



## WLANs Tab

---

The WLAN tab on the menu bar enables you to create, configure, and delete wireless local area networks (WLANs) on your Cisco WLC. Use the left navigation pane to access specific WLAN parameters.

You can access the following pages from the WLANs tab:

- [WLANs](#)
- [AP Groups](#)

When you choose **WLANs** and click the blue arrow adjacent the profile, you can access the following options:

- [Deleting WLANs](#)
- [Mobility Anchors](#)
- [802.11u](#)
- [HotSpot 2.0](#)
- [Foreign Maps](#)
- [Service Advertisement](#)

## WLANs

Click **WLANs** to navigate to the WLANs page.

This page shows a summary of the wireless local area networks (WLANs) that you have configured on your network. From this page, you can add, remove, enable, disable, or edit WLANs.



### Note

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

The Cisco UWN (Unified Wireless Network) solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID (Service Set Identifier), and it can be assigned with unique security policies. All Cisco WLCs publish up to 16 WLANs to each connected access point, but you can create up to 512 WLANs and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

**Note**

All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A Cisco WLC with OfficeExtend access points in an access point group publishes up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID, but for Cisco OEAP 600, this is not applicable.

**Note**

The Cisco OEAP 600 Series access point supports only two WLANs and one RLAN, and the WLAN ID must be from 1 to 8.

You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group. See the [AP Groups](#) page for more information on access point groups.

**WLAN List Filter**

Click the **Change Filter** link to display the Search WLANs dialog box to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire WLAN list.

You can create a filter to display the list of WLANs by profile name, SSID, status, or a combination of SSID and status.

The current filter parameters are displayed in the Current Filter field.

**Note**

When you enable the Profile Name filter, other filter options are disabled. When you enable the SSID or the Status filter, the Profile Name filter is disabled.

The Search WLANs dialog box enables you to search configured WLANs based on the following filters:

- Profile Name—Select the **Profile Name** check box and enter a profile name.
- SSID—Select the SSID check box and enter an SSID.
- Status—Select the Status check box and choose **Enabled** or **Disabled**.
- Find—Click **Find** to search for the WLAN based on the filter parameters.

## WLAN Information Table

Click WLANs from the left navigation menu to view the WLAN page. The WLANs page displays a summary of the configured WLANs.

*Table 3-1 WLANs Summary*

Parameter	Description
WLAN ID	ID of the WLAN.
Type	Type of LAN: WLAN, Guest LAN, or Remote LAN.
Profile Name	Profile name of the WLAN.
WLAN SSID	Definable name of the WLAN (text string).

**Table 3-1**      *WLANs Summary*

Parameter	Description
Admin Status	Status of the WLAN is either enabled or disabled.
Security Policies	Security policies enabled on the WLAN.

Click the WLAN ID to modify the selected WLAN characteristics. The [Editing WLANs](#) page appears.

To view mobility anchor settings, click the blue arrow adjacent to the profile and choose **Mobility Anchors**.

To enable or disable a WLAN from the WLANs page, select the check box to the left of the WLAN or WLANs, choose **Enable Selected** or **Disable Selected** from the drop-down list, and click **Go**.

To delete a WLAN, do one of the following:

- Click the blue arrow adjacent to the profile and choose **Remove**. You are prompted to confirm the removal of the selected WLAN.
- Select the check box for the WLAN or WLANs, choose **Remove Selected** from the drop-down list, and select **Go**. You are prompted to confirm the removal of the selected WLAN.
- Click **Go** to select an option from the drop-down list.

## Creating New WLANs

To configure a new WLAN for a wired guest LAN, choose **Create New** from the drop-down list and click **Go** to navigate to the New WLAN page.

**Table 3-2**      *WLAN > New Parameters*

Parameter	Description
Type	Type of WLAN: Guest WLAN, WLAN, or Remote LAN <b>Note</b> Cisco 2504 Controllers does not support wired guest services.
Profile Name	Profile name of the WLAN

Table 3-2 WLAN &gt; New Parameters

Parameter	Description
SSID	SSID field is displayed if you choose WLAN from the <b>Type</b> drop-down list. Definable name of the WLAN (text string). This is the SSID broadcast name for the WLAN.
ID	<p>ID number for the WLAN</p> <p>Guest LAN—Enter guest LAN identifier between 1 and 5.</p> <p>WLAN—Enter WLAN identifier between 1 and 512. If there is more than one two WLANs enabled for an AP group, disable all WLANs and then enable only two of them.</p> <p>Remote LAN—Enter remote LAN identifier between 1 and 512. If there is more than one remote LAN enabled for an AP group, disable all remote LANs and then enable only one of them.</p> <p><b>Note</b> If the Cisco OEAP 600 is in the default group, the WLAN/Remote LAN IDs must be set as less than ID 8.</p>

## Creating a WLAN

- Step 1** Choose a WLAN type (Guest LAN, WLAN, or Remote LAN) from the drop-down list.



**Note** The WLANs that are not assigned to the access points are denoted with an asterisk (\*) symbol.



**Note** To connect wired clients to a corporate network via an Office Extended AP, choose **Remote LAN** from the WLAN Type drop-down list. Once a user creates a remote LAN, it shows up on the list page as a distinct WLAN type.



**Note** Remote LANs should be removed from a Cisco WLC's configuration before moving to a code base that does not support the remote LAN functionality. The remote LAN is called a WLAN in releases earlier than Cisco WLC Release 7.0.116.0, which may cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LANs are supported only in Cisco WLC Release 7.0.116.0 and later.

- Step 2** Enter a profile name for the WLAN in the Profile Name text box (spaces are supported in the profile name).

- Step 3** Enter a text name for the WLAN in the WLAN SSID text box. (This is the SSID broadcast name for the WLAN.)



**Note** The SSID field is not available for Guest LANs and Remote LANs.

- Step 4** Choose the ID number for the WLAN from the WLAN ID drop-down list.
- Step 5** Click **Apply** to bring up the [Editing WLANs](#) page, where you can continue configuring the WLAN. Once created, the selected WLAN type shows up in the list page as a distinct WLAN type: guest LAN, WLAN, or remote WLAN.
- 

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

## Creating a Remote LAN

This section describes configuring remote LANs.



### Caution

You must remove all the remote LANs from the configuration of the Cisco WLC before moving to a release that does not support the remote LAN functionality. The remote LAN is called a WLAN in releases earlier than Cisco WLC Release 7.0.116.0, which may cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LANs are supported only in Cisco WLC 7.0.116.0 and later .

---



### Note

Only four clients can connect to an OEAP 600 series access point through a remote LAN port. This number does not affect the fifteen limit imposed for the Cisco WLC WLANs. The Remote LAN client limit supports connecting a switch or hub to the Remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices will be able to connect until one of the devices is idle for more than one minute.

---

- Step 1** Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs and remote LANs currently configured on the Cisco WLC. For each WLAN, you can see its WLAN/Remote LAN ID, profile name, type, SSID, status, and security policies. The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.



### Note

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

---

- Step 2** Create a new WLAN by choosing **Create New** from the drop-down list and clicking **Go**. The WLANs > New page appears.
- Step 3** From the Type drop-down list, choose **Remote LAN** to create a remote LAN.
- Step 4** In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN. The profile name must be unique.
- Step 5** From the WLAN ID drop-down list, choose the ID number for this WLAN.
- Step 6** 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 7** 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 8** 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 9** Save your configuration.

## Editing WLANs

To edit your WLAN settings, choose **WLANs** and click the Profile name to navigate to the WLANs > Edit page. For new WLANs, create a new WLAN as described in [Creating New WLANs](#) page, and then click **Apply** to navigate to this page.

This page enables you to edit the configurable parameters for a WLAN.

The WLAN > Edit page consists of the following four tabs:

- General
- Security
- QoS
- Policy-Mapping
- Advanced

### General Tab

**Table 3-3** General Tab Parameters

Parameter	Description
Profile Name	Configured profile name of the WLAN
Type	Type of LAN that is configured in the WLANs > New page: WLAN, Guest LAN, or Remote LAN
SSID	SSID of the WLAN
Status	WLAN that you want to enable or disable; the default is enabled
Security Policies	Security policies for a WLAN that you set from the Security tab
	<b>Note</b> This field appears when you choose WLAN as the Type in the WLANs > New page.

Table 3-3 General Tab Parameters

Parameter	Description
Radio Policy	<p>WLAN radio policy to apply to All (802.11a/b/g), 802.11a only, 802.11g only, 802.11b/g only, or 802.11a/g only. This setting requires that the selected bands be enabled on the <a href="#">802.11a/n/ac Global Parameters</a> and <a href="#">802.11a/n/ac Client Roaming</a> pages.</p> <p><b>Note</b> This field appears only when you choose WLAN as the Type in the WLANs &gt; New page.</p>
Interface/Interface Group (G)	<p>Limited to the nonservice port and nonvirtual interface names configured on the <a href="#">Interfaces</a> page.</p> <p><b>Note</b> This field appears only when you choose WLAN as the Type in the WLANs &gt; New page.</p>
Multicast VLAN Feature	<p>Check box that you can select to enable the multicast VLAN feature. The default option is none.</p> <p><b>Note</b> The Multicast Interface field appears only after you enable the Multicast VLAN feature text box.</p> <p><b>Note</b> You have to configure the multicast VLAN feature only once if you want to use the multicast feature.</p>
Broadcast SSID	Service Set Identifier for this WLAN.
Ingress Interface	<p>Guest LAN's ingress interface. By default, None is selected.</p> <p><b>Note</b> This field is available only for guest LANs.</p>
Egress Interface	<p>Remote LAN's or guest LAN's egress interface. By default, management is selected.</p> <p><b>Note</b> This field is available only for remote LANs and guest LANs.</p>
NAS-ID	<p>Network Access Server identifier. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters.</p> <p>Beginning in Release 7.4 and later releases, you can configure the NAS-ID on the interface, WLAN, or an access point group. The order of priority is AP Group NAS-ID &gt; WLAN NAS-ID &gt; Interface NAS-ID.</p>

**Security Tab**

- [Layer 2 Tab Parameters](#)
- [Layer 3 Tab \(for WLAN\) Parameters](#) or [Layer 3 Tab \(for Guest LAN and Remote LAN\) Parameters](#)
- [AAA Servers Tab Parameters](#)

**Important Limitations and Guidelines:**

- CCX is not supported on the Cisco OEAP 600 access points and all elements related to CCX are not supported.
- Layer 2 security is not supported on guest LANs.
- Only the following options are supported for Cisco OEAP 600 Series access points: None, WPA+WPA2, Static WEP, and 802.1X (only for remote LANs).

- Beginning in Release 7.4 and later releases, the controller performs both web authentication (WebAuth) and 802.1X authentication in the same WLAN. The clients are initially authenticated with 802.1X. After a successful authentication, the client must provide the WebAuth credentials. After a successful WebAuth authentication, the client is moved to the run state.
  - 802.1x authentication can be performed using AAA or a local database.
- For auto-anchored guest WLANs, the guidelines are as follows:
  - Only the anchor controller must have both dot1x and WebAuth configured.
  - Both anchor and foreign controller must be configured for dot1x.

