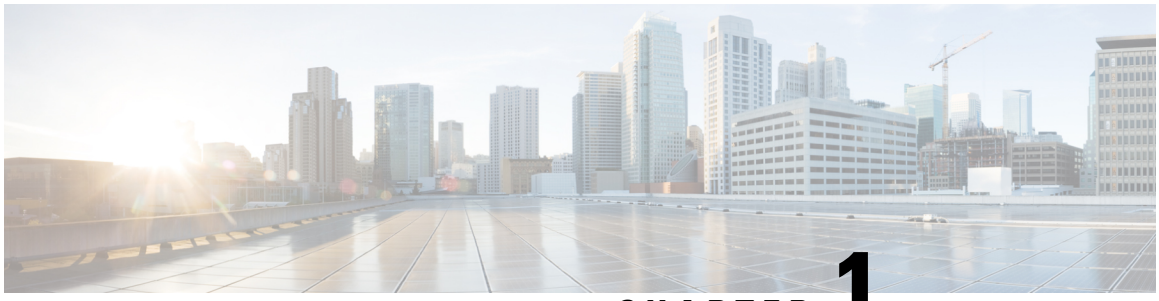
Cisco Mobility Express Deployment Guide Release 8.7

First Published: 2018-04-18

Last Modified: 2019-07-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Mobility Express Overview

With more devices attaching to the network and more bandwidth-intensive applications in use, mobile usage continues to rise. How do small and medium-sized businesses with little or no IT staff keep pace with unexpected growth?

The Cisco Mobility Express Solution is specifically designed to help small and medium-sized businesses easily and cost-effectively deliver enterprise-class wireless access to both employees and customers. It is a virtual Wireless LAN controller function embedded on Cisco Aironet® 1560, 1815W, 1815I,1830, 1850, 2800 and 3800 series 802.11ac Wave 2 Access Points. With the Cisco Mobility Express Solution, small and mid-sized networks can now enjoy the same quality user experiences as large enterprises.

Cisco Mobility Express Solution is an on-premise, managed Wi-Fi solution that:

- Is ideal for small and medium-sized deployments of up to 100 access points.
- Provides an easy, over-the-air deployment in under 10 minutes. In addition, one can use Network Plug and Play to bring up a new site.
- Removes the need for a physical controller while supporting Cisco's advanced features.
- Is supported on Cisco Aironet® 1560, 1815W, 1815I, 1815M, 1830, 1850, 2800 and 3800 Series 802.11ac Wave 2 Access Points.
- Can control other Aironet® access points, such as the 1700, 2700, and 3700 Series.
- Can be used to perform Site Survey.
- Is the Next Generation Autonomous. 802.11ac Wave 2 Access Point do not support the legacy autonomous mode.
- Industry-leading Cisco technology allows small and medium-sized networks to reduce the number of devices needed to enjoy enterprise-grade Wi-Fi. Advanced features such as Guest, BYOD and Cisco High Density Experience (HDX) are activated by default for compatible access points, making the deployment process even easier. CMX can be added to gain presence-based services and deep analytics.

- Supported Cisco Aironet® Access Points, on page 1

Supported Cisco Aironet® Access Points

Cisco Mobility Express solution consists of the following components:

- Master Access Point - Cisco Aironet® 1560, 1815W, 1815I, 1815M,1830, 1850, 2800 and 3800 Series 802.11ac Wave 2 Access Points running the virtual Wireless LAN Controller function.
- Subordinate Access Points - Cisco Aironet® Access Points which are managed by Master Access Point similar to how a Wireless LAN Controller manages Access Points.

Note Master Access Point functions as Wireless LAN Controller, manages Subordinate Access Points and also serves clients at the same time.

Master Access Points

Cisco Aironet® Access Points which support the Wireless LAN Controller function and operate as Master Access points are listed in the table below:

Table 1: Cisco Aironet® Access Points capable of operating as Master Access Points

Master Access Points	Supported Model Numbers
Cisco Aironet® 1540 Series	AIR-AP1540I-x-K9 AIR-AP1540D-x-K9
Cisco Aironet® 1560 Series	AIR-AP1562I-x-K9 AIR-AP1562E-x-K9 AIR-AP1562D-x-K9
Cisco Aironet® 1815I Series	AIR-AP1815I-x-K9C
Cisco Aironet® 1815M Series	AIR-AP1815M-x-K9C
Cisco Aironet® 1815W Series	AIR-AP1815W-x-K9C
Cisco Aironet® 1830 Series	AIR-AP1832I-x-K9C
Cisco Aironet® 1850 Series	AIR-AP1852I-x-K9C AIR-AP1852E-x-K9C
Cisco Aironet® 2800 Series	AIR-AP2802I-x-K9C AIR-AP2802E-x-K9C
Cisco Aironet® 3800Series	AIR-AP3802I-x-K9C AIR-AP3802E-x-K9C

Note The -x- in the other model numbers is a placeholder for the actual letter indicating the model's regulatory domain. For information on regulatory domains, see http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Subordinate Access Points

Cisco Aironet® Access Points which operate as Subordinate Access Points and serve clients are listed in the table below:

Table 2: Cisco Aironet® Access Points capable of operating as Subordinate Access Points

Subordinate Access Points	Supported Model Numbers
Cisco Aironet® 700i Series	AIR-CAP702I-x-K9
Cisco Aironet® 700w Series	AIR-CAP702W-x-K9
Cisco Aironet® 1540 Series	AIR-AP1540I-x-K9 AIR-AP1540D-x-K9
Cisco Aironet® 1560Series	AIR-AP1562I-x-K9 AIR-AP1562E-x-K9 AIR-AP1562D-x-K9
Cisco Aironet® 1700 Series	AIR-CAP1702I-x-K9
Cisco Aironet® 1810 Series	AIR-AP1810W-x-K9
Cisco Aironet® 1815I Series	AIR-AP1815I-x-K9C
Cisco Aironet® 1815M Series	AIR-AP1815M-x-K9C
Cisco Aironet® 1815W Series	AIR-AP1815W-x-K9C
Cisco Aironet® 1830 Series	AIR-AP1832I-x-K9C
Cisco Aironet® 1850 Series	AIR-AP1852I-x-K9C AIR-AP1852E-x-K9C
Cisco Aironet® 2700 Series	AIR-CAP2702I-x-K9 AIR-CAP2702E-x-K9
Cisco Aironet® 2800 Series	AIR-AP2802I-x-K9C AIR-AP2802E-x-K9C
Cisco Aironet® 3700 Series	AIR-CAP3702I-x-K9 AIR-CAP3702E-x-K9
Cisco Aironet® 3800 Series	AIR-AP3802I-x-K9C AIR-AP3802E-x-K9C

Note The -x- in the other model numbers is a placeholder for the actual letter indicating the model's regulatory domain. For information on regulatory domains, see http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

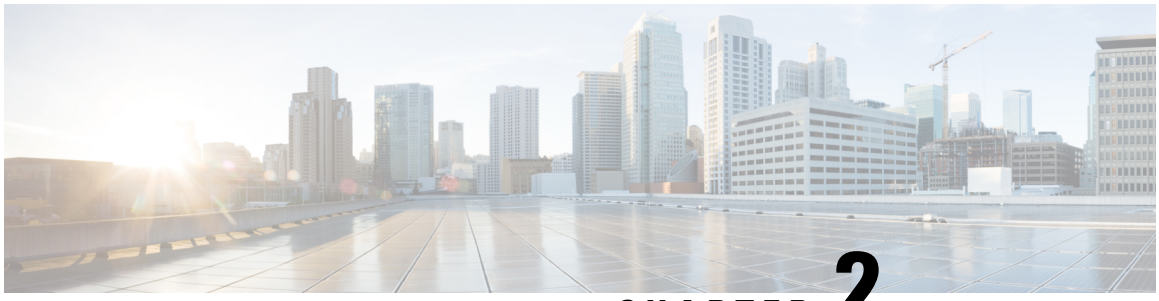
Cisco Mobility Express Scale Limits

Cisco Mobility Express supports up to 100 Access Points and 2000 Clients in a single deployment. Given below are the scale limits per Master Access Point.

Table 3: Cisco Mobility Express Scale Limits

Master Access Points	# of Access Points Supported	# of Clients Supported
Cisco Aironet® 1540 Series	50	1000
Cisco Aironet® 1560 Series	100	2000
Cisco Aironet® 1815I Series	50	1000
Cisco Aironet® 1815M Series	50	1000
Cisco Aironet® 1815W Series	50	1000
Cisco Aironet® 1830 Series	50	1000
Cisco Aironet® 1850 Series	50	1000
Cisco Aironet® 2800 Series	100	2000
Cisco Aironet® 3800 Series	100	2000

Note If there are more than 50 Access Points in a Mobility Express network, the Master AP(running the Wireless LAN controller function) can service a maximum of 20 clients. This limit only applies to Master AP and not any other Access Point in the Mobility Express network.



CHAPTER 2

Deploying Cisco Mobility Express

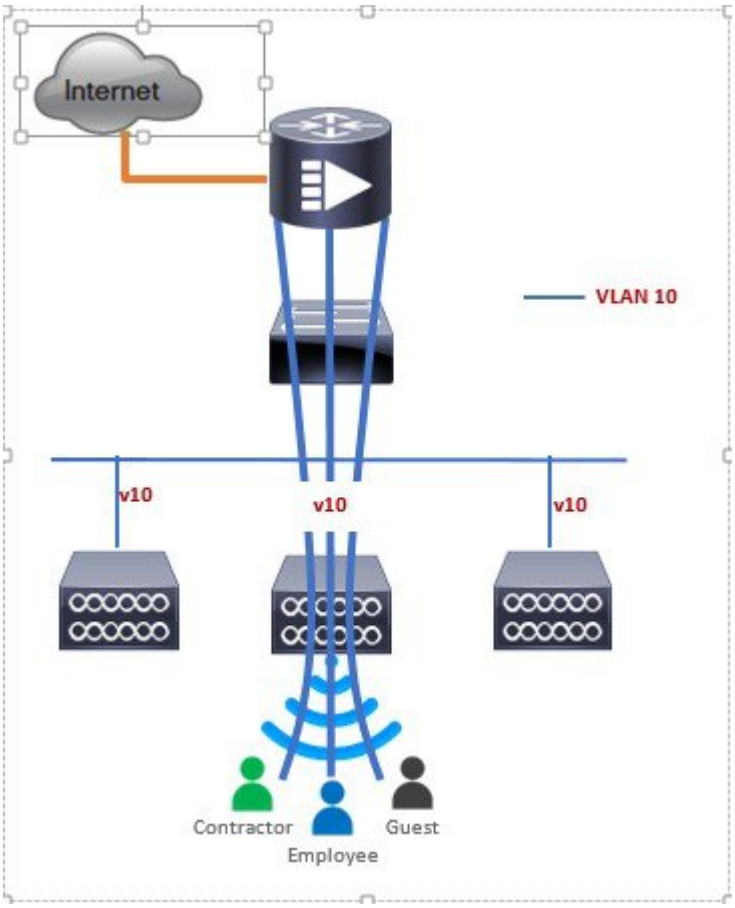
Pre-requisites for Deploying Mobility Express Solution

1. You must not have other Cisco Wireless LAN Controllers; neither appliance nor virtual in the same network during set up or during daily operation of a Cisco Mobility Express network. The Mobility Express controller cannot interoperate or co-exist with other Wireless LAN Controllers in the same network.
2. Decide on the first Access Point to be configured as a Master Access Point. This Access Point should be capable of supporting the Wireless LAN Controller function.
3. A DHCP server must be available on the network so that Access Points and clients can obtain an IP Address. Starting AireOS® Release 8.3.102.0 or later, one can configure a DHCP server on the Master Access Point as well but this is typically used for Site Survey.

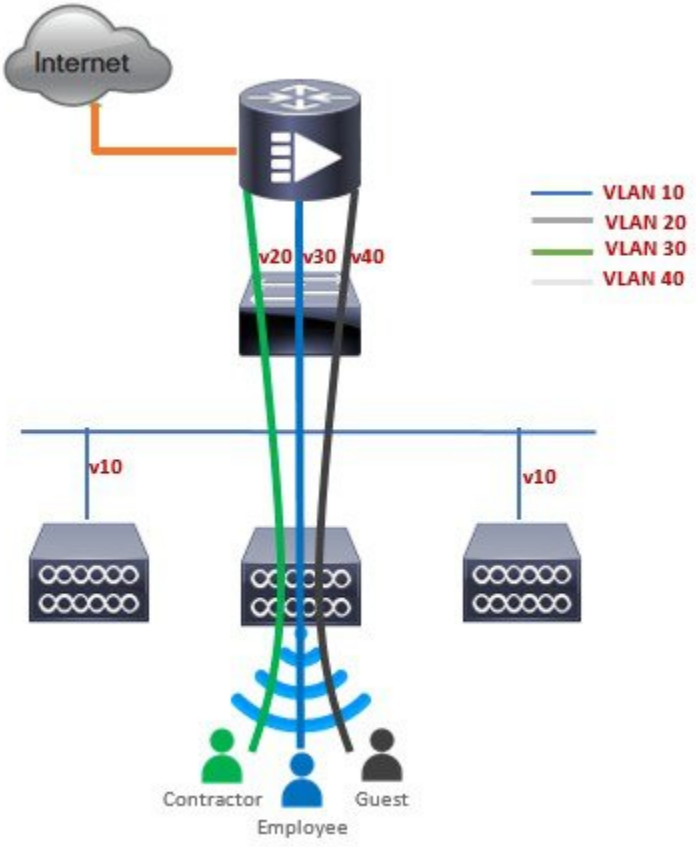
Connecting Mobility Express capable Access Point to the network

Depending on the deployment, Mobility Express capable Access Points can be connected to an access port or a trunk port on the switch.

If Access Points and WLANs are all on the same network, Mobility Express capable Access Points can connect to an access port on the switch as shown below.



On Mobility Express, management traffic is untagged. If Access Points and WLANs are all on different VLANs, Mobility Express capable Access Points will connect to a trunk port on the switch and traffic for individual WLANs will be switched locally on individual VLANs. Shown below is a deployment with Access Points and WLANs on different VLANs.




```
interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 40
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

Determining image on the Access Point

The Cisco Aironet® 1540, 1560, 1815, 1830, 1850, 2800 and 3800 series access points can either have CAPWAP image or the Cisco Mobility Express image which is capable of running the virtual Wireless LAN controller function on the Access Point.

To determine the image and capability of an Access Point, follow the procedure below:

Procedure

Step 1 Login to the Access Point CLI using a console and type **AP#show version** and check the full output of show version. The default login credentials are Username:cisco and Password:cisco.

Step 2 If ***show version*** output **does not** display **AP Image Type** and **AP Configuration** parameters as highlighted below, it means that AP is running the CAPWAP image and a conversion to Cisco Mobility Express is required if you want to run the controller function on the Access Point. To convert from a CAPWAP Access Point to Mobility Express, go to Conversion section.

```
cisco AIR-AP1852E-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.2.100.0
Primary Boot Image : 8.2.100.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
0 Gigabit Ethernet interfaces
0 802.11 Radios
Radio FW version . 1401b63d12113073a3C08aa67f0c039c0
NSS FW version : NSS.AK.1.0.c4-0Z026-E_cust C-1.24160
```

If the **show version** displays **AP Image Type: MOBILITY EXPRESS IMAGE** and **AP Configuration: NOT MOBILITY EXPRESS CAPABLE** , it means that even though the Access Point has the Cisco Mobility Express image, it is configured to run as a CAPWAP Access Point. In this case Access Point will not run the controller function and will not participate in the Master Election process upon failure of the active Master AP.

```
cisco AI R-AP1852E-UXK9 ARMv7 Processor rev 0 (v7I) with 997184/726252K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.2.101.0
Primary Boot Image : 8.2.100.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : NOT MOBILITY EXPRESS CAPABLE
```

For this AP to run the controller function, **AP Configuration** has to be changed to **MOBILITY EXPRESS CAPABLE** . To change the AP Configuration, execute the following command from the AP CLI. **AP#ap-type mobility-express tftp://**

Access Point will reboot and after it comes up, it will be capable of running the controller function. You can check the output of ***show version*** again to confirm that ***AP Configuration*** has changed to ***MOBILITY EXPRESS CAPABLE*** .

If the **show version** displays **AP Image Type: MOBILITY EXPRESS IMAGE** and **AP Configuration: MOBILITY EXPRESS CAPABLE** , it means that the Access Point has the Mobility Express image and is capable of running the controller function. For this scenario, the output of the **show version** is shown below:

```
cisco AIR-AP3802I-B-K9 ARMv7 Processor rev 1 (v7l) with 1028384/255032K bytes of memory.
Processor board ID FCW2034NXAV
AP Running Image     : 8.4.2.66
Primary Boot Image   : 8.4.2.66
Backup Boot Image    : 8.4.2.34
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
1 Multigigabit Ethernet interfaces
1 Gigabit Ethernet interfaces
2 802.11 Radios
Radio Driver version : 9.0.5.5-W8964
Radio FW version : 9.1.8.1
NSS FW version : 2.4.18
```

Conversion

One can convert an Access Point running CAPWAP to Cisco Mobility Express and vice versa.

Converting Access Point from CAPWAP to Cisco Mobility Express

Cisco Mobility Express support on 11ac Wave 2 Access Points is introduced in different AireOS releases and it is important to note that before an Access Point can be converted to Mobility Express, it must have the minimum AireOS CAPWAP image which supported Cisco Mobility Express capability for that Access Point. Given below is the minimum AireOS release for an Access Point which will support conversion from CAPWAP to Cisco Mobility Express.

Table 4: Minimum AireOS release supporting Cisco Mobility Express

Access Point	Minimum AireOS Release with CAPWAP image
Cisco Aironet® 1540Series	Release 8.5 or later
Cisco Aironet® 1560 Series	Release 8.4 or later
Cisco Aironet® 1815I Series	Release 8.4 or later
Cisco Aironet® 1815M Series	Release 8.5 or later
Cisco Aironet® 1815W Series	Release 8.4 or later
Cisco Aironet® 1830 Series	Release 8.1 MR2 or later
Cisco Aironet® 1850 Series	Release 8.1 MR2 or later
Cisco Aironet® 2800 Series	Release 8.3 or later
Cisco Aironet® 3800 Series	Release 8.3 or later

Note If the CAPWAP image on the Access Point is older than the minimum AireOS release capable of supporting Cisco Mobility Express, Access Point MUST first join a WLC running the minimum AireOS release or higher to upgrade its CAPWAP image. After the CAPWAP image of the AP has been upgraded, conversion of AP from CAPWAP to Mobility Express can be performed.

To perform a conversion on an Access Point running CAPWAP to Mobility Express, follow the procedure below:

Procedure

Step 1 Download the conversion image for the Access Point from cisco.com to the TFTP server. It is a tar file. Do not untar the file. The following table lists the Cisco Mobility Express software for Cisco Wireless Release **8.7.102.0.**

Table 5: Conversion tar file for Access Points

Access Points supported as Master AP	Software to be used only for Conversion from Unified Wireless Network Lightweight AP Software to Cisco Mobility Express
Cisco Aironet® 1540 Series	AIR-AP1540-K9-8-7-102-0.tar
Cisco Aironet® 1560 Series	AIR-AP1560-K9-8-7-102-0.tar

Access Points supported as Master AP	Software to be used only for Conversion from Unified Wireless Network Lightweight AP Software to Cisco Mobility Express
Cisco Aironet® 1815I Series	AIR-AP1815-K9-8-7-102-0.tar
Cisco Aironet® 1815M Series	AIR-AP1815-K9-8-7-102-0.tar
Cisco Aironet® 1815W Series	AIR-AP1815-K9-8-7-102-0.tar
Cisco Aironet® 1830 Series	AIR-AP1830-K9-8-7-102-0.tar
Cisco Aironet® 1850 Series	AIR-AP1850-K9-8-7-102-0.tar
Cisco Aironet® 2800 Series	AIR-AP2800-K9-8-7-102-0.tar
Cisco Aironet® 3800 Series	AIR-AP3800-K9-8-7-102-0.tar

Step 2 Login to the Access Point.

Step 3 Execute **AP#show version** on the Access Point CLI. From the show version output, you can determine the **AP Image type** and **AP Configuration** and can then proceed with the conversion

Case 1: If the **AP Image type** is **MOBILITY EXPRESS IMAGE** and **AP configuration** is **NOT MOBILITY EXPRESS CAPABLE**, enter the command below to change the **AP Configuration** to **MOBILITY EXPRESS CAPABLE** .

AP#ap-type mobility-express

Note Since the Access Point has **AP Image type: MOBILITY EXPRESS IMAGE**, a new image will not be downloaded. After the command is executed, the Access Point will reboot and after it comes up, the **AP Configuration** will be changed to **MOBILITY EXPRESS CAPABLE**.

Case 2 : If the **AP Image type** and **AP Configuration** are not available, it means that the AP is running CAPWAP image. To do the conversion, execute the command below:

AP#ap-type mobility-express tftp://<TFTP Server IP>/<path to tar file>

Example:

```
AP#ap-type mobility-express tftp://10.18.22.34/AIR-AP1850-K9-8.7.102.0.tar

Starting the ME image download...
It may take few minutes to finish the download.

Image downloaded, writing to flash...
do PREDOWNLOAD, part1 is active part
sh: CHECK_ME: unknown operand
Image start 0x40355008 size 0x01dae41a file size 0x01dae7ca
Key start 0x42103422 size 0x00000230
Sinature start 0x42103652 size 0x00000180
Verify returns 0
btldr rel is 16 vs 16, does not need update
part to upgrade is part2
activate part2, set BOOT to part2
AP primary version: 8.1.105.37
Archive done.
Oe as AP needs to boot up with ME image

The system is going down Now!
sent SIGTERM to all processes
sent SIGKILL to all processes
```

```
Requesting system reboot79]
[07/24/2015 18:19:43.0887] Restarting system.
[07/24/2015 18:19:43.1257] Going down for restart now
```

Note After the image download is complete, it will be written to the flash followed by a reboot. After the AP comes up, ***AP Image type*** will be ***MOBILITY EXPRESS IMAGE*** and ***AP Configuration*** will ***MOBILITY EXPRESS CAPABLE*** .

Step 4 If this is the first Access Point in the network, it will start the controller function and will broadcast the ***CiscoAirProvison*** SSID.

Converting Access Point from Cisco Mobility Express to CAPWAP

There are typically two reasons why one would want to convert an Access Point running Mobility Express image to CAPWAP. There are as follows:

1. You want to keep the Access Point in a Mobility Express deployment but do not want the Access point to participate in the Master election process upon a failover of the Master AP.
2. You want to migrate one or more Access Points with Mobility Express to an appliance or vWLC based deployment.

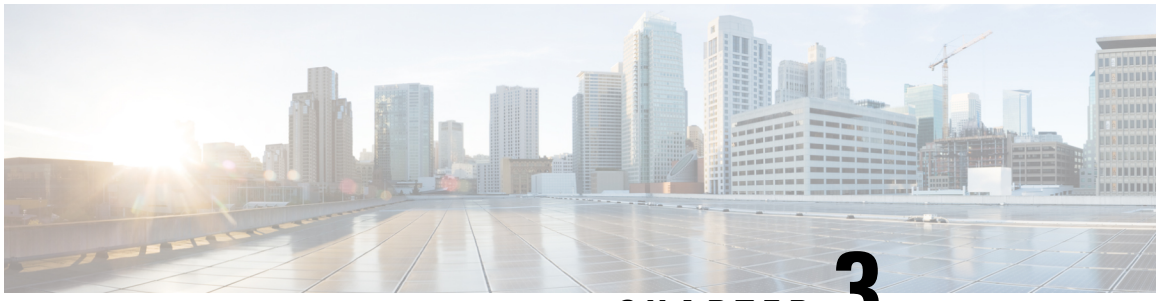
1. If your reason to convert to CAPWAP is 1 above, follow the procedure below:
   a. Login to the Access Point CLI either through console or ssh and go to exec mode. If you are trying to convert the Master AP to CAPWAP, connecting a console will lead you to the controller CLI. To get to the AP CLI, type **apciscochell** at the controller prompt and login to the Access Point shell.
   b. Execute **ap#ap-type capwap** CLI. This will change the **AP Configuration** to **NOT MOBILITY EXPRESS** and the Access Point will no longer participate in the Master election process.

2. If your reason to convert to CAPWAP is 2 above, follow the procedure below:
   a. Login to the Access Point CLI either via console or ssh and go to exec mode.
   b. Execute the following CLI.

