Using the Cisco Wireless Controller (Cisco WLC) Web User Interface

Overview

The Web User Interface is built into each Cisco WLC. The Web User Interface enables up to five users simultaneously to browse the built-in controller HTTP or HTTPS (HTTP + SSL) Web server, configure parameters, and monitor operational status for the Cisco WLC and its associated access points.

Because the Web User Interface works with one Cisco WLC at a time, the Web User Interface is useful when you want to configure or monitor a single Cisco WLC and its associated access points.

The Web User Interface has two views:

- Main Dashboard View, page 1-1
- Advanced View, page 1-3

Main Dashboard View

Introduced in Release 8.1, the Main Dashboard is displayed when you log on to the Cisco WLC.

You can view the following on the Main Dashboard:

- **AP or Client** search bar—Search for an AP or a client by typing its name.
- **Advanced**—To go to the Advanced view, that is the classic Web UI mode. In the Advanced View, click **Home** to return to the Main Dashboard view.
- Dashboard Settings—Use this to set the landing page, view system information, or log out of Cisco WLC Web UI.
- **Monitoring** pane—A pane on the left hand side with Monitoring menus using which you can monitor the access points and clients and their performance details. You can view the following menus on the **Monitoring** pane:
  - Network Summary
  - Wireless Dashboard
  - Best Practices

Network Summary

The **Network Summary** page displays the following:

- A set of widgets that display information about wireless networks, access points, active clients, rogues, and interferers.
- A set of dashlets that display information about access points, clients, applications, and clients in both graphical and tabular format.

  Following are some of the actions you can perform with the dashlets:

  – You can toggle between the graphical view and the tabular view.

  – You can export the tabular information to a spreadsheet.

  – You can rearrange the dashlets by dragging and dropping them according to your needs.

Access Points

The **Access Points** page gives you a detailed information about access points that are associated with the Cisco WLC, in a tabular format. The AP information can be viewed for 2.4-GHz and 5-GHz bandwidth separately.

Clients

The **Clients** page gives you a detailed information about clients that are associated with the access points.

Wireless Dashboard

The **Wireless Dashboard** displays an overview of information about access points and clients in both graphical and tabular format.

Following are some of the actions you can perform with the dashlets:

– You can toggle between the graphical view and the tabular view.

– You can export the tabular information to a spreadsheet.

– You can rearrange the dashlets by dragging and dropping them according to your needs.

AP Performance

The **AP Performance** page displays the following dashlets:

- Coverage—Shows bottom 10 APs based on coverage hole detection (CHD)
- Client Load—Shows top 10 APs based on client count. It also shows AP throughput
- Interference—Shows top 10 APs based on noise
- Channel Utilization—Shows top 10 APs by interference, data traffic, and available capacity

Client Performance

The **Client Performance** page displays the following dashlets:

- Clients by signal strength
- Client by signal quality
- Client connections
- Connection rate
- Client Troubleshooting

Best Practices

The **Best Practices** page offers current compliance assessment and available categories of best practices. The Best Practices are enabled by default if you have used the Cisco WLAN Express Setup to configure the WLC.

Note The Best Practices are not enabled through CLI setup wizard or image upgrades.

The Best Practices categories include:

- Infrastructure
- Security
- RF Management

Click the + icon to select a recommended Best Practice parameter, read an expert recommendation, and click **Fix it Now** or later reverse the Best Practice configuration option by clicking **Restore Default**.

Click **Learn More** to go to the relevant section in the *Cisco Wireless Controller Best Practices* document.

Click **Manual Configuration** to manually configure the recommended best practice.

Click **Ignore** to ignore the recommended best practice, wherever applicable.

Advanced View

The Advanced View shows the Cisco WLC in the classic Web UI mode and contains the following:

- Menu Bar
- Left Navigation Pane
- Main Data Page
- Toolbar
- Buttons

Menu Bar

The Menu Bar contains the following tabs:

- Monitor Tab
- WLANs Tab
- Controller Tab

- Wireless Tab
- Security Tab
- Management Tab
- Commands Tab
- Help—Launches this online help document that gives descriptions of the Web UI elements.
- Feedback Tab—Option to provide your feedback on the Cisco WLC.

Left Navigation Pane

The left navigation pane enables you to select a new configuration panel under the menu area that you have selected. You may select a single configuration panel from several available choices for data to be displayed or configured. The left navigation pane options vary based on the menu that you select.

Main Data Page

The main data page depends on what information the menu requires. Input fields are of two basic types:

- Text boxes into which you may enter data using the keyboard
- Drop-down lists from which you can choose from several available options

To perform an action, you may need to enter or select data on the page. To save your changes in the Cisco WLC, click the **Apply** button available on the right-hand side, top corner of the page.

Note Microsoft Internet Explorer generates a submit action on the next available button when you press the enter key while you are in an input field. On most menus, this action triggers the apply function.

Toolbar

This area provides shortcuts to the following administrative functions used on a regular basis when configuring a controller through the Web User Interface.

- Save Configuration—Saves data to the Cisco WLC in nonvolatile RAM (NVRAM) and is preserved in the event of a power cycle. If you reboot the Cisco WLC, all applied changes are lost unless the configuration has been saved. Click **Save** to save the current configuration.
- Ping—Sends a ping to a network element.

  This alert box enables you to tell the Cisco WLC to send a ping request to a specified IP address to help determine if there is connectivity between the Cisco WLC and a particular IP station. Once you click the **Submit** button, three pings are sent and the results of the pings are displayed in the alert box. If a reply to the ping is not received, it displays “No Reply Received from IP xxx.xxx.xxx.xxx”; otherwise, it displays “Reply received from IP xxx.xxx.xxx.xxx: (send count = 3, receive count = n).”
- Logout—Exits the current Web User Interface session.
- Refresh—Updates the data on the current page from the Cisco WLC.
- Home—Opens the Main Dashboard.

Buttons

At the right side of the main data page, you can click command buttons to apply or refresh the data that is displayed on the main data page.

Buttons take immediate effect when you select them and information goes to the controller about the state of the menu at that time. The most commonly used buttons are as follows:

- Apply—Sends data to the Cisco WLC but data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Back—Takes you back to the previously viewed page.

There are additional buttons that perform other actions; not all main data pages have all buttons. The functionality of these buttons is described in the respective help topics.

Navigating Pages with Many APs

If your Cisco WLC is associated with many access points and if they cannot be displayed in a single page, you can use one of the following options to navigate the pages that list the access points by clicking the buttons on the top right-hand corner of the page.

- Click the individual page number to go to a specific page.
- Click the forward and backward buttons at the extreme end of the page to go to the first or last pages.
- Click the forward or backward buttons to skip to the next five pages.

Applying Parameters

After you save the new parameters or settings that you entered, the page is refreshed. However, in some cases, the settings may appear different than the ones that you specified because the affected code takes some time to execute. You should refresh the menu or the page to see the expected results.

Note When applying parameters on a page, some parameters may need to have the network to be down so that they can be applied. When configuring such parameters using the GUI, if the network is up and running, you may see an error message indicating that the network is operational.

Refreshing the Page

Using the refresh function from the Web User Interface refreshes all pages and displays the default initial window in the main data page.

If you want to refresh a page in the main data area, and there is no refresh button present, use your mouse to right-click the main data area page, and select the refresh option.

Monitor Tab

The Monitor tab on the menu bar enables you to access the controller and APs' summary details. Use the left navigation pane to access the respective network details.

Information available via the Monitor tab:

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- Cisco Discovery Protocol
- Rogues
- Redundancy
- Clients
- Sleeping Clients
- Multicast Groups
- Applications
- Lync
- Local Profiling

Summary

Choose **MONITOR > Summary** to navigate to the Summary page.

The summary page provides a top level description of your controller, access points, clients, WLANs, and rogues. Rogues are unauthorized devices (access points, clients) that are connected to your network.

The controller image is displayed at the top of the summary page and gives information about the controller model number and the number of access points supported by the controller.

Note All parameters on this page are read-only parameters.

This page is automatically refreshed every 30 seconds.

This table describes the monitor summary parameters.

Table 2-1 Summary Parameters

Parameters	Description
Controller Summary	
Management IP Address	Management IPv4/IPv6 address of the controller. From Release 8.0, IPv6 is also supported for configuring Management interface.
Service Port IP Address	IPv4/IPv6 address of the controller front-panel service port. From Release 8.0, IPv6 is also supported for configuring Service interface.
Software Version	Version of the Operating System running on the controller.
Field Recovery Image Version	Version of the boot software ER.aes file. **Note** If a boot software ER.aes file is not installed, the Field Recovery Image Version field shows an error.
System Name	Controller name specified by the operator.
Up Time	Time elapsed since the controller was last rebooted.
System Time	Current time set on the controller.
Redundancy Mode	Redundancy mode operational on the device. The redundancy modes are as follows: • 0—No redundancy • SSO—Hot Standby Mode • RPR—Cold Standby Mode
Internal Temperature	The internal temperature of the controller.
802.11a/n Network State	Network that is enabled or disabled.
802.11b/g/n Network State	Network that is enabled or disabled.
Local Mobility Group	Name of the default mobility group.
CPU Usage	Percentage of the CPU in use.
Individual CPU Usage (5500 series controller only)	Percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level. This field appears only for the Cisco 5500 Series Controller.
Memory Usage	Percentage of memory in use.
Access Point Summary	
802.11a/n/ac Radios	Number of 802.11a/n Cisco Radios. Click **Detail** for additional information about 802.11a/n/ac Radios.
802.11b/g/n Radios	Number of 802.11b/g/n Cisco Radios. Click **Detail** for additional information about 802.11b/g/n Radios.
Dual-Band Radios	Number of 802.11a/b/g/n Cisco Radios. Click **Detail** for additional information about Dual-Band Radios.
All APs	Number of access points associated with this controller. Click **Detail** for additional information about All APs.
Client Summary	
Current Clients	Number of clients currently associated with the controller. Click **Detail** for additional information about current Clients.

Table 2-1 Summary Parameters

Parameters	Description
Excluded Clients	Number of excluded client computers by MAC address that you can enable or disable. Click **Detail** for additional information about excluded clients.
Disabled Clients	Number of clients that are currently disabled. Click **Detail** for additional information about disabled clients.
Rogue Summary	
Active Rogue APs	Number of unauthorized access points detected by the controller. Click **Detail** for additional information about active Unclassified Rogue APs.
Active Rogue Clients	Number of active clients associated with a rogue access point. Click **Detail** for additional information about Rogue Client Details.
Adhoc Rogues	Number of ad-hoc rogues. Click **Detail** for additional information about Adhoc Rogues.
Rogues on Wired Network	Number of rogues on a wired network. Click **Detail** for additional information.
Session Timeout	
Session Timeout	• If you leave the check box unchecked, the **Monitor > Summary** page gets refreshed every 30 seconds. • If you check the check box, the **Monitor > Summary** page does not get refreshed automatically every 30 seconds.
Top WLANs	
Profile Name	Name of the WLAN as specified by the operator.
# of Clients by SSID	Number of clients associated with the WLAN based on SSID.
Most Recent Traps	Log of most recent SNMP traps. Click **View All** to view all SNMP Trap Logs.
Top Applications	
Application Name	Top 10 applications detected by the Cisco WLC in the last three minutes that appear according to their total byte count. These applications include both upstream and downstream applications.
Packet Count	Packet count of the application.
Byte Count	Byte count of the application.
Top Flex Applications	
Application Name	Top 10 FlexConnect applications detected by the Cisco WLC in the last three minutes that appear according to their total byte count. These applications include both upstream and downstream applications.
Packet Count	Packet count of the application.
Byte Count	Byte count of the application.

Access Points

Choose **MONITOR > Access Points** to navigate to the Access Points page. From here you can choose the following:

- **MONITOR > Access Points > Radios > 802.11a/n/ac** to view the Cisco radio profile for your 802.11a/n/ac RF network.
- **MONITOR > Access Points > Radios > 802.11b/g/n** to view the Cisco radio profile for your 802.11b/g/n RF network.
- **MONITOR > Access Points > Radios > Dual-Band Radios** to view the Cisco radio profile for your 802.11a/b/g/n RF network.

802.11a/n/ac Radios

Choose **MONITOR > Access Points > Radios** > **802.11a/n/ac** to navigate to the 802.11a/n/ac Radios page.

The 802.11a/n/ac Radios page displays the Cisco Radio profile for your 802.11a/n/ac RF network. The page also displays the status of each 802.11a/n/ac Cisco Radio that is configured on the controller and its profile.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the figure below) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC address or AP name.

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

- MAC Address—MAC address.
- AP Name—Access point name.
- CleanAir Oper Status—Operational status of the CleanAir-capable access point. Choose from the following available statuses:
  - UP
  - DOWN
  - ERROR
  - N/A

Note When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11a/n/ac Radios page. The Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

802.11a/n/ac and 802.11b/g/n Radio Profile

To access the details for each Cisco Radio, click the **Detail** link (see Radio Statistics for more information).

To access the details of air quality, click the blue arrow adjacent the desired radio and click **CleanAir** (see Cisco CleanAir for more information).

This table describes the 802.11a/n /ac radio parameters.

Table 2-2 802.11a/n /ac Radio Parameters

Parameters	Description
AP Name	Name assigned to the access point.
Radio Slot #	Slot where the radio is installed.
Base Radio MAC	MAC address of the access point.
Sub Band	Radio sub band, if it is active: 4.9 GHz or 5.8 GHz.
Operational Status	Operational status of the Cisco Radios: UP or DOWN.
Radio Role	Radio role: UPLINK or DOWNLINK.
Load Profile	Radio Resource Management (RRM) profile for the Cisco Radio. The profile status is displayed as a pass or fail with details provided on the Radio Statistics page. **Note** For Cisco OEAP 600 Series access points, the following parameters show the value as N/A: – Load Profile – Noise Profile – Interference Profile – Coverage Profile
Noise Profile	
Interference Profile	
Coverage Profile	
CleanAir Admin Status	CleanAir admin status.
CleanAir Oper Status	Spectrum sensor status for this access point.

Radio Statistics

Choose **MONITOR > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n**, click the blue arrow adjacent the desired access point and choose **Detail** to navigate to the Radio Statistics page.

Note Rx Neighbors, Radar Information, and Band Select Statistics are not displayed for outdoor mesh access points.

This page displays the RF (Radio Frequency) statistics for the selected Cisco Radio. You can alternate between the Graphics View and the Text View by clicking the **Graphics View/Text View** button. You can view and refresh detailed statistics by selecting them (using the check boxes) and then clicking the **Refresh** button on the data page.

Link Parameters

These parameters are displayed for 802.11a/n/ac radios on Mesh access points.

- Radio Role—Radio role for the backhaul: UPLINK or DOWNLINK.
- Source Backhaul MAC—MAC address of the source backhaul radio.

VoIP Stats

Note VoIP Stats parameters are not displayed for outdoor mesh access points.

The VoIP Stats shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the Cisco WLC.

SIP CAC Call Stats

Note The SIP CAC Call Stats parameters are not displayed for outdoor mesh access points.

The SIP CAC Call stats section shows the following information:

- Total number of SIP calls in progress
- Number of roaming SIP calls in progress
- Total number of SIP calls since AP joined
- Total number of roaming SIP calls since AP joined
- Total number of SIP calls rejected due to insufficient bandwidth
- Total number of SIP roam calls rejected due to insufficient bandwidth
- Total number of SIP calls rejected due to maximum call limit
- Total number of SIP roam calls rejected due to maximum call limit

Preferred Call Stats

The Preferred Call Stats section shows the following information:

- Total number of preferred calls received
- Total number of preferred calls accepted

KTS CAC Call Stats

The KTS CAC Call Stats section shows the following information:

- Total number of KTS calls in progress
- Number of roaming KTS calls in progress
- Total number of KTS calls since AP joined
- Total number of roaming KTS calls since AP joined
- Total number of KTS calls rejected due to insufficient bandwidth
- Total number of KTS roam calls rejected due to insufficient bandwidth

Video Call Admission Control (CAC) Stats

The Video Call Admission Control (CAC) Stats section shows the following information:

- Video Bandwidth in use (% of config bandwidth)
- Video Roam Bandwidth in use (% of config bandwidth)
- Total Bandwidth in use for Video

TPSEC Video CAC Call Stats

The TPSEC Video CAC Call Stats section shows the following information:

- Total number of video calls in progress
- Number of roaming video calls in progress
- Total number of video calls since AP joined
- Total number of roaming video calls since AP joined
- Number of video calls rejected since AP joined
- Number of roaming video calls rejected since AP joined
- Number of video calls rejected due to insufficient bandwidth
- Number of video roam calls rejected due to invalid parameters
- Number of video roam calls rejected due to the physical layer (PHY) rate
- Number of video roam calls rejected due to the QoS policy

SIP Video CAC Call Stats

The SIP Video CAC Call Stats section shows the following information:

- Total number of video calls in progress
- Number of roaming video calls in progress
- Total number of video calls since AP joined
- Total number of roaming video calls since AP joined
- Number of video calls rejected due to insufficient bandwidth
- Number of roaming video calls rejected due to insufficient bandwidth

Profile Information—Graphics View and Text View

The RF statistics are used to derive the RRM profile for each Cisco Radio in your network (see the following figure). The controller uses the Radio Resource Management (RRM) profile to adjust the Cisco Radio transmit and receive levels in order to maintain the most efficient configuration for your network. This data view also displays the RF properties of the controller and its clients.

- The Radio Resource Management (RRM) PASSED/FAILED thresholds are globally set for all access points in the 802.11a/n/ac RF Grouping and 802.11b/g/n RF Grouping pages.
- The Radio Resource Management (RRM) PASSED/FAILED thresholds are individually set for this access point in the Performance Profile of 802.11a/n/ac Access Points page.

Click **Graphics View** to view the RRM profile information as a graph.

Click **Text View** to view the RRM profile information as tables.

The following sections describe each of the Graphical and Text results.

Noise vs. Channel

Each channel of the access point appears with the corresponding non-802.11 noise that interferes with the currently assigned channel.

Interference by Channel

Each channel of the access point appears with the corresponding traffic interference from other 802.11 sources.

Load Statistics

The total Receive and Transmit bandwidth and channel utilization appears for transmitting and receiving traffic on this Cisco Radio. The number of attached clients is also displayed.

% Client Count vs. RSSI

This graphic view sorts attached clients by their Received Signal Strengths.

% Client Count vs. SNR

This graphic view sorts attached clients by their Signal to Noise Ratios.

Rx Neighbors Information

This area displays the Cisco Radio's neighboring access points and their IP address and RSSI values. These details are used for channel allotment and RF coverage area shaping.

Information similar to the following appears:

```
AP 00:0b:85:00:83:00 Interface 0         172.16.16.10
```

where

- AP is an access point.
- 00:0b:85:00:83:00 is the MAC address of the neighboring access point.
- Interface x is the interface number of the neighboring access point.
- 172.16.16.10 is the IP address of the access point's controller.

Radar Information

The Dynamic Frequency Selection (DFS) capability of the Cisco IOS software detects radar signals (typically military and weather) within the operating range of the access point. If a radar is detected, then the Cisco IOS access point will decide which channel to go on and report that information to the Cisco WLC. The Cisco WLC will then be responsible for maintaining a 30-minute timeout for the channels on which the radar was detected. When the access point is in FlexConnect standalone mode, it changes the channel when it detects a radar and reports back to the Cisco WLC after the next successful join.

802.11 MAC Counters

Table 2-3 802.11 MAC Counters

Counter	Description
Tx Fragment Count	Counter that is incremented for an acknowledged MPDU (MAC Protocol Data Unit) with an individual address in the address 1 field.
Tx Failed Count	Counter that increments when an MSDU (MAC Service Data Unit) is successfully transmitted after one or more retransmissions.
Multiple Retry Count (Graphics view only)	Counter that increments when an MSDU is successfully transmitted after more than one retransmission.
RTS Success Count	Counter that increments when a CTS (Clear To Send) is received in response to an RTS (Request To Send).
ACK Failure Count	Counter that increments when an ACK is not received when expected.
Multicast Rx Frame Count	Counter that increments when an MSDU is received with the multicast bit set in the destination MAC address.
Tx Frame Count	Counter that increments for each successfully transmitted MSDU.
Multicast Tx Frame Count	Counter that increments only when the multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the access point, this frame count implies having received an acknowledgment to all associated MPDUs.
Retry Count	Counter that increments when an MSDU is successfully transmitted after one or more retransmissions.
Frame Duplicate Count	Counter that increments when a frame is received that the Sequence Control field indicates is a duplicate.
RTS Failure Count	Counter that increments when a CTS is not received in response to an RTS.
Rx Fragment Count	Counter that increments for each successfully received MPDU of type Data or Management.
FCS Error Count	Counter that increments when an FCS error is detected in a received MPDU.
WEP Undecryptable Count	Counter that increments when a frame received with the WEP subfield of the Frame Control field is set to one and the WEP On value for the key that is mapped to the MAC address of the TA indicates that the frame should not have been encrypted or that the frame has been discarded because to the receiving STA has not implemented the privacy option.

Band Select Statistics

The Band Select Statistics section shows the following information:

- Number of dual band client
- Number of dual band client added
- Number of dual band client expired
- Number of dual band client replaced

- Number of dual band client detected
- Number of suppressed client
- Number of suppressed client expired
- Number of suppressed client replaced

CleanAir Parameters

The CleanAir operational status is displayed by the **Operational Status** parameter.

802.11b/g/n Radios

Choose **MONITOR > Access Points > Radios > 802.11b/g/n** to navigate to this page.

This page displays the Cisco Radio profile for your 802.11b/802.11g RF network. It shows the status of each 802.11b/g Cisco Radio configured and its profile.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access point by MAC address or AP name.

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

- MAC Address—MAC address.
- AP Name—Access point name.
- CleanAir Oper Status—Operational status of the CleanAir capable access point. Choose from the following available statuses:
  - UP
  - DOWN
  - ERROR
  - N/A

Note When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

802.11b/g/n Radios

To access details for each Cisco Radio, click the **Detail** link (see Radio Statistics for more information).

To access details of the air quality, click the blue arrow adjacent the desired access point radio and choose **CleanAir** (see Cisco CleanAir for more information).

Table 2-4 802.11b/g/n Radio Parameters

Parameters	Description
AP Name	Name assigned to the access point.
Radio Slot #	Slot where the radio is installed.
Base Radio MAC	MAC address of the access point.
Operational Status	Operational status of the Cisco Radios: UP or DOWN.
Load Profile	Radio Resource Management (RRM) profile for the Cisco Radio. The profile status is displayed as a pass or fail with details provided on the Radio Statistics data page.
Noise Profile	
Interference Profile	
Coverage Profile	
CleanAir Admin Status	Status of the CleanAir admin.
CleanAir Oper Status	Status of the spectrum sensor for this access point.

CleanAir Radio Monitoring Rapid Update

Choose **MONITOR > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n.** Click the blue arrow adjacent the desired access point radio and choose **CleanAir**. The 802.11a/n/ac (or 802.11b/g/n) > *Access Point Name* > Radio Monitoring Rapid Update page appears.

The Radio Monitoring Rapid Update page displays the CleanAir statistics for the selected Cisco Radio. You can alternate between the Graphics View and the Text View by clicking the **Graphics View/Text View** button. You can view and refresh the following statistics by selecting them (using the check boxes) and then clicking the **Refresh** button on the data page.

Active Interferer Parameters

Table 2-5 Active Interferer Parameters

Parameter	Description
Interferer Type	Type of the interferer.
Affected Channel	Channel that the device affects.
Detected Time	Time at which the interference was detected.
Severity	Severity index of the interfering device.
Duty Cycle (%)	Proportion of time during which the interfering device was active.
RSSI (dBm)	Receive signal strength indicator (RSSI) of the access point.
DevID	Device identification number that uniquely identifies the interfering device.
ClusterID	Cluster identification number that uniquely identifies the type of the devices.

Air Quality

The air quality provides a graphical representation of the average air quality for the access point on this radio.

Non-Wi-Fi Channel Utilization

The non-Wi-Fi channel utilization provides a graphical representation of the non-Wi-Fi channel utilization. The graph displays the percentage of spectrum used by the interference source.

Interference Power

The interference power provides a graphical representation of the non-Wi-Fi based interference source and displays the power level of the channel being affected.

Dual-Band Radios

Choose **MONITOR > Access Points > Radios > Dual-Band** to navigate to the Dual-Band Radios page.

This page displays the Cisco Radio profile and summary for your 802.11a/b/g/n RF network.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access point by MAC address or AP name.

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

- MAC Address—MAC address.
- AP Name—Access point name.
- CleanAir Oper Status—Operational status of the CleanAir capable access point. Choose from the following available statuses:
  - UP
  - DOWN
  - ERROR
  - N/A

Note When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the Dual-Band Radio page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Dual-Band Radios Summary

Table 2-6 Dual-Band Radio Parameters

Parameters	Description
AP Name	Name assigned to the access point.
Radio Slot #	Slot where the radio is installed.
Base Radio MAC	MAC address of the access point.
Operational Status	Operational status of the Cisco Radios: UP or DOWN.
Load Profile	Radio Resource Management (RRM) profile for the Cisco Radio. The profile status is displayed as a pass or fail with details provided on the Radio Statistics data page.
Noise Profile	
Interference Profile	
Coverage Profile	
CleanAir Admin Status	Status of the CleanAir admin.
CleanAir Oper Status	Status of the spectrum sensor for this access point.

Cisco CleanAir

Choose **Monitor > Cisco CleanAir** to view the Interference Devices or the Air Quality Report pages. From here, you can choose the following:

- **MONITOR > Cisco CleanAir > 802.11 a/n/ac** (or **802.11 b/g/n**) > **Interference Devices** to view the the list of the interference devices in your 802.11a/n/ac or 802.11b/g/n RF network. See Cisco CleanAir Interference Devices for more information.
- **MONITOR > Cisco CleanAir > 802.11 a/n/ac** or **802.11 b/g/n** > **Air Quality Report**. to view the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. See Cisco CleanAir Air Quality Report for more information.

Cisco CleanAir Interference Devices

Choose **Monitor > Cisco CleanAir > 802.11 a/n/ac** (or **802.11 b/g/n**) > **Interference Devices** to navigate to the Cisco CleanAir Interference Devices page. This page displays the list of the interference devices.

Table 2-7 Interference Device Parameters

Parameter	Description
AP Name	Name of the access point where the interference device is detected.
Radio Slot #	Slot that detects the interferers.
Device Type	Type of the device.
Affected Channel	Channel that the device affects.
Detected Time	Time at which the interference was detected.
Severity	Severity index of the interfering device.

Table 2-7 Interference Device Parameters

Parameter	Description
Duty Cycle (%)	Proportion of time during which the interfering device was active.
RSSI	Receive signal strength indicator (RSSI) of the access point.
DevID	Device identification number that uniquely identifies the interfering device.
ClusterID	Cluster identification number that uniquely identifies the type of the devices. When a CleanAir-enabled access point detects interference devices, these detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which causes the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is removed from the spectrum database. In cases when all the interferer detections for a specific device are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged to the original cluster ID and the device detection history is preserved. For example, some Bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption such as turning off the transmitter when it is not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and merges them again into a single record upon detection. Preventing bouncing smoothens the interference device records and allows the records to accurately represent the device history.

Click **Change Filter** to display the information about interference devices based on a particular criteria. Click **Clear Filter** to remove the filter and display entire access point list.

You can create a filter to display the list of interference devices that are based on the following filtering parameters:

- Cluster ID—To filter based on the Cluster ID, select the check box and enter the Cluster ID in the text box next to this field.

Note When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which allows the spectrum sensor to temporarily stop detecting the device. The device is then marked as down. A down device would be correctly removed from the spectrum database. In cases when all the interferer detections for a specific device are reported down, the cluster is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged to the original cluster and all the device history over time is kept together. For example, some Bluetooth headsets operate on battery power. These devices employ a power saving mode such as turning off the transmitter when it is not actually needed. Such devices can appear up and down. Bouncing prevention smoothens the interferer device records and accurately represents the device history.

- AP Name—To filter based on the access point name, select the check box and enter the access point name in the text box next to this field.

- Interferer Type—To filter based on the type of the interference device, select the check box and select the interferer device from the options.

  Select one of the following interferer devices:

  - TDD Transmit
  - Jammer
  - Continuous TX
  - DECT Phone
  - Video Camera
  - WiFi Inverted
  - WiFi Inv. Ch
  - SuperAG
  - Canopy
  - WiMax Mobile
  - WiMax Fixed
  - WiFi ACI
  - Unclassified
- Affected Channels
- Severity
- Duty Cycle (%)
- RSSI

Click **Find** to commit your changes.

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

Cisco CleanAir > 802.11b/g/n > BLE Beacons

Choose **Monitor > Cisco CleanAir > 802.11 b/g/n > BLE Beacons** to navigate to the **802.11b/g/n Cisco APs > BLE Beacons** page, which shows the following details:

- AP Name
- Radio Slot#
- Device Type
- Affected Channel
- Detected Time
- Severity
- Duty Cycle(%)
- RSSI
- DevID
- Cluster ID

Cisco CleanAir Air Quality Report

Choose **Monitor > Cisco CleanAir > 802.11 a/n/ac** or **802.11 b/g/n > Air Quality Report** to navigate to the Air Quality Report page. This page displays the air quality on the access points. Air Quality is checked on all channels if you have a monitor module for an Cisco Aironet 3600 series access point.

Table 2-8 Cisco CleanAir Air Quality Report Parameters

Parameter	Description
AP Name	Name of the access point.
Radio Slot #	Slot where the interference is detected.
Channel	Channel where the air quality is monitored.
Average AQ	Average air quality observed.
Minimum AQ	Minimum air quality observed.
Interferer	Number of devices that affect a particular channel.
DFS (Dynamic Frequency Selection)	Whether DFS is enabled.

Cisco CleanAir Worst Air Quality Report

Choose **Monitor > Cisco CleanAir > Worst Air Quality Report**. to navigate to the the Worst Air Quality Report page. This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands.

Table 2-9 Cisco CleanAir Worst Air Quality

Parameter	Description
AP Name	Name of the access point that reported the worst air quality for the 802.11a/n/ac or 802.11b/g/n radio band.
Channel Number	Radio channel with the worst reported air quality.
Minimum Air Quality Index (1 to 100)	Minimum air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
Average Air Quality Index (1 to 100)	Average air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
Interference Device Count	Number of interferers detected by the radios on the 802.11a/n/ac or 802.11b/g/n radio band.

To view a list of persistent sources of interference for a specific access point radio, follow these steps:

Step 1 **Choose Wireless > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 2 Click the blue arrow adjacent the desired access point radio and choose **CleanAir-RRM**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > *Access Point Name* > Persistent Devices page appears.

This page lists the device types of persistent sources of interference detected by this access point radio. It also shows the channel on which the interference was detected, the percentage of time that the interferer was active (duty cycle), the received signal strength (RSSI) of the interferer, and the day and time when the interferer was last detected.

Statistics

Choose **MONITOR > Statistics** to navigate to the Statistics page. From here, you can choose the following:

- **MONITOR > Statistics > Controller** to view the controller statistics.

  See Controller Statistics for more information.
- **MONITOR > Statistics > AP Join** to view all the access points that have joined or have tried to join to the controller.

  See AP Join Statistics for more information.
- **MONITOR > Statistics > Port** to view the status of each port on the controller.

  See Port Statistics for more information.
- **MONITOR > Statistics > RADIUS Servers** to view addressing and status information of your RADIUS servers.

  See RADIUS Server Statistics for more information.
- **MONITOR > Statistics > Mobility Statistics** to view the statistics for mobility group events.

  See Mobility Statistics for more information.
- **MONITOR > Statistics > IPv6 Neighbor Bind Counters** to view counter statistics for the following Neighbor Discovery Protocol (NDP) and Dynamic Host Configuration Protocol (DHCP) packets.

  See IPv6 Neighbor Bind Counters for more information.
- **MONITOR > Statistics > PMIPv6 LMA Statistics** to view the statistics of all the LMA (Local Mobility Anchor) that the controller is connected to.

  See PMIPv6 LMA Statistics for more information.
- **MONITOR > Statistics > Preferred Mode Statistics** to view the details of the APs on which the IP config (Global/ AP Group) has been configured.

  See Preferred Mode for more information.
- **MONITOR > Statistics > Optimized Roaming** to view the details of optimized roaming.

Controller Statistics

Choose **MONITOR > Statistics > Controller** to view the controller statistics.

Note All the statistics related to received packets are Ethernet packets received on the controller port . These packets are a combination of CAPWAP packets, and packets from any wired infrastructure that reach the controller.
All the statistics related to packets transmitted from the controller include CAPWAP packets to access points and non-encapsulated packets to wired infrastructure.

Table 2-10 Controller Summary Statistics

Parameter	Description
Octets Received	Total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Error	Total number of packets received by the processor.
Unicast Packets Received	Number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	Total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	Total number of packets received that were directed to the broadcast address.
Receive Packets Discarded	Number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	Total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	Total number of packets transmitted out of the interface.
Unicast Packets Transmitted	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those packets that were discarded or not sent.
Multicast Packets Transmitted	Total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	Number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	Number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	Highest number of Forwarding Database Address Table entries that have been learned by this controller since the most recent reboot.
Address Entries in Use	Number of learned and static entries in the Forwarding Database Address Table for this controller.

Table 2-10 Controller Summary Statistics

Parameter	Description
Maximum VLAN Entries	Maximum number of Virtual LANs (VLANs) allowed on this controller.
Most VLAN Entries Ever Used	Largest number of VLANs that have been active on this controller since the last reboot.
Static VLAN Entries	Number of presently active VLAN entries on this controller that have been created statically.
Time Since Counters Last Cleared	Elapsed time, in days, hours, minutes, and seconds, since the statistics for this controller were last cleared.