Table 3-4 Layer 2 Tab Parameters

Parameter		Description
Layer 2 Security	None	No Layer 2 security selected.
	WPA+WPA2	Wi-Fi Protected Access. For information on these settings, see the <a href="#">Layer 2 WPA + WPA2 Parameters</a> topic.
	802.1X	WEP 802.1X data encryption type. For information on these settings, see the <a href="#">Layer 2 802.1X Parameters</a> topic.
	Static WEP	Static WEP encryption parameters. For information on these settings, see the <a href="#">Layer 2 Static WEP Parameters</a> topic.
	Static WEP + 802.1X	Both Static WEP and 802.1X parameters. For information on these settings, see the <a href="#">Layer 2 Static WEP Parameters</a> and <a href="#">Layer 2 802.1X Parameters</a> topics.
	CKIP	Cisco Key Integrity Protocol (CKIP). Functional on AP Models 1100, 1130, and 1200, but not AP 1000. Aironet IE needs to be enabled for this feature to work. CKIP expands the encryption keys to 16 bytes. For information on these settings, see the <a href="#">Layer 2 CKIP Parameters</a> topic.
	None + EAP Passthrough	Both None and Extensible Authentication Protocol Passthrough parameters. If EAP-Passthrough on the WLAN is enabled, the WLAN might be exposed to security attacks on the network.
MAC Filtering	MAC address filtering. You can locally configure clients by their MAC addresses in the <a href="#">Adding MAC Filters</a> page. Otherwise, configure the clients on a RADIUS server.	



Table 3-4 Layer 2 Tab Parameters

Parameter	Description
Mac Auth or Dot1x	<p>MAC authentication failover to Dot1x authentication for the WLAN. The prerequisites for the failover to work are as follows:</p> <ul style="list-style-type: none"> <li>• MAC Filtering must be enabled.</li> <li>• Layer 2 security must be 802.1X and Static WEP.</li> </ul> <p>The failover does not work with RADIUS NAC feature.</p> <p>If MAC authentication is successful and the client sends an EAP start request to start 802.1X authentication, the client must pass 802.1X authentication to send data traffic, or the client is deauthenticated.</p> <p>When MAC Auth fails, the client authenticates using 802.1X or it is deauthenticated. If MAC Auth passes, then the client authenticates using 802.1X if required (for Static WEP Clients) depending on the client configuration.</p>
<b>Fast Transition</b>	
Fast Transition	Check box to enable or disable a fast transition between access points.
Over the DS	Check box to enable or disable a fast transition over a distributed system.
Reassociation Timeout	Time in seconds after which a fast transition reassociation times out.
<b>Lobby Admin Configuration</b>	
Lobby Admin Access	Check box to enable or disable lobby administrator access

Table 3-5 Layer 2 WPA + WPA2 Parameters

Parameter	Description
<b>Fast Transition</b>	
Fast Transition	Check box to enable or disable a fast transition between access points.
Over the DS	Check box to enable or disable a fast transition over a distributed system.
Re-association Timeout	Time in seconds after which a fast transition reassociation times out.
<b>Protected Management Frame</b>	
PMF	<p>Drop-down list from which you can choose the following:</p> <ul style="list-style-type: none"> <li>• Disabled—Disables 802.11w MFP protection on a WLAN.</li> <li>• Optional—Enables 802.11w MFP protection on a WLAN.</li> <li>• Required—Requires clients to negotiate 802.11w MFP protection on a WLAN.</li> </ul> <p>802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast management frames. IGTK is a random value, assigned by the authenticator station (Cisco WLC) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the 4 way handshake and is used only on WLANs configured with WPA or WPA2 security at Layer 2.</p>

Table 3-5 Layer 2 WPA + WPA2 Parameters

Parameter	Description
Comeback Timer	Association comeback interval, in seconds. This is the interval for which an associated client must wait for before the association is tried again after it is denied with the status code 30 message:  Association request rejected temporarily; Try again later. The range is from 1 to 10 seconds. The default value is 1 second.
SA Query Timeout	Security Association (SA) query interval, in ms. The timeout is an interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the Cisco WLC.  The range is from 100 to 500. The default value is 200.
<b>WPA+WPA2 Parameters</b>	
WPA Policy	Check box to enable or disable the WPA Policy.
WPA2 Policy	Check box to enable or disable the WPA2 Policy.
WPA2 Encryption	WPA2 encryption type: TKIP or AES. Available only if the WPA2 Policy is enabled.
OSEN Policy	Check box to enable or disable the OSEN Policy.
OSEN Encryption	OSEN encryption type: TKIP or AES. Available only if the WPA2 Policy is enabled.
<b>Authentication Key Management</b>	
802.1x	An access point that supports 802.1X acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network. If 802.1X is selected, only 802.1X clients are supported.
CCKM	Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 ms.
PSK	ASCII or HEX format that you can choose, after which you enter the preshared key.
FT 802.1x	Authentication key management for fast transition using 802.1X. <b>Note</b> You can configure FT 802.1X only if you enable the WPA2 policy.
FT PSK	ASCII or HEX format that you can choose, after which you enter the preshared key for fast transition. <b>Note</b> You can configure FT PSK only if you enable the WPA2 policy.
PMF 802.1x	802.1X authentication for protection of management frames (PMF).
PMF PSK	Preshared keys (PSK) for PMF. Select an ASCII or HEX format, and enter the preshared key for PMF.

**Table 3-5** *Layer 2 WPA + WPA2 Parameters*

Parameter	Description
WPA gtk-randomize State	Drop-down list to enable or disable the WPA group temporal key (GTK) randomize state.
<b>Note</b>	For the Cisco OEAP 600 Series APs, do not choose CCKM. Choose either 802.1X or PSK.
<b>Note</b>	For the Cisco OEAP 600 Series access point, security encryption settings must be identical for WPA and WPA2 for TKIP and AES.
<b>Note</b>	Fast roaming for clients is not supported on the Cisco OEAP 600 Series access points. Dual mode voice clients might experience reduced call quality when they roam between the two spectrum's on the Cisco OEAP 600 Series access point. We recommend that you configure voice devices to only connect on one band, either the 2.4-GHz to 5.0-GHz radio.

**Table 3-6** *Layer 2 802.1X Parameters*

Parameter	Description
802.11 data encryption	WEP 802.11 data encryption type.
Type	Security type.
Key size	Key size that you can choose: <ul style="list-style-type: none"> <li>• None</li> <li>• 40 bits</li> <li>• 104 bits</li> </ul> <p><b>Note</b> The third-party AP WLAN (17) can only be configured with 802.1X encryption. Drop-down configurable 802.1X parameters are not available for this WLAN.</p>

**Layer 2 802.1X Port Parameters for a Remote LAN**

Host Mode	<p>Modes of authentication for IEEE 802.1X. It can either be Single Host or Multi Host.</p> <ul style="list-style-type: none"> <li>• In the Single Host mode, when the port link state goes up, the AP detects the client by sending EAPOL frame. If the client leaves or is replaced with another client, the AP changes its port link state to down, making the port unauthorized.</li> <li>• In the Multi Host mode, only one client has to be authenticated for all the clients to gain network access in a port. If the port becomes unauthorized, access is denied to all the attached clients.</li> </ul>
Violation Mode	<p>When a security violation occurs, the port is protected depending on the configured violation action, which can be Shutdown, Replace, or Protect.</p> <ul style="list-style-type: none"> <li>• Shutdown—Disables the port.</li> <li>• Replace—Removes the current session and initiates the authentication for a new host. This is the default behavior.</li> <li>• Protect—Drops packets with unexpected MAC addresses without generating a system message.</li> </ul>

**Table 3-6** *Layer 2 802.1X Parameters*

Parameter	Description
Pre-Authentication	Configures pre-authentication VLAN for remote LAN 802.1X.
MAB Mode	Enables port-based access control using the MAC address of an endpoint.

**Table 3-7** *Layer 2 Static WEP Parameters*

Parameter	Description
802.11 Data Encryption	Static WEP encryption type.
Type	Security type.
Key size	Key size that you can choose: <ul style="list-style-type: none"><li>• not set</li><li>• 40 bits</li><li>• 104 bits</li></ul>
Key Index	Key index, from 1 to 4. <b>Note</b> One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.

**Table 3-8** *Layer 2 CKIP Parameters*

Parameter	Description
802.11 Data Encryption	Current key information.
Key size	Key size that you can choose: <ul style="list-style-type: none"><li>• not set</li><li>• 40 bits</li><li>• 104 bits</li></ul>
Key Index	Key index, from 1 to 4. <b>Note</b> One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.

Table 3-8 Layer 2 CKIP Parameters

Parameter	Description
MMH Mode	Multimodular Hash (MMH) mode that you can enable; the default is enabled.
Key Permutation	Key permutation that you can enable or disable. The default is enabled. Key permutation is a data encryption technique that uses the basic encryption key and the current initialization vector (IV) to create a new key.

Table 3-9 Layer 3 Tab (for WLAN) Parameters

Parameter	Description	
Layer 3 Security	None	Setting that indicates that no Layer 3 security is selected.
	IPSec	<p>Setting to enable IPSec. Check software availability and client hardware compatibility before implementing IPSec.</p> <p><b>Note</b> You must have the optional VPN/Enhanced Security Module (crypto processor card) installed to enable IPSec. Verify that it is installed on your Cisco WLC using the <a href="#">Inventory</a> page.</p>
	VPN Pass-Through	<p>VPN pass-through that you can enable or disable.</p> <p><b>Note</b> This option is not available on Cisco 5508 WLC. However, you can replicate this functionality on the Cisco 5508 WLC by creating an open WLAN using an ACL.</p> <p>For information on these settings, see <a href="#">Layer 3 VPN Passthrough Parameters</a>.</p>

Table 3-9 Layer 3 Tab (for WLAN) Parameters

Parameter	Description
Web Policy	<p>Check box that you can select to enable Web Policy.</p> <p><b>Note</b> The Cisco WLC forwards DNS traffic to and from wireless clients prior to authentication if there is no explicit deny rule for DNS traffic in the Pre-Auth ACL.</p> <p><b>Note</b> Web Policy cannot be used with IPsec or VPN pass-through options.</p> <p>The following parameters are displayed:</p> <ul style="list-style-type: none"> <li>• Authentication—Prompts the user for username and password while connecting the client to the wireless network.</li> <li>• Passthrough—Enables the user to access the network directly without entering the username and password.</li> <li>• Conditional Web Redirect—Enables the user to be conditionally redirected to a particular web page after 802.1X authentication has completed successfully. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server.</li> <li>• Splash Page Web Redirect—Redirects the user to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the splash web page on your RADIUS server.</li> <li>• On MAC Filter failure—Enables web authentication MAC filter failures.</li> <li>• Web policy done locally on AP</li> </ul> <p>This option is supported only on ap1g2 and ap3g2 platforms.</p>
Captive Network Assistant Bypass	You can select enable, disable or none. Option 'none' applies the global configuration.
Preauthentication ACL	IPv4 or IPv6 ACLs to be used for traffic between the client and the Cisco WLC. Refer to the <a href="#">Access Control Lists</a> topic for more information.
WebAuth FlexACL	<p>Drop-down list from which you can choose the FlexConnect ACL for external web authentication in locally switched WLANs.</p> <p>For more information about creating FlexConnect ACLs, see <a href="#">Adding Access Control Lists</a>.</p> <p><b>Note</b> The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.</p>
Sleeping Client	Check box that you can select to enable support for sleeping clients. This feature is not applicable for remote LANs and guest LANs.
Sleeping Client Timeout	Maximum amount of time after the idle timeout, in hours, before a sleeping client is forced to reauthenticate. The range is from 1 to 720. The default value is 12. This field is enabled only when you select the Sleeping Client check box. Also, the clients need not provide the login credentials when they move from one Cisco WLC to another (if Cisco WLCs are in the same mobility group) between the sleep and wake up times.