```
(Cisco Controller) >config ap unifiedmode <switch_name> <switch_ip_address>

<switch_name> and <switch_ip_address> is the name and IP address respectively of the WLC
to which the APs need to be migrate.
```

Note The above command converts all connected Access Points with **AP Configuration: MOBILITY EXPRESS CAPABLE** to **AP Configuration: NOT MOBILITY EXPRESS CAPABLE** . When this command is issued, the APs are reloaded, and they come back up and look for the controller (switch_ip_address) to join.



CHAPTER 3

Configuring Cisco Mobility Express controller

There are multiple ways one can configure a Cisco Mobility Express controller. They are as follows:

1. CLI Setup Wizard
2. Over–the–Air Setup Wizard
3. Network Plug and Play

CLI Setup Wizard

To use the Setup Wizard from CLI, you must connect to the console port of the Access Point. The default parameters for the console ports are 9600 baud, eight data bits, one stop bit, and no parity. The console ports do not support hardware flow control.

After connecting to the console port on the Access Point, power up the Access Point. After a few minutes, Access Point will start the Controller.

To configure the Mobility Express controller, follow the steps as shown in the example below:

```
System Name [Cisco_2c:3a:40] (31 characters max): me-wlc
Enter Country Code list (enter 'help' for a list of countries) [US]:

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Note! Default NTP servers will be used

Management Interface IP Address: 40.40.40.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 40.40.40.1
Cleaning up Provisioning SSID
Create Management DHCP Scope? [yes][NO]: yes
DHCP Network : 40.40.40.0
DHCP Netmask : 255.255.255.0
Router IP: 40.40.40.1
Start DHCP IP address: 40.40.40.11
Stop DHCP IP address: 40.40.40.254
DomainName :
```

```
DNS Server : [OPENDNS][user DNS]
Create Employee Network? [YES][no]: YES
Employee Network Name (SSID)?: WestAutoBody-Employee
Employee VLAN Identifier? [MGMT][1-4095]: MGMT
Employee Network Security? [PSK][enterprise]: PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]: YES
Guest Network Name (SSID)?: WestAutoBody-Guest
Guest VLAN Identifier? [EMPLOYEE][1-4095]: EMPLOYEE
Guest Network Security? [WEB-CONSENT][psk]: WEB-CONSENT
Create Guest DHCP Scope? [yes][NO]: NO
Enable RF Parameter Optimization? [YES][no]: YES
Client Density [TYPICAL][Low][High]: TYPICAL
Traffic with Voice [NO][Yes]: Yes

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Cleaning up Provisioning SSID
```

Note The Access Point will reboot and after it comes back up, login to the Mobility Express controller WebUI from the browser using **https://<mangement_ip_address>** Cisco Mobility Express controller uses a self-signed certificate for HTTPS. Therefore, all browsers display a warning message and asks whether you wish to proceed with an exception or not when the certificate is presented to the browser. Accept the risk and proceed to access the Mobility Express Wireless LAN Controller login page.

Over-the-Air Setup Wizard

Over-the-air is a simple and easy way to configure Mobility Express out of the box. Over-the-Air provisioning can be done using a WiFi enabled device or the **Cisco Wireless** app which can be downloaded from App Store for iOS devices and Play Store for Android Devices. The **Cisco Wireless** app provides a minimum set of configurable options to deploy Mobility Express in just a few minutes.

Procedure

Step 1 When the LED on the Access Point **chirps green**, connect a WiFi enabled laptop to the **CiscoAirProvision** SSID. The default password is **password**. The laptop will get an IP address from subnet 192.168.1.0/24.

Note **CiscoAirProvision** SSID is broadcast at **2.4GHz**.

Step 2 Open a web browser and browse to **http://mobilityexpress.cisco.** This will redirect to configuration wizard and the admin account page will appear.

Step 3 Create an admin account on the controller by specifying the following parameters and then click on the **Start** button.

- Enter the admin username. Maximum up to 24 ASCII characters.
- Enter the password. Maximum up to 24 ASCII characters. When specifying a password, ensure that:
  - 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 can be repeated more than three times consecutively.
- The new password must not be the same as the associated username and the username reversed.
- The password must not be cisco, ocsic, or any variants 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 4 In the **Set up Your Controller** section, configure the following:

- Enter the System Name
- Select the Country from the drop-down list
- Date and Time should be auto-filled but one can manually configure it as well
- Select the Timezone from the drop-down list
- Enter the IP address of NTP Server if there is one available. If left blank, NTP Pools will be automatically configured
- Enter the Management IP Address of the controller
- Enter the Subnet Mask
- Enter the Default Gateway

Step 5 Disable **Enable DHCP Server(Management Network)** if an external DHCP server is being used. If internal DHCP server on the Mobility Express controller has to be used, specify the DHCP server related information.

Step 6 Click **Next**.

Step 7 In the **Create Your Wireless Network,** under **Employee Network**, configure the following:

- Enter the Network Name
- Select Security as WPA2 Personal or WPA2 Enterprise from the drop-down list
- If WPA2 Personal is selected, enter the Passphrase

Step 8 One can also enable **RF Parameter Optimization** and configure the following:

- Move the **Client Density** slider as needed
- From the **Traffic Type,** select **Data** or **Data and Voice**

Step 9 Click **Next**.

Step 10 Confirm the settings on the page and click on the **Apply** button. The Access Point will reboot and after it comes up, it will run the controller.

Note The Access Point will reboot and after it comes back up, login to the Mobility Express controller WebUI from the browser using **https:<management_ip_address>.** Cisco Mobility Express controller uses a self-signed certificate for HTTPS. Therefore, all browsers display a warning message and asks whether you wish to proceed with an exception or not when the certificate is presented to the browser. Accept the risk and proceed to access the Mobility Express Wireless LAN Controller login page.

Network Plug and Play

Introduction

The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new site rollouts for provisioning Cisco Mobility Express. The solution allows use of Cloud Redirection service, on-prem, or combination which provide a unified approach to provision enterprise networks comprised of Cisco Mobility Express, Cisco routers, switches, with a near zero touch deployment experience.

You can use the Cisco Network Plug and Play application to pre-provision the site and add Cisco Mobility Express capable access points to the site. This includes entering access point information and uploading a controller configuration file for virtual controller which will run on Mobility Express capable access points.

When an installer installs and powers up the Cisco Mobility Express capable access points, it auto-discovers the Cisco APIC-EM controller by using the DHCP, DNS or cloud redirection service. After the auto-discovery process is complete, the AP downloads the controller configuration file from local PnP server, or communicates with the cloud redirection service for direction to target PnP server.

Pre-requisites

1. APIC-EM Release 1.4 or later with Cisco Network Plug and Play, virtually hosted in a Cisco UCS or equivalent server.
2. Access Points–Cisco 802.11ac Wave 2 access points running Cisco Mobility Express software.
3. Controller Configuration–Cisco Mobility Express controller configuration file to be uploaded on Network PnP.

APIC-EM discovery options

1. DHCP server configured with option 43 to allow Cisco Mobility Express capable access points to auto-discover the APIC-EM controller (option 43 is not required if only testing cloud redirection). DHCP option 43 consists of a string value that is a configured DHCP server: option 43 ascii "5A1N;B2;K4;I192.168.1.123;J80"

Note 192.168.1.123 is the IP address of the APCI-EM Server

2. On–prem PnP server can be added to DNS using ‘pnpserver.yourlocal.domain’ If DHCP discovery fails to get the IP address of the APIC-EM controller, for example, because option 43 is not configured, the Cisco Plug and Play Agent falls back on a DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the APIC-EM controller, using the preset hostname pnpserver. For example, if the DHCP server returns the domain name " customer.com ", the Cisco Plug and Play IOS Agent constructs the FQDN "pnpserver.customer.com ". It then uses the local name server to resolve the IP address for this FQDN

3. Cloud redirection service requires a connection to the internet, and valid DNS server that can resolve 'devicehelper.cisco.com'. The cloud redirection service redirect Cisco Mobility Express Access Point to APIC-EM.

Configuring APIC-EM / Network PnP server

Site Pre-Provisioning Workflow

Cisco Network Plug and Play allows you to pre-provision and plan for new sites. When you create a new site, Cisco Network Plug and Play enables you to pre-provision Cisco Mobility Express access point(s) controller, configuration file, product ID, and product serial # for selected Access Points. This simplifies and accelerates the time that it takes to get a site fully functional.

For detailed info pm PnP Config about other functionality, see http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-installation-and-configuration-guides-list.html

To pre-provision a site on your network, perform these steps:

1. Importing Cisco Mobility Express controller configuration file to Network PnP
2. Creating a Project
3. Adding Cisco Mobility Express capable Access Point to the Project and associating the controller config.

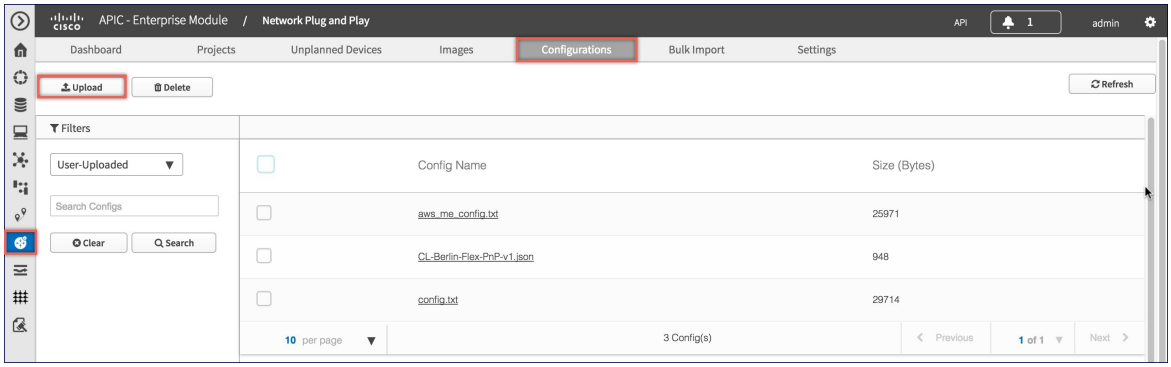
Importing Cisco Mobility Express configuration file to Network PnP

Procedure

Step 1 Login to APIC-EM controller and navigate to Network Plug and Play > Configurations

Step 2 Click on Upload to upload the controller configuration

Step 3 Select a controller configuration file from your local machine

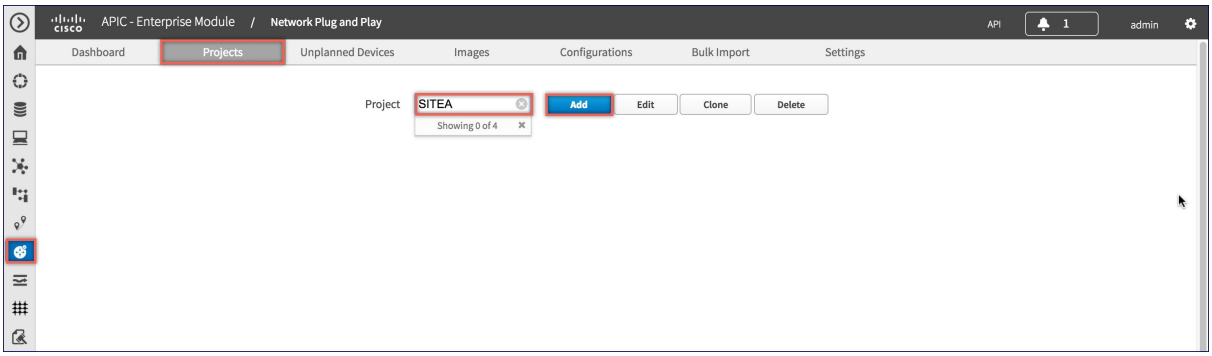


Creating a Project

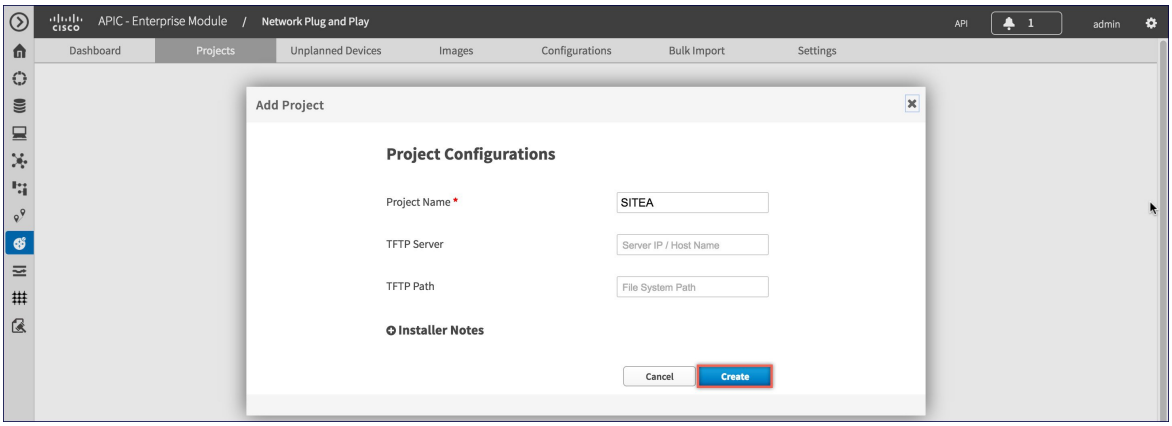
Procedure

Step 1 Navigate to **Network Plug and Play** > **Projects**.

Step 2 Enter the name for the Project and click on the Add button.



Step 3 Click on the Create button to create the Project.



Adding Cisco Mobility Express capable Access Point to the Project and associating the controller config

Procedure

Step 1 Navigate to **Network Plug and Play** > **Projects**.

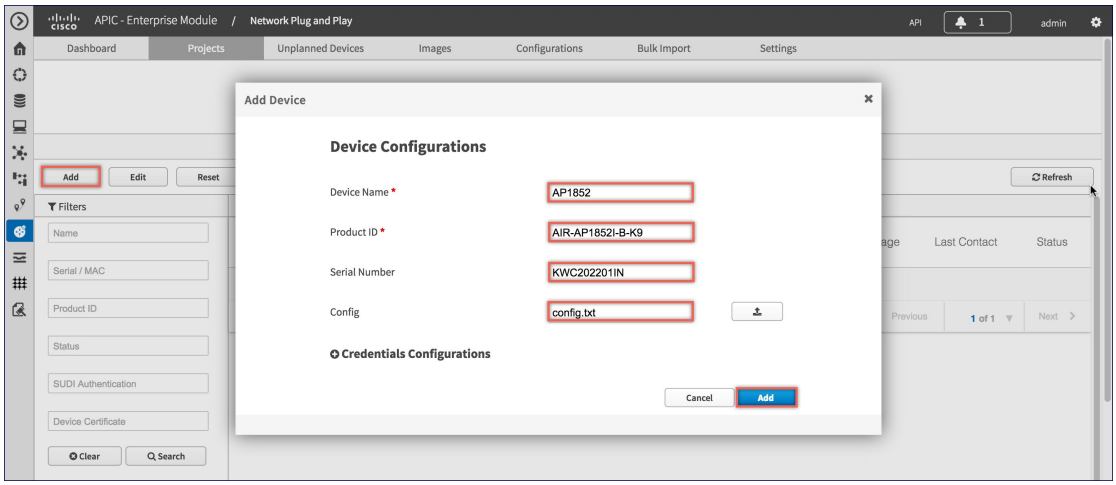
Step 2 Click on Add button under Project Devices.

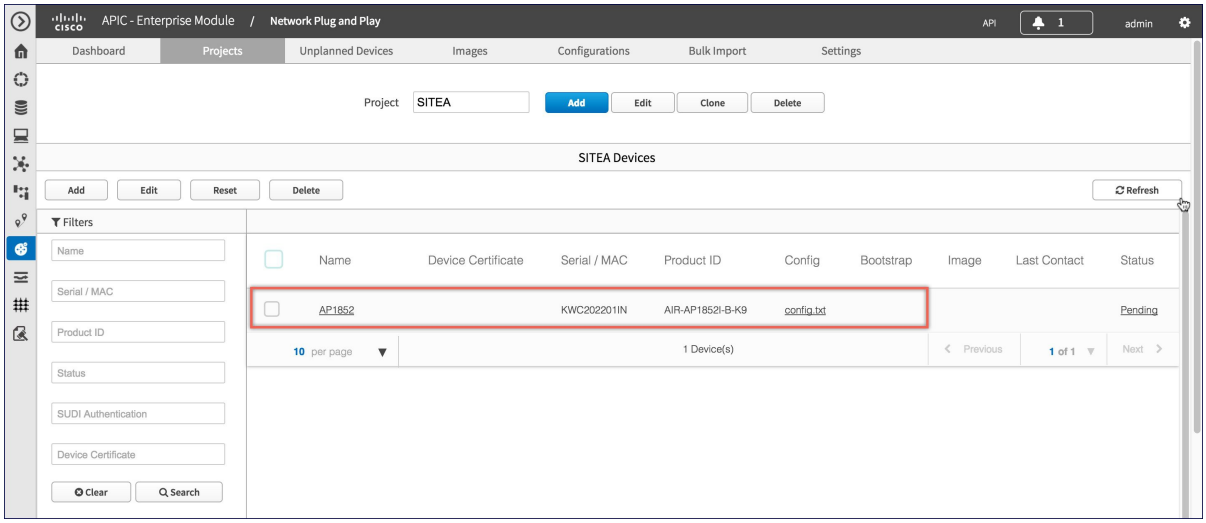
Step 3 In the Add Device window, enter the following:

- Device Name–Enter the device name; unique for each site
- Product ID–Select the Access Point device ID from the drop-down list

- Serial Number–Enter the Serial Number of the Mobility Express Access Point
- Config–You can either upload a new configuration or select the configuration file which was added earlier

Step 4 Click on the Add button.





APIC-EM Network Plug and Play Deployment Options with Cisco Mobility Express

There are two deployment options supported for deploying Cisco Mobility Express with Network Plug and Play.

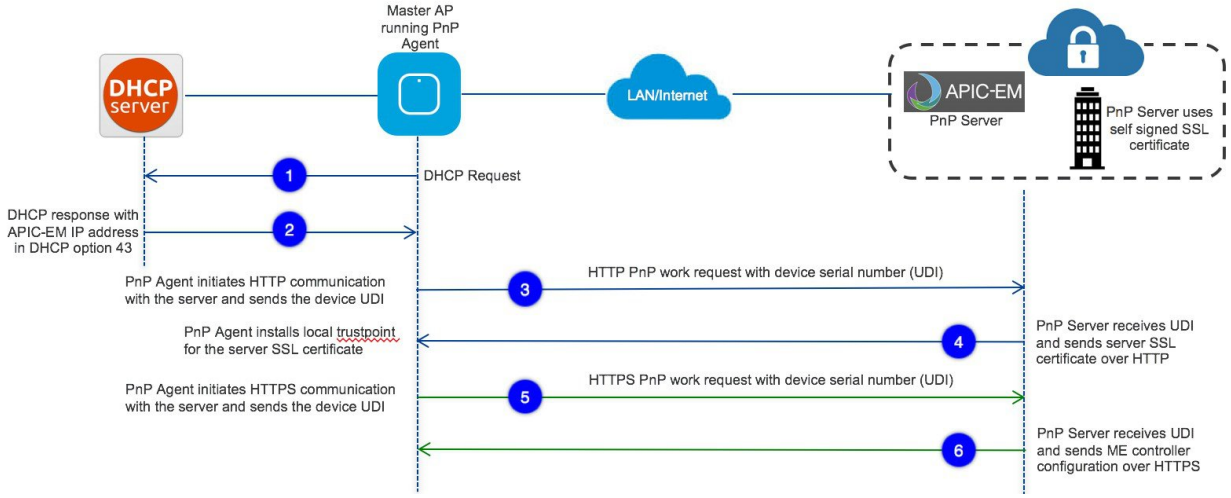
APIC-EM controller in Private Cloud

Cloud Plug and Play Connect redirect to APIC-EM controller

APIC-EM controller in Private Cloud

In this deployment option, there will be an On-Prem APIC-EM controller which can be discovered by Cisco Mobility Express Access Points using option 43 or DNS discovery.

Figure 1: APIC-EM controller in Private Cloud flow



Option 43 points to APIC-EM controller IP address. To configure DHCP scope with Option 43, it is important follow the format as shown below. In the example below, 192.168.1.123 is the IP address of APIC-EM controller

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 43 ascii "5A1N;B2;K4;I192.168.1.123;J80"
```

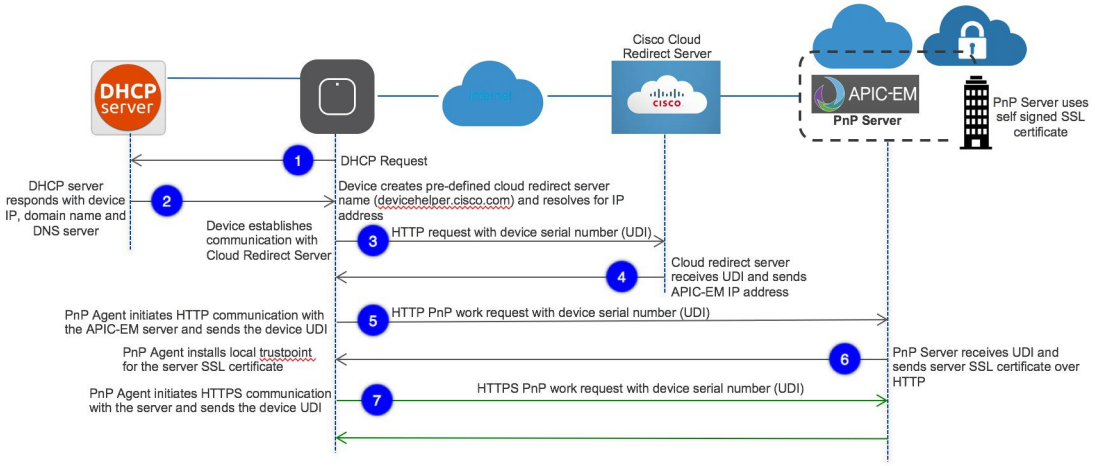
To discover APIC-EM controller using the DNS discovery options, configure the DNS server and domain name on the DHCP scope.