Click **Clear Counters** to set all summary and detailed controller statistics counters to zero; also resets the Time Since Counters Last Cleared field.

AP Join Statistics

Choose **MONITOR > Statistics > AP Join** to navigate to the AP Join Statistics page.

The join statistics for an access point that send a CAPWAP discovery request to the controller at least once are maintained on the controller even if the access point is rebooted or disconnected. These statistics are removed only if the controller is rebooted or if you choose to clear the statistics.

This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can access these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

AP List Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access point by MAC address or AP name.

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

- **Ethernet MAC Address—**MAC address.
- **AP Name—**Access point name.

Note When you enable one of these filters, the other filter is disabled automatically.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Show All**.

Click the MAC address of the radio to see detailed statistics for each port on the AP Join Stats Detail page (see AP Join Statistics Detail for more information).

To remove an access point from the list, click the blue arrow adjacent the desired access point and choose **Remove**.

Click **Clear Stats on All APs** to clear the statistics for all access points.

AP Join Statistics Detail

Choose **MONITOR > Statistics > AP Join** and then click the base radio MAC address to navigate to the **AP Join Stats Detail** page. This page provides information on each phase of the join process and shows any errors that have occurred.

Port Statistics

Choose **MONITOR > Statistics > Ports** to navigate to the Ports Statistics page. This page displays the status of each port on the controller. This table describes the ports statistics parameters.

Table 2-11 Summary Parameters

Parameter	Description	Range
Port No	Port number on the controller.	1–12 for 10/100BASE-T, 13 for 1000BASE-T or 1000BASE-SX. 1–24 for 10/100BASE-T, 25 for 1000BASE-T or 1000BASE-SX. 1 for 1000BASE-SX on a Cisco 4100 Series Wireless LAN Controller. 1 for 1000BASE-SX on a Cisco 4100 Series Wireless LAN Controller.
Admin Status	State of the port.	Enable or Disable.
Physical Mode	Configuration of the port physical interface.	Auto. 100 Mbps full duplex. 100 Mbps half duplex. 10 Mbps full duplex. 10 Mbps half duplex. 1000 Mbps full duplex. **Note** In a Cisco NMWLC6 controller, the physical mode is always set to Auto.

Table 2-11 Summary Parameters

Parameter	Description	Range
Physical Status	Actual port physical interface.	Auto. 100 Mbps full duplex. 100 Mbps half duplex. 10 Mbps full duplex. 10 Mbps half duplex. 1000 Mbps full duplex.
Link Status	Displays the status of the link.	Link Up or Link Down.

The Physical Mode and Status may reflect different values depending on the link status. For example, the Physical Mode may be set to Auto while the link actually runs at 10 Mbps half duplex.

Ports Statistics Details

Choose **MONITOR > Statistics > Ports** and then click **View Stats** to view the port details.

Table 2-12 Port Statistics

Parameter	Received Description	Transmitted Description
Total Bytes	Total number of octets of data (including those octets in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percentage of utilization of the Ethernet segment on a scale of 0 to 100 percent.	Number of octets of data (including those octets in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets (64 Octets)	Total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets (65-127 Octets)	Total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Table 2-12 Port Statistics

Parameter	Received Description	Transmitted Description
Packets (128-255 Octets)	Total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (256-511 Octets)	Total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (512-1023 Octets)	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (1024-1518 Octets)	Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).	Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (> 1518 Octets)	Total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.	Total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Maximum Info size allowed—The maximum size of the Info (non-MAC) field that this port receives or transmits.

Table 2-13 Successful Packets

Parameter	Received Description	Transmitted Description
Total	Total number of packets received that were without errors.	Total number of packets transmitted that were without errors.
Unicast Packets	Number of subnetwork-unicast packets delivered to a higher-layer protocol.	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those packets that were discarded or not sent.

Table 2-13 Successful Packets

Parameter	Received Description	Transmitted Description
Multicast Packets	Total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.	Total number of packets that higher-level protocols requested be transmitted to a multicast address, including those packets that were discarded or not sent.
Broadcast Packets	Total number of good packets received that were directed to the broadcast address.	Total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those packets that were discarded or not sent.

Table 2-14 Protocol Statistics

Parameter	Received Description	Transmitted Description
802.3x Pause Frames Received	Media Access Control (MAC) frames received on this interface with an opcode indicating a PAUSE. This counter does not increment when the interface operates in half-duplex mode.	–

Time Since Counters Last Cleared—The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

Click **Clear Counters** to set all summary and controller detailed statistics counters to zero and to reset the "Time Since Counters Last Cleared" field.

Table 2-15 Received Packets with MAC Errors Parameters

Parameter	Description
Total	Total number of inbound packets that contained errors preventing them from delivery to a higher-layer protocol.
Jabbers	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). This definition of jabber differs from the definition in IEEE 802.3, section 8.2.1.5 (10BASE-5) and section 10.3.1.4 (10BASE-2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments/ Undersize	Number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors	Number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a nonintegral number of octets.

Table 2-15 Received Packets with MAC Errors Parameters

Parameter	Description
FCS Errors	Number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
Overruns	Number of frames discarded because this port was overloaded with incoming packets and could not keep up with the inflow.

Table 2-16 Details of Received Packets Not Forwarded

Parameter	Description
Total	Count of valid frames received that were discarded or filtered by the forwarding process.
Local Traffic Frames	Total number of dropped frames in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	Count of MAC control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface operates in half-duplex mode.
Unacceptable Frame Type	Number of frames discarded from this port due to unacceptable frame types.
VLAN Membership Mismatch	Number of frames discarded on this port due to ingress filtering.
VLAN Viable Discards	Number of frames discarded on this port because a lookup on a particular VLAN occurred while that entry in the VLAN table was modified, or if the VLAN had not been configured.
Multicast Tree Viable Discards	Number of frames discarded because a lookup in the multicast tree for a VLAN occurred while that tree was modified.
Reserved Address Discards	Number of frames discarded that were destined to an IEEE 802.1 reserved address and were not supported by the system.
CFI Discards	Number of frames discarded that had the CFI bit set and the addresses in RIF were in noncanonical format.
Upstream Threshold	Number of frames discarded due to a lack of cell descriptors available for that packet's priority level.

Table 2-17 Transmit Error Parameters

Parameter	Description
Total Errors	Sum of Single, Multiple, and Excessive Collisions.
FCS Errors	Total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.

Table 2-17 Transmit Error Parameters

Parameter	Description
Oversized	Number of frames that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mbps.
Underrun Errors	Number of frames discarded because the transmit FIFO buffer became empty during the frame transmission.

Table 2-18 Transmit Discard Parameters

Parameter	Description
Total Discards	Sum of discarded single collision frames, discarded multiple collision frames, and discarded excessive frames.
Single Collision Frames	Count of the number of successfully transmitted frames on a particular interface for which transmission was inhibited by one collision.
Excessive Collisions	Count of frames for which transmission on a particular interface failed due to excessive collisions.
Port Membership	Number of frames discarded on egress for this port due to egress filtering being enabled.
VLAN Viable Discards	Number of frames discarded on this port because a lookup on a particular VLAN occurred while that entry in the VLAN table was modified, or if the VLAN had not been configured.
Multiple Collision Frames	Count of the number of successfully transmitted frames on a particular interface for which transmission was inhibited by more than one collision.

RADIUS Server Statistics

Choose **MONITOR > Statistics > RADIUS Servers** to navigate to the **RADIUS Servers** page.

This page displays addressing and status information for your Remote Authentication Dial-In User Servers (RADIUS). Configure the authentication and accounting servers by choosing the Security tab from the menu bar.

Table 2-19 Authentication Server and Accounting Server Status Parameters

Parameter	Description
Index	Access priority number for RADIUS servers. Up to 17 authentication and 17 accounting servers can be configured. The controller polling of the servers starts with Index 1, Index 2 second, and so forth. The index number is based on the server index priority that is selected for a RADIUS server when it is added to the controller.
Address	IP address of the RADIUS server.
Port	Communication port.
Admin Status	Enabled or disabled.

RADIUS Servers Authentication Statistics

Choose **MONITOR > Statistics > RADIUS Servers** and then click **Stats** in a RADIUS Authentication entry to navigate to the RADIUS Server Authentication Stats page.

This page displays addressing and status information for your RADIUS servers.

Authentication Server Addressing

Table 2-20 Authentication Server Addressing Parameters

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to 17 servers can be configured. The controller polling of the servers starts with Index 1 first, Index 2 second, and so on. The index number is based on the server index priority that is selected for a RADIUS server when it is added to the controller.
Server Address	IP address of the RADIUS server.
Admin Status	State of the server.

Authentication Server Statistics

Table 2-21 Authentication Server Statistics Parameters

Parameter	Description
Msg Round Trip Time	Time interval between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
First Requests	Number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Retry Requests	Number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.
Accept Responses	Number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Reject Responses	Number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Challenge Responses	Number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Malformed Messages	Number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators, signature attributes, or unknown types are not included as malformed access responses.
Bad Authenticator Msgs	Number of RADIUS Access-Response packets that contain invalid authenticators or signature attributes received from this server.
Pending Requests	Number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, a timeout, or retransmission.

Table 2-21 Authentication Server Statistics Parameters

Parameter	Description
Timeout Requests	Number of authentication timeouts to this server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Type Msgs	Number of RADIUS packets of unknown type received from this server on the authentication port.
Other Drops	Number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

RADIUS Servers Accounting Statistics

Choose **MONITOR > Statistics > RADIUS Servers** and then click **Stats** in a RADIUS Accounting entry to navigate to the RADIUS Servers Accounting Stats page.

This page displays addressing and status information for your Remote Authentication Dial-In User Servers.

Accounting Server Addressing

Table 2-22 Accounting Server Addressing Parameters

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to 17 servers can be configured. The controller polling of the servers starts with Index 1 first, Index 2 second, and so on. The index number is based on the server index priority that is selected for a RADIUS server when it is added to the controller.
Server Address	IP address of the RADIUS server.
Admin Status	State of the server.

Accounting Server Statistics

Table 2-23 Accounting Server Statistics Parameters

Parameter	Description
Msg Round Trip Time	Time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
First Requests	Number of RADIUS Accounting-Request packets sent. This number does not include retransmissions.
Retry Requests	Number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Accounting Responses	Number of RADIUS packets received on the accounting port from this server.

Table 2-23 Accounting Server Statistics Parameters

Parameter	Description
Malformed Messages	Number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticator Msgs	Number of RADIUS Accounting-Response packets that contained invalid authenticators received from this server.
Pending Requests	Number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout, or a retransmission.
Timeout Requests	Number of accounting timeouts to this server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Unknown Type Msgs	Number of RADIUS packets of unknown type received from this server on the accounting port.
Other Drops	Number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

Mobility Statistics

Choose **MONITOR > Statistics > Mobility Statistics** to navigate to the Mobility Statistics page.

This page displays the statistics for mobility group events and is divided into the following three groups:

- Global Statistics that affect all mobility transactions.
- Mobility Initiator Statistics generated by the controller that initiates the mobility event.
- Mobility Responder Statistics generated by the controller that responds to a mobility event.

Global Mobility Statistics

Table 2-24 Global Mobility Statistics Parameters

Parameter	Description
Rx Errors	Generic protocol packet receive errors (such as the packet was too short or format was incorrect).
Tx Errors	Generic protocol packet transmit errors, such as the packet transmission failed.
Responses Retransmitted	Number of retransmitted responses. The mobility protocol uses UDP and it resends requests several times if it does not receive a response. Because of network or processing delays, the responder may receive one or more retry requests after it initially responds to a request. This count includes the response resends.

Table 2-24 Global Mobility Statistics Parameters

Parameter	Description
Handoff Requests Received	Number of handoff requests received, ignored, or responded.
Handoff End Requests Received	Total number of handoff end requests received. These requests are sent by the anchor or the foreign controller to notify the other about the close of a client session.
State Transitions Disallowed	Number of disallowed state transitions. PEM (policy enforcement module) has denied a client state transition, which results in an aborted handoff.
Resource Unavailable	Unavailable resource, such as a buffer, which resulted in an aborted handoff.

Mobility Initiator Statistics

Table 2-25 Mobility Initiator Statistics

Parameter	Description
Handoff Requests Sent	Number of clients that have associated with the controller and have been announced to the mobility group.
Handoff Replies Received	Number of handoff replies that have been received in response to the requests sent.
Handoff as Local Received	Number of handoffs in which the entire client session has been transferred.
Handoff as Foreign Received	Number of handoffs in which the client session was anchored elsewhere.
Handoff Denys Received	Number of handoffs that were denied.
Anchor Request Sent	Number of anchor requests that were sent for a three party (foreign to foreign) handoff. The handoff was received from another foreign controller and the new controller is requesting the anchor controller to move the client.
Anchor Deny Received	Number of anchor requests that were denied by the current anchor.
Anchor Grant Received	Number of anchor requests that were approved by the current anchor.
Anchor Transfer Received	Number of anchor requests that closed the session on the current anchor and transferred the anchor back to the requestor.

Mobility Responder Statistics

Table 2-26 Mobility Responder Statistics

Parameter	Description
Handoff Requests Ignored	Number of handoff requests/client announcements that were ignored. The controller had no knowledge of that client.
Ping Pong Handoff Requests Dropped	Number of handoff requests that were denied because the handoff period was too short (3 seconds).
Handoff Requests Dropped	Number of handoff requests that were dropped due to a either an incomplete knowledge of the client or a problem with the packet.
Handoff Requests Denied	Number of handoff requests that were actively denied.
Client Handoff as Local	Number of handoffs responses sent while in the local role.
Client Handoff as Foreign	Number of handoffs responses sent while in the foreign role.
Anchor Requests Received	Number of anchor requests received.
Anchor Requests Denied	Number of anchor requests denied.
Anchor Requests Granted	Number of anchor requests granted.
Anchor Transferred	Number of anchors transferred because the client moved from a foreign controller to a controller on the same subnet as the current anchor.

IPv6 Neighbor Bind Counters

Choose **MONITOR > Statistics > IPv6 Neighbor Bind Counters** to navigate to the IPv6 Neighbor Bind Counters page.

This page displays counter statistics for the following Neighbor Discovery Protocol (NDP) and Dynamic Host Configuration Protocol (DHCP) packets:

- Received Messages
- Bridged Messages
- Dropped Messages
- NDSUPRRESS Drop counters
- SNOOPING Drop counters

Received Messages

Table 2-27 Received Message Statistics

Parameter	Description
NDP Router Solicitation	Number of received messages originated by the hosts to request a router to send a router advertisement.
NDP Router Advertisement	Number of received messages originated by the routers to advertise their presence and link-specific parameters such as link prefixes, link MTU, and hop limits. These messages are sent periodically and also in response to router solicitation messages.
NDP Neighbor Solicitation	Number of received messages originated by the nodes to request the link layer address of another node and also for functions such as duplicate address detection and neighbor unreachability detection.
NDP Neighbor Advertisement	Number of received messages in response to neighbor solicitation messages. If a node changes its link-layer address, it can send an unsolicited neighbor advertisement to advertise the new address.
NDP Redirect	Number of received messages to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor.
NDP Certificate Solicit	Number of received messages to know the certification path to the trust anchor. Hosts will send the Certification Path Solicitations.
NDP Certificate Advert	Number of received messages to know the certification path to the trust anchor. Routers will send the Certification Path Advertisement messages.
DHCPv6 Solicitation	Number of received messages sent by a client to locate DHCPv6 servers.
DHCPv6 Advertisement	Number of received messages sent by a DHCPv6 server in response to a DHCPv6 solicitation message to indicate availability.
DHCPv6 Request	Number of received messages sent by a client to request addresses or configuration settings from a server.
DHCPv6 Reply	Number of received messages sent by a DHCPv6 server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Inform	Number of received messages sent by a client to request configuration settings (but not addresses).
DHCPv6 Confirm	Number of received messages sent by a client to all servers to determine if a client's configuration is valid for the connected link.

Table 2-27 Received Message Statistics

Parameter	Description
DHCPv6 Renew	Number of received messages sent by a client to a server to extend the lifetime of assigned addresses and obtain updated configuration settings.
DHCPv6 Rebind	Number of received messages sent by a client to any server when a response to the DHCPv6 Renew message is not received.
DHCPv6 Release	Number of received messages sent by a server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Decline	Number of received messages sent by a client to a server to indicate that the assigned address is already in use.
DHCPv6 Reconfigure	Number of received messages sent by a server to a client to indicate that the server has new or updated configuration settings.
DHCPv6 Relay Forward	Number of received messages sent by a relay agent to forward a message to a server. Contains a client message encapsulated as the DHCPv6 Relay-Message option.
DHCPv6 Relay Reply	Number of received messages sent by a server to send a message to a client through a relay agent. Contains a server message encapsulated as the DHCPv6 Relay-Message option.

Bridged Messages

Table 2-28 Bridged Message Statistics

Parameter	Description
NDP Router Solicitation	Number of received bridged messages originated by the hosts to request a router to send a router advertisement.
NDP Router Advertisement	Number of received bridged messages originated by the routers to advertise their presence and link specific parameters such as link prefixes, link MTU, and hop limits. These messages are sent periodically and also in response to Router Solicitation messages.
NDP Neighbor Solicitation	Number of received bridged messages originated by the nodes to request another node's link layer address and also for functions such as duplicate address detection and neighbor unreachability detection.
NDP Neighbor Advertisement	Number of received bridged messages in response to Neighbor Solicitation messages. If a node changes its link-layer address, it can send an unsolicited Neighbor Advertisement to advertise the new address.

Table 2-28 Bridged Message Statistics

Parameter	Description
NDP Redirect	Number of received bridged messages to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor.
NDP Certificate Solicit	Number of received bridged messages to know the certification path to the trust anchor. Hosts will send the Certification Path Solicitations.
NDP Certificate Advert	Number of received bridged messages to know the certification path to the trust anchor. Routers will send the Certification Path Advertisement messages.
DHCPv6 Solicitation	Number of received bridged messages sent by a client to locate DHCPv6 servers.
DHCPv6 Advertisement	Number of received bridged messages sent by a DHCPv6 server in response to a DHCPv6 Solicitation message to indicate availability.
DHCPv6 Request	Number of received bridged messages sent by a client to request addresses or configuration settings from a server.
DHCPv6 Reply	Number of received bridged messages sent by a DHCPv6 server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Inform	Number of received bridged messages sent by a client to request configuration settings (but not addresses).
DHCPv6 Confirm	Number of received bridged messages sent by a client to all servers to determine if a client's configuration is valid for the connected link.
DHCPv6 Renew	Number of received bridged messages sent by a client to a server to extend the lifetime of assigned addresses and obtain updated configuration settings.
DHCPv6 Rebind	Number of received bridged messages sent by a client to any server when a response to the DHCPv6 Renew message is not received.
DHCPv6 Release	Number of received bridged messages sent by a server to a client in response to a DHCPv6 Solicitation, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Decline	Number of received bridged messages sent by a client to a server to indicate that the assigned address is already in use.
DHCPv6 Reconfigure	Number of received bridged messages sent by a server to a client to indicate that the server has new or updated configuration settings. The client then sends either a Renew or Information-Request message.

Table 2-28 Bridged Message Statistics

Parameter	Description
DHCPv6 Relay Forward	Number of received bridged messages sent by a relay agent to forward a message to a server. Contains a client message encapsulated as the DHCPv6 Relay-Message option.
DHCPv6 Relay Reply	Number of received bridged messages sent by a server to send a message to a client through a relay agent. Contains a server message encapsulated as the DHCPv6 Relay-Message option.

Dropped Messages

Table 2-29 Dropped Message Statistics

Parameter	Description
NDP RS Drop (Router Solicitation)	Number of messages dropped that are originated by the hosts to request a router to send a Router Advertisement.
NDP RA Drop (Router Advertisement)	Number of messages dropped that are originated by the routers to advertise their presence and link-specific parameters such as link prefixes, link MTU, and hop limits. These messages are sent periodically and also in response to Router Solicitation messages.
NDP NS Drop (Neighbor Solicitation)	Number of messages dropped that are originated by the nodes to request another node's link layer address and also for functions such as duplicate address detection and neighbor unreachability detection.
NDP NA Drop (Neighbor Advertisement)	Number of messages dropped in response to Neighbor Solicitation messages. If a node changes its link-layer address, it can send an unsolicited Neighbor Advertisement to advertise the new address.
DHCPv6 Solicitation	Number of messages dropped that are sent by a client to locate DHCPv6 servers.
DHCPv6 Advertisement	Number of messages dropped that are sent by a DHCPv6 server in response to a DHCPv6 Solicitation message to indicate availability.
DHCPv6 Reply	Number of messages dropped that are sent by a DHCPv6 server to a client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Inform	Number of messages dropped that are sent by a client to request configuration settings (but not addresses).

NDSUPRRESS Drop Counters

Table 2-30 NDSUPRESS Drop Counter Statistics

Parameter	Description
total	Total number of NDSUPRESS dropped messages.
silent	Number of silently dropped messages.
ns_in_out	Number of Neighbor Solicitation (NS) owner messages on the input interface.
ns_dad	Number of NS Duplicate Address Detection (DAD) messages suppressed.
unicast	Number of NS unicast messages suppressed.
multicast	Number of NS multicast messages suppressed.
internal	Number of internal failure messages.

SNOOPING Drop Counters

Table 2-31 SNOOPING Drop Counter Statistics

Parameter	Description
Dropped Messages	Name of the dropped messages.
total	Total number of dropped messages.
silent	Number of silently dropped messages.
internal	Number of internal failure messages.
CGA_vfy	Number of messages where Cryptographically Generated Address (CGA) option is not getting verified.
RSA_vfy	Number of messages where RSA signature is not getting verified.
limit	Number of messages in which the address limit is reached.
martian	Number of Martian packets. A Martian packet is an IP packet which specifies a source or destination address that is reserved for special-use by Internet Assigned Numbers Authority (IANA) and cannot actually originate as claimed or be delivered. Martian packets commonly arise from IP address spoofing in denial-of-service attacks, but can also arise from network equipment malfunction or misconfiguration of a host.
martian_mac	Number of Martian MAC packets.
no_trust	Number of packets marked for detection of policy and collision.

Table 2-31 SNOOPING Drop Counter Statistics

Parameter	Description
not_auth	Number of packets that are not authorized on port.
stop	Number of packets that are accepted, but not forwarded.

CacheMiss Statistics

Table 2-32 CacheMiss Statistics

Parameter	Description
Multicast NS Forwarded	Total number of NS-forwarded multicast messages.
Multicast NS Dropped	Total number of NS-dropped multicast messages.

Click **Clear Count** to set all IPv6 Neighbor Bind Counter statistics to zero.

PMIPv6 LMA Statistics

Choose **MONITOR > Statistics > PMIPv6 LMA Statistics** to navigate to the PMIPv6 LMA Statistics page.

This page enables you to view the statistics of all the LMA (Local Mobility Anchor) that the controller is connected to. This table describes the LMA statistics.

Table 2-33 LMA Statistics

Parameter	Description
LMA Name	Name of the LMA.
Total Bindings	Total number of binding updates sent to the LMA by the controller.
PBU Sent	Total number of Proxy Binding Updates (PBUs) sent to the LMA by the controller. PBU is a request message sent by the Mobile Access Gateway (MAG) to a mobile node's LMA for establishing a binding between the mobile node's interface and its current care-of address (Proxy-CoA).
PBA Received	Total number of Proxy Binding Acknowledgements (PBAs) received by the controller for the LMA. PBA is a reply message sent by an LMA in response to a PBU message that it received from a MAG.
PBRI Sent	Total number of Proxy Binding Revocation Indications (PBRIs) sent by the controller to the LMA.

Table 2-33 LMA Statistics

Parameter	Description
PBRI Received	Total number of PBRIs received from the LMA by the controller.
PBRA Sent	Total number of Proxy Binding Revocation Acknowledgements (PBRAs) sent by the controller to the LMA.
PBRA Received	Total number of PBRAs received from the LMA by the controller.
Number of Handoff	Number of handoffs between the controller and the LMA.
PBU Dropped	Number of PBUs dropped between the controller and the LMA.

Preferred Mode

Choose **MONITOR > Statistics > Preferred Mode** to navigate to the Preferred Mode Statistics page.

This page enables you to view the details of the APs on which the IP config (Global/ AP Group) has been configured.

Table 2-34 Preferred Mode Statistics

Parameter	Description
Prefer Mode of Global/AP Groups	The name of the AP that is configured with either IPv4, IPv6 or global.
Total	The total count of APs configured with preferred mode.
Success	Counts the number of times the AP was successfully configured with the preferred mode.
Unsupported	The number of APs that are not supported with the controller.
Already Configured	Counts the attempts made to configure an already configured AP.
Per AP Group Configured	Preferred mode configured on per AP group
Failure	Counts the number of times the AP was failed to get configured with the preferred mode.

Optimized Roaming

Choose **MONITOR > Statistics > Optimized Roaming** to navigate to the **Optimized Roaming Statistics** page.

The **Optimized Roaming Statistics** page provides statistics related to disassociations and rejections on 802.11a and 802.11b radios.

Cisco Discovery Protocol

Choose **MONITOR > CDP** to navigate to the CDP page. From here, you can choose the following:

- **MONITOR > CDP > Interface Neighbors** to view a list of all CDP neighbors on all interfaces.
  See CDP Interface Neighbors for more information.
- **MONITOR > CDP > AP Neighbors** to view a all access points with CDP neighbors.
  See CDP AP Neighbors for more information.
- **MONITOR > CDP > Traffic Metrics** to display CDP traffic information.
  See CDP Traffic Metrics for more information.

CDP Interface Neighbors

Choose **MONITOR > CDP > Interface Neighbors** to navigate to the CDP Interface Neighbors page.

This page enables you to view a list of all Cisco Discovery Protocol neighbors on all interfaces.

This table describes the CDP interface neighbor parameters.

Table 2-35 CDP Interface Neighbor Parameters

Parameter	Description
Local Interface	Local interface name.
Neighbor Name	Name of each CDP neighbor.
Neighbor Address	IPv4 or IPv6 address of the CDP neighbor.
Neighbor Port	IP address of each CDP neighbor.
TTL	Time left (in seconds) before each CDP neighbor entry expires.
Capability	Functional capability of each CDP neighbor: • R—Router • T—Trans Bridge • B—Source Route Bridge • S—Switch • H—Host • I—IGMP • r—Repeater • M—Remotely Managed Device
Platform	CDP neighbor device platform.

CDP Interface Neighbors Details

Choose **MONITOR > CDP > Interface Neighbors**, and then click the neighbor name for the desired interface to view the CDP Interface Neighbors Details page. This page enables you to view detailed information about the Cisco Discovery Protocol neighbor of each interface.

Table 2-36 CDP Neighbor Detail Parameters

Parameter	Description
Local Interface	controller port on which the CDP packets were received.
Neighbor Name	Name of the CDP neighbor.
Neighbor Address	IPv4 or IPv6 address of the CDP neighbor.
Neighbor Port	Port used by the CDP neighbor for transmitting CDP packets.
Duplex	Duplex type of the CDP neighbor.
Advt Version	CDP version being advertised (v1 or v2).
TTL	Time left (in seconds) before the CDP neighbor entry expires.
Capability	Functional capability of the CDP neighbor: • Router • Trans Bridge • Source Route Bridge • Switch • Host • IGMP • Repeater • Remotely Managed Device
Platform	Hardware platform of the CDP neighbor device.
Software Version	Software running on the CDP neighbor.

CDP AP Neighbors

Choose **MONITOR > CDP > AP Neighbors** to navigate to the AP Neighbors page. This page enables you to view a list of all access points with CDP neighbors.

Table 2-37 CDP AP Neighbor Details

Parameter	Description
AP Name	Access point name.
CDP Neighbors	CDP neighbor name.

Click **CDP Neighbors** to view the CDP neighbors for the access points that are connected to the controller in the CDP Neighbors page.

CDP Neighbors

Choose **MONITOR > CDP > AP Neighbors** and then click **CDP Neighbors** for an access point to navigate to the CDP Neighbors page. This page enables you to view the CDP neighbors for the access points that are connected to the controller.

Table 2-38 AP Neighbor Parameters

Parameter	Description
AP Name	Access point name.
AP IP Address	IP address of the access point.
Neighbor Name	Name of the neighbor.
Neighbor Address	IP address of the neighbor.
Neighbor Port	Port number of the neighbor.
Advt Version	Advertised CDP version (v1 or v2).

CDP Neighbors Details

Choose **MONITOR > CDP > AP Neighbors**, and then click the access point name for the desired access point and view the CDP AP Neighbors Details page. This page enables you to view to see more detailed information about an access point's CDP neighbor.

The following AP neighbor details are displayed:

- AP Name—The name of the access point
- Basic Radio MAC—The MAC address of the access point's radio
- AP IP Address—The IP address of the access point
- Local Interface—The interface on which the CDP packets were received
- Neighbor Name—The name of the CDP neighbor
- Neighbor Address—The IPv4 and IPv6 address of the CDP neighbor
- Neighbor Port—The port used by the CDP neighbor
- Advt Version—The CDP version being advertised (v1 or v2)
- TTL—The time left (in seconds) before the CDP neighbor entry expires
- Capability—The functional capability of the CDP neighbor:
  - Router
  - Trans Bridge
  - Source Route Bridge
  - Switch
  - Host
  - IGMP
  - Repeater
  - Remotely Managed Device
- Platform—The hardware platform of the CDP neighbor device

- Software Version—The software running on the CDP neighbor

CDP Traffic Metrics

Choose **MONITOR > CDP > Traffic Metrics** to navigate to the CDP Traffic Metrics page. This page displays CDP traffic information.

Table 2-39 CDP Traffic Metrics

Parameter	Description
Packets In	Number of CDP packets received by the controller.
Packet Out	Number of CDP packets sent from the controller.
Checksum Errors	Number of packets that experienced a checksum error.
No Memory Errors	Number of packets dropped due to insufficient memory.
Invalid Packets	Number of invalid packets.

Rogues

Choose **MONITOR > Rogues** to navigate to the Rogues page. From here, you can choose the following:

- **MONITOR > Rogues > Friendly APs** to view rogue access points that are classified as Friendly.

  See Friendly Rogue APs for more information.
- **MONITOR > Rogues > Malicious APs** to view rogue access points that are classified as Malicious.

  See Malicious Rogue APs for more information.
- **MONITOR > Rogues > Custom APs** to view rogue access points that are classified as Custom.

  See Custom Rogue APs for more information.
- **MONITOR > Rogues > Unclassified APs** to view rogue access points that are unclassified.

  See Unclassified Rogue APs for more information.
- **MONITOR > Rogues > Rogue Clients** to view information about rogue clients that are detected.

  See Rogue Clients for more information.
- **MONITOR > Rogues > Adhoc Rogues** to view information about ad-hoc rogue clients that are detected.

  See Adhoc Rogues for more information.
- **MONITOR > Rogues > Rogue AP ignore-lists** to view the MAC addresses of access points that are configured to be ignored.

  See Rogue AP Ignore-list for more information.

Filtering AP Results by MAC Address

The rogue AP search results can be filtered by AP MAC address. This filter is available on all the **Monitor > Rogue** pages.

Step 1 Click **Change Filter**.

Step 2 Check the **MAC Address** check box.

Step 3 Enter the AP MAC address in the box.

Step 4 Click **Apply.**

Friendly Rogue APs

Choose **MONITOR > Rogues > Friendly APs** to navigate to the Friendly Rogue APs page.

This page displays rogue access points that are classified as Friendly.

Table 2-40 Friendly Rogue Access Point Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID that is broadcast by the rogue access point radio.
Channel	Channel number of the access point that has detected this friendly rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of this radio relative to the network or controller. The status of rogue access point radios is one of the following: • Internal—The unknown access point is inside the network and poses no threat to WLAN security. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. For example, the access points belonging to a neighboring coffee shop are external rogue access points. • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list.

This page reports rogue access points until the “Expiration Timeout for Rogue AP Entries” (set on the Friendly Rogues page) expires.

The MAC address links in on this page take you to the respective Rogue AP Detail page when selected.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove Selected**.

To remove all access points, select the check box in the table header row and access points are automatically selected. Click **Remove Selected**.

Malicious Rogue APs

Choose **MONITOR > Rogues > Malicious APs** to navigate to the Malicious Rogue APs page.

This page displays the rogue access points that are classified as Malicious. This page reports rogue access points until the "Expiration Timeout for Rogue AP Entries" (set on the Friendly Rogues page) expires.

The MAC address links in the rogue access point radios table take you to the respective Rogue AP Detail page when selected.

To remove a rogue access point from the list, click the blue arrow adjacent the desired rogue access point and choose **Remove**.

Table 2-41 Malicious Rogue Access Point Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID being broadcast by the rogue access point radio.
Channel	Channel number of the access point that has detected this rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of the radio relative to the network or controller. The status of rogue access point radios is one of the following: • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. • Threat—The unknown access point is found to be on the network and poses a threat to WLAN security. • Contained—The unknown access point is contained. • Containment Pending—The unknown access point is marked "Contained," but the action is delayed due to unavailable resources.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove**.

To move the Malicious rogue APs that are being contained or were contained back to Alert state, click **Move to Alert** button on the respective pages.

To remove all access points, select the check box in the table header row. All access points are automatically selected. Click **Remove**.

Custom Rogue APs

Choose **MONITOR > Rogues > Custom APs** to navigate to the Custom Rogue APs page.

