Managing the Cisco Mobility Express Deployment

- Managing Access Points, on page 1
- Adding Access Points to Mobility Express Network , on page 3
- Optimal Join, on page 4
- Configuring SFTP or TFTP for AP Join, on page 5
- Configuring Cisco.com for AP Join, on page 5
- Configuring Access Point as 802.1x Supplicant, on page 6
- Configuring RF Profiles, on page 6
- Configuring Management Access , on page 9
- Managing Admin Accounts , on page 9
- Managing TACACS+ and RADIUS Servers, on page 10
- Managing TIME on Cisco Mobility Express, on page 13
- Updating Cisco Mobility Express Software, on page 13
- CALEA Support, on page 22

Managing Access Points

Starting Release 8.4, Cisco Mobility Express supports up to 100 Access Points. To view the list or modify parameters on an Access Points, follow the procedure below:

Procedure

Step 1 Navigate to **Wireless Settings** > **Access Points**.

Note The first Access Point with the **P** icon is the Primary AP and the rest of them are Subordinate Access Points.

Step 2 To modify the parameters on an access point, click on the **Edit** button. The Access Point window will come up displaying the General parameters about the Access Point.

- Operating Mode(Read only field)-For a Primary AP, this field displays AP & Controller. For other associated APs, this field displays AP only.

- AP Mac(Read only field)–Displays the MAC address of the Access Point.
- AP Model(Read only field)-Displays the model details of the Access Point.
- IP Configuration–Choose Obtain from DHCP to allow the IP address of the AP be assigned by a DHCP server on the network, or choose Static IP address. If you choose Static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields.
- AP Name–Edit the name of access point. This is a free text field.
- Location–Edit the location for the access point. This is a free text field.

Step 3 Under the **Controller** tab (Available only for Primary AP), one can modify the following parameters:

- System Name–Enter the System Name for Mobility Express
- IP Address–IP address decides the login URL to the controller's web interface. The URL is in https://<ip address> format. If you change this IP address, the login URL also changes.
- Subnet Mask–Enter the Subnet Mask.
- Country Code–Enter the Country Code.

Step 4 Under Radio 1 (2.4 GHz) and Radio 2 (5 GHz), one can edit the following parameters:

- Admin Mode–Enabled/Disabled. This enables or disables the corresponding radio on the AP (2.4 GHz for 802.11 b/g/n or 5 Ghz for 802.11 a/n/ac).
- Channel–Default is Automatic. Automatic enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the Mobility Express controller. This prevents neighboring APs from broadcasting over the same channel and hence prevents interference and other communication problems. For the 2.4GHz radio, 11 channels are offered in the US, up to 14 in other parts of the world, but only 1-6-11 can be considered non-overlapping if they are used by neighboring APs. For the 5GHz radio, up to 23 non-overlapping channels are offered. Assigning a specific value statically assigns a channel to that AP.
  - 802.11 b/g/n–1 to 11.
  - 802.11 a/n/ac –40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165.
- Channel Width - 20 MHz for 2.4GHz and for 20, 40 and 80 for 5 GHz.
- Transmit Power - 1 to 8. The default value is Automatic.

This is a logarithmic scale of the transmit power, that is the transmission energy used by the AP, 1 being the highest,2 being half of it, 3 being 1/4th and so on. Selecting Automatic adjusts the radio transmitter output power based on the varying signal level at the receiver. This allows the transmitter to operate at less than maximum power for most of the time; when fading conditions occur, transmit power will be increased as needed until the maximum is reached.

Step 5 Click **Apply**.

Adding Access Points to Mobility Express Network

When adding Access Points to Cisco Mobility Express network, the following have to be considered:

Software Version on the Access Point - If the software code of the access point, which is being added, is different than what is on the Primary AP, software download of the code running on the Primary AP has to happen on the Access Point being added. For the new Access Point to download the code that is running on the Primary AP, one of the following has to be configured:

- Optimal Join–Optimal Join is a feature which enables downloading of the code from the Primary AP if the if the AP being added is of the same AP model as the Primary AP. For this feature, you do not need any external server to host the code running on the Primary AP.

Note This feature is supported on 2800, 3800 and 1560 series Access Points.

- SFTP or TFTP server details and the Access Point images path information has to be configured on the Software Update page.
- If the Primary AP has 8.3.102.0 or later code, one can configure the Cisco.com login credentials on the Software Update page and the code on the new Access Point will be automatically downloaded from cisco.com when an Access Point joins.

