Creating Wireless Networks

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 Primary 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. s

   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 Create the pre-authentication ACL under **security policies** section and apply the ACL to the required 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.

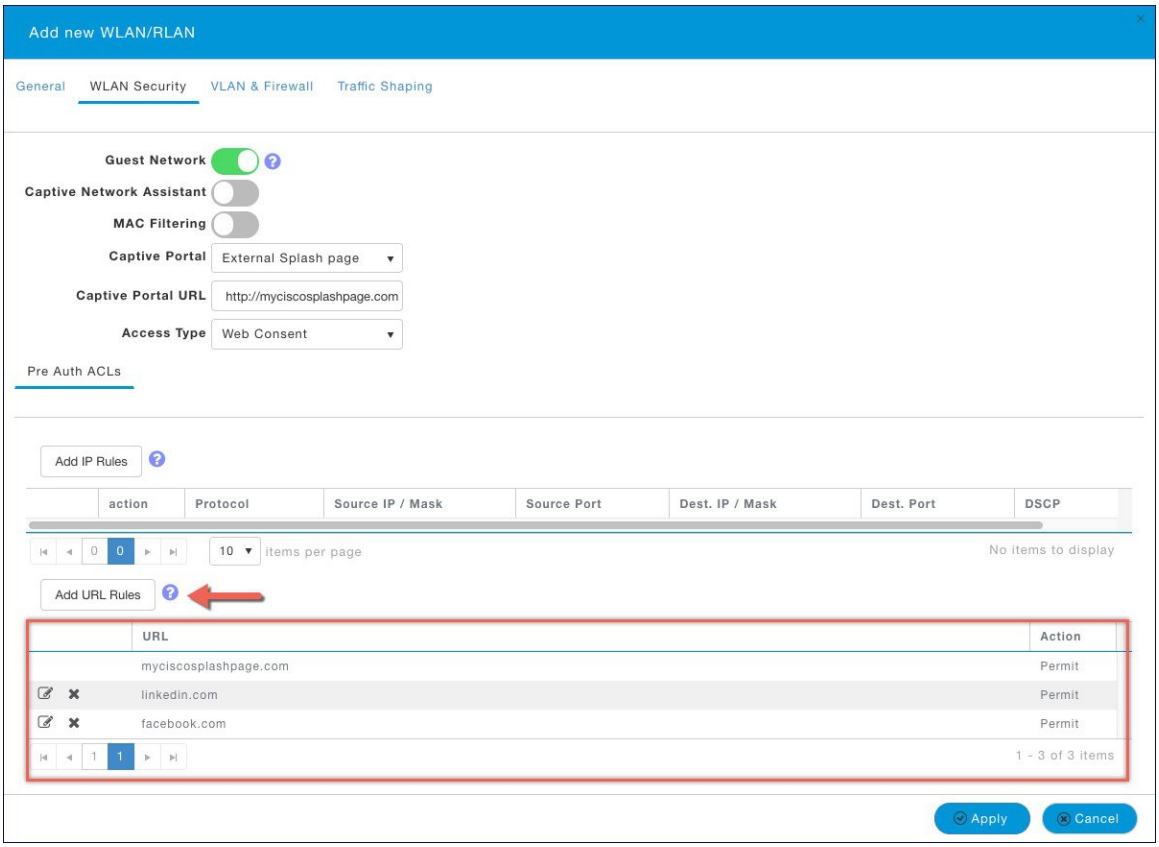
Starting release 8.7, one can configure DNS Pre-Auth ACLs as well as IPv4 based pre-auth ACLs on a WLAN. A maximum of 20 URL rules per ACL are supported and size of each URL is maximum of 255 characters. Wildcards are supported in the URL as well.

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:

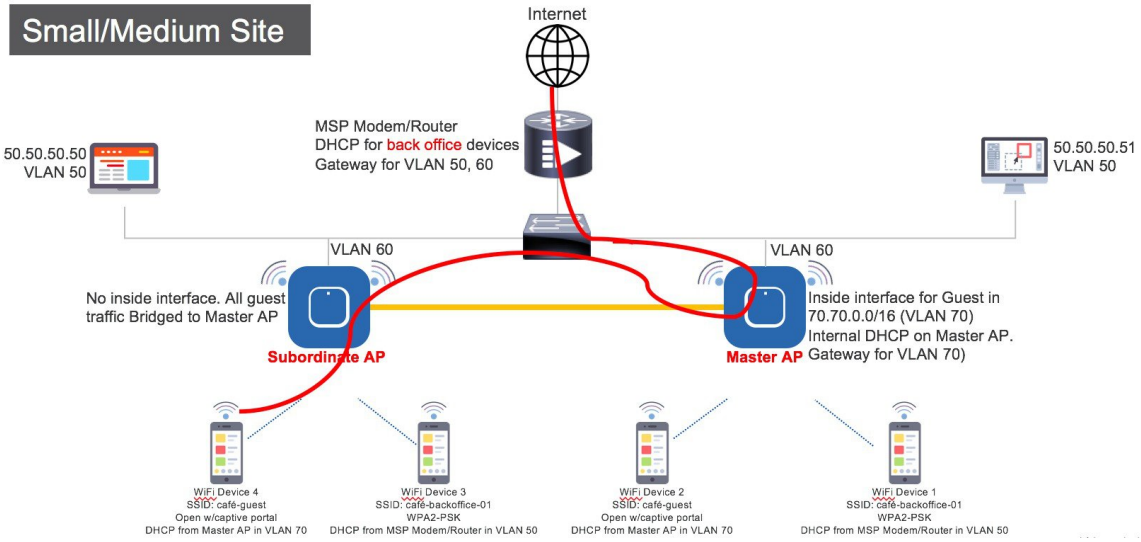
- **Page Type**–Select as **Customized**.

- **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 Primary AP so that and all guest traffic can be routed via the Primary 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 Nam**e (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**

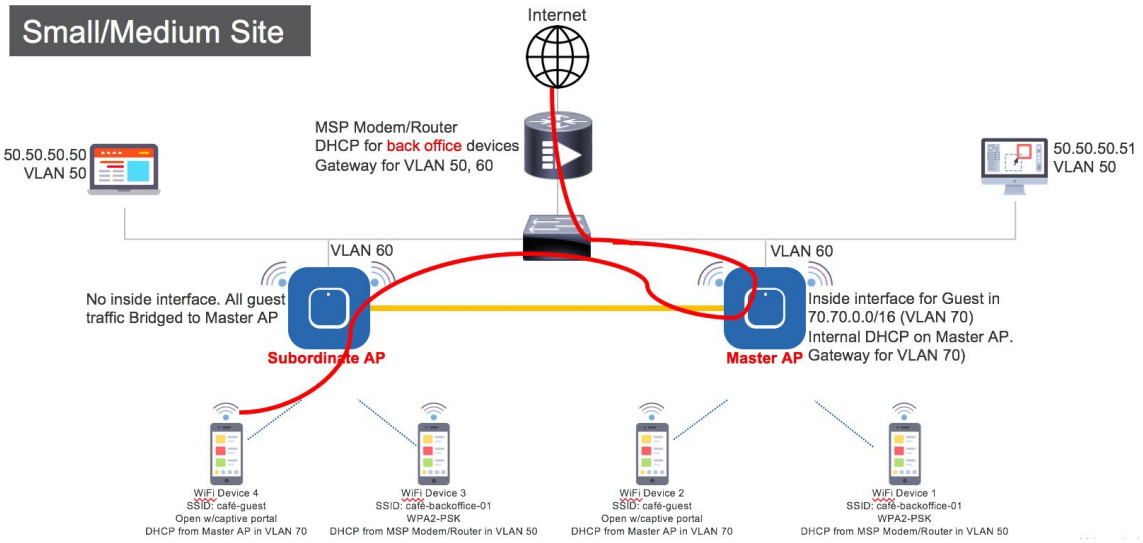
Step 3 Under the **Traffic Shaping** tab, configure the Rate Limits as required.

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 Primary AP so that and all guest traffic can be routed via the Primary Access Point.

Note To use the centralized NAT feature, ensure that the VLAN, WLAN being NATed is present on the ME AP.



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 in an allowed list or a blocked-list. 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 in an allowed list or a blocked list
- **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**.