Invalid Response,” and returns you to the wizard prompt.
- Press the **hyphen** key if you ever need to return to the previous command line.

Step 1 When prompted to terminate the autoinstall process (the CLI Initial Configuration Wizard), wait for 30 seconds. The CLI Initial Configuration Wizard begins after 30 seconds.

To terminate and exit the process, enter **yes**.

The wizard downloads a configuration file from a TFTP server and then loads the configuration onto the controller automatically.

Step 2 Enter the **Administrative Username** and **Administrative password** to be assigned to this controller. You can enter up to 24 ASCII characters for each.

The following is the password policy:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 3 Enter the **System Name**, which is the name that you want to assign to the controller. You can enter up to 31 ASCII characters.

Step 4 Enter the code for the country in which the Mobility Express network is located.

Note Enter **help** to view the list of available country codes.

Step 5 If you want the controller to receive its time setting from an external Network Time Protocol (NTP) server when it powers up, enter **YES** to configure an NTP server. Otherwise, enter **no**.

If you entered **YES**, then enter the NTP server's IP address.

If you entered **no**, then enter the following to manually set the time and date:

- Enter the date in MM/DD/YY format.
- Enter the time in HH:MM:SS format.

Step 6 Enter the timezone location index to set the timezone. Enter **help** for a list of timezones listed by their indexes.

Step 7 Enter the IP address of the management interface.

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services.

Step 8 Enter the IP address and subnet mask of the management interface.

Step 9 Enter the IP address of the default gateway router.

Step 10 To enable and configure a management DHCP scope, enter **yes**. Otherwise enter **NO**.

If you have entered **YES**, you will need to enter the following:

a. DHCP Network IP address.

b. DHCP Netmask.

c. Router IP address.

d. Start DHCP IP address and Stop DHCP IP address, for the IP address range.

e. Domain Name.

f. Specify whether you want OpenDNS or user DNS.

Step 11 To enable the Employee Network, enter **YES**. Otherwise enter **no**.

If you have entered **YES**, then enter the following:

a. Employee Network Name (SSID)

b. Employee VLAN Identifier (0 = untagged)

c. Employee Network Security. You can enter **PSK** or **enterprise**.

d. If you have entered Employee Network Security as **enterprise**, specify the following:

- RADIUS Server's Address.
- RADIUS Server's Port.
- RADIUS Server's Secret (password).

e. If you have entered Employee Network Security as **PSK**, specify the following:

- Enter PSK Pass phrase (8 to 38 characters).
- Re-Enter PSK Pass phrase (8 to 38 characters).

Step 12 To enable and configure an employee DHCP scope, enter **yes**. Otherwise enter **NO**.

If you have entered **YES**, you will need to enter the following:

a. DHCP Network IP address.

b. DHCP Netmask.

c. Router IP address.

d. Start DHCP IP address and Stop DHCP IP address, for the IP address range.

e. Domain Name.

f. Specify whether you want OpenDNS or user DNS.

Step 13 To enable the Guest Network, enter **YES**. Otherwise enter **no**.

If you have entered **YES**, then enter the following:

a. Guest Network Name (SSID).

b. Guest VLAN Identifier (0 = untagged).

c. Guest Network Security. You can enter **WEB_CONSENT** or **psk**.

d. If you have entered Guest Network Security as **PSK**, specify the following:

- Enter Guest Pass phrase (8 to 38 characters).
- Re-Enter Guest Pass phrase (8 to 38 characters).

Step 14 To enable RF Parameter Optimization, enter **YES**. Otherwise, enter **no**.

If you have entered **YES**, then enter the following:

a. Client Density. You can enter **TYPICAL**, **Low**, or **High**, as per your requirement.

b. Traffic with Voice. You can enter **NO** or **yes**, as per your requirement.

Step 15 When prompted to verify that the configuration is correct, enter **yes** or **NO**.

The controller saves your configuration when you enter **yes**, reboots, and prompts you to log on.

CLI Procedures

Changing the SNMPv3 User Default Values

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMPv3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

Before you begin

SNMPv3 is time sensitive. Ensure that you configure the correct time and time zone on your controller.

