Managing the Network

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 *https://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.

- **HSTS Mode**—To enable HSTS mode, which allows access to the controller GUI only by using *https://ip-address* through a web browser supporting HTTPS protocol, choose **Enabled** from the **HSTS Mode** drop-down list. Otherwise, choose **Disabled**.

  The default value is **Disabled**.

  Note HSTS mode max-age when enabled is one year.

- **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 Admin Accounts

You can manage the Cisco Mobility Express network through the Cisco Mobility Express controller GUI based on the privileges assigned to your user account. This prevents unauthorized users from accessing or configuring the controller.

You can log in to the Cisco Mobility Express GUI using an admin account having one of the following access types:

- **Read/Write**—This administrative account has complete access to view and modify the controller configuration.

- **Read Only**—This limited access administrative account allows the user to only view the controller configuration. This user is restricted from making any changes to the configuration.

- **Lobby Ambassador**—This restricted administrative account allows the user to only create and manage guest user accounts. The lobby ambassador can also print or email the guest user account credentials.

  For information about creating guest user accounts, see Creating a Guest User Account.

Adding an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.

The total count of admin accounts on the Cisco Mobility Express controller is displayed at the top of this window while the table provides a detailed listing of all the available admin accounts.

The **Admin Accounts** window is displayed.

Step 2 Click **Add New User** to add a new admin user.
A new editable row entry appears in the table.

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**
  - **Read/Write**
  - **Lobby Ambassador**
- **Password**—The password is case sensitive and should be created based on the following guidelines:
  - It should have at least eight characters using a combination of numbers, special characters, as well as upper and lower case letters.
  - It should neither contain the word Cisco or a management username nor be a variant of these words obtained by:
    - Reversing the letters of these words
    - Changing the capitalization of the letters
    - Substituting the following:
      - 1, |, or ! for i
      - 0 for o
      - $ for s
  - No character can be repeated more than three times consecutively in the password.

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 3.

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.

Managing Guest Users using the Lobby Admin account

Guest user accounts are created to allow temporary access to the network. This network access is granted after successful authentication of the guest account credentials.

You can create and manage guest user accounts using the lobby ambassador admin account. To know more about lobby ambassador accounts, see Managing Admin Accounts, on page 2.

Creating a Guest User Account

Before you begin

You need to have at least one lobby ambassador user account before you can create a guest user account. For information about creating a lobby ambassador account, see Adding an Admin Account, on page 3.

Step 1 In your browser, navigate to the Cisco Mobility Express GUI.

Step 2 Login using valid **Lobby Ambassador** credentials.

The **Lobby Ambassador Guest Management** window appears.

Step 3 Click **Add Guest User**.

The **Add Guest User** dialog box appears.

Step 4 Enter the following details for the guest user account:

- **User Name**

- **Wireless Network**—Select the desired guest WLANs that have already been configured for guest access to the network. If no guest WLANs have been cofigured or no guest WLAN is selected, then **All Guest WLANs** is selected by default.

  Note To know more about creating a guest WLAN, see Adding a WLAN.

- **Permanent User**—Select this check box to allow this guest user account access to the network without any time restriction.
- **Expiry Date & Time**—Specify the date and time by clicking the calendar and clock icons respectively. The guest user account gets disabled at the specified date and time preventing access to the guest network.

  Note If the **Permanent User** check box is selected, then this field disappears from the dialog box.

- **Generate Password**—Click this radio button to automatically generate a password for the guest user account being created.

  If you prefer to manually specify a password for the guest user account, enter it in the **Password** and **Confirm Password** fields.

- **Password**

  Note If you have clicked the **Generate Password** radio button, then this field disappears from the dialog box.

- **Confirm Password**—Ensure that this entry matches what you have typed in the **Password** field.
- **Description**

Step 5 Click **Update**.

You can choose to share the account credentials with the guest user either via email or by printing it out.

The **Guest User Credentials** pop-up appears while the **Guest Users List** table refreshes to include this new guest user account entry.

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.

Using NTP Servers to Automatically Set the Date and Time

You can have up to three Network Time Protocol (NTP) servers, to which the controller can automatically sync to set the date and time.

