Managing the Network

- Setting the Management Access Interface, page 1
- Managing Administrator Accounts, page 2
- Setting Date and Time, page 4
- Updating the Cisco Mobility Express Software, page 5

Setting the Management Access Interface

The Management Access Interface is the default interface for in-band management of the controller and connectivity to enterprise services. It is also used for communication between the controller and access points (APs). The management interface has the only consistently pingable in-band interface IP address on the controller. You can access the web interface of the controller by entering the management interface IP address of the controller in your browser's address bar.

For APs, the controller requires one management interface to control all inter-controller communications and one AP manager interface to control all controller-to-access point communications, regardless of the number of ports.

To enable or disable the different types of management access to the controller:

Step 1 Choose **Management** > **Access**.
The **Management Access** window is displayed. The number of enabled management types are displayed at the top of the window.

Step 2 You can enable or disable the following types of management access to the controller, by choosing the appropriate option from the drop-down list:

- **HTTP Access—**To enable HTTP access mode, which allows you to access the controller GUI using *http://<ip-address>* through a web browser, choose **Enabled** from the **HTTP Access** drop-down list. Otherwise, choose **Disabled**.

  The default value is **Disabled**.

  Note HTTP access mode is not a secure connection.

- **HTTPs Access—**To enable HTTPS access mode, which allows you to access the controller GUI using *http://ip-address* through a web browser, choose **Enabled** from the **HTTPS Access** drop-down list. Otherwise, choose **Disabled**.

  The default value is **Enabled**.

  Note HTTPs access mode is a secure connection.
- **Telnet Access—**To enable Telnet access mode, which allows remote access to the controller's CLI using your laptop's command prompt, choose **Enabled** from the **Telnet Access** drop-down list. Otherwise, choose **Disabled**.

  The default value is **Disabled**.

  Note Telnet access mode is not a secure connection.
- **SSHv2 Access—**To enable Secure Shell Version 2 (SSHv2) access mode, which is a more secure version of Telnet that uses data encryption and a secure channel for data transfer, choose **Enabled** from the SSHv2 Access drop-down list. Otherwise, choose **Disabled**.

  The default value is **Enabled**.

  Note The SSHv2 access mode is a secure connection.

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

Managing Administrator Accounts

You require administrative (or admin) user accounts for logging in to the controller user interface, for configuring the controller, and for viewing configuration information. This prevents unauthorized users from accessing or configuring the controller.

Adding an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.
The **Admin Accounts** window is displayed, and lists all the admin accounts present on the Cisco Mobility Express controller. The total count of admin accounts on the controller is displayed at the top of the window.

Step 2 Click **Add New User** to add a new admin user.

Step 3 Set the following parameters as required:

- **Account name—**The login user name used by the administrative user. Admin account names must be unique.
- **Access—**Set one of the following access privileges for the administrator:
  - **Read-Only—**This option creates an administrative account with read-only privileges. The admin user can view the controller configuration but cannot make any changes to the configuration.

- **Read-Write—**This option creates an administrative account with read and write privileges. The admin user can view and make changes to the controller configuration.

- **Password—**Enter a password for the administrative user account, based on the following rules:
  - Passwords are case sensitive.
  - The password should contain a minimum of eight characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
  - No character in the password can be repeated more than three times consecutively.
  - The password should not contain the word Cisco or a management username. The password should not be any variant of these words, obtained by reversing the letters of these words, or by changing the capitalization of letters, or by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 4 Click **Apply** to save your changes.

Editing an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.
The **Admin Accounts** page is displayed, along with the list of all the admin accounts present on the Cisco Mobility Express controller. The total count of admin accounts on the controller is displayed at the top of the page.

Step 2 Click the **Edit** icon adjacent to the account you want to edit.

Step 3 Modify the admin account parameters, as required. For descriptions of these parameters, see Adding an Admin Account, on page 2.

Step 4 Click **Apply**.

Deleting an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.
The **Admin Accounts** window is displayed, along with the list of all the admin accounts present on the Cisco Mobility Express controller. The total count of admin accounts on the controller is displayed at the top of the page.

Step 2 Click the Delete icon adjacent to the account you want to delete.

Step 3 Click **Ok** in the confirmation dialog box.

Setting Date and Time

The date and time on the Cisco Mobility Express controller is first set when running the initial configuration setup wizard of the controller. You can either enter the date and time manually or you can specify a Network Time Protocol (NTP) server that sets the time and date.

To change the date and time that has already been set, you should follow either one of the procedures listed below:

- Configuring Date and Time Manually, on page 4
- Specifying an NTP Server to Automatically Set Date and Time, on page 4

Specifying an NTP Server to Automatically Set Date and Time

You can specify a Network Time Protocol (NTP) server, which the controller can use to automatically set the date and time. The synchronization of the date and time with the NTP server will occur every time the controller reboots and at each user-defined polling interval.

Step 1 Choose **Management** > **Time**.
The **Time Settings** window is displayed, with the set time zone shown at the top of the page. The current date and time are displayed in the **Set Time Manually** field.

Step 2 From the **NTP State** drop-down list, choose **Enable**.
Note The current date and time in the**Set Time Manually** field cannot be edited if the **NTP State** is set to **Enable**.