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
domain-name cisco.com
dns-server 172.20.229.8
```

Cloud Plug and Play Connect redirect to APIC-EM controller

Cloud re-direction service uses Cisco public hosted cloud to re-direct Cisco Mobility Express capable access points to APIC-EM controller. The minimal requirement is that the Mobility Express Access Points network have DHCP and DNS, and connectivity reachable to Cisco public cloud. There is no need to configure Option 43 on DHCP scope with this deployment option. A simple test would be to obtain DHCP address and ping 'devicehelper.cisco.com' from where the Mobility Express AP will be deployed.

Figure 2: Cloud Plug and Play Device Redirect to APIC-EM controller flow



Cloud Plug and Play Device Redirect Provisioning Workflow

This section describes the steps to redirect Cisco Mobility Express Access Points to APIC-EM controller using Cloud Plug and Play Connect service.

To configure cloud Plug and Play connect redirect service, perform the following steps:

1. Obtain a Smart Account
2. Create APIC-EM Controller Profile
3. Adding Mobility Express capable Access Point to the Devices list
4. Associate Mobility Express capable Access Point to APIC-EM Controller profile

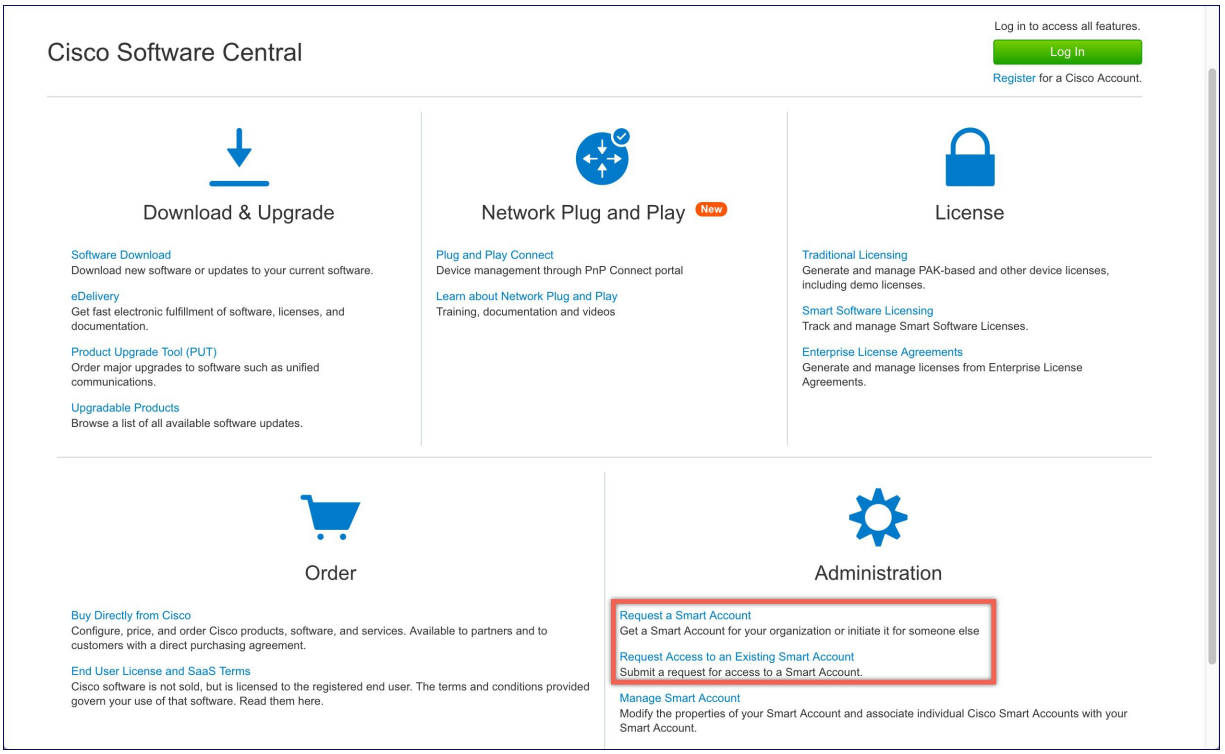
For detailed info on PnP Config about other functionality, see https://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-installation-and-configuration-guides-list.html

Obtain a Smart Account

Procedure

Step 1 Go to http://software.cisco.com

Step 2 Request a Smart Account or Log In (existing Smart Account holders)

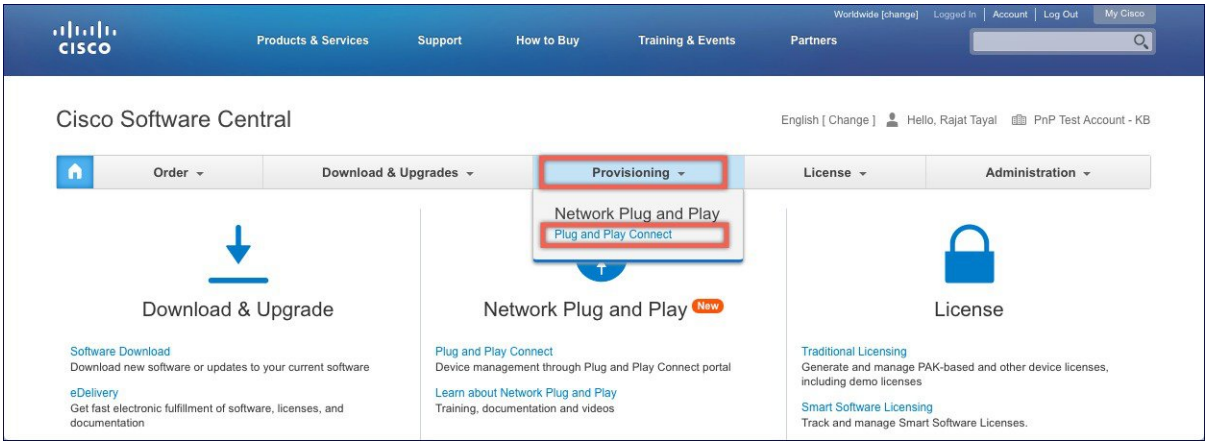


Create APIC-EM Controller Profile

Procedure

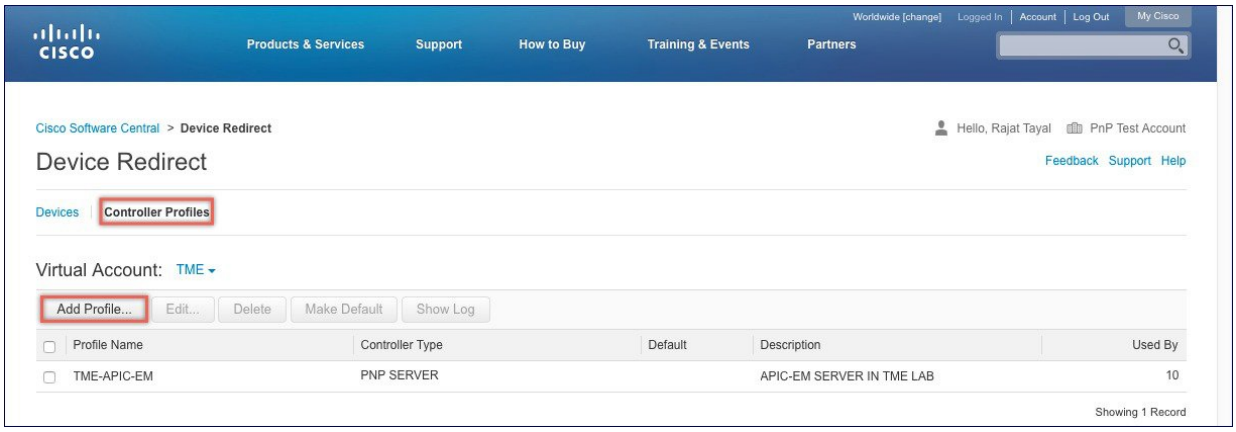
Step 1 Go to http://software.cisco.com and login

Step 2 Navigate to Provisioning > Plug and Play Connect

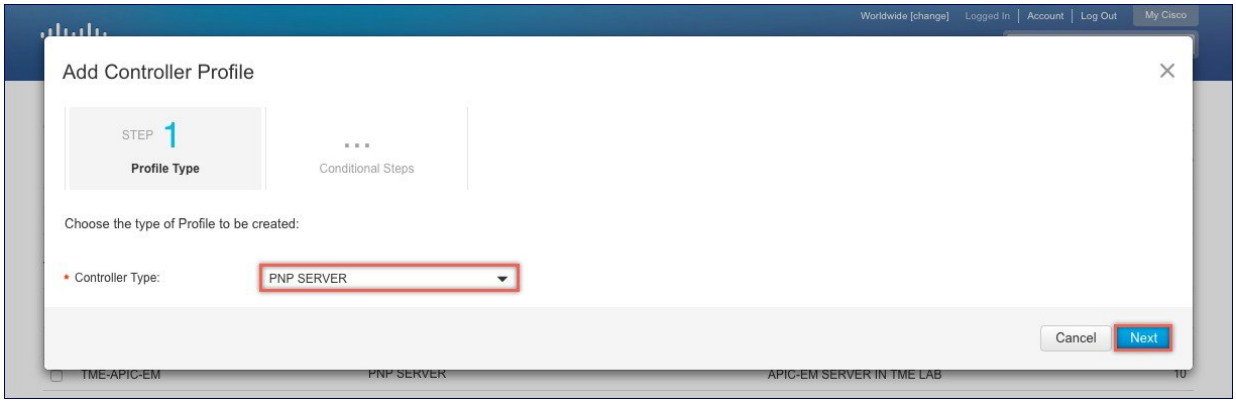


Step 3 Click on Controller Profiles. Select a Virtual Account. If you do have one, create a Virtual Account first.

Step 4 Click on the Add Profile to create a new controller profile.



Step 5 Select Controller Type as PNP Server from the drop-down list and click on Next.



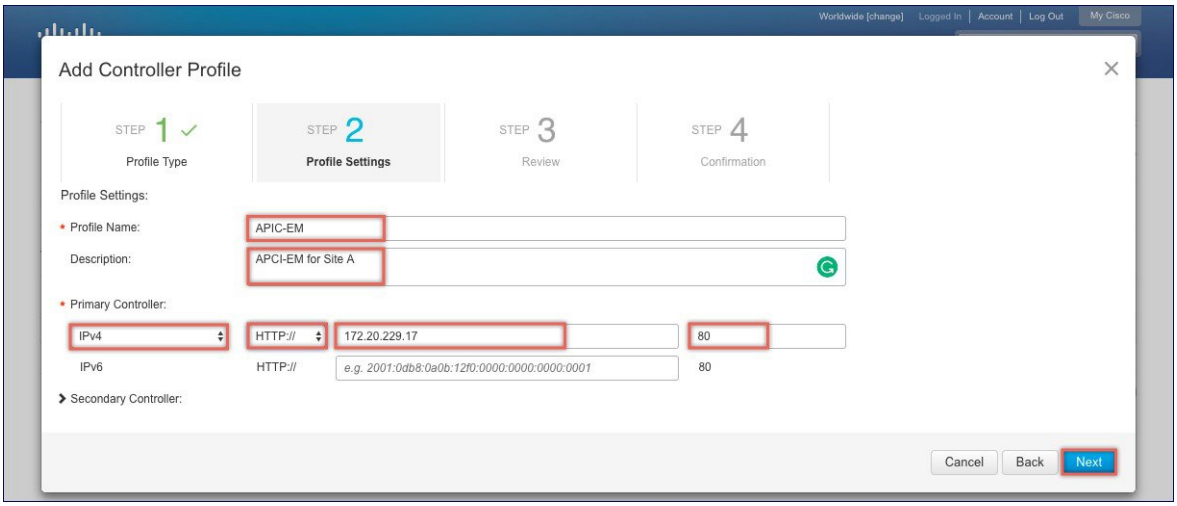
Step 6 Enter the following and click **Next**.

a. Profile Name

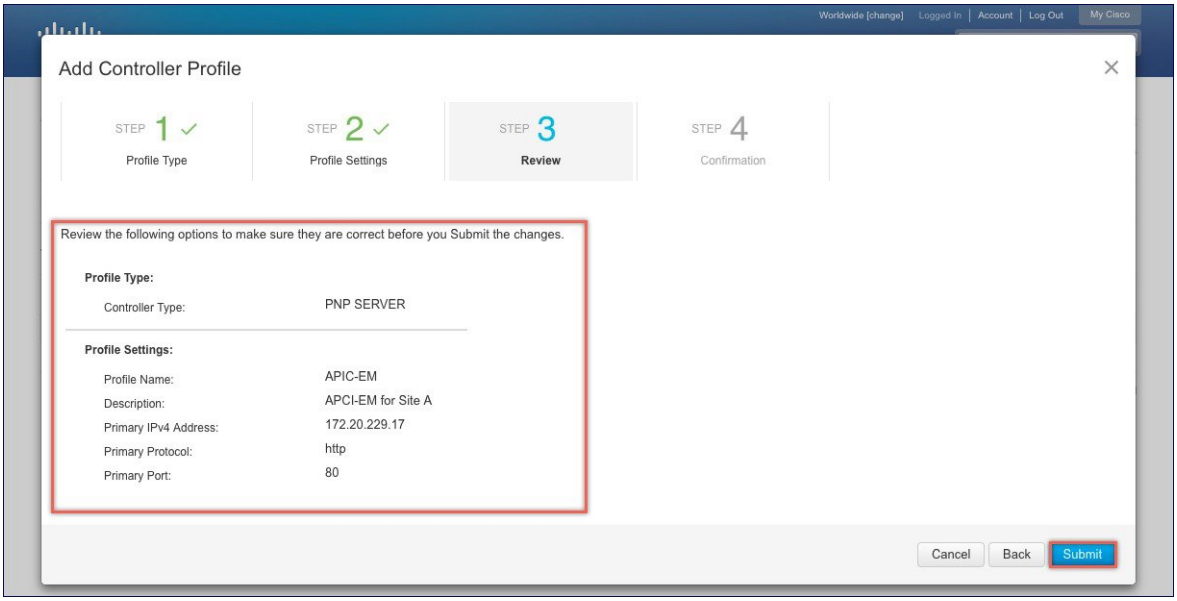
b. Description

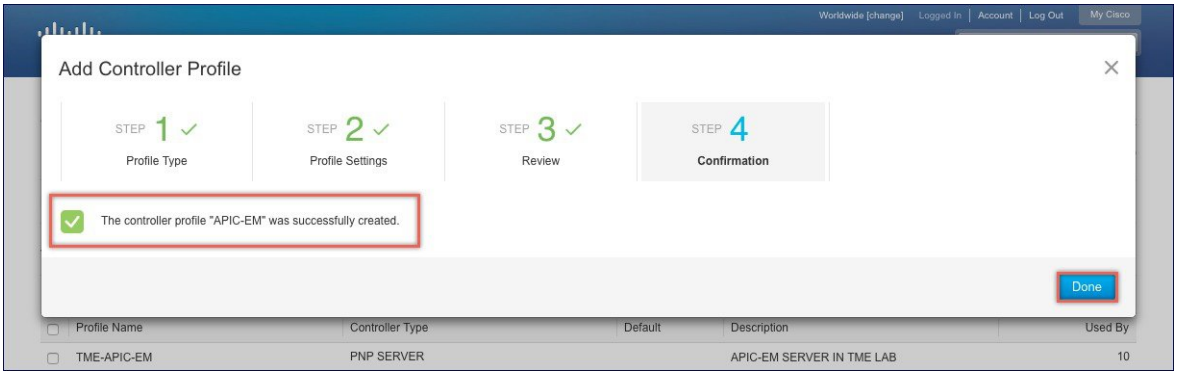
c. Select IPv4 or IPv6, HTTP or HTTPS and enter the IP address if the PNP Server

Note If you select HTTPS, then you would have import a SSL certificate. Also, optionally one can enter information of the secondary controller.



Step 7 Review the entries and click on Submit button to add the Controller Profile and finally click **Done**.





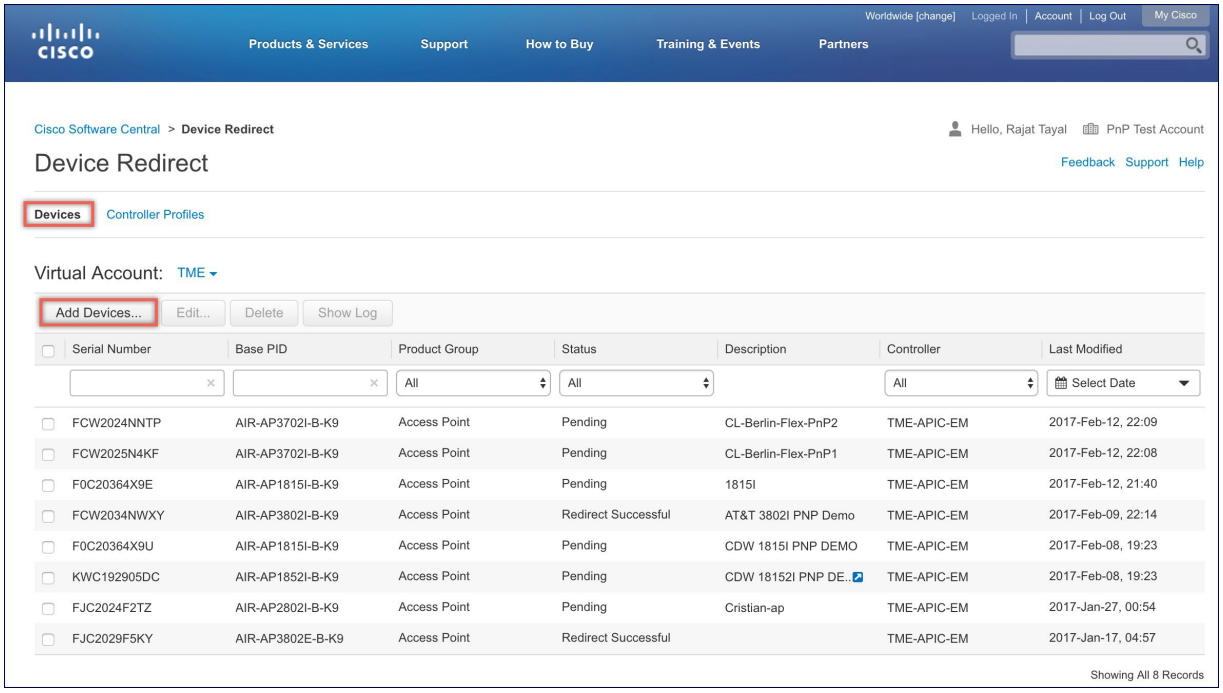
Adding Cisco Mobility Express capable Access Point to the Devices list

Procedure

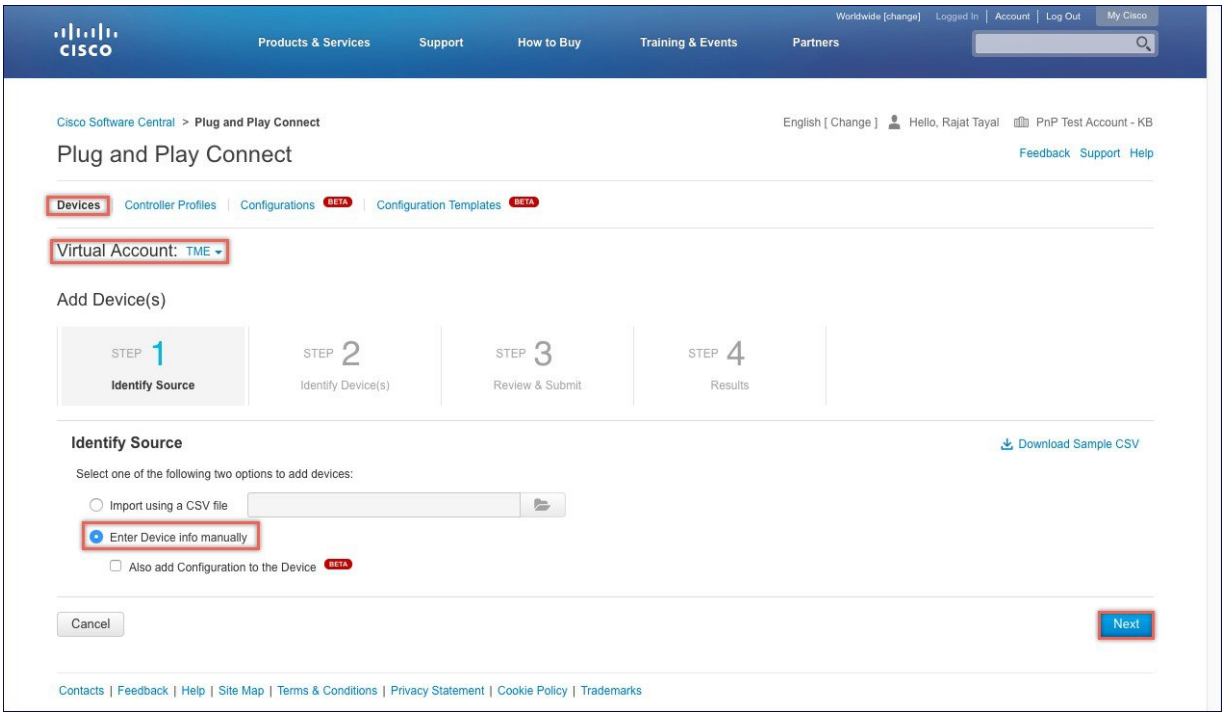
Step 1 Navigate to Provisioning > Plug and Play Connect. Click on Devices.

Step 2 Click on Devices. Select a Virtual Account. If you do have one, create a Virtual Account first.

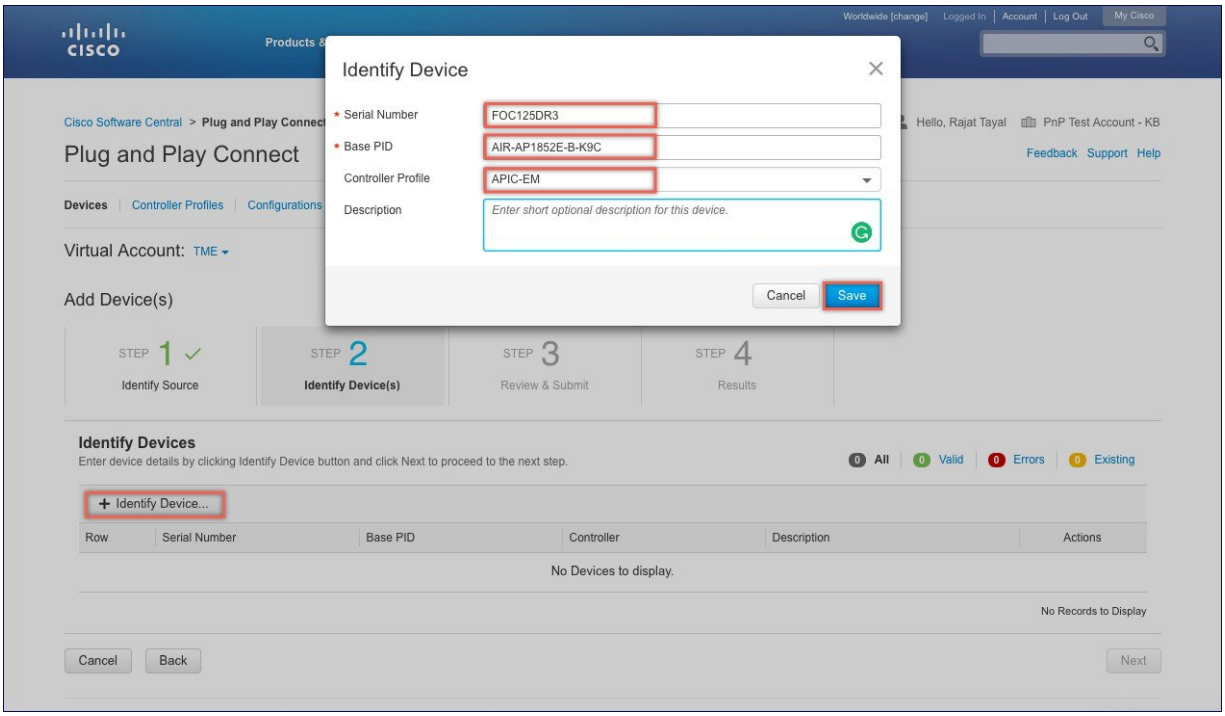
Step 3 Click on Add Devices button to add a new device (Mobility Express Access Point).



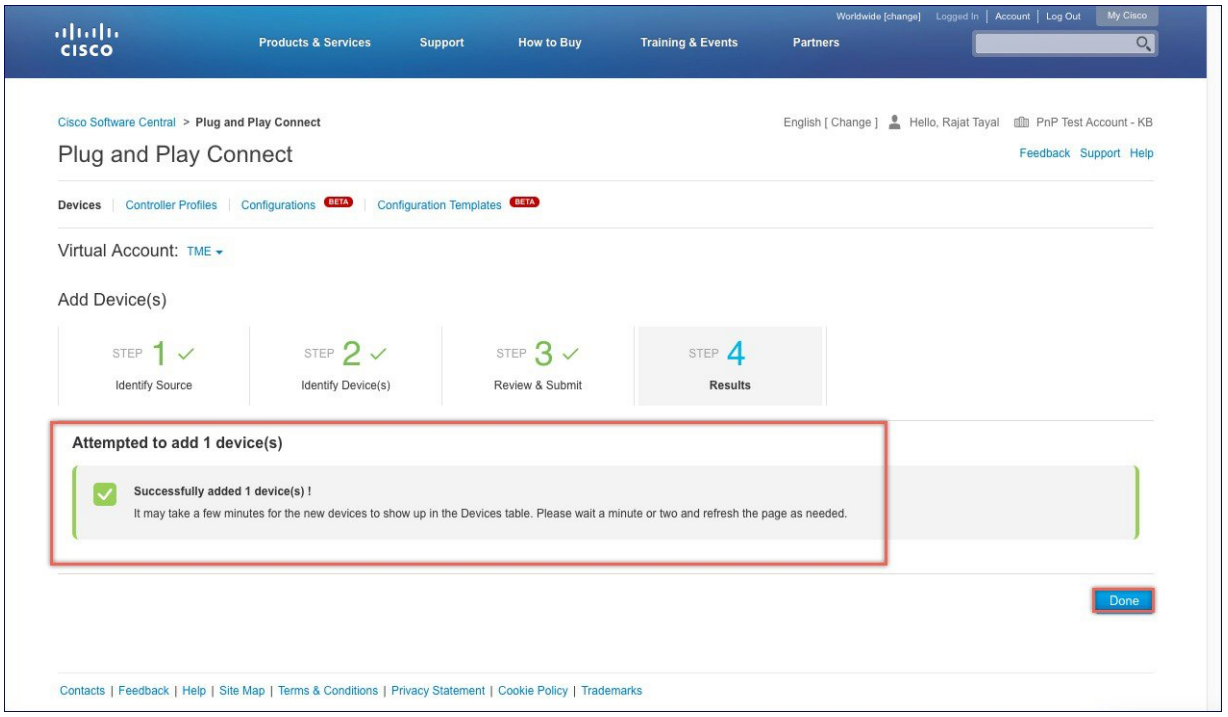
Step 4 Import a csv file with the Device info or select Enter Device info manually. Click **Next**.



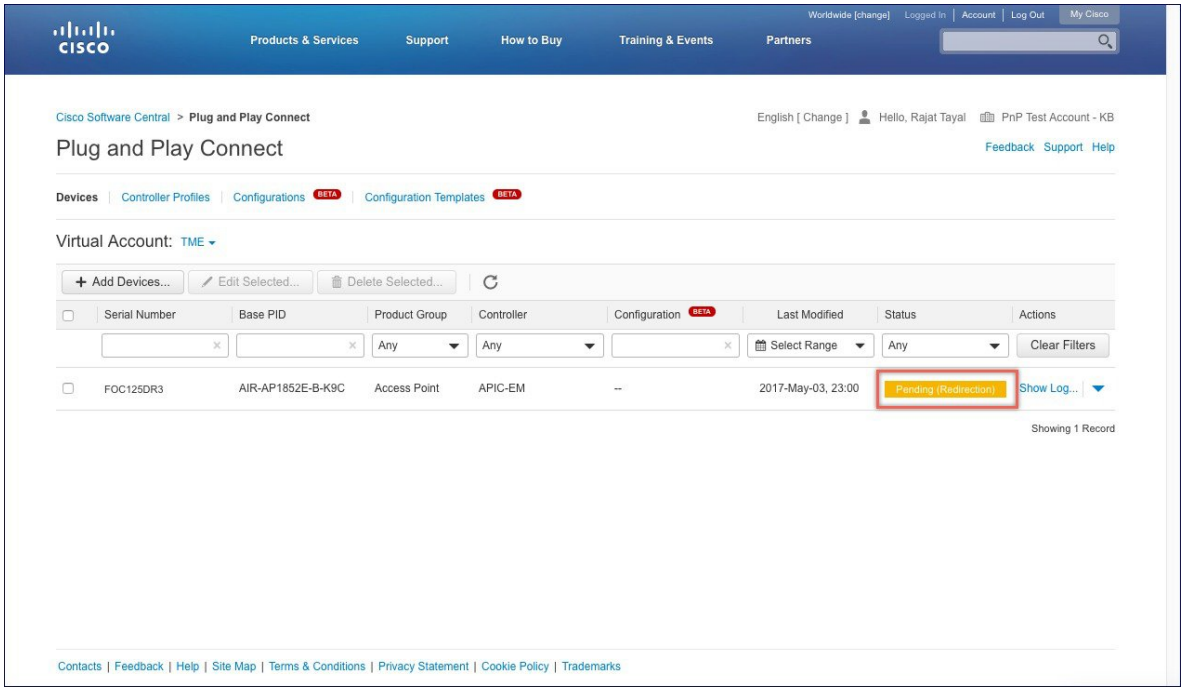
Step 5 Click on Identify Device button. The Identify Device window will pop up. Enter Serial Number, select Base PID, and Controller Profile(created earlier). Click on the Save button followed by Next button.



Step 6 Review the entries and click on Submit button to add the Device. Finally, click Done.



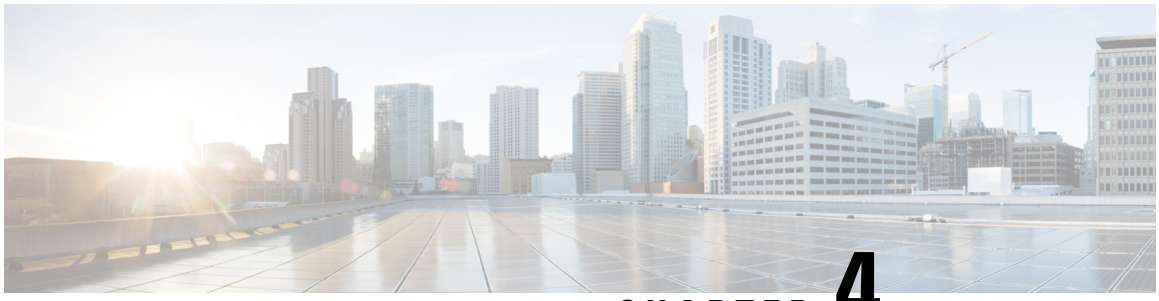
Step 7 Verify that the Device has been added and the status is Pending (Redirection).



Connecting Cisco Mobility Access Points

To bring up a new Mobility Express site, make sure that Plug and Play service has been configured with Mobility Express Access Points with related controller configuration. If APIC-EM controller in Private Cloud deployment option is used, Option 43 or DNS discovery on DHCP scope must be configured. If Cloud Plug and Play Connect redirect to APIC-EM controller deployment option is used, make sure all the related configuration on Cloud Plug and Play Connect has also been done for successful redirect to APIC-EM controller.

Now, it is time to connect the Mobility Express Access Points at the site. One may connect one or more Access Points at a site. It is important to note that if multiple Mobility Express Access Points are connected at a site, Master Election will happen first and only after Master Access Point has been elected, it will initiate communication with the Network Plug and Play service and download the controller configuration file regardless of the deployment option. The other Access Points will not initiate communicate with the Network Plug and Play service. After the controller configuration file has been downloaded on the Access Point, it will reboot and after it comes up, it will run the controller. The rest of the Access Points at the site will join this Master Access Point as Subordinate Access Points.



CHAPTER 4

Using internal DHCP server on Cisco Mobility Express

Starting Release 8.3.102.0, one can enable internal DHCP Server and create scopes for Access Points and WLANs. A total of 17 DHCP scopes are supported on Cisco Mobility Express. Using the internal DHCP server also enables Cisco Mobility Express to be used for performing Site Survey without the need of an external DHCP server.

Note Using a mix of Internal DHCP server and External DHCP server at the same time in a Mobility Express Deployment is not supported at this time.

• Creating a DHCP Scope, on page 29

Creating a DHCP Scope

Internal DHCP server can be enabled and DHCP scope created during Day 0 from Setup Wizard as well as in Day 1 using the controller WebUI. Typically, one would create DHCP scopes in Day 1 if they want to associate the scopes with WLANs.

To create a scope and associate it to a WLAN using the controller WebUI, follow the procedure below:

Procedure

Step 1 Navigate to **Wireless Settings** > **DHCP Server** > **Add new Pool** . The **Add DHCP Pool** window will pop up.

Step 2 On the **Add DHCP Pool** window. Enter the following fields:

- Enter the **Pool Name** for the WLAN
- Enable the **Pool Status**
- Enter the **VLAN ID** for the WLAN
- Enter the **Lease Period** for the DHCP clients. Default is 1 Day
- Enter the **Network/Mask**

- Enter the **Start IP** for the DHCP pool
- Enter the End IP for the DHCP pool

  Note If the scope is for client devices connecting to the Centralized NAT, one must select **Mobility Express Controller** for **Default Gateway**