By default three NTP servers are automatically created. The default fully qualified domain names (FQDN) of the NTP servers are:

- 0.ciscome.pool.ntp.org, with NTP Index value 1.
- 1.ciscome.pool.ntp.org, with NTP Index value 2.

- 2.ciscome.pool.ntp.org, with NTP Index value 3.

You can specify the IPv4 address or the FQDN name of an NTP server during the initial configuration wizard. This will be applied to the server having NTP Index 1, thereby overwriting its default FQDN, *0.ciscome.pool.ntp.org* .

For adding and editing NTP server details, go to **Management > Time**. This opens the Time Settings page.

Adding and Editing NTP Servers

You can have up to three Network Time Protocol (NTP) servers, using which the controller can automatically set the date and time.

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. Existing NTP servers, if any, are listed in the order of their **NTP Index** values.

Step 2 In the **NTP Polling Interval** field, specify the polling interval, in seconds.

Step 3 To edit an existing NTP server, click its adjacent **Edit** icon. To add a new NTP server, click **Add NTP Server**.

Step 4 You can add or edit the following values for an NTP server:

a) In the **NTP Index** box, specify an NTP Index value to set the priority of the NTP server. NTP Index values can be set from 1 to 3, in the order of decreasing priority. The controller will try and sync with the NTP server with the highest priority first, until the specified polling interval time runs out. If the sync is successful, the controller does not continue trying to sync with any remaining NTP servers. If the sync is unsuccessful, then the controller will try to sync with the next NTP server.

b) In the **NTP Server** box, specify the IP address or the fully qualified domain name (FQDN) for the NTP server. When you specify an FQDN, a DNS lookup is done. If the lookup fails, an error will be logged in the Syslog server. The controller will continue to resolve this FQDN and errors will be logged until you change the NTP configuration or specify a valid FQDN.

c) Enable the **Apply for APs** option if you want all the APs (both internal and external) to synchronize with the same NTP server that the controller synchronizes with.

- You can set only one NTP server at a time with the *Apply for APs* option. When one NTP server is set with this option, all the other configured NTP servers become redundant and there will be no connection to these redundant servers. There also will not be any NTP server fallback.
- If you enable this option, the NTP service will be restarted at the controller.
- If you are upgrading from a release that does not support the *Apply for APs* option to a release that supports this option, the global NTP server is not set by default with the *Apply for APs* option.
- If you downgrade from a release that supports the *Apply for APs* option to an earlier release that does not support this option, the *Apply for APs* setting is lost after the downgrade.
- In a High Availability scenario, the *Apply for APs* option setting is synchronized with the standby unit.

Step 5 Click **Apply**.

Configuring Global NTP Server (CLI)

Step 1 Set the global NTP server that will be used by the controller to get information about time and sent to external APs by entering this command:

config advanced apgroup-global-ntp add *ntp-server-index*

Step 2 (Optional) Delete the global NTP server by entering this command:

config advanced apgroup-global-ntp delete

Step 3 See information about the global NTP server for an AP or for all APs by entering this command:

show ap ntp-server-info {**all** | *cisco-ap*}

Step 4 See information about the global NTP server configured for AP groups by entering this command:

show advanced apgroup-global-ntp

Refreshing NTP Server Status

The NTP server table on the **Time Settings** page, displays the status of the connection to each NTP server in the **NTP Status** column. The status maybe one of the following:

- **Not Tried**—A sync has not been attempted yet.
- **In Sync**—The controller time is in sync with the NTP server.
- **Not Synched**—The controller time is not in sync with the NTP server.
- **In Progress**—A sync is being attempted.

Click **Refresh** at any time to see the updated NTP statuses.

Deleting and Disabling NTP Servers

To delete an NTP server, choose **Management > Time**. In the **Time Settings** page that is displayed, click the **Delete** icon adjacent the NTP server you want to delete. Click **OK** in the confirmation dialog, and then click **Apply**.

To disable setting the date and time using NTP servers, you will need to delete all configured NTP servers by following the above process.

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. Current configurations on the Cisco Mobility Express controller will not be deleted.

The following table shows the software update methods available.