This page displays rogue access points that are classified as Custom.

Table 2-42 Custom Rogue Access Point Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID that is broadcast by the rogue access point radio.
Channel	Channel number of the access point that has detected this friendly rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of this radio relative to the network or controller. The status of rogue access point radios is one of the following: • Internal—The unknown access point is inside the network and poses no threat to WLAN security. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. For example, the access points belonging to a neighboring coffee shop are external rogue access points. • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list.

This page reports rogue access points until the Expiration Timeout for Rogue AP Entries (set on the Friendly Rogues page) expires.

The MAC address links in on this page take you to the respective Rogue AP Detail page when selected.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove**.

To remove all access points, select the check box in the table header row and access points are automatically selected. Click **Remove**.

Unclassified Rogue APs

Choose **MONITOR > Rogues > Unclassified APs** or **MONITOR > Summary** and click **Active Rogue APs** under the Rogue Summary section to navigate to the Unclassified Rogue APs page.

This page reports rogue access points until the expiration timeout for rogue AP entries (set on the Friendly Roguespage) expires. The MAC address links in the rogue access point radios table take you to the respective Rogue AP Detail page when selected.

To remove a rogue access point from the list, click the blue arrow adjacent the desired rogue access point and choose **Remove**.

This page displays rogue access points that did not match the Malicious or Friendly rules.

Table 2-43 Rogue Access Point Radio Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
SSID	SSID being broadcast by the rogue access point radio.

Table 2-43 Rogue Access Point Radio Parameters

Parameter	Description
Channel	Channel number of the access point that has detected this unclassified rogue access point.
# Detecting Radios	Number of Cisco Radios that detect the rogue access point radio.
Number of Clients	Number of clients associated with the rogue access point.
Status	Automatic and configurable state of this radio relative to the network or controller. The status of rogue access point radios is one of the following: • Pending—On first detection, the unknown access point is put in the "Pending" state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point. • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained. • Containment Pending—The unknown access point is marked "Contained," but the action is delayed due to unavailable resources.

To remove rogue access points from the list, select the check boxes that correspond to the access point and click **Remove**.

To move the Malicious rogue APs that are being contained or were contained back to Alert state, click **Move to Alert** button on the respective pages.

To remove all access points, select the check box in the table header row. All access points are automatically selected. Click **Remove**.

Rogue AP Detail

Choose **MONITOR > Summary**, click **Detail** in the Active Rogue APs row of the Rogue Summary section, and then click the MAC address of the AP to navigate to the Rogue AP Detail page.

This page displays the access point details of the unauthorized or unknown radio. This table describes the new rule parameters.

Rogue Access Point Radio Details

Table 2-44 Rogue Access Point Radio Details

Parameter	Description
MAC Address	MAC address of the rogue access point.
Type	Rogue access point type: • AP—Infrastructure access point • Ad Hoc—Client-to-Client
Is Rogue on Wired Network?	Yes or No. Unknown if WEP is enabled, as shown below on this page.

Table 2-44 Rogue Access Point Radio Details

Parameter	Description
First Time Reported On	Date and time that the radio was first scanned by the controller.
Last Time Reported On	Date and time that the radio was last scanned by the controller.
Classification Change By	Classification of the rogue access point either manually, by default, or by rogue rule.
Class Type	Class of this radio as follows: • Friendly—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained. • Malicious—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the "Friendly" or "Unclassified" classification type. **Note** Once an access point is classified as "Malicious," you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the "Unclassified" classification type, you must delete the access point and allow the controller to reclassify it. • Unclassified—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the "Friendly" or "Malicious" classification type automatically in accordance with user-defined rules or manually by the user. • Custom—An unknown access point that matches the user-defined classification type.
Manually Contained	Whether the rogue is manually contained or automatically contained.
State	Status of this radio as follows: • Alert • Internal • External • Contain • Pending

Table 2-44 Rogue Access Point Radio Details

Parameter	Description
Update Status[1]	Configurable state of this rogue access point in the controller. You may set the status to one of the following: • Internal—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly. • External—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly. • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified. • Alert—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.
Maximum number of APs to contain this rogue	Maximum number of access points used to contain this rogue (1, 2, 3, or 4).

1. Do not attempt to contain rogue access points operated by other establishments, such as the cafe hotspot across the street.

APs that Detected this Rogue

Table 2-45 APs that Detected this Rogue

Parameter	Description
Base Radio MAC	MAC address of the Cisco access point that identified the rogue access point radio.
AP Name	Name of the Cisco access point that identified the rogue access point radio.
SSID	SSID being broadcast by the rogue access point radio.
Channel	Channel the rogue access point is broadcasting on.
Channel Width (Mhz)	Channel bandwidth: 20 MHz or 40 MHz.
Radio Type	Protocol of the rogue access point that is either 802.11a, 802.11b, 802.11g, or 802.11n.
WEP	Whether WEP is enabled or disabled.
WPA	Type of security protocol is Enabled or Disabled.
Pre-Amble	Preamble type of the AP that detected this rogue.

Table 2-45 APs that Detected this Rogue

Parameter	Description
RSSI	Receive signal strength indicator (RSSI) of rogue access point radio at the access point. If RSSI indicates –80 dBm or lower, the rogue access point is far away or transmitting at a low signal strength. If RSSI indicates –60 dBm or higher, the rogue access point is close and/or transmitting at a high signal strength.
SNR	Signal to noise ratio (SNR) of rogue access point radio at the access point.
Containment Type	Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status Maximum Number; otherwise this field is blank.
Containment Channel	Current channel or channels if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status; otherwise this field is blank.

Clients Associated with this Rogue AP

Table 2-46 Clients Associated with this Rogue AP

Parameter	Description
MAC Address	MAC address of the rogue client.
Last Time Heard	Last time the Cisco access point detected the rogue access point client.

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

Rogue Clients

Choose **MONITOR > Rogues > Rogue Clients** or **MONITOR > Summary** and click **Detail** in the Active Rogue Clients row of the Rogue Summary section to view the Rogue Clients page. This page displays information about rogue clients that are detected.

Table 2-47 Rogue Client Parameters

Parameters	Description
MAC Address	MAC address of the rogue client.
AP MAC Address	MAC address of the Cisco access point.
SSID	Service Set Identifier being broadcast by the rogue client.

Table 2-47 Rogue Client Parameters

Parameters	Description
# Detecting Radios	Number of Cisco radios detecting the rogue client.
Last Seen On	Last time that the Cisco access point detected the rogue access point client.
Status	Configurable state of this radio relative to the network or controller: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action.
Wired	Whether the client is on a wired network or not.

Rogue Client Details

Choose **MONITOR > Rogues > Rogue Clients** and then click the MAC address link to navigate to the Rogue Client Details page. This page displays details of unauthorized clients.

Rogue Client Details

Table 2-48 Rogue Client Detail Parameters

Parameter	Description
MAC Address	MAC address of the rogue access point.
APs MAC Address	MAC address of the Cisco access point that identified the rogue access point radio.
Radio Type	
SSID	SSID being broadcast by the rogue access point radio.
IP Address	IPv4 or IPv6 address of the rogue client or Unknown.
First Time Reported On	Date and time that the radio was first scanned by the controller.
Last Time Reported On	Date and time that the radio was last scanned by the controller.
State	Status of this radio is as follows: • Contain • Alert
Update Status[1]	Configurable state of this rogue access point in the controller. You may set the status to one of the following: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action.

1. Do not attempt to contain rogue access points operated by other establishments, such as the cafe hotspot across the street!

APs that Detected this Rogue Client

Table 2-49 APs Detected Rogue Clients Parameters

Parameter	Description
Base Radio MAC	MAC of the access point.
AP Name	Access points that identified the rogue access point radio.
Channel	Channel that the access point is broadcasting on.
Radio Type	Protocol of the rogue access point is either 802.11a, 802.11b, 802.11g, 802.11n, or Unknown.
RSSI	Receive signal strength indicator (RSSI) of access point radio at the access point. –80 dBm or lower, the rogue access point is far away or transmitting at a low signal strength. –60 dBm or higher, the rogue access point is close and/or transmitting at a high signal strength).
SNR	Signal to noise ratio (SNR) of the access point.

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

Click **Ping** to send a ping to a network element.

Adhoc Rogues

Choose **MONITOR > Rogues > Adhoc Rogues** or **MONITOR > Summary** and click **Detail** in the Adhoc Rogues row of the Rogue Summary section to navigate to the Adhoc Rogues page. You can see details of friendly, malicious, custom, and unclassified ad-hoc rogues in separate pages.

Table 2-50 Adhoc Rogues Parameters

Parameters	Description
MAC Address	MAC address of the rogue client.
BSSID	MAC address of the Cisco access point.
SSID	SSID that is broadcast by the rogue client.

Table 2-50 Adhoc Rogues Parameters

Parameters	Description
# Detecting Radios	Number of Cisco Radios that detect the rogue client.
Status	Status of this radio as follows: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action. • Internal—The controller trusts this rogue access point. • External—The controller acknowledges the presence of this rogue access point.

Adhoc Rogue Details

Choose **MONITOR > Rogues > Adhoc Rogues** and click the MAC address link in the ad-hoc rogue table to navigate to the Adhoc Rogues Details page.

This page displays details about ad-hoc rogue access points.

Adhoc Rogues

Table 2-51 Adhoc Rogues Details Parameters

Parameters	Description
MAC Address	MAC address of the ad-hoc rogue.
BSSID	BSSID of the ad-hoc rogue.
First Time Reported On	Date and time that the rogue was first scanned by the controller.
Last Time Reported On	Date and time that the rogue was last scanned by the controller.
Classification Change By	Classification of the rogue access point either manually, by default, or by rogue rule.
Classified by AP	MAC address of the access point that classified the rogue access point.
Classified RSSI	RSSI of the rogue access point.
Rule Name	Name of the custom rogue rule.
Severity Score	Custom classification severity score for the rogue rule. The range is from 1 to 100.
State Change By	Cause of the state change of the rogue access point.

Table 2-51 Adhoc Rogues Details Parameters

Parameters	Description
Class Type	Classification type of the rogue access point. It can be one of the following: • Friendly—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained. • Malicious—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the "Friendly" or "Unclassified" classification type. **Note** Once an access point is classified as "Malicious," you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the "Unclassified" classification type, you must delete the access point and allow the controller to reclassify it. • Unclassified—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the "Friendly" or "Malicious" classification type automatically in accordance with user-defined rules or manually by the user. • Custom—An unknown access point that matches the user-defined classification type.
State	Current state of this rogue access point in the controller. It can be one of the following: • Internal—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly. • External—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly. • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified. • Alert—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

Table 2-51 Adhoc Rogues Details Parameters

Parameters	Description
Update Status[1]	Configurable state of this rogue access point in the controller. You may set the status to one of the following: • Contain—The controller contains the offending device so that its signals no longer interfere with authorized clients. • Alert—The controller forwards an immediate alert to the system administrator for further action. • Internal—The controller trusts this rogue access point. • External—The controller acknowledges the presence of this rogue access point.
Maximum number of APs to contain this rogue	Maximum number of access points used to contain this rogue (1, 2, 3, or 4).

1. Do not attempt to contain rogue access points operated by other establishments, such as the cafe hotspot across the street!

APs that Detected this Rogue

Table 2-52 AP Detected Rogue Parameters

Parameter	Description
Base Radio MAC	MAC of the access point.
AP Name	Access points that identified the access point radio.
SSID	SSID of the access point.
Channel	Channel on which the rogue access point is broadcasting.
Radio Type	Protocol of the rogue access point that is either 802.11a, 802.11b, 802.11g, 802.11n, or Unknown.
WEP	Whether WEP is enabled on the access point.
WPA	Whether WPA is enabled on the access point.
Pre-Amble	Preamble type of either Long or Short.
RSSI	RSSI of the access point.
SNR	Signal to noise ratio (SNR) of the access point at the Cisco access point.
Containment Type	Type of containment.
Containment Channels	Channels on which the access point contained the ad-hoc rogue.

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

Rogue AP Ignore-list

Choose **MONITOR > Rogues > Rogue AP ignore-list** to navigate to the **Rogue AP Ignore-list** page.

This page shows the MAC addresses of any access points that are configured to be ignored.

The rogue-ignore list contains a list of any autonomous access points that have been manually added to Prime Infrastructure (PI) maps by PI users. The controller regards these autonomous access points as rogues even though Prime Infrastructure is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

- When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
- If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
- If the unknown access point is not in the rogue-ignore list, the controller sends a trap to PI . If PI finds this access point in its autonomous access point list, PI sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
- If you remove an autonomous access point from the PI, the PI sends a command to the controller to remove this access point from the rogue-ignore list.

Redundancy

Choose **MONITOR > Redundancy** to view information about redundancy. The available options are as follows:

- To view redundancy statistics, choose **MONITOR > Redundancy > Statistics**.

  See Redundancy Statistics more information.
- To view redundancy peer statistics, choose **MONITOR > Redundancy > Peer Statistics**.

  See
- To view the redundancy summary, choose **MONITOR > Redundancy > Summary**.

  See Redundancy Summary more information.

Redundancy Statistics

Choose **MONITOR > Redundancy > Statistics** to navigate to the Redundancy Statistics page.

This page displays information about the redundancy statistics.

Note You can view the redundancy statistics only if the SSO mode is enabled.

Table 2-53 Redundancy Statistics

Parameter	Description
Category	Drop down box from which you can select one of the following category: • All • Infra • Transport • Keepalive • GW-Reachability • Config-Sync • None
RF Client Brief	Displays the RF Clients list.
Sanity Counters	
Sanity Messages successfully sent	Displays the number of Sanity messages i.e. health check messages sent from this box.
Sanity Messages failed to send	Displays the number of Sanity messages failed to send from the controller.
Sanity Messages received from peer	Displays the number of Sanity messages received from the Peer WLC.
Transport Counters	
Number of messages in the hold Queue	Displays information about number of IPC messages in queue.
Application message Max Size	Displays information about number of IPC messages in queue.
IPC message Max Size	Displays maximum supported MTU size IPC messages.
Time to hold IPC messages	Displays maximum time to hold the IPC messages if the IPC buffer is not full.
IPC sequence number in the TX side	Displays IPC sequence number in the transmitter window.
IPC sequence number in the RX side	Displays IPC sequence number in the receiver window.
IPC sequence number mismatches (Low)	Displays low watermark of IPC sequence number mismatches.
IPC sequence number mismatches (high)	Displays high watermark of IPC sequence number mismatches.
Keepalive Counters	
Keep Alive Request Received	Displays the number of Keep Alive request received from the peer through RP.
Keep Alive Responses Received	Displays the number of Keep Alive response received from the peer through RP.
Keep Alive Request Sent	Displays the number of Keep Alive Requests sent to peer.

Table 2-53 Redundancy Statistics

Parameter	Description
Keep Alive Response Sent	Displays the number of Keep Alive Responses sent from the controller.
Keep Alive Requests failed to send	Displays the number of Keep Alive Requests failed to send from the controller.
Keep Alive Responses to failed to send	Displays the number of Keep Alive Responses failed to send from the controller.
Number of times two Keep alives are lost consecutively	Displays the number of times 2 keepalives are lost consecutively. i.e twice did not get the response for keep alive requests.
Network Latencies (RTT) for the Peer Reachability in microsec	
Peer Reachability Latency	Displays the latency between peers through RMI.
Gx Reachability	
Gw Pings Succesfully sent	Displays the number of Pings successfully sent to Gateway from the controller.
Gw Pings Failed to send	Displays the number of Pings failed to send to Gateway from the controller.
Gw Responses Received	Displays the number of Pings successfully received from the Gateway to the controller.
Current consecutive Gw Responses Lost	Displays the number of consecutive GW responses lost i.e number of consecutive responses not received.
High Water Mark of Gw Responses Lost	Displays the highest consecutive GW responses lost to the controller.
Network Latencies (RTT) for the Management Gateway Reachability in microsec	
Gateway Reachability Latency	Displays the latency between the controller and the GW.
Ping Request and Response	
Ping Requests sent to Peer	Displays the number of ping requests sent to peer through RMI.
Ping Response received from Peer	Displays the number of ping responses received from the peer through RMI.
Config Sync Counter	
Usmdb Functions sent for Sync	Displays the total number of Usmdb functions sent for Sync to Standby
Failed sync for Usmdb Sync	Displays the total number of Usmdb functions failed to send for Sync to Standby.
UsmDbs which failed to sync from Active to Standby	
Index	Displays the index of UsmDb failed to sync.
Failed UsmDb	Displays the information about the UsmDb that is failed to sync to standby.
Port Information	

Table 2-53 Redundancy Statistics

Parameter	Description
Local Physical Ports	Indicate the ports that are operationally up in the controller.
Peer Physical Ports	Indicate the ports that are operationally up in the peer controller.

Peer Statistics

Choose **MONITOR > Redundancy > Peer Statistics** to navigate to the Peer Statistics page.

The CPU and memory statistics of all the threads of the standby WLC are synchronized with the active controller every 10 seconds. This information is displayed when you query for the peer statistics on the active WLC.

This page displays the following information:

- Peer-System statistics
- Peer-Process CPU statistics
- Peer-Process Memory statistics

Redundancy Summary

Choose **MONITOR > Redundancy > Summary** to navigate to the Redundancy Summary page.

This page displays information about the Redundancy Facilitator states on the active and peer unit in the redundancy mode and the switch of activity (swact).

Table 2-54 Redundancy Facilitator Summary

Parameter	Description
Local State	Current state of the Redundancy Facilitator of the controller. It can be Active, Standby HOT, or Standby COLD.
Peer State	Current state of the Redundancy Facilitator of the peer controller. It can be Active, or Standby HOT, or Standby COLD.
Unit	Type of controller that can be primary or secondary.
Unit ID	Unique ID of the redundant unit. It can be the MAC address of the controller.
Redundancy State	Redundancy mode operational on the controller. The redundancy modes are as follows: • 0—No redundancy • SSO—Hot Standby Mode • RPR—Cold Standby Mode
Maintenance Mode	Maintenance mode that can be enabled or disabled. Indicates if the redundant units can communicate synch messages with each other. If the controllers cannot reach each other through the redundant port or through the Redundant Management Interface, the standby controller goes into the maintenance mode.

Table 2-54 Redundancy Facilitator Summary (continued)

Parameter	Description
Maintenance Cause	Cause of the switchover to the maintenance mode.
Average Redundancy Peer Reachability Latency	Average delay to reach the peer controller in seconds.
Average Management Gateway Reachability Latency	Average delay to reach the management gateway in seconds.
BulkSync Status	Indicates whether the bulk sync is completed once the Standby boots up and moves to STANDBY HOT state. This can be: • In-Progress • Pending and • Complete

Redundancy Detail

Choose **MONITOR > Redundancy > Detail** to navigate to the Redundancy details page.

Table 2-55 Redundancy Detail Parameters

Parameter	Description
Redundancy Management	This is the IP address of Redundancy Management Interface of the controller.
Peer Redundancy Management	This is the IP address of the Redundancy Management Address of the Peer controller.
Redundancy port IP	This is the IP address of the Redundancy Port of the controller.
Peer Redundancy port IP	This is the IP address of the Redundancy Port of the Peer controller.
Peer Service Port IP	This is the IP address of the Service port of the Peer controller.
Switchover History Table	
Previous Active	Information about controller that was previously Active before Switchover. This will have the RMI IP of previous Active.
Current Active	Information about controller that was currently Active after Switchover. This will have the RMI IP of current Active.
Switchover Reason	Information about the switchover reason whether it is User initiated, GW not reachable or Active Failed.
Switchover Time	Information about when the switchover has happened.
Redundancy Timeout Values	
Keep Alive TimeOut	Information about the timeout the controller can wait for Keep Alive responses before considering keep alive is lost.
Peer Search TimeOut	Information about the timeout the controller can wait for peer search responses before considering peer is not reachable.
Network Routes Peer	

Table 2-55 Redundancy Detail Parameters (continued)

Parameter	Description
Number of Routes	Total number of Network Routes this controller holds.
IP Address	IP address of target network/IP address.
IP Netmask	IP network mask information of the routes of this controller.
Gateway IP Address	Information about the next hop gateway for this route.

Clients

Choose **MONITOR > Clients** or **MONITOR > Summary** and click **Detail** in the row that corresponds to Current Clients in the Client Summary section to navigate to the Clients page.

This page displays information about the clients associated with the access points.

Client List Filter

You can create a filter to display the client list by MAC address or a combination of access point name, WLAN profile name, status, radio type, workgroup bridge (WGB), or PMIP.

Note When you enable the MAC address filter, other filter options are disabled.

When you enable the AP name, WLAN profile name, status, radio type, or workgroup bridge (WGB) filter, the MAC address filter is disabled.

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

Click **Change Filter** to display the Search Clients dialog box (see the following figure) and to create or change filter parameters. Click **Show All** to remove the filter and display the entire client list.

- MAC Address—MAC address that you enter as 6 two-digit hexadecimal numbers separated by colons (for example, 01:23:45:67:89:AB).
- IP Address—IP address of the client.
- AP Name—Access point name.
- User Name—Username associated with the client.
- WLAN Profile—WLAN profile name. You can select a WLAN profile by selecting one of the configured WLANs on your wireless network.
- WLAN SSID—SSID of the WLAN that the client is associated with.
- Status—One or more status types: Associated, Authenticated, Excluded, Idle.
- Radio Type—802.11a, 802.11b, 802.11g, 802.11an, 802.11bn, Mobile radio type.
- WGB—WGB wired clients that are associated with the access points.
- Apply—Filter settings.

Client Information Table

This table displays a list of all clients attached to the controller. Client information includes the following:

- Client MAC Addr—MAC address of the client.
- IP Address—IP address of the client.
- AP Name—Name of the access point.
- WLAN Profile—Name of the WLAN used by the client.
- WLAN SSID—SSID of the WLAN that the client is associated with.
- User Name—Username associated with the client.
- Protocol—Remote LAN clients that shows Ethernet as the protocol.
- Status—Status of the client connection.
- Auth—Authorization status.
- Port—Port number of the client's associated access point.
- Slot ID—Slot number of the interface that can be from 0 to 3 that the client is connected to.
- PMIPv6—Whether the client is a PMIP client.
- WGB—Workgroup bridge (WGB) status.

  A workgroup bridge is a mode that can be configured on an autonomous Cisco IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point.
- Device Type—Type of client device.

Click the blue arrow adjacent the desired client and choose one of the following:

- Show Wired Clients—Shows details of any wired clients that are connected to a particular WGB on the WGB Wired Clients topic. (This option is available if the client is a WGB.)
- LinkTest—Tests the link to the client, reports the client MAC address, and reports the number of test packets sent and received, the local signal strength, and the local signal to noise ratio. The LinkTest does not work for IPsec links and may not work for some clients.
- Disable—Manually disables a client on the Adding Disabled Clients page.
- Remove—Dissociates the client.
- 802.11aTSM or 802.11b/gTSM—Displays Traffic Stream Metrics for these radios.

Click the MAC address of the desired client to display the Client Details page.

Client Details

Choose **MONITOR > Clients** and then click the client MAC address to navigate to the Client Details page.

This page displays the details of the client's session and the AVC statistics. Information is displayed for both the client and its associated access point.

You can view the top 10 applications used by the client in the AVC Statistics tab. Client statistics are only collected for the first 128 applications classified in 90 seconds.

Client Properties

Table 2-56 Client Properties Parameters

Parameter	Description
MAC Address	MAC address of the client.
IPv4 Address	List of IPv4 address of the clients.
IPv6 Address	List the IPv6 address of the clients.
Client Type	Regular, WGB, WGB client, or Unknown type.
Number of Wired Client(s)	Number of wired clients that are connected to this WGB if the client type is WGB.
User Name	Login client name from RADIUS or controller authentication.
Port Number	Controller port used for the client's associated access point.
Interface	User-defined name for this interface; for example, management, service-port, virtual.
VLAN ID	VLAN tag identifier, or 0 for no VLAN tag.
CCX Version	Cisco Client Extensions (CCX) version in use, if supported. If the client supports Cisco Client Extensions version 5, two additional button are displayed: • Send CCXV5 Request • Display See the Client Reporting page for more information about Cisco Client Extensions version 5 client reporting.
E2E Version	End-to-End version in use, if supported.
Mobility Role	Local when the client has not roamed from its original controller or when the client has roamed to another controller on the same subnet. Foreign when the client has roamed from its original controller to another controller on a different subnet. Anchor when the client has roamed back to its original controller after roaming to another controller on a different subnet.
Mobility Peer IP Address	N/A when the client is Local (has not roamed from its original subnet). Anchor IP address (the IP address of the original controller) when the client is Foreign (has roamed to another controller on a different subnet). Foreign IP address (the IP address of the original controller) when the client is Anchor (has roamed back to another controller on a different subnet).
Policy Manager State	DHCP_REQD when a DHCP server is required to complete the security policy. 8021X_REQD when 802.1X is the required policy. Other messages to be determined.
Management Frame Protection	Management frame protection (MFP) provides security for the unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.

Table 2-56 Client Properties Parameters

Parameter	Description
UpTime (Sec)	Time in seconds since the client has been up.
Power Save Mode	Power save mode of the client.
Current TxRateSet	Current transmission rate.
Data RateSet	Data rate for the client.
KTS CAC Capability	KTS-based CAC capability of the client.
802.11u	Hotspot is a solution that enables 802.1X capable clients to interwork with external networks. This feature provides service availability information to clients and can help them to associate available networks.
802.11v BSS Transition	802.11v refers to the IEEE (Institute of Electrical and Electronics Engineers) 802.11 Wireless Network Management (Amendment 8). Stations that supports WNM (Wireless network management) can exchange information with each other (Access Points and wireless clients) in order to improve their performance.
Fastlane Client	Specifies whether the client has Fastlane QoS.

Security Information

Table 2-57 Security Information Parameters

Parameter	Description
Security Policy Completed	No (when the security policy checks have not been completed) or Yes (when the security policy checks have been completed).
Auth Key Mgmt	Type of Authenticated Key Management that can be one of the following: • 802.1X • CCKM • PSK • FT 802.1X • FT PSK • SUITEB-1X • SUITEB192-1X • 802.1X+CCKM • WPA gtk-randomize State
EAP Type	–
SNMP NAC State	Current state of the client: Quarantine, Access, or Invalid.
RADIUS NAC State	Current state of the client in the RADIUS NAC-enabled WLAN. When a client is associated to the controller on a RADIUS NAC-enabled WLAN, the controller forwards the request to the ISE server. The state of the client can be DHCP_REQD or POSTURE_REQD.
CTS Security Group Tag	Cisco TrustSec Security Group Tag information.

Table 2-57 Security Information Parameters

Parameter	Description
AAA Override ACL Name	Name of the AAA Override ACL. This ACL is in addition to the VLAN ACL that is applied to the VLAN on the Ethernet interface. If a client gets an AAA Override of the VLAN, the client is placed on the overridden VLAN and the ACL on the VLAN applies to the client. To support centralized access control through an AAA server, such as ISE or ACS, an ACL must be configured on the controller and the WLAN must be configured with the AAA override-enabled feature.
AAA Override ACL Applied Status	Status of the client that indicates if the client has been authenticated after the application of an AAA Override ACL.
AAA Override Flex ACL	Name of the IPv4 ACL that is the FlexConnect ACL for clients connected to FlexConnect access points.
AAA Override Flex ACL Applied Status	Status of the client that indicates if the client has been authenticated after the application of the AAA Override FlexConnect ACL.
Redirect URL	Redirect URL that the client should be directed to after authentication.
IPv4 ACL Name	Name of the IPv4 ACL.
IPv4 ACL Applied Status	Status of whether the IPv4 ACL was applied to the client's WLAN.
IPv6 ACL Name	Name of the IPv6 ACL.
IPv6 ACL Applied Status	Status of whether the IPv6 ACL was applied to the client's WLAN.
mDNS Profile Name	mDNS profile associated with the service that the client is using.
mDNS Service Advertisement Count	Count of the mDNS service advertisements that the client received for a requested service.
AAA Role Type	Role of the user.
Local Policy Applied	Policy applied to the client device.

Quality of Service Properties

Table 2-58 Quality of Service Parameters

Parameter	Description
WMM State	WMM state that you enable or disable. Wi-Fi Multimedia (WMM) is a QoS protocol and a subset of 802.11e standard. WMM technology identifies packets of voice, video, audio or other types of data and prioritizes their delivery based on traffic conditions. Videos transmitted over wireless networks suffer greatly if packets are delayed or dropped. So video data is given priority over other types of data on a network.
QoS Level	Quality of Service level that you set on the Editing QoS Profile page: • Platinum (Voice)—Assures a high QoS for Voice over Wireless. • Gold (Video)—Supports the high-quality video applications. • Silver (Best Effort)—Supports the normal bandwidth for clients. • Bronze (Background)— Provides lowest bandwidth for guest services. VoIP clients should be set to Platinum, Gold or Silver, while low-bandwidth clients can be set to Bronze.
Diff Serv Code Point (DSCP)	Prioritization of packets by the 6 bits in the DSCP that you set on the Editing QoS Profile page.
802.1P Tag	VLAN tag (1-7) received from the client, defining the access priority. This tag maps to the QoS Level for client-to-network packets. You set this tag on the Editing QoS Profile page.
Average Data Rate	Operator-defined average data rate for non-UDP traffic that you set on the Editing QoS Profile page.
Average Real-Time Rate	Operator-defined average data rate for UDP traffic that you set on the Editing QoS Profile page.
Burst Data Rate	Operator-defined peak data rate for non-UDP traffic that you set on the Editing QoS Profile page.
Burst Real-Time Rate	Operator-defined peak data rate for UDP traffic that you set on the Editing QoS Profile page.

Client Statistics

Table 2-59 Client Statistics Parameters

Parameter	Description
Bytes Received	Number of bytes received by the controller from the client.
Bytes Sent	Number of bytes sent to the client from the controller.
Packets Received	Number of packets received by the controller from the client.
Packets Sent	Number of packets sent to the client from the controller.
Policy Errors	Number of policy errors for the client.
RSSI	Receive signal strength indicator of the client RF session.
SNR	Signal to Noise Ratio of the client.

Table 2-59 Client Statistics Parameters

Parameter	Description
Sample Time	Time that the client statistics snapshot was taken.
Excessive Retries	Number of excessive retries before the access point looks for another controller.
Retries	Number of retries before the access point finds a controller.
Success Count	Counter increments when a CTS is received in response to an RTS.
Fail Count	Modem failure count.
Tx Filtered	Number of filtered error frames.
Data Retries	Number of data retries by the client.
RTS Retries	Number of request-to-send retries by the client.
Duplicates	Number of duplicate packets received.
Decrypt Failed	Number of decrypt packets that failed.
Mic Errors	Number of packets that have MIC errors.
Mic Missing Frames	Number of packets that do not have MIC.
RA Packets Dropped	Number of router advertisement packets that are dropped.
Interim Updates Sent	Number of times the interim updates were sent.

Client Rate Limiting Statistics

Table 2-60 Client Rate Limiting Statistics Parameters

Parameter	Description
Data Bytes Received	Number of data bytes received by the controller from the client.
Data Rx Bytes Dropped	Number of Rx data bytes dropped by the controller from the client.
Data Rx Packets Dropped	Number of Rx packets dropped by the controller from the client.
Real-time Packets Received	Number of real-time packets received by the controller from the client.
Real-time Rx Packets Dropped	Number of Rx real-time packets dropped by the controller from the client.
Real-time Bytes Received	Number of real-time bytes received by the controller from the client.
Rx Data Bytes Dropped	Number of Rx data bytes dropped by the controller from the client.
Rx Real-time Bytes Dropped	Number of Rx real-time bytes dropped by the controller from the client.
Data Packets Sent	Number of packets sent to the client from the controller.
Data Bytes Sent	Number of data bytes sent to the client from the controller.
Real-time Bytes Sent	Number of real-time bytes sent to the client from the controller.
Tx Data Bytes Dropped	Number of Tx data bytes dropped by the controller from the client.
Tx Real-time Bytes Dropped	Number of Tx real-time bytes dropped by the controller from the client.
Data Packets Received	Number of data packets received by the controller from the client.

Table 2-60 Client Rate Limiting Statistics Parameters

Parameter	Description
Real-time Packets Sent	Number of real-time packets sent to the client from the controller.
Real-time Tx Packets Dropped	Number of Tx real-time packets dropped by the controller from the client.
Tx Data Packets Dropped	Number of Tx data packets dropped by the controller from the client.
Tx Real-time Bytes Dropped	Number of Tx real-time packets dropped by the controller from the client.

PMIP Properties

Table 2-61 PMIP Properties

Parameter	Description
Mobility Type	Type of PMIP mobility for the client. The type can be None or PMIPv6.
Network Access ID (NAI)	Network Access ID of the PMIP profile.
PMIP State	State state of the PMIP client. The available states are as follows: • Unknown—Indicates that the state of the client cannot be determined. • Activated—Indicates that the client is ready to establish a tunnel. • Tunneled—Indicates that a bidirectional tunnel is established.
Connected Interface	Connected interface of the controller.
Home Address	Address of the mobile node. The mobile node can use this address if it is attached to the access network that is in the scope of that Proxy Mobile IPv6 domain.