Step 1 See the current list of SNMPv3 users for this controller by entering this command:

show snmpv3user

Step 2 If "default" appears in the SNMPv3 User Name column, enter this command to delete this user:

config snmp v3user delete *username*

The *username* parameter is the SNMPv3 username (in this case, "default").

Step 3 Create a new SNMPv3 user by entering this command:

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des | aescfb128**} *auth_key encrypt_key*

where

- *username* is the SNMPv3 username.

- **ro** is read-only mode and **rw** is read-write mode.
- **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options.
- **none**, **des**, and **aescfb128** are the privacy protocol options.
- *auth_key is the authentication shared secret key.*
- *encrypt_key is the encryption shared secret key.*

  Do not enter "default" for the *username*, *auth_key*, and *encrypt_key* parameters.

Step 4 Enter the **save config** command.

Step 5 Reboot the controller so that the SNMPv3 user that you added takes effect by entering **reset system** command.

Configuring 802.11r Fast Transition

Step 1 To enable or disable 802.11r fast transition parameters, use the **config wlan security ft** {**enable** | **disable**} *wlan-id* command.

By default, the fast transition is disabled.

Step 2 To enable or disable 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* command.

By default, the fast transition over a distributed system is disabled.

Step 3 To enable or disable the authentication key management for fast transition using preshared keys (PSK), use the **config wlan security wpa akm ft-psk** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management using PSK is disabled.

Step 4 To enable or disable the authentication key management for fast transition using 802.1X, use the **config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management using 802.1X is disabled.

Step 5 To enable or disable 802.11r fast transition reassociation timeout, use the **config wlan security ft reassociation-timeout** *timeout-in-seconds wlan-id* command.

The valid range is 1 to 100 seconds. The default value of reassociation timeout is 20 seconds.

Step 6 To enable or disable the authentication key management for fast transition over a distributed system, use the **config wlan security wpa akm ft over-the-ds** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management for fast transition over a distributed system is enabled.

Step 7 To view the fast transition configuration on a client, use the **show client detailed** *client-mac* command.

Step 8 To view the fast transition configuration on a WLAN, use the **show wlan** *wlan-id* command.

Step 9 To enable or disable debugging of fast transition events, use the **debug ft events** {**enable** | **disable**} command.

Step 10 To enable or disable debugging of key generation for fast transition, use the **debug ft keys** {**enable** | **disable**} command.

Configuring CDP Timer

Note You cannot set the CDP hold time by configuring it from the controller console on the primary AP. The controller's hold time configuration is ignored since both the controller and internal AP on the Cisco Mobility Express primary AP share the same interface on the switch.

Configuring Cisco Umbrella on Cisco Mobility Express (CLI)

This section describes the procedure to configure Cisco Umbrella on Cisco Mobility Express:

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Step 1 To enable or disable Cisco Umbrella, use the **config opendns** {**enable** | **disable**}

Example:

```
(Cisco Controller) > config opendns enable
```

Enables or disables the Cisco Umbrella global configuration.

Step 2 **config opendns api-token** *api-token*

Example:

```
(Cisco Controller) > config opendns api-token D0986C18DC334FB2E3AA46148D600A4001E5997
```

Registers the Cisco Umbrella API token on the network.

Step 3 **config opendns profile** {**create** | **delete** | **refresh**} *profilename*

Example:

```
(Cisco Controller) > config opendns profile create profile1
```

Creates, deletes, or refreshes a Cisco Umbrella profile that can be applied over a WLAN.

Step 4 **config wlan opendns-profile** *wlan-id profile-name* {**enable** | **disable**}

Example:

```
(Cisco Controller) > config wlan opendns-profile 1 profile-name enable
```

Maps the Cisco Umbrella profile identity to a WLAN.

Step 5 **config wlan opendns-dhcp-opt6** *wlan-id* {**enable** | **disable**}

Example:

```
(Cisco Controller) >config wlan opendns-dhcp-opt6 1 enable
```

Enables or disables DHCP option 6 per WLAN.

Step 6 **config wlan opendns-mode** *wlan-id* {**ignore** | **forced**}

Example:

```
(Cisco Controller) >config wlan opendns-mode 1 forced
```

Ignores or Forces the Cisco Umbrella mode on the WLAN.

Controller CLI Commands