Table 1: Cisco Mobility Express Software Supported Upgrade Methods

Method	Link to Method
Updating the software using HTTP **Note** This method is possible only if your network consists of only Cisco Aironet 1815, 1830, 1850, 2800, and 3800 access points (which support ap1g4, ap1g5, and ap3g3, images).	See Updating the Software using HTTP, on page 10.
Updating the software using TFTP	See Updating the Software using TFTP, on page 12.
Updating the software using SFTP	See Updating the Software using SFTP, on page 13

Note

- Updating the Cisco Mobility Express software directly from Cisco.com is no longer supported. To update the software, you may use the other methods listed in Table 1: Cisco Mobility Express Software Supported Upgrade Methods, on page 8.
- After restoring the Mobility Express configuration using any one of the download methods, the device reboots to load the downloaded configuration file. To prevent the AP from possibly entering a non-responsive state after restoring the configuration, we recommend that you reboot the device for the second time.

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 primary 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 primary AP and if a mismatch is detected, the new AP requests for a software upgrade. The primary AP facilitates the transfer of the new software from the TFTP server or the HTTP path, to the new 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 The software of up to five access points can be concurrently updated.

Efficient AP Join for Heterogeneous Network

In the Efficient AP Join feature, when a new AP joins the network, the AP downloads the image from the image primary AP instead of downloading from the network file server. When the new AP joins the network, and another AP of the same image type is already present in the network, the new AP downloads the image from the existing AP (image primary). Therefore, the traffic on the WAN network is reduced.

The sequence of the efficient AP join image download, is as follows:

- When a new AP (subordinate AP) joins the Mobility Express (ME) network, ME first checks if the Efficient AP Join feature is enabled, if the AP type is Cisco Wave 2 AP, and if image version is 8.8 or later versions.
- ME sends the primary and subordinate configuration messages to the selected primary. Trigger messages are sent to the subordinate as a response to the join message.
- Thereafter, the subordinate AP contacts the image primary AP to download the image via TFTP. If there is no response from the image primary AP, the subordinate AP continuously sends TFTP requests to the image primary AP and goes back to the discovery mode if the retry count is exceeded.
- If the subordinate AP downloads the image from the image primary successfully, the subordinate AP reboots and joins the ME with the new image.

Note

If the system does not have sufficient memory, the fallback is to stream image from external server down to new AP join.

This fallback is not supported if you have configured the transfer mode as HTTP.

Configuring Efficient AP Join

Before you begin

The Cisco Wireless Release version should be 8.8 or later versions, to support the Efficient AP Join feature.

Step 1 Navigate to **Management** > **Software Update**.

Step 2 Enable the Efficient Join option and click the Apply button.

To enable or disable the efficient join feature, use the command given below. By default, the feature is enabled.

```
(Cisco Controller) > config flexconnect group default-flexgroup efficient-join {enable | disable}
```

Verifying the Status of Efficient AP Join

To verify the status of the efficient AP join feature on ME, use the following **show** command:

```
(Cisco Controller) > show flexconnect group detail default-flexgroup
```

To verify the progress of the download, use the following **show** commands:

```
(Cisco Controller) > show ap image all
```

```
(Cisco Controller) > show flexconnect efficient-upgrade aps
```

Updating the Software using HTTP

Before you begin

You can perform the software update via HTTP only if your network consists of only Cisco Aironet 1815, 1830, 1850, 2800, and 3800 access points (which support ap1g4, ap1g5, and ap3g3, images). If you have other supported AP models in your network, then use TFTP or update directly from Cisco.com.

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

a) Using a computer, browse to the Cisco Download Software page at: https://www.cisco.com/c/en/us/support/wireless/mobility-express/series.html.
b) Choose the AP model to view the currently available software releases under the **Downloads** tab.
c) Choose a software release number.
d) Click **Download** corresponding to the ZIP file.
e) Read Cisco’s End User Software License Agreement and then click **Agree**.
f) Save the ZIP file to your computer's hard drive, and then extract the contents to a directory on your computer.

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 **Transfer Mode** drop-down list, choose **HTTP**.

Step 4 Click the **Browse** button adjacent the **File** field, browse to the folder having the unpacked ZIP file contents, and choose the software file as indicated in the following table.