Table 2-61 PMIP Properties

Parameter	Description
Access Technology Type (ATT)	8-bit field that specifies the access technology through which the mobile node is connected to the access link on the Mobile Access Gateway (MAG). The values and the corresponding access technology are as follows: • 0—Reserved • 1—Logical Network Interface • 2—Point-to-Point Protocol • 3—Ethernet • 4—Wireless LAN • 5—WIMAX • 6—3GPP GSM EDGE Radio Access Network (3GPP GERAN) • 7—3GPP Universal Terrestrial Radio Access Network (3GPP UTRAN) • 8—3GPP ETRAN (3GPP Evolutions of the Transport in the UTRAN) • 9—3GPP2 eHRPD (3GPP2 Evolved High Rate Packet Data) • 10—3GPP2 HRPD (3GPP2 High Rate Packet Data) • 11—3GPP2 1xRTT • 12—3GPP2 UMB (3GPP2 Ultra Mobile Broadband)
Local Link Identifier	Local link identifier of the client.
LMA Name	Name of the LMA to which the client is connected.
Life Time	Duration of the PMIP client association.

AP Properties

Note The AP Properties table identifies the properties of the access point of the client and of the negotiated session of the client.

Table 2-62 AP Properties Parameters

Parameter	Description
AP Address	MAC address of the access point.
AP Name	Name of the access point.
AP Type	Access point's RF type.
AP radio Slot ID	Slot ID of the AP radio.
WLAN Profile	Name of the WLAN.
Status	Status of client from status code (see Status Code below).
Association ID	Client's access point association identification number.
802.11 Authentication	Authentication algorithm of client.

Table 2-62 AP Properties Parameters

Parameter	Description
Reason Code	Client reason code: • no reason code (0)—Normal operation. • unspecified reason (1)—The client is associated but no longer authorized. • previousAuthNotValid (2)—The client is associated but not authorized. • deauthenticationLeaving (3)—The access point went offline, deauthenticating the client. • disassociationDueToInactivity (4)—The client session timeout has been exceeded. • disassociationAPBusy (5)—The access point is busy (performing load balancing, for example). • class2FrameFromNonAuthStation (6)—The client attempted to transfer data before it was authenticated. • class2FrameFromNonAssStation (7)—The client attempted to transfer data before it was associated. • disassociationStaHasLeft (8)—The operating system moved the client to another access point using nonaggressive load balancing. • staReqAssociationWithoutAuth (9)—The client has not been authorized yet; the client has been attempting to associate with access point. • missingReasonCode (99)—The client was momentarily in an unknown state.
Status Code	Client status code: • idle (0)—Normal operation: no rejections of client association requests. • aaaPending (1)—The client is completing an AAA transaction. • authenticated (2)—802.11 authentication is completed. • associated (3)—802.11 association is completed. • powersave (4)—The client is in powersave mode. • disassociated (5)—802.11 disassociation is completed. • tobedeleted (6)—To be deleted after disassociation. • probing (7)—The client has not been associated or authorized yet. • disabled (8)—The client has automatically been disabled by the Operating System for an operator-defined time.
CF Pollable	Whether the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.
CF Poll Request	Whether CFP is requested by the client.

Table 2-62 AP Properties Parameters

Parameter	Description
Short Preamble	Attribute, when true, that indicates that the short preamble option as defined in subclause 18.2.2.2 is implemented. This parameter must be disabled to optimize this controller for some clients, including SpectraLink NetLink Telephones.
PBCC	Attribute, when true, that indicates that the PBCC modulation option as defined in subclause 18.4.6.6 is implemented. The default value of this attribute is not implemented.
Channel Agility	Physical channel agility functionality that is or is not implemented.
Timeout	Client Session timeout (maximum amount of time before a client is forced to reauthenticate).
WEP State	WEP security state of the client.
Data Switching	Whether the client's data traffic is local or centrally switched. It shows up only for FlexConnect associated clients.

AVC Statistics

You can view the last 90 seconds and the cumulative statistics of the top 10 applications used by the client as a pie chart. Each application appears with the corresponding usage percentage. The applications are color coded for clarity. You can also view details of the applications such as packet count, byte count, and average packet size. Client statistics are only collected for the first 128 applications classified in 90 seconds. You can see upstream and downstream AVC statistics for the client.

This section describes the following command buttons:

- Click **Apply** to send data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Click **Link Test** to use the built-in test circuitry to test the link between the client and the controller, reports the client MAC address, and reports the number of test packets sent and received, the local signal strength, and the local signal to noise ratio. LinkTest does not work for IPsec links and may not work for some clients.
- Click **Remove** to disconnect the client. If the client supports Cisco Client Extensions version 5, two additional buttons are displayed:
  - Click **Send CCXV5 Request** send the report request to the client.
  - Click **Display** to open the Client Reporting page.

WGB Wired Clients

The WGB Wired Clients page displays information about the WGB wired clients that are associated with the access points.

Note The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.

Client Information Table

This table displays a list of all clients attached to the controller. Client information includes the following:

- WGB MAC address
- MAC address of the client
- Name of the access point to which client is attached
- Name of WLAN used by the client
- Type of client (802.11a, 802.11b, 802.11g, or 802.11n)
- Status of the client connection
- Authorization status
- Port number of the client's associated access point

Click the blue arrow adjacent the desired client and choose one of the following:

- LinkTest—Indicates that the Link Test is not supported for WGB-wired clients.
- Disable—Manually disables a client on the Adding Disabled Clients page.
- Remove—Dissociates the client.
- 802.11aTSM or 802.11b/gTSM—Displays Traffic Stream Metrics for these radios.

Click the MAC address of the desired client to display the Client Details page.

Traffic Stream Metrics Collection

Choose **MONITOR > Clients** and click **802aTSM** or **802b/gTSM** to navigate to the Traffic Stream Metrics Collection page.

Traffic stream metrics (TSM) involves collecting of uplink statistics and downlink statistics between an access point and a CCX v4 client and then propagating these statistics periodically back to the controller. If the client is not CCXv4 compliant, then only the downlink statistics are captured. You configure traffic stream metrics collection on a per-interface band basis (such as all 802.11a/n radios). The controller saves this option in flash memory so that it persists across reboots. Once an access point receives this message, it enables the traffic metrics collection on the specified interface type.

Every 5 seconds, the access point gets a measurement report for both the uplink (client side) and downlink (local side) measurements. The aggregation of 5-second reports and preparation of 90-second reports are done at the access point. Every 90 seconds, the access point prepares an IAPP data packet and sends it to the controller for further processing. The controller stores the data in its structures and then provides "usmdB" access ChooseAPIs to the CLI module and the PI for displaying it on the UI.

Four variables are affected by the WLAN that can affect audio quality:

- Packet latency
- Packet jitter
- Packet loss
- Roaming time

You can isolate the problem of bad voice quality by studying these variables. The traffic stream metrics feature addresses the voice quality issue by providing statistics for each of these four variables.

Client Reporting

The Client Reporting page displays details about the client and wireless network adapter.

Table 2-63 Client Reporting Parameters

Parameter	Description
Client Profile	Displays all the available configuration profiles as well as the current profile in use on the wireless network adaptor. Click a profile name to display the Profile Details page.
Operating Parameters	Displays various operating settings that the client is currently using.
Manufacturer's Information	Displays all the static manufacturer-specific data about the client and wireless network adapter.
Client Capability	Displays the range of capabilities that are available on the wireless network adapter.

Note This group displays the available capabilities, not current settings.

Profile Details

The Profile Details page displays the details about the selected profile on the wireless network adapter.

Sleeping Clients

Choose **MONITOR > Sleeping Clients** to navigate to the Sleeping Clients page. This page displays details about the sleeping clients that are managed by the WLANs configured in the controller.

Table 2-64 Sleeping Clients Parameters

Parameter	Description
Client MAC	MAC address of the client.
WLAN SSID	SSID of the WLAN that the client is associated with.
User Name	Username associated with the client.
Remaining Time	Time, in hours and minutes, after the idle timeout of the sleeping client.

Multicast Groups

Choose **MONITOR > Multicast** to navigate to the Multicast page.

This page displays the details of the Layer 3 and Layer 2 multicast groups and their corresponding multicast group IDs (MGIDs).

Click the link for a specific MGID to see a list of all the clients joined to the multicast group in that particular MGID.

Layer 3 MGID Mapping

Table 2-65 Layer 3 MGID Parameters

Parameter	Description
Group address	Layer 3 MGID group address.
VLAN	Layer 3 MGID group VLAN.
MGID	Layer 3 MGID.
IGMP/MLD	Internet Group Management Protocol (IGMP) snooping that is used to limit the flooding of multicast traffic for IPv4. For IPv6, Multicast Listener Discovery (MLD) snooping is used.

Layer 2 MGID Mapping

Table 2-66 Layer 2 MGID Parameters

Parameter	Description
Interface name	Layer 2 MGID interface name.
VLAN ID	Layer 2 MGID VLAN ID.
MGID	Layer 2 multicast group ID.

Applications

Applications > WLAN

Choose **MONITOR > Applications > WLAN** to navigate to the **WLANs** page.

This page displays details of the WLANs that have Application Visibility and Control (AVC) profiles configured on them. Click the WLAN ID to navigate to the **WLANs > Application Statistics** page. Only WLANS on local mode access points or centrally switched on a FlexConnect access point are capable of having applications recognized by NBAR.

You can view the last 90 seconds and the cumulative statistics of the top 10 applications as a pie chart. Each application appears with the corresponding usage percentage. The applications are color coded for clarity. You can also view details of the applications such as packet count, byte count, and average packet size.

Applications > FlexConnect Groups

Choose **MONITOR > Applications > FlexConnect Groups** to navigate to the **FlexConnect Groups** page.

This page displays details of the FlexConnect groups that have Application Visibility and Control (AVC) profiles configured on them.

Lync

This section contains the following topics:

- Active Calls, page 2-73
- History Calls, page 2-73

Active Calls

Choose **MONITOR > Lync > Active Calls** to navigate to Lync Active Calls page. This page shows the following call details:

- ID
- Call Type
- Caller User ID
- Caller IP Address (IPv4/IPv6)
- Caller MAC Address
- Caller AP Name
- Callee User ID
- Callee IP Address (IPv4/IPv6)
- Callee MAC Address
- Callee AP Name

History Calls

Choose **MONITOR > Lync > History Calls** to navigate to Lync History Calls page. This page shows the following call details:

- ID
- Call Type
- Caller IP
- Caller MAC Address
- Callee IP
- Callee MAC Address
- Status
- Duration

- MOS
- Jitter

Local Profiling

This page shows the following information:

- Device Stats
- Device Type and Count
- Manufacturer Stats
- Manufacturer Type and Count

Note This page displays only top 10 client counts.

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 **Note** Cisco 2504 Controllers does not support wired guest services.
Profile Name	Profile name of the WLAN

Table 3-2 WLAN > New Parameters

Parameter	Description
SSID	SSID field is displayed if you choose WLAN from the **Type** drop-down list. Definable name of the WLAN (text string). This is the SSID broadcast name for the WLAN.
ID	ID number for the WLAN Guest LAN—Enter guest LAN identifier between 1 and 5. 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. 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. **Note** If the Cisco OEAP 600 is in the default group, the WLAN/Remote LAN IDs must be set as less than ID 8.

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 **Note** 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	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 802.11a/n/ac Global Parameters and 802.11a/n/ac Client Roaming pages. **Note** This field appears only when you choose WLAN as the Type in the WLANs > New page.
Interface/Interface Group (G)	Limited to the nonservice port and nonvirtual interface names configured on the Interfaces page. **Note** This field appears only when you choose WLAN as the Type in the WLANs > New page.
Multicast VLAN Feature	Check box that you can select to enable the multicast VLAN feature. The default option is none. **Note** The Multicast Interface field appears only after you enable the Multicast VLAN feature text box. **Note** You have to configure the multicast VLAN feature only once if you want to use the multicast feature.
Broadcast SSID	Service Set Identifier for this WLAN.
Ingress Interface	Guest LAN's ingress interface. By default, None is selected. **Note** This field is available only for guest LANs.
Egress Interface	Remote LAN's or guest LAN's egress interface. By default, management is selected. **Note** This field is available only for remote LANs and guest LANs.
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.

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 Layer 2 WPA + WPA2 Parameters topic.
	802.1X	WEP 802.1X data encryption type. For information on these settings, see the Layer 2 802.1X Parameters topic.
	Static WEP	Static WEP encryption parameters. For information on these settings, see the Layer 2 Static WEP Parameters topic.
	Static WEP + 802.1X	Both Static WEP and 802.1X parameters. For information on these settings, see the Layer 2 Static WEP Parameters and Layer 2 802.1X Parameters 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 Layer 2 CKIP Parameters 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 Adding MAC Filters page. Otherwise, configure the clients on a RADIUS server.	

Table 3-4 Layer 2 Tab Parameters

Parameter	Description
Mac Auth or Dot1x	MAC authentication failover to Dot1x authentication for the WLAN. The prerequisites for the failover to work are as follows: • MAC Filtering must be enabled. • Layer 2 security must be 802.1X and Static WEP. The failover does not work with RADIUS NAC feature. 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. 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.
Fast Transition	
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.
Lobby Admin Configuration	
Lobby Admin Access	Check box to enable or disable lobby administrator access

Table 3-5 Layer 2 WPA + WPA2 Parameters

Parameter	Description
Fast Transition	
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.
Protected Management Frame	
PMF	Drop-down list from which you can choose the following: • Disabled—Disables 802.11w MFP protection on a WLAN. • Optional—Enables 802.11w MFP protection on a WLAN. • Required—Requires clients to negotiate 802.11w MFP protection on a WLAN. 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.

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.
WPA+WPA2 Parameters	
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.
Authentication Key Management	
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. **Note** 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. **Note** 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.

Note For the Cisco OEAP 600 Series APs, do not choose CCKM. Choose either 802.1X or PSK.

Note For the Cisco OEAP 600 Series access point, security encryption settings must be identical for WPA and WPA2 for TKIP and AES.

Note 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: • None • 40 bits • 104 bits **Note** 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.
Layer 2 802.1X Port Parameters for a Remote LAN	
Host Mode	Modes of authentication for IEEE 802.1X. It can either be Single Host or Multi Host. • 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. • 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.
Violation Mode	When a security violation occurs, the port is protected depending on the configured violation action, which can be Shutdown, Replace, or Protect. • Shutdown—Disables the port. • Replace—Removes the current session and initiates the authentication for a new host. This is the default behavior. • Protect—Drops packets with unexpected MAC addresses without generating a system message.

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: • not set • 40 bits • 104 bits
Key Index	Key index, from 1 to 4. **Note** 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: • not set • 40 bits • 104 bits
Key Index	Key index, from 1 to 4. **Note** 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	Setting to enable IPsec. Check software availability and client hardware compatibility before implementing IPsec. **Note** 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 Inventory page.
	VPN Pass-Through	VPN pass-through that you can enable or disable. **Note** 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. For information on these settings, see Layer 3 VPN Passthrough Parameters.

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

Parameter	Description
Web Policy	Check box that you can select to enable Web Policy. **Note** 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. **Note** Web Policy cannot be used with IPsec or VPN pass-through options. The following parameters are displayed: • Authentication—Prompts the user for username and password while connecting the client to the wireless network. • Passthrough—Enables the user to access the network directly without entering the username and password. • 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. • 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. • On MAC Filter failure—Enables web authentication MAC filter failures. • Web policy done locally on AP This option is supported only on ap1g2 and ap3g2 platforms.
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 Access Control Lists topic for more information.
WebAuth FlexACL	Drop-down list from which you can choose the FlexConnect ACL for external web authentication in locally switched WLANs. For more information about creating FlexConnect ACLs, see Adding Access Control Lists. **Note** 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.
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 Web Login Page.
Web Auth type	Setting that is displayed if you choose Web Policy and Override Global Config. Type of web authentication: • Internal • Customized (Downloaded) – Login Page—Choose a login page from the drop-down list. – Login Failure page—Choose a login page that displays to the client if web authentication fails. – Logout page—Choose a login page that displays to the client when the user logs out of the system. • External (Redirect to external server) – URL—Enter the URL of the external server.
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 Access Control Lists topic for more information.	
Override Global Config	Check box that you enable to override the global authentication configuration set on the Web Login Page.	

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

Parameter	Description
Web Auth type	Setting that is displayed if you selected Override Global Config. Type of web authentication: • Internal • Customized (Downloaded) – Login Page—Choose a login page from the drop-down list. – Login Failure page—Choose a login page that displays to the client if web authentication fails. – Logout page—Choose a login page that displays to the client when the user logs out of the system. • External (Redirect to external server) – URL—Enter the URL of the external server.
Email Input	Setting that is displayed if you selected Web Passthrough. If you choose this option, you will be prompted for your e-mail address while connecting to the network.

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	RADIUS Server Overwrite Interface that you can enable or disable. The default is disabled. 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. **Note** You cannot enable the Radius Server Overwrite Interface when a diagnostic channel is enabled.
RADIUS Server Client Interface	RADIUS Server Client Interface that you can enable or disable on the WLAN. The default is disabled. When you enable the RADIUS Server Client Interface, the RADIUS server packets pass through the same VLAN as the data traffic of the client.

Table 3-12 AAA Servers Tab Parameters

Parameter	Description	
RADIUS Servers	**Authentication Servers**	**Accounting Servers**
	RADIUS server (configured from the RADIUS Authentication Servers page) that you choose from the drop-down lists. 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. You can choose up to three RADIUS servers, which are tried in priority order.	RADIUS accounting server that you can enable or disable. The default is Enabled. Choose a RADIUS server (configured from the RADIUS Accounting Servers page) from the drop-down lists. 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. You can choose up to six RADIUS servers, which are tried in priority order.
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	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). **Note** The Interim Update check box can be selected only if you have the RADIUS accounting servers enabled.	
LDAP Servers	LDAP server (configured from the LDAP Servers page) that you can choose from the drop-down list. You can choose up to three LDAP servers, which are tried in a priority order.	
Local EAP Authentication[1]	Local EAP authentication that you can enable or disable. The default is disabled.	
EAP Profile Name[1]	EAP profile name (configured from the Local EAP Profiles page).	
Authentication priority order for web-auth user	Order in which user credentials are retrieved from the back-end database servers. Highlight the desired database from the left box. Use the left and right arrows and the Up and Down buttons to move the desired database to the top of the right box. If you select the RADIUS NAC feature for authentication, the priority for web authentication must only contain RADIUS.	

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)	Quality of Service Level, set on the Editing QoS Profile page: • Platinum (voice)—Assures a high Quality of Service for Voice over Wireless. • Gold (video)—Supports the high-quality video applications. • Silver (best effort)—Supports the normal bandwidth for clients. • Bronze (background)— Supports the lowest bandwidth for guest services. VoIP clients should be set to Platinum, Gold, or Silver, while low-bandwidth clients can be set to Bronze. **Note** Media Session Snooping is supported only for Platinum QoS profiles.
Application Visibility	Check box that you can select to view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology. To view all the supported applications, choose **WIRELESS > Application Visibility and Control > Applications**. To view all classified applications, choose **Monitor > Applications** and click the WLAN ID to navigate to the Monitor > Clients page.
AVC Profile	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 **WIRELESS > Application Visibility and Control > Applications** and click **New**. 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.
NetFlow Monitor	Drop-down list from which you can choose a NetFlow monitor for the WLAN. To configure a new NetFlow monitor, choose **WIRELESS > Netflow > Monitor** and click **New**.

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. **Note** Fastlane must be disabled on the WLAN before disabling QoS Fastlane.
Override Per-User Bandwidth Contracts	
Note 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).
Override Per-SSID Rate Limits **Note** The values that you set override the values configured in the QoS profile page.	
Override WLAN QoS Parameters	
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).
WMM	
WMM Policy[1]	WMM Policy. Choose one of the following: • Disabled—Disables this WMM policy. • Allowed—Allows the clients to communicate with the WLAN. • Required—Ensures that it is mandatory for the clients to have WMM features enabled on them to communicate with the WLAN.

Table 3-13 QoS Tab Parameters

Parameter	Description
7920 AP CAC[1]	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[1]	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.
Media Stream	
Multicast Direct	Check box to enable Multicast Direct on the WLAN.
Lync Policy	
• Audio • Video • Application-Sharing • File-Transfer	The following QoS policies can be applied for each of the Lync policies: • Bronze • Silver • Gold • Platinum **Note** WLAN QoS must meet or exceed Lync policy QoS settings in order for Lync priorities to achieve the configured levels.

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 **Security > Local Policies > New**.

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	AAA Override for global WLAN parameters that you can enable or disable. 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.) 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. 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. The AAA Override values may come from a RADIUS server, for example. **Note** AAA Override is not supported with FlexConnect.
Coverage Hole Detection	Coverage hole detection (CHD) on this WLAN that you can enable or disable. This option is not available for guest LANs and remote LANs. By default, CHD is enabled on all WLANs on the Cisco WLC. You can disable CHD on a WLAN. 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. **Note** For the Cisco OEAP 600 Series access point, do not enable Coverage Hole Detection.
Enable Session Timeout	Session timeout that you can enable or disable. Maximum time in seconds for a client session before requiring reauthorization.
Aironet IE	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. **Note** For the Cisco OEAP 600 Series access point, do not enable Aironet IE.
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	Access Control List (ACL) that overrides the ACL configured for the interface on this WLAN. ACLs are configured on the Access Control Lists page. • IPv4 ACL—Lists the IPv4 ACL that needs to be applied on this WLAN. ACLs are configured on the Access Control Lists page. • IPv6 ACL—Lists the IPv6 ACL that needs to be applied on this WLAN. ACLs are configured on the Access Control Lists page.
Layer 2 ACL	List the layer 2 ACL that needs to be applied to the WLAN. ACLs are configured on the Access Control Lists page.
URL ACL	List the URL ACL that needs to be applied to the WLAN. URL ACLs are configured on the Access Control Lists.

Table 3-15 Advanced Tab Parameters

Parameter	Description
P2P Blocking Action	Peer-to-peer blocking settings that you can choose. • Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the Cisco WLC whenever possible. **Note** Traffic is never bridged across VLANs in the Cisco WLC. • Drop—Causes the Cisco WLC to discard the packets. • 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. For FlexConnect local switching WLANs, the settings are as follows: • Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the AP whenever possible. • Drop—Causes the AP to discard the packets. • Forward-UpStream—Causes the AP to discard the packets.
Client Exclusion	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 Client Details 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.
Maximum Allowed Clients	Maximum clients allowed per Cisco WLC. 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. The number of clients that you can configure for a specific platform is as follows: • Cisco 5500 Series Controller—7000 • Cisco 7500 Series Controller—30000 • WiSM2—15000 **Note** The maximum number of clients per WLAN feature is supported only for access points that are in connected mode. **Note** This feature is not supported when you use FlexConnect local authentication and is not applicable for remote and guest LANs.
Static IP Tunneling	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: • Auto anchoring mobility (guest tunneling) cannot be configured for the same WLAN. • FlexConnect local authentication cannot be configured for the same WLAN. • DHCP required option cannot be configured for the same WLAN. **Note** Dynamic anchoring of static IP clients cannot be configured with FlexConnect local switching.

Table 3-15 Advanced Tab Parameters

Parameter	Description
Wi-Fi Direct Clients Policy	Drop-down list from which you can choose a Wi-Fi Direct Clients Policy for a WLAN. 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. **Note** Wi-Fi Direct Clients Policy is applicable to WLANs that have APs in local mode only. The following options are available: • **Disabled**—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct clients • **Allow**—Allows Wi-Fi Direct clients to associate with the WLAN • **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN • **Xconnect-Not-Allow**—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
Maximum Allowed Clients Per AP Radio	Maximum number of clients that are allowed to connect to an AP. The maximum number you can configure is 200.
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 relam with the realm configured on RADIUS authentication and accounting servers.
11ac MU-MIMO	Check box that you can use to enable or disable 802.11ac MU-MIMO for Cisco Aironet 1850 Series APs. **Note** MU-MIMO stands for Multiple User Multiple Input, Multiple Output.
Off Channel Scanning Defer	
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.
FlexConnect	

Table 3-15 Advanced Tab Parameters

Parameter	Description
FlexConnect Local Switching	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. **Note** 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. **Note** The FlexConnect Local Switching text box must be enabled to enable local authentication.
FlexConnect Local Auth	FlexConnect local authentication that you can enable or disable.
Learn Client IP Address	Client IP address learning (this option is available when you enable FlexConnect Local Switching) that you can enable or disable. **Note** 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.
VLAN based Central Switching	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. 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. VLAN central switching does not support: • FlexConnect Local Authentication • Layer 3 roaming of local switching client
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.
Lync	
Lync Server	To enable or disable WLAN Lync SDN service.
11k	
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. **Note** 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. **Note** DHCP address assignment (Required) is not supported for wired Guest LANs. **Note** 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. **Note** The Cisco OEAP 600 Series access point does not support MFP. **Note** 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	Enables SNMP NAC or ISE NAC. • SNMP—Enables SNMP NAC support for the WLAN. • ISE NAC—Enables RADIUS NAC support for the WLAN. 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. 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. 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. 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. The following restrictions apply: • ISE NAC functionality with VLAN override is not available. • During slow roaming, the client goes through posture validation. • Guest tunneling mobility is supported for ISE NAC-enabled WLANs. • The VLAN select feature is not supported. • The NAC agent may also be available in a non-NAC-enabled WLAN. • The workgroup bridges are not supported. • The AP group over NAC feature is not supported over ISE NAC. **Note** 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. 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. 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.

Table 3-15 Advanced Tab Parameters

Parameter	Description
	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. Cisco WLC software configured with RADIUS NAC does not support change of authorization (CoA) on the service port.
Load Balancing and Band Select	
Note 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	Client radio band that you can enable or disable. **Note** Band Select is configurable only when the radio policy is set to **All** in the General Tab.
Passive Client	
Passive Client	Passive clients that you can enable or disable on your WLAN. 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. 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: • The upstream device that sends out the ARP request to the client cannot know where the client is located. • Power for battery-operated devices such as mobile phones and printers is preserved because they do not need to respond to every ARP request. 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. This feature enables ARP requests and responses to be exchanged between wired and wireless clients. 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. **Note** This feature is supported only on the Cisco 5500 Series Controllers. **Note** Passive clients are not supported with AP groups and FlexConnect centrally switched WLANs. This feature works on the multicast-multicast mode of multicast operation.
Voice	
Media Session Snooping	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. See the Radio Statistics page to see the VoIP statistics for your access point radios. See the SNMP Trap Logs page to see the traps generated for failed calls.

Table 3-15 Advanced Tab Parameters

Parameter	Description
Re-anchor Roamed Voice Clients	Reanchoring of roamed voice clients that you can enable or disable. 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. 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. **Note** The ongoing data session may be affected due to dissociation and reassociation. **Note** This feature is supported for TSPEC-based calls and non-TSPEC-SIP based calls only when admission control is enabled. **Note** You can reanchor roaming of voice clients for each WLAN. **Note** This feature is not recommended for use on the Cisco 792x phone.
KTS based CAC Policy	To enable or disable CAC that is based on Key Telephone System (KTS) for the WLAN. 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. 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. 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. 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. Limitations: • KTS-based CAC is not supported on FlexConnect access points with the WLAN in the local switching mode. • The Cisco WLC ignores the SSID capability check request message from the clients. • Preferred call is not supported for KTS CAC clients. • Reason code 17 is not supported in inter Cisco WLC roaming scenarios. • This feature is applicable only when the QoS profile is set to Platinum for the WLAN.

Table 3-15 Advanced Tab Parameters

Parameter	Description
RADIUS Client Profiling	
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.
PMIP	
PMIP Mobility Type	Choose the type of PMIP mobility for the WLAN. The following options are available: • None—Configures the WLAN with Simple IP. • PMIPv6—Configures the WLAN with only PMIPv6.
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.
Universal AP Admin Support	
Universal AP Admin	Check box to enable or disable Universal AP Admin support. For more information, see *Universal AP Regulatory Domain Deployment Guide*.
11v BSS Transition Support	
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.
Tunneling	
Tunnel Profile	Choose the EoGRE tunnel profile that you have created.
mDNS	
mDNS Snooping	Check box to enable or disable mDNS snooping on the WLAN. To check if global mDNS snooping is enabled, choose **CONTROLLER > mDNS > General**. 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
TrustSec	
Security Group Tag	Text box to enter Security Group Tag value.
OpenDNS	
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.
Fabric Configuration	
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.
Mobility	
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 **local** 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	Network type that you can set on this WLAN. The following options are available: • Private Network • Private Network with Guest Access • Chargeable Public Network • Free Public Network • Emergency Services Only Network • Personal Device Network • Test or Experimental • Wildcard The default value is Chargeable Public Network.
Network Auth Type	Network authentication type that you can set on this WLAN for 802.11u. The following options are available: • Not configured • Acceptance of terms and conditions • Online enrollment • HTTP/HTTPS redirection • DNS Redirection
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: • Unknown • Not available • Public address • Port-restricted • Single NATed private • Double NATed private • Port-restricted and single NATed • Port-restricted and double NATed
IPv6Type	IPv6type address. The following options are available: • Unknown • Not available • Available The default value is Unknown.

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, AABBDF.
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: • LEAP • PEAP • EAP-PEAP • EAP-TLS • EAP-FAST • EAP-SIM • EAP-TTLS • EAP-AKA
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: • Not configured • Link Up • Link Down • Link in Test
WAN Symmetric Link Status	Downlink and uplink speed of the WAN backhaul link. The following options are available: • Same • Different
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: • ICMP • FTP/SSH/TLS/PPTP VPN/VOIP • IKEv2 (IPSec VPN/VoIP/ESP)
Port No.	Port number used for the IP. The following options are available: • ICMP/ESP (IPSec-VPN) • FTP • SSH • HTTP • TLS-VPN • IKEv2 • PPTP-VPN • IPSec-NAT • VoIP

Table 3-26 Port Config List Parameters

Parameter	Description
Status	Status of the IP port. The following options are available: • Closed • Open • Unknown
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 gruop 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	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. **Note** The CAPWAP Preferred Mode can either be configured Globally (Controller > General Tab > CAPWAP Preferred Mode) or on a AP Group. If you unselect the check box, global configuration will take precedence. **Note** The above configuration will be displayed in the Wireless > ALL APs > General Tab > IP Config. **Note** The CAPWAP Preferred Mode field does not appear under the **default-group**. The APs by default are part of the default-group.

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	SNMP NAC out-of-band support for this access point group that you can enable or disable. **Note** If you enable SNMP NAC out-of-band support, be sure to choose the quarantine VLAN from the **Interface Name** drop-down list.
Add button/Cancel button	Click **Add** to add this WLAN to the access point group. Click **Cancel** 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 **AP Name** check box to select all APs, and click **Remove APs**.
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 **AP Name** check box to select all APs, and click **Add APs**.

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: • Unspecified • Assembly • Business • Educational • Factory and Industrial • Institutional • Mercantile • Residential • Storage • Utility and Misc • Vehicular • Outdoor
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. **Note** 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.

Controller Tab

This tab on the menu bar enables you to access the Cisco WLC configuration details. Use the left navigation pane to access specific Cisco WLC parameters.

You can access the following page from the Controller tab:

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Redundancy
- Internal DHCP Server
- Mobility Management
- Ports
- NTP
- CDP
- PMIPv6
- Tunneling
- IPv6
- mDNS
- Advanced

General

Choose **CONTROLLER > General** to navigate to this page.

Table 4-1 Controller Configuration Parameters

Parameter	Description
Name	Controller name
802.3x Flow Control Mode	802.3x flow control mode that you enable or disable when you choose the corresponding line on the drop-down list. By default, this option is disabled.
LAG Mode on next reboot	Link Aggregation Group (LAG) mode that you can set as follows: Enabled—Enables link aggregation on the Cisco WLC. Disabled—Disables link aggregation on the Cisco WLC. LAG is disabled by default on the Cisco 5500 Series Controllers. LAG is supported on Cisco 2500, 2504, 8500, and Flex 7500 Series Controllers. For more information, see the Inventory topic.
Broadcast Forwarding	Broadcast forwarding that you can enable or disable. The default is disabled state.
AP Multicast Mode	IPv4 Packet forwarding policy that the controller uses. Choose one of the following options from the drop-down list: • Unicast—Enables the controller, when it receives a multicast packet, to forward the packet as a unicast packet to all associated access points. • Multicast—Enables the controller to forward a packet as a multicast packet. Enter the IPv4 address of the multicast group in the multicast group address text box. **Note** Cisco 2500 Series controllers support only multicast-multicast mode, and by default the multicast IP address is zero.
AP IPv6 Multicast Mode	IPv6 Packet forwarding policy that the controller uses. Choose one of the following options from the drop-down list: • Unicast—Enables the controller, when it receives a multicast packet, to forward the packet as a unicast packet to all associated access points. • Multicast—Enables the controller to forward a packet as a multicast packet. Enter the IPv6 address of the multicast group in the multicast group address text box. **Note** Cisco 2500 Series controllers support only multicast-multicast mode, and by default the multicast IP address is zero. You must configure the multicast address for IPv6 to function.
AP Fallback	Access point fallback that you can enable or disable. Determines whether or not an access point that lost a primary controller connection automatically returns to service when the primary controller becomes functional again.