Step 3 In the **NTP Polling Interval** field, specify the polling interval, in seconds.

Step 4 In the **NTP Server** field, enter the server's IPv4 address.

Step 5 Click **Apply**.

Configuring Date and Time Manually

Step 1 Choose **Management** > **Time**.
The **Time Settings** window is displayed, with the set time zone shown at the top of the page. The current date and time are displayed in the **Set Time Manually** field.
Note These fields cannot be edited if the **NTP State** is set to **Enable**.

Step 2 From the **NTP State** drop-down list, choose **Disable**.

Step 3 From the **Time Zone** drop-down list, choose your local time zone.
When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the U.S., DST starts on the second Sunday in March and ends on the first Sunday in November.

Step 4 Select the **Set Time Automatically from Current Location** check box to set the time based on the time zone specified.

Step 5 In the **Set Time Manually** field:

- Click the calendar icon and choose the month, day, and year.
- Click the clock icon and specify the time, in hour and minutes.

Step 6 Click **Apply**.

Updating the Cisco Mobility Express Software

To view the current software version of your Cisco Mobility Express controller:

- Click the gear icon at the top-right corner of the web interface, and then click **System Information**.
- Choose **Management** > **Software Update**.

  This displays the **Software Update** window, with the current software version number displayed at the top.

You can update the Cisco Mobility Express controller software using the controller's web interface. This will prevent the current configurations on the Cisco Mobility Express controller from being deleted.

A software update ensures that both the internal controller software and the AP software on all the associated APs are updated. APs that have older Cisco Mobility Express AP software, on joining the master AP after the software upgrade are automatically upgraded to the latest Cisco Mobility Express AP software. This is because, during the software update process, the latest Cisco Mobility Express software for all Cisco Mobility Express-supported APs that are associated with the controller is also downloaded. An AP joining the controller compares its Cisco Mobility Express software version with that on the master AP and if a mismatch is detected, the new AP requests for a software upgrade. The master AP facilitates the transfer of the new software from the TFTP server to the new AP.

Downloading a newer version of the Cisco Mobility Express software image from the TFTP server to the Cisco Mobility Express network that has to be upgraded can take around 5 minutes per AP. The software download happens in the background, without impacting the network. The upgrades are automatically sequenced to ensure that the network performance is not impacted by software update.

Note Ensure that the TFTP server always has the same Cisco Mobility Express software bundle as that on the Cisco Mobility Express controller, or the latest software bundle.

Guidelines for Preparing a TFTP Server

Follow these guidelines while preparing the TFTP server for hosting the Cisco Mobility Express software file:

- Ensure that the TFTP server supports extended TFTP for file sizes greater than 32 MB. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Cisco Prime Infrastructure.

- If you attempt to download the controller software and your TFTP server does not support files of this size, the following error message appears:

  ```
  TFTP failure while storing in flash.
  ```

- If you are upgrading through the distribution system network port, the TFTP server can be on the same subnet or a different subnet because the distribution system port is routable.

Note Ensure that the TFTP server always has the same Cisco Mobility Express software bundle as that on the Cisco Mobility Express controller, or the latest software bundle.

Performing the Software Update

Before You Begin

- A TFTP server should be configured and accessible. See Guidelines for Preparing a TFTP Server, on page 5.
- A computer that can access Cisco.com and the TFTP server should be available.

Step 1 Get the controller software image by following these steps:

a) Using a computer, browse to the Cisco Download Software page at: http://www.cisco.com/cisco/software/navigator.html.
b) Browse to your AP model and click **Mobility Express Software** to view the list of currently available software, with the latest release at the top.
c) Choose a software release number.
d) Click the filename.
e) Click **Download**.
f) Read Cisco's End User Software License Agreement and then click **Agree**.
g) Save the file to your computer's hard drive.
h) Copy the file from your computer's hard drive and extract them to the default directory on your TFTP server.

Step 2 From the Cisco Mobility Express controller web interface, choose **Management > Software Update**.
The **Software Update** window, with the current software version number, is displayed.

Step 3 In the **IP Address (IPv4)** field, enter the IP address of the TFTP server.

Step 4 In the **File Path** field, enter the TFTP server directory path of the software file, along with the name of the file.

Step 5 Click **Save Tftp Parameters** to save the TFTP parameters that you have specified.
These parameters will remain saved unless you specifically change them in future. You do not have to enter these parameters afresh for the next software update.

Step 6 You can choose to perform the update right away or schedule it for a later time.

- To proceed with the update right away, click **Update Now**. The Preimage Download Section on the page indicates the status of the download. Do not manually power down or reset the controller or any AP during this process;

otherwise, you might corrupt the software image. After the download is complete, click **Restart** to reboot the controller.

- To perform the update at a later time, up to a maximum of 5 days from the current date, specify the later date and time in the **Set Reboot Time** field, and then click **Schedule Later**. After the preimage download is complete, the controller automatically reboots.

For more information on the Preimage Download feature, see Predownloading an Image to an Access Point.

Step 7 Log in to the controller and verify the controller software version in the **Software Update** window.