Cisco AP Series of the Mobility Express Controller	Software File to be Chosen
1830, 1850	ap1g4
1815	ap1g5
2800, 3800	ap3g3

Note The file explorer that opens here is an operating system-specific explorer depending on the OS of your computer.

Step 5 To set the controller to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box.

You can also manually reboot the controller, after the upgrade, by choosing **Advanced** > **Controller Tools**, and clicking **Restart Controller**.

Step 6 Click **Apply** to save the 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 7 Click **Update Now**, and then click **Ok** in the confirmation dialog.

The top section of 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.

The Image Pre-Download Status section of the page shows the status of the pre-image download to the APs in the network.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 8 After the image pre-download is complete, the controller must restart (or reboot) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the controller, after the upgrade, by choosing **Advanced** > **Controller Tools**, and clicking **Restart Controller**.

For more information on the image pre-download feature, see Predownloading an Image to an Access Point.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 9 Log in to the controller and verify the controller software version in the **Software Update** window.

Updating the Software using TFTP

Before you begin

- Prepare a TFTP server, following these guidelines, 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, this 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.
- A computer that can access Cisco.com and the TFTP server, should be available.

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.

See the **Cisco Mobility Express Software Release Information** section in Cisco Mobility Express Release Notes to download the correct AP image bundle.

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

a) Using a computer, browse to the Cisco Mobility Express software download page at: https://www.cisco.com/c/en/us/support/wireless/mobility-express/series.html.
b) Choose the AP model to view the currently available software releases under the **Downloads** tab.
c) Choose a software release number.
d) Click the filename.
e) Click **Download** corresponding to the ZIP file.
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 then unzip and extract the entire contents 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 **Transfer Mode** drop-down list, choose **TFTP**.

Step 4 In the **IP Address (IPv4)** field, enter the IP address of the TFTP server.

Step 5 In the **File Path** field, enter the TFTP server directory path of the software file, along with the name of the file.

Step 6 To set the controller to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box.

You can also manually reboot the controller, after the upgrade, by clicking **Advanced** > **Controller Tools** > **Restart Controller**.

Step 7 Click **Apply** to save the 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 8 You can perform the update right away or schedule it for a later time.

- To proceed with the update right away, click **Update Now**, and then click **Ok** in the confirmation dialog.
- 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 Update Time** field, and then click **Schedule Update**.

The top section of 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.

The Image Pre-Download Status section of the page shows the status of the pre-image download to the APs in the network.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 9 After the image pre-download is complete, the controller must restart (or reboot) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the controller, after the upgrade, click **Advanced** > **Controller Tools** > **Restart Controller**.

For more information on the image pre-download feature, see Predownloading an Image to an Access Point.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 10 Log in to the controller and verify the controller software version in the **Software Update** window.

Updating the Software using SFTP

Software Update through SFTP Transfer Mode works for all Access Points supported in a Cisco Mobility Express Deployment. You would need a SFTP server which can communicate with the Primary Access Point to use this upgrade method. This update method is supported from controller WebUI as well as CLI.

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

a) Using a computer, browse to the Cisco Download Software page.
b) Navigate to the desired AP model and click **Mobility Express Software** to view the list of currently available software, with the latest release at the top.
c) Choose the desired software release number.
d) Click the filename.
e) Click **Download** corresponding to the ZIP file.
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 then unzip and extract the entire contents to the default directory on your SFTP 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 **Transfer Mode** drop-down list, choose **SFTP**.

Step 4 In the **IP Address (IPv4)/Name** field, enter the IP address or the domain name of the SFTP server.

Step 5 In the **Port Number** field, enter the port number. The default is 22.

Step 6 In the **File Path** field, enter the SFTP server directory path of the software file.

Step 7 Enter the username and password to log in to the SFTP server.

Step 8 You can perform the update right away or schedule it for a later time.

- To proceed with the update right away, click **Update**, and then click **Ok** in the confirmation dialog.
- To perform the update at a later time, up to a maximum of 5 days from the current date, click the **Schedule Update** toggle button and specify the later date and time in the **Set Update Time** field.

Step 9 To set the controller to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box.

You can also manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

Step 10 Click **Apply** to save the 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 11 After the image pre-download is complete, the controller must restart (or reboot) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

For more information on the image pre-download feature, see Predownloading an Image to an Access Point.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 12 Log in to the controller and verify the controller software version in the **Software Update** window.