Table 4-1 Controller Configuration Parameters

Parameter	Description
CAPWAP Preferred Mode	Select check box to configure CAPWAP Preferred Mode globally. The preferred mode can be either IPv4 or IPv6.
Fast SSID Change	Fast SSID Change that you can enable or disable. When you enable Fast SSID Change, the controller allows clients to move between SSIDs. When the client sends a new association request for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID. When FastSSID Change is disabled, the controller enforces a delay before clients are allowed to move to a new SSID.
Link Local Bridging	Enable to configure bridging of the link local traffic at local site.
Default Mobility Domain Name	Operator-defined Mobility Group Name.
RF Group Name	RF group name. The valid range for the RF group name is 8 to 19 characters. Radio Resource Management (RRM) neighbor packets are distributed among access points within an RF group. Cisco access points only accept RRM neighbor packets sent with this RF group name. The RRM neighbor packets sent with different RF group names are dropped.
User Idle Timeout	Timeout for idle clients in seconds. The factory default is 300. When the timeout expires, the client loses authentication, briefly disassociates from the access point, reassociates, and reauthenticates. The range is 15 to 100000.
ARP Timeout	Timeout in seconds for the Address Resolution Protocol. By default, this is set to 300. The range is 10 to 2147483647.
Web Radius Authentication	PAP, CHAP, or MD5-CHAP password authentication.
Operating Environment	Operating environment for the controller. **Note** Not supported in Cisco Flex 7500 Series Controllers.
Internal Temp Alarm Limits	Acceptable temperature range for operation of the controller. An alarm is triggered if the temperature raises or falls below the range. **Note** Not supported in Cisco Flex 7500 Series Controllers.

Table 4-1 Controller Configuration Parameters

Parameter	Description
WebAuth Proxy Redirection Mode	Mode that enables or disables the web authentication proxy redirection. This feature enables clients that have manual web proxy enabled in the browser to facilitate authentication with the controller. If the client's browser is configured with manual proxy settings (on 8080 or 3128) and if the client requests any URL, the controller responds with a web page prompting the user to change the Internet settings to automatically detect the proxy settings. This is to ensure that the browser's manual proxy settings information does not get lost. After enabling this settings, the user can get access to the network through the web authentication policy. This functionality is given for port 8080 and 3128 because these ports are the most commonly used ports for web proxy server.
WebAuth Proxy Redirection Port	Port numbers on which the controller listens to web authentication proxy redirection. The default ports are 80, 8080, and 3128. If you configured the web authentication redirection port to any port other than these values, you must specify that value.
Global IPv6 Config	Drop-down list from which you can enable or disable the global IPv6 configuration.
Web Color Theme	Drop-down list from which you can select red color as the UI default color.
HA SKU Secondary Unit	Enable or disable the high availability SKU secondary unit.
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.
HTTP Profiling Port	Enter the port number to be profiled by the WLC. Default value is 80.
DNS Server IP	IP address of the DNS server.
HTTP-Proxy IP Address	IP address of the HTTP-Proxy server.

Icons

Choose **CONTROLLER > Icons** to navigate to this page.

This page identifies icons to be used for the service provider.

Table 4-2 Icon Parameters

Parameter	Description
Filename	Filename of the icon.
File Type	File type of the icon.
Lang Code	Language code.
Width	Width of the icon.
Height	Height of the icon.
Size (KB)	Size of the icon in KB.

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

Inventory

Choose **CONTROLLER > Inventory** to navigate to this page.

This page identifies Cisco WLAN Solution product information assigned by the manufacturer.

Table 4-3 Inventory Parameters

Parameter	Description
Model No.	Model number as defined by the factory.
Burned-in MAC Address	Burned-in Ethernet MAC address for this Cisco WLC management interface.
Maximum number of APs supported	Maximum number of access points supported by the Cisco WLC.
FIPS Prerequisite Mode	Federal Information Processing Standards–US Government requirement for cryptographic modules.
WLANCC Prerequisite Mode	If the shared secret for IPSec is not configured, the default radius shared secret is used. If the authentication method is PSK, WLANCC should be enabled to use the IPSec shared secret.By default, WLANCC is disabled.
UCAPL Prerequisite Mode	If the shared secret for IPSec is not configured, the default radius shared secret is used. If the authentication method is PSK, UCAPL should be enabled to use the IPSec shared secret. By default, UCAPL is disabled.
UDI	
Product Identifier Description	Vendor-specific model name.
Version Identifier Description	Vendor-specific hardware revision.
Serial Number	Unique serial number for this Cisco WLC.
Entity Name	Textual name of the physical entity.
Entity Description	Textual description of the physical entity.

Interfaces

Choose **CONTROLLER > Interfaces** to navigate to this page.

- To edit the parameters for an interface, click the interface name (Interfaces > Edit).
- To remove an interface, hover your cursor over the blue drop-down arrow for the interface and choose **Remove**. You are prompted for confirmation of the interface removal.

Table 4-4 Controller Interface Parameters

Parameter	Description
Interface Name	Name of the interface: • Management—802.11 Distribution System wired network. • Redundancy-management—Interface used for peer to peer communication using a gateway. This interface appears irrespective of the state of redundancy. • Redundancy-port—Interface used for peer to peer communication. Role negotiation, config sync are done using this port. This interface appears irrespective of the state of redundancy. • Service-port—System Service interface. • Virtual—Unused IP address used as the virtual gateway address. • AP-manager—Can be on the same subnet as the management IP address, but must have a different IP address than the management interface. • <name>—Operator-Defined Interface assignment, without any spaces.
VLAN Identifier	Virtual LAN assignment of the interface.
IP Address	IPv4 address of the Cisco WLC and its distribution port.
Interface Type	Static—Management, AP-Manager, Service-Port, and Virtual interfaces. Dynamic—Operator-defined interfaces.
Dynamic AP Management	Dynamic access point management status. The status could be Enabled, Disabled, or Not Supported. This option is disabled by default when LAG is enabled, and any other user-defined dynamic interface is deleted.
IPv6 Address	IPv6 address of the Cisco WLCs management and service port.

Buttons

- New**:** Adds a new interface.

Interfaces > New

Choose **CONTROLLER > Interfaces** and then **New** to navigate to this page.

Add a new Cisco WLC operator-defined interface by entering the following parameters:

- Interface Name—Enter the name of the new operator-defined interface without any spaces. The interface name can be up to 32 characters and can include special characters.
- VLAN Id—Enter the VLAN identifier for this new interface, or enter **0** for an untagged VLAN.

Note IPv6 is not supported on Dynamic Interface.

Buttons

- Back: Returns to the previous page.
- Apply: Displays the Interfaces > Edit page and continues configuring the new operator-defined interface.

Interfaces > Edit

Choose **CONTROLLER > Interfaces** and then click on an interface name to navigate to this page.

The top of this page displays the operator-defined Interface Name, and may include the interface MAC address.

Edit Management, VLAN, Operator-Defined, Service Port, Virtual, and AP-Manager interfaces as described in the following tables.

Management Interface Parameters

Note If you made any changes to the management interface, reboot the controller so that your changes take effect.

Note The IPv4 and IPv6 configurations cannot be changed in redundancy mode.

Table 4-5 Management Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Configuration	
Quarantine	Quarantine status. Check the check box to indicate that this VLAN is a quarantine VLAN. When a client is assigned to a quarantine VLAN, its data switching is always central.

Table 4-5 Management Interface Parameters

Parameter	Description
Quarantine VLAN ID	Quarantine VLAN ID. Enter a nonzero value for the quarantine VLAN ID. **Note** We recommend that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, you must have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, you must have different quarantine VLANs if there is only one NAC appliance in the network.
NAS-ID	ID that is sent to the RADIUS server by the controller through an authentication request to classify users to different groups so that the RADIUS server can send a customized authentication response.
NAT Address **Note** This option is available only for Cisco WLCs that are configured for dynamic AP management.	
Enable NAT Address	NAT addresses that you can enable. Check the check box to deploy the Cisco WLC behind a router or other gateway device that is using a one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's Intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.
NAT IP Address	External NAT IP address.
Interface Address	
VLAN Identifier	Virtual LAN assigned to the interface. Enter **0** for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface. **Note** For Cisco 5500 Series Controllers in a nonlink-aggregation (non-LAG) configuration, the management interface must be on a different VLAN than any dynamic AP-manager interface. Otherwise, the management interface cannot fail over to the port that the AP-manager is on.
IP Address	IPv4 address of the interface.
Netmask	Interface subnet mask (IPv4).
Gateway	Interface gateway router IP address.
IPv6 Address	IPv6 address of the interface.
Prefix Length	Interface subnet mask (IPv6).
IPv6 Gateway	Link local address of the interface gateway router. **Note** An error is thrown when the IPv6 gateway is not a link local IPv6 address.

Table 4-5 Management Interface Parameters

Parameter	Description
Link Local IPv6 Address	IPv6 unicast address that is configured on the interface. Link local IPv6 address is used for addressing a single link for automatic address configuration or neighbor discovery protocol.
Physical Information	
Port Number	Primary port for the interface.
Backup Port	Backup port. If the primary port for an interface fails, the interface moves to the backup port.
Active Port	Active port for the interface.
Enable Dynamic AP Management	AP-manager interface. **Note** Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface. **Caution** Do not define a backup port for an AP-manager interface. Port redundancy is not supported for AP-manager interfaces. If the AP-manager interface fails, all of the access points connected to the controller through that interface are evenly distributed among the other configured AP-manager interfaces.
DHCP Information	
Primary DHCP Server	Interface that uses this DHCP server first to obtain an IPv4 address. **Note** IPv6 is not supported for DHCP.
Secondary DHCP Server	Interface that uses this DHCP server as a backup to obtain an IP address. **Note** IPv6 is not supported for DHCP.

Table 4-5 Management Interface Parameters

Parameter	Description
DHCP Proxy Mode	Drop-down list from which you can choose the DHCP Proxy Mode that can be one of the following: • Global—Uses the global DHCP proxy mode on the controller. • Enabled—Enables the DHCP proxy mode on the interface. When you enable DHCP proxy on the controller, the controller unicasts the DHCP requests from the client to the configured servers. You must configure at least one DHCP server on either the interface associated with the WLAN or on the WLAN. • Disabled—Disables the DHCP proxy mode on the interface. When you disable the DHCP proxy on the controller, the DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled. **Note** The DHCP Proxy mode is disabled by default when the interface uses IPv6 address. DHCP does not support IPv6.
Enable DHCP Option 82	Check box that allows you to enable the DHCP Option 82 on the dynamic interface. DHCP option 82 provides additional security when DHCP is used to allocate network addresses.
Enable DHCP Option 82-Link Select	Option 82-Link Select pads the extra information to get the IP address in the required subnet.
Link Select relay source	Allows to specify the required interface/subnet on which the DHCP client require an IP address.
Enable DHCP Option 82 - VPN Select	Enables the VPN select. This is used in conjunction with the link select relay source.
VPN select - VRF Name	VPN Select-VRF Name is a string that is used to select a DHCP pool based on the VRF name.
VPN select - VPN ID	VPN Select-VPN ID is an ASCII value that is used to select a DHCP pool based on the identifier.
Access Control List	
ACL Name	Drop-down list from which you can choose an IPv4 ACL. **Note** Applying an ACL to the management interface does not affect wired devices. To block access to wired devices, you must configure an ACL on the upstream device port.
IPv6 ACL Name	Drop-down list from which you can choose an IPv6 ACL. **Note** Guest LAN does not support IPv6 ACL.

Table 4-5 Management Interface Parameters

Parameter	Description
URL ACL	Drop-down list from which you can choose the URL ACL profile for the interface. Interface URL ACL profiles have higher priority than WLAN URL ACL profiles.
mDNS	
mDNS Profile	Drop-down list from which you can choose the mDNS profile for the interface. Interface mDNS profiles have higher priority than WLAN mDNS profiles. Clients receive service advertisements only for the services associated with the profile.

Redundancy-Management Interface Parameters

Table 4-6 Redundancy-Management Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
Interface Address	
IP Address	IP address of the interface.

Service Port Interface Parameters

Table 4-7 Service Port Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Interface Address	
IPv4	
DHCP Protocol	Check box that you check to have the Service Port interface use a DHCP server to obtain its IP address.
IP Address	IP address of the Service Port interface.
Netmask	Interface subnet mask.
Note The service port cannot be configured with the same IP address or on the same subnet as the network distribution system.	
IPv6	
SLACC	Enable SLACC to auto-configure the IPv6 address. You can configure a static IPv6 address by disabling the check box.
Primary Address	This field is enabled for static IPv6 configuration. Enter the IPv6 address. For SLACC, the service port generates the IPv6 address provided a valid prefix length is used.

Table 4-7 Service Port Interface Parameters

Parameter	Description
Prefix Length	Enter IPv6 prefix length of the management interface. The valid prefix length is between 1-127.
Link Local Address	The link-local IPv6 address.

Virtual Interface Parameters

Note If you made any changes to the virtual interface, reboot the controller so that your changes take effect.

Table 4-8 Virtual Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Interface Address	
IP Address	Gateway IP address. Any fictitious, unassigned IP address (such as 10.1.10.1) to be used by Layer 3 Security and Mobility managers. Reboot the Cisco WLC to have this change take effect.
DNS Host Name	Gateway hostname. Used by Layer 3 Security and Mobility managers to verify the source of certificates when Web Auth is enabled. Reboot the Cisco WLC to have this change take effect.
Note You must configure the virtual gateway address to enable Layer 3 Web Auth, configured on the Editing WLANs page.	

AP-Manager Interface Parameter

Note For Cisco 5508 WLCs, you do not have to configure an AP-manager interface because the management interface acts like an AP-manager interface by default.

Table 4-9 AP Manager Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Interface Address	
VLAN Identifier	Virtual LAN assigned to the interface.
IP Address	IP address of the Cisco WLC Layer 3 CAPWAP protocol manager. This IP address cannot be the same IP address used by the management interface.

Table 4-9 AP Manager Interface Parameters

Parameter	Description
Netmask	Interface subnet mask.
Gateway	Interface gateway router IP address.
Physical Information	
Port Number	Primary port for the interface.
Backup Port	Backup port. If the primary port for an interface fails, the interface moves to the backup port.
Active Port	Active port for the interface.
Enable Dynamic AP Management	AP-Manager interface. Select the check box to indicate that the interface is an AP-manager interface. **Note** This enables only IPv4 based AP manager for dynamic interface.
DHCP Information	
Primary DHCP Server	DHCP server that the interface uses first to obtain an IP address.
Secondary DHCP Server	DHCP server that the interface uses as a backup to obtain an IP address.
Access Control List	
ACL Name	Access control list names currently available on the Access Control Lists page.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Note Applying interface changes may cause WLANs to temporarily drop client connections. You are prompted to confirm the changes if this is the case.

Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where an interface group can be reused either while configuring multiple WLANs or while overriding a WLAN interface per AP group. An interface group can contain either quarantine or nonquarantine interfaces.

A WLAN can be mapped to a single interface or multiple interfaces using an interface group. Wireless clients that are associated to this WLAN get their IP addresses from a pool of subnets that are identified by the interfaces using a MAC based hashing algorithm.

VLAN select feature also enables you to associate a client to different subnets based on the foreign controller that they are connected to. The anchor controller maintains a mapping between the foreign MAC and the interface group.

Choose **CONTROLLER > Interface Groups** to navigate to this page.

- To edit the parameters for an interface, click the interface name (Interfaces > Edit).

- To remove an interface group, hover your cursor over the blue drop-down arrow for the interface group and choose **Remove**. You are prompted for confirmation of the interface group removal.

Note A WLAN can be mapped to a single interface or multiple interfaces. A maximum of 20 interfaces can be added to an interface group.

Table 4-10 Controller Interface Groups Parameters

Parameter	Description
Interface Group Name	Name of the interface group.
Description	Description for the interface group.
mDNS Profile	Drop-down list from which you can choose the mDNS profile for the interface group. Clients receive service advertisements only for the services associated with the profile. Interface group mDNS profiles have higher priority than WLAN mDNS profiles.

Buttons

Add Group**:** Adds a new interface group.

Interface Groups > Add Group

Choose **CONTROLLER > Interface Groups** and then click **Add Group** to navigate to this page.

Add a new Cisco WLC operator-defined interface group by entering the following parameters:

- Interface Group Name—Enter the name of the new operator-defined interface group. The interface group name can be up to 32 characters and can include special characters.
- Description—Enter the description for this new interface group.

Buttons

- Add: Adds a new interface group.
- Cancel: Disregards any settings or changes.

Interface Groups > Edit

Choose **CONTROLLER > Interface Groups** and then click on an interface group name to navigate to this page.

Table 4-11 Management Interface Parameters

Parameter	Description
Interface Group Name	Name of the interface group.
Property	Quarantine status of the VLAN.

Table 4-11 Management Interface Parameters

Parameter	Description
Interface Name	Name of the interface.
Add Interface	Add Interface button that allows you to add an interface to the interface group. You can choose the interface to add from the Interface Name drop-down list.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Multicast

Choose **CONTROLLER > Multicast** to navigate to this page.

This page enables you to configure Internet Group Management Protocol (IGMP) snooping and to set the IGMP timeout.

When you enable IGMP snooping, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients that are listening to any multicast group. The access points then forward multicast packets only to those clients.

Table 4-12 Multicast

Parameter	Description
Enable Global Multicast Mode	Multicast mode that you can enable or disable. Disabled—Disables multicast support on the Cisco WLC (default). Unicast—Enables the controller when it receives a multicast packet to forward the packet as a unicast packet to all the associated access points. FlexConnect supports only Unicast Mode. Multicast—Enables multicast support on the Cisco WLC. Enter the IP address of the multicast group in the Multicast Group Address text box.
Enable IGMP Snooping	IGMP snooping that you can enable or disable. The default is enable.
IGMP Timeout (seconds)	IGMP timeout, in seconds. Valid values are from 30 and 7200. When the timeout expires, the controller sends a query on all WLANs, causing all clients that are listening to a multicast group to send a packet back to the controller.
IGMP Query Interval (seconds)	IGMP query interval, in seconds that you can set. The query interval value is the frequency at which the controller sends the IGMP queries. Valid range is from 15 and 2400 seconds.
Enable MLD Snooping	Multicast Listener Discovery (MLD) that you can enable for efficient distribution of IPv6 multicast data to clients and routers in a switched network. By default it is enabled. To enable IPv6 multicast, both Global Multicast Mode and MLD snooping must be enabled.

Table 4-12 Multicast

Parameter	Description
MLD Timeout (seconds)	MLD timeout, in seconds. Valid values are from 30 and 7200. When the timeout expires, the controller sends a query on all WLANs, causing all clients that are listening to a multicast group to send a packet back to the controller.
MLD Query Interval (seconds)	MLD query interval, in seconds that you can set. The query interval value is the frequency at which the controller sends the MLD queries. Valid range is from 15 and 2400 seconds.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Network Routes

This page provides a summary of existing IPv4 and IPv6 based service port network routes to network or element management systems on a different subnet. You can choose **IP Address**, **IP Netmask**, or **Gateway IP Address**.

Network Routes > IPv4 Routes

This page provides a summary of existing IPv4 based service port network routes to network or element management systems on a different subnet. You can choose **IP Address**, **IP Netmask**, or **Gateway IP Address**.

- To remove a network route, hover your cursor over the blue drop-down arrow for the route and choose **Remove**. You are prompted to confirm the Network Route removal.

Buttons

New: Adds a new IPv4 based network route.

IPv4 Routes > New

Choose **CONTROLLER > Network Routes > IPv4 Routes** and then click **New** to navigate to this page.

To add a new network route for the service port.

- Route Type—Select IPv4 as the route type.

Enter the following information in the text boxes:

- IP Address—Destination network IP address range
- IP Netmask—Destination subnet mask
- Gateway IP Address—IP address of the service port gateway router

Buttons

- Back: Returns to the previous page.

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

Network Routes > IPv6 Routes

Choose **CONTROLLER > Network Routes > IPv6 Routes** to navigate to this page.

This page provides a summary of existing IPv6 based service port network routes to network or element management systems on a different subnet. You can choose **IP Address**, **IP Netmask**, or **Gateway IP Address**.

- To remove a network route, hover your cursor over the blue drop-down arrow for the route and choose **Remove**. You are prompted to confirm the Network Route removal.

Buttons

New: Adds a new IPv6 based network route.

IPv6 Routes > New

Choose **CONTROLLER > Network Routes > IPv6 Routes** and then click **New** to navigate to this page.

To add a new network route for the service port.

Route Type—Select IPv6 as the route type.

Enter the following information in the text boxes:

- IP Address—Destination network IP address range
- IP Netmask/Prefix Length—The prefix length assigned to the destination IPv6 address.
- Gateway IP Address—IP address of the service port gateway router

Buttons

- Back: Returns to the previous page.

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

Fabric Configuration > Control Plane

Choose **CONTROLLER > Fabric Configuration > Control Plane** to navigate to this page.

You can enable fabric and configure parameters on the enterprise and guest controllers, using the **Fabric Enable/Disable** button at the top of the screen.

Table 4-13 Fabric Control Plane Configuration Details

Parameter	Description
Enterprise	
Primary IP Address	Primary IP address for the enterprise fabric.
Pre Shared Key	The secret value for the pre-shared key.
Secondary IP Address	Secondary IP address for the enterprise fabric.
Pre Shared Key	The secret value for the pre-shared key.
Connection Status	Displays the connection status.
Guest	
Primary IP Address	Primary IP address for the guest fabric.
Pre Shared Key	The secret value for the pre-shared key.
Secondary IP Address	Secondary IP address for the guest fabric.
Pre Shared Key	The secret value for the pre-shared key.
Connection Status	Displays the connection status.

Fabric Configuration > Interface

Choose **CONTROLLER > Fabric Configuration > Interface** to navigate to this page.

This page provides a summary of existing fabric networks. You can view the Fabric Interface Name, L2 Instance ID, Network IP address, IP subnet mask, and L3 Instance ID. To remove a fabric interface, hover your cursor over the blue drop-down arrow for the interface and choose **Remove**. You are prompted to confirm the Fabric Interface removal.

Buttons

New: Adds a new fabric interface.

Table 4-14 Fabric Interface Configuration Details

Parameter	Description
Fabric Interface Name	Identifier for the enterprise fabric.
L2 Instance ID	Layer 2 instance ID.
Network IP	IP address of the network.
Subnet Mask	Subnet mask.
L2 Instance ID	Layer 3 instance ID.

Buttons

Apply: Commits your changes.

Fabric Configuration > Templates

Choose **CONTROLLER > Fabric Configuration > Templates** to navigate to this page.

This page provides a summary of existing fabric configuration templates. You can view the Fabric ACL templates and its Status. To remove a fabric template, hover your cursor over the blue drop-down arrow for the interface and choose **Remove**. You are prompted to confirm the Fabric Template removal.

Buttons

New: Adds a new fabric template.

Copy: Copies parameters from an existing template.

Table 4-15 Fabric Template Copy Details

Parameter	Description
Fabric Template Name	Identifier for the enterprise fabric template.
Existing Fabric Templates	Lists the existing templates.

Buttons

Apply: Commits your changes.

Redundancy

In a high availability (HA) architecture, one controller is in the Active state and a second controller is in the Standby state, which continuously monitors the health of the Active controller through a direct wired connection over a dedicated HA port. Both controllers share the same configurations including the IP address of the management interface.

Choose **CONTROLLER > Redundancy to configure the redundancy parameters and peer network routes:**

- To enable redundancy and configure redundancy parameters on the primary and secondary controllers, choose **CONTROLLER > Redundancy > Global Configuration**.
- To configure service port network routes for the peer controller, choose **CONTROLLER > Redundancy > Peer Network Route**.

Redundancy > Global Configuration

Choose **CONTROLLER > Redundancy > Global Configuration** to navigate to this page.

You can enable redundancy and configure redundancy parameters on the primary and secondary controllers.

The controllers reboot to negotiate the HA role based on the configuration. The standby controller downloads the configuration from the active controller and reboots. In the next bootup process, after the role of the controller is determined, the standby controller tries to validate the configuration again to establish itself as the controller in the Standby state.

After the controllers are rebooted and the XML configuration is synchronized, the active controller transitions to the Active state, and the standby controller transitions to the Standby HOT state. From this point, GUI, Telnet, and SSH for the standby controller on the management interface do not work because all the configurations and management have to be done through the active controller. The standby controller can only be managed through the console or the service port. Also, when a controller transitions to the Standby HOT state, the Standby keyword is automatically appended to the prompt of the controller.

To see the redundancy status of the active controller, choose **Monitor > Redundancy > Summary** to navigate the Redundancy Summary page.

Table 4-16 Global Configuration Parameters

Parameter	Description
Redundancy Mgmt IP	Redundancy Management IP address of the controller. Ensure that the Redundant Management IP address for both controllers is the same.
Peer Redundancy Mgmt IP	Redundancy Management IP address of the peer controller. Ensure that the Peer Redundant Management IP address for both the controllers is the same.
Redundancy port IP	IP address of the redundancy port of the controller. Controllers in a HA environment use the redundancy port to do HA role negotiation. The redundancy port is responsible for configuration and operational data synchronization between active and standby controllers.
Peer Redundancy port IP	IP address of the redundancy port of the peer controller. The redundancy port in standalone controllers and the redundancy VLAN in Cisco WiSM2 are assigned an automatically generated IP address where the last two octets are picked from the last two octets of the Redundancy Management Interface. The first two octets are always 169.254. For example, if the IP address of the Redundancy Management Interface is 209.165.200.225, the IP address of the redundancy port is 169.254.200.225.
Redundant Unit	Controller that can be primary or secondary.
Mobility MAC Address	MAC address that is an identifier for the active and standby controller pair. If an HA pair is to be added as a mobility member for a mobility group, the mobility MAC address (instead of the system MAC address of the active or standby controller) should be used. Normally, the mobility MAC address is chosen as the MAC address of the active controller and you do not have to manually configure this.
Keep Alive Timer	Timer that controls how often the primary controller sends a heartbeat keepalive signal to the standby controller. The range is from 100 to 1000 milliseconds, in multiples of 50.
Keep Alive Retries	The number of times keep alive packets are send between the HA peers. The valid range is between 100 to 1000 milliseconds.

Table 4-16 Global Configuration Parameters

Parameter	Description
Peer Search Timer	Timer that controls how often the primary controller sends a peer search signal to the standby controller. The range is from 60 to 300 seconds.
Management Gateway Failure	If the Management interface gateway is unreachable, then the HA tigger can be enabled /disabled.
SSO	Drop-down list from which you can choose **Enable** to enable AP and client SSO. After you enable an SSO, the service port peer IP address and the service port netmask appear on the configuration page. Note that the service port peer IP address and the netmask can be pushed to the peer only if the HA peer is available and operational. When you enable high availability, you do not have to configure the service port peer IP address and the service port netmask parameters. You must configure the parameters only when the HA peer is available and operational. After you enable SSO, both the controllers are rebooted. During the reboot process, the controllers negotiate the HA role through the redundant port based on the configuration. If the controllers cannot reach each other through the redundant port or through the Redundant Management Interface, the standby controller goes into the maintenance mode.
Service Port Peer IP	IP address of the service port of the peer controller. When the HA pair becomes available and operational, you can configure the peer service port IP address and netmask when service port is configured as static. If you enable DHCP on the service port, you do not have to configure these parameters on the Global Configuration page.
Service Port Peer Netmask	Netmask of the service port of the peer controller.

Buttons

- Apply: Commits your changes.
- Save Configuration: Saves the changes

Redundancy > Peer Network Route

Choose **CONTROLLER > Redundancy > Peer Network Route** to navigate to this page.

This page provides a summary of existing service port network routes of the peer controller to network or element management systems on a different subnet. You can view the IP address, IP netmask, and gateway IP address. To remove a peer network route, hover your cursor over the blue drop-down arrow for the route and choose **Remove**. You are prompted to confirm the Network Route removal.

Buttons

- New: Adds a new peer network route.

Internal DHCP Server

Choose **CONTROLLER > Internal DHCP Server** to navigate to this page. From here you can choose the following:

- **CONTROLLER > Internal DHCP Server > DHCP Scope** to view the existing DHCP server scopes.

  See Internal DHCP Server > DHCP Scope for more information.

- **CONTROLLER > Internal DHCP Server > DHCP Allocated Lease** to view the MAC address, the IP address, and the remaining lease time for wireless clients.

  See Internal DHCP Server > DHCP Allocated Lease for more information.

Internal DHCP Server > DHCP Scope

Choose **CONTROLLER > Internal DHCP Server > DHCP Scope** to navigate to this page.

The controllers have built-in DHCP relay agents. However, when you want network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes (Dynamic Host Configuration Protocol servers) that assign IP addresses and subnet masks to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. (Only lightweight access points are supported.)

Typically, one Cisco WLC can have one or more DHCP scopes that each provide a range of IP addresses. This page shows the existing DHCP server scope names.

Each DHCP Scope displays the following entries, which are a subset of those set on the DHCP Scope > Edit page:

- Scope Name
- Address Pool—IP address range. This pool must be unique for each DHCP scope and must not include the static IP addresses of routers and other servers
- Lease Time—Number of seconds that an IP address is granted to a client or access point
- Status—Scope is Enabled or Disabled

Click the scope name to go to the DHCP Scope > Edit page to change the DHCP scope settings.

Remove a DHCP Scope by hovering your cursor over the blue drop-down arrow and choosing **Remove**. You are prompted to confirm the DHCP Scope removal.

Buttons

- New**:** Creates a new DHCP Scope.

DHCP Scope > New

Choose **CONTROLLER > Internal DHCP Server > DHCP Scope** and then click **New** to navigate to this page.

The controllers have built-in DHCP relay agents. However, if you want network segments that do not have a separate DHCP server, the controllers also have built-in DHCP scopes (servers) that assign IP addresses and subnet masks to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. (Only lightweight access points are supported.)

Typically, one Cisco WLC can have one or more DHCP scopes that each provide a range of IP addresses. This page enables you to add a DHCP server scope name.

Add a new DHCP scope by entering the DHCP scope name and then clicking **Apply**. The Cisco WLAN Solution saves the DHCP scope name and returns you to the Internal DHCP Server > DHCP Scope page. On the Internal DHCP Server > DHCP Scope page, click the scope name to set the DHCP scope parameters on the DHCP Scope > Edit page.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

DHCP Scope > Edit

Choose **CONTROLLER > Internal DHCP Server > DHCP Scope** and then click the scope name to navigate to this page.

The controllers have built-in DHCP relay agents. However, when you want network segments that do not have a separate DHCP server, the controllers also have built-in DHCP scopes (servers) that assign IP addresses and subnet masks to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. (Only lightweight access points are supported.)

Typically, one Cisco WLC can have one or more DHCP scopes that each provide a range of IP addresses. This page enables you to edit a DHCP server scope.

This page shows the name of the DHCP Scope you are editing.

Table 4-17 DHCP Scope Parameters

Parameters	Description
Pool Start Address	Starting IP address in the range assigned to clients and access points. This pool must be unique for each DHCP scope. The pool must not include the static IP addresses of routers and other servers.
Pool End Address	Ending IP address in the range assigned to clients and access points. This pool must be unique for each DHCP scope. The pool must not include the static IP addresses of routers and other servers.
Network	Network served by this DHCP scope. This IP address is used by the management interface with the netmask applied, listed on the Interfaces page.
Netmask	Subnet mask assigned to all clients and access points.

Table 4-17 DHCP Scope Parameters

Parameters	Description
Lease Time	How many seconds an IP address is granted to a client or access point, from 120 to 8640000.
DNS Domain Name	Optional DNS (Domain Name System) domain name of this DHCP scope for use with one or more DNS servers.
DNS Servers	IP address of the optional DNS servers. Each DNS server must be able to update a client DNS entry to match the IP address assigned by this DHCP scope.
NetBIOS Name Servers	IP address of the optional Microsoft NetBIOS (Network Basic Input Output System) name servers, such as a WINS (Windows Internet Naming Service) server.
Status	Setting that enables you to configure the DHCP scope. The values can be Enable or Disable.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Internal DHCP Server > DHCP Allocated Lease

Choose **CONTROLLER > Internal DHCP Server > DHCP Allocated Leases** to navigate to this page.

This page displays the MAC address, the IP address, and the remaining lease time for wireless clients.

Mobility Management

Choose **CONTROLLER > Mobility Management** to navigate to this page. From here you can choose the following:

- **CONTROLLER > Mobility Management > Mobility Configuration** to configure hierarchical mobility on the controller.

  See Mobility Management > Mobility Configuration for more information.
- **CONTROLLER > Mobility Management > Mobility Groups** to view existing mobility group members.

  See Mobility Management > Mobility Groups for more information.
- **CONTROLLER > Mobility Management > Mobility Anchor Config** to configure the symmetric mobility tunneling for mobile clients.

  See Mobility Management > Mobility Anchor Configuration for more information.

- **CONTROLLER > Mobility Management > Multicast Messaging** to configure the controller to use multicast to send the Mobile Announce messages.

  See Mobility Management > Mobility Multicast Messaging for more information.
- **CONTROLLER > Mobility Management > Switch Peer Group** to view existing mobility switch peer groups and their details.

  See Mobility Management > Switch Peer Group for more information.
- **CONTROLLER > Mobility Management > Switch Peer Group Member** to add or remove members to the switch peer group.

  See Mobility Management > Switch Peer Group Member for more information.
- **CONTROLLER > Mobility Management > Mobility Controller** to view all the mobility controllers and their link status.

  See Mobility Management > Mobility Controllers for more information.
- **CONTROLLER > Mobility Management > Mobility Clients** to view all the mobility clients and their parameters.

  See Mobility Management > Mobility Clients for more information.

Mobility Management > Mobility Configuration

Choose **CONTROLLER > Mobility Management > Mobility Configuration** to navigate to this page.

This page allows you to enable New Mobility and configure its parameters.