**Table 3-9** *Layer 3 Tab (for WLAN) Parameters*

Parameter	Description
Override Global Config	Setting that is displayed if you choose Authentication. Select this check box to override the global authentication configuration set on the <a href="#">Web Login Page</a> .
Web Auth type	Setting that is displayed if you choose Web Policy and Override Global Config. Type of web authentication: <ul style="list-style-type: none"> <li>Internal</li> <li>Customized (Downloaded) <ul style="list-style-type: none"> <li>Login Page—Choose a login page from the drop-down list.</li> <li>Login Failure page—Choose a login page that displays to the client if web authentication fails.</li> <li>Logout page—Choose a login page that displays to the client when the user logs out of the system.</li> </ul> </li> <li>External (Redirect to external server) <ul style="list-style-type: none"> <li>URL—Enter the URL of the external server.</li> </ul> </li> </ul>
QR Code Scanning	Setting that is displayed if you choose Passthrough. If you choose this option, you are prompted to specify the Redirect URL and Shared Key.
Email Input	Setting that is displayed if you choose Passthrough. If you choose this option, you are prompted to specify your e-mail address when you try to connect to the network.

**Table 3-10** *Layer 3 Tab (for Guest LAN and Remote LAN) Parameters*

Parameter	Description	
Layer 3 Security	None	Indicates that no Layer 3 security is selected.
	Web authentication	Prompts you for your username and password while connecting the client to the network.
	Web Passthrough	Enables you to access the network directly without entering the username and password.
Preauthentication ACL	IPv4 or IPv6 ACLs to be used for traffic between the client and the Cisco WLC. See the <a href="#">Access Control Lists</a> topic for more information.	
Override Global Config	Check box that you enable to override the global authentication configuration set on the <a href="#">Web Login Page</a> .	

**Table 3-10** *Layer 3 Tab (for Guest LAN and Remote LAN) Parameters*

Parameter	Description
Web Auth type	<p>Setting that is displayed if you selected Override Global Config.</p> <p>Type of web authentication:</p> <ul style="list-style-type: none"> <li>• Internal</li> <li>• Customized (Downloaded) <ul style="list-style-type: none"> <li>– Login Page—Choose a login page from the drop-down list.</li> <li>– Login Failure page—Choose a login page that displays to the client if web authentication fails.</li> <li>– Logout page—Choose a login page that displays to the client when the user logs out of the system.</li> </ul> </li> <li>• External (Redirect to external server) <ul style="list-style-type: none"> <li>– URL—Enter the URL of the external server.</li> </ul> </li> </ul>
Email Input	<p>Setting that is displayed if you selected Web Passthrough.</p> <p>If you choose this option, you will be prompted for your e-mail address while connecting to the network.</p>

**Table 3-11** *Layer 3 VPN Passthrough Parameters*


Parameter	Description
VPN Gateway Address	VPN gateway IPsec passthrough address.

**Table 3-12** *AAA Servers Tab Parameters*

Parameter	Description
RADIUS Server Overwrite Interface	<p>RADIUS Server Overwrite Interface that you can enable or disable. The default is disabled.</p> <p>When you enable the RADIUS Server Overwrite Interface, the client authentication request is sent through the dynamic interface that is set on the WLAN. The Cisco WLC sources all RADIUS traffic to a WLAN using the dynamic interface configured on the WLAN.</p> <p><b>Note</b> You cannot enable the Radius Server Overwrite Interface when a diagnostic channel is enabled.</p>
RADIUS Server Client Interface	<p>RADIUS Server Client Interface that you can enable or disable on the WLAN. The default is disabled.</p> <p>When you enable the RADIUS Server Client Interface, the RADIUS server packets pass through the same VLAN as the data traffic of the client.</p>



Table 3-12 AAA Servers Tab Parameters

Parameter	Description
RADIUS Servers	<div> <b>Authentication Servers</b> </div> <p>RADIUS server (configured from the <a href="#">RADIUS Authentication Servers</a> page) that you choose from the drop-down lists.</p> <p>If this server is chosen, it will be the default RADIUS authentication server for the specified WLAN and overrides the RADIUS server that is configured for the network.</p> <p>You can choose up to three RADIUS servers, which are tried in priority order.</p>
	<div> <b>Accounting Servers</b> </div> <p>RADIUS accounting server that you can enable or disable. The default is Enabled.</p> <p>Choose a RADIUS server (configured from the <a href="#">RADIUS Accounting Servers</a> page) from the drop-down lists.</p> <p>If this server is chosen, it is the default RADIUS accounting server for the specified WLAN and overrides the RADIUS server that is configured for the network.</p> <p>You can choose up to six RADIUS servers, which are tried in priority order.</p>
Apply Cisco ISE Default Settings	You can enable or disable the Cisco ISE. Enabling Cisco ISE will reset the ISE values to default.
RADIUS Server Accounting	<p>If you select the Interim Update check box, the statistical usage information about the client is sent in the interim interval that you specify. By default, the statistical information is sent every 600 seconds (10 minutes).</p> <div>  <p><b>Note</b> The Interim Update check box can be selected only if you have the RADIUS accounting servers enabled.</p> </div>
LDAP Servers	<p>LDAP server (configured from the <a href="#">LDAP Servers</a> page) that you can choose from the drop-down list.</p> <p>You can choose up to three LDAP servers, which are tried in a priority order.</p>
Local EAP Authentication <sup>1</sup>	Local EAP authentication that you can enable or disable. The default is disabled.
EAP Profile Name <sup>1</sup>	EAP profile name (configured from the <a href="#">Local EAP Profiles</a> page).
Authentication priority order for web-auth user	<p>Order in which user credentials are retrieved from the back-end database servers.</p> <p>Highlight the desired database from the left box.</p> <p>Use the left and right arrows and the Up and Down buttons to move the desired database to the top of the right box.</p> <p>If you select the RADIUS NAC feature for authentication, the priority for web authentication must only contain RADIUS.</p>

1. This option is not available for guest LANs.

## QoS Tab




**Note** The Cisco OEAP 600 Series access point does not support CAC. Therefore, we recommend that you do not enable 7920 AP CAC and 7920 Client CAC parameters.

You can override the defined values in the QoS profile when you specify some or all of the rate-limiting parameters in the QoS tab.

**Table 3-13** *QoS Tab Parameters*

Parameter	Description
Quality of Service (QoS)	<p>Quality of Service Level, set on the <a href="#">Editing QoS Profile</a> page:</p> <ul style="list-style-type: none"> <li>Platinum (voice)—Assures a high Quality of Service for Voice over Wireless.</li> <li>Gold (video)—Supports the high-quality video applications.</li> <li>Silver (best effort)—Supports the normal bandwidth for clients.</li> <li>Bronze (background)— Supports the lowest bandwidth for guest services.</li> </ul> <p>VoIP clients should be set to Platinum, Gold, or Silver, while low-bandwidth clients can be set to Bronze.</p> <p><b>Note</b> Media Session Snooping is supported only for Platinum QoS profiles.</p>
Application Visibility	<p>Check box that you can select to view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology.</p> <p>To view all the supported applications, choose <b>WIRELESS &gt; Application Visibility and Control &gt; Applications</b>.</p> <p>To view all classified applications, choose <b>Monitor &gt; Applications</b> and click the WLAN ID to navigate to the Monitor &gt; Clients page.</p>
AVC Profile	<p>Drop-down list from which you can choose an Application Visibility and Control (AVC) profile for the WLAN. To configure a new AVC profile, choose <b>WIRELESS &gt; Application Visibility and Control &gt; Applications</b> and click <b>New</b>.</p> <p>You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or a Drop action for one application, which allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs. Only WLANs on local mode access points, or centrally switched on FlexConnect access points can have applications recognized by NBAR.</p>
NetFlow Monitor	<p>Drop-down list from which you can choose a NetFlow monitor for the WLAN. To configure a new NetFlow monitor, choose <b>WIRELESS &gt; Netflow &gt; Monitor</b> and click <b>New</b>.</p>

Table 3-13 QoS Tab Parameters

Parameter	Description
Fastlane	Drop-down list from which you can choose to enable or disable QoS Fastlane for the WLAN.   <b>Note</b> Fastlane must be disabled on the WLAN before disabling QoS Fastlane.
<b>Override Per-User Bandwidth Contracts</b>	
<b>Note</b>	When you set the Per-User Bandwidth Contracts parameters to 0 (OFF), the traffic allowed is unlimited and is restricted by only other 802.11 limitations. The values that you set override the values configured in the QoS profile page.
Average Data Rate	User-defined average data rate (kbps) for non-UDP traffic. The range is from 0 to 512,000; the default is 0 (OFF).
Burst Data Rate	User-defined peak data rate (kbps) for non-UDP traffic. Valid values are from 0 to 512,000; the default is 0 (OFF).
Average Real-Time Rate	User-defined average data rate (kbps) for UDP traffic. Valid values are from 0 to 512,000; the default is 0 (OFF).
Burst Real-Time Rate	User-defined peak data rate (kbps) for UDP traffic. Valid values are from 0 to 512,000; the default is 0 (OFF).
<b>Override Per-SSID Rate Limits</b>	
<b>Note</b>	The values that you set override the values configured in the QoS profile page.
<b>Override WLAN QoS Parameters</b>	
Average Data Rate	User-defined average data rate (kbps) for non-UDP traffic. The range is from 0 to 512,000; the default is 0 (OFF).
Burst Data Rate	User-defined peak data rate (kbps) for non-UDP traffic. The range is from 0 to 512,000; the default is 0 (OFF).
Average Real-Time Rate	User-defined average data rate (kbps) for UDP traffic. The range is from 0 to 512,000; the default is 0 (OFF).
Burst Real-Time Rate	User-defined peak data rate (kbps) for UDP traffic. The range is from 0 to 512,000; the default is 0 (OFF).
<b>WMM</b>	
WMM Policy <sup>1</sup>	WMM Policy. Choose one of the following: <ul style="list-style-type: none"> <li>Disabled—Disables this WMM policy.</li> <li>Allowed—Allows the clients to communicate with the WLAN.</li> <li>Required—Ensures that it is mandatory for the clients to have WMM features enabled on them to communicate with the WLAN.</li> </ul>