- Enter the Default Gateway for the DHCP pool
- Enter the **Gateway IP** for the DHCP pool
- Enter the **Domain Name** (Optional) for the DHCP pool
- For **Name Servers**, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated

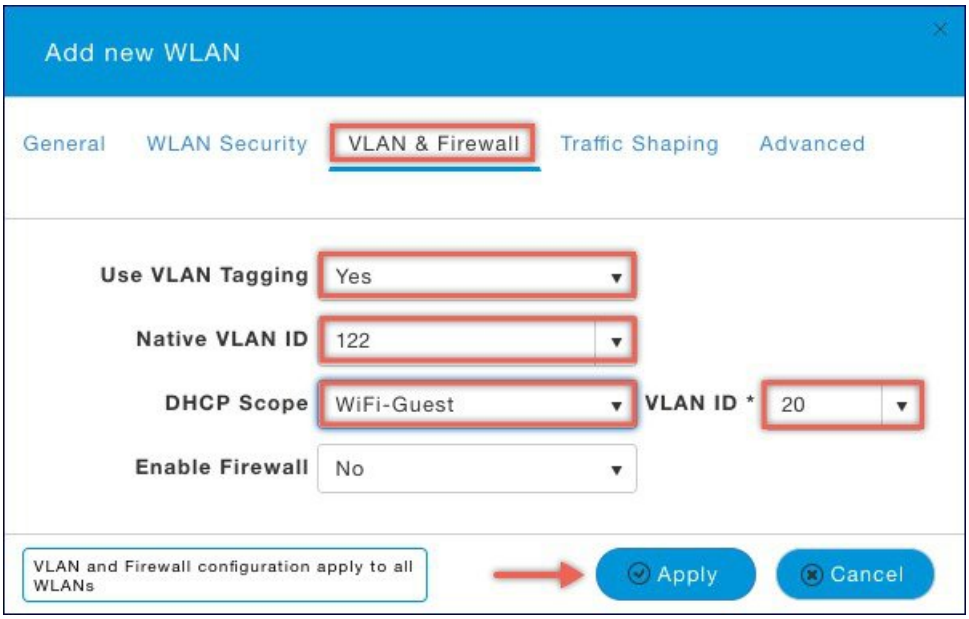
Step 3 Click **Appl**y.

Step 4 After creating the scope, it is time to assign the VLAN mapped to the DHCP scope to the WLAN. To assign a VLAN to WLAN, navigate to **Wireless Settings > WLANs** .

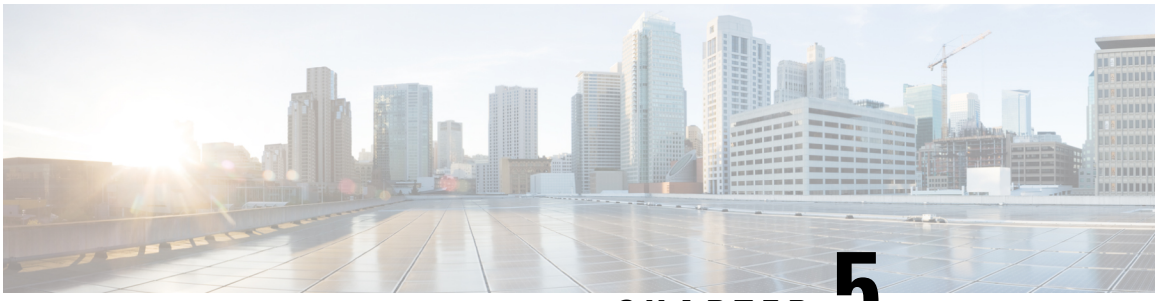
Step 5 If the WLAN does not exist, create a WLAN or if one does exist, edit the existing WLAN and click on the **VLAN and Firewall** tab.

Step 6 On the **VLAN and Firewall** tab, configure the following:

- Select **Network(Default)** for **Client IP Management** or **Mobility Express Controller** if this scope is for Centralized NAT'ed WLAN
- Select **Yes** to Use VLAN Tagging
- Enter the **Native VLAN ID**
- Select the **DHCP Scope** which was created previously for the WLAN. **VLAN ID** should be automatically populated after the DHCP scope is selected



Step 7 Click **Apply**.



CHAPTER 5

TLS Support on Mobility Express

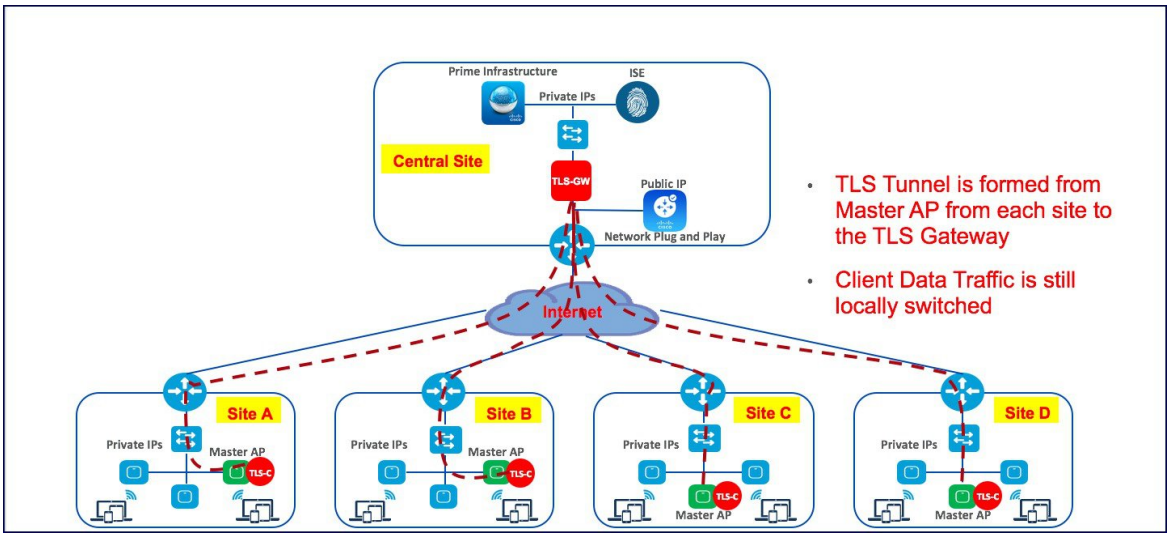
Cisco Mobility Express is a virtual wireless controller function embedded on 802.11ac Wave 2 Access points. With the flexibility of running a wireless LAN controller function on an access point, customers can deploy an Enterprise wireless solution on a single site or multiple sites with up to 100 Access Points at each site. In a multi-site deployment, customers can manage each of the sites using Cisco Prime Infrastructure which would typically be deployed in a central site. However, if the individual sites are connected to the internet via an ISP and are not connected via a dedicated WAN, managing these multi-site deployments can pose a challenge.

To overcome this challenge, starting AireOS Release 8.6, Cisco Mobility Express, customers can now manage the multi-site deployment using Cisco Prime Infrastructure over a TLS Tunnel. In addition to managing these sites, they can also aggregate their DOT1x authentication request to a RADIUS(ISE) which can be deployed along site CPI at the central site.

Please note that only SNMP, RADIUS and SSH traffic flows on the TLS tunnel to the central site and data traffic is still switched locally at individual sites.

TLS Tunnel has two components

1. TLS Client–Starting AireOS Release 8.6, TLS Client has been embedded in the Cisco Mobility Express code and will run on the Master AP
2. TLS Gateway –This is a Virtual Machine which is deployed at the central site to establish the TLS Tunnel. TLS Gateway has two network interfaces
   a. Public Network–This is the public IP which is reachable from every Master AP. The TLS client establishes a TLS tunnel between Master AP and TLS Gateway using this address.
   b. Private Network–This the IP address of the private network behind the TLS Gateway where the Cisco Prime Infrastructure, RADIUS and other network devices are deployed.



• TLS Gateway, on page 34
• TLS Client, on page 44

TLS Gateway

TLS Gateway is virtual machine and is deployed at the central site.

Note TLS Gateway does not support Cisco Mobility Express platform.

System Requirement for TLS Gateway

1. Hypervisor: VMware–ESXi 5.5.0/ESXI 6.0
2. VM Resources
   a. 4 vCPU
   b. 8GB RAM
   c. 100 GB Storage
   d. 2 NICs (One for Public network and one Private network)
3. IP routing requirements
   a. Routing enabled from TLS-GW Private network towards Prime-infra(SNMP), ISE(Radius), DHCP servers, SSH, Monitoring system and vice-versa
4. TLS-GW public IP should be Reachable from Management IP of ME-AP

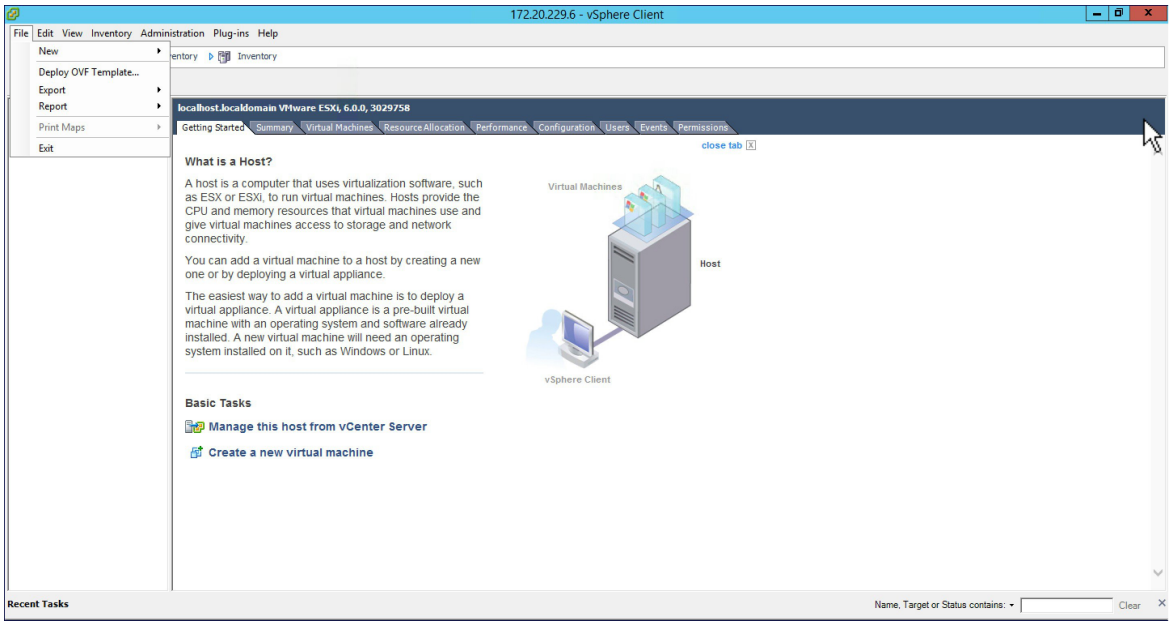
Deploying TLS Gateway

Please follow the steps below to deploy a TLS Gateway at the central site.

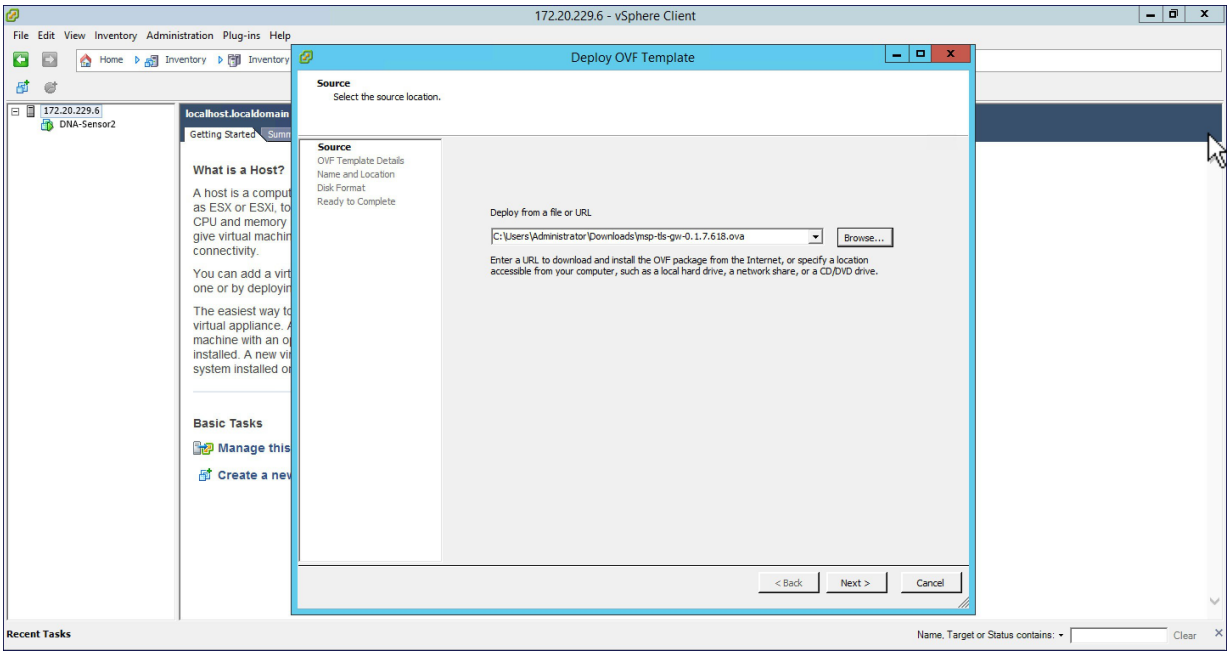
Procedure

Step 1 Secure the TLS Gateway OVA File

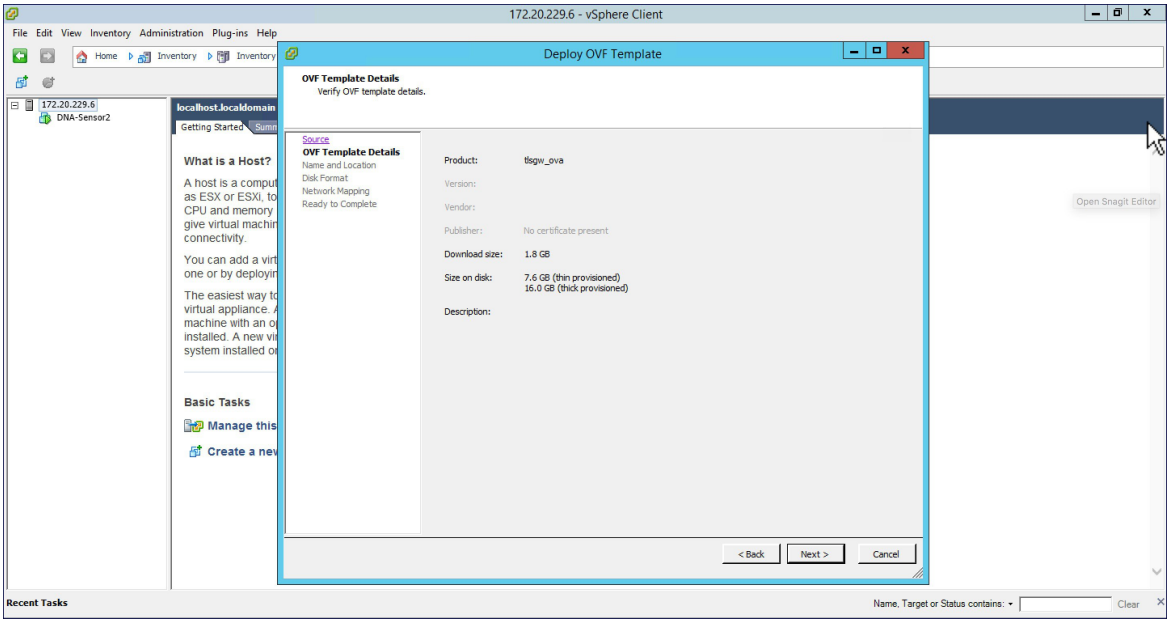
Step 2 Navigate to File > Deploy OVF Template on the vSphere Client UI.



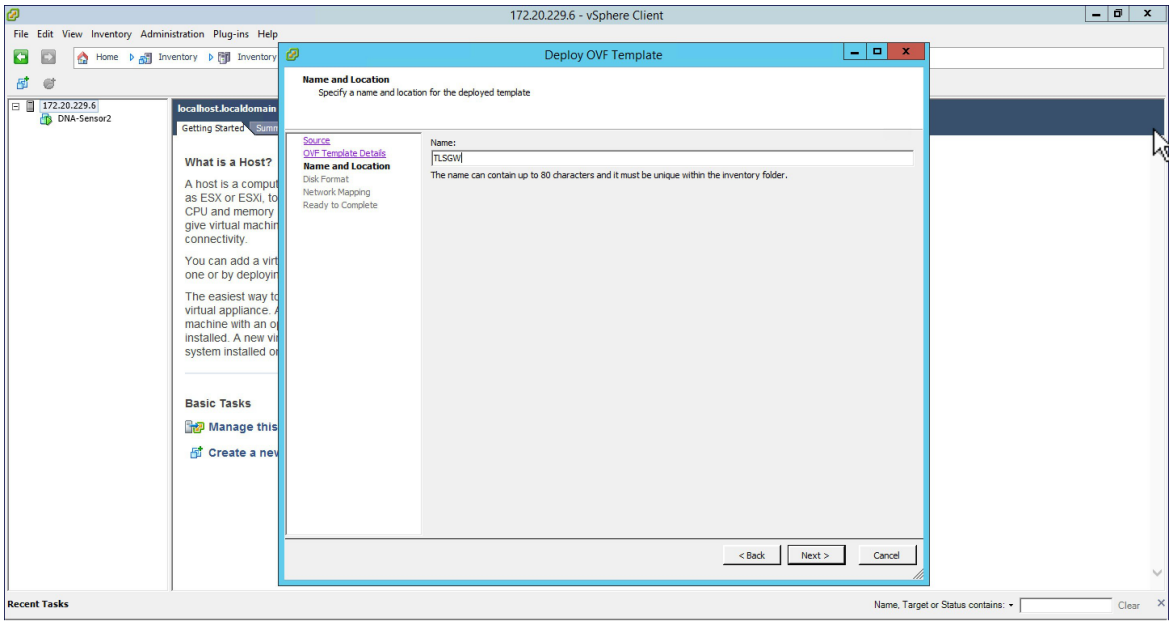
Step 3 Browse to the TLS Gateway OVA file on your local machine. Click Next.



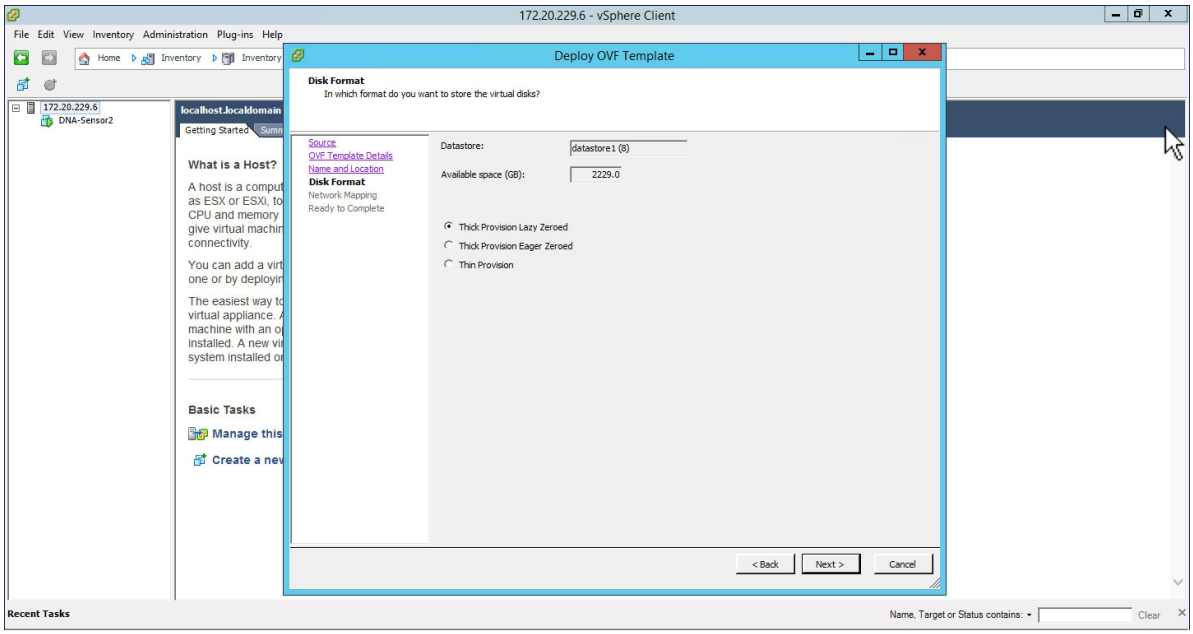
Step 4 Check the OVF Template details and click Next.



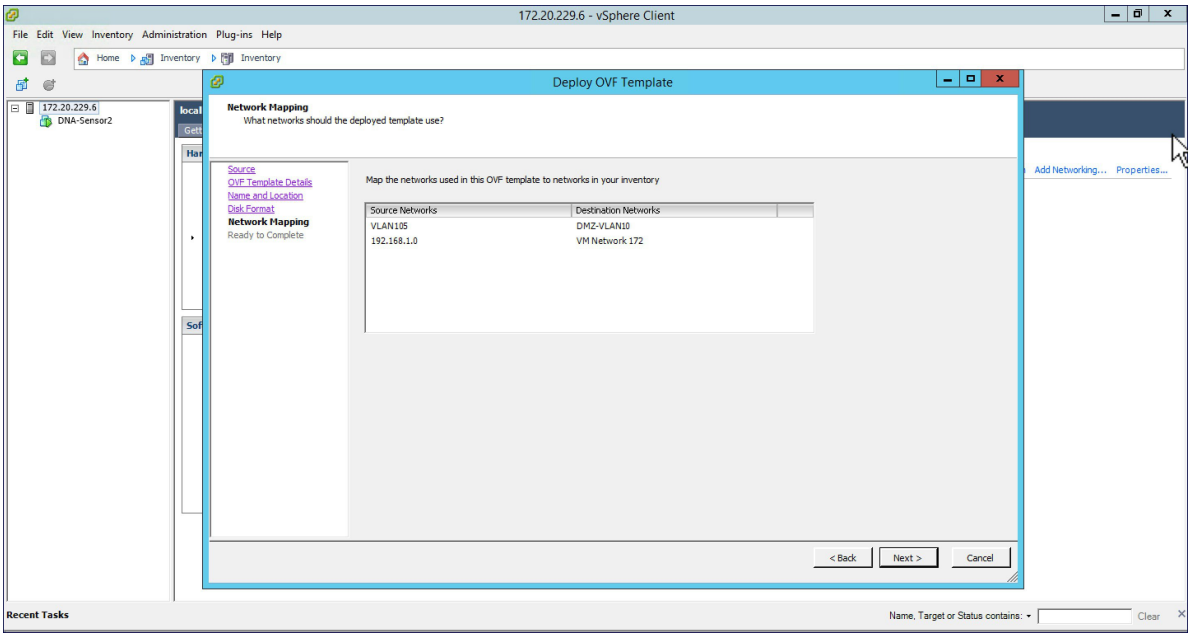
Step 5 Specify the name for the TLS Gateway Virtual Machine.



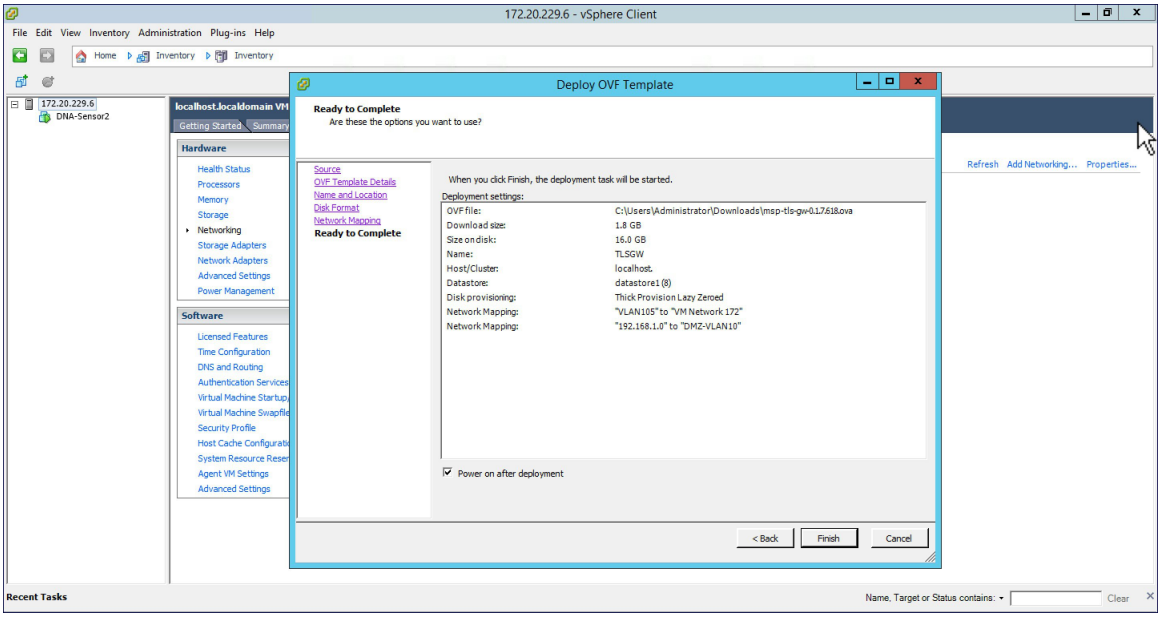
Step 6 For Disk Format, stay with the default and click Next.



Step 7 For Network Mapping, select the Destination Network for the Public Network interface. Click on Next.



Step 8 Verify the Deployment Settings. Enable the 'Power On after deployment' check box and click Finish.



Configuring TLS Gateway

Configuring the TLS Gateway comprises of 3 things:

1. Configure the IP address for Public and Private network interfaces
2. Configure the TLS Gateway configuration file and start the service

3. Configuring the PSK ID-KEY Pair

After the OVA for TLS Gateway is deployed and powered up, follow the steps below to configure the TLS Gateway.

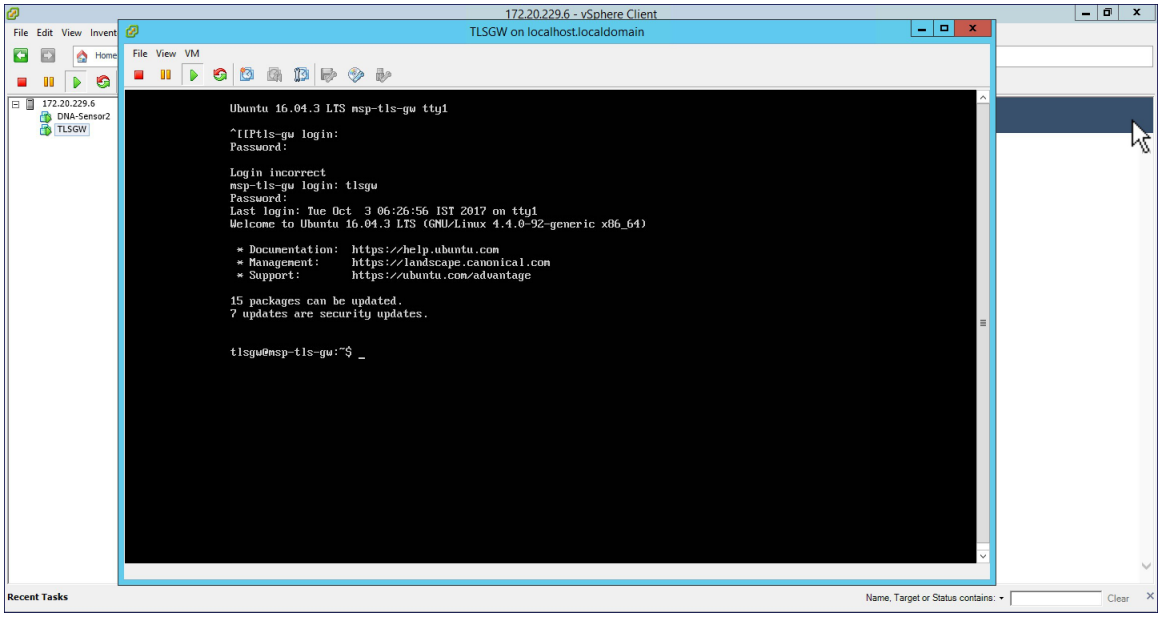
Configuring IP Address for Public and Private network interfaces

Procedure

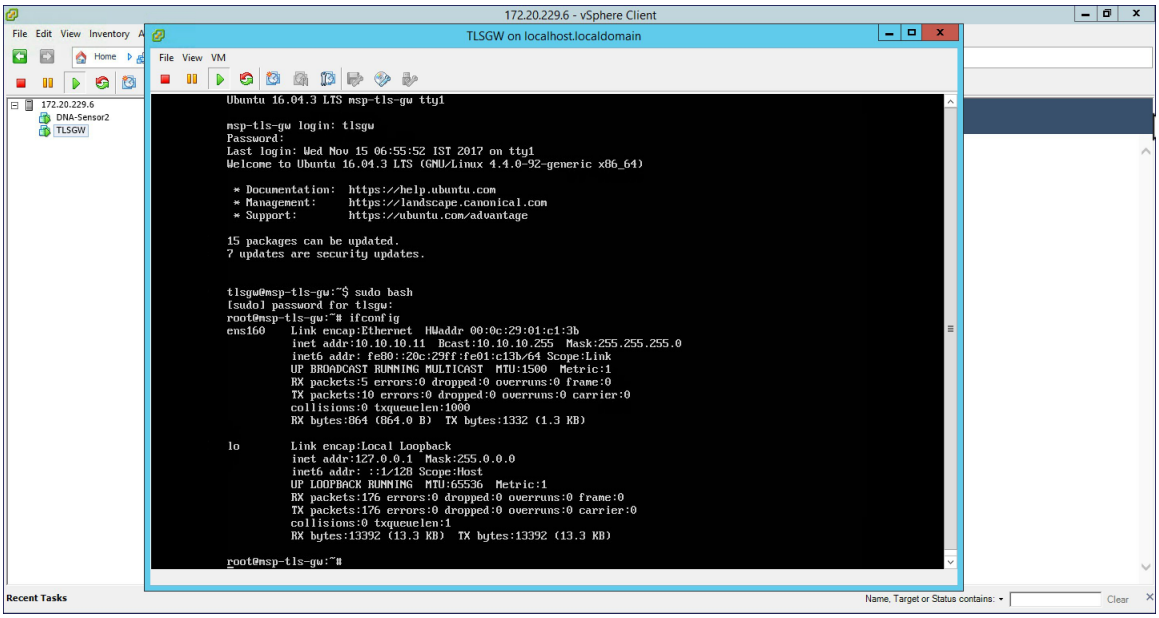
Step 1 Open a console session to the TLS Gateway VM and login using the following credentials:

username: tlsgw

password: tlsgw



Step 2 Type ***ifconfig*** to verify the IP address of the Public and Private interfaces as shown below.

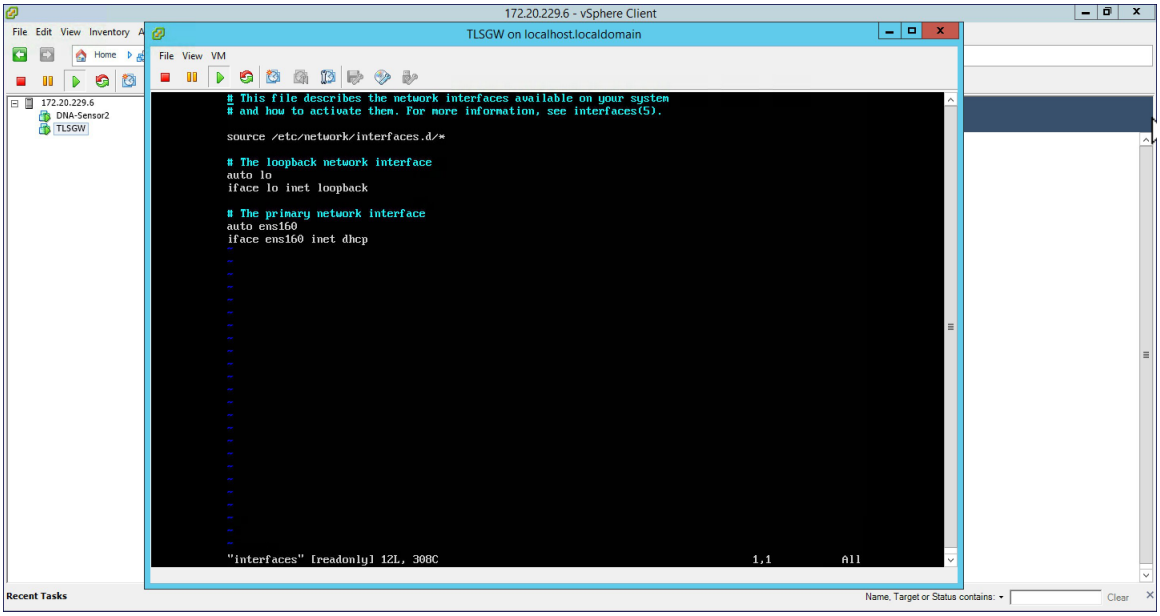


Note ***ens160*** corresponds to the Public network interface and in the above example it has got the IP of ***10.10.10.11*** from the DHCP server. One can also statically assign the IP address which will be shown the steps ahead. Also, there is no interface for the Private network in the ***ifconfig*** output above. We can also manually configure this and is shown in the steps ahead.

Step 3 At the **tlsgw@msp-tls-gw:** prompt type ***sudo bash*** and enter ***tlsgw*** as the [sudo] password for tlsgw.

Step 4 To configure IP address for Public and Private network interface go to ***/etc/network*** directory by typing ***cd /etc/interfaces*** at the shell.

Step 5 Open the ***interfaces*** file using vi editor by typing ***vi interfaces*** at the shell.

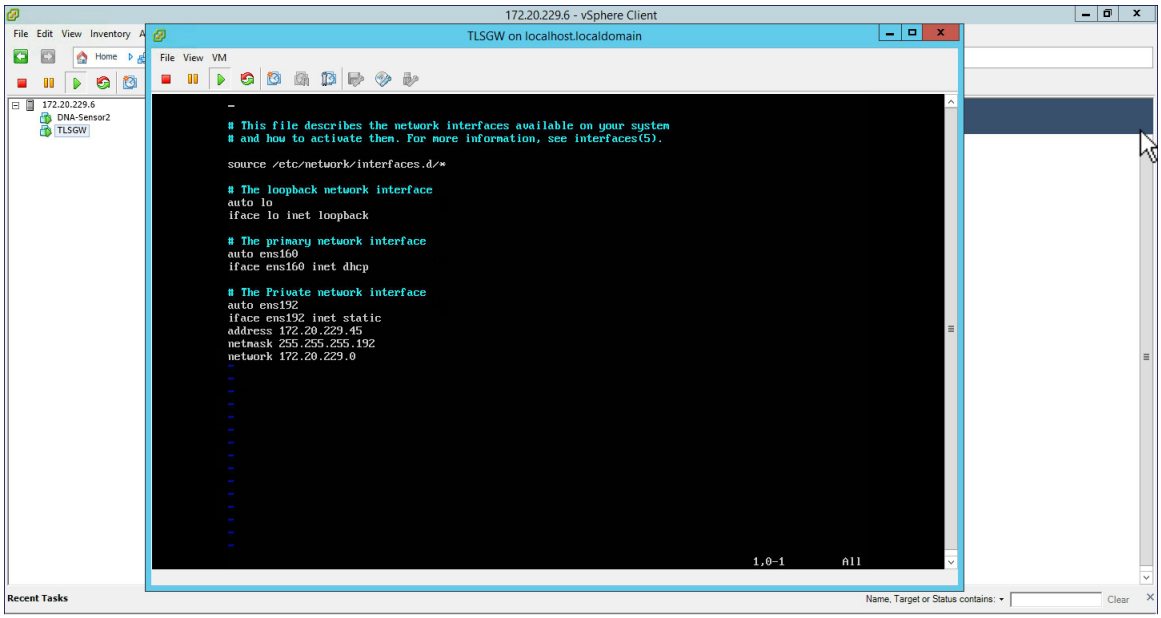


Note : ***ens160*** is Public network interface and is configured for DHCP by default. If you want to statically configure the IP address of Public network interface, replace the ***ens160*** setting with the following as shown below in the example.

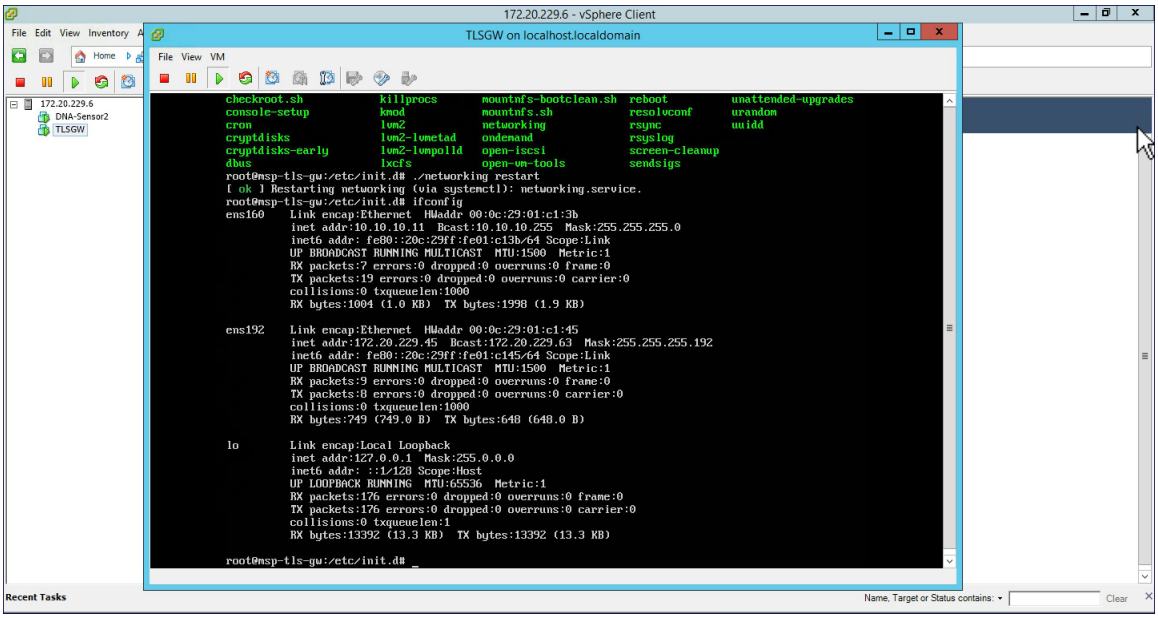
```
auto ens160
iface ens160 inet static
address 10.10.10.11
netmask 255.255.255.0
network 10.10.10.0
```

Step 6 To configure the Private network interface IP address, add the following in the ***interfaces*** file as shown below and save the file.