Table 4-18 Mobility Configuration Parameters

Parameter	Description
General	
Enable New Mobility	Check box that you can check to enable or disable New Mobility. **Note** When you enable hierarchical mobility, you must save the configuration and reboot the controller.
Mobility Parameters	
Mobility Oracle	Check box that you can select to enable the controller as a Mobility Oracle. The Mobility Oracle is optional, it maintains the client database under one complete mobility domain.
Multicast Mode	Check box that you can select to enable or disable multicast mode in a mobility group.
Multicast IP Address	Multicast IP address of the switch peer group.
Mobility Oracle IP Address	IP address of the Mobility Oracle. You cannot enter the value if you have checked the Mobility Oracle check box.
Mobility Controller Public IP Address	IP address of the controller, if there is no NAT. If the controller has NAT configured, the public IP address will be the NATed IP address.

Table 4-18 Mobility Configuration Parameters

Parameter	Description
Mobility Keep Alive Interval	Amount of time (in seconds) between each ping request sent to an peer controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.
Mobility Keep Alive Count	Number of times a ping request is sent to an peer controller before the peer is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
Mobility DSCP Value	DSCP value that you can set for the mobility controller. The valid range is 0 to 63, and the default value is 0.

Buttons

- Apply**:** Sends data to the controller but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Mobility Groups

Choose **CONTROLLER > Mobility Management > Mobility Groups** to navigate to this page.

This page lists existing mobility group members by their MAC address and IP address and also indicates whether the mobility group member is local (this Cisco WLC) or remote (any other mobility group member). The first entry is the local Cisco WLC, which cannot be deleted. The following entries are other controllers in the mobility group that can be deleted at any time by choosing **Remove**. You can also view the hash key of the virtual controller in your domain.

Note You can ping any of the static mobility group members by choosing **Ping**.

You set the Mobility Group Name that is set on the General page.

Buttons

- New**:** Adds a new mobility group member.
- Edit All: Displays the Mobility Group Member > Edit All page.

Mobility Group Member > New

Choose **CONTROLLER > Mobility Management > Mobility Groups** and then click **New** to navigate to this page.

This page enables you to add mobility group members.

- Member IP Address—Enables you to enter the management interface IP address of the controller to be added. Both, IPv4 and IPv6 are supported.

Note If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller's management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

Also, client mobility among controllers works only if you enable auto-anchor mobility or symmetric mobility tunneling. Asymmetric tunneling is not supported when mobility controllers are behind a NAT device.

- Public IP Address(IPv4/IPv6)—IP address of the Cisco WLC if there is no NAT.
- Member MAC Address—Enables you to enter the MAC address of the controller to be added. Both, IPv4 and IPv6 are supported.
- Group Name—Enables you to enter the name of the mobility group.

Note The mobility group name is case sensitive.

- Hash—Enables you to configure hash key of the peer mobility controller. This is not supported for IPv6 members.

Note You must configure the hash only if the peer mobility controller is a virtual controller.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Group Member > Edit All

Choose **CONTROLLER > Mobility Management > Mobility Groups** and then click **Edit All** to navigate to this page.

This page enables you to edit all the existing Mobility Group members' MAC addresses, IPv4 and IPv6 addresses in a text box and then to cut and paste all the entries from one Cisco WLC to the other controllers in the mobility group.

You can edit existing entries in the box and/or paste new entries into the box. In all cases, leave one space between the MAC address and IP address on each line.

The text box on this page makes it easy to avoid data-entry errors while copying the mobility group members list to all the controllers in the same mobility group. Some guidelines are as follows:

- Notice that the text box starts with the local Cisco WLC MAC address and IPv4/IPv6 address.
- In the text box, add the MAC addresses, IPv4/IPv6 addresses, and the mobility group name for the rest of the controllers in the same geographical location (such as a campus or building) that you want to add to the static mobility group.

- When you have added all the Cisco WLC MAC addresses and IP v4/IPv6 addresses to the static mobility group, you can cut and paste the complete list into the corresponding boxes in the Mobility Group Member > Edit All pages in other mobility group member Web User Interface pages.

Note The mobility Group supports a maximum of 72 mobility peers.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Mobility Anchor Configuration

Choose **CONTROLLER > Mobility Management > Mobility Anchor Config** to navigate to this page. This page enables you to configure the symmetric mobility tunneling for mobile client features.

Guest N+1 Redundancy

The guest N+1 redundancy feature enables the foreign controller to periodically send ping requests to each anchor controller in the mobility group and enables you to configure the number and interval of requests sent to each anchor controller. Once a failed anchor controller is detected, all of the clients anchored to this controller are deauthenticated so that they can quickly become anchored to another controller.

When using the guest N+1 redundancy and mobility failover features with a firewall, ensure that the following ports are open:

- UDP 16666 for tunnel control traffic
- UDP 16667 for encrypted traffic
- IP Protocol 97 for user data traffic
- TCP 161 and 162 for SNMP

To view the current state of the data and control paths of controllers that have already been configured as mobility anchors, use the Mobility Anchors page.

Symmetric Mobility Tunneling

Note When controllers in the mobility list are running different software releases (such as 5.2, 6.0, and 7.0), Layer 2 or Layer 3 client roaming is not supported between them. It is supported only between controllers running the same release.

The controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. This mobility is asymmetric so that the client traffic to the wired network is routed directly through the foreign controller.

This mechanism breaks when an upstream router has reverse path filtering (RPF) enabled. In this case, the client traffic is dropped at the router because the RPF check ensures that the path back to the source address matches the path from which the packet is coming.

When symmetric mobility tunneling is enabled, all client traffic is sent to the anchor controller and can then successfully pass the RPF check.

You should also enable symmetric mobility tunneling if a firewall installation in the client packet path may drop the packets whose source IP address does not match the subnet on which the packets are received.

Note Although a Cisco 2000 Series Controller cannot be designated as an anchor for a WLAN when using auto-anchor mobility, it can serve as an anchor in symmetric mobility tunneling to process and forward the upstream client data traffic tunneled from the foreign controller.

Mobility Anchor Config Parameters

Table 4-19 Mobility Anchor Config Parameters

Parameter	Description
Keep Alive Count	Number of times a ping request is sent to an anchor controller before the anchor is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
Keep Alive Interval	Amount of time (in seconds) between each ping request sent to an anchor controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.
Symmetric Mobility Tunneling mode	Enabled (Default).
DSCP Value	DSCP value that you can set for the mobility anchor. The valid range is 0 to 63.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Mobility Multicast Messaging

Choose **CONTROLLER > Mobility Management > Multicast Messaging** to navigate to this page.

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it.

You can configure the controller to use multicast to send the Mobile Announce messages. This behavior enables the controller to send only one copy of the message to the network, which designates it to the multicast group that contains all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that it be enabled or disabled on all group members.

- Enable Multicast Messaging—Enables the controller to use multicast to send the Mobile Announce messages. If you leave it unselected, the controller uses unicast mode to send the Mobile Announce messages. The default value is unselected.
- Local Group Multicast IPv4 Address—Enables you to enter the multicast group IPv4 address for the local mobility group. This address is used for multicast mobility messaging.

Note To use multicast messaging, you must configure the IPv4 address for the local mobility group.

- Mobility Group—Lists the names of all the currently configured mobility groups.

Note IPv6 is not supported for mobility multicast.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Multicast Messaging > Edit

Choose **CONTROLLER > Mobility Management > Multicast Messaging** and then click the name of the local mobility group to navigate to this page.

- Mobility Group—Lists the name of all the mobility group.
- Local Group Multicast IP Address—Enables you to enter the multicast group IP address for the nonlocal mobility group. This address is used for multicast mobility messaging.

Note If you do not configure the multicast IP address for nonlocal groups, the controller uses unicast mode to send mobility messages to those members.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Switch Peer Group

Choose **CONTROLLER > Mobility Management > Switch Peer Group** to navigate to this page.

This page lists all the switch peer groups and their details like bridge domain ID, multicast IP address, and status of the multicast mode. Click the name of the switch peer group to navigate to the Edit page and update the parameters if required.

Mobility Management > Switch Peer Group Member

Choose **CONTROLLER > Mobility Management > Switch Peer Member** to navigate to this page.

This page lists all the members of the switch peer group along with their group name, IP address, and public IP address.

Buttons

- New: Adds a new member to the switch peer group.

Mobility Management > Mobility Controllers

Choose **CONTROLLER > Mobility Management > Mobility Controllers** to navigate to this page.

This page lists all the mobility controllers. Mobility Controllers are controllers that provide mobility management services for an inter proximity group.

You can see the total number of mobility controllers and details like IP address, MAC address, client count, and link status.

Buttons

- New: Adds a new member to the switch peer group.

Mobility Management > Mobility Clients

Choose **CONTROLLER > Mobility Management > Mobility Clients** to navigate to this page.

This page lists the total number of mobility clients and their parameters.

Table 4-20 Mobility Client Parameters

Parameter	Description
Client MAC Address	MAC address of the mobility client.
Client IP Address	IP address of the mobility client.
Anchor MC IP Address	IP address of the anchor Mobility Controller.
Anchor MC Public IP Address	Public IP address of the anchor Mobility Controller.
Foreign MC IP Address	IP address of the foreign Mobility Controller.
Foreign MC Public IP Address	Public IP address of the foreign Mobility Controller.
Client Association Time	Time when the mobility client associated with the Mobility Controller.
Client Entry Update Timestamp	Timestamp when the client entry is updated.

Ports

Choose **CONTROLLER > Ports** to navigate to this page.

This page displays the status of each physical port on the Cisco WLC.

- To edit global parameters across all ports, click **Configure All** to open the Ports > Configure page.
- To edit the parameters for a single port, click the port number link for the port you want to configure. This action brings up a Ports > Configure page.

Note The physical mode and status may reflect different values depending on the link status. For example, the physical mode may be set to Auto while the actual link is running at 10 Mbps half duplex.

Table 4-21 Summary Parameters

Parameter	Description
Port No	Port number on the Cisco WLC.
Admin Status	State of the port as either Enabled or Disabled.
Physical Mode	Configuration of the port physical interface. Available values are as follows: • Auto • 100 Mbps Full Duplex • 100 Mbps Half Duplex • 10 Mbps Full Duplex • 10 Mbps Half Duplex **Note** In Cisco NM-AIR-WLC6-K9, Cisco 5500 Series, and Cisco Flex 7500 Series controllers, the physical mode is always set to Auto.
Physical Status	Displays the actual port physical interface. Available values are as follows: • Auto • 100 Mbps Full Duplex • 100 Mbps Half Duplex • 10 Mbps Full Duplex • 10 Mbps Half Duplex • 10000 Mbps Full Duplex
Link Status	Status of the link. Values are Link up or Link Down
Link Trap	Port that is set to send a trap when the link status changes. Values include Enable or Disable.

Buttons

- Configure All**:** Opens the Global Port configuration data page.

Ports > Configure

Choose **CONTROLLER > Ports** and then click **ConfigureAll** to navigate to this page.

This page enables you to change the parameters of all front-panel physical ports on the Cisco WLC simultaneously.

Table 4-22 Port Configuration Details

Parameter	Description	Range
Admin Status	Sets the state of all ports to Don't Apply, Enable or Disable.	
Physical Mode	Displays the physical mode of all ports.	• Don't Apply • Auto • 100 Mbps Full Duplex • 100 Mbps Half Duplex • 10 Mbps Full Duplex • 10 Mbps Half Duplex • 10000 Mbps Full Duplex **Note** In Cisco NM-AIR-WLC6-K9, 5500 series, and 7500 series controllers, the physical mode is always set to Auto.
Link Trap	Sets all ports to send or not to send a trap when link status changes. The factory default is Don't Apply.	

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Ports > Configure

Choose **CONTROLLER > Ports** and then click on a **Port No** to navigate to this page.

This page enables you to change the parameters of a single physical port on the Cisco WLC.

General Port Configuration

Table 4-23 General Port Configuration Parameters

Parameter	Description	Range
Port No	Identifies the current port.	13 for optional 1000Base-T or 1000Base-SX module 25 for optional 1000Base-T or 1000Base-SX module 1 for Cisco 4100 Series Wireless LAN Controller 1000Base-SX ports.
Admin Status	Sets the state of the port.	Enable Disable

Table 4-23 General Port Configuration Parameters

Parameter	Description	Range
Physical Mode	Sets the physical mode of the port.	Auto 100 Mbps Full Duplex 100 Mbps Half Duplex 10 Mbps Full Duplex 10 Mbps Half Duplex 10000 Mbps Full Duplex **Note** In Cisco NM-AIR-WLC6-K9, 5500 series, and 7500 series controllers, the physical mode is always set to Auto.
Physical Status	Displays the current physical port interface status.	100 Mbps Full Duplex 100 Mbps Half Duplex 10 Mbps Full Duplex 10 Mbps Half Duplex 10000 Mbps Full Duplex
Link Status	Displays the status of the link.	Link Up Link Down
Link Trap	Sets the port to send or not to send a trap when link status changes. The default is enabled.	Enable Disable

NTP

Choose **CONTROLLER > NTP** to navigate to this page. From here you can choose the following:

- **CONTROLLER > NTP > Server** to configure the Network Time Protocol parameters.

  See NTP > NTP Servers for more information.
- **CONTROLLER > NTP > Keys** to configure the Network Time Protocol keys.

  See NTP > NTP Keys for more information.

NTP > NTP Servers

Choose **CONTROLLER > NTP > Server** to navigate to this page. Use this page to set the Network Time Protocol parameters.

Table 4-24 NTP Parameters

Parameter	Description
NTP Polling Interval Seconds	Network polling time interval in seconds.
Server Index	NTP server index. The Cisco WLC tries Index 1 first, and then Index 2 through 3, in a descending order. If your network is using only one NTP server, you should use Index 1.
Server Address (IPv4/IPv6)	IP address or a Fully Qualified Domain Name (FQDN) of the NTP server.
Key Index	NTP key index.
NTP Msg Auth Status	Authentication Status of NTP message. It could either be AUTH SUCCESS or AUTH DISABLE.

Click a server index number to go to the NTP Server > Edit page to change the NTP server IP address.

Remove an NTP server entry by hovering your cursor over the blue drop-down arrow and choosing **Remove**. You are prompted for confirmation of the NTP server removal.

Ping the NTP server by hovering your cursor over the blue drop-down arrow and choosing **Ping**.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- New: Adds a new item to a list. To set up a new NTP server, click to open the NTP Server > New page.

NTP Server > New

Choose **CONTROLLER > NTP > Server** and click **New** to navigate to this page. This page enables you to add a new NTP server.

Table 4-25 New Network Time Protocol Server Configuration

Parameter	Description
Server Index (Priority)	NTP server index. The Cisco WLC tries Index 1 first, and then Index 2 through 3, in a descending order. Set this to 1 if your network is using only one NTP server.
Server IP Address (IPv4/IPv6)	IP address or a Fully Qualified Domain Name (FQDN) of the NTP server
Enable NTP Authentication	Select or uncheck the check box to enable or disable NTP authentication
Key Index	Key index of the NTP server. This parameter is available when you enable NTP authentication.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

NTP Server > Edit

Choose **CONTROLLER > NTP** and then click the server index number to navigate to this page. This page enables you to change the NTP server.

Table 4-26 Network Time Protocol Server Configuration Parameters

Parameter	Description
Server Address (IPv4/IPv6)	IP address or a Fully Qualified Domain Name (FQDN) of the NTP server
Enable NTP Authentication	Check box that you can select to enable or disable NTP authentication

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

NTP > NTP Keys

Choose **CONTROLLER > NTP > Keys** to navigate to this page. This page enables you to set the Network Time Protocol keys.

Table 4-27 NTP Key Parameters

Parameter	Description
Index	NTP server index
Key Index	NTP key index

Click a index number to go to the NTP Keys > Edit page to change the NTP key details.

Remove an NTP key entry by hovering your cursor over the blue drop-down arrow and choosing **Remove**. You are prompted for confirmation of the NTP key removal.

Buttons

New: Adds a new item to a list. To add a new NTP key, click to open the NTP Keys > New page.

NTP Keys > New

Choose **CONTROLLER > NTP > Keys** and then click **New** to navigate to this page. This page enables you to associate a new NTP key to a Server index.

Table 4-28 New Network Time Protocol Key Configuration

Parameter	Description
Key Index	NTP server index to which you want to associate the NTP key
Checksum	Checksum that is md5 by default
Key Format	Format of the key Choose either ASCII or HEX from the drop-down list.
Key	NTP key value

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

NTP Keys > Edit

Choose **CONTROLLER > NTP > Keys** and then click the index number to navigate to this page. This page enables you to change the NTP key.

Table 4-29 Network Time Protocol Key Configuration Parameters

Parameter	Description
Key Index	NTP server index to which you want to associate the NTP key.
Key Format	Format of the key. Choose either ASCII or HEX from the drop-down list.
Key	NTP key value.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

CDP

Controller Configuration

Choose **CONTROLLER > CDP > Controller Configuration** to navigate to this page. This page enables you to configure the Cisco Discovery Protocol (CDP).

Cisco Discovery Protocol Overview

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.

The default value for the frequency of periodic transmissions is 60 seconds, and the default advertised time-to-live value is 180 seconds. The second and latest version of the protocol, CDPv2, introduces new time-length-values (TLVs) and provides a reporting mechanism that allows for more rapid error tracking, reducing down time.

CDPv1 and CDPv2 are supported on the following devices:

- Cisco Flex 7500 and 5500 Series Controllers
- Lightweight access points
- An access point connected directly to a Cisco Flex 7500 and 5500 Series Controller

This support enables network management applications to discover Cisco devices.

The following TLVs are supported by both the controller and the access point:

- Device-ID TLV: 0x0001—The hostname of the controller, the access point, or the CDP neighbor.
- Address TLV: 0x0002—The IP address of the controller, the access point, or the CDP neighbor.
- Port-ID TLV: 0x0003—The name of the interface on which CDP packets are sent out.
- Capabilities TLV: 0x0004—The capabilities of the device. The controller sends out this TLV with a value of Host: 0x10, and the access point sends out this TLV with a value of Transparent Bridge: 0x02.
- Version TLV: 0x0005—The software version of the controller, the access point, or the CDP neighbor.
- Platform TLV: 0x0006—The hardware platform of the controller, the access point, or the CDP neighbor.
- Power Available TLV: 0x001a—The amount of power available to be transmitted by Power Sourcing Equipment to permit a device to negotiate and select an appropriate power setting.

The following TLVs are supported only by the access point:

- Full/Half Duplex TLV: 0x000b—The full- or half-duplex mode of the Ethernet link on which CDP packets are sent out. This TLV is not supported on access points that are connected directly to a Cisco 5500 Series Controller.
- Power Consumption TLV: 0x0010—The maximum amount of power consumed by the access point. This TLV is not supported on access points that are connected directly to a Cisco Flex 7500, 5500, Series Controllers.
- Power Request TLV:0x0019—The amount of power to be transmitted by a powerable device in order to negotiate a suitable power level with the supplier of the network power.

Note Changing the CDP configuration on the controller does not change the CDP configuration on the access points that are connected to the controller. You must enable and disable CDP separately for each access point.

Parameters and Descriptions

Table 4-30 CDP Global Configuration Parameters

Parameter	Description	Range	Default
CDP Protocol Status	Parameter that allows you to enable or disable CDP on the controller. **Note** You also need to enable CDP on the access point. **Note** Enabling or disabling this feature will be applicable to all the controller ports.	—	Enabled
CDP Advertisement Version	Highest CDP version supported on the controller.	Version 1 (v1) or version 2 (v2)	v1
Refresh-time Interval (seconds)	Interval at which CDP messages are to be generated.	5 to 254 seconds	60 seconds
Holdtime (seconds)	Amount of time to be advertised as the time-to-live value in generated CDP packets.	10 to 255 seconds	180 seconds

For information on displaying CDP neighbor information, see the following topics:

- CDP Neighbors Details
- CDP Neighbors
- CDP AP Neighbors
- CDP Traffic Metrics

Buttons

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

PMIPv6

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol. The controller uses the PMIPv6 protocol and works with the Mobile Access Gateway (MAG) and ASR5K, the partner Local Mobility Anchor (LMA), to provide seamless mobility of mobile clients. MAG tracks the mobile node and signals the mobile node's LMA.

Choose **CONTROLLER > PMIP** to navigate to this page. From here you can choose the following:

- **CONTROLLER > PMIP > General** to configure global parameters for PMIPv6.

See PMIPv6 > General for more information.

- **CONTROLLER > PMIP > LMA** to add new and view existing Local Mobility Anchor (LMA) to the controller.

  See PMIPv6 > LMA for more information.

- **CONTROLLER > PMIPv6 > Profile** to view existing PMIPv6 profiles.

  See PMIPv6 > Profile for more information.

PMIPv6 > General

Choose **CONTROLLER > PMIP > General** to configure global parameters for PMIPv6.

Note For timer parameters, default values appear in the UI when you reconfigure the domain name.

Table 4-31 General Parameters

Parameter	Description
Domain Name	Name of the PMIPv6 domain. The domain name can be up to 127 case-sensitive, alphanumeric characters.
MAG Name	Name of the MAG.
Interface	Interface of the controller used for PMIPv6.
MAG APN	Access Point Name (APN) if you subscribe to a MAG. MAG can be configured for one of the following roles: • 3gpp—Specifies the role as 3GPP (Third Generation Partnership Project standard) • lte—Specifies the role as Long Term Evolution (LTE) standard • wimax—Specifies the role as WiMax • wlan—Specifies the role as WLAN By default, the MAG role is WLAN. However, for lightweight access points, the MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.
Maximum Bindings Allowed	Maximum number of binding entries in the MAG. The range is from 0 to 40000. The default value is 10000.
Binding Lifetime	Lifetime of the binding entries in the controller. The binding lifetime should be a multiple of 4 seconds. The range is from 10 to 65535 seconds. The default value is 3600.
Binding Refresh Time	Refresh time of the binding entries in the MAG. The binding refresh time should be a multiple of 4 seconds. The range is from 4 to 65535 seconds. The default value is 300 seconds.
Binding Initial Retry Timeout	Initial timeout between the proxy binding updates (PBUs) when the MAG does not receive the proxy binding acknowledgements (PBAs). The range is from 100 to 65535 seconds. The default value is 1000 seconds.

Table 4-31 General Parameters

Parameter	Description
Binding Maximum Retry Timeout	Maximum timeout between the proxy binding updates (PBUs) when the MAG does not receive the proxy binding acknowledgments (PBAs). The range is from 100 to 65535 seconds. The default value is 32000 seconds.
Replay Protection Timestamp	Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The range is from 1 to 255 milliseconds. The default value is 7 milliseconds.
Minimum BRI Retransmit Timeout	Minimum amount of time that the MAG waits before retransmitting the BRI message. The range is from 500 to 65535 seconds. The default value is 1000 seconds.
Maximum BRI Retransmit Timeout	Maximum amount of time that the MAG waits before retransmitting the Binding Revocation Indication (BRI) message. The range is from 500 to 65535 seconds. The default value is 2000 seconds.
BRI Retries	Maximum number of times that the MAG retransmits the BRI message before receiving the Binding Revocation Acknowledgment (BRA) message. The range is from 1 to 10. The default value is 1.

PMIPv6 > LMA

Choose **CONTROLLER > PMIP > LMA** to add new and view existing Local Mobility Anchor (LMA) to the controller.

Click **New** to add a new LMA to the controller.

Table 4-32 LMA Parameters

Parameter	Description
Member Name	Name of the LMA connected to the controller. The LMA name can be up to 127 case-sensitive, alphanumeric characters.
Member IP Address	IP address of the LMA connected to the controller.

Buttons

Apply: Adds a new LMA member.

PMIPv6 > Profile

Choose **CONTROLLER > PMIPv6 > Profile** to navigate to this page. This page lists existing PMIPv6 profiles.

Buttons

- New**:** Adds a new PMIPv6 profile.

Click a PMIPv6 profile to edit the configurations of the PMIPv6 profile.

PMIPv6 Profile > New

Choose **CONTROLLER > PMIPv6 > Profile** and then click **New** to navigate to this page. This page allows you to create a new PMIPv6 profile.

Table 4-33 Profile Parameters

Parameter	Description
Profile Name	Name of the PMIPv6 profile.
Network Access Identifier	Name of the Network Access Identifier (NAI) associated with the profile. The NAI can be up to 127 case-sensitive alphanumeric characters.
LMA Name	Name of the LMA to which the profile is associated. The LMA name can be up to 127 alphanumeric, case-sensitive characters.
Access point node	Name of the access point node connected to the controller.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

PMIPv6 Profile > Edit

Choose **CONTROLLER > PMIP > Profile** and then click on any profile to navigate to this page. This page allows you to add more NAIs and remove any of the existing NAIs.

Button

- Add NAI: Allows you to add more NAIs.

Tunneling

EoGRE

Choose **CONTROLLER > Tunneling > EoGRE** to navigate to this page.

Table 4-34 EoGRE Parameters

Parameter	Description
Interface Name	Name of the interface that is used as the tunnel interface
Heartbeat Interval (Seconds)	The heartbeat is used by Cisco WLC and Cisco AP to check the status of the tunnel gateway depending on the mode. • If the AP is in Local mode and WLAN is centrally switched, the heartbeat is from Cisco WLC. • If the AP is in FlexConnect mode and the WLAN is locally switched, the AP checks the tunnel gateway connectivity.
Max Heartbeat Skip Count	Number of consecutive keepalive retries before a member status is marked 'Down'.
Add New TGW	
TGW Name	Name of the tunnel gateway.
TGW IP Address	IPv4 or IPv6 address of the tunnel gateway.
TGW List	Shows details of the tunnel gateways added. The details include name of the TGW, IPv4 or IPv6 address of the TGW, status of TGW (Up or Down), and the total number of clients associated. Click **Get Statistics** to view tunnel gateway statistics.
Add New Domain	
Domain Name	Name of the domain
TGW-1	Specify the name of TGW and the role as either primary/active or secondary/standby TGW. **Note** In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active or primary gateway. Clients will have to associate again with the secondary gateway. During and after failover, Cisco WLC continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6. This feature is supported on all Wave 1 and Wave 2 APs that are supported in this release.
TGW-2	Specify the name of TGW and the role as either primary/active or secondary/standby TGW.
Domain List	Shows details of the domains added. The details include domain name, the two TGWs associated with the domain, the name of the active TGW, and its role as either the primary or secondary gateway.

Profiles

Choose **CONTROLLER > Tunneling > Profiles** to navigate to this page.

Table 4-35 Profile Parameters

Parameter	Description
Add New	
Profile Name	The heartbeat is used in the failover mechanism for the AP to detect if the Active TGW went down

IPv6

Neighbor Binding Timers

Choose **CONTROLLER > IPv6 > Neighbor Binding Timers** to navigate to this page. This page enables you to configure the Neighbor Binding timers.

Parameters and Descriptions

Table 4-36 Neighbor Binding Timer Parameters

Parameter	Description	Range	Default
Down Lifetime	Maximum time, in seconds, that an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.	0–86400 seconds	300 seconds
Reachable Lifetime	Maximum time, in seconds, that an entry is considered reachable without getting a proof of reachability (direct reachability through tracking or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale.	0–86400 seconds	300 seconds
Stale Lifetime	Maximum time, in seconds, that a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.	0–86400 seconds	86400 seconds
Unknown Address Multicast NS Forwarding	The controller forwards the IPv6 packets without validating the multicast Neighbor Solicitation (NS) frame.	—	—

Buttons

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

RA Throttle Policy

Choose **CONTROLLER > IPv6 > RA Throttle Policy** to navigate to this page. This page enables you to configure the RA Throttle Policy.

The purpose of the RA Throttle Policy is to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network.

Parameters and Descriptions

Table 4-37 RA Throttle Policy Parameters

Parameter	Description	Range	Default
Enable RA Throttle Policy	IPv6 RA throttling.	–	Disabled
Throttle Period	Duration of throttle period in seconds.	10–86400 seconds	600 seconds
Max Through	Number of RAs that will pass through over a period.	0–256	10
Interval Option	Behavior RAs that have an interval option.	Ignore, Passthrough, or Throttle	Passthrough
Allow At-least	Minimum number of RAs that will not be throttled per router.	0–32	1
Allow At-most	Maximum number of RAs that will not be throttled per router.	0–256	1
No Limit	No limit to be placed on the maximum number of RAs that will not be throttled per router.	–	Disabled

Buttons

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

RA Guard

Choose **CONTROLLER > IPv6 > RA Guard** to navigate to this page. This page enables you to configure router advertisement (RA) filtering.

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

mDNS

Multicast DNS (mDNS) Service Discovery provides a way to announce and discover devices like printers, computers, and services on the local network. mDNS performs DNS queries over IP multicast. mDNS supports zero configuration IP networking. mDNS uses the multicast IP address 224.0.0.251 as the destination address and 5353 as the UDP destination port.

Choose **CONTROLLER > mDNS > General** to navigate to this page. From here, you can choose the following:

- **CONTROLLER > mDNS** to configure the global mDNS parameters.

  See mDNS > General for more information.
- **CONTROLLER > mDNS > Profiles** to view the mDNS profiles configured on the controller and create new mDNS profiles.

  See mDNS > Profiles for more information.
- **CONTROLLER > mDNS > Domain Names** to view the domain names and other details of the service providers.

  See mDNS > Domain Names for more information.
- **CONTROLLER > mDNS > mDNS Browser t**o view the domain names and other details of the service providers.

  See mDNS Browser for more information.
- **CONTROLLER > mDNS > mDNS Policies** to view the total number of mDNS Service groups.

  See mDNS Service Groups for more information.

mDNS > General

Choose **CONTROLLER > mDNS > General** to navigate to this page. This page enables you to configure the global mDNS parameters and update the Master Services database.

,

Table 4-38 Profile Parameters

Parameter	Description
Global Configuration	
mDNS Global Snooping	Check box that you can check to enable snooping of mDNS packets. **Note** The controller does not support IPv6 mDNS packets even when you enable mDNS snooping.
mDNS Policy	Check box that you can check to enable mDNS policy. **Note** If global mDNS access policy is enabled, LSS will be ignored.
Query Interval	mDNS query interval, in minutes, that you can set. The query interval is the frequency at which the Cisco WLC sends periodic queries to all the services defined in the Master Service database. The range is from 10 to 120 minutes. The default value is 15 minutes.
Master Services Database	

Table 4-38 Profile Parameters

Parameter	Description
Service	Drop-down list from which you can choose the supported services that can be queried. The following services are available: • Air Tunes • Apple File Sharing Protocol (AFP) • Scanner • FTP • NFS • iTunes Music Sharing • iTunes Home Sharing • iTunes Wireless Device Syncing • Apple Remote Desktop • Apple CD/DVD Sharing • Time Capsule Backup Click **Add** after you choose a service. To add a new mDNS-supported service, choose **Other**. Specify the service name and service string. The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database.The controller can snoop and learn a maximum of 64 services.
Service Name	Name of the mDNS service.
Service String	Unique string associated to an mDNS service. For example," _airplay._tcp.local." is the service string associated to Apple TV.
Query Status	Check box that you can check to enable an mDNS query for a service.
LSS Status	Check box that you can check to enable LSS status.
Origin	Specify the origin of the service from the following options: • All • Wireless • Wired

To view the details of an mDNS service, hover your cursor over the blue drop-down arrow of a service, and choose **Details**. The mDNS > Service > Detail page appears, for more information, see mDNS > Service > Detail.

mDNS > Service > Detail

Choose **CONTROLLER > mDNS > General**, hover your cursor over the blue drop-down arrow for a service, and choose **Details** to navigate to this page. This page enables you to view the details of each service.

Table 4-39 Service Detail Parameters

Parameter	Description
Service Name	Name of the mDNS service.
Service String	Unique string associated to an mDNS service. For example," _airplay._tcp.local." is the service string associated to Apple TV.
Service ID	Unique service ID associated to an mDNS service.
Service Query Status	Status of the service query that indicates if the service can be queried by the Cisco WLC. The Cisco WLC queries the service only if the query status is enabled for the service.
Profile Count	Number of profiles associated with the service. You can associate multiple services to a profile and map the profile to a WLAN, interface, or an interface group.
Service Provider Count	Number of service providers or hosts that provide the service.
Profile Information	
Profile Name	Names of the profiles associated with the service.
Service Provider Information	
MAC Address	MAC address of the service provider.
Service Provider Name	Name of the service provider. Beginning in Release 8.0 and later releases, the maximum number of service providers for different controller models are as follows: • Cisco 5500 and 2500 Series Controllers—6400 • Cisco Wireless Services Module 2—6400 • Cisco 8500 and 7500 Series Controllers—16000
VLAN ID	VLAN ID of the service provider.
Type	Type of service provider that is one of the following: • Wired— Service provider is on the infrastructure side. • Wireless— Service provider is a wireless client. • Wired guest— Service provider is on a guest LAN.
TTL	Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the controller when the TTL expires.
Time Left	Time left in seconds before the service provider is removed from the controller.

mDNS > Profiles

Choose **CONTROLLER > mDNS > Profiles** to view the mDNS profiles configured on the controller and create new mDNS profiles.

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

For more information, see the following topics:

- Mapping mDNS Profiles to an Interface Group
- Mapping mDNS Profiles to an Interface
- Mapping mDNS Profiles to a WLAN

Table 4-40 mDNS Profile Parameters

Parameter	Description
Number of profiles	Number of mDNS profiles configured on the controller.
Profile Name	Name of the mDNS profile. You can create a maximum of 16 profiles.
Number of Services	Number of services in an mDNS profile.

Buttons

New: Creates a new mDNS profile.

Mapping mDNS Profiles to an Interface Group

To map a profile to an interface group, follow these steps:

Step 1 Choose **CONTROLLER > Interface Groups** and click the Interface Group name to navigate to the Interface Groups > Edit page.

Step 2 Choose an mDNS profile from the drop-down list.