**Table 3-13** *QoS Tab Parameters*

Parameter	Description
7920 AP CAC <sup>1</sup>	Cisco 7920 AP CAC that you can enable or disable. Use this setting if you want the WLAN to support the newer version of the software on your Cisco 7920 phones. In newer versions, the CAC limit is advertised by the access points.
7920 Client CAC <sup>1</sup>	Cisco 7920 client CAC. Use this setting if you want the WLAN to support the older version of the software on your Cisco 7920 phones. In older versions, the CAC limit is set on the client.
<b>Media Stream</b>	
Multicast Direct	Check box to enable Multicast Direct on the WLAN.
<b>Lync Policy</b>	
<ul style="list-style-type: none"> <li>Audio</li> <li>Video</li> <li>Application-Sharing</li> <li>File-Transfer</li> </ul>	<p>The following QoS policies can be applied for each of the Lync policies:</p> <ul style="list-style-type: none"> <li>Bronze</li> <li>Silver</li> <li>Gold</li> <li>Platinum</li> </ul> <p><b>Note</b> WLAN QoS must meet or exceed Lync policy QoS settings in order for Lync priorities to achieve the configured levels.</p>

1. This option is not available for guest LANs and Remote LAN.

## Policy Mapping Tab

**Table 3-14** *Policy-Mapping Parameters*

Parameter	Description
Priority Index	Priority index of the policy configured on the WLAN. The policies are applied to the clients according to the priority index. The range is from 1 to 16.
Local Policy	Policy applied on the WLAN. To define new policies, choose <b>Security &gt; Local Policies &gt; New</b> .

## Advanced Tab



### Caution

Do not enable Coverage Hole Detection and Aironet IE for the Cisco OEAP 600 Series access point.

This table describes the advanced parameters.

Table 3-15 Advanced Tab Parameters

Parameter	Description
Allow AAA Override	<p>AAA Override for global WLAN parameters that you can enable or disable.</p> <p>When AAA Override is enabled, and a client has conflicting AAA and Cisco WLC WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution WLAN VLAN to a VLAN returned by the AAA server and predefined in the Cisco WLC interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system also uses QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, if they are predefined in the Cisco WLC interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.)</p> <p>If the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.</p> <p>When AAA Override is disabled, all client authentication defaults to the Cisco WLC authentication parameter settings, and authentication is only performed by the AAA server if the Cisco WLC WLAN does not contain any client-specific authentication parameters.</p> <p>The AAA Override values may come from a RADIUS server, for example.</p> <p><b>Note</b> AAA Override is not supported with FlexConnect.</p>
Coverage Hole Detection	<p>Coverage hole detection (CHD) on this WLAN that you can enable or disable.</p> <p>This option is not available for guest LANs and remote LANs.</p> <p>By default, CHD is enabled on all WLANs on the Cisco WLC. You can disable CHD on a WLAN.</p> <p>When you disable CHD on a WLAN, a coverage hole alert is still sent to the Cisco WLC, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.</p> <p><b>Note</b> For the Cisco OEAP 600 Series access point, do not enable Coverage Hole Detection.</p>
Enable Session Timeout	Session timeout that you can enable or disable. Maximum time in seconds for a client session before requiring reauthorization.
Aironet IE	<p>Support of Aironet IEs on a per WLAN basis that you can enable or disable. The default is disabled. This option is not available for guest LANs and remote LANs.</p> <p><b>Note</b> For the Cisco OEAP 600 Series access point, do not enable Aironet IE.</p>
Diagnostic Channel	Diagnostic channel support on the WLAN that you can enable or disable. The default is disabled. This option is not available for guest LANs and remote LANs.
Override Interface ACL	<p>Access Control List (ACL) that overrides the ACL configured for the interface on this WLAN. ACLs are configured on the <a href="#">Access Control Lists</a> page.</p> <ul style="list-style-type: none"> <li>IPv4 ACL—Lists the IPv4 ACL that needs to be applied on this WLAN. ACLs are configured on the <a href="#">Access Control Lists</a> page.</li> <li>IPv6 ACL—Lists the IPv6 ACL that needs to be applied on this WLAN. ACLs are configured on the <a href="#">Access Control Lists</a> page.</li> </ul>
Layer 2 ACL	List the layer 2 ACL that needs to be applied to the WLAN. ACLs are configured on the <a href="#">Access Control Lists</a> page.
URL ACL	List the URL ACL that needs to be applied to the WLAN. URL ACLs are configured on the <a href="#">Access Control Lists</a> .

Table 3-15 Advanced Tab Parameters

Parameter	Description
P2P Blocking Action	<p>Peer-to-peer blocking settings that you can choose.</p> <ul style="list-style-type: none"> <li>Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the Cisco WLC whenever possible.</li> </ul> <p><b>Note</b> Traffic is never bridged across VLANs in the Cisco WLC.</p> <ul style="list-style-type: none"> <li>Drop—Causes the Cisco WLC to discard the packets.</li> <li>Forward-UpStream—Causes the packets to be forwarded on the upstream VLAN. The device above the Cisco WLC decides what action to take regarding the packets.</li> </ul> <p>For FlexConnect local switching WLANs, the settings are as follows:</p> <ul style="list-style-type: none"> <li>Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the AP whenever possible.</li> <li>Drop—Causes the AP to discard the packets.</li> <li>Forward-UpStream—Causes the AP to discard the packets.</li> </ul>
Client Exclusion	<p>Timeout in seconds for disabled client machines that you can enable or disable. Client machines are disabled by their MAC address and their status can be observed on the <a href="#">Client Details</a> page. A timeout setting of 0 indicates that administrative control is required to re-enable the client. The default is enabled and the timeout setting configured as 60 seconds.</p>
Maximum Allowed Clients	<p>Maximum clients allowed per Cisco WLC.</p> <p>You can set a limit to the number of clients that can connect to a WLAN. This feature is useful in scenarios where you have a limited number of clients that can connect to a Cisco WLC. For example, consider a scenario where the Cisco WLC can server up to 256 clients on a WLAN that can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using. The range is from 1 to 200.</p> <p>The number of clients that you can configure for a specific platform is as follows:</p> <ul style="list-style-type: none"> <li>Cisco 5500 Series Controller—7000</li> <li>Cisco 7500 Series Controller—30000</li> <li>WiSM2—15000</li> </ul> <p><b>Note</b> The maximum number of clients per WLAN feature is supported only for access points that are in connected mode.</p> <p><b>Note</b> This feature is not supported when you use FlexConnect local authentication and is not applicable for remote and guest LANs.</p>
Static IP Tunneling	<p>Check box that you enable to configure static IP client tunneling support on a WLAN. The following restrictions apply when configuring Static IP tunneling in coordination with other features on the same WLAN:</p> <ul style="list-style-type: none"> <li>Auto anchoring mobility (guest tunneling) cannot be configured for the same WLAN.</li> <li>FlexConnect local authentication cannot be configured for the same WLAN.</li> <li>DHCP required option cannot be configured for the same WLAN.</li> </ul> <p><b>Note</b> Dynamic anchoring of static IP clients cannot be configured with FlexConnect local switching.</p>

Table 3-15 Advanced Tab Parameters

Parameter	Description
Wi-Fi Direct Clients Policy	<p>Drop-down list from which you can choose a Wi-Fi Direct Clients Policy for a WLAN.</p> <p>Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure WLANs concurrently. Use the Cisco WLC to configure the Wi-Fi Direct Clients Policy, on a per WLAN basis, where you can allow or disallow the association of Wi-Fi devices with infrastructure WLANs, or disable the Wi-Fi Direct Clients Policy for WLANs.</p> <p><b>Note</b> Wi-Fi Direct Clients Policy is applicable to WLANs that have APs in local mode only.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b>—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct clients</li> <li>• <b>Allow</b>—Allows Wi-Fi Direct clients to associate with the WLAN</li> <li>• <b>Not-Allow</b>—Disallows the Wi-Fi Direct clients from associating with the WLAN</li> <li>• <b>Xconnect-Not-Allow</b>—Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection</li> </ul>
Maximum Allowed Clients Per AP Radio	<p>Maximum number of clients that are allowed to connect to an AP.</p> <p>The maximum number you can configure is 200.</p>
Clear HotSpot Configuration	WLAN HotSpot configuration that you can clear.
Client User Idle Timeout	Timeout for idle client sessions for a WLAN. This value overrides the global timeout value. The range is from 15 to 100000 seconds. The default value is 300 seconds.
Client User Idle Threshold	Threshold data sent by the client during the idle timeout for the client session. If the client send traffic less than the defined threshold, the client is removed on timeout. The range is from 0 bytes to 10 MB. The default value is 0 bytes.
RADIUS NAI-Realm	Enable this to match any incoming EAP request from clients that contain realm with the realm configured on RADIUS authentication and accounting servers.
11ac MU-MIMO	<p>Check box that you can use to enable or disable 802.11ac MU-MIMO for Cisco Aironet 1850 Series APs.</p> <p><b>Note</b> MU-MIMO stands for Multiple User Multiple Input, Multiple Output.</p>
<b>Off Channel Scanning Defer</b>	
Scan Defer Priority	Assign a defer priority for the channel scan by clicking on the priority argument. The valid range for the priority is 0 to 7. The priority is 0 to 7 (this value should be set to 6 on the client and on the WLAN).
Scan Defer Time (msecs)	Assign the channel scan defer time in milliseconds. The valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN.
<b>FlexConnect</b>	

Table 3-15 Advanced Tab Parameters

Parameter	Description
FlexConnect Local Switching	<p>FlexConnect local switching that you can enable or disable. Any remote access point that advertises this WLAN, instead of tunneling to the Cisco WLC, can locally switch data packets.</p> <p><b>Note</b> In a network architecture where the WLAN is configured in FlexConnect local switching mode, if the client and Cisco WLC are in the same VLAN, a ping action will fail. Ping actions from the client to the Cisco WLC will work if both the client and Cisco WLC are on different VLANs.</p> <p><b>Note</b> The FlexConnect Local Switching text box must be enabled to enable local authentication.</p>
FlexConnect Local Auth	FlexConnect local authentication that you can enable or disable.
Learn Client IP Address	<p>Client IP address learning (this option is available when you enable FlexConnect Local Switching) that you can enable or disable.</p> <p><b>Note</b> If the client is configured with Fortress Layer 2 encryption, the Cisco WLC cannot learn the client IP address and will periodically drop the client. Disable this option so that the Cisco WLC maintains the client connection without waiting to learn the client IP address.</p>
VLAN based Central Switching	<p>VLAN central switching that you can enable or disable on the WLAN. You must enable FlexConnect local switching and an AAA override on the WLAN.</p> <p>When you enable VLAN central switching, the access point bridges the traffic locally if the AAA override VLAN for the client is configured on the local IEEE 802.1Q link. If the AAA override VLAN is not configured on the access point, the AP tunnels the traffic back to the Cisco WLC and the Cisco WLC bridges the traffic to the corresponding VLAN.</p> <p>VLAN central switching does not support:</p> <ul style="list-style-type: none"> <li>• FlexConnect Local Authentication</li> <li>• Layer 3 roaming of local switching client</li> </ul>
Central DHCP Processing	Check box to enable or disable the feature. When you enable this feature, the DHCP packets received from AP are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
Override DNS	Check box to enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.
NAT-PAT	Check box to enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.
Central Assoc	Check box to maintain the association table centrally on the controller. Disable this check box to maintain the association table locally on the AP.
<b>Lync</b>	
Lync Server	To enable or disable WLAN Lync SDN service.
<b>11k</b>	
Assisted Roaming Prediction Optimization	Check box to enable or disable assisted roaming prediction optimization for the WLAN.
Neighbor List	Check box to enable or disable 802.11k neighbor list for the WLAN.