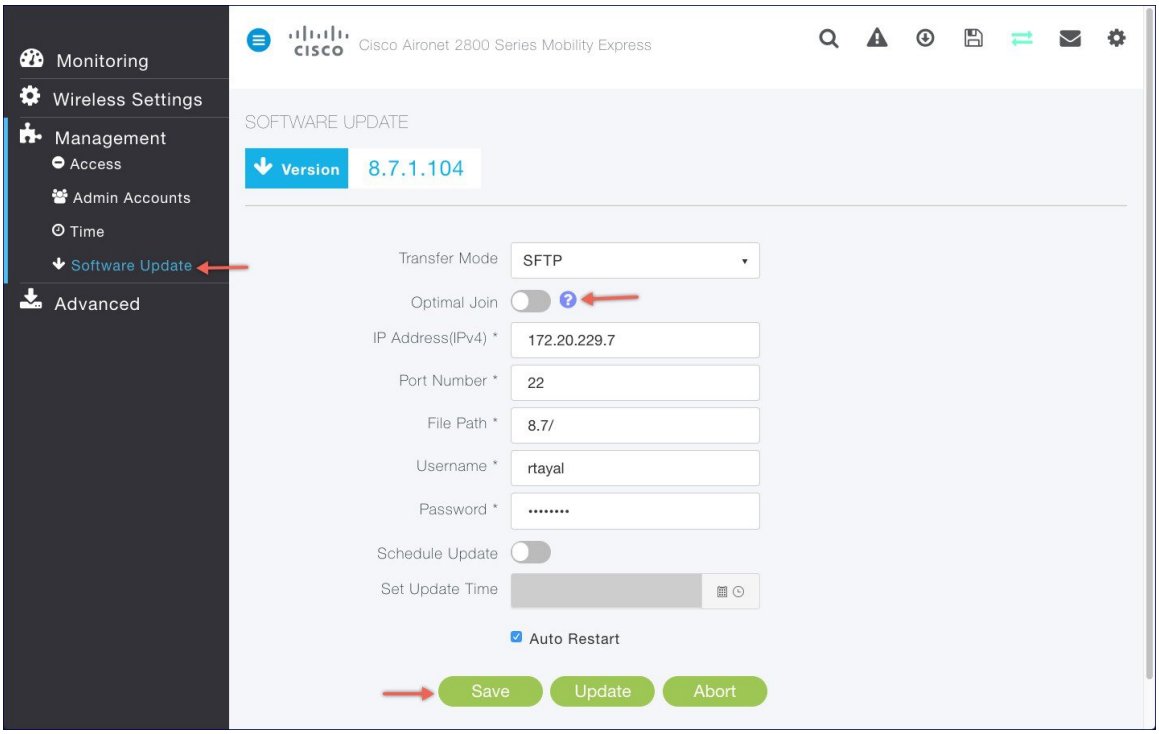
Note For Software download to take place directly from Cisco.com, Primary AP should be the one with the SMARTNet Contract.

Optimal Join–To enable Optimal join, follow the procedure below-

Procedure

Step 1 Navigate to **Management** > **Software Update**. Select **TFTP or SFTP** for **Transfer Mode** and configure the SFTP or TFTP Parameters.

Step 2 Enable **Optimal Join** as shown below.



Step 3 Click **Save**.