Mapping mDNS Profiles to an Interface

To map a profile to an interface, follow these steps:

Step 1 Choose **CONTROLLER > Interfaces** and then click on an interface name to navigate to the Interfaces > Edit page.

Step 2 Choose an mDNS profile from the drop-down list.

Mapping mDNS Profiles to a WLAN

To map a profile to a WLAN, follow these steps:

Step 1 Choose **WLANs** and click the Profile name to navigate to the WLANs > Edit page.

Step 2 Select the mDNS check box.

Step 3 Choose an mDNS profile from the drop-down list.

mDNS Profile > Edit

Choose **CONTROLLER > mDNS > Profiles** and click the profile name to navigate to the **mDNS Profile > Edit** page. You can view the following details of the profile:

- Profile Name
- Profile ID
- Service Count
- Number of interfaces attached
- Number of interface groups attached
- Interface groups
- Number of WLANs attached
- WLAN IDs
- Number of Guest LANs attached
- Guest LAN IDs
- Number of Local Policies attached
- Local Policy IDs

To add more services to the profile, choose a service from the **Service Name** drop-down list and click **Add**. You can choose from a list of services that are configured in the Master service database. To update the Master service database, choose **CONTROLLER > mDNS > General**.

mDNS > Domain Names

Choose **CONTROLLER > mDNS > Domain Names** to view the domain names and other details of the service providers.

Each service advertisement contains a record that maps the domain name of the service provider to the IP address. The mapping also contains details such as the client MAC address, the VLAN ID, the TTL, and the IPv4 address.

Table 4-41 Domain Names Parameters

Parameter	Description
Number of Domain Name-IP Entries	Count of the domain name IP address mappings.
Domain Name	Hostname assigned to each service provider machine.
MAC Address	MAC address of the service provider machine.
IP Address	IP address of the service provider.
VLAN ID	VLAN ID of the service provider.

Table 4-41 Domain Names Parameters

Parameter	Description
Type	Origin of service that can be one of the following: • Wired • Wireless • Wired guest
TTL	Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the controller when the TTL expires.
Time Left	Time left in seconds before the service provider is removed from the controller.

mDNS Browser

Choose **CONTROLLER > mDNS > mDNS Browser** to view the total number of services added in the master database.

Table 4-42 mDNS Browser Parameters

Parameter	Description
Number of Services	Total number of services added in the Master database.
Origin	From where mDNS service instances are snooped (source). Can be WIRED/WIRELESS/mDNS-AP/WIRED GUEST.
VLAN	Snooped Service instance VLAN.
TTL (seconds)	Service instance advertised that service will be available for TTL seconds (time to live).
TTL Left (seconds)	Service instance available run time.
Client MAC	MAC address of service instance.
AP MAC	Service instance joined AP Base MAC.
Service String	Unique string associated to an mDNS service, for example, _airplay._tcp.local. is the service string associated with Apple TV.

mDNS Service Groups

Choose **CONTROLLER > mDNS > mDNS Policies** to view total number of mDNS Service groups.

Table 4-43 mDNS Service Groups Parameters

Parameter	Description
Number of mDNS Policies	Total number of mDNS Service groups. This includes admin created / ISE dynamic policy / SNMP.
Number of Admin Created Policies	Total number of mDNS service groups created by WLC admin.
mDNS Service Group Name	Service group name.
Description	Service group description.
Origin	Service group origin that is created by WLC admin/ISE/SNMP.

Creating mDNS Service Group

Step 1 Choose **CONTROLLER > mDNS > mDNS Policies** and click the **Add Group** button.

Step 2 Enter a service group name in the **mDNS Service Group Name** box.

Step 3 Add a description for the service group in the **Description** box.

Step 4 Click **Add** to create a new mDNS Service Group.

mDNS Service Group > Edit

Choose **CONTROLLER > mDNS > Policies** and click the mDNS Service Group Name to navigate to the **mDNS Service Groups > Edit** page. You can add a MAC Address and a rule to the Service Group.

Table 4-44 mDNS Service Group > Edit Parameters

Parameters	Description
mDNS Service Group Name	Displays the name of the mDNS Service Group selected for editing.
Service Instance List	
MAC Address	MAC address of the service provider
Name	Name of the service provider
Location Type	Choose from the following options: • AP Group • AP Name • AP Location

Table 4-44 mDNS Service Group > Edit Parameters

Parameters	Description
Location	Location to be specified. If the Location is specified as Any, the policy checks on the Location attribute are not performed. **Note** In the case of mDNS policy filtered by AP groups, the design is for substring match. The policy is applied on the first substring match.
Policy/Rule	
Role Names	User type or user group of the user, for example, student, employee.
User Names	Name of the user.

Advanced

This section contains the following topics:

- DHCP, page 4-53
- Master Controller Mode, page 4-55

DHCP

Choose **CONTROLLER > Advanced > DHCP** to navigate to this page. This page enables you to set the following DHCP parameters:

Table 4-45 DHCP Parameters

Parameter	Description
Enable DHCP Proxy	Drop-down list from which you can choose to enable or disable DHCP proxy on a global basis, rather than on a WLAN basis. DHCP proxy is enabled by default. When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself. **Note** IPv6 is not supported for DHCP.
DHCP Option 82 Remote Id field format	Provides additional security when DHCP is used to allocate network addresses. Specifically, it enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. The controller can be configured to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server. **Note** For DHCP option 82 to work as expected, you must enable DHCP proxy. **Note** DHCP option 82 is not supported for use with auto-anchor mobility. See Mobility Anchors for information about anchor mobility. • AP-MAC—Adds the MAC address of the access point to the DHCP option 82 payload. This is the default value. • AP-MAC-SSID—Adds the MAC address and SSID of the access point to the DHCP option 82 payload. • AP-ETHMAC—Adds the Ethernet MAC address of the access point to the DHCP option 82 payload. • AP-NAME-SSID—Adds the name and SSID of the access point to the DHCP option 82 payload. • AP-GROUP-NAME—Adds the AP group name of the access point to the DHCP option 82 payload. • FLEX-GROUP-NAME—Adds the FlexConnect group name of the access point to the DHCP option 82 payload. • AP-LOCATION—Adds the location of the access point to the DHCP option 82 payload. • AP-MAC-VLAN-ID—Adds the MAC address and VLAN ID of the access point to the DHCP option 82 payload. • AP-NAME-VLAN-ID—Adds the name and VLAN ID of the access point to the DHCP option 82 payload. • AP-ETHMAC-SSID—Adds the MAC address and SSID of the access point to the DHCP option 82 payload.
DHCP Timeout	Sets the DHCP timeout in seconds. This value is applicable globally. The valid range is 5 to 120 seconds.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Master Controller Mode

Choose **CONTROLLER > Advanced > Master Controller Mode** to navigate to this page.

This page enables the Cisco WLC to be configured as the master Cisco WLC for your access points that are connected in appliance mode. When there is a master Cisco WLC enabled, all newly added access points with no primary, secondary, or tertiary controllers assigned associate with the master Cisco WLC on the same subnet. This feature enables you to verify the access point configuration and assign primary, secondary, and tertiary controllers to the access point using the All AP Details page.

Note The master Cisco WLC is normally used only while adding new access points to the Cisco Wireless LAN Solution (Cisco WLAN Solution). When no more access points are being added to the network, you should disable the master Cisco WLC.

Note Because the master Cisco WLC is normally not used in a deployed network, the master Cisco WLC setting is disabled upon reboot or OS code upgrade.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Wireless Tab

The Wireless tab on the menu bar provides access to the Cisco WLAN Solution wireless network configuration. Use the left navigation pane to access specific wireless network parameters.

All APs

Choose **WIRELESS > Access Points > All APs** or **MONITOR > Summary** and click **All APs** under the AP Summary section to navigate to the All APs page.

This page displays the access points associated with the Cisco WLC. This section consists of the following topics:

- All APs Details
- VLAN Mappings for FlexConnect Access Points
- WebAuth and WebPolicy ACL Mappings for FlexConnect Access Points
- VLAN Mappings for Mesh Access Points
- Neighbor Information of Access Points
- Access Points Statistics

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

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

- MAC Address—MAC address.

Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- AP Name—Access point name. If you do not know the exact name of the AP, you can specify the name partially by entering one or more successive characters that are part of the AP name.
- AP Model—Access point model check box where you select and enter the model of the access point.
- Operating Status—Operating status of the access points:
  - UP—The access point is up and running.
  - DOWN—The access point is not operational.

  - REG—The access point is registered to the controller.
  - DEREG—The access point is not registered to the controller.
  - DOWNLOAD—The controller is downloading its software image to the access point.
- Admin Status—Whether the access points are enabled or disabled on the controller.
- AP Mode—Options to specify the operating mode of the access points: Local, FlexConnect, REAP, Monitor, Rogue Detector, Sniffer, Bridge, and SE Connect. Depending on the capabilities and support available for the APs, one or more options are displayed.

Note To configure an access point for wIPS, you must set the AP mode to one of the following from the AP Mode drop-down list: Local, FlexConnect, and Monitor.

- Certificate Type—Check boxes that you can select to specify the types of certificates installed on the access points:
  - MIC—Manufactured-installed certificate
  - SSC—Self-signed certificate
  - LSC—Local significant certificate
- Primary S/W Version—Primary software version.
- Secondary S/W Version—Secondary software version.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the All APs page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0, AP Name:pmsk-ap, Operational Status:UP, Status: Enabled, and so on).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

All APs Summary

This table describes the AP parameters.

Table 5-1 All APs Summary Parameters

Parameter	Description
AP Name	Operator-defined name of the access point.
IP Address (IPv4/IPv6)	The IPv4/IPv6 address of the AP. From Release 8.0, Cisco WLC supports IPv6.
AP Model	Access point model name.
AP MAC	MAC address of the access point.
AP Up Time	Amount of time that the access point has been powered up.
Admin Status	Administration state of the access point.
Operational Status	Operational status of the access point that is either registered (REG) or not registered (DEREG).

Table 5-1 All APs Summary Parameters

Parameter	Description
PoE Status	The power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). The controller auto-detects the access point's power source and displays the power level.
No: Of Clients	The maximum number of clients to be allowed per AP.
Port	Access point port number.
AP Mode	Access point mode of operation: • Local • FlexConnect • Monitor • Rogue Detector • Sniffer • Bridge • SE Connect **Note** Depending on the capabilities and support available for the APs, one or more of the above options are displayed.
Certificate Type	Type of certificate: • MIC (manufactured-installed certificate) • SSC (self-signed certificate) • LSC (local significant certificate)
OEAP (OfficeExtend AP)	Whether this access point is an OfficeExtend access point.
Primary SW Version	Primary image software version available in the access point.
Backup SW Version	Backup image software version available in the access point.
AP Sub Mode	• AP Sub Mode field that shows wIPS if the access point in is monitor mode and the wIPS submode is configured on the access point. • None is displayed if the access point is in local/FlexConnect mode and wIPS submode is not configured.
Download Status	Download status of the upgrade image on this access point.
Upgrade Role (Master/Slave)	Role of the access point in the upgrade process. Valid values are **Master** and **Slave**.
mDNS Status	Status of mDNS.
Universal AP	Shows whether the AP is an universal AP or not. **Note** Cisco Aironet Universal Access Points address the worldwide regulatory compliance requirements for APs, by dynamically setting their regulatory domain and country configurations based on their geographical location. A universal access point, hence, allows the user to reconfigure its regulatory domain whenever required by the user.
Hyperlocation	Status of Cisco Hyperlocation on the AP.

For details on a particular access point, click the access point name to open the All APs Details page for that access point.

To view statistics for an access point in Bridge AP mode, click the blue arrow adjacent the desired access point and choose **Statistics**. The Access Points Statistics page for the selected access point appears.

To view neighbor statistics for an access point in Bridge AP mode, click the blue arrow adjacent the desired access point and choose **Neighbor Information**. The Neighbor Information of Access Points page for the selected access point appears.

All APs Details

Choose **WIRELESS > Access Points > All APs** and then click an AP name to navigate to the AP Details page.

This page shows the details of the selected access point including the hardware, operating system software, and boot version details.

General Tab

The following parameters are not displayed for ODM access point under General parameters:

- AP Mode
- AP Sub Mode

This table describes the general AP parameters.

Table 5-2 General Tab Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Location	User-definable location name for the access point. You can enter up to 254 characters.
AP MAC Address	MAC address of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
Admin Status	Administration state of the access point.

Table 5-2 General Tab Parameters

Parameter	Description
AP Mode	Access point mode of operation. The options are as follows: **Note** The Cisco OEAP 600 Series access point uses local mode and these settings cannot be altered. Monitor mode, Sniffer mode, Rogue detector mode, Bridge mode, and SE- Connect modes are not supported on the 600 OEAP series. • Local—Default option. • FlexConnect—AP mode that is used for APs that support FlexConnect mode. • Monitor—Monitor-only mode. • Rogue Detector—AP mode that monitors the rogue APs; the mode does not transmit or contain rogue APs. • Sniffer—AP mode that starts sniffing the wireless network on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). It will include information on timestamps, signal strength, packet size and so on. See the Sniffer Feature topic for more details. • Bridge—AP mode that is a bridge if you are connecting a root AP. **Note** This option is displayed only if the AP is bridge capable. **Note** If the AP mode is set to “Bridge” and the AP is not REAP capable, an error is displayed. • SE-Connect—AP mode that is SE-Connect if you want the access point to perform spectrum intelligence. This field does not appear for Cisco Aironet 1520 and 1550 Series access points. **Note** Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir. **Note** When an access point is configured in SE-Connect mode, the access point reboots and rejoins the controller. Access points configured in this mode will not serve clients. **Note** To configure an access point for wIPS, you must set the AP mode to one of the following from the AP Mode drop-down list: Local, FlexConnect, or Monitor.
AP Sub Mode	Access Point submode. The available options are as follows: • WIPS—The AP is in local, FlexConnect, or monitor mode and the wIPS submode is configured on the access point. • None—The AP is in local/FlexConnect mode and WIPS submode is not configured on the AP.
Operational Status	Operational status of the access point that comes up as either registered (REG) or not registered (DEREG) automatically by the Cisco WLC.
Port Number	Access point that is connected to this Cisco WLC port.

Table 5-2 General Tab Parameters

Parameter	Description
Network Spectrum Interface Key	32-digit Network Spectrum Interface (NSI) key. The NSI key is required to configure spectrum expert mode. **Note** This parameter is shown only for CleanAir capable access points for only Local, FlexConnect, and SE-Connected mode.
Venue Group	Drop-down list from which you can choose a Hotspot group that groups similar Hotspot venues. The following options are available: • Unspecified • Assembly • Business • Educational • Factory and Industrial • Institutional • Mercantile • Residential • Storage • Utility and Misc • Vehicular • Outdoor
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. 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.
Network Spectrum Interface (NSI) Key	When an access point in SE-Connect mode joins a controller, it sends a Spectrum Capabilities notification message, and the controller responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the controller for use in NSI authentication. The controller generates one key per access point, which the access point stores until it is rebooted.
The following parameters are applicable to Cisco 1570 Series Access Points	
Internal Temperature	The Internal Temperature of the AP is displayed in both Celsius and Fahrenheit.

Table 5-2 General Tab Parameters

Parameter	Description
Temperature State	The Temperature State is shown to be in one of three states: GREEN, YELLOW, or RED. The GREEN state indicates that the AP is functioning normally and the internal temperature is at an optimal operating temperature; the YELLOW state indicates that the AP state is in transition to either GREEN or RED state; if the AP is in RED state, it means that the internal temperature of the AP has increased and the number of antennas that are used for transmission will be reduced.
Heater Status	Not applicable to 1570 APs.
PoE Out State	The PoE Out State shows the status of the Power over Ethernet output port from the AP. The PoE Out State can be in OFF or ON state depending on the input power source for the AP.

This table describes the GPS Location parameters. GPS parameters do not appear if the access point does not have a GPS module or the GPS information is invalid.

Table 5-3 GPS Location Parameters

Parameter	Description
GPS Present	GPS module that is installed on the access point or not.
Latitude	Latitude information of the access point in the GPS data received.
Longitude	Longitude information of the access point in the GPS data received.
Altitude	Altitude information of the access point in the GPS data received.
GPS Location Age	Time when the GPS data was collected.

This table describes the Cable Modem statistics. The Cable Modem statistics are updated every 5 minutes after the AP is associated with the WLC. The Cable Modem statistics are applicable for Cisco 1572C (internal or external antenna cable modem) access points in local or bridge/Flex-bridge modes.

Table 5-4 Cable Modem Statistics

Parameter	Description
Cable Modem Statistics	Information about the following is shown: • AP Name • AP MAC Address • CM MAC Address • CM Software Version • Ethernet Speed • Ethernet Status • Docsis Registration Status • CM Serial Number • CM Mask
US Channel Status	Information about the following is shown: • Channel ID • Power Level • Center Frequency • Carrier to Noise Ratio
DS Channel Status	Information about the following is shown: • Channel ID • Power Level • Center Frequency

Table 5-5 Version Parameters

Parameter	Description
Primary Software Version	Primary software version.
Backup Software Version	Version of the backup software on this access point.
Predownload Status	Predownload status on this access point.
Predownloaded Version	Version of the software that is being predownloaded.
Predownload Next Retry time	Time duration after which this access point will try to perform a predownload operation.
Predownload Retry Count	Number of times this access point has tried to perform the predownload operation.
Boot Version	Boot ROM versions.
IOS Version	Cisco IOS software version.
Mini IOS Version	Mini-IOS software version.

Table 5-5 Version Parameters

Parameter	Description
GPS Location	GPS parameters do not appear if the access point does not have a GPS module or the GPS information is invalid.
GPS Present	GPS module that is installed on the access point or not.
Latitude	Latitude information of the access point in the GPS data received.
Longitude	Longitude information of the access point in the GPS data received.
Altitude	Altitude information of the access point in the GPS data received.
GPS Location Age	Time when the GPS data was collected.

Table 5-6 IP Config Parameters

Parameter	Description
CAPWAP Preferred Mode	Displays the current CAPWAP Preferred mode of the AP. It can be: • IP Config (Global)— Configured at Controller > General. • IP Config (AP Group Config)—Configured at WLAN > Advanced > AP Groups > General Tab.
DHCPv6 Address	Displays the DHCP IPv6 address.

Table 5-6 IP Config Parameters

Parameter	Description
Static IP (IPv4/IPv6)	Check box to enable configuration of the AP using static IP address. From Release 8.0, IPv4 and IPv6 are supported.
Static IP (IPv4/IPv6)	Static IP address of the access point. When an access point boots up, it tries to determine if its static IP address is configured or not. If the access point has been configured with a static IP address that is not valid on the network, the access point cannot join the controller and cannot communicate with the rest of the network. In such a scenario, the only way to recover that access point is to manually open the access point door and connect a serial console for configuration purpose. The access point can be configured in such a way that, even if its static IP address is not valid on the network, it initiates a DHCP process to get a new IP address and use it for communication. This configuration enables the access point to join the controllers on the network. **Note** An access point cannot discover the controller using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. Options for this parameter are as follows: • Unselected—When this check box is not selected, the static IP address is disabled and the access point initiates a DHCP process when it boots up to procure the IP address. • Checked—When this check box is selected, you can set the following: – The static IPv4/IPv6 address of the access point. – The subnet mask/ prefix length assigned to the access point IPv4/IPv6 address. – The IPv4/IPv6 gateway of the access point. Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IP address that you specified in is sent to the access point. You can now configure the DNS server IP address and domain name. To do so, follow these steps: – In the DNS IP Address text box, enter the IPv4/IPv6address of the DNS server. – In the Domain Name text box, enter the name of the domain to which the access point belongs. Click **Apply** to commit your changes.

Table 5-7 Time Statistics Parameters

Parameter	Description
UP Time	Amount of time that the access point has been powered up.
Controller Associated Time	Amount of time that the access point has been associated with the controller.
Controller Associated Latency	Amount of time that the access point took to associate with the controller.

- Click **Reset AP Now** to reset the access point.
- Click **Clear All Config** to reset the access point parameters to the factory defaults.
- Click **Clear Config Except Static IP** to reset the access point parameters to the factory defaults but retains the static IP address information.

Credentials Tab

Note The Credentials Tab is not displayed for ODM access points.

Table 5-8 Credentials Tab Parameters

Parameter	Description
Over-ride Global credentials	Access point that is prevented from inheriting the global username, password, and enable password from the controller. The default value is unselected.
Username	Unique username for this access point.
Password	Unique password for this access point.
Enable Password	Unique enable password for this access point.

Table 5-9 802.11X Supplicant Credentials Parameters

Parameter	Description
Over-ride Global credentials	Access point that is prevented from inheriting the global authentication username and password from the controller. The default value is unselected.
Username	Unique username for this access point.
Password	Unique password for this access point. **Note** You must enter a strong password. Strong passwords have the following characteristics: • They are at least eight characters long. • They contain a combination of uppercase and lowercase letters, numbers, and symbols. • They are not words in any language.
Confirm Password	Unique password that you can reenter for this access point.

Interfaces Tab

Note To enable or disable CDP either on an Ethernet or radio interface, you should enable the global CDP for that particular access point. See Global Configuration for more information.

Note CDP over radio interface is applicable only for mesh APs.

Note The CDP state and CDP configuration are not displayed for the Cisco OEAP 600 Series access point under the Ethernet Interfaces parameters.

Table 5-10 Ethernet Interface Parameters

Parameter	Description
CDP Configuration	
Ethernet Interface#	Ethernet interface number.
CDP State	Current configured state of CDP on all or a specific Ethernet interface. The status could be enabled or disabled. **Note** You can enable or disable CDP on all or a specific Ethernet interface by choosing **WIRELESS > Access points > Global Configuration** and select **CDP State** check box over a particular Ethernet interface.
Interface	CDP interface name.
Operational Status	Status of the interface.
Tx Unicast Packets	Number of unicast packets transmitted.
Rx Unicast Packets	Number of unicast packets received.
Tx Non-Unicast Packets	Number of nonunicast packets transmitted.
Rx Non-Unicast Packets	Number of nonunicast packets received.

Table 5-11 Interface Properties Parameters

Parameter Name	Description
AP Name	Name of the access point.
Link speed	Speed of the interface in Mbps.
RX Bytes	Total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Total number of unicast packets received on the interface.

Table 5-11 Interface Properties Parameters

Parameter Name	Description
RX Non-Unicast Packets	Total number of nonunicast or multicast packets received on the interface.
Input CRC	Total number of CRC error in packets received on the interface.
Input Errors	Sum of all errors in the packets while receiving on the interface.
Input Overrun	Number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver's capability to handle the data.
Input Resource	Total number of resource errors in packets received on the interface.
Runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
Throttle	Total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Total number of packets retransmitted due to an Ethernet collision.
Output Resource	Resource errors in packets transmitted on the interface.
Output Errors	Errors that prevented the final transmission of packets out of the interface.
Operational Status	Operational state of the physical Ethernet interface on the AP.
Duplex	Interface's duplex mode.
TX Bytes	Number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Total number of nonunicast or multicast packets transmitted on the interface.
Input Aborts	Total number of packets aborted while receiving on the interface.
Input Frames	Total number of packets received incorrectly that had a CRC error and a noninteger number of octets on the interface.
Input Drops	Total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Total number of packets discarded on the interface due to an unknown protocol.

Table 5-11 Interface Properties Parameters

Parameter Name	Description
Giants	Number of packets that are discarded because they exceeded the medium's maximum packet size.
Interface Resets	Number of times that an interface has been completely reset.
Output No Buffer	Total number of packets discarded because there was no buffer space.
Output Underrun	Number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Total number of packets dropped while transmitting from the interface because the queue was full.

Table 5-12 Radio Interface Parameters

Parameter	Description
Number of Radio interfaces	Number of radio interfaces.
CDP Configuration	
Radio Slot#	Slot where the radio is installed.
CDP State	Current configured state of CDP on the radio slot. The status could be enabled or disabled. **Note** You can enable or disable CDP on all or a specific access point by choosing **WIRELESS > Access points > Global Configuration** and selecting the **CDP State** check box over a particular radio interface.
Radio Interface Type	Cisco Radio type. The value is either 802.11a/n/ac, 802.11b/g/n, or 802.11a/b/g/n/ac. 802.11a/b/g/n/ac appears if you have the monitor module for 3600 access points.
Module Type	Access Point module type.
Sub Band	Radio sub band, if it is active. The value is either 4.9 GHz or 5.8 GHz.
Admin Status	Cisco Radio interface status.
Oper Status	Cisco Radio operational status.
CleanAir Admin Status	CleanAir administration status.
CleanAir Oper Status	CleanAir operational status.
Regulatory Domain	Regulatory domain that is supported or unsupported.

High Availability Tab

The high availability feature is used to help an AP move over to a controller when the current controller fails. The backup and secondary are the fourth and fifth in the order of controllers if primary, secondary, and tertiary controllers are configured under the AP. If the primary, secondary, and tertiary controllers are not configured, then the AP will use the backup primary if the current controller fails.

Note If the AP supports IPv6 then it can discover a WLC over IPv6 CAPWAP tunnel.

Table 5-13 High Availability Parameters

Parameter	Description
Primary Controller	Name and management IP address of the primary controller.
Secondary Controller	Name and management IP address of the secondary controller.
Tertiary Controller	Name and management IP address of the tertiary controller.
AP Failover Priority	Priority for the access point: • Low—Assigns the access point to the level 1 priority, which is the lowest priority level. This is the default value. • Medium—Assigns the access point to the level 2 priority. • High—Assigns the access point to the level 3 priority. • Critical—Assigns the access point to the level 4 priority, which is the highest priority level.

Inventory Tab

Table 5-14 Inventory Tab Parameters

Parameter	Description
Product ID	Model of the access point.
Version ID	Version of the access point.
Serial Number	Serial number of the access point; for example, FTX0916T134.
Entity Name	Entity name of the access point.
Entity Description	Entity description of the access point.

Table 5-14 Inventory Tab Parameters

Parameter	Description
Certificate Type	Certificate type as either Self Signed or Manufacture Installed.
FlexConnect Mode Supported	Whether the access point can be configured as a remote edge lightweight access point. The values are Yes or No. **Note** By default, a VLAN is not enabled on the FlexConnect. After it is enabled, FlexConnect inherits the VLAN name (interface name) and VLAN ID associated to WLANs. This configuration is saved in the access point and received after the successful join response. By default, no VLAN is set as a native VLAN. There must be one native VLAN configured per REAP in a VLAN-enabled domain. Otherwise, REAP cannot send packets to or receive packets from the controller. When the client gets assigned a VLAN from the RADIUS server for the client, that VLAN is associated to the local switched WLAN. **Note** Black list—FlexConnect supports the first 128 entries in the list in the standalone mode.

Mesh Tab

Note This tab appears if you set the AP Mode on the General Tab to Bridge.

Table 5-15 Mesh Tab Parameters

Parameter	Description
AP Role	Root AP or Mesh AP. Root APs have a wired CAPWAP (Control and Provisioning of Wireless Access Points) protocol connection back to a controller. This connection uses the backhaul wireless interface to communicate to neighboring Mesh APs. Root APs are parent nodes to any bridging or mesh network and connect a bridge or mesh network to the wired network. You can have only one Root AP for any bridged or mesh network. Mesh APs have no wired connection to a controller. They can be completely wireless supporting clients, communicating to other Mesh APs and a Root AP to get access to the network, or they can be wired and serve as a bridge to a remote wired network.
Bridge Type	(Display Only Field) Whether the access point is an indoor or outdoor access point.
Bridge Group Name	Bridge group name. Use bridge group names to logically group the access points and to avoid two networks on the same channel from communicating with each other. **Note** For the access points to communicate with each other, they must have the same bridge group name.

Table 5-15 Mesh Tab Parameters

Parameter	Description
Ethernet Bridging	Ethernet bridging on the access point. If the AP Mode is Root AP, Ethernet bridging is enabled by default. If the AP Mode is Mesh AP, Ethernet bridging is disabled by default. Enable Ethernet bridging on a Mesh AP if you want to do one of the following: • Use the mesh nodes as bridges. • Connect an Ethernet device on the Mesh AP using its Ethernet port. **Note** When you enable Ethernet Bridging and click **Apply**, the Ethernet Bridging Parameters area appears and lists the four Ethernet ports of the mesh access point.
Backhaul Interface	(Display Only Field) Backhaul interface (802.11a, 802.11b, 802.11g, or 802.11n).
Bridge Data Rate (Mbps)	Rate at which data is shared between the access points. The drop-down list displays the data rates depending on the Backhaul Interface set. The correct range of values depend on the backhaul interfaces used by the access points. The data rates (Mbps) are as follows: • 802.11a: auto, 6, 9, 12, 18, 24, 36, 48, 54 **Note** In previous software releases, the default value for bridge data rate for 802.11a was 24 Mbps. In controller release 6.0, the default value for the bridge data rate is auto. If you configured the default bridge data rate value (24 Mbps) in a previous controller software release, the bridge data rate is configured with the new default value (auto) when you upgrade to controller software release 6.0. However, if you configured a nondefault value (for example, 18 Mbps) in a previous controller software release, that configuration setting is preserved when you upgrade to software release 6.0. When the bridge data rate is set to auto, the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates). • 802.11b: 1, 2, 5.5, 11 • 802.11g: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54
Ethernet Link Status	Status of the Ethernet (LAP1510) or Gigabit Ethernet (LAP1522) links. For each link, the status can be Up, Dn, or Na.
Heater Status	Status of the heater.
Internal Temperature	Internal temperature of the access point in Fahrenheit and Celsius.

Note The following parameters appear when you enable Ethernet Bridging and click **Apply**.

This table describes the Ethernet bridging parameters.

Table 5-16 Ethernet Bridging Parameters

Parameter	Description
Interface Name	Name of the interface. Click the interface name to open the VLAN Mappings for Mesh Access Points page. To configure access mode on a Mesh access point, click the **gigabitEthernet1** interface. To configure trunk mode on a Root or Mesh access point, click the **gigabitEthernet0** interface.
Oper Status	Operational status of the interface.
Mode	Mode of the interface: Normal, Access, or Trunk.
VLAN ID	VLAN ID of the interface.

FlexConnect Tab

Note This tab appears if you set the AP Mode on the General Tab to FlexConnect.

Table 5-17 FlexConnect Parameters

Parameter	Description
VLAN Support	Check box to configure the native VLAN ID and the VLAN mappings. **Note** After you enable VLAN support, click **Apply** to activate the VLAN Mappings button.
Inheritance Level	Shows the status of the VLAN Support configuration. If Native VLAN on AP is overridden, then this is shown as Group Specific.
Make VLAN AP Specific/Remove VLAN AP Specific	Drop-down list to configure VLAN support for the FlexConnect AP. When the override flag at the FlexConnect group is disabled, this additional inheritance level configuration is available for the FlexConnect AP. If you choose "Make VLAN AP Specific," then the VLAN support, Native VLAN ID, and WLAN-VLAN mappings are made specific to this AP and not to the FlexConnect group.
Native VLAN ID	VLAN ID number.
VLAN Mappings	VLAN mappings for the locally switched WLANs. Click the **VLAN Mappings** button. You can also view VLAN-ACL mappings on the AP via FlexConnect groups.
FlexConnect Group Name	Name of the group if the access point belongs to a FlexConnect group. See the FlexConnect Groups section for more information about FlexConnect groups.
PreAuthentication Access Control Lists	
External WebAuthentication ACLs	ACLs for external web authentication. Click the **External WebAuthentication ACLs** link to view and configure the ACL mappings and web policy ACLs.

Table 5-17 FlexConnect Parameters

Parameter	Description
Local Split ACLs	ACLs for the local split WLANs. Click the **Local Split ACLs** link to view and configure the local split ACLs of the REAP groups. These ACLs locally switch traffic in centrally switched WLANs.
Central DHCP Processing	Central DHCP processing parameters. Click the Central DHCP Processing link to view the WLAN DHCP mappings and configure WLAN DHCP parameters such as Central DHCP, Override DNS, and NAT/PAT. Click **Add** to create a new WLAN DHCP mapping.
Layer2 ACLs	Layer2 ACL Mappings are displayed.

Advanced Tab

The following parameters are not displayed for the Cisco OEAP 600 series access point:

- Cisco Discovery Protocol
- Rogue Detection
- Telnet
- SSH

Table 5-18 Advanced Tab Parameters

Parameter	Description
Regulatory Domains	Regulatory domain of the AP.
Country Code	Country code. See the Country topic for information on configuring the country code.
Cisco Discovery Protocol	Cisco Discovery Protocol that you can enable or disable. The default is unselected. **Note** If CDP is disabled at the controller level, a message “Controller CDP Disabled” appears.
AP Group Name	AP Group’s VLANs that you have created. To associate an AP group VLAN with an access point, follow these steps: 1. Select an AP group VLAN from the drop-down list. 2. Click **Apply**. For more information on creating a new AP group and mapping it to an interface, see the AP Groups page.
Statistics Timer	Time in seconds that the access point sends its 802.11 statistics to the Cisco WLC.