Table 3-15 Advanced Tab Parameters

Parameter	Description
Neighbor List Dual Band	Check box to enable or disable a dual-band 802.11k neighbor list for the WLAN.
DHCP	
DHCP Server	When Override is selected, you can enter the IPv4 address of a DHCP server to be used by overriding the Primary/Secondary DHCP servers specified within the interface configuration. <b>Note</b> IPv6 is not supported for DHCP Server override.
DHCP Addr. Assignment (Required)	Requires all WLAN clients to obtain an IP address from the DHCP Server. <b>Note</b> DHCP address assignment (Required) is not supported for wired Guest LANs. <b>Note</b> DHCP Server override is applicable only for the default group.
OEAP	
Split Tunnel	Check box to enable split tunneling on OEAP access points.
Management Frame Protection (MFP)	
MFP Client Protection	Disabled, Optional, or Required.  The client MFP will only be active for a session if the client supports Cisco Compatible eXtensions (CCX) MFP, and if WPA2 is negotiated with the client. If Optional is selected, clients that do not negotiate MFP will be allowed to associate. If Required is selected, only clients that successfully negotiate MFP will be allowed to associate.  This option is not available for guest LANs and remote LANs. <b>Note</b> The Cisco OEAP 600 Series access point does not support MFP.  <b>Note</b> This check box represents the status of the Cisco MFP and not the status of 802.11w, introduced in Release 7.4
DTIM Period (in beacon intervals)	
802.11a/n (1 - 255)	Delivery Traffic Indication Map (DTIM) Period. Number of beacon intervals that elapse between the transmission of beacon frames that contain a TIM element whose DTIM Count field is 0. Valid values are from 1 to 255; the default value is 1. This option is not available for guest LANs and remote LANs.
802.11b/g/n (1 - 255)	
NAC	

Table 3-15 Advanced Tab Parameters

Parameter	Description
NAC State	<p>Enables SNMP NAC or ISE NAC.</p> <ul style="list-style-type: none"> <li>• SNMP—Enables SNMP NAC support for the WLAN.</li> <li>• ISE NAC—Enables RADIUS NAC support for the WLAN.</li> </ul> <p>Cisco Identity Services Engine (ISE) is a next-generation, context-based access control solution that provides the functions of Cisco secure Access Control System (ACS) and Cisco Network Admission Control (NAC) in one integrated platform.</p> <p>Cisco ISE can be used to provide advanced security for your deployed network. It is an authentication server that you can configure on your Cisco WLC. When a client associates to the Cisco WLC on a ISE NAC-enabled WLAN, the Cisco WLC forwards the request to the ISE server.</p> <p>The ISE server validates the user in the database and on successful authentication, the URL and pre-AUTH ACL is sent to the client. The client then moves to the “Posture Required” state and is redirected to the URL returned by the ISE server. The NAC agent in the client triggers the posture validation process. On a successful posture validation by the ISE server, the client is moved to the RUN state.</p> <p>This feature enables you to create a ISE NAC-enabled WLAN with open authentication and MAC filtering. If you are using local web authentication with ISE NAC, the Layer 3 web authentication must also be enabled. Both internal and external web authentication are supported.</p> <p>The following restrictions apply:</p> <ul style="list-style-type: none"> <li>• ISE NAC functionality with VLAN override is not available.</li> <li>• During slow roaming, the client goes through posture validation.</li> <li>• Guest tunneling mobility is supported for ISE NAC-enabled WLANs.</li> <li>• The VLAN select feature is not supported.</li> <li>• The NAC agent may also be available in a non-NAC-enabled WLAN.</li> <li>• The workgroup bridges are not supported.</li> <li>• The AP group over NAC feature is not supported over ISE NAC.</li> </ul> <p><b>Note</b> Do not swap AAA server indexes in a live network. This action might result in clients being disconnected and having to reconnect to the RADIUS server and log messages to be appended to the ISE server logs.</p> <p>When clients move from one WLAN to another, the Cisco WLC retains the client’s audit session ID if it returns to the WLAN before the idle timeout occurs. As a result, when clients join back to the Cisco WLC before the idle timeout session expires, they are immediately moved to the RUN state. The clients are validated if they reassociate with the Cisco WLC after the session timeout.</p> <p>Suppose you have two WLANs, where WLAN 1 is configured on a Cisco WLC (WLC1) and WLAN2 configured on another Cisco WLC (WLC2) and both are ISE NAC-enabled. The client first connects to WLC1 and moves to the RUN state after posture validation. Assume that the client now moved to WLC2. If the client connects back to WLC1 before the PMK expires for this client in WLC1, the posture validation is skipped for the client. The client directly moves to the RUN state bypassing posture validation as the Cisco WLC retains the old audit session ID for the client that is already known to ISE.</p>

Table 3-15 Advanced Tab Parameters

Parameter	Description
	<p>When deploying RADIUS NAC in your wireless network, do not configure a primary and secondary ISE server. Instead, we recommend that you configure HA between the two ISE servers. Having a primary and secondary ISE setup will require a posture validation to happen before the clients move to the RUN state. If HA is configured, the client is automatically moved to the RUN state in the fallback ISE server.</p> <p>Cisco WLC software configured with RADIUS NAC does not support change of authorization (CoA) on the service port.</p>
<b>Load Balancing and Band Select</b>	
<b>Note</b> Client Load Balancing and Client Band Select is not available for the Cisco OEAP 600.	
Client Load Balancing	Client load balancing that you can enable or disable.
Client Band Select	<p>Client radio band that you can enable or disable.</p> <p><b>Note</b> Band Select is configurable only when the radio policy is set to <b>All</b> in the General Tab.</p>
<b>Passive Client</b>	
Passive Client	<p>Passive clients that you can enable or disable on your WLAN.</p> <p>Passive clients are wireless devices such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the Cisco WLC will never know the IP address unless they use DHCP.</p> <p>Cisco WLC currently act as a proxy for ARP requests. On receiving an ARP request, the Cisco WLC responds with an ARP response instead of passing the request directly to the client. This has two advantages:</p> <ul style="list-style-type: none"> <li>• The upstream device that sends out the ARP request to the client cannot know where the client is located.</li> <li>• Power for battery-operated devices such as mobile phones and printers is preserved because they do not need to respond to every ARP request.</li> </ul> <p>Since the wireless Cisco WLC does not have any IP-related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Any application that tries to access a passive client results in a failure.</p> <p>This feature enables ARP requests and responses to be exchanged between wired and wireless clients.</p> <p>This feature when enabled allows the Cisco WLC to pass ARP requests from wired to wireless clients until the desired wireless client gets to RUN state.</p> <p><b>Note</b> This feature is supported only on the Cisco 5500 Series Controllers.</p> <p><b>Note</b> Passive clients are not supported with AP groups and FlexConnect centrally switched WLANs.</p> <p>This feature works on the multicast-multicast mode of multicast operation.</p>
<b>Voice</b>	
Media Session Snooping	<p>Access points that you can enable or disable to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the Cisco WLC and PI.</p> <p>See the <a href="#">Radio Statistics</a> page to see the VoIP statistics for your access point radios.</p> <p>See the <a href="#">SNMP Trap Logs</a> page to see the traps generated for failed calls.</p>

Table 3-15 Advanced Tab Parameters

Parameter	Description
Re-anchor Roamed Voice Clients	<p>Reanchoring of roamed voice clients that you can enable or disable.</p> <p>This feature allows the voice client to get anchored on the best suited and nearest available Cisco WLC. In the case of inter Cisco WLC roaming, it avoids the use of tunnels to carry traffic between the foreign Cisco WLC and the anchor Cisco WLC, which removes unnecessary traffic from the network.</p> <p>The ongoing call during roaming is not affected and it continues without any problem. The traffic passes through proper tunnels that are established between the foreign Cisco WLC and the anchor Cisco WLC. When the call ends, disassociation occurs and the client gets reassociated to a new Cisco WLC. By default, this feature is disabled.</p> <p><b>Note</b> The ongoing data session may be affected due to disassociation and reassociation.</p> <p><b>Note</b> This feature is supported for TSPEC-based calls and non-TSPEC-SIP based calls only when admission control is enabled.</p> <p><b>Note</b> You can reanchor roaming of voice clients for each WLAN.</p> <p><b>Note</b> This feature is not recommended for use on the Cisco 792x phone.</p>
KTS based CAC Policy	<p>To enable or disable CAC that is based on Key Telephone System (KTS) for the WLAN.</p> <p>KTS-based CAC is a protocol that is used in NEC MH240 wireless IP telephones. You can configure the Cisco WLC to support CAC on KTS-based SIP clients, to process bandwidth request message from such clients, to allocate required bandwidth on the AP radio, and to handle other messages that are part of the protocol.</p> <p>When a call is initiated, the KTS-based CAC client sends a Bandwidth Request message to which the Cisco WLC responds with a Bandwidth Confirm message indicating whether the bandwidth is allocated or not. The call is allowed only if the bandwidth is available. If the client roams from one AP to another, then the client sends another Bandwidth Request message to the Cisco WLC.</p> <p>Bandwidth allocation depends on the medium time calculated using the data rate from the Bandwidth Request message and the packetization interval. For KTS-based CAC clients, G.711 codec with 20 milliseconds as packetization interval is used for computing the medium time.</p> <p>The Cisco WLC releases the bandwidth after it receives the bandwidth release message from the clients. When the client roams to another AP, the Cisco WLC takes care of releasing the bandwidth on the previous AP and allocates bandwidth on the new AP, in both intra Cisco WLC and inter Cisco WLC roaming scenarios. The bandwidth is released if the client is dissociated or if there is inactivity for 120 seconds. The Cisco WLC does not inform the client when the bandwidth is released for the client due to inactivity or dissociation of the client.</p> <p>Limitations:</p> <ul style="list-style-type: none"> <li>• KTS-based CAC is not supported on FlexConnect access points with the WLAN in the local switching mode.</li> <li>• The Cisco WLC ignores the SSID capability check request message from the clients.</li> <li>• Preferred call is not supported for KTS CAC clients.</li> <li>• Reason code 17 is not supported in inter Cisco WLC roaming scenarios.</li> <li>• This feature is applicable only when the QoS profile is set to Platinum for the WLAN.</li> </ul>