```
auto ens192
iface ens192 inet static
address 172.20.229.60
netmask 255.255.255.192
network 172.20.229.0
```



Step 7 To restart the network service, go to ***/etc/init.d*** and type ***./networking restart*** . Now, do a ifconfig and you should see both the Public interface IP address and Private interface IP address. Ping both Public and Private IP address to verify connectivity.



Configure the TLS Gateway configuration file and start the service

Procedure

Step 1 : Go to ***/opt/cisco/msp-tls-gw/bin/*** and edit the ***tlsgw_config.txt*** with the following:

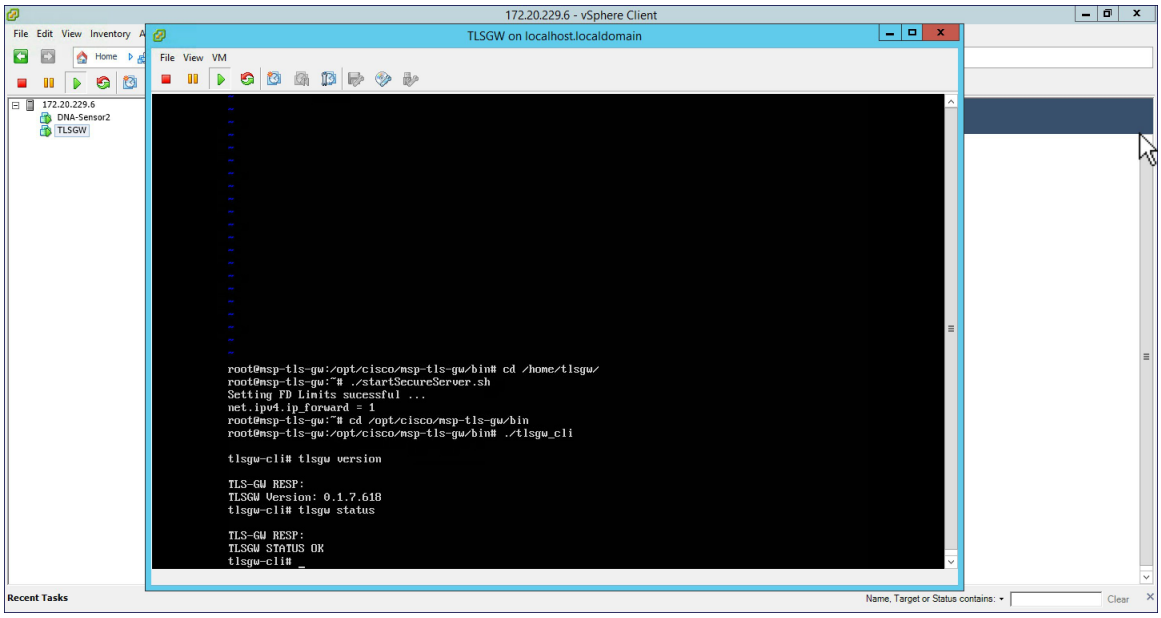
```
server_listening_ipv4_address=10.10.10.11 // Public IP of TLS Gateway
server_listening_port=443 // Port
server_private_ipv4_address=172.20.229.45 // Private IP of TLS Gateway
prefix_subnet=172.20.229.0 // Private IP network of TLS Gateway
prefix_length=26
debug_level=4 // Loglevel for TLS Gateway
dhcp_static_pool_ipv4=20.1.0.0:255.255.0.0 // Local IP pool configured for TLS Client IP
allocation
dpd_interval=60 // Dead Pear Detection timer value for client
rekey_interval=3600 // Rekey timer value  for client
retry_interval=20 // Retry timer value for client
```

Note If you are using a DHCP server behind the TLS Gateway, do not configure dhcp_static_pool_ipv4 in tlsgw_config.txt file. This is because broadcast is sent via Private IP of tls-gw and if DHCP server exists behind the TLS Gateway, it should assign TLS Client an IP address.

Step 2 Save the file.

Step 3 Go to ***/home/tlsgw*** and start the TLS Gateway service with script ***./startSecureServer.sh***

Step 4 To verify that the TLS Gateway service is running successfully, go to ***/opt/cisco/msp-tls-gw/bin/*** and run ***./tlsgw_cli*** as shown below.



Configuring the PSK ID-KEY pair

Configure the Pre Shared Key(PSK) on the TLS Gateway. This will be used by the TLS client on the Master AP to authenticate with the TLS Gateway.

Note A maximum of 3 PSK ID-KEY pairs can be set for TLSGW. PSK-ID can be any character string of length (3-50), PSK password(or key) can be any character string of length (5-256) , Character ':' or 'space' or 'tab' are not allowed for both psk-id and psk-key.

To configure, follow the steps below:

Procedure

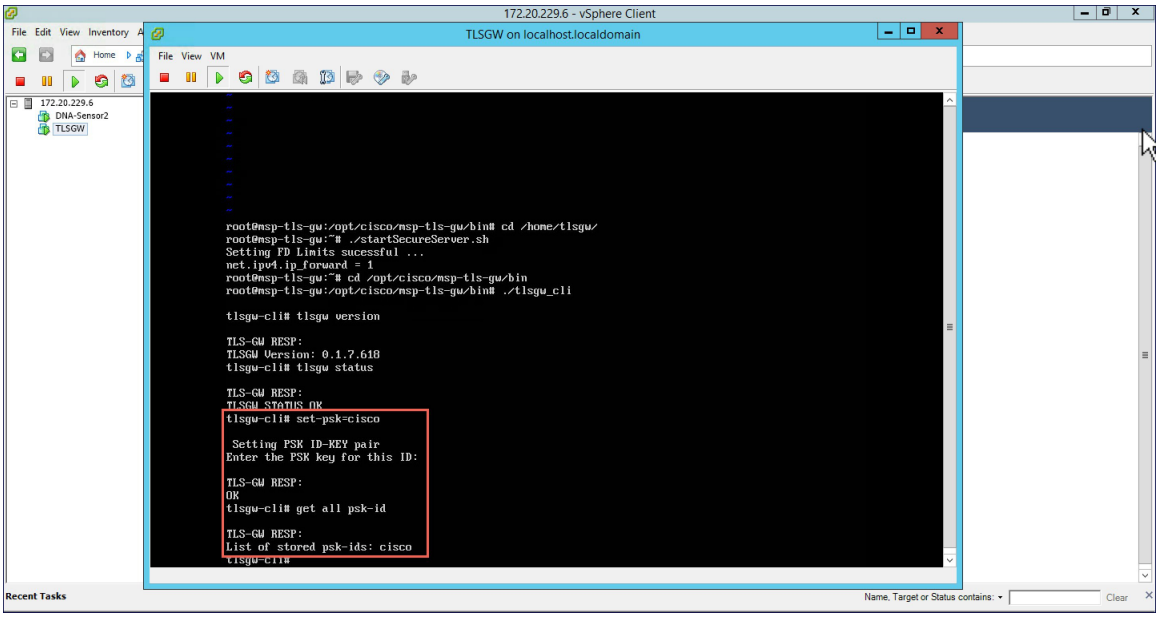
Step 1 : Go to ***/opt/cisco/msp-tls-gw/bin/*** and run ***./tlsgw_cli***

Step 2 Configure the PSK using the following CLI:

```
tlsgw-cli# set-psk=cisco
 Setting PSK ID-KEY pair
Enter the PSK key for this ID:
TLS-GW RESP:
OK
```

Step 3 Verify that the PSK ID is configured using the following CLI:

```
tlsgw-cli# get all psk-id
TLS-GW RESP:
List of stored psk-ids: cisco
```



TLS Client

TLS Client is integrated in the AireOS Release 8.6 and is natively present in the code. For TLS client to establish a TLS tunnel with TLS Gateway, Master AP should be able to communicate with the Public IP of the TLS Gateway.

Pre-Requisites for TLS Client

1. Cisco Mobility Express AireOS release 8.6 or higher
2. TLS Gateway Public IP address should be reachable from the Master AP. If TLS Gateway FQDN is used then, TLS_GW FQDN should be configured in the local DNS server, and same DNS server IP should be configuring on ME controller to Resolve the FQDN of TLS Gateway

Configuring TLS Tunnel

There are two ways to configure the TLS Tunnel between TLS Client and TLS Gateway. They are as follows:

Option 1: Zero touch provisioning using Network PnP

During Day 0, one can download the controller configuration from Network PnP. The TLS Tunnel configuration can also be included in the controller configuration file such that after the Master AP downloads the configuration file, reboots, and comes back up, it will automatically establish a TLS Tunnel with the TLS Gateway.

Option 2: Manually configure the TLS Tunnel from WebUI

To configure the TLS Tunnel from the ME WebUI, follow the steps below:

Procedure

Step 1 Switch to Expert View on the Controller WebUI

Step 2 Navigate to Services > TLS from the menu on the left

Step 3 On the TLS Tunnel page, configure the following parameters:

a. Enter the TLS Gateway Public IP address or FQDN

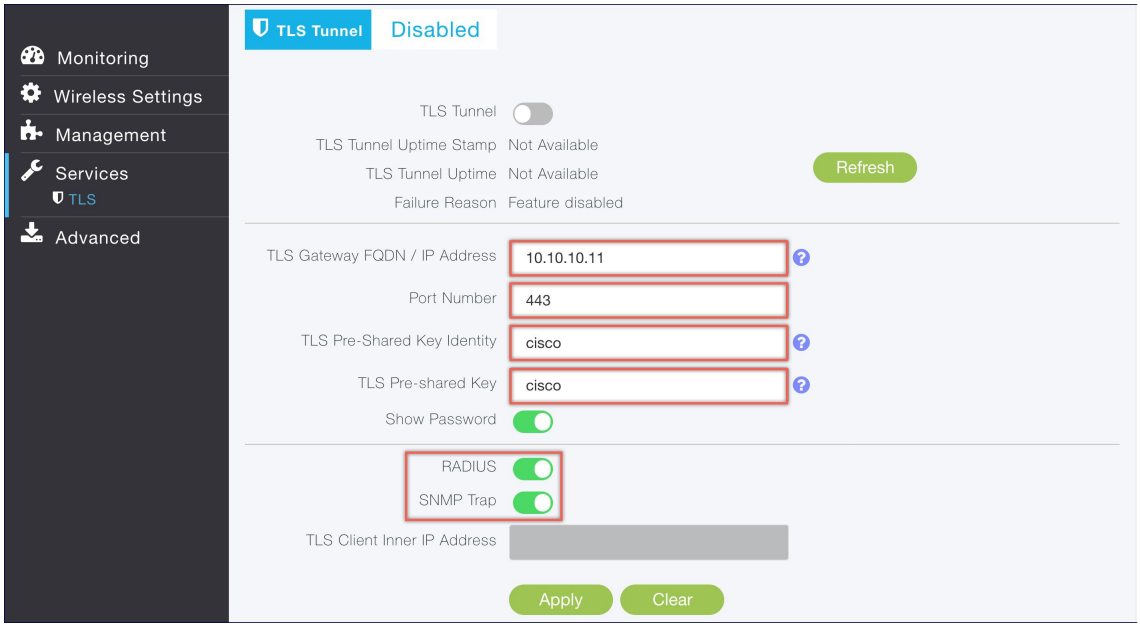
b. Enter the port number. Default is 443

c. Enter the PSK ID

d. Enter the PSK Key

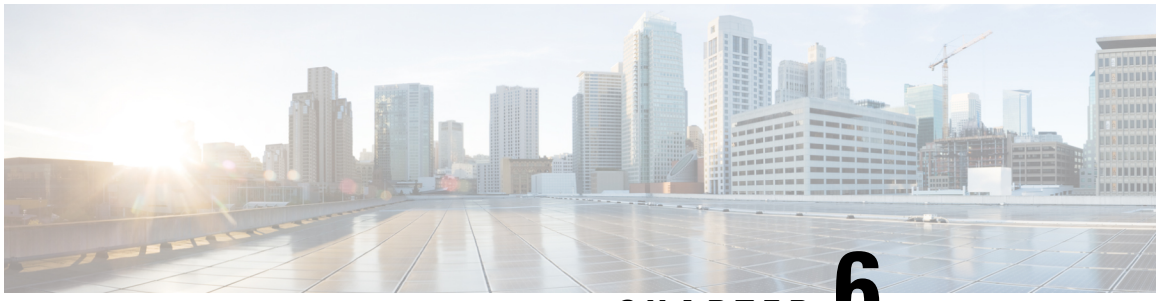
e. Enable RADIUS and SNMP

Note RADIUS would be used for ISE and SNMP would be used for Prime Infrastructure.



Step 4 Click Apply.

Step 5 Finally, enable the TLS Tunnel at the top of the page. If all pre-requisites are met, a tunnel would be created from the Master AP to the Public interface if TLS Gateway.



CHAPTER 6

Configuring Cisco Mobility Express for Site Survey

Configuring Cisco Mobility Express for Site Survey

Cisco 802.11ac Wave 2 access points are capable of running Cisco Mobility Express which a virtual wireless controller function embedded on an Access Point.

Cisco Mobility Express access point running the wireless controller function will also provide wireless connectivity to the clients. It also supports internal DHCP server which enables Access Point to be used for Site Survey.

Pre-requisites

1. Access Points–Cisco 802.11ac Wave 2 access points running Cisco Mobility Express software. The following APs support Cisco Mobility Express:

Access Point	Release supporting Site Survey capability
1540 Series	AireOS® Release 8.5 and later
1560 Series	AireOS Release 8.3.111.0 and later
1815I Series	AireOS Release 8.4 and later
1815M Series	AireOS® Release 8.5 and later
1815W Series	AireOS Release 8.4 and later
1830 Series	AireOS Release 8.3.111.0 and later
1850 Series	AireOS Release 8.3.111.0 and later
2800 Series	AireOS Release 8.3.111.0 and later
3800 Series	AireOS Release 8.3.111.0 and later

2. Power Source–Depending on the Access Point being used for Site Survey, one can use a power adapter or a battery pack capable of providing sufficient power to the Access Point.

3. Console Cable(Optional)–Cisco Mobility Express can be configure using the CLI or Over-the-air. For configuring Cisco Mobility Express via CLI, a console connect to the Access Point would be required.

Configuring Mobility Express for Site Survey using CLI

Procedure

Step 1 Connect to the console of the Access Point.

Step 2 Power up the Access Point using a power adapter or battery pack.

Step 3 Wait for the Access Point to boot up completely such that it is running the Wireless Controller and is waiting to be configured.

Step 4 Configure the Wireless Controller using the CLI Setup Wizard:

Note For Site Survey, a DHCP server is required and is supported on Cisco Mobility Express. DHCP Server configuration highlighted below is mandatory if you want to enable DHCP server on Cisco Mobility Express.

```
Would you like to terminate autoinstall? [yes]:yes
Enter Administrative User Name (24 characters max):admin
Enter Administrative Password (3 to 24 characters max):Cisco123
Re-enter Administrative Password: Cisco123
System Name:[Cisco_3a:d2:b4] (31 characters max):me-wlc
Enter Country Code list(enter 'help' for a list of countries)[US]:US
Configure a NTP server now?[YES][no]:no
Configure the system time now?[YES][no]:yes
Enter the date in MM/DD/YY format:02/28/17
Enter the time in HH:MM:SS format:11:30:00
Enter timezone location index(enter 'help' for a list of timezones):5
Management Interface IP Address: 10.10.10.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Create Management DHCP Scope?[yes][NO]:yes
DHCP Network: 10.10.10.0
DHCP Netmask: 255.255.255.0
Router IP: 10.10.10.1
Start DHCP IP address: 10.10.10.10
Stop DHCP IP address: 10.10.10.250
DomainName: mewlc.local
DNS Server:[OPENDNS][user DNS]OPENDNS
Create Employee Network?[YES][no]:yes
Employee Network Name(SSID)?:site_survey
Employee VLAN Identifier?[MGMT][1-4095]:MGMT
Employee Network Security?[PSK][enterprise]:PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]:NO
Enable RF Parameter Optimization?[YES][no]:no
Configuration correct? If yes, system will save it and reset.[yes][NO]:yes
```

Step 5 Wait for the Access Point to boot up completely. After the Wireless controller has started, log back in to the controller using administrative username or password configured during the initial setup wizard.

Step 6 (Optional): During the CLI setup wizard, Employee Network Security was configured to PSK. This can be disabled for easy association of clients and also disable SSID broadcast to avoid unwanted clients from joining the SSID. To disable PSK and SSID broadcast, enter the following commands in the Controller CLI.

```
(Cisco Controller)>config wlan disable 1
(Cisco Controller)>config wlan security wpa disable 1
(Cisco Controller)>config wlan broadcast-ssid disable wlan 1
(Cisco Controller)>config wlan enable 1
(Cisco Controller)>save config
```

Step 7 To configure channel, TX power, and channel bandwidth for the radios, disable the radio first, make the changes and then re-enable it.

To change the 2.4GHz radio to channel 6, follow the steps below:

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b channel <ap name> <ap name> 6
(Cisco Controller)>config 802.11b enable <ap name>
```

To change the 2.4GHz radio Transmit Power to power level 3, follow the steps below:

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b txPower <ap name> <ap name> 3
(Cisco Controller)>config 802.11b enable <ap name>
```

To change the 5 GHz radio to channel 44, follow the steps below:

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a channel <ap name> <ap name> 44
(Cisco Controller)>config 802.11a enable <ap name>
```

To change the 5 GHz radio Transmit Power to level 5, follow the steps below:

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a txPower <ap name> <ap name> 5
(Cisco Controller)>config 802.11a enable <ap name>
```

To change the 5 GHz radio channel width to 40MHz, follow the steps below:

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a chan_width <ap name> 40
(Cisco Controller)>config 802.11a enable <ap name>
```

If 2800 and 3800 series access points are being used for Site Survey, please note the following with respect to the XOR radio.

a. Default operation state of XOR radio is 2.4GHz.

b. One can configure the XOR radio on internal (I) Access Points from 2.4GHz to 5 and vice versa. On an external (E) Access Point, one must have an external antenna plugged into the DART connector prior to changing any configuration on the XOR radio.

c. When the XOR (2.4 GHz) radio is configured to operate at 5GHz, 100MHz frequency separation is required from dedicated 5GHz radio.

d. When the XOR radio is configured to operate in 5GHz mode on an internal (I) Access Points, the Transmit power (tx) power will be fixed and cannot be modified.

To configure the XOR (2.4GHz) radio to operate at 5GHz on 2800 and 3800 Series Access Points, follow the steps below:

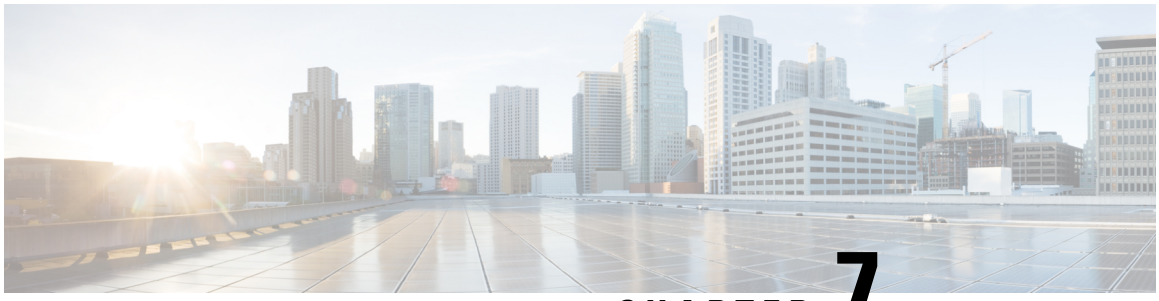
```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn role ap manual client-serving
(Cisco Controller) >config 802.11-abgn band ap ap 5GHz
(Cisco Controller) >config 802.11-abgn enable ap
```

To configure the XOR radio operating at 5 GHz to channel 40, follow the steps below:

```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn channel ap ap 40
(Cisco Controller) >config 802.11-abgn enable ap
```

To configure the XOR radio operating at 5 GHz channel width to 40MHz, follow the steps below:

```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn chan_width ap 40
(Cisco Controller) >config 802.11-abgn enable ap
```



CHAPTER 7

Creating Wireless Networks

WLANs

Cisco Mobility Express solution supports a maximum of 16 WLANs. Each WLAN has a unique WLAN ID (1 through 16), a unique Profile Name, SSID, and can be assigned different security policies.

Access Points broadcast all active WLAN SSIDs and enforce the policies that you define for each WLAN.

A number of WLAN Security options are supported on Cisco Mobility Express solution and are outlined below:

1. Open
2. WPA2 Personal
3. WPA2 Enterprise (External RADIUS, AP)

For Guest WLAN, a number of capabilities are supported:

1. CMX Guest Connect

2. WPA2 Personal
3. Captive Portal (AP)
4. Captive Portal (External Web Server)

Creating Employee WLANs

Creating Employee WLAN with WPA2 Personal

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and then click on **Add new WLAN** button. The **Add new WLAN** Window will pop up.

Step 2 In the **Add new WLAN** window, on the General page, configure the following:

a) Enter the **Profile Name**.
b) Enter the **SSID**.

Step 3 Click on the WLAN Security and configure the following:

a) Select **Security** as *WPA2 Personal*.
b) Enter the **Passphrase** and Confirm **PassPhrase**.

Step 4 Click **Apply**.

Creating Employee WLAN using WPA2 Enterprise with External Radius Server

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and then click on **Add new WLAN** button. The **Add new WLAN** Window will pop up.

Step 2 In the **Add new WLAN** window, on the General page configure the following:

a) Enter the **Profile Name**.
b) Enter the **SSID**.

Step 3 Click on the **WLAN Security** and configure the following:

a) Select **Security Type** as **WPA2 Enterprise**.
b) Select **Authentication Server** as **External Radius**.

Step 4 Add the Radius server and configure the following:

- Enter the Radius IP
- Enter the Radius Port

- Enter the Shared Secret
- Click on **tick** icon

Step 5 Click **Apply**.

Creating Employee WLAN with WPA2 Enterprise and Authentication Server as AP

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and then click on **Add new WLAN** button. The **Add new WLAN** Window will pop up.

Step 2 In the **Add new WLAN** window, on the General page configure the following:

a) Enter the **Profile Name**.
b) Enter the **SSID**.

Step 3 Click on the **WLAN Security** and configure the following:

a) Select **Security** as **WPA2 Enterprise**.
b) Select **Authentication Server** as **AP**.

Note AP is the Master AP running the controller function. In this use case, controller is the Authentication Server and therefore Local WLAN user account must exist to onboard the clients.

Step 4 Click the **Apply**.

Creating Employee WLAN with WPA2 Enterprise/External RADIUS and MAC Filtering

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and then click on **Add new WLAN** button. The Add new WLAN Window will pop up.

Step 2 In the Add new WLAN window, on the **General** tab, configure the following:

- Enter the **Profile Name**
- Enter the **SSID**

Step 3 Click on the **WLAN Security** tab and configure the following:

- Enable **MAC Filtering**

- Select **Security Type** as **WPA2 Enterprise**
- Select **Authentication Server** as **External RADIUS**
- Select **RADIUS Compatibility** from the drop-down list
- Select **MAC Delimiter** from the drop-down list

Step 4 Add the Radius server and configure the following:

- Enter the **Radius IP**
- Enter the **Radius Port**
- Enter the **Shared Secret**
- Click on **tick** icon.

Step 5 Click **Apply**.

Central Web Authentication Support on WLAN

The user associates to the web authentication SSID, which is in fact open+macfiltering and no layer 3 security.

1. The user opens the browser.
2. The WLC redirects to the guest portal.
3. The user authenticates on the portal.
4. The ISE sends a RADIUS Change of Authorization (CoA - UDP Port 1700) to indicate to the controller that the user is valid, and eventually pushes RADIUS attributes such as the Access Control List (ACL).

Central Web Authentication Support on WLAN

Central Web Authentication allows capability for Guest users to be redirected to portals for device registration and self-provisioning before they can be granted access on the network. The flow for the CWA includes the following:

1. The user associates to the web authentication SSID, which is in fact open+macfiltering and no layer 3 security.
2. The user opens the browser.
3. The WLC redirects to the guest portal.
4. The user authenticates on the portal.
5. The ISE sends a RADIUS Change of Authorization (CoA - UDP Port 1700) to indicate to the controller that the user is valid, and eventually pushes RADIUS attributes such as the Access Control List (ACL).

To create a WLAN with Central Web Authentication, follow the steps below:

Procedure

Step 1 Navigate to **Wireless Settings > WLANs** and click **Add new WLAN/RLAN**.

Step 2 Select the **Security Type** as **Central Web Auth**.

Step 3 Click on the **Add the RADIUS Authentication Server** which is hosting the portal for device registration.

Step 4 Click **Apply**.

Note As part of the CWA WLAN creation, a Pre-Auth ACL will be automatically created and AAA Override, CoA and ISE NAC will be enabled on WLAN.

Note You would still need to configure the ISE for CWA to work.

Creating Guest WLANs

Mobility Express controller can provide guest user access on WLANs which are specifically designated for use by guest users. To set this WLAN exclusively for guest user access, enable the **Guest Network** under the **WLAN Security** tab.

Creating Guest WLAN with Captive Portal on CMX Connect

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and then click on **Add new WLAN** button. The Add new WLAN Window will pop up.

Step 2 In the Add new WLAN window, on the **General** tab, configure the following:

- Enter the **Profile Name**
- Enter the **SSID**

Step 3 Enable the **Guest Network** under the **WLAN Security** tab.

Step 4 Select **Captive Portal** as **CMX Connect.**

Step 5 Enter **Captive Portal URL**.

Note Captive Portal URL must have the following format: https://yya7lc.cmxcisco.com/visitor/login where **yya7lc** is your Account ID.

Step 6 Click **Apply**.

Note Additional steps are required on CMX Cloud to create the Captive Portal, Site with Access Points and associating Captive Portal to the Site.

Creating Guest WLAN with Internal Splash Page

There is an internal splash page built into the Mobility Express controller which can be used to onboard the clients connecting to Guest WLANs. This internal splash page can also be customized by uploading a customized bundle. To upload a customized internal splash page, navigate to **Wireless Settings** > **Guest WLANs**. Select **Page Type** as **Customized** and click on the **Upload** button to upload a customized page bundle.

For internal splash page, Cisco Mobility Express supports multiple options for **Access Type**. They are as follows:

1. Local User Account
2. Web Consent
3. Email Address
4. RADIUS
5. WPA2 Personal

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and then click on **Add new WLAN** button. The Add new WLAN Window will pop up.

Step 2 In the Add new WLAN window, on the **General** tab, configure the following:

- Enter the Profile Name
- Enter the SSID

Step 3 Enable the **Guest Network** under the **WLAN Security** tab.

Step 4 Select **Captive Portal** as **Internal Splash Page.**

Step 5 Select one of the following **Access Type** as needed:

a. **Local User Account**–Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients.

b. **Web Consent**–Splash Page will present the user to acknowledge before network access is granted.

c. **Email Address**–Splash Page will present the user to enter the email address before network access is granted.

d. **RADIUS**–Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select **Access Type** as **RADIUS** and enter the RADIUS server configuration.

e. **WPA2 Personal**–This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select **Access Type** as **WPA2 Personal** and enter the **Passphrase**.

Step 6 Click **Apply**.

Creating Guest WLAN with External Splash Page

An external splash page is one which resides on an external Web Server. Similar to the internal splash page, Cisco Mobility Express supports multiple options for **Access Type** with external splash page. They are as follows:

1. Local User Account
2. Web Consent
3. Email Address
4. RADIUS
5. WPA2 Personal

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and then click on **Add new WLAN** button. The Add new WLAN Window will pop up.

Step 2 In the Add new WLAN window, on the **General** tab, configure the following:

- Enter the **Profile Name**
- Enter the **SSID**

Step 3 Enable the **Guest Network** under the **WLAN Security** tab.

Step 4 Select **Captive Portal** as **External Splash Page.**

Step 5 Select one of the following **Access Type** as needed:

a. **Local User Account**–Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients.

b. **Web Consent**–Splash Page will present the user to acknowledge before network access is granted.

c. **Email Address**–Splash Page will present the user to enter the email address before network access is granted.

d. **RADIUS**–Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select **Access Type** as **RADIUS** and enter the RADIUS server configuration.

e. **WPA2 Personal**–This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select **Access Type** as **WPA2 Personal** and enter the **Passphrase**.

Step 6 Click **Apply**.

Walled Garden (DNS Pre-Auth ACLs)

When a client connects to a Guest WLAN, typically, Splash Page or Guest Portal is configured to block Internet access until authentication is successful but certain domains and IP addresses have to be added to allow websites in order for authentication to complete.

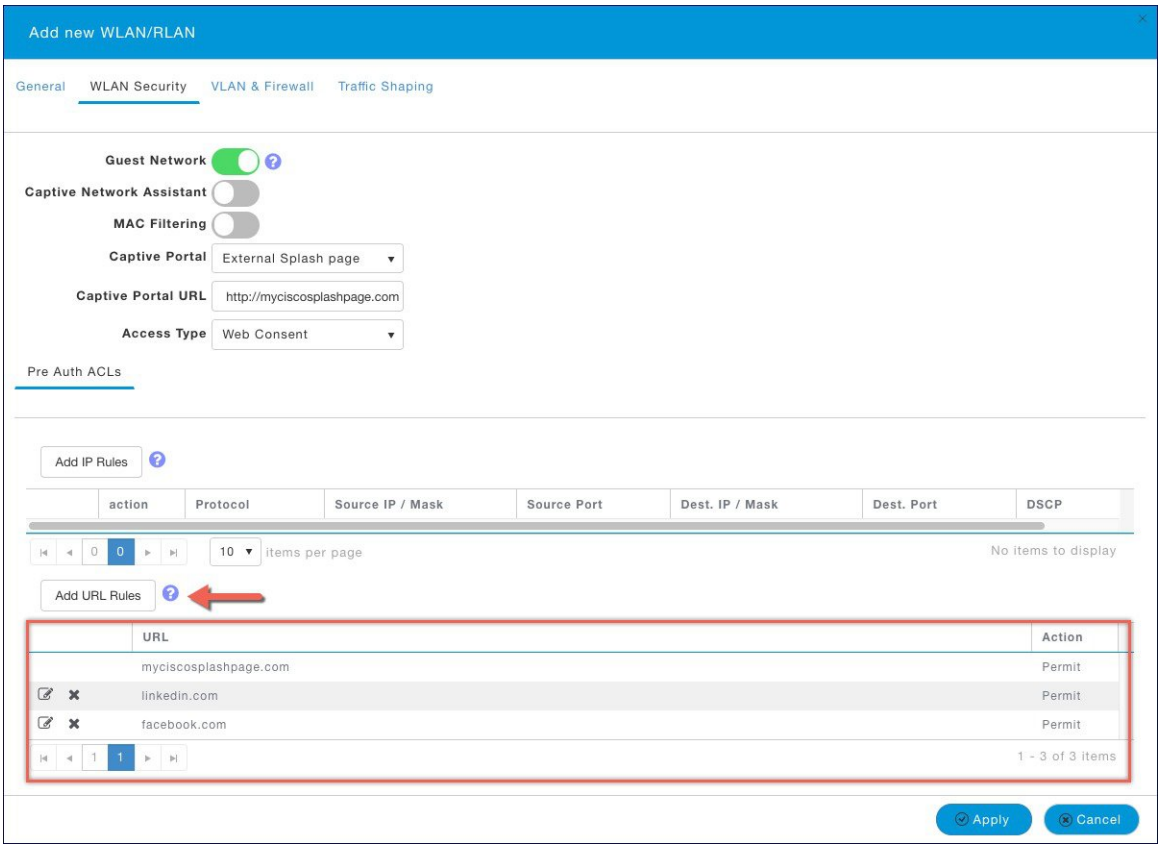
Starting release 8.7, one can configure DNS Pre-Auth ACLs as well as IPv4 based pre-auth ACLs on a WLAN. A maximum of 20 URL rules per ACL are supported and size of each URL is maximum of 255 characters. Wildcards are supported in the URL as well.

Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN**

Step 2 Under **General** tab, enter the WLAN values as needed.

Step 3 Under the **WLAN Security** tab, enable Guest Network. Select Captive Portal as External Splash Page and enter the Captive Portal URL. Select Access Type as Web Consent. To add DNS Pre-Auth ACLs, click on the Add URL Rules button and add the URL(s) you want to permit/deny.



Step 4 Click **Apply**.

Internal Splash Page for Web Authentication

Cisco Mobility Express supports a default internal guest portal that comes built-in and also a customized page, which can be imported by the user.

Using default internal guest portal

To use the default Guest Portal Page or import a customized Guest Portal page, follow the procedure below:

Procedure

Step 1 Navigate to **Wireless Settings** > **Guest WLANs**.

Step 2 Configure the following on the Guest WLAN page:

- **Page Type**–Select as Internal (Default).
- **Preview**–You can Preview the page by clicking on the **Preview** button.
- **Display Cisco Logo**–To hide the Cisco logo that appears in the top right corner of the default page, you can choose No. This field is set to Yes by default.
- **Redirect URL After Login**–To have the guest users redirected to a particular URL (such as the URL for your company) after login, enter the desired URL in this text box. You can enter up to 254 characters.
- **Page Headline**–To create your own headline on the login page, enter the desired text in this text box. You can enter up to 127 characters. The default headline is Welcome to the Cisco Wireless Network.
- **Page Message**–To create your own message on the login page, enter the desired text in this text box. You can enter up to 2047 characters. The default message is Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

Step 3 Click **Apply**.

Using customized internal guest portal

If a customized guest portal has to be presented to guest users, a sample page can be downloaded from cisco.com which can then be edited and imported to the Cisco Mobility Express controller. After the page has been edited and ready to be uploaded to the Cisco Mobility Express controller, follow the steps below.

Procedure

Step 1 Navigate to **Wireless Settings** > **Guest WLANs**.

Step 2 Configure the following on the Guest WLAN page:

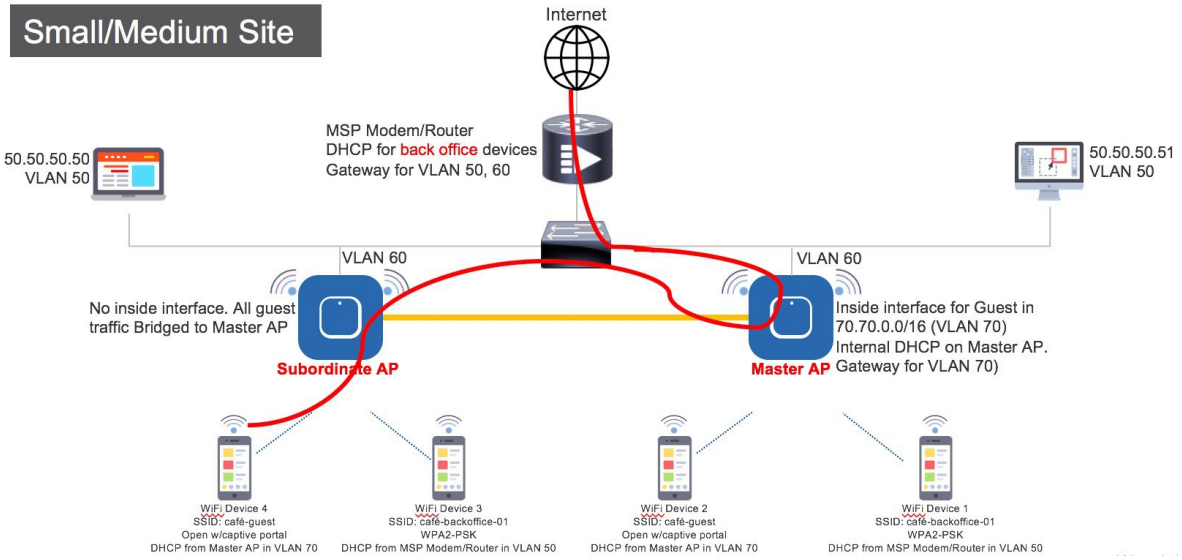
- **Page Type**–Select as **Customized**.

- **Customized page Bundle**–Click on the **Upload** button to upload the he customized page bundle to the Mobility Express controller.
- **Preview**–You can Preview the Guest portal by clicking on the **Preview** button.
- **Redirect URL After Login**–To have the guest users redirected to a particular URL (such as the URL for your company) after login, enter the desired URL in this text box. You can enter up to 254 characters.

Step 3 Click **Apply**.

Centralized NAT on Guest WLANs

Managed Service Providers provide managed WiFi services at Hotels, Retail locations with 1 - 70 APs on site with up 300 or more concurrent wireless clients. In such locations aggregate throughput is limited by WAN connectivity and is typically less than 250 Mbps. Use of external DHCP server for clients is limited to back office devices/clients due to scale limitations. For Guest devices, expectation is to use internal DHCP server on Master AP so that and all guest traffic can be routed via the Master Access Point.



To configure centralized NAT on Guest WLANs, follow the procedure below:

Procedure

Step 1 Add a DHCP Pool for the WLAN which has to bed NAT'ed. To create the scope, navigate to **Wireless Settings > DHCP Server > Add new Pool**. The **Add DHCP Pool** window will pop up. On the **Add DHCP Pool** window, configure the following:

- Enter the **Pool Name** for the WLAN
- Enable the **Pool Status**
- Enter the **VLAN ID** for the WLAN
- Enter the **Lease Period** for the DHCP clients. Default is 1 Day

- Enter the **Network**/**Mask**
- Enter the **Start IP** for the DHCP pool
- Enter the **End IP** for the DHCP pool
- Enter the **Default Gateway** for the DHCP pool

  Note If the scope is for client devices connecting to the Centralized NAT, one must select **Mobility Express Controller** for **Default Gateway**.

- Enter the **Domain Name** (Optional) for the DHCP pool
- For **Name Servers**, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated
- Click **Apply**.

Step 2 To create WLAN, navigate to **Wireless Settings > WLANs.** On the **Add new WLAN** or **Edit WLAN** window, click on the **VLAN and Firewall** tab and configure the following:

- For **Client IP Management**, select **Mobility Express Controller**
- Check the **Peer to Peer Block** to disable communication between two clients on that WLAN
- Enter the **Native VLAN ID**
- Select the **DHCP Scope** which was created for Guest clients on the Mobility Express controller

Note The VLAN for this WLAN should be configured on all the switch ports to which APs are connected.

Step 3 Click **Apply**.

Managing WLAN Users

Cisco Mobility Express supports creation of local user accounts. These users can be authenticated for WLANs configured to use Security as WPA2 Enterprise with Authentication Server set to AP or Guest WLANs configured to use internal or external splash page with **Access Type** as **Local User Account.**

To create local user accounts, follow the procedure below:

Procedure

Step 1 Navigate to **Wireless Settings** > **WLAN Users** and then click on **Add WLAN User** button.

Step 2 Configure the following for the WLAN user:

- **User Name**–Enter the username
- **Guest User**–For Guest user, enable the **Guest User** checkbox
- **Lifetime**–For Guest User, define the user account validity. Default is 86400 seconds (or, 24 hours) from the time of its creation.
- **WLAN Profile**–Select the WLAN to which the user will connect

- **Password**–Enter the password for the user account
- **Description**–Additional details or comments for the user account
- Click on **tick**icon.

Configuring Maximum number of clients on a WLAN

Mobility Express supports a maximum of 100 APs and 2000 clients. To limit the maximum number of clients which can connect to a WLAN, follow the procedure below:

Procedure

Step 1 Enable **Expert View**.

Step 2 Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN**.

Step 3 Under the **Advanced** tab, enter a value for **Maximum Allowed Clients** or select a number from the drop-down list.

Step 4 Click **Apply**.

Configuring Maximum number of clients on per AP Radio

Mobility Express supports a maximum of 200 clients per radio. To limit the maximum number of clients which can connect to a radio, follow the procedure below:

Procedure

Step 1 Enable **Expert View**.

Step 2 Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN**

Step 3 Under the **Advanced** tab, enter a value for **Maximum Allowed Clients per AP Radio**.

Step 4 Click **Apply**.

AAA Override on WLAN

AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN, Access Control Lists (ACLs) and Quality of Service (QoS) to individual WLANs on the returned RADIUS attributes from the AAA server.

Procedure

Step 1 Enable **Expert View**.

Step 2 Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN**

Step 3 Under the **Advanced** tab, enable the **Allow AAA Override**.

Step 4 Click **Apply**.

Bi-Directional Rate Limiting

Starting AireOS 8.7, Bi-Directional Rate limiting is supported on the following:

- Per Client
- Per BSSID
- Per WLAN

Procedure

Step 1 Enable **Expert View**.

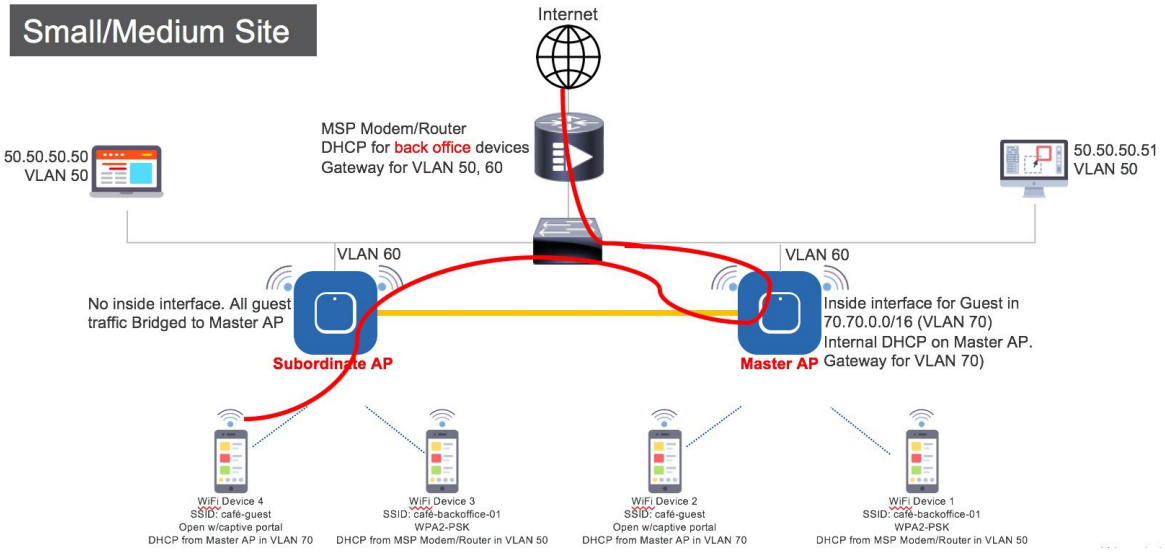
Step 2 Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN**

Step 3 Under the **Traffic Shaping** tab, configure the Rate Limits as required.

Step 4 Click **Apply**.

Centralized NAT on WLANs

Managed Service Providers provide managed WiFi services at Hotels, Retail locations with 1 - 70 APs on site with up 300 or more concurrent wireless clients. In such locations aggregate throughput is limited by WAN connectivity and is typically less than 250 Mbps. Use of external DHCP server for clients is limited to back office devices/clients due to scale limitations. For Guest devices, expectation is to use internal DHCP server on Master AP so that and all guest traffic can be routed via the Master Access Point.



To configure centralized NAT on WLANs, follow the procedure below:

Procedure

Step 1 Add a DHCP Pool for the WLAN which has to bed NAT'ed. To create the scope, navigate to **Wireless Settings > DHCP Server > Add new Pool**. The **Add DHCP Pool** window will pop up. On the **Add DHCP Pool** window, configure the following:

- Enter the **Pool Name** for the WLAN
- Enable the **Pool Status**
- Enter the **VLAN ID** for the WLAN
- Enter the **Lease Period** for the DHCP clients. Default is 1 Day
- Enter the **Network**/**Mask**
- Enter the **Start IP** for the DHCP pool
- Enter the **End IP** for the DHCP pool
- Enter the **Default Gateway** for the DHCP pool

  Note If the scope is for client devices connecting to the Centralized NAT, one must select **Mobility Express Controller** for **Default Gateway**.

- Enter the **Domain Name**(Optional) for the DHCP pool
- For **Name Servers**, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated
- Click **Apply**

Note When creating DHCP Pool, one **must** select **Mobility Express Controller** for the **Default Gateway** if this scope has to be used for WLAN configured for Centralized NAT.

Step 2 To create WLAN, navigate to **Wireless Settings > WLANs.** On the **Add new WLAN** or **Edit WLAN** window, click on the **VLAN and Firewall** tab and configure the following:

- For **Client IP Management**, select **Mobility Express Controller**
- Check the **Peer to Peer Block** to disable communication between two clients on that WLAN
- Enter the **Native VLAN ID**
- Select the **DHCP Scope** which was created for Guest clients

Note The VLAN for this WLAN should be configured on all the switch ports to which APs are connected.

Step 3 Click **Apply**.

Adding MAC for Local MAC Filtering on WLANs

Cisco Mobility Express supports MAC Filtering on WLANs on controller as well as with external RADIUS. MAC addresses can be added to the controller and be either Whitelisted or Blacklisted. To add MAC addresses to the controller, follow the procedure below:

Procedure

Step 1 Navigate to **Wireless Settings** > **WLAN Users** and click on **Local MAC Addresses.**

Step 2 Click **Add MAC Address**.

Step 3 In the **Add MAC Address** window, configure the following:

- **MAC Address**–Enter the MAC Address of the device
- **Description**–Enter the description
- **Type**–Select whether this MAC has to be WhitleList of BlackList
- **Profile Name**–Select the WLAN to which the user will connect

Step 4 Click **Apply**.

WLAN Passpoint Support

Starting Release 8.5, Cisco Mobility Express will add support for Passpoint on WLANs. Access Points which supports IEEE 802.11u-based network information and phone client devices that are certified for WiFi Alliance's are able to work together to support the Passpoint functionality.

The 802.11u enabled phone client devices discover and select target AP based on the information gathered during the pre-association stage from an 802.11u-enabled AP/Cisco Mobility Express controller. A phone client device has pre-provisioned network information such as home OI Information, realm name and domain name, presented as configuration file inside the phone client device. In addition, the phone client device may obtain home network information using the IMSI data derived from the inserted SIM/USIM card.

The 802.11u AP provides various information listings that provide the HotSpot owner details, roaming partners, realm list, 3GPP cellular information, and domain name. The realm list also provides listings of the realm name and its associated EAP authentication type mappings. Knowing this information is essential for the phone client device so that correct EAP credential exchange may take place.

Through the WLAN configuration, single SSID and multiple SSID will be configured with necessary Passpoint information. This additional Passpoint information will be added on beacon or probe response information, so that Passpoint-enabled phone client device can detect and query AP to get further information. During the query process, standard protocol format called ANQP-Access Network Query Protocol-is followed. Here, the protocol describes the standard 2-way or 4-way handshake process to get enough information from the AP and ANQP server to determine the best AP that the phone client device can authenticate and associate with. This handshake process is called GAS-Generic Advertisement Service-protocol that is defined on IEEE 802.11u standard.

To configure Passpoint, 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. This will enable the 802.11u and Hotspot 2.0 tabs on the WLANs.

Step 2 To configure 802.11u and Hotspot 2.0 on WLAN, navigate to **Wireless Settings > WLANs.** On the **Add new WLAN** or **Edit WLAN** window, click on the **802.11u** tab and **Hotspot 2.0** tab to enter the relevant configuration.

Step 3 Click **Apply**.

RLAN support on Mobility Express

Starting Release 8.7, one can create RLANs on Cisco Mobility Express allowing the Wired Ports on the 1810W and 1815W to be managed.

Since Mobility Express supports local switching of Data Traffic, RLAN data traffic will also be locally switched. In the example below, we will configure RLAN for local switching using 802.1x authentication and associate them to Ethernet LAN ports on the AIR-AP1815W for Wired Access. The following are the tasks which we will configure:

1. Create RLANs with 802.1x Authentication
2. Create AP Groups, associate RLAN to AP Group, add APs to AP Group and finally associate Wired Ports to RLANs.

To create RLAN with 802.1x Authentication , follow the procedure below:

Procedure

Step 1 Navigate to **Wireless Settings > WLANs** and click on **Add new WLAN/RLAN** button.

Step 2 Under the **General** tab, select **RLAN** for Type drop down list.

Step 3 Enter the **Profile Name**.

Step 4 Under the **RLAN Security,** select **802.1x** for **Security Type**.

Step 5 Since we are using 802.1x authentication for wired clients, enter the RADIUS server by clicking on the **Add RADIUS Authentication** Server.

Step 6 Under the **VLAN & Firewall** tab, enable **Use VLAN Tagging**, and enter the **Native VLAN ID** as well as the **VLAN ID** which will be used for Data traffic.

Step 7 Click **Apply**.

Create AP Groups and add 1815W to AP Group

To create AP Groups and add 1815W to AP Group, follow the procedure below:

Procedure

Step 1 Navigate to **Wireless Settings** > **Access Point Groups** and click on **Add new group** button.

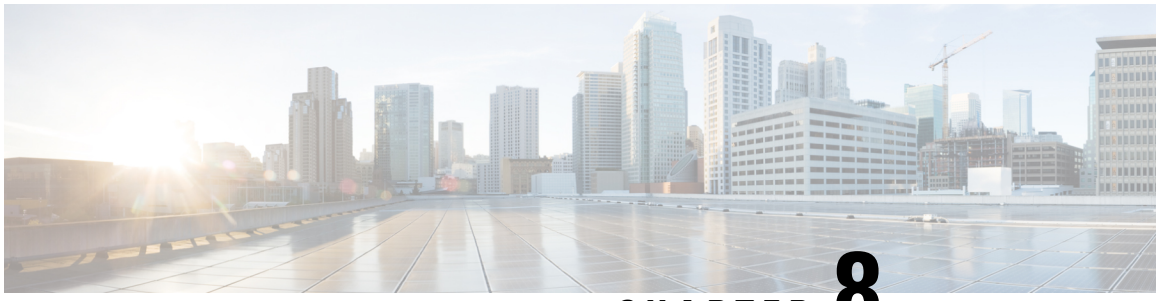
Step 2 Under the **General** tab, enter the **AP Group Name, description.**

Step 3 Under the **WLANs tab, click on the Add new WLAN/RLAN button and select the RLAN** to be added to the AP Group.

Step 4 Under the **Access Points** tab, select the Wall Plate APs to be added to this AP Group.

Step 5 Under the **Ports** Tab, enable the required LAN ports, and select the RLAN for the port.

Step 6 Click **Apply**.



CHAPTER 8

Managing Services with Cisco Mobility Express

There are a number of services supported in a Cisco Mobility Express deployment. In this section, the following Services will be covered.

Application Visibility and Control

Network Based Application Recognition (NBAR) provides application-aware control on a wireless network and enhances manageability and productivity. It also extends Cisco's Application Visibility and Control (AVC) as an end-to-end solution, which gives a complete visibility of applications in the network and allows the administrator to take some action on the same.

NBAR is a deep-packet inspection technology, which supports stateful L4 - L7 classification. The key use cases for NBAR are capacity planning, network usage base lining and better understanding of what applications are consuming bandwidth. Trending of application usage helps network admin improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic. The AVC/NBAR2 engine interoperates with QoS settings on the specific WLAN.

Enabling Application Visibility on WLAN

To configure Application Visibility on a WLAN, follow the procedure below:

Procedure

To enable Application Visibility on WLAN, navigate to **Wireless Settings > WLANs.** On the **Add new WLAN** or **Edit WLAN** window, click on the **Traffic Shaping** tab. To enable Application Visibility on this WLAN, select **Enabled** for **Application Visibility Control**.

Enabling Application Control on WLAN

After Application Visibility has been enabled on the WLAN, one can add control for various applications. There are two way to add control for applications. One can either add control directly from the **Applications** widget on the **Network Summary** page or one can navigate to **Monitoring > Applications** and add control for applications as needed.

Adding Application Control from Network Summary Page

Procedure

Step 1 Add the **Applications** widget on the **Network Summary** Page. To add the **Applications** widget, click on the + icon on the right of the **Network Summary** banner. Select the **Applications** widget. The **Applications** widget will display the top 10 applications being browsed by the clients in the Mobility Express network.

Step 2 Click on the application you wish to add control. The **Add AVC Rule** window will pop up. Select the **Action**. Action can be **Mark**, **Drop** or **Rate Limit**. For **Mark**, one can select DSCP as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specific he DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application.

Step 3 Select one or more **AVC Profile/SSID** combinations.

Step 4 Click **Apply**.

Adding Application Control from Applications Page

Procedure

Step 1 Navigate to **Monitoring** > **Application**s Page.

Step 2 Click on the application you wish to add control. The **Add AVC Rule** window will pop up. Select the **Action**. Action can be **Mark**, **Drop** or **Rate Limit**. For **Mark**, one can select DSCP as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specific he DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application.

Step 3 Select one or more **AVC Profile/SSID** combinations.

Step 4 Click Apply.

iOS Optimized WiFi connectivity and Fast Lane

Configuring Optimized WiFi Connectivity

802.11r enabled WLAN provides faster roaming for wireless client devices. It is desired that iOS devices running iOS 10 will be able to join a WLAN with 11r enabled for better roaming experience. However, if 11r is enabled on a WLAN, the legacy devices that do not recognize the FT AKM's beacons and probe responses will not be able to join the WLAN. We need a way to identify the Client device capability and allow 11r

capable device to join on the WLAN as an FT enabled device and at the same time to allow legacy device to join as an 11i/WPA2 device.

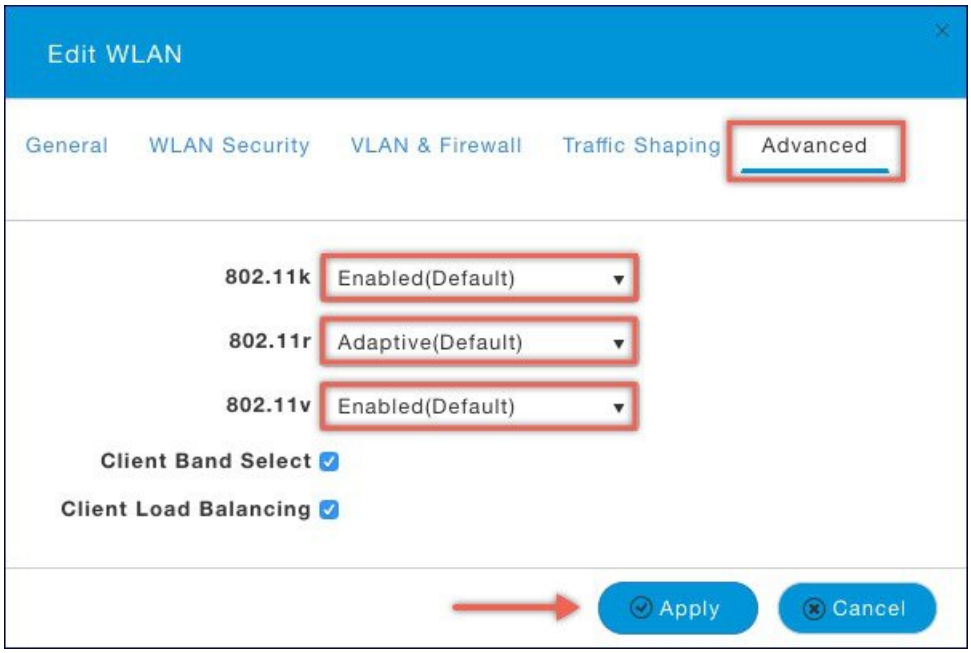
Cisco Mobility Express Release 8.4 will enable 802.11r on an 802.11i-enabled WLAN selectively for iOS devices. The capable iOS devices will identify this functionality and perform an FT Association on the WLAN. The Cisco Wireless infrastructure will allow FT association on the WLAN from devices that can negotiate FT association on a non-FT WLAN. In addition, with Mobility Express running AireOS 8.4, 802.11k and 11v features are enabled by default on an SSID. These features help clients roam better by telling them when to roam and providing them with information about neighboring APs so that no time is wasted scanning when roaming is needed. Since iOS devices support dual band, the 802.11k neighbor list is updated on dual-band, adaptively for iOS devices.

To configure 11k, r, v on a WLAN, 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 Navigate to **Wireless Settings** > **WLANs.** On the **Add new WLAN** or **Edit WLAN** window, click on the **Advanced** tab. Configure 802.11k, r, v as needed on this page.



Step 3 Click **Apply**.

Configuring Fast Lane

Apple iOS device mark QoS as per IETF recommendations. With Mobility Express running AireOS 8.5, one can enable the Fastlane feature from CLI, which enables several beneficial functions:

- Your WLC QoS configuration is optimized globally to better support real-time applications.
- iOS 10 devices can send upstream voice traffic without the requirement to perform WMM TSPEC/TCLAS negotiation. The infrastructure will honor the voice marking for these devices.
- You can apply a QoS profile to your iOS 10 devices, and decide which applications should receive QoS marking upstream, and which applications should be sent as best effort or background.

To configure Fast Lane on a WLAN from UI, follow the procedure below:

Procedure

Step 1 To enable Application Visibility on WLAN, navigate to **Wireless Settings > WLANs.** On the **Add new WLAN** or **Edit WLAN** window, click on the **Traffic Shaping** tab. To enable **Fastlane** on this WLAN, select **Enabled** for **Fastlane**.

Step 2 Click **Apply**.

Cisco Mobility Express with CMX Cloud

Cisco CMX Cloud

Cisco Connected Mobile Experiences Cloud (Cisco CMX Cloud) is an simple and scalable offering which enables delivery of wireless guest access and in-venue analytics, integrating seamlessly with Cisco wireless infrastructure.

This cloud-delivered Software-as-a-Service (SaaS) offering is quick to deploy and intuitive to use. It is based on CMX 10.x code and is compatible with Cisco Mobility Express Release 8.3. It offers the following services:

- Connect for Guest Access-Providing an easy-to-use guest-access solution for visitors through a custom portal using various authentication methods including social, self-registration, and Short Message Service (SMS).
- Presence Analytics-Detecting all Wi-Fi devices (the "devices") in the venue and providing analytics on their presence, including dwell times, new vs. repeat visitors, and peak time.

Cisco CMX Cloud Solution Compatibility Matrix

- Cisco Mobility Express running AireOS Release 8.3 and later
- All Cisco Mobility Express supported Access Points

Minimum requirements for Cisco CMX Cloud deployment

Below are the minimum requirements for CMX Cloud deployment:

1. Verify Cisco CMX Cloud Solution Compatibility Matrix above.
2. Recommended browser is Chrome 45 or later.
3. Signup at https://cmxcisco.com for 60 day trial or go to Cisco Commerce Workspace (CCW) and purchase license for your choice of CMX Cloud service

Enabling CMX Cloud Service on Mobility Express for Presence Analytics

After CMX Cloud Account has been created, next step is to configure and enable the CMX Cloud Service on Master Access Point so that it can send data to the CMX Cloud. To configure, follow the procedure below:

Procedure

Step 1 On Cisco Mobility Express WebUI, navigate to **Advanced** > **CMX**.

Step 2 Enter the **CMX Server URL** (Site URL).

Step 3 Enter the **CMX Server Token** (Account Token).

Step 4 Click **Apply**.

Tip Click the Test Link button to verify connectivity from Master AP to CMX Cloud Site using the configured information.

Configuring Site on CMX Cloud for Presence Analytics

To create a site and add Access Points to the site in CMX Cloud for Presence Analytics, follow the procedure below:

Procedure

Step 1 Login to CMX Cloud account at https://cmscisco.com/

Step 2 Navigate to **Manage** > **Cloud Enabled WLC** and verify that the IP address of the WLC shows up on the list.

Step 3 Navigate to **PRESENCE ANALYTICS** > **Manage**. You should be in the **Sites** pane. Click on the **Add Site** button to create a site.

Step 4 In the **NEW SITE** window, configure the following details:

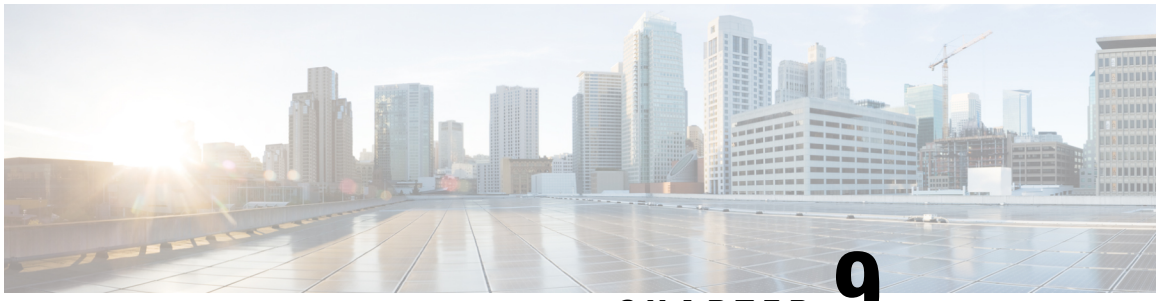
- Enter the **Name** for the site
- Enter the **Address** for the site
- Select **Timezone** from the drop-down list
- Select the **Signal Strength Threshold** for Ignore, Passerby, and Visitors
- Enter the **Minimum Dwell Time for Visitor** (minutes)

Step 5 Click **Save** to create the Site.

Step 6 After the Site is created, click on **Access Points** under **PRESENCE ANALYTICS** > **Manage.**

Step 7 Select the Access Points and add them to the Site by clicking on **Add to Site** button and selecting the Site from the drop-down list.

Step 8 Finally, navigate to **Presence Analytics** dashboard. Select the **Site** you created. Within a few minutes, you should begin to see **Presence** data get populated.



CHAPTER 9

Managing the Cisco Mobility Express Deployment

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 Master 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 master 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 Master 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 Master AP, software download of the code running on the Master AP has to happen on the Access Point being added. For the new Access Point to download the code that is running on the Master AP, one of the following has to be configured:

- Optimal Join is a feature which enables downloading of the software from the Master AP if the AP being added has the same AP software type. This feature is supported on 3800, 2800, and 1560 Series AP because all these Access Points have the same image. For example, if 2800 Series AP is the Master AP, one can add another 2800, 3800 or 1560 and the software will be sent from the Master AP(2800).

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 Master 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.

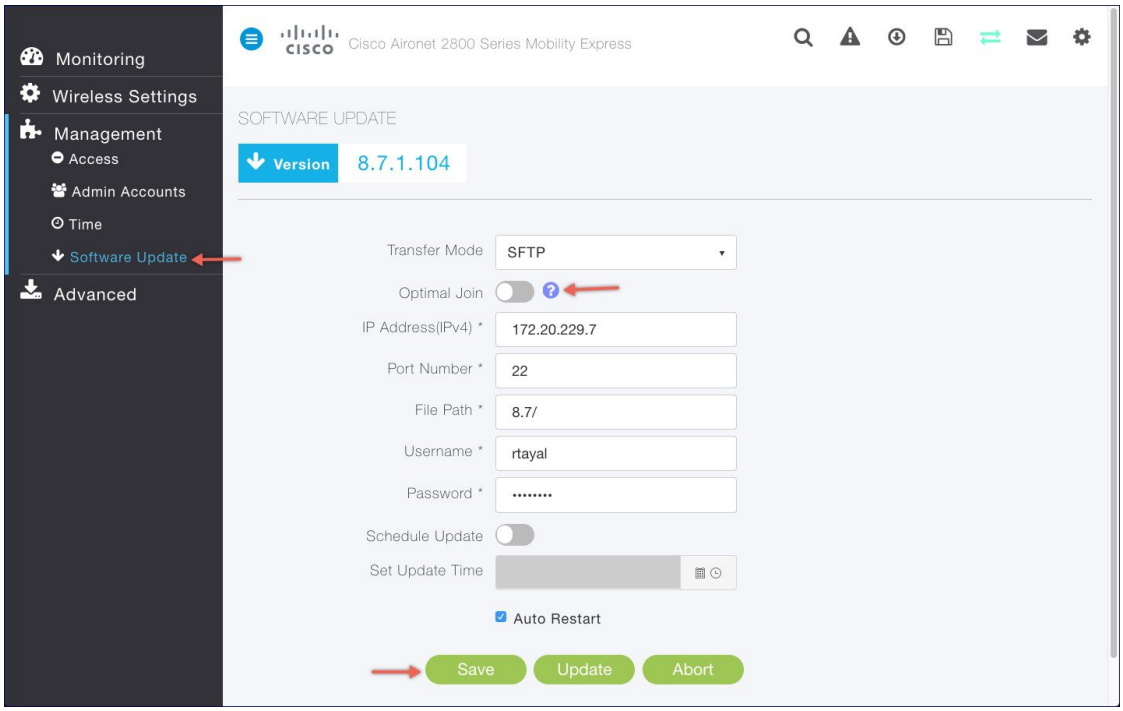
Note For Software download to take place directly from Cisco.com, Master AP should be the one with the SMARTNet Contract.

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**.

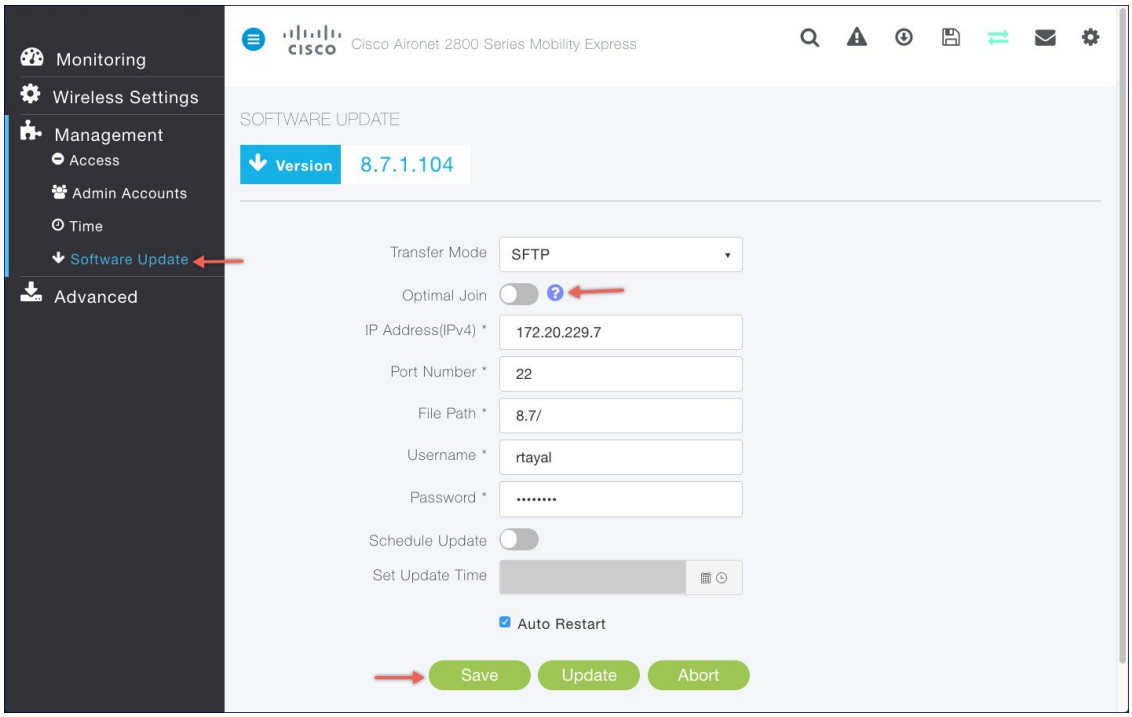
Optimal Join

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 Master 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 Master 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 Master 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 Master 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 Master 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
Cisco Aironet® 1815W Series	ap1g5
Cisco Aironet® 1830 Series	ap1g4

Access Point	Access Point Image
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 Master 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 Master 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:

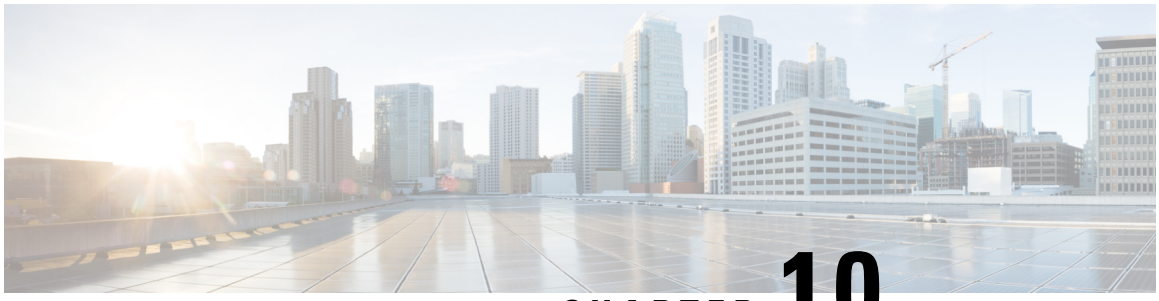
Procedure

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**.



CHAPTER 10

Master AP Failover and Electing a new Master

Cisco Mobility Express is supported on Cisco 1560, 1815I, 1815M, 1815W, 1830, 1850, 2800 and 3800 series Access Points. If you have a mix of these Access Points in a Cisco Mobility Express deployment, the Master AP election process determines which of the supported Access Point will be elected to run Mobility Express controller function in case of a Failover of the Active Master AP. VRRP is used to detect the failure of Master AP which initiates the election of a new Master.

Note Mobility Express uses MAC 00-00-5E-00-01-VRID where VRID is 1 so if there are other instances of VRRP running in the environment, use VRID other than 1 for those instances.

Master AP Failover

To have redundancy in the Mobility Express network, it must have two or more Mobility Express capable Access Points. These Access Points should have AP Image type as MOBILITY EXPRESS IMAGE and AP Configuration as MOBILITY EXPRESS CAPABLE. In an event of a failure of Master AP, another Mobility Express capable AP is elected as a Master automatically. The newly elected Master AP has the same IP and configuration as the original Master AP.

Note Given Access Point models support different scale limits in terms of the number of Access Points supported, it is highly recommended to have at least two or more Access Points which support the same scale limits. For example, if you need to support scale of 100 Access Points, you should have at least two or more of either 3800, 2800 or a combination of both.

Note Access Points, which have the Mobility Express Image but **AP Configuration**, is **NOT MOBILITY EXPRESS CAPABLE**, will not participate in the Master AP election process.

Electing a new Master Access Point

Master election process is based on a set of priorities. When an active Master Access Point fails, the election process gets initiated and it elects the Access Point with the highest priority as the Master AP.

Note During the Master Election process, even though the Master AP running the controller function is down, the remaining Access Points will fall into Standalone mode and will continue to service connected clients and switch data traffic locally. After the new Master is elected, the Standalone Access points will move to connected mode.

As mentioned above, Master Access Point election is based on a set of priorities. The priorities are as follows:

Procedure

Step 1 **User Defined Master**–User can select an Access Point to be the Master Access Point. If such a selection is made, no new Master will be elected in case of a failure of the active Master. After five minutes, if the current Master is still not active, it will be assumed dead and Master Election will begin to elect a new Master. To manually define a Master, follow the procedure below:

a) Navigate to **Wireless Settings** > **Access Points**.
b) From the list of Access Points, click **Edit** icon of the Access Point which you would like to select as the Master AP.
c) Under the **General** tab, click on **Make me Controller** button.
d) Click **Yes** on the Confirmation window.

Note The previous Master will reboot and the selected Access Point will immediately launch the controller and become the active Master.

Step 2 **Next Preferred Master**–Admin can configure the **Next Preferred Master** UI and CLI. When this is configured and the active Master AP fails, the one configured as the **Next Preferred Master** will be elected as a Master. To configure the **Next Preferred Master**, follow the procedure below:

Note Only one **Next Preferred Master** can be configured on Cisco Mobility Express.

a) Navigate to **Wireless Settings** > **Access Points.**
b) Edit the AP which you would like to make it as a **Next Preferred Master**
c) In the **Edit AP** window, enable the **Set as Preferred Master** toggle.
d) Click **Apply**.

To configure the **Next Preferred Master** from the controller CLI, please follow the steps below:

To configure the Next Preferred Master, execute the following CLI:

```
(Cisco Controller) >config ap next-preferred-master <Cisco AP>
       <Cisco AP> Enter the name of the Cisco AP
```

To see the Next Preferred Master, execute the following CLI:

```
(Cisco Controller) >show ap next-preferred-master
```

To clear the Next Preferred Master, execute the following CLI:

```
Cisco Controller) >clear ap next-preferred-master
```

Step 3 **Most Capable Access Point**– If the first two priorities are not configured, Master AP election algorithm will select the new Master based on the capability of the Access Point. For example, 3800 is the most capable followed by 2800, 1850, 1830 and finally the 1815 Series.

Note All 1815 Series Access Points have the same capability.

Step 4 **Least Client Load**– If here are multiple Access Points with the same capability i.e. multiple 3800 Access points, the one with least client load is elected as the Master Access Point.

Step 5 **Lowest MAC Address**–If all of the Access Points are the same and have the same client load, then Access Point with the lowest MAC will be elected as a Master.