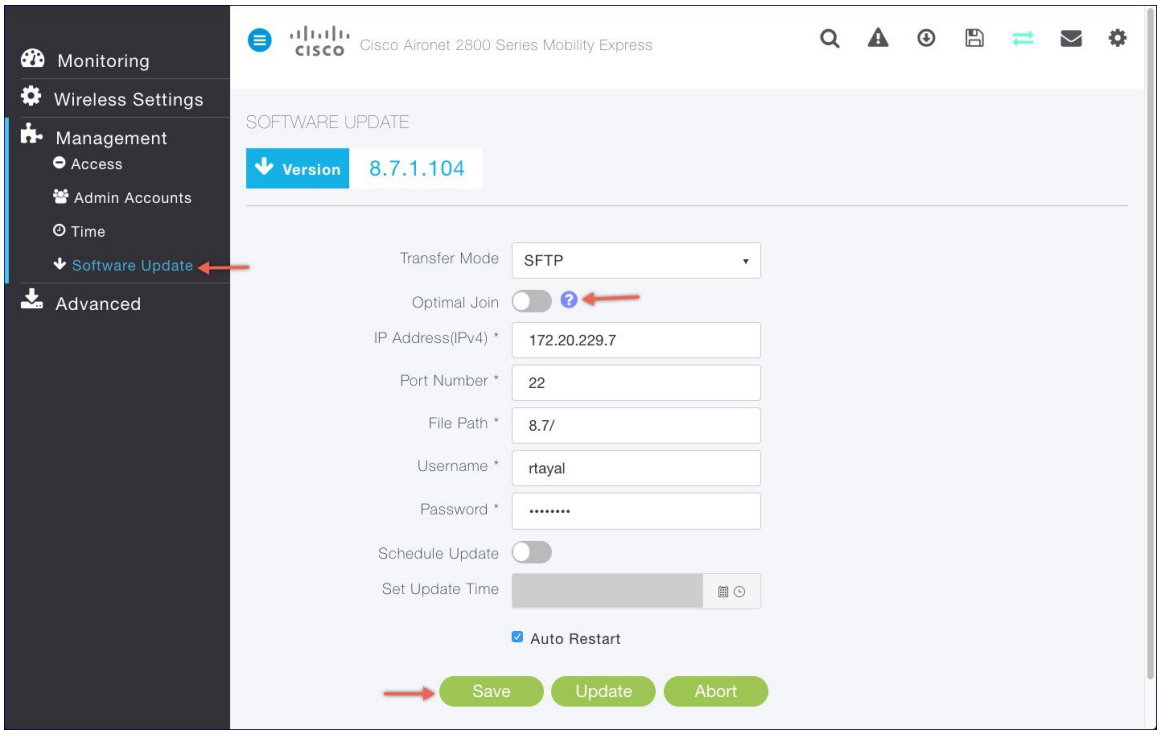
Optimal Join

To enable Optimal join, follow the procedure below:

Procedure

Step 1 Navigate to **Management > Software Update**. Select **TFTP or SFTP** for **Transfer Mode** and configure the SFTP or TFTP Parameters.

Step 2 Enable **Optimal Join** as shown below.



Step 3 Click **Save**.

Configuring SFTP or TFTP for AP Join

Procedure

Step 1 Download the Access Point image zip file from cisco.com on a TFTP server. The bundle version must be the same as the one running on the Primary AP. Unzip the file to extract the individual Access Point images.

Step 2 Navigate to **Management > Software Update**. Select **SFTP** or **TFTP** for **Transfer Mode** and configure the SFTP or TFTP Parameters.

Configuring Cisco.com for AP Join

Procedure

Navigate to **Management > Software Update**. Select **Cisco.com** as the **Transfer Mode** and configure parameters related to the Cisco.com user account.

Note During the image download, there is no service interruption. After the image download is complete, the AP automatically re-boots and join the Primary AP.

Configuring Access Point as 802.1x Supplicant

Starting AireOS Release 8.7, one can configure Access Points running Cisco Mobility Express as a 802.1x supplicant. Mobility Express APs can act as the 802.1x supplicant and is authenticated by the switch against the ISE that using EAP-FAST, and EAP-TLS and PEAP. Once the port is configured for 802.1x authentication, the switch does not allow any traffic other than 802.1x traffic to pass through the port until the device connected to the port authenticates successfully. An AP can be authenticated either before it joins the ME-WLC or after it has joined an ME-WLC, in which case you configure 802.1x on the switch after the Access Point joins the WLC.

Procedure

Step 1 Navigate to **Wireless Settings > Access Points.**

Step 2 Click on the **Global AP Configuration** button and configure the following under the **Credentials(802.1x)** tab:

- **Username**
- **Password**
- **Enable Password**

Step 3 Select **EAP Method and LSC AP Auth State.**

Step 4 Click **Apply**.

Configuring RF Profiles

Starting AireOS Release 8.6, Cisco Mobility Express will support six pre-built RF Profiles as well as creation of RF Profiles.

RF Profiles allows you to tune groups of APs that share a common coverage zone together and selectively change how RRM will operates the APs within that coverage zone. For example, a university might deploy a high density of APs in an area where a high number of users will congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage. Using RF profiles and AP groups allows you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for the 802.11 radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings. The RF profile gives you the control over the data rates and power (TPC) values. One can either associate a build in RF Profile with AP Groups or create a new RF Profile and then associate that with the AP Group.

Configuring RF Profiles

To configure RF Profiles, enable ***Expert View*** on Cisco Mobility Express. ***Expert View*** is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view.

Procedure

Step 1 Navigate to **Advanced** > **RF Profiles**

Step 2 Click on the **Add new RF Profile** button.

Step 3 Under the **General** tab, configure the following:

- RF Profile Name
- RF Profile Description
- Band
- Maximum clients per radio
- RxSOP Threshold
- Multicast datarates

Step 4 Under the 802.11 tab, configure the following:

- Data rates
- MCS Settings

Step 5 Under the RRM tab, configure the following:

- Channel Width
- Select DCS Channels

Step 6 Under the Client Distribution tab, configure the following:

- Window (0 to 20 clients)
- Denial (1 to 10)

Configuring Access Point Groups

To configure AP Groups, enable **Expert View** on Cisco Mobility Express. **Expert View** is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view.

Procedure

Step 1 Navigate to **Wireless Settings > Access Point Groups**.

Step 2 Click on the **Add new group button**.

Step 3 Under the **General** tab, configure the following:

- **AP Group Name**
- **AP Group Description**
- **NAS-ID (Optional**
- **Venue Group (Optional)**
- **Venue Type (Optional**

Step 4 Under the **WLANs** tab, click on the **Add WLAN** button to add the WLAN to the AP Group

Step 5 Under the **Access Points** tab, select the Access Points which must be added to the AP Group

Step 6 Under the **RF Profiles** tab, select the RF Profile for 2.4 and 5.0 GHz band. The RF Profile will be applied to this AP Group.

Step 7 Click **Apply**.

Configuring Access Point Groups

Starting AireOS Release 8.6, Cisco Mobility Express will support upto 100 AP Groups depending on model of the AP running the Wireless controller function.

AP Group is a logical grouping of Access Points in the wireless network. AP Groups enable location based services i.e. if you want to broadcast an SSID on a set of Access Points and a another SSID on different set of Access Points, you can do so by creating AP Groups and adding the Access Points accordingly.

Note Maximum of 50 AP Groups are supported on Mobility Express and a maximum of 100 APs can be added to a single AP Group.

Configuring Management Access

The Management Access Interface on the Mobility Express controller is the default interface for in-band management of the controller and connectivity to enterprise services. It is also used for communications between the controller and access points.

There are four types of Management Access supported on the Mobility Express controller.

1. **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. HTTP access mode is not a secure connection.
2. **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. HTTPS access mode is a secure connection.
3. **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. The Telnet access mode is not a secure connection.
4. **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. The SSHv2 access mode is a secure connection.

To enable or disable the different types of management access to the controller, follow the procedure below:

Procedure

Step 1 Navigate to **Management** > **Access**.

Step 2 For the various Access Types, select either **Enabled** or **Disabled**.

Note There must be at least one access enabled else admin user will locked out of Mobility Express Controller and will have to use console to make changes to provide access again.

Step 3 Click **Apply** to submit changes.

Managing Admin Accounts

Cisco Mobility Express Cisco Mobility Express supports creation of admin accounts to prevent unauthorized users from reconfiguring the controller and viewing configuration. It supports the following three access levels for Admin user accounts:

1. Read/Write–Accounts with read and write privilege have full provisioning and monitoring capability
2. Read only–Accounts with Read only privilege only have monitoring capability and can browse all screens
3. Lobby Ambassador–A Lobby Ambassador can create and manage guest user accounts on the Cisco Mobility Express. The lobby ambassador has limited configuration privileges and can access only the web pages used to manage the guest accounts.

Note The local user database is limited to a maximum of 2048 entries, which is also the default value. This database is shared by local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries. Together they cannot exceed the maximum value.

To create admin users, follow the procedure below:

Procedure

Step 1 Navigate to **Management** > **Admin Accounts** and click on the **Add New User** button.

Step 2 Enter the following to configure the admin user account.

- **Account Name**–Enter the admin user name. Username is case-sensitive and can contain up to 24 ASCII characters. Username cannot contain spaces and must be unique.
- **Access** - Select Read/Write, Read Only or Lobby Ambassador access for the admin account.
- **New Password & Confirm Password** - Enter a password for the admin user account, in-keeping with the following rules:
  - Passwords are case sensitive and cannot contain spaces
  - The password should contain a minimum of 8 characters from ALL of the following classes:
    - Lowercase letters
    - Uppercase letters
    - Digits
    - 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 also 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 3 Click **tick** icon.

Managing TACACS+ and RADIUS Servers

Starting Release 8.5, Cisco Mobility Express will support up to Six RADIUS and Three TACACS Servers. To configure RADIUS and TACACS+ Servers, enable **Expert View** on Cisco Mobility Express. **Expert View** is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view.