Table 3-15 Advanced Tab Parameters

Parameter	Description
<b>RADIUS Client Profiling</b>	
DHCP Profiling	Check box to enable or disable DHCP profiling of all the clients that are associated with the WLAN. When you enable DHCP profiling, the Cisco WLC collects the DHCP attributes of clients for profiling.
HTTP Profiling	Check box to enable or disable HTTP profiling of all the clients that are associated with the WLAN. When you enable HTTP profiling, the Cisco WLC collects the HTTP attributes of clients for profiling.
<b>PMIP</b>	
PMIP Mobility Type	Choose the type of PMIP mobility for the WLAN. The following options are available: <ul style="list-style-type: none"> <li>None—Configures the WLAN with Simple IP.</li> <li>PMIPv6—Configures the WLAN with only PMIPv6.</li> </ul>
PMIP NAI Type	Drop-down list from which you can choose the PMIP NAI Type as Hexadecimal or Decimal.
PMIP Profile	Drop-down list from which you can choose a PMIP profile. You can configure the PMIP profile irrespective of the mobility type.
PMIP Realm	Default realm of the PMIPv6 WLAN.
<b>Universal AP Admin Support</b>	
Universal AP Admin	Check box to enable or disable Universal AP Admin support. For more information, see <a href="#">Universal AP Regulatory Domain Deployment Guide</a> .
<b>11v BSS Transition Support</b>	
BSS Transition	Check box to enable or disable Basic Service Set (BSS) transition on the WLAN.
Dissassociation Imminent	Check box to enable or disable dissassociation imminent.
Dissassociation Timer	Text box to enter the Target Beacon Transmission Time (TBTT).
Optimized Roaming Dissassociation Timer	Text box to enter TBTT value.
BSS Max Idle Service	Check box to enable or disable BSS max idle service.
Directed Multicast Service	Check box to enable or disable Directed Multicast Service.
<b>Tunneling</b>	
Tunnel Profile	Choose the EoGRE tunnel profile that you have created.
<b>mDNS</b>	
mDNS Snooping	Check box to enable or disable mDNS snooping on the WLAN. To check if global mDNS snooping is enabled, choose <b>CONTROLLER &gt; mDNS &gt; General</b> . mDNS snooping works on guest LANs and not on remote LANs.
mDNS Profile	Drop-down list from which you can choose the mDNS profile for the WLAN. Clients receive service advertisements only for the services associated with the profile.

Table 3-15 Advanced Tab Parameters

Parameter	Description
<b>TrustSec</b>	
Security Group Tag	Text box to enter Security Group Tag value.
<b>OpenDNS</b>	
OpenDNS Mode	Drop-down list from which you can choose the OpenDNS mode for the WLAN.
OpenDNS Profile	Drop-down list from which you can choose the OpenDNS profile for the WLAN.
<b>Fabric Configuration</b>	
Fabric	Checkbox to enable or disable the fabric configuration.
Fabric Interface Name	Drop-down list from which you can choose the fabric interface.
L2 instance ID	Text box to enter the Layer 2 instance ID.
Peer IP	Text box to enter peer IP address.
Fabric ACL	Drop-down list from which you can choose the fabric ACL name.
Fabric AVC	Drop- list from which you can choose the fabric AVC name.
<b>Mobility</b>	
AVC Based Reanchor	Check box that you can use to enable or disable AVC-based reanchoring.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

## Activating URL Filtering ACL (WLAN)

- 
- Step 1** Click the **WLANs** tab. This displays the list of WLANs.
  - Step 2** Click the WLAN ID you want to activate URL ACL on.
  - Step 3** Click **Advanced** tab, select the URL ACL from the drop-down list.
  - Step 4** Click **Apply**.
- 

## Mapping Policy to WLAN

- 
- Step 1** Click the **WLANs** tab. This displays the list of WLANs.
  - Step 2** Click the WLAN ID you want to map.
  - Step 3** Click **Policy-Mapping** tab. enter the **Priority Index** value, choose the **Local Policy** from the drop-down list.

**Step 4** Click **Add**.

---

## Mapping Policy to an AP Group

---

- Step 1** Click the **WLANs** tab.
- Step 2** Click **Advanced > AP Groups**.
- Step 3** Choose the AP Group.
- Step 4** Click the **WLANs** tab. Hover the mouse cursor over the blue drop-down arrow of the required WLAN, select **Policy-Mapping**.
- Step 5** Enter the **Priority Index** value.
- Step 6** Choose the **Local Policy** from the drop-down list.
- Step 7** Click **Apply**.
- 

## Deleting WLANs

Click the **WLANs** tab. This displays the list of WLANs. Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Remove** to delete the WLAN, Remote LAN, or Guest LAN. When you delete the WLAN, it will be removed from the AP group too.

## Mobility Anchors

Click the **WLANs** tab. This displays the list of WLANs. Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Mobility Anchors** to navigate to the Mobility Anchors page.

This page lists the Cisco WLCs that have already been configured as mobility anchors and shows the current state of their data and control paths. Cisco WLCs within a mobility group communicate among themselves over a well-known UDP port and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. Cisco WLCs send mpings and epings. Mpings test the mobility control packet reachability over the management interface over mobility UDP port 16666 and epings test the mobility data traffic over the management interface over EoIP port 97. The Control Path field shows whether mpings have passed (up) or failed (down), and the Data Path field shows whether epings have passed (up) or failed (down). If the Data Path field shows “down,” the mobility anchor cannot be reached and is considered failed.

Mobility anchors can also be used to provide geographic load balancing, because WLANs can be used to represent a particular section of the building such as engineering, marketing, and so on.

Table 3-16 Mobility Anchor Parameters

Parameter	Description
WLAN SSID	WLAN SSID.
Switch IP Address (Anchor)	IP address of the Cisco WLC that is designated as a mobility anchor.  Choose <b>local</b> from the drop-down list for the anchor Cisco WLC and all Cisco WLCs that are auto-anchors for this WLAN.  For foreign Cisco WLCs, select the anchor Cisco WLC from the drop-down list. Only Cisco WLCs configured as a mobility group members are available in the drop-down list.
Data Path	Whether epings have passed (up) or failed (down). If the Data Path field shows down, the mobility anchor cannot be reached and is considered failed.
Control Path	Whether mpings have passed (up) or failed (down).
Mobility Anchor Create	Mobility anchor that you can create. The selected Cisco WLC becomes an anchor for the WLAN.
Switch IP Address (Anchor)	Cisco WLC IP address from the drop-down list. You can select from either local, IPv4 address or an IPv6 address.

## Creating a Mobility Anchor

- 
- Step 1** Click the **WLANs** tab. This displays the list of WLANs.
- Step 2** Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Mobility Anchors** to navigate to the Mobility Anchors page.
- Step 3** Choose a Cisco WLC IP address from the Switch IP Address (Anchor) drop-down list. From Release 8.0, the controller supports both IPv4 and IPv6.
- Step 4** Click **Mobility Anchor Create**.
- The selected Cisco WLC now becomes an anchor for the WLAN.
- 

## Removing a Mobility Anchor

- 
- Step 1** Click the **WLANs** tab. This displays the list of WLANs.
- Step 2** Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Mobility Anchors** to navigate to the Mobility Anchors page.
- Step 3** Click the blue arrow adjacent the corresponding Mobility Anchor and choose **Remove**.
-



# 802.11u

Click the **WLANs** tab. This displays the list of WLANs. Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **802.11u** to navigate to the 802.11u page.

This page lists the 802.11u configuration options available for the selected WLAN. You can configure a WLAN to enable interworking with external networks such as hotspots or other public Wi-Fi.

IEEE 802.11u is an extension to the IEEE 802.11 standard to improve the ability of devices to discover, authenticate, and use nearby Wi-Fi access points. IEEE 802.11u enables automatic WLAN offload for 802.1X devices at the hotspot of mobile or roaming partners.

**Table 3-17**      *801.11u General Parameters*

Parameter	Description
802.11u Status	802.11u that you can enable or disable on this WLAN.
Internet Access	Check box that you check or uncheck to enable or disable Internet access on this WLAN.
Network Type	<p>Network type that you can set on this WLAN. The following options are available:</p> <ul style="list-style-type: none"> <li>• Private Network</li> <li>• Private Network with Guest Access</li> <li>• Chargeable Public Network</li> <li>• Free Public Network</li> <li>• Emergency Services Only Network</li> <li>• Personal Device Network</li> <li>• Test or Experimental</li> <li>• Wildcard</li> </ul> <p>The default value is Chargeable Public Network.</p>
Network Auth Type	<p>Network authentication type that you can set on this WLAN for 802.11u. The following options are available:</p> <ul style="list-style-type: none"> <li>• Not configured</li> <li>• Acceptance of terms and conditions</li> <li>• Online enrollment</li> <li>• HTTP/HTTPS redirection</li> <li>• DNS Redirection</li> </ul>
HESSID	Homogenous Extended Service Set Identifier (HESSID) that you can enter. The HESSID must be a valid MAC address that uniquely identifies the network. We recommend that the HESSID must be the actual BSSID of the first access point.

**Table 3-17** 801.11u General Parameters

Parameter	Description
IPv4Type	IPv4 type address. The following options are available: <ul style="list-style-type: none"> <li>Unknown</li> <li>Not available</li> <li>Public address</li> <li>Port-restricted</li> <li>Single NATed private</li> <li>Double NATed private</li> <li>Port-restricted and single NATed</li> <li>Port-restricted and double NATed</li> </ul>
IPv6Type	IPv6type address. The following options are available: <ul style="list-style-type: none"> <li>Unknown</li> <li>Not available</li> <li>Available</li> </ul> <p>The default value is Unknown.</p>

**Table 3-18** OUI List Parameters

Parameter	Description
OUI	Organization Unique Identifier that you can enter. The OUI must be a hexadecimal number represented in six or ten characters. For example, AABBDFF.
Is Beacon	OUI beacon responses that you can enable or disable. You can have a maximum of 3 OUIs with this field enabled.
OUI Index	Organization Unique Identifier index. Choose a value between 1 and 32 from the drop-down list. The default is 1.

Click **Add** to add the OUI details.

This table describes the domain list parameters.

**Table 3-19** Domain List Parameters

Parameter	Description
Domain Name	Domain name that is operating in the WLAN network. The domain name is case sensitive and you can use alphanumeric characters.
Domain Index	Domain index of the domain name. Choose a value between 1 and 32 from the drop-down list. The default is 1.

Click **Add** to add the Domain List parameters.

**Table 3-20** *Realm List Parameters*

Parameter	Description
Realm	Realm name that you can assign for this WLAN.
Realm Index	Realm index that you can assign to this realm name. Choose a value between 1 and 32 from the drop-down list. The default is 1.
EAP List	Field that appears when you click on a realm name. It allows you to define the EAP method and EAP index for the realm.
EAP Method	EAP method for the realm in the WLAN. The following options are available: <ul style="list-style-type: none"> <li>• LEAP</li> <li>• PEAP</li> <li>• EAP-PEAP</li> <li>• EAP-TLS</li> <li>• EAP-FAST</li> <li>• EAP-SIM</li> <li>• EAP-TTLS</li> <li>• EAP-AKA</li> </ul>
EAP Index	EAP index. The range is 1 to 4.

Click **Add** to add a realm.

**Table 3-21** *Cellular Network Information List*

Parameter	Description
Country Code	Mobile country code in Binary Coded Decimal (BCD) format. The country code should be 3 characters.
Cellular Index	Cellular Index. The range is from 1 to 32.
Network Code	Mobile network code in BCD format. The network code can be 2 or 3 characters.

Click **Add** to add the Cellular Network Information.

**Table 3-22** *Online Signup Details*

Parameter	Description
Service Provider Name	Name of the service provider
OSU Index	Online signup index
Language Code	User-defined language code; for example, ENG for English.
Description	Description of the service provider
URI	Uniform resource identifier

Table 3-22 Online Signup Details

Parameter	Description
NAI	Network access identifier
Icon Filename	Filename of the icon

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

## HotSpot 2.0

Click the **WLANs** tab. This displays the list of WLANs. Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Hotspot 2.0** to navigate to the HotSpot 2.0 page.

Hotspot 2.0 improves the ability of Wi-Fi devices to discover and securely connect to public Wi-Fi hotspots which enables easier roaming between public Wi-Fi networks.

You can enable or disable a hotspot by choosing the appropriate option from the **HotSpot2 Enable** drop-down list.

Table 3-23 HotSpot 2.0 General Parameters

Parameter	Description
HotSpot2	HotSpot2 that you can enable or disable on this WLAN.
Domain ID	Domain Identifier
OSU SSID	Online Signup SSID
WAN Link Status	Link status. The following options are available: <ul style="list-style-type: none"> <li>• Not configured</li> <li>• Link Up</li> <li>• Link Down</li> <li>• Link in Test</li> </ul>
WAN Symmetric Link Status	Downlink and uplink speed of the WAN backhaul link. The following options are available: <ul style="list-style-type: none"> <li>• Same</li> <li>• Different</li> </ul>
WAN Downlink Speed	Downlink speed of the WAN backhaul link in Kbps. The maximum value is 4,294,967,295 Kbps.
WAN Uplink Speed	Uplink speed of the WAN backhaul link in Kbps. The maximum value is 4,294,967,295 Kbps.

**Table 3-24**      *Online Signup List Parameters*

Parameter	Description
OSU Index	Online signup index
Lang Code	Language code
SP Name	Name of the service provider
Description	Description of the service provider

**Table 3-25**      *Operator Name List Parameters*

Parameter	Description
Operator Name	Operator name of the hotspot provider that you can enter.
Operator Index	Operator index of the hotspot provider that you can assign. Choose a value between 1 and 32 from the drop-down list. The default is 1.
Language code	Language code that you can enter. For example, you can enter ENG for English.

Click **Add** to add the operator name.

**Table 3-26**      *Port Config List Parameters*

Parameter	Description
IP Protocol	Internet protocol name that you can select. This parameter provides information on the connection status of the most commonly used communication protocols and ports.  The following options are available: <ul style="list-style-type: none"> <li>• ICMP</li> <li>• FTP/SSH/TLS/PPTP VPN/VOIP</li> <li>• IKEv2 (IPSec VPN/VoIP/ESP)</li> </ul>
Port No.	Port number used for the IP. The following options are available: <ul style="list-style-type: none"> <li>• ICMP/ESP (IPSec-VPN)</li> <li>• FTP</li> <li>• SSH</li> <li>• HTTP</li> <li>• TLS-VPN</li> <li>• IKEv2</li> <li>• PPTP-VPN</li> <li>• IPSec-NAT</li> <li>• VoIP</li> </ul>

**Table 3-26** *Port Config List Parameters*

Parameter	Description
Status	Status of the IP port. The following options are available: <ul style="list-style-type: none"><li>• Closed</li><li>• Open</li><li>• Unknown</li></ul>
Index	Port configuration index that you can configure. Choose a value between 1 and 10 from the drop-down list. The default is 1.

## Foreign Maps

Click the **WLANs** tab. This displays the list of WLANs.

Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Foreign Maps** to navigate to the Foreign Controller Interface Mapping page.

Whenever a wireless client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. Release 7.0 and prior releases of the Cisco WLC software enabled you to associate one VLAN with a WLAN. Each VLAN required a single IP subnet. As a result, a WLAN required a large subnet to accommodate more clients. In a large venue such as an auditorium, a stadium, or a conference where there may be numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN select feature enables you to use a single WLAN that can support multiple VLANs. Clients can get assigned to one of the configured VLANs. This feature enables you to map a WLAN to a single or multiple interfaces using interface groups. Wireless clients that associate to the WLAN get an IP address from a pool of subnets identified by the interfaces using a MAC based hashing algorithm. This feature also extends the current AP Group where AP groups can override an interface or interface group in a WLAN by an interface. This feature also provides the solution to guest anchor restrictions where a wireless guest user on a foreign location can get an IP address from multiple subnets based on their foreign locations or foreign Cisco WLCs from the same anchor Cisco WLC.

When a client roams from one Cisco WLC to another, the foreign Cisco WLC sends the VLAN information as part of the mobility announce message. Based on the VLAN information received, the anchor decides whether the tunnel should be created between the anchor Cisco WLC and the foreign Cisco WLC. If the same VLAN is available on the foreign Cisco WLC, the client context is completely deleted from the anchor and the foreign Cisco WLC becomes the new anchor Cisco WLC for the client.

As part of VLAN select feature, the mobility announce message carries an additional vendor payload that contains the list of VLAN interfaces that are mapped to a WLAN. This list helps the anchor to decide on a Local->Local type of handoff.

**Note**

VLAN Select applies to wireless clients only.

Table 3-27 Foreign Map Parameters

Parameter	Description
WLAN SSID	WLAN SSID.
Foreign Controller MAC Address	Foreign Cisco WLC MAC address on a WLAN.
Interface/Interface Group Name (G)	Interface/interface group name that is mapped to a foreign switch.
Add Mapping	Mobility foreign map that you can add to a WLAN.
Foreign Controller MAC Address	Information about the MAC address of the foreign Cisco WLC to this interface/interface group.
Interface/Interface Group (G)	Interface/interface group.

## Creating a Foreign Cisco WLC Interface Mapping

- 
- Step 1** Click the **WLANs** tab. This displays the list of WLANs.
  - Step 2** Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Foreign Maps** to navigate to the Foreign Controller Interface Mapping page.
  - Step 3** From the Foreign Controller MAC Address drop-down list, choose a foreign Cisco WLC MAC address.
  - Step 4** From the Interface/Interface Group Name drop-down list, choose the interface/interface group name to be mapped to a foreign switch.
  - Step 5** Click **Add Mapping**.
- 

## Removing Foreign Maps

- 
- Step 1** Click the **WLANs** tab. This displays the list of WLANs.
  - Step 2** Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Foreign Maps** to navigate to the Foreign Controller Interface Mapping page.
  - Step 3** Click the blue arrow adjacent the corresponding Foreign Controller and click **Remove**.
- 

## Service Advertisement

Click the **WLANs** tab. This displays the list of WLANs.

Click the blue arrow adjacent the corresponding WLAN, and from the drop-down list that is displayed, choose **Service Advertisement** to navigate to the Service Advertisement page.

This page allows you to configure the Mobility Service Advertisement Protocol (MSAP) parameters on a WLAN. MSAP is used primarily by mobile devices that are configured with a set of policies for establishing network services. Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement.

Table 3-28 MSAP Parameters

Parameter	Description
MSAP Enable	Service advertisements that you can enable or disable on the WLAN.
Server Index	MSAP server ID. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID. The range is from 1 to 10.

## Configuring Dynamic Anchoring for Clients with a Static IP Address

You might need to configure static IP addresses for wireless clients. When these wireless clients move in a network, they try to associate with other Cisco WLCs. If the clients try to associate with a Cisco WLC that does not support the same subnet as the static IP, the clients fail to connect to the network. You can now enable dynamic tunneling of clients with static IP addresses. Using this feature, clients with static IP addresses can be associated with other Cisco WLCs where the client's subnet is supported by tunneling the traffic to another Cisco WLC in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.

The following sequence occurs when a client with a static IP address tries to associate with a Cisco WLC:

1. When a client associates with a Cisco WLC, such as WLC-1, it performs a mobility announcement. If a Cisco WLC in the mobility group responds (such as WLC-2), the client traffic is tunneled to the Cisco WLC WLC-2. As a result, WLC 1 becomes foreign and WLC-2 becomes the anchor.
2. If none of the Cisco WLCs responds, the client is treated as a local client and authentication is performed. The IP address for the client is updated either through orphan packet handling or ARP request processing. If the client's IP subnet is supported in the Cisco WLC (WLC-1), the client remains as a local client and traffic for this client is serviced by this Cisco WLC (WLC-1).
3. If the Cisco WLC (WLC-1) cannot service the client IP subnet, it sends a static IP client announcement. If a Cisco WLC in the mobility group responds (such as WLC2), the client is tunneled to WLC2. If there are multiple Cisco WLCs in the mobility group that respond to the static IP client announcement, the first Cisco WLC with a 50 percent or less load is selected for tunneling. If there are no Cisco WLCs with a 50 percent or less load, the Cisco WLC with the least load is selected.
4. If the maximum number of clients per WLAN is configured, the percentage load is calculated by using the following formula:
  - (total clients present in that WLAN/maximum clients supported in that WLAN) x 100.
  - or
  - (total clients present in the WLC/maximum clients supported) x 100.
5. Once the acknowledgement is received, the client traffic is tunneled between the anchor and the Cisco WLC (WLC-1).



### Note

If a WLAN is configured with an interface group and any of the interfaces in the interface group support the static IP client subnet, the client is assigned to that interface. This situation occurs in the local or remote (static IP anchor) Cisco WLC. For native IPv6 clients, that is clients with only IPv6 addresses, in the interface group, static IP is not supported.