Configuration Management

Configuration Management Enhancements

In Release 8.10, the following configuration management enhancements are available:

- Scheduling of configuration file download: In Release 8.10, you can schedule the download of the configuration file. You can set it for a one-time download or a recurrent download.

  Before Release 8.10, instant download of the configuration file was supported.

  This enhancement has the following options:

  - **One-time download**: You can configure the absolute time for the configuration file download and this configuration is persistent even after the reboot.

  - **Recurrent download**: You can schedule the configuration file to be downloaded recurrently at the following periodic intervals: Hourly, weekly, and monthly.

- FQDN as an option for server address: Before Release 8.10, with the instant download feature, you could configure only IP address as the server address. In Release 8.10, you can configure FQDN also as the server address to download configuration file.
- Restart of the controller after configuration download: Before Release 8.10, after the successful download of configuration file and deployed on ME, you must reboot ME for the new configuration to take effect. This complete boot of ME takes a long time, which increases the downtime of the network. In Release 8.10, instead of rebooting the complete ME platform, only the controller service running on ME is rebooted.
- Roll back to previous configuration in case of errors: If any error is encountered in the process of downloading and deploying the new configuration file, the system automatically rolls back to the previous configuration file.

Guidelines and Restrictions

- You can configure only one download policy, which can be enhanced further.
- You can schedule download of only configuration data type.
- We recommend that you configure download policy with NTP enabled because the manually configured ME system time does not elapse across reboots.

Updating Configuration (GUI)

Step 1 From the Cisco Mobility Express controller web interface, choose **Advanced** > **Controller Tools**.

Step 2 Click the **Configuration Management** tab.

Step 3 From the **Direction** drop-down list, choose to either **Upload** or **Download** the configuration file.

- Upload - Transfers configuration from external source to controller.
- Download - Transfers configuration from controller to external source.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- FTP
- HTTP
- SFTP
- TFTP

Step 5 In the **IP Address(IPv4)/FQDN** box, enter either the IPv4 address of the fully qualified domain name of the server.

Step 6 In the **Port Number** box, specify the port number.

Step 7 In the **File Path** box, enter the path of the configuration file.

Note The following characters are not allowed in the path or the filename: \, :, *, ?, ", <, >, and | are not allowed in the path or file name. Use forward slash '/' as path separator.

Step 8 In the **File Name** box, enter the name of the configuration file.

Step 9 Specify the username and password.

Step 10 Set **Schedule Update** to enabled state to schedule the download of configuration file.

Step 11 Set **Active** to enabled state to enable the scheduling of configuration file download.

Step 12 Set the frequency of configuration file download.

Step 13 Set the day and time at which the configuration file should be downloaded.

Step 14 In the **Schedule Window** box, set the transfer schedule distribution window. Valid range is between 5 to 180 minutes.

Step 15 Click **Apply.**

Updating Configuration (CLI)

Step 1 Create a new download policy or delete an existing one for the download of configuration files by entering this command:

transfer schedule {**create** | **delete**} *policy-name*

Step 2 Activate or deactivate a download policy by entering this command:

transfer schedule {**start** | **stop**} *policy-name*

Step 3 Set various transfer download related parameters to a given profile by entering this command:

transfer schedule parameter *policy-name*

The following parameter options are available:

Parameter	Description
datatype	Sets file type
direction	Sets direction for schedule policy
filename	Sets filename on the server
mode	Sets transfer mode
password	Sets server login password
path	Sets file path on the server
port	Changes default server port
serverIP	Sets server IP address or FQDN
tftpMaxRetries	Maximum number of TFTP packet retries allowed. Valid range is between 1 and 254
tftpPktTimeout	TFTP packet timeout in terms of seconds. Valid range is between 1 and 254
username	Sets server login user name

Parameter	Description
window	Sets transfer schedule distribution window
frequency	Sets frequency for the download policy. Options include hourly, daily, weekly, and monthly

Step 4 See a summary of scheduled policies which includes policy name, datatype and schedule status by entering this command:

show transfer-schedule summary

Step 5 See detailed information of a download policy by entering this command:

show transfer-schedule detailed *policy-name*