Adding TACACS+ Servers

Procedure

Step 1 Navigate to **Management** > **Admin Accounts.**

Step 2 To add TACACS+ servers, click on TACACS+ tab. Click on the **Add TACACS+ Authentication Server** button and enter the following:

- Server Index–Select 1 through 3
- State–Enable the state
- Server IP Address–Enter the IPv4 address of the TACACS+ server
- Shared Secret–Enter the shared secret
- Port Number–Enter the port number being used for communicating with the TACACS+ server
- Server Timeout–Enter the server timeout

Step 3 Do the same of the RAIDUS Authorization Servers.

Adding RADIUS Servers

Procedure

Step 1 Navigate to **Management > Admin Accounts.**

Step 2 To add RADIUS servers, click on RADIUS tab. Click on the **Add RADIUS Authentication Server** button and enter the following:

- Server Index–Select 1 thru 6
- State–Enable the state
- Server IP Address–Enter the IPv4 address of the RADIUS server
- Shared Secret–Enter the shared secret
- Port Number–Enter the port number being used for communicating with the RADIUS server
- Server Timeout–Enter the server timeout

Step 3 Do the same of the RAIDUS Authorization Servers.

Configuring AP SSH Credentials

On Cisco Mobility Express, AP SSH credentials are configured as controller credentials by default. To change the AP SSH credentials on all the APs, follow the procedure below.

Procedure

Step 1 Navigate to **Wireless Settings > Access Points.**

Step 2 Click on the **Global AP Configuration** button and configure the following under the Credentials(SSH) tab:

- **Username**
- **Password**
- **Enable Password**

Step 3 Click **Apply**.

Managing Admin User Priority

Prior to Release 8.5, admin accounts on Cisco Mobility Express were created locally on the controller. In Release 8.5 TACACS+ and RADIUS servers can also be used for authentication admin users.

When multiple databases are configured, it is important to configure the admin account user priority. To configure the priority, follow the Procedure below.

Procedure

Step 1 Enable **Expert View** on Cisco Mobility Express. **Expert View** is available on the top banner of the Cisco Mobility Express WebUI as shown below and enables various configurable parameters which are not available in Standard view.

Step 2 Navigate to **Management** > **Admin Accounts** and click on the **Management User Priority Order**.

Note By default, the local database is always queried first. If the username is not found, the controller switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default setting is local and then RADIUS.

Step 3 To change the priority, between TACACS+ and RADIUS, click on either and move UP or DOWN. Please note Local Admin Accounts cannot be moved to Priority 3. It can only be either 1 or 2.

Managing TIME on Cisco Mobility Express

The system date and time on the Cisco Mobility Express controller is typically configured when running the initial Wireless Express setup wizard.

Configuring NTP Server

Up to three Network Time Protocol (NTP) servers can be configured to sync date and time if one was not configured during the Wireless Express setup. Time Zone can be configured to offset the clock.

To configure Time Zone and NTP servers, follow the procedure below:

Procedure

Step 1 Navigate to **Management** > **Time**.

Step 2 Choose the desired **Time Zone** .

Step 3 Enter the **NTP Polling Interval**. The polling interval ranges from 3600 to 604800 seconds.

Step 4 To add an NTP server, click **Add NTP Server** button and configure the following:

- **NTP Index**–It can be 1, 2 or 3.
- **NTP Server** - This can be the NTP Server IP address, NTP Server Name or pool. A maximum of three NTP Servers are supported.
- Click **tick** icon.

Note Synchronization of the date and time with the NTP Server occurs each time the controller reboots and at each user-defined polling interval.

Updating Cisco Mobility Express Software

Cisco Mobility Express controller software update can be performed using the controller's web interface. Software update ensures that both the controller software and all the Access Points associated are updated.

An AP joining the controller compares its software version with the Primary AP version and incase of mismatch, the new AP requests for a software update. For software update, one must configure the **Transfer Mode** and corresponding details on the Software Update page.

Note Primary AP does not have AP images. It facilitates the transfer of new software from the configured **Transfer Mode** to the Access Points requesting for Software Update.

Software download on the Access Points is automatically sequenced to ensure that not more than 5 APs are downloading the software simultaneously and the queue refreshes till all the Access Points requiring upgrade have downloaded the new image.

Cisco Mobility Express supports the following **Transfer Mode** for Software Update:

1. Cisco.com
2. HTTP
3. SFTP
4. TFTP

Note There is no service interruption during pre-image download. After pre-image download is complete on all APs, a Manual or scheduled reboot of Mobility Express network can be triggered.