Table 5-18 Advanced Tab Parameters

Parameter	Description
Data Encryption	Datagram Transport Layer Security (DTLS) data encryption that you can enable or disable. The default is unselected. Cisco 5500 Series Wireless Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the access point and the controller using DTLS. DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established. **Note** If an access point with data encryption enabled tries to join any other controller, the access point joins the controller, but data packets are sent unencrypted. DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points. Most access points are deployed in a secure network within a company building, so data encryption is not necessary. The traffic between an OfficeExtend access point and the controller travels through an unsecure public network, so data encryption is more important for these access points. When data encryption is enabled, traffic is encrypted at the access point before it is sent to the controller and at the controller before it is sent to the client. **Note** Encryption limits throughput at both the controller and the access point, and maximum throughput is desired for most enterprise networks. The availability of data DTLS for the 7.1 release is as follows: • The Cisco 5500 Series Controller will be available with two licenses options. One that allows data DTLS without any license requirements and another image requiring a license to use data DTLS. The images for the DTLS and licensed DTLS images are as follows: – Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes – Non licensed DTLS—AS_5500_x_x_x_x.aes • Cisco 7500, 2500, WiSM2, WLC2—These platforms by default will not contain DTLS. To turn on data DTLS, a license must be installed. That is, these platforms will have a single image with data DTLS turned off. To use data DTLS you must have a license. **Note** If your controller does not have data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted. The following are some of the guidelines when upgrading to or from a DTLS image: • You cannot install a regular image (DTLS enabled) once a non-DTLS image is installed. • You can upgrade from one licensed DTLS image to another licensed DTLS image. • You can upgrade from a regular image (DTLS) to a licensed DTLS image in a two step process. • You cannot upgrade from a licensed DTLS image to any regular image.
Rogue Detection	Rogue detection for individual access points that you can enable or disable. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). The default is unselected.

Table 5-18 Advanced Tab Parameters

Parameter	Description
AP Sub Mode	AP submode that displays *wIPS* if the access point is in Monitor mode (from the **AP Mode** drop-down list on the General Tab) and the wIPS submode is configured on the access point or *None* if the access point is in local/FlexConnect modes and wIPS submode is not configured.
Telnet	Telnet or SSH connectivity on this access point. The default is unselected.
SSH	These protocols make debugging the access point easier, especially when the access point is unable to connect to the controller.
TCP Adjust MSS	Enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router on a per AP basis. From Release 8.0, the controller supports IPv6. Use the following Global TCP Adjust MSS values for: • IPv4—Specify a value between 536 and 1363. • IPv6—Specify a value between 1220 and 1331. **Note** Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP
UDP Lite	Displays the per AP UDP lite status. **Note** The UDP Lite field is displayed only for APs that are associated using CAPWAP v6. This field is not displayed for APs associated using IPv4 address.
Disable LAN Ports	Parameter that makes the AP work only as a wireless AP. **Note** This option is applicable only for Cisco 600 Series OfficeExtend Access Points.
Disable Personal SSID	Parameter that disallows users from setting up personal SSIDs. **Note** This option is applicable only for Cisco 600 Series OfficeExtend Access Points.
LED State	Parameter to enable or disable the LED state of the AP to be shown.
LED Flash State	• Click the LED flash duration for the AP option and enter the duration range from 1 to 3600 seconds • Click the **Indefinite** option to configure the LED to flash indefinitely • Click the **Disable** option to stop flashing the LED
Hyperlocation BLE Module	Shows whether a Hyperlocation BLE module is present or not.
BLE Beacon Configuration **Note** To configure the following local BLE beacon parameters.	
Beacon ID	Five available options: Beacon1 to Beacon5
Major	Configures beacon's major value.
Minor	Configures beacon's minor value.
TxPower (–52 to 0) dBm	Configures selected beacon's transmission power.
Link Latency **Note** The Link Latency parameters are not displayed for ODM access points.	

Table 5-18 Advanced Tab Parameters

Parameter	Description
Enable Link Latency	Link latency for this access point. Enable link latency to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect access points (in connected mode) and OfficeExtend access points, for which the link could be a slow or unreliable WAN connection. **Note** FlexConnect access points in standalone mode are not supported.
Current (mSec)	Current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
Minimum (mSec)	Minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back since link latency has been enabled or reset.
Maximum (mSec)	Maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back since link latency has been enabled or reset.
Reset Link Latency	Link latency statistics on the controller for this access point.
AP Image Download	
Note The 1120, 1230, and 1310 access points do not support predownloading of images.	
Perform a primary image pre-download for this AP	Primary image predownload. Click **Download Primary** to perform a primary image predownload for this access point. An alert box displays the version that would be downloaded when the access point boots. Click **OK** to continue.
Perform an interchange of both the images on this AP	Interchange of images. Click **Interchange Image** to change the images on this access point. A dialog box prompts you to confirm if you want to interchange the images. Click **OK** to continue.
Perform a backup image pre-download for this AP	Backup image predownload. Click **Download Backup** to predownload a backup image for this access point. A pop-up window displays the version that would be downloaded when the access point boots. Click **OK** to continue.
Power Over Ethernet Settings	
Note The Power Over Ethernet Settings parameters are not displayed for Cisco OEAP 600 Series access points.	
PoE Status	Status that applies only to 1250 series access points that are powered using PoE. This field shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This field is not configurable. The controller automatically detects the access point's power source and displays the power level here. **Note** There are two other ways to tell if the access point is operating at a lower power level. First, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section on the Configuring 802.11a/n APs page. Second, the "PoE Status: degraded operation" message appears in the controller's trap log on the Trap Logs page.
Pre-Standard State	Whether the access point is being powered by a high-power Cisco switch. Unselect the check box if power is being provided by a power injector. This option is disabled by default.

Table 5-18 Advanced Tab Parameters

Parameter	Description
Power Injector State	Whether the attached switch supports intelligent power management (IPM) and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.
Power Injector Selection	One of the following options: • Installed—Select the check box if you want the access point to examine and remember the MAC address of the currently connected switch port (this selection assumes that a power injector is connected). If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC address text box. • Override—Select the check box to enable the access point to operate in high-power mode without first verifying a matching MAC address.
Injector Switch MAC Address	MAC address of the connected switch port.
AP Core Dump Settings	
Note The File Compression parameter is not displayed for ODM access points.	
AP Core Dump	Upload the access point core dump. The default is enabled.
TFTP Server IP	IP address of the TFTP server. From release 8.0, the TFTP server supports IPv6 address too.
File name	Access point core dump file (for example, dump.log).
File Compression	File compression of the access point core dump file. When you enable this option, the file is saved with a .gz extension (for example, dump.log.gz). This file can be opened with WinZip. The default is disabled.
AP Retransmit Config Parameters	
AP Retransmit Count	Number of times that you want the access point to retransmit the request to the controller and vice versa. The range is from 3 to 8.
AP Retransmit Interval	Time duration between retransmission of requests. The range is from 2 to 5.
VLAN Tagging Settings	
VLAN Tagging	VLAN tagging of the CAPWAP packets that you can enable or disable.
Trunk VLAN ID	ID of the trunk VLAN. If the access point is unable to route traffic through the specified trunk VLAN, it untags the packets and reassociates with the controller. The controller sends a trap to a trap server such as the Cisco PI, which indicates the failure of the trunk VLAN. If the trunk VLAN ID is zero, the access point untags the CAPWAP packets.
VLAN Tag Status	Whether the access point tags or untags the CAPWAP packets.
Trusted Security	
TrustSec Config	Configures Cisco TrustSec. Click **TrustSec Config** link to view and configure Cisco TrustSec.

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

Sniffer Feature

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AirMagnet Enterprise Analyzer, Airopeek, or Wireshark. These packets contain information on timestamps, signal strengths, packet sizes and so on.

Note You can enable the sniffer feature only if you are running Airopeek or Wireshark (third-party network analyzer software that supports decoding of data packets).

Note You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module running software release 6.0. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable** command from the controller CLI.

Note You must enable WLAN 1 to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module running software release 6.0. If WLAN 1 is disabled, the access point cannot send packets.

Before using the sniffer feature, you must configure an access point in sniffer mode at the remote site. See the *Cisco Wireless LAN Controller Configuration Guide* for installation information for AirMagnet Enterprise Analyzer, Airopeek, and Wireshark packet analyzers for IEEE 802.11 wireless LANs.

Traffic Stream Metrics Collection

Choose **MONITOR > Wireless > Clients** and then click **802aTSM** or **802b/gTSM** to navigate to the Traffic Stream Metrics page.

Traffic stream metrics involves collecting of uplink statistics and downlink statistics between an AP and a CCX v4 client and then propagating these statistics periodically back to the controller. If the client is not CCXv4 compliant, then only downlink statistics are captured.

Traffic stream metrics collection can be configured by the user for each interface band (for example, all 802.11a radios). The controller also saves this option in flash memory so that it persists across reboots. Once an AP receives this message, it enables traffic metrics collection feature on the specified interface type.

Every 5 seconds, the AP gets a measurement report for both the uplink (client side) and downlink (local side) measurements. The aggregation of 5-second reports and preparation of 90-second reports is done at the AP. Every 90 seconds, the AP prepares an IAPP data packet and sends it to the controller for further processing. The controller stores the data in its structures and then provides “usmdB” access APIs to the CLI module and the WCS for displaying it on the UI.

Four variables are affected by the WLAN that can affect audio quality: packet latency, packet jitter, packet loss and roaming time. You can isolate the problem of bad voice quality by studying these variables. The traffic stream metrics feature addresses the voice quality issue by providing an administrator with statistics for each of these four variables.

OfficeExtend Access Points

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The experience of the teleworker at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Guidelines and Limitations

1. OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. In controller software release 6.0 or later releases, only one OfficeExtend access point can be deployed behind a single NAT device.
2. Rogue detection is disabled when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point by selecting the Rogue Detection check box on the All APs Details for (Advanced) page. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.
3. DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point by selecting the Data Encryption check box on the All APs Details for (Advanced) page.
4. Telnet and SSH access are disabled when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by selecting the Telnet or SSH check box on the All APs Details for (Advanced) page.
5. Link latency is enabled when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point by selecting the Enable Link Latency check box on the All APs Details for (Advanced) page.
6. The Cisco 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 Cisco OEAP 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 Cisco OEAP 600 Series is in the default group. The WLAN/remote LAN IDs must be less than 8.
7. Only four clients can connect to an Cisco OEAP 600 Series access point through a remote LAN port. This number does not affect the 15-client 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.
8. CAC is not supported on the Cisco OEAP 600 Series access points.
9. Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the Cisco WLC.

The following access point modes are not supported on the Cisco OEAP 600 Series access points:

- Monitor mode
- FlexConnect mode
- Sniffer mode

- Rogue Detector Bridge mode
- SE-Connect mode

VLAN Mappings for FlexConnect Access Points

Choose **WIRELESS > Access Points > All APs**, click the AP name of a FlexConnect access point, click the **FlexConnect** tab, and then click **VLAN Mapping** to navigate to the VLAN Mappings page. This page enables you to assign a VLAN ID to the FlexConnect access point and configure VLAN mappings for the locally switched WLANs. You can also view VLAN-ACL mappings on the AP via the FlexConnect group.

Table 5-19 VLAN Mapping Parameters

Parameter	Description
AP Name	Name of the access point
Base Radio MAC	MAC address of the 802.11a/b/g/n radio
WLAN VLAN Mapping	
Drop-down list	To make the WLAN-VLAN mapping as either specific the FlexConnect AP or to remove the configuration
WLAN ID	WLAN ID number
SSID	Name of the WLAN
VLAN ID	Number of the VLAN from which the clients receive an IP address when doing local switching
NAT-PAT	Status of Network Address Translation and Port Address Translation on the locally switched WLANs
Inheritance	Shows the VLAN support inheritance status
Centrally Switched WLANs	
WLAN ID	WLAN ID to which this is mapped to
SSID	Service Set Identifier of the WLAN
VLAN ID	VLAN ID of the WLAN
AP	Access point name
AP Level VLAN ACL Mapping	
VLAN ID	VLAN ID number
Ingress ACL	Name of the Ingress ACL
Egress ACL	Name of the Egress ACL
Group Level VLAN ACL Mapping	
VLAN ID	VLAN ID number
Ingress ACL	Name of the Ingress ACL
Egress ACL	Name of the Egress ACL

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.

WebAuth and WebPolicy ACL Mappings for FlexConnect Access Points

Choose **WIRELESS > Access Points > All APs, >** ***AP_name*** **> FlexConnect** tab, and click the **External WebAuthentication ACLs** link to navigate to the External WebAuthentication ACLs page. This page enables you to configure WLAN ACL mappings for FlexConnect access points and to add WebPolicy ACLs.

Table 5-20 WebAuth and WebPolicy ACL Mappings for FlexConnect Access Points

Parameter	Description
AP Name	Name of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
WLAN ACL Mapping	
WLAN ID	WLAN ID number.
WebAuth ACL	Drop-down list from which you can choose the FlexConnect ACL for external web authentication in locally switched WLANs. Click **Add** to configure the WLAN ACL Mapping.
WebPolicies	
WebPolicy ACL	Drop-down list from which you can select a FlexConnect ACL to be added as a web policy. Click **Add** to add the WebPolicy ACL. **Note** You can configure up to 16 WebPolicy ACLs that are specific to an access point.

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.

Local Split ACL Mappings (for FlexConnect Access Points)

Choose **WIRELESS > Access Points > All APs, >** ***AP_name*** **> FlexConnect** tab, and click the **Local Split ACLs** link to navigate to the Local Split ACLs page. This page enables you to configure local split ACLs for FlexConnect APs.

Table 5-21 Local Split ACL Mappings for FlexConnect Access Points

Parameter	Description
AP Name	Name of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
WLAN ACL Mapping	

Table 5-21 Local Split ACL Mappings for FlexConnect Access Points

Parameter	Description
WLAN ID	WLAN ID number.
Local-split ACL	Drop-down list from which you can choose the Local Split ACL to locally switch traffic in centrally switched WLANs. Click **Add** to configure the local split ACL mappings. Local-split configuration is applied specific to a WLAN. You can also apply this configuration from a FlexConnect group or from an AP. If the local-split configuration is applied at both the FlexConnect group level and AP level, then the configuration applied at the AP level has higher priority. In other words, the FlexConnect ACL specific to the AP has higher priority.

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.

Central DHCP ACL Mappings for FlexConnect Access Points

Choose **WIRELESS > Access Points > All APs, >** ***AP_name*** **> FlexConnect** tab, and click the **Central DHCP Processing** link to navigate to the Central DHCP Processing page. This page enables you to configure central DHCP, override DNS, and enable NAT/PAT on a WLAN.

Table 5-22 Central DHCP Mappings for FlexConnect Access Points

Parameter	Description
AP Name	Name of the access point.
Base Radio MAC	MAC address of the 802.11a/b/g/n radio.
WLAN DHCP Mapping	
WLAN ID	WLAN ID number.

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.

TrustSec Config

Choose **WIRELESS > Access Points > All APs, >** ***AP_name*** **> Advanced** tab, and click the **TrustSec Config** link to navigate to the **Trusted Security** page. This page enables you to configure SGACL, Inline tagging, and SXP on a WLAN.

Table 5-23 TrustSec Config Parameters

Parameter	Description
AP Name	Name of the AP
Base Radio MAC	MAC address of the 802.11a/b/g/n radio
Trusted Security	

Table 5-23 TrustSec Config Parameters

Parameter	Description
SGACL Enforcement	By default, SGACL enforcement is enabled only if Cisco TrustSec is in enabled state globally.
Inline Tagging	Check box to check to enable inline tagging **Note** Inline tagging is supported only on FlexConnect mode APs (applicable to 802.11ac APs).
Total AP SXP Connections	Displays the number of SXP connections that are configured on APs
AP SXP State	By default, the SXP connections are disabled
Default Password	Displays the password for MD5 authentication of SXP messages
SXP Listener Min Hold Time (seconds)	Displays the SXP listener minimum hold time
SXP Listener Max Hold Time (seconds)	Displays the SXP listener maximum hold time
SXP Speaker Hold Time (seconds)	Displays the speaker hold time
Reconciliation Time Period (seconds)	Displays the reconciliation time period
Retry Period (seconds)	SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000 seconds. The SXP retry period determines how often the controller retries for an SXP connection.
Peer IP Config	
Peer IP Address	IP address of the peer.
Password	Password is set to Default.
Mode	Mode of the controller. The controller is always set to Speaker mode.
Click **ADD** to add the peer IP configuration details.	

You get to view the Peer IP Address, Source IP Address, Password, Sxp Mode, Listener Status, Speaker status, and Sxp Version.

Click **Apply** to send data to the Cisco WLC.

Note SXPv4 (Listener or Speaker or Both) is supported on Flex and Flex+bridge access points (applicable to 11ac AP). Also, Cisco 5508/7510/8510/WiSM2/vWLC wireless controllers support only SXPv4 Speaker mode for Flex mode access point. Sgacl Enforcement and Inline Tagging are supported only on Cisco 5520 or 8540 WLCs.

VLAN Mappings for Mesh Access Points

Choose **WIRELESS > Access Points > All APs**, click the AP name of a mesh (bridge) access point, click the **Mesh** tab, and then click an Ethernet interface from the Ethernet Bridging area to navigate to the VLAN Mappings page.

Note The Ethernet Bridging area appears after you enable Ethernet Bridging and click **Apply**.

Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

Configure access mode on gigabitEthernet1. Configure trunk mode on gigabitEthernet0.

Note Configurations on gigabitEthernet2 and gigabitEthernet3 interfaces are not supported.

Configuring Access Mode

To configure a mesh access point (MAP) access port, follow these steps:

Step 1 Choose **access** from the mode drop-down list.

Step 2 Enter a VLAN ID. The VLAN ID can be any value between 1 and 4095.

Step 3 Click **Apply**.

Note VLAN ID 1 is not reserved as the default VLAN.

Note A maximum of 16 VLANs are supported across all of a RAP's subordinate MAPs.

Configuring Trunk Mode

To configure a root access point (RAP) or MAP trunk port, follow these steps:

Step 1 Choose **trunk** from the mode drop-down list.

Step 2 Enter a native VLAN ID for the incoming traffic. The native VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to a user-VLAN (access).

Step 3 Click **Apply**.

A trunk VLAN ID text box and a summary of configured VLANs appears at the bottom of the page. The trunk VLAN ID text box is for outgoing packets.

Step 4 Enter a trunk VLAN ID for outgoing packets:

a. If forwarding untagged packets, do not change the default trunk VLAN ID value of zero (MAP-to-MAP bridging, campus environment).

b. If forwarding tagged packets, enter a VLAN ID (1 to 4095) that is not already assigned (RAP to switch on wired network).

Step 5 Click **Add** to add the trunk VLAN ID to the allowed VLAN list. The newly added VLAN appears under Configured VLANs on the page.

To remove a VLAN from the list, click the blue arrow adjacent the desired VLAN and choose **Remove**.

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.

Neighbor Information of Access Points

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Neighbor Information** to navigate to the Neighbor Information page.

This page lists the parent, children, and neighbors of the access point. It provides each access point's name and radio MAC address.

To perform a link test between the access point and its parent or children, click the blue arrow adjacent the desired access point and choose **LinkTest**. A dialog box appears.

Click **Submit** to start the link test. The link test results appear on the Mesh > LinkTest Results page.

- To view the details for any access point on this page, click the blue arrow adjacent the desired access point your cursor over the blue drop-down arrow for the desired access point and choose **Details**. The Link Details of Access Points page appears.
- To view statistics for any access point on this page, click the blue arrow adjacent the desired access point and choose **Stats**. The Mesh Neighbor Statistics page appears.

Link Details of Access Points

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Details** to navigate to the Link Details page.

This page displays the following details:

- Neighbor Local Mode AP Fast Heartbeat Timeout (1 to 10)
- Neighbor MAC Address
- Neighbor Type
- Channel
- Backhaul Data Rate
- Link SNR
- Time of Last Hello

Mesh Neighbor Statistics

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Stats** to navigate to the Neighbor Statistics page.

This page displays the following details:

- Neighbor AP Name/MAC Address
- Neighbor Base Radio MAC Address
- Packets Transmitted as Parent
- Packets Received as Parent
- Total Tx Packets

- Total Tx Successful
- Total Tx Retries
- Poor SNR Rx

Access Points Statistics

Choose **WIRELESS > Access Points > All APs**, click the blue arrow adjacent the desired access point and choose **Statistics** to navigate to the Access Points Statistics page.

This page provides the following information:

- AP Role—Role of the access point in the mesh network RootAP or MeshAP
- Bridge Group Name—Name of the bridge group to which the access point belongs
- Backhaul Interface—Backhaul interface on which the access point operates
- Switch Physical Port—Number of the physical switch port

Mesh Node Stats

Table 5-24 Mesh Node Parameters

Parameter	Description
Malformed Neighbor Packets	Number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
Poor Neighbor SNR Reporting	Number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
Excluded Packets	Number of packets received from excluded neighbor mesh access points.
Insufficient Memory Reporting	Number of insufficient memory conditions.
Rx Neighbor Requests	Number of broadcast and unicast requests received from the neighbor mesh access points.
Rx Neighbor Responses	Number of responses received from the neighbor mesh access points.
Tx Neighbor Requests	Number of unicast and broadcast requests sent to the neighbor mesh access points.
Tx Neighbor Responses	Number of responses sent to the neighbor mesh access points.
Parent Changes Count	Number of times that a mesh access point (child) moves to another parent.
Neighbor Timeouts Count	Number of neighbor timeouts.

Queue Stats

Table 5-25 Queue Statistics Parameters

Parameter	Description
Gold Queue	Average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval.
Silver Queue	Average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval.
Platinum Queue	Average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval.
Bronze Queue	Average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval.
Management Queue	Average and peak number of packets waiting in the management queue during the defined statistics time interval.

Mesh Node Security Stats

Table 5-26 Mesh Node Security Statistics Parameters

Parameter	Description
Transmitted Packets	Number of packets transmitted during security negotiations by the selected mesh access point.
Received Packets	Number of packets received during security negotiations by the selected mesh access point.
Association Request Failures	Number of association request failures that occur between the selected mesh access point and its parent.
Association Request Timeouts	Number of association request timeouts that occur between the selected mesh access point and its parent.
Association Requests Successful	Number of successful association requests that occur between the selected mesh access point and its parent.
Authentication Request Failures	Number of failed authentication requests that occur between the selected mesh access point and its parent.
Authentication Request Timeouts	Number of authentication request timeouts that occur between the selected mesh access point and its parent.
Authentication Requests Successful	Number of successful authentication requests between the selected mesh access point and its parent.
Reassociation Request Failures	Number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Number of reassociation request timeouts between the selected mesh access point and its parent.
Reassociation Requests Successful	Number of successful reassociation requests between the selected mesh access point and its parent.
Reauthentication Request Failures	Number of failed reauthentication requests between the selected mesh access point and its parent.

Table 5-26 Mesh Node Security Statistics Parameters

Parameter	Description
Reauthentication Request Timeouts	Number of reauthentication request timeouts that occur between the selected mesh access point and its parent.
Reauthentication Requests Successful	Number of successful reauthentication requests that occur between the selected mesh access point and its parent.
Unknown Association Requests	Number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
Invalid Association Requests	Number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state may occur when the selected child is a valid neighbor but is not in a state that allows association.
Reauthentication Requests	Number of unknown reauthentication requests received by the parent mesh access point node from its child. This state may occur when a child mesh access point is an unknown neighbor.
Invalid Reauthentication Requests	Number of invalid reauthentication requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reauthentication.
Unknown Reassociation Requests	Number of unknown reassociation requests received by the parent mesh access point from a child. This state may occur when a child mesh access point is an unknown neighbor.
Invalid Reassociation Requests	Number of invalid reassociation requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reassociation.

Link Test

Choose **WIRELESS > Access Points > All APs/Detail,** and then click **Link Test** to navigate to the Link Test page.

You can test the status of a bridge connection using the link test. Using the link test, you can configure and execute tests, check the status of a test, and access test data.

This test involves one transmitting WRAP and one receiving WRAP. A WRAP can run only one test at a time; you cannot have multiple WRAPs transmitting to one receiving WRAP.

The link test page displays the link test parameters and the results of the last link tests, sorted by the link test ID. The link test ID is the receiving access point's ID.

Table 5-27 Link Test Parameters

Parameter	Description
AP Name	(Display Only Field) The transmitting WRAP name.
AP MAC address	(Display Only Field) The transmitting WRAP MAC address.
AP Role	(Display Only Field) The transmitting WRAP role.
Bridged Neighbor AP	WRAP whose link you want to test. This is the Link Test ID. Make sure to clear the existing link test results using the Clear option at the bottom of that WRAP's Link Test Results area. For example, if you are conducting the link test on Bridged Neighbor AP 8, go to the Link Test Results section, scroll to the Link Test ID 8, and click **Clear**.
Packet Size	Packet size. The range is from 0 to 2300.
Bytes per Second	Bytes per second. This value can be up to 80% of the data rate.
Duration in Seconds	Test duration. The range is from 10 to 300 seconds.
Data Rate (Mbps)	The valid data rates are as follows: • 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 • 802.11b: 1, 2, 5.5, 11 • 802.11g: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54

Note Before conducting a link test on a receiving WRAP, go to the Link Test Results of that WRAP and click **Clear** to clear the existing Link Test Results.

Specify your link test values and click **Link Test**.

The link test is conducted for the duration that you specify. If the test is successful, the Link Test Results field parameters are populated with the latest link test results for the selected Bridged Neighbor AP (Link Test ID).

Link Test Results

Table 5-28 Link Test Result Parameters

Parameter	Description
Link Test ID	Receiving WRAP ID specified using the Bridged Neighbor AP field.
Bridged Neighbor AP	Receiving WRAP whose link was tested.
Tx Packets	Number of packets transmitted during the link test duration.
Tx Dropped Packets	Number of transmitting packets dropped during the link test duration. The transmitting WRAP can only send data at a certain rate. If more data is received than can be sent, it is stored in the buffer. If the buffer is full, some packets are dropped.
Rx Good Packets	Number of good packets received during the link test duration.
Rx Lost Packets	Number of lost packets during the link test duration.
Rx Out of Order Packets	Number of packets received that were not in the order at which they were transmitted during the link test duration. Packets are received by the receiving WRAP in the order that they were sent by the transmitting WRAP. For example, the second packet transmitted is expected to reach the receiving WRAP as the second packet. If the packet that was sent second reaches the receiving WRAP after it received the forth packet, the second packet is an out of order packet.

Radios

This section contains the following topics:

- 802.11a/n/ac Radios, page 5-36
- 802.11b/g/n Radios, page 5-49
- Dual-Band Radios, page 5-59

802.11a/n/ac Radios

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac** or **MONITOR > Summary** and click **802.11 a/n/ac** radios to navigate to the 802.11 a/n/ac Radios page.

This page displays an overview of your 802.11a/n/ac Cisco Radio network. The status of each 802.11a/n/ac Cisco Radio configured on this Cisco WLC and its profile is detailed here.

Beginning in controller Release 7.5 and later, 802.11ac APs are supported in the controller. 802.11ac, a 5 GHz-only technology, is a faster and a more scalable version of 802.11n. The 802.11n inherits the properties of the 802.11n radio.

- To configure the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Configure** (Configuring 802.11a/n APs).
- To view details about the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Details** (802.11a/n/ac AP Interfaces Details).

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) to create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC addresses or AP names.

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

- MAC Address—MAC address text box where you enter a MAC address.
- AP Name—AP Name text box where you enter an access point name.
- CleanAir Oper Status—Operational status of the CleanAir capable access point.

Note When you enable filtering by the MAC address, the other filters are disabled automatically. However, you can use a combination of the AP name and CleanAir operational status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11a/n/ac Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

This table lists the 802.11 a/n/ac radio parameters.

Table 5-29 802.11 a/n/ac Cisco Radio Summary Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Radio Slot#	Slot in which the radio is installed. **Note** Radio slot 2 information for all the AP 3600 radios appears when the 802.11ac radio is plugged in.
Base Radio MAC	MAC address of the 802.11a/n/ac radio.
Sub Band	Radio sub band, if it is active. The value is 4.9 GHz or 5.8 GHz.
Admin Status	Admin status of the access point on this radio.
Operational Status	Cisco Radio operational status.
Channel	Channel number of the access point.

Table 5-29 802.11 a/n/ac Cisco Radio Summary Parameters

Parameter	Description
CleanAir Admin Status	Administration status of the spectrum sensor for the access point.
CleanAir Oper Status	Status of the spectrum sensor for this access point. The CleanAir status is one of the following: • UP—The spectrum sensor for the access point radio is operational (error code 0). • DOWN—The spectrum sensor for the access point radio is not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio. • ERROR—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable CleanAir functionality on the radio. • N/A—This access point radio cannot support CleanAir functionality. Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir. **Note** You can create a filter to make the 802.11a/n Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP page, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).
Radio Role	Radio role for the backhaul, either UPLINK or DOWNLINK.
Power Level	Transmit power level for the access point: • 1 = Maximum power allowed per Country Code setting • 2 = 50% power • 3 = 25% power • 4 = 6.25 to 12.5% power • 5 = 0.195 to 6.25% power **Note** The power levels and available channels are defined by the Country Code setting and are regulated on a country by country basis.
Antenna	Internal or external antennas.

Configuring 802.11a/n APs

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac**, click the blue arrow adjacent the desired access point and choose **Configure** to navigate to the Configure page. For details on configuring an 802.11ac radio on access points, see Configuring 802.11ac Radio in Access Points.

This page enables you to configure parameters specifically for this Cisco Radio including the antenna type, RF channel, and Tx power level assignments. The performance profile for this Cisco Radio is also accessed through this page.

General

Table 5-30 General Parameters

Parameter	Description
AP Name	(Display Only Field) Customer-definable name of the access point.
Admin Status	Interface status of enabled or disabled. The default is enabled. **Note** If you disable 802.11n, the 802.11ac radio is also disabled.
Operational Status	(Display Only Field) Cisco Radio operational status: either UP or DOWN. The default is UP.
Slot #	Slot where the radio is installed.

Link Parameters

These parameters are displayed for the 802.11a/n/ac radios on the Mesh access points.

Table 5-31 Link Parameters

Parameter	Description
Radio Role	Radio role for the backhaul of UPLINK or DOWNLINK.
Source Backhaul MAC	MAC address of the source backhaul radio.

11n Parameters

Table 5-32 11n Parameters

Parameter	Description
11n Supported	(Display Only Field) Indicates whether 802.11n is supported.
11ac Supported	(Display Only Field) Indicates whether 802.11ac is supported. This field appears only for 802.11ac slave radios on slot 2.

CleanAir

Table 5-33 CleanAir Parameters

Parameter	Description
CleanAir Capable	(Display Only Field) CleanAir capability of the access point. Whether the access point is CleanAir capable.
CleanAir Admin Status	Status of the CleanAir admin that you can enable or disable. The default is disabled.

Antenna Parameters

Table 5-34 Antenna Parameters

Parameter	Description
Antenna Type	Internal or external antenna type.
Antenna (Displayed if 11n is supported)	Specific antennae for the access point that you can enable or disable: • A—Right antenna port • B—Left antenna port • C—Center antenna port • D—Dua-band antenna By default, all are selected. For example, to enable transmissions from antenna ports A and B and receptions from antenna port C, you should select the following check boxes: Tx: A and B and Rx: C. Valid combinations are A, A+B, A+B+C, or A+B+C+D. When you select a dual-mode antenna, you can apply only a single spatial 802.11n stream rate. The range is from MCS 0 to 7. When you select two dual-mode antennae, you can apply only two spatial 802.11n stream rates: The range is from MCS 0 to 15. You must enable two antennae for dual-band access points such as Cisco Aironet 1600 Series Access Point and Cisco Aironet 3600 Series Access Point.

Table 5-34 Antenna Parameters

Parameter	Description
Diversity (Displayed if 11n is not supported)	Select one of the following: • Enable—Enables diversity on both the connectors. • Right—Enables diversity for the Right (Connector B) antenna. • Left—Enables diversity for the Left (Connector A) antenna.
Antenna Gain	Antenna gain. If you have a high-gain antenna, enter a value that is twice the actual dBi value (see the Cisco Aironet Antenna Reference Guide for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4 dBi gain, multiply the 4.4 dBi by 2 and round down to enter only the whole number (8). The controller reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations. **Note** This option is available only if the antenna type is set to **external**.

Sniffer Channel Assignment

Note This area is displayed if you set the AP Mode on the General Tab to Sniffer.

Table 5-35 Sniffer Channel Assignment Parameters

Parameter	Description
Sniff	Sniffer operation that you can enable or disable. When enabled, the access point begins capturing and forwarding all the packets from the client on a specific channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). The default value is disabled (or unselected).
Channel	Channel on which the access points sniffs for packets. The default value is 1.
Server IP Address	IP address of the remote machine running Airopeek or Wireshark.

RF Channel Assignment

Note This area is displayed if you set the AP Mode on the General Tab to Sniffer.

Table 5-36 RF Channel Assignment Parameters

Parameter	Description
Current Channel	(Display Only Field) Channel number of the access point. **Note** The channels 1, 6, and 11 are nonoverlapping.
Channel Width[1]	Set the RF channel Assignment Method to Custom, and select one of the following channel widths: • 20 MHz—Enables the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value. • 40 MHz—Enables 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose from the Assignment Method drop-down list as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose a primary channel of 44, the controller would use channel 48 as the extension channel. If you choose a primary channel of 48, the controller would use channel 44 as the extension channel. • 80 MHz—Enables the radio to communicate using 80-MHz channels. This option is supported only for 802.11ac capable radios. 802.11ac channelization uses four adjacent 20-MHz channels. From the drop-down list you can select the primary channel and based on the available channel pairing, appropriate secondary 20-MHz and secondary 40-MHz extension channels can be configured for the radio. **Note** To select the channel width as 80-MHz, 802.11ac support must be enabled in **WIRELESS > 802.11a/n/ac > High Throughput (802.11n/ac)**.
Assignment Method	Assignment method that you can choose: • Global—Use this setting if you set the channel of the access point globally by the Cisco WLC. • Custom—Use this setting if you set the channel locally. Choose a channel from the drop-down list. **Note** The assignