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.

Adding a WLAN

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

The **WLAN Configuration** window is displayed.

Step 2 To create a new WLAN, 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**—Enter up to 32 characters for the profile name to be assigned to this WLAN. The profile name must be unique.
- **SSID**—Enter up to 32 characters for the SSID to be assigned to this WLAN.
- **Admin State**—From the drop-down list, choose **Enabled** to enable this WLAN. Otherwise choose **Disabled**. The default is Enabled.
- **Radio Policy**—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 (the 802.11b or 802.11g modes) or on 5GHz (802.11a mode) or both.

  Set the RF profiles for APs that are associated with the controller. Choose one of the following from the **Radio Policy** drop-down list:

  - **All** (default)
  - **802.11a only**
  - **802.11a/g**
  - **802.11g only**
  - **802.11b/g**

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

- **Security**—Choose one of the following security authentication options from this drop-down list:
  - **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 Authentication** drop-down list:

- **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 6.
- **Display Terms & Conditions**—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.

- **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.
- **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 **Shared Key** field.
- **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.

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.

Note VLAN trunking is also disabled by default in Cisco Mobility Express. To enable VLAN trunking, execute **config ap vlan-trunking enable** *ap-name* on the command line interface of the Cisco Mobility Express controller.

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 creating or editing user accounts for this WLAN. See Viewing and Managing WLAN Users, on page 6.

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.

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**.

  For information on adding WLANs, see Adding a WLAN, on page 2.
- 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.

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.

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:

- **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:

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

- **System Name**—Edit the name that you have assigned to this controller. You can enter up to 31 ASCII characters. The system name is first specified during the initial configuration wizard.
- **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**—You can set the country code for the controller and all associated APs using this drop-down list. Once you apply your changes, the country codes on all subordinate APs are automatically changed, the APs reboot and come back online with the new country code, and rejoin the controller. However the change will not be applied on the controller and the primary AP until the primary AP is manually rebooted.

Step 5 Under the **802.11 b/g/n** tab, you can set the following parameters:

- **Admin Mode**—Enabled or Disabled. This enables or disables the corresponding radio on the AP (2.4 GHz for 802.11 b/g/n)
- **Channel**—Automatic, 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.
- **Channel Width**—20 MHz

  The channel width for 2.4 GHz can only be 20 MHz.

  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**—Automatic, 1 to 8.

This is a logarithmic scale of the transmit power, that 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 Under the **802.11 a/n/ac** tab, you can set the following parameters:

- **Admin Mode**—Enabled or Disabled. This enables or disables the corresponding radio on the AP (5 GHz for 802.11a/n/ac).
- **Channel**—Automatic, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 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**—20, 40, 80 MHz

  The channel width for 5 GHz can be set to 20, 40, or 80 MHz, if channel bonding is used.
- **Transmit Power**—1 to 8.

  This is a logarithmic scale of the transmit power, that 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 7 Click **Apply** to save your changes and exit.

Creating a Customized Login Page for Guest WLAN Users

Before you begin

To allow a guest user the 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 6.

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 In the window that is displayed, set the following parameters:

- **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 3 Click **Apply**.