Software Update using cisco.com Transfer Mode

Software Update via Cisco.com works for all Access Points supported in a Cisco Mobility Express Deployment. Below requirements must be met to initiate a Software Update from cisco.com.

- Internet access is required for software download from cisco.com to APs. However, no proxy is required.
- A valid cisco.com (CCO) account with username & password required.
- EULA acceptance on a per user basis. Only Primary AP (not all APs in the network) must have SMARTNet contract else Software Update will not start.

Note Software Update from cisco.com is supported via GUI only.

In order to perform Software Update using cisco.com Transfer Mode, follow the procedure below:

Procedure

Step 1 To perform Software Update via Cisco.com, navigate to **Management** > **Software Update** and configure the following:

- Select **Cisco.com** for **Transfer Mode**.
- Enter **Cisco.com Username**.
- Enter **Cisco.com Password**.
- Enable **Automatically Check for Updates**. Check is done once in 30 days.
- Click on the **Check Now** button to retrieve the Latest Software Release and the Recommended Software Release from Cisco.com.

Step 2 Click **Apply**.

Step 3 Click **Update** to initiate software update wizard.

Step 4 In the Software Update Wizard, select the Recommended Software Release or Latest Software Release. Click **Next**.

Step 5 Select **Update Now** to initiate software update immediately or **Schedule the Update for Later**.

Note If **Schedule the Update for Later** is selected, configure the **Set Update Time field**.

Step 6 Click on the **Auto Restart** checkbox if automatic restart of all access points in the network is desired after the software update is finished. Click **Next**.

Step 7 Click **Confirm** to start the software update.

To monitor the download progress on individual Access Points, expand the **Predownload image status.**

Software Update using HTTP Transfer Mode

If you have the same model of Access Points in the Mobility Express deployment, HTTP Transfer mode can be used to perform Software Update. For HTTP Transfer mode, one can simply upload the Access Point upgrade image from the local machine. To perform Software Update using HTTP Transfer Mode, follow the procedure below:

Procedure

Step 1 Download the AP Image bundle from cisco.com to the local machine. The table below points to Release 8.7.102.0 images.

Access Point	Access Point image bundle. Contains individual AP images to be used for Software Update
Cisco Aironet® 1540 Series	AIR-AP1540-K9-ME-8-7-102-0.zip
Cisco Aironet® 1560 Series	AIR-AP1560-K9-ME-8-7-102-0.zip
Cisco Aironet® 1815I Series	AIR-AP1815-K9-ME-8-7-102-0.zip
Cisco Aironet® 1815M Series	AIR-AP1815-K9-ME-8-7-102-0.zip
Cisco Aironet® 1815W Series	AIR-AP1815-K9-ME-8-7-102-0.zip
Cisco Aironet® 1830 Series	AIR-AP1830-K9-ME-8-7-102-0.zip
Cisco Aironet® 1850 Series	AIR-AP1850-K9-ME-8-7-102-0.zip
Cisco Aironet® 2800 Series	AIR-AP2800-K9-ME-8-7-102-0.zip
Cisco Aironet® 3800 Series	AIR-AP3800-K9-ME-8-7-102-0.zip

Note The above images are for AireOS Release 8.4.100.0. The image bundle would be different for different releases.

Step 2

Step 3 Unzip the AP Image bundle to extract individual AP Images. Mapping of Access Points to their corresponding images is shown below:

Access Point	Access Point Image
Cisco Aironet® 1540 Series	ap1g5
Cisco Aironet® 1560 Series	ap3g3
Cisco Aironet® 1815I Series	ap1g5
Cisco Aironet® 1815M Series	ap1g5

Access Point	Access Point Image
Cisco Aironet® 1815W Series	ap1g5
Cisco Aironet® 1830 Series	ap1g4
Cisco Aironet® 1850 Series	ap1g4
Cisco Aironet® 2800 Series	ap3g3
Cisco Aironet® 3800 Series	ap3g3

Step 4 To perform Software Update via **HTTP** Transfer Mode, navigate to **Management** > **Software Update** and configure the following:

- Select **HTTP** for **Transfer Mode**
- Browse to the local AP image, corresponding to the Access Point in your network
- Click on the Auto Restart checkbox if automatic restart of all access points in the network is desired after the software update is finished

Step 5 Click **Apply**.

Step 6 Click on **Update**to initiate software update.

Software Update using SFTP Transfer Mode

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.

Upgrading from WebUI

To perform Software Update using SFTP Transfer mode from WebUI, follow the procedure below:

Procedure

Step 1 Download the AP Image bundle from cisco.com to the SFTP server.

Step 2 Unzip the AP Image bundle to extract individual AP Images.

Step 3 To perform Software Update via **SFTP** Transfer Mode, navigate to **Management** > **Software Update** and configure the following:

- Select **SFTP** for **Transfer Mode**
- Enter the **IP Address** and **Port Number** of the **SFTP** server.
- Enter the **File Path** to the unzipped AP images on the SFTP Server.
- Enter the **Username** and **Password** of the SFTP Server

Note The most common mistake made is entering this path correctly. It is important that this path be entered correctly before going to the next step. Do not point to individual AP image. You need to only point to the directory which contains the AP images.

Step 4 Click on the **Auto Restart** checkbox if automatic restart of all access points in the network is desired after the software download is finished.

Step 5 Click **Apply**.

Step 6 Click on **Update Now** button to initiate software update.

Note To Schedule Update at a later time, user must select a date and time in **Set Update Time** field and then click on the **Schedule Later** button. It is recommended that the Set Reboot Time should be at least 2 hours from the time pre-image download was initiated. This will ensure that pre-image download on all Access Points in the Mobility Express Network has completed.

Software Update using TFTP Transfer Mode

Software Update via TFTP Transfer Mode works for all Access Points supported in a Cisco Mobility Express Deployment. You would need a TFTP 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.

Upgrading from WebUI

To perform Software Update using TFTP Transfer mode from WebUI, follow the procedure below:

Procedure

Step 1 Download the AP Image bundle from cisco.com to the TFTP server.

Step 2 Unzip the AP Image bundle to extract individual AP Images.

Step 3 To perform Software Update via **TFTP** Transfer Mode, navigate to **Management > Software Update** and configure the following:

- Select **TFTP** for **Transfer Mode**.
- Enter the **IP Address** of the **TFTP** server in the **IP Address (IPv4)** field.
- Enter the **File Path** to the unzipped AP images on the TFTP Server.

Note The most common mistake made is entering this path correctly. It is important that this path be entered correctly before going to the next step. Do not point to individual AP image. You need to only point to the directory which contains the AP images.

Step 4 Click **Apply**.

Step 5 Click **Update Now** to initiate software update.

Note To Schedule Update at a later time, user must select a date and time in **Set Update Time** field and then click on the **Schedule Later** button. It is recommended that the Set Reboot Time should be at least 2 hours from the time pre-image download was initiated. This will ensure that pre-image download on all Access Points in the Mobility Express Network has completed.

Upgrading from CLI

Procedure

Step 1 Login to AP running Mobility Express controller via SSH or Telnet(if it is enabled).

Step 2 Specify the datatype.

```
(Cisco Controller) >transfer download datatype ap-image
```

Step 3 Specify the transfer mode.

```
(Cisco Controller) >transfer download ap-images mode tftp
```

Step 4 Specify the IP address of the TFTP server.

```
(Cisco Controller) >transfer download ap-images serverIp <IP addr>
```

Step 5 Specify the path of the AP images on the TFTP server.

```
(Cisco Controller) >transfer download ap-images imagePath <path to AP images>
```

Note The most common mistake made is entering this path correctly. It is important that this path be entered correctly before going to the next step. Do not point to individual AP image. You need to only point to the directory which contains the AP images.

Step 6 Start pre-downloading of the image on the APs.

```
(Cisco Controller) >transfer download start
Mode..................................... TFTP
Data Type................................ ap-image
TFTP Server IP........................... 10.1.1.77
TFTP Packet Timeout...................... 10
TFTP Max Retries......................... 10
TFTP Path................................ ap_bundle_8.1.112.30/
This may take some time.
Are you sure you want to start? (y/N) y
TFTP Code transfer starting.
Triggered APs to pre-download the image.
Reboot the controller once AP Image pre-download is complete
```

Step 7 Check the pre-download status by executing the CLI below.

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

Total number of APs.............. 3
Number of APs
       Initiated.......................1
       Predownloading..................2
       Completed predownloading..........0
       Not Supported.....................0
       Failed/BackedOff to Predownload...0
```

```
                    Primary    Backup  Predownload Predownload Next Retry  Retry Failure
AP Name               Image     Image     Status      Version    Time       Count Reason
--------------   ----------  ---------  --------    ---------   -------   ----  -----
AP6412.256e.0e78 8.1.112.21  8.1.112.21 Predownloading   --          NA    NA
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Predownloading   --          NA    NA
3600-gemini   8.1.112.21  8.1.112.21 Predownloading   --            NA
```

Step 8 Wait for the pre-image download to complete on the Access Points.

```
(Cisco Controller) >show ap image all
Total number of APs..... 3
Number of APs
       Initiated.....................1
       Predownloading................2
       Completed predownloading.....0
       Not Supported.................0
       Failed/BackedOff to Predownload...0

                     Primary    Backup  Predownload Predownload Next Retry Retry Failure
AP Name                Image     Image     Status      Version    Time       Count Reason
 --------------   ----------  ---------  --------    ---------   -------   ----  -----
AP6412.256e.0e78 8.1.112.21  8.1.112.21 Complete     --          NA           NA
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Complete     --          NA           NA
3600-gemini   8.1.112.21  8.1.112.21 Complete   --              NA
```

Step 9 After the pre-download is complete, issue a reset system as shown below.

```
(Cisco Controller) >reset system
The system has unsaved changes.
Would you like to save them now? (y/N) y
Configuration Saved!
System will now restart!
```

Passive Client Support Mobility Express

Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point.

For FlexConnect APs with locally switched WLANs, passive client feature enables the broadcast of ARP requests and the APs respond on behalf of the client.

Note Passive Client support is not available for Guest and CWA WLANs.

To enable Passive Client on AP, follow the procedure below:

Procedure

Step 1 Enable **Expert View**.

Step 2 Navigate to **Wireless Settings > WLANs** and click on **Add new WLAN/RLAN** button.

Step 3 Under the **Advanced** tab, enable **Passive Client** for the WLAN.

Step 4 Enter the **Multicast IP**.

Step 5 Click **Apply**.

Managing Advanced RF Parameters

Cisco Mobility supports a number RF Parameters which can be configured the administrator to optimize their network deployment. To manage advanced RF Parameters, follow the procedure below:

Procedure

Step 1 Enable **Expert View** on Cisco Mobility Express. **Expert View** is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view.

Step 2 Under **Advanced RF Parameters**, the following parameters are available:

- **2.4 GHz Band** - This is a global setting and can be enabled or disabled.
- **5.0 GHz Band** - This is a global setting and can be enabled or disabled.
- **Automatic Flexible Radio Assignment** - If there are 2800 and 3800 series access points in the Cisco Mobility Express deployment which supports Flexible Radio Assignment, one can choose to enable or disable it.
- **Optimized Roaming**–This is a global setting and can be enabled or disabled.
- **Event Driven RRM**–This is a global setting and can be enabled or disabled.
- **CleanAir Detection**–CleanAir is supported on 2800 and 3800 series access points and one can choose to enable or disable it.
- **5.0 GHz Channel Width**–Global setting is configured to best but one can select 20, 40, 80 or 160 MHz for channel width.
- **2.4 GHz Data Rates**–Move the slider to disable/enable data rates in the 2.4 GHz band
- **5.0 GHz Data Rates**–Move the slider to disable/enable data rates in the 5.0 GHz band
- **Select DCA Channels**–One can select (click on individual channels) the channels to be included in DCA for both 2.4 GHz and 5.0 GHz band

Note Green with an underline below the channel indicates that it is selected.

Step 3 Click **Apply**.

Uploading OUI, EAP Device Cert, EAP CA Cert from UI

Prior to 8.7, uploading OUI file, EAP Device Certificate and EAP CA Certificate was only available from CLI. Starting 8.7, this functionality is available from WebUI via using local file upload(HTP), FTP or TFTP.

To upload, follow the procedure below:

Procedure

Step 1 Navigate to **Advanced** > **Controller Tools** > **Upload File**

Step 2 Select the File Type to upload. This can be OUI file, EAP Device Cert, and EAP CA Cert.

Step 3 Select HTTP, FTP or TFTP for Transfer Mode and provide applicable details.

Step 4 If the **Transfer Mode** is **HTTP(Local Machine),** click on the Browse button and upload the file.

Step 5 Click **Apply settings** and **Import**.

CALEA Support

Support for The Communications Assistance for Law Enforcement Act (CALEA) is available in Cisco Mobility Express starting Release 8.5. To configure CALEA Server, follow the procedure below:

Procedure

Step 1 Enable **Expert View** on Cisco Mobility Express. **Expert View** is available on the top banner of the Cisco Mobility Express WebUI as shown below.

Step 2 Navigate to **Advanced** > **Controller Tools.** Click on the **CALEA** Tab and configure the following:

- Enable the **CALEA status**
- Enter the **CALEA server IP address** and **Port**
- Enter the **Sync** interval in minutes
- Enter the **Venue** information

Step 3 Click **Apply**.