Specifying Wireless Settings

Setting Up WLANs and WLAN Users

About WLANs in a Cisco Mobility Express Network

You can create and manage Wireless Local Area Networks (WLANs) through the **WLAN Configuration** window. Choose **Wireless Settings** > **WLANs**.

The total number of active WLANs is displayed at the top of the **WLAN Configuration** window along with a list of all the WLANs currently configured on the primary AP's controller. This list displays the following details for each WLAN:

- Whether the WLAN is enabled or disabled.
- Name of the WLAN.
- Security Policy on WLAN.
- Radio Policy on WLAN.

Guidelines and Limitations for Setting Up WLANs

- You can associate up to 16 WLANs with the Cisco Mobility Express controller. Cisco recommends a maximum of 4 WLANs. The controller assigns all the configured WLANs to all the connected APs.
- Each WLAN has a unique WLAN ID, a unique profile name, and an SSID.
- The WLAN name and SSID can have up to 32 characters.
- Each connected AP advertises only the WLANs that are in an **Enabled** state. The APs do not advertise disabled WLANs.

- The controller uses different attributes to differentiate between WLANs with the same SSID.
- Peer-to-peer blocking does not apply to multicast traffic.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.
- Dual-stack clients with static IPv4 addresses are not supported.
- When creating WLANs with the same SSID, create a unique profile name for each WLAN.
- Starting from Release 8.10.142.0, new SSID and WLAN profile names can have up to four leading spaces. If there are more than four leading spaces in an SSID or WLAN profile name, an error message is displayed. If you upgrade to this release, the existing SSID and WLAN profile names that contain more than four leading spaces are not impacted.

Note In a Cisco Mobility Express deployment, if you download the Day 0 configuration file through PnP on an AP, leading spaces in SSID names are not checked because of an XML limitation. However, if you convert the AP from another mode to the Mobility Express mode, leading spaces are checked during SSID creation.

Adding a WLAN

Step 1 Choose **Wireless Settings** > **WLANs**.

The **WLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN**.
The **Add New WLAN** window is displayed.

Step 3 Under the **General** tab, set the following parameters:

- **WLAN ID**—From the drop-down list, choose an ID number for this WLAN.
- **Profile Name**— The profile name must be unique and should not exceed 32 characters.
- **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.
- **Admin State**—From the drop-down list, choose **Enabled** to enable this WLAN, else choose **Disabled**.

  The default is **Enabled**.
- **Radio Policy**—From the drop-down list, choose among the following options:
  - **All**—Configures the WLAN to support dual-band (2.4 GHz and 5 GHz) capable clients
  - **2.4 GHz only**—Configures the WLAN to support 802.11b/g/n capable clients only
  - **5 GHz only**—Configures the WLAN to support 802.11a/n/ac capable clients only

  The radio policy allows you to optimize the RF settings for all the APs associated with a WLAN. The selected radio policy applies to the 802.11 radios. Each radio policy specifies which part of the spectrum the WLAN is advertised on, whether it is on 2.4 GHz, 5 GHz, or both.

- **Broadcast SSID**—The default is **Enabled**. If you toggle it to make the SSID discoverable. Else, the SSID is hidden.
- **Local Profiling**

Step 4 Under the **WLAN Security** tab, set one of the following security authentication options from the **Security** drop-down list:

- **Open**—This option stands for Open authentication, which allows any device to authenticate and then attempt to communicate with an AP. Using open authentication, any wireless device can authenticate with the AP.
- **Enhanced Open**—The Enhanced Open feature is based on Opportunistic Wireless Encryption (OWE) and provides encryption to open (unencrypted) wireless networks and a higher level of security against passive sniffing and simple attacks when compared to a public PSK wireless network.

  With Enhanced Open, clients and Mobility Express perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise secret with the 4-way handshake.

  Enhanced Open requires no special configuration or user interaction, but provides better security than a common, shared, and public PSK.

  If you select **Enhanced Open**, you have the option to enable or disable **OWE Transition Mode**.

  The OWE transition mode enables OWE and non-OWE STAs to connect to the same DS simultaneously. All the OWE STAs, when they see an AP in OWE transition mode, connect it to OWE WLAN.

  Both the WLANs, the open WLAN and the OWE WLAN, transmit beacon frames. Beacon and probe response frames from the OWE WLANs include the Wi-Fi Alliance vendor IE to encapsulate the BSSID and SSID of the open WLAN.

  OWE-capable STAs display only the SSID of the OWE WLAN (extracted from the Wi-Fi Alliance vendor IE in the open WLAN's beacons and probe responses) to the corresponding user in the list of available networks; display of the open WLAN is suppressed. OWE-capable STAs associate only with the OWE WLAN of an AP in OWE transition mode.

  OWE WLAN must have PMF as it is a mandatory configuration.

  For more information about Enhanced Open, see the Wi-Fi Alliance's website.

- **Personal**—This WPA3 standard provides a replacement to the WPA2's PSK with Simultaneous Authentication of Equals (SAE), as defined in the IEEE 802.11-2016 standard. With SAE, the user experience is the same (choose a passphrase to connect), but the SAE automatically adds a step to the *handshake*, which makes brute force attacks ineffective. With SAE, the passphrase is not exposed, making it impossible for attackers to find the passphrase through brute force dictionary attacks. The Protected Management Frames (PMF) are required to be used for all WPA3-Personal connections. Previously, PMF was an optional capability for users. With WPA3, PMF must be negotiated for all WPA3 connections that provide an additional layer of protection from deauthentication and disassociation attacks.