**Note**

A security level 2 authentication is performed only in the local (static IP foreign) Cisco WLC, also known as the exported foreign Cisco WLC.

**Note**

If AAA is used for authentication, the VLAN override is ignored if static IP tunneling is required. You must configure the local Cisco WLC with the correct AAA server where this client entry is present.

The following restrictions apply when configuring static IP tunneling with other features on the same WLAN:

- Auto anchoring mobility (guest tunneling) cannot be configured for the same WLAN.
- FlexConnect local authentication cannot be configured for the same WLAN.
- The DHCP required option cannot be configured for the same WLAN.

**Note**

Dynamic anchoring of static IP clients cannot be configured with FlexConnect local switching.

## Configuring Dynamic Anchoring of Static IP Clients

- 
- Step 1** Choose **WLANs** to open the WLANs page.
- Step 2** Click the ID number of the desired WLAN on which you want to enable dynamic anchoring of IP clients. The WLANs > Edit page appears.
- Step 3** Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.
- Step 4** Enable dynamic anchoring of static IP clients by selecting the **Static IP Tunneling** check box.
- Step 5** Click **Apply** to commit your changes.
- 

## Configuring the Maximum Number of Clients Per WLAN

You can set a limit to the number of clients that can connect to a WLAN. This feature is useful in scenarios where you have a limited number of clients that can connect to a Cisco WLC. For example, consider a scenario where the Cisco WLC can server up to 256 clients on a WLAN that can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using. The range is from 1 to 200.

- 
- Step 1** Choose **WLANs** to open the WLANs page.
- Step 2** Click the ID number of the WLAN for which you wish to limit the number of clients. The WLANs > Edit page appears.
- Step 3** On the Advanced tab, set the Maximum Allowed Clients text box.
-

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

## AP Groups

Choose **WLAN > Advanced > AP Groups** to navigate to the AP Groups page. This page displays a summary of the AP groups configured on your network. This page enables you to add, remove, or view details of an AP group.

After you create up to 512 WLANs on the Cisco WLC, you can selectively publish them (using access point groups) to different access points to better manage your wireless network.

After all access points have joined the Cisco WLC, you can create up to 150 access point groups and assign up to 16 WLANs to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group.



### Note

The Cisco WLC creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it and you cannot delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the Cisco WLC with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.



### Note

If you clear the configuration on the Cisco WLC, all of the access point groups disappear except for the default-group access point group.



### Note

The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP group if the 600 Series OEAP is in the default group. The WLAN/remote LAN IDs must be less than 8.

To remove an AP group, click the blue arrow adjacent the group and choose **Remove**.

An error message appears if you try to delete an access point group that is used by at least one access point. Before you can delete an AP group, move all APs in this group to another group. The access points are not moved to the default-group access point group as in previous releases.

- To see the APs, click the AP group name, and choose the **APs** tab.
- To move APs, click the AP group name, choose the **APs** tab, check the check box to the left of the AP name, or select the AP name check box to select all APs, and click the **Add APs**.

## Prohibit One VLAN for Local Switching by FlexConnect

Choose an interface for Prohibit Local Switching from the drop-down list in the interface list page. Click **Apply** to prohibit local switching of the interface by the Cisco WLC. Click **New** to select another VLAN for the same action.

## Creating a New AP Group

- 
- Step 1** On the WLAN > AP Groups page, click **Add Group** to display the Add New AP Group area.
- Step 2** In the AP Group Name text box, enter the name of the AP group.
- Step 3** In the Description text box, enter a brief description of the AP group.
- Step 4** Click **Add** to add the AP group.
- The AP group is created.
- 

## Editing AP Groups

Choose **WLAN > Advanced > AP Groups** and then click an AP group name to navigate to this page.

### General Tab



**Note**

AP 3600 with the 802.11ac module advertises only the first eight WLANs on the 5-GHz radios.

**Table 3-29** General Parameters

Parameter	Description
AP Group Name	AP group name.
AP Group Description	AP group description.
NAS-ID	Network Access Server identifier. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters.  Beginning in Release 7.4 and later releases, you can configure the NAS-ID on the interface, WLAN, or an access point group. The order of priority is AP Group NAS-ID > WLAN NAS-ID > Interface NAS-ID.
Enable Client Traffic QinQ	When enabled, double 802.1q tagging is enabled for client traffic associated to APs that are part of the WLAN and AP-Group.  QinQ Service VLAN ID must be configured for this to work.
Enable DHCPv4 QinQ	When enabled, double 802.1q tagging is enabled for client DHCPv4 packets associated to APs that are part of the WLAN and AP-Group.  QinQ Service VLAN ID must be configured for this to work.

Table 3-29 General Parameters

Parameter	Description
QinQ Service VLAN ID	QinQ Service VLAN ID is the outer VLAN ID and the Interface mapped to WLAN in AP-Group will act as inner VLAN ID.
CAPWAP Preferred Mode	<p>Select the check box to configure the CAPWAP Preferred mode for the AP Group. You can select between an IPv4 or IPv6. By field is by default un-configured.</p> <p><b>Note</b> The CAPWAP Preferred Mode can either be configured Globally (Controller &gt; General Tab &gt; CAPWAP Preferred Mode) or on a AP Group. If you unselect the check box, global configuration will take precedence.</p> <p><b>Note</b> The above configuration will be displayed in the Wireless &gt; ALL APs &gt; General Tab &gt; IP Config.</p> <p><b>Note</b> The CAPWAP Preferred Mode field does not appear under the <b>default-group</b>. The APs by default are part of the default-group.</p>

**WLANs Tab**

Click **Add New** to assign a WLAN to an access point group.

Table 3-30 WLANs Tab Parameters

Parameter	Description
WLAN SSID	WLAN SSID that you can select from the drop-down list.
Interface/Interface Group (G)	Interface name that you can select from the drop-down list.
SNMP NAC State	<p>SNMP NAC out-of-band support for this access point group that you can enable or disable.</p> <p><b>Note</b> If you enable SNMP NAC out-of-band support, be sure to choose the quarantine VLAN from the <b>Interface Name</b> drop-down list.</p>
Add button/Cancel button	Click <b>Add</b> to add this WLAN to the access point group. Click <b>Cancel</b> to close the Add New area without making any changes.
WLAN ID	Information about the WLANs that are currently assigned to this access point group.
WLAN SSID	Information about the WLAN SSID.
Interface Name/Interface Group (G)	Interface name or interface group that you can select from the drop-down list.
SNMP NAC State	SNMP NAC state that you can enable or disable.

Click the blue arrow adjacent the corresponding WLAN and choose one of the following options:

- **NAC Enable/NAC Disable**—Changes the SNMP NAC state.
- **Policy-Mapping**—Configures the policies for the WLAN.

You can configure a maximum of 16 policies. In the **AP Group > Policy Mappings** page, you can configure a priority index and the local policy. To define new policies, choose **Security > Local Policies > New**.

- **Remove**—Removes a WLAN from the access point group.

### RF Profile Tab

Table 3-31 RF Profile Tab Parameters

Parameter	Description
802.11a	Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
802.11b	Drop-down list from which you can choose an RF profile for APs with 802.11b radios.

Click **Apply** to apply the RF profile selected for the APs.



**Note** Applying an RF profile results in a reboot of all the APs associated with the AP Group.

### APs Tab

Table 3-32 APs Tab Parameters

Parameter	Description
APs currently in the Group	Access points that are currently assigned to this group. To remove an access point, select the check box to the left of the AP name or select the <b>AP Name</b> check box to select all APs, and click <b>Remove APs</b> .
Add APs to the Group	Access points that are available to be added to the group. To add an access point, select the check box to the left of the AP Name or select the <b>AP Name</b> check box to select all APs, and click <b>Add APs</b> .

## 802.11u Tab

Table 3-33 802.11u Parameters

Parameter	Description
Venue Group	Drop-down list from which you can choose a Hotspot group that groups similar Hotspot venues. The following options are available: <ul style="list-style-type: none"> <li>• Unspecified</li> <li>• Assembly</li> <li>• Business</li> <li>• Educational</li> <li>• Factory and Industrial</li> <li>• Institutional</li> <li>• Mercantile</li> <li>• Residential</li> <li>• Storage</li> <li>• Utility and Misc</li> <li>• Vehicular</li> <li>• Outdoor</li> </ul>
Venue Type	Drop-down list from which you can choose the type of venue based on the Venue Group that you choose.
Venue Name	Venue name that you can provide for this access point. This name is associated with the basic service set (BSS). This name is used in cases where the SSID does not provide enough information about the venue. The venue name is case sensitive and can be up to 252 alphanumeric characters.
Language	Language used at the venue. You must specify the language before you specify the venue name. ISO-639 encoded string defining the language used at the venue. This string is a three-character language code. For example, you can enter ENG for English.
Operating class	Select the check box to choose the 802.11u operating class. The different operating classes are 81, 83, 84, 112, 113, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127.  You can add a maximum of 10 operating classes.

Click **Add New Venue** to add a new venue for the AP group.

Click **Apply** to apply the Operating class to the AP group.

**Location Tab****Table 3-34** *HyperLocation Config Parameters*

Parameter	Description
Enable Hyperlocation	Based on AP and installed module, selecting the Enable Hyperlocation checkbox enables different location service (PRL-based, AoA-based, or BLE-based).
Packet Detection RSSI Minimum (dBm)	This is the minimum level at which a data packet can be heard by the WSM modules for use in location calculations. Valid range is between –100 dBm and –50 dBm. Default value is –100 dBm.  It is recommended that this value be increased if you want to have only strong signals used in calculating locations.
Scan Count Threshold for Idle Client Detection	The Scan Count Threshold represent the number of off-channel scan cycles the AP will wait before sending a Block Acknowledgment Request (BAR) to idle clients. Valid range is between 1 and 100. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off channel scan cycle.
NTP Server	This is the IPv4/IPv6 address of the NTP server that all AP that are involved in this calculation need to sync to.  We recommend that you use the same NTP server as is used by the general Cisco WLC infrastructure. The scans from multiple APs must be synced up for the location to be accurately calculated. An IPv4 address is required.  <b>Note</b> IPv6 address format is not supported.

**Ports/Module Tab**

LAN Ports—In the LAN Ports area, you can configure the parameters used to associate RLAN with Ethernet LAN ports on an AP group. To enable the LAN ports, check the **Enable** check box for the applicable LAN ports. If POE has to be enabled on LAN1, check the POE check box. To associate RLAN with the LAN ports, select the RLAN from the RLAN drop-down list for each of the LAN ports.

**Note**

Different RLANs can be applied to individual LAN ports.

External Module 3G/4G—In the External Module 3G/4G area, you can configure the parameters used to associate RLAN with an external 3G/4G module on an AP group. To enable the external 3G/4G module, check the **Enable** check box. To associate RLAN with the external 3G/4G module, select the RLAN from the RLAN drop-down list.