  If you choose **Personal**, you will need to configure iPSK and a passphrase.

  For more information about WPA3, see the the Wi-Fi Alliance's website.

  Note iPSK is not supported for SAE security; only common passphrase security association is supported.

- **WPA2 Enterprise**—This option stands for Wi-Fi Protected Access 2, with a local authentication server or a RADIUS server. This is the default option.

  To have a local authentication method, choose **AP** in the **Authentication Server** drop-down list. This option is a Local EAP authentication method that allows users and wireless clients to be authenticated locally. The controller

in the primary AP serves as the authentication server and the local user database, which removes dependence on an external authentication server.

To have a RADIUS server-based authentication method, choose **External Radius** in the **Authentication Server** drop-down list. RADIUS is a client/server protocol that enables communication with a central server to authenticate users and authorize their access to the WLAN. You can specify up to two RADIUS authentication servers. For each server you need to specify the following details:

- **RADIUS IP**—IPv4 address of the RADIUS server.
- **RADIUS Port**—Enter the communication port of the RADIUS server. The default value is 1812.
- **Shared Secret**—Enter the secret key used by the RADIUS server, in ASCII format.

Note You may configure multiple RADIUS authentication and accounting servers on the ME controller. However, the ports of all the authentication, accounting, mail, logs servers configured should use the same default or non-default port number.

- **Guest**—The 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, choose the **Security** as **Guest**.

  You can set the authentication for guest users by choosing one of the following options in the **Guest Type** drop-down list:

  - **WPA2 Personal**—This option stands for Wi-Fi Protected Access 2 with pre-shared key (PSK). WPA2 Personal is a method used for securing your network with the use of a PSK authentication. The PSK is configured separately both on the controller AP, under the WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network. This option is used when you do not have an enterprise authentication server.

    If you choose this option, then specify the PSK in the **Passphrase** field, and confirm it by specifying it again in the **Confirm Passphrase** field. The PSK you enter is hidden under asterisks for security purposes. Check the **Show Passphrase** checkbox to reveal it.

  - **Captive Portal (AP)**—Choose this option to set a captive portal which presents one of the following **Captive Portal Type**s to users:
    - **Require Username and Password**—This is the default option. Choose this option to authenticate guests using the username and password which you can specify for guest users of this WLAN, under **Wireless Settings > WLAN Users**. For more information, see Viewing and Managing WLAN Users, on page 8.
    - **Web Consent**—Choose this option to allow guests access to the WLAN upon acceptance of displayed terms and conditions. This option allows guest users to access the WLAN without entering a username and password.
    - **Require Email Address**—Choose this option, if you want guest users to be prompted for their e-mail address when attempting to access the WLAN. Upon entering a valid email address, access it provided. This option allows guest users to access the WLAN without entering a username and password.
  - **Captive Portal (External Web Server)**—Choose this option to have external captive portal authentication, using a web server outside your network. Also specify the URL of the server in the **Site URL** field.
  - **CMX Guest Connect**—Choose this option to authenticate guests using the Cisco CMX Connect. Also, specify the URL of your CMX Cloud site in the **Site URL** field.

Step 5 Under the **VLAN & Firewall** tab, in the **Use VLAN Tagging** drop-down list, choose **Yes** to enable VLAN tagging of packets. Then, choose a **VLAN ID** from the drop-down list, to use for the tagging. By default VLAN Tagging is disabled.

By enabling VLAN Tagging, the chosen VLAN ID is inserted into a packet header in order to identify which VLAN (Virtual Local Area Network) the packet belongs to. This enables the controller to use the VLAN ID to determine which VLAN to send a broadcast packet to, thereby providing traffic separation between VLANs.

Step 6 If you have chosen to enable VLAN Tagging, then you have an option to enable a firewall for the WLAN based on Access Control Lists (ACLs). An ACL is a set of rules used to limit access to a particular WLAN to control data traffic to and from wireless clients or to the controller CPU to control all traffic destined for the CPU.

To enable an ACL-based firewall:

a. In the **Enable Firewall** drop-down list, choose **Yes**.

b. In the **ACL Name** field, enter a name for the new ACL. You can enter up to 32 alphanumeric characters. The ACL name must be unique.

c. Click Apply.

d. To set rules for the ACL, click **Add Rule**.

Note that ACL rules are applied to the VLAN. Multiple WLANs can use the same VLAN, hence inheriting ACL rules, if any.

Configure a rule for this ACL as follows:

a. From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets or **Permit** to cause this ACL to allow packets. The default is Permit. The controller can permit or deny only IP packets in an ACL. Other types of packets (such as ARP packets) cannot be specified.

b. From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options:

- **Any**—Any protocol (this is the default value)
- **TCP**—Transmission Control Protocol
- **UDP**—User Datagram Protocol
- **ICMP**—Internet Control Message Protocol

  ESP—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
- **Eth Over IP**—Ethernet-over-Internet Protocol
- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet Assigned Numbers Authority (IANA) protocol. If you choose Other, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the IANA website.

c. In the **Dest. IP/Mask** field, enter the IP address and netmask of the specific destination.

d. If you have chosen TCP or UDP, you will need specify a **Destination Port**. This destination port can be used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.

e. From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet. You can choose:

- Any—Any DSCP (this is the default value)
- Specific—A specific DSCP from 0 to 63, which you enter in the DSCP edit box

f. Click the **Apply** icon to commit your changes.

Step 7 Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority, including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

The Cisco Mobility Express controller supports the following four QoS levels. Under the **QoS** tab, from the **QoS** drop-down list, choose one of the following QoS levels:

- **Platinum (Voice)**—Ensures a high quality of service for voice over wireless.
- **Gold (Video)**—Supports high-quality video applications.
- **Silver (Best Effort)**—Supports normal bandwidth for clients.
- **Bronze (Background)**—Provides the lowest bandwidth for guest services.

Step 8 **Application Visibility** classifies applications using the Network-Based Application Recognition (NBAR2) engine, and provides application-level visibility in wireless networks. Application Visibility enables the controller to detect and recognize more than 1000 applications and perform real-time analysis, and monitor network congestion and network link usage. This feature contributes to the **Applications By Usage** statistic in the **Monitoring** > **Network Summary**.

To enable **Application Visibility**, choose **Enabled** (the default option) from the **Application Visibility** drop-down list. Otherwise, choose **Disabled**.

Step 9 Click **Apply**.

What to do next

You can proceed to create or edit user accounts for a WLAN. See Viewing and Managing WLAN Users, on page 8.

Enabling and Disabling a WLAN

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 2 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
The **Edit WLAN** window is displayed.

Step 3 Choose **General** > **Admin State** and select **Enabled** or **Disabled**, as required.

Step 4 Click **Apply**.

Note Clicking **Apply** after creating a new WLAN or editing an existing one always enables the WLAN irrespective of whether it was previously enabled or disabled.

Editing and Deleting a WLAN

Choose **Wireless Settings** > **WLANs**. In the window that is displayed, perform one of the following actions:

- To edit a WLAN, click the **Edit** icon adjacent to it.
- To delete a WLAN, click the **Delete** icon adjacent to it.

Limit Clients per WLAN

Depending on the primary AP, Cisco Mobility Express supports up to a maximum of 100 APs and 2000 clients per WLAN. To limit the number of clients on the Cisco Mobility Express network, do the following:

Before you begin

Step 1 In the **Expert** view, navigate to **Wireless Settings** > **WLANs**.

The **WLAN/RLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN/RLAN**.

To modify the client limit for an existing WLAN, navigate to the desired WLAN in the **WLAN/RLAN** table and click the edit icon.

The **Add New WLAN/RLAN** page is displayed.

Step 3 Under the **Advanced** tab, choose or enter the desired value for **Maximum Allowed Clients** in the corresponding drop-down list.

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

The **WLAN/RLAN Configuration** window is displayed.

The chosen WLAN is now configured with the specified maximum number of clients.

Limit Clients per AP Radio

Cisco Mobility Express supports a maximum of 200 connected clients on a single AP radio. Beginning Cisco Wireless Release 8.7, this limit can be changed by doing the following:

Before you begin

Step 1 In the **Expert** view, navigate to **Wireless Settings** > **WLANs**.

The **WLAN/RLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN/RLAN**.

To modify the maximum client limit per AP radio for an existing WLAN, navigate to the desired WLAN in the **WLAN/RLAN** table and click the edit icon.

The **Add New WLAN/RLAN** page is displayed.

Step 3 Under the **Advanced** tab, choose or enter the desired value for **Maximum Allowed Clients Per AP Radio** in the corresponding drop-down list.

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

The **WLAN/RLAN Configuration** window is displayed.

The selected WLAN is now configured with a revised maximum number of clients that can be connected to the AP radio.

Viewing and Managing WLAN Users

To view and manage WLAN users, choose **Wireless Settings** > **WLAN Users**.

The **WLAN Users** window is displayed, along with the total number of WLAN users configured on the controller. It also lists all the WLAN users in the network along with the following details for each:

- **User name**—Name of the WLAN user.
- **Guest user**—If this checkbox is selected, then this is a guest user account with a limited validity of only 86400 seconds (or 24 hours) from the time of its creation.
- **WLAN Profile**—The WLANs that this user can connect to.
- **Password**—The password to be used when connecting to a WLAN.
- **Description**—Additional details or comments about the user.

You can view and manage WLAN users only for the WPA2 Enterprise with Local Server setup. To use your Cisco Mobility Express wireless network, a wireless client should connect to a WLAN in the network. To connect to a WLAN, the wireless client will have to use the user credentials set for that WLAN. If this WLAN uses WPA2-Personal as a Security Policy, then the user must provide the appropriate WPA2-PSK set for that WLAN on the Controller AP. If the Security Policy is set to WPA2-Enterprise, the user must provide a valid user identity and the corresponding password set in the RADIUS user database.

Adding a WLAN User

To add a WLAN user, click **Add WLAN User**, and then fill in the following details:

- User name—Specify a name for WLAN user account.
- Guest user—Select this checkbox if this is meant to be a guest WLAN user account. You can also specify the validity of this account from the time of its creation, in seconds, the **Lifetime** field. The default value is 86400 seconds (that is, 24 hours). You can specify a lifetime value from 60 to 31536000 seconds (that is, 1 minute to 1 year).

- WLAN Profile—Select the WLAN that this user can connect to. From the drop-down list, choose a particular WLAN, or choose **Any WLAN** to apply this account for all WLANs set up on the controller.

  This drop-down list is populated with the WLANs which have been configured under **Wireless Settings > WLANs**.

- Password—The password to be used when connecting to a WLAN.
- Description—Additional details or comments on the user.

Editing a WLAN User

To edit a WLAN user, click the **Edit** icon adjacent to the WLAN user whose details you want to edit and make the necessary changes.

Deleting a WLAN User

To delete a WLAN user, click the **Delete** icon adjacent to the WLAN user you want to delete. and then click **Ok** in the confirmation dialog box.

Bidirectional Bandwidth Rate Limiting

You can define throughput limits for client devices, WLANs, and BSSIDs on the Cisco Mobility Express network. Bidirectional rate limiting ensures that the network bandwidth is fairly distributed among all users. To set the bidirectional bandwidth rate limit for client devices, WLANs, and BSSIDs on the Cisco Mobility Express network, follow the instructions below:

- Bidirectional Rate Limiting per Client, on page 9
- Bidirectional Rate Limiting per BSSID, on page 10
- Bidirectional Rate Limiting per WLAN, on page 11

Bidirectional Rate Limiting per Client

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

The **WLAN/RLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN/RLAN**.

To modify the bidirectional rate limit for an existing WLAN, navigate to the desired WLAN in the table and click the edit icon.

The **Add New WLAN/RLAN** page is displayed.

Step 3 Under the **Traffic Shaping** tab, choose or enter the desired value for per-client downstream and upstream bandwidth limit.

In the **Standard** view, choose the desired values (in Mbps) for the following by moving the corresponding slider:

- **Per-client downstream bandwidth limit**
- **Per-client upstream bandwidth limit**

In the **Expert** view, specify the desired values (in kbps) in the following fields under the **Rate limits per client** section:

- **Average downstream bandwidth limit**
- **Average real-time downstream bandwidth limit**
- **Average upstream bandwidth limit**
- **Average real-time upstream bandwidth limit**

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

The **WLAN/RLAN Configuration** window is displayed.

The bidirectional bandwidth is now limited per client device as per the new configuration.

Bidirectional Rate Limiting per BSSID

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

The **WLAN/RLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN/RLAN**.

To modify the bidirectional rate limit for an existing WLAN, navigate to the desired WLAN in the table and click the edit icon.

The **Add New WLAN/RLAN** page is displayed.

Step 3 Under the **Traffic Shaping** tab, choose or enter the desired value for per-BSSID downstream and upstream bandwidth limit.

In the **Standard** view, choose the desired values (in Mbps) for the following by moving the corresponding slider:

- **Per-BSSID downstream bandwidth limit**
- **Per-BSSID upstream bandwidth limit**

In the **Expert** view, specify the desired values (in kbps) in the following fields under the **Rate limits per BSSID** section:

- **Average downstream bandwidth limit**
- **Average real-time downstream bandwidth limit**
- **Average upstream bandwidth limit**
- **Average real-time upstream bandwidth limit**

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

The **WLAN/RLAN Configuration** window is displayed.

The bidirectional bandwidth is now limited per BSSID as per the new configuration.

Bidirectional Rate Limiting per WLAN

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

The **WLAN/RLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN/RLAN**.

To modify the bidirectional rate limit for an existing WLAN, navigate to the desired WLAN in the table and click the edit icon.

The **Add New WLAN/RLAN** page is displayed.

Step 3 Under the **Traffic Shaping** tab, choose or enter the desired value for per-WLAN downstream and upstream bandwidth limit.

In the **Standard** view, choose the desired values (in Mbps) for the following by moving the corresponding slider:

- **Per-WLAN downstream bandwidth limit**
- **Per-WLAN upstream bandwidth limit**

In the **Expert** view, specify the desired values (in kbps) in the following fields under the **Rate limits per WLAN** section:

- **Average downstream bandwidth limit**
- **Average real-time downstream bandwidth limit**
- **Average upstream bandwidth limit**
- **Average real-time upstream bandwidth limit**

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

The **WLAN/RLAN Configuration** window is displayed.

The bidirectional bandwidth is now limited on the WLANs as per the newly specified values.

Remote LANs in a Cisco Mobility Express network

You can create and manage Remote Local Area Networks (RLANs) through the **WLAN/RLAN Configuration** window which can be accessed via **Wireless Settings** > **WLANs**. RLANs allow wired port management on Cisco APs like 1810W and 1815W.

To enable RLAN functionality on the Cisco Mobility Express network, perform the following tasks in the given order:

- Create an RLAN.
- Create an AP group.
- Associate the RLAN to the AP group.
- Add APs (with wired ports that need to be managed) to the AP group.

- Associate the wired port to the RLAN.

Create Remote LAN

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

This window displays a count of all the WLANs and remote LANs configured on the Cisco Mobility Express controller. It also displays a table listing the details of the configured WLANs and RLANs.

For each remote LAN, you can see its profile **Name**, admin state, **Type** (RLAN), and **Security Policy**. If the table listing the WLANs and remote LANs spans multiple pages, you can access these pages by clicking the page number links.

The **WLAN/RLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN/RLAN**.

The **Add New WLAN/RLAN** page is displayed.

Step 3 Choose **WLANs** to open the WLANs page.

This page lists all the WLANs and remote LANs currently configured on the controller. For each WLAN, you can see its WLAN/remote LAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs/Remote LANs appears in the upper right-hand corner of the page. If the list of WLANs/Remote LANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a Remote LAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or select the check box to the left of the row, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the remote LAN is removed from any access point group to which it is assigned and from the access point's radio.

Step 4 Create a new Remote-LAN by choosing **Create New** from the drop-down list and clicking **Go**. The WLANs > New page appears.

Step 5 From the Type drop-down list, choose **Remote LAN** to create a remote LAN.

Step 6 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this Remote WLAN. The profile name must be unique.

Step 7 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Step 8 Click **Apply** to commit your changes. The **WLANs > Edit** page appears.

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Step 9 Use the parameters on the General, Security, and Advanced tabs to configure this remote LAN. See the sections in the rest of this chapter for instructions on configuring specific features.

Step 10 On the General tab, select the **Status** check box to enable this remote LAN. Be sure to leave it unselected until you have finished making configuration changes to the remote LAN.

Note You can also enable or disable remote LANs from the WLANs page by selecting the check boxes to the left of the IDs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down list, and clicking **Go**.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Managing Associated Access Points

Choose **Wireless Settings** > **Access Points**. The **Access Points Administration** window is displayed. The number of APs associated with the controller is displayed at the top of the window, along with the following details:

- **Manage**—The icons shown below indicate whether the AP is acting as Primary Controller (or Primary AP) or a subordinate AP.

  Figure 1: Primary Controller (or Primary AP) icon

  

  Figure 2: Subordinate AP icon

  

- **Location**—Location of the AP.
- **Name**—Name of the AP.
- **IP Address**—IP address of the AP.
- **AP MAC**—The MAC address of the AP.
- **Up Time**—Shows how long the AP has been associated to the controller.
- **AP Model**—The model number of the access point.

Note When an AP joins an AP group; or the RF profile of the AP group is changed, the CAPWAP process of the AP is restarted, to avoid rebooting of all the APs. A new CAPWAP restart payload is sent to the AP so that only the CAPWAP process is restarted. As a response, the AP will receive the new configuration specific to the new AP group or RF profile. The APs connection to the controller is lost and the AP reloads and re-joins the network.

Administering Access Points

Step 1 Choose **Wireless Settings** > **Access Points**.

The **Access Points Administration** window is displayed. You can only administer those APs that are associated to the controller.

Step 2 Click the **Edit** icon adjacent to the AP you want to manage.
The **Edit** window with the **General** tab is displayed.

Step 3 Under the **General** tab, you can edit the following AP parameters:

- **Operating Mode** and **Make me Controller**—For a primary AP, the **Operating Mode** field shows *AP & Controller*. For other associated APs, this field shows **AP Only**.

  The **Make me Controller** button is available only for subordinate APs that are capable of participating in the primary Election process. Click this button to make this AP the primary AP.

- **IP Configuration**—Choose **Obtain from DHCP** to let the IP address of the AP be assigned by a DHCP server on the network, or choose to have a **Static IP** address. If you choose to have a static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields.
- **AP Name**—Edit the name of the AP. This is a free text field.
- **Location**—Edit a location for the AP. This is a free text field.

The following non-editable AP parameters are also displayed under the **General** tab:

- AP MAC address
- AP Model number
- IP Address of the access point (non-editable only if **Obtain from DHCP** has been selected).
- Subnet mask (non-editable only if **Obtain from DHCP** has been selected).
- Gateway (non-editable only if **Obtain from DHCP** has been selected).

Step 4 (Only for the primary AP) Under the **Controller** tab, you can manually edit the following controller parameters for the integrated Mobility Express wireless LAN controller:

- **IP Address**—This IP address decides the login URL to the controller's web interface. The URL is in the format *https://<ip address>*. If you change this IP address, the login URL also changes.
- **Subnet Mask**
- **Country Code**

Step 5 Under the **Radio 1** and **Radio 2** tabs you can set the following parameters.

Note The **Radio 1** tab corresponds to the 2.4 GHz (802.11 b/g/n) radio on all APs, except the Cisco Aironet 3800 and 2800 series APs. On these APs, it can be set to either 2.4 GHz (802.11 b/g/n) or 5 GHz (802.11a/n/ac). The **Radio 2** tab corresponds to only the 5 GHz (802.11a/n/ac) radio on all APs.

The radio tab name also indicates the operational radio band within brackets.

Parameter	Description
Admin Mode	Enable or Disable the corresponding radio on the AP.
Band	Only present for Radio 1. It is set to 2.4 GHz by default. For 3800 and 2800 series APs you can change it to 5 GHz.

Parameter	Description	
Channel	For 2.4 GHz, you can set this to Automatic, or set a value from 1 to 11. Selecting **Automatic** enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the primary AP. This prevents neighboring APs from broadcasting over the same channel and prevents interference and other communication problems. For the 2.4 GHz radio, 11 channels are offered in the U.S. and up to 14 in other parts of the world. However, only 1-6-11 can be considered non-overlapping if they are used by neighboring APs. Assigning a specific value statically assigns a channel to that AP.	For 5 GHz, you can set this to Automatic, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, or 165. For the 5 GHz radio, up to 23 non-overlapping channels are offered. Assigning a specific value statically assigns a channel to that AP.
Channel Width	The channel width for 2.4 GHz can only be 20 MHz.	The channel width for 5 GHz can be set to Automatic, or to 20, 40, or 80 MHz, if channel bonding is used. Channel bonding groups the channels by 2 or 4 for a single radio stream. This increases the speed and the throughput. Because the number of channels is insufficient in 2.4 GHz, channel bonding cannot be used to enable multiple non-overlapping channels.
Transmit Power	You can set it to Automatic, or set a value from 1 to 8. This is a logarithmic scale of the transmit power, which is the transmission energy used by the AP, with 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 required until the maximum is reached.	

Step 6 Click **Apply** to save your changes and exit.

Configuring External Antennas

Before you begin

Antenna configuration is done for the external antenna that have been configured for access points. Configuring antennas are important for receiving better signals. The Antenna Configuration tab is visible in the **AP Edit** window only when there an external antenna configured with the access point (AP).

Step 1 Choose **Wireless Settings** > **Access Points**.

The Access Points Administration window is displayed. The number of APs associated with the controller is displayed at the top of the window

Step 2 Click the **Edit** icon adjacent to the AP you want to configure the external antenna.

Note The Antenna Configuration tab is visible only when there is an external antenna configured with the AP.

The Edit window with the Antenna Configuration tab is displayed.

Step 3 Under the **Antenna Configuration** tab, set the following parameters:

a. Under **Radio 2 (5GHz)**, complete the following parameters:

1. **Diversity** - From the drop-down list select one of the following options:
   - **a.** **Enable**: Select Enable to set the right and the left antennas to operate in the diversity mode. Both the right and left antennas will be enabled for sending and receiving signals.
   - **b.** **Right**: Select the Right option to set the right antenna for receiving and transmitting signals.
   - **c.** **Left**: Select the Left option to set the left antenna for receiving and transmitting signals.
2. Select the following antenna combinations for receiving and transmitting:
   - **a.** **A**—Use antenna A
   - **b.** **AB**—Use antennas A and B
   - **c.** **ABC**—Use antennas A, B, and C
   - **d.** **ABCD**—Use antennas A, B, C, and D

   Note If you select an invalid combination an error message is displayed.
3. **Antenna Gain** - Specify the resultant gain of the antenna attached to the device. Enter a value from –128 to 128 dB. If necessary, you can use a decimal in the value, such as 1.5.

b. Click **Apply** for the changes to take place.

Setting a Login Page for WLAN Guest Users

Before you begin, follow these steps to provide guest users with access to your network:

1. Set up a new WLAN or decide on an existing WLAN, to which you will provide access for guest users.

   You can also specifically set up a WLAN exclusively for guest access. This is done by setting the **WLAN Security** as **Guest** for that WLAN. For more information, see Adding a WLAN, on page 2.

2. Set up a guest user account. Go to **Wireless Settings > WLAN Users**, and set up an account with the **Guest User** check box selected. For more information, see Viewing and Managing WLAN Users, on page 8.

You can present the Guest users of your WLAN with either of the following login page options:

- A simple minimalist default login page with a few modification options. To configure this, see Setting the Default Login Page, on page 17.
- A customized login page uploaded into the controller. To configure this, see Setting a Customized Login Page, on page 18.

Setting the Default Login Page

Right out of the box, the default login page contains a Cisco logo and Cisco-specific text. You can choose to modify this default login page as described here.

Step 1 Choose **Wireless Settings** > **Guest WLAN**.

The Guest WLAN page is displayed. The number of Guest WLANs currently set up in the network is displayed at the top of the page.

Step 2 To use the default login page, in the **Page Type** drop-down list, choose **Internal**.

Step 3 Set the following parameters to modify the default internal login page:

- **Display Cisco Logo**—This field is set to **Yes** by default. To hide the Cisco logo that appears at the top-right corner of the default window, choose **No**. This field is set to **Yes** by default. However, you do not have an option to display any other logo.
- **Redirect URL After Login**— To have guest users redirected to a particular URL (such as the URL for your company) after login, enter the URL in this field. You can enter up to 254 characters.
- **Page Headline**—The default headline is *Welcome to the Cisco Wireless Network*. To create your own headline on the login page, enter the desired text in this field. You can enter up to 127 characters.
- **Page Message**— 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*. To create your own message on the login page, enter the desired text in this field, You can enter up to 2047 characters.

Step 4 Click **Apply**.

Setting a Customized Login Page

You can create a custom login page on a computer, compress the page and image files into a .TAR file, and then upload it to the controller. The upload is done via HTTP.

Note When you save the controller's configuration, it does not include extra files or components, such as the web authentication bundle, that you download and store on your controller. Hence, manually save external backup copies of such files.

Note Cisco TAC is not responsible for creating a custom web authentication bundle.

Before you begin

- Create a custom login page on a computer while ensuring the following:
  - Name the login page **`login.html`**. The controller prepares the web authentication URL based on this name. If the server does not find this file after the web authentication bundle has been untarred, the bundle is discarded, and an error message appears.
  - The page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal controller web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection.
  - Include input text boxes for the username and the password.
  - Extract and set the action URL in the page from the original URL.
  - Include scripts to decode the return status code.
  - All paths used in the main page (to refer to images, for example) are of relative type.
  - No filenames within the bundle are longer than 30 characters.
- Compress the page and image files into a ,TAR file. The maximum allowed size of the files in their uncompressed state is 1 MB.

  Cisco recommends that you use an application that complies with GNUstandards to compress the .TAR file (also referred to as the web authentication bundle.). If you load a web authentication bundle with a .TAR compression application that is not GNU compliant, the controller will not be able to extract the files in the bundle.

  The .TAR file enters the controller’s file system as an untarred file.

Note If you have a complex customized web authentication bundle which does not comply with the aforementioned prerequisites, then Cisco recommends that you host it on an external web server. See (..)

Step 1 Choose **Wireless Settings** > **Guest WLAN**.

The **Guest WLAN** page is displayed. The number of Guest WLANs currently set up in the network is displayed at the top of the page.

Step 2 To upload a customized login page into the controller, in the **Page Type** drop-down list, choose **Customized**.

Step 3 Click **Upload**, to browse to and upload the .TAR file of the customized web authentication bundle.

Step 4 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter that URL in the **Redirect URL After Login** text box. You can enter up to 254 characters.

Step 5 Click **Apply**.

Click **Preview** to view your customized web authentication login page.

Managing the Internal DHCP Server

The Cisco Mobility Express controller contains an internal DHCP server which manages the DHCP addresses assigned to network devices associated with it. The IP addresses assigned to client devices are not preserved across reboots. This enables reuse of IP addresses across multiple client devices. To resolve IP address conflicts, client devices need to release their existing IP address and request for a new one.

Starting Cisco Wireless Release 8.3, you can configure the internal DHCP server using the Cisco Mobility Express web interface.

Add DHCP Pool

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Click **Add New Pool**.

The **Add DHCP Pool** window appears.

Step 3 In the **Pool Name** field, enter the desired name.

The DHCP pool name must meet the following conditions:

Step 4 From the **Active** drop-down list, select either **Enabled** or **Disabled**.

The default setting is **Disabled**.

Step 5 In the **VLAN ID** field, specify the VLAN ID for the DHCP Pool.

Note Select the **Management Network** checkbox to set the management interface IP address of the Cisco Mobility Express controller as the DHCP server IP address.

Step 6 In the **Network/Mask** fields, specify the IP address of the network and the subnet mask.

Step 7 In the **Start IP** field, specify the starting IP address for the network.

Step 8 In the **End IP** field, specify the ending IP address for the network.

Step 9 In the **Default Gateway** field, specify the IP address for the default gateway to the network.

Note The default gateway, starting IP address, and the ending IP address must be in the same subnet.

Step 10 In the **Domain Name** field, enter the desired name.

The domain name must meet the following conditions:

Step 11 From the **Name Servers** drop-down list, select either **OpenDNS** or **User Defined**.

The default setting is **OpenDNS**.

Step 12 Enter the IP address for the name servers in the provided fields.

Edit DHCP Pool

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Click the <edit_icon.gif> icon in the row containing the DHCP Pool whose details you wish to modify.

The desired row in the DHCP Pool table becomes editable (or the **Edit DHCP Pool** window appears.)

Step 3 In the DHCP Pool table, make the desired modifications inline (or in the **Edit DHCP Pool** window).

Step 4 Click **Apply**.

The DHCP Pool table is refreshed and the updated entry appears in this table.

Delete DHCP Pool

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Click the **X** icon in the row containing the DHCP pool you wish to delete.

A warning message appears.

Step 3 Click **Yes** in the pop-up window.

The DHCP pool table is refreshed and the deleted entry is removed from this table.

View DHCP Lease Details

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Under the DHCP pool table, click **DHCP Leases**.

The **DHCP Pool Information** window appears where you can view details such as the host name, its MAC address, assigned IP address, and lease expiry details.

Note You can release a specific IP address by removing the lease to the host in the corresponding entry of the **DHCP Pool Information** table.

Export Details of Leased IP Addresses

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Under the DHCP pool table, click **DHCP Leases**.

The **DHCP Pool Information** window appears.

Step 3 Below the **DHCP Pool Information** table, click **Export**.

Step 4 Choose the format in which you wish to export the details of the leased IP addresses and the corresponding hosts.

Release Leased IP Address

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Under the DHCP pool table, click **DHCP Leases**.

The **DHCP Pool Information** window appears.

Step 3 In the row containing the the host assigned the leased IP address you wish to delete, click the <release_icon.gif> icon.

A warning message appears.

Step 4 You can release a specific IP address by removing the lease to in the corresponding entry of the **DHCP Pool Information** table.

Step 5 Click **Yes** in the pop-up window.

The **DHCP Pool Information** table is refreshed and the deleted entry is removed from this table.

Information about Authentication Caching

With the Authentication Caching feature, client information essential for authentication is stored locally in the cache on the Controller, when the authentication with the RADIUS Server is successful. When the connectivity to the RADIUS server is lost, the information stored in the cache is used for the authentication of clients.

You can also configure cache when the RADIUS Server is up and running. If the client details are not available locally, the the request for authentication is sent through the RADIUS Server.

The following security types are supported:

- MAC Filtering using RADIUS Server
- WPA/WPA2-Dot1x Authentication
- Web-Auth on MAC Filtering Failure
- Identity PSK (iPSK)

Configuring WPA/WPA2 Dot1x Authentication

Follow the procedure given below to configure WPA/WPA2 Dot1x Authentication:

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN/RLAN Configuration** page is displayed.

Step 2 Click **Add new WLAN/RLAN**.
The Add new WLAN/RLAN window is displayed.

Step 3 Under the **General** tab, set the following parameters:

a) **Profile Name**— The profile name must be unique and should not exceed 32 characters.
b) **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.

Step 4 Under the **WLAN Security** tab, set one of the following security authentication options from the **Security** drop-down list:

a) **WPA2 Enterprise**—This option stands for Wi-Fi Protected Access 2, with a local authentication server or a RADIUS server.
b) In the **Radius Server** section, enable **Authentication Caching**, enter the **User Cache Timeout** in minutes, and enable **User Cache Reuse**, if required. By default, **User Cache Reuse** is disabled.
c) Click **Add RADIUS Authentication Server**. Enter the server details and click **Apply**.

Note The following are the AV Pairs configured on the RADIUS Server:

- **AC-Supported=yes** - It is sent through ACCESS-REQUEST only to indicate authentication cache support is enabled.
- **AC-User-Name** - Username of the dot1x use is sent as part of ACCESS-ACCEPT.
- **AC-Credential-Hash** - User password hashed using RFC2865 is sent as part of ACCESS-ACCEPT.

Step 5 Choose the **Advanced** tab.

Step 6 Use the **Allow AAA Override** toggle button to enable AAA override.

Step 7 Click **Apply**.

Configuring MAC Filtering on RADIUS Server

Follow the procedure given below to configure MAC Filtering and to enable the On MAC Filter Failure on the RADIUS Server:

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN/RLAN Configuration** page is displayed.

Step 2 Click **Add new WLAN/RLAN**.
The Add new WLAN/RLAN window is displayed.

Step 3 Under the **General** tab, set the following parameters:

a) **Profile Name**— The profile name must be unique and should not exceed 32 characters.
b) **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.

Step 4 Under the **WLAN Security** tab, set the following parameters:

a) Enable **Guest Network**.
b) Enable **MAC Filtering**.
c) Select **Captive Portal** as **`External Splash Page`**.
d) In the **Captive Portal URL** field, enter the Web Server URL.
e) Select the **Access Type** as **`RADIUS`**.
f) Enable **On MAC Filter Failure**.
g) Click **Add RADIUS Authentication Server**. Enter the server details and click **Apply**.

Step 5 Choose the **Advanced** tab.

Step 6 Use the **Allow AAA Override** toggle button to enable AAA override.

Step 7 Click **Apply**.

Configuring Identity PSK

Follow the procedure given below to configure Identity PSK:

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN/RLAN Configuration** page is displayed.

Step 2 Click **Add new WLAN/RLAN**.
The Add new WLAN/RLAN window is displayed.

Step 3 Under the **General** tab, set the following parameters:

a) **Profile Name**— The profile name must be unique and should not exceed 32 characters.

b) **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.

Step 4 Under the **WLAN Security** tab:

a) Enable **MAC Filtering**.

b) Set the following security authentication option from the **Security Type** drop-down list:**WPA2 Personal**—This option stands for Wi-Fi Protected Access 2 with pre-shared key (PSK). WPA2 Personal is a method used for securing your network with the use of a PSK authentication.

c) Select the **Passphrase Format** as either **`HEX`** or **`ASCII`**.

d) Enter the **Passphrase** and **Confirm Passphrase**.

e) In the **Radius Server** section, enable **Authentication Caching**, enter the **User Cache Timeout** in minutes, and enable **User Cache Reuse**, if required. By default, **User Cache Reuse** is disabled.

f) Click **Add RADIUS Authentication Server**. Enter the server details and click **Apply**.

After a successful MAC authentication, RADIUS Server returns the following Cisco AVPair attributes:

- **psk-mode** - Value could be either **`ASCII`**, **`HEX`**, **`asciiEnc`**, or **`hexEnc`**.
- **psk**

Note The key is stored in the local cache along with the MAC Address, and is used for subsequent authentications.

Note The psk value could be a simple **`ASCII`** or **`HEX`** value or encrypted bytes in case of **`asciiEnc`** or**`hexEnc`**. The algorithm used for encryption or decryption is as perRFC2865 (user-password section – 16 bytes authenticator followed by encrypted key).

Step 5 Choose the **Advanced** tab.

Step 6 Use the **Allow AAA Override** toggle button to enable AAA override.

Step 7 Click **Apply**.

Verifying Authentication Cached Users

Step 1 To verify the authenticated cached users, choose **Management** > **Admin Accounts**.
The Admin Accounts page is displayed.

Step 2 In the **Admin Accounts** page, choose the **Auth Cached Users** tab.
The auth cached user summary is displayed with details such as, MacAddress, Username, SSID, Timeout, and Remaining Time.

Step 3 Double-click the listed auth cached user to view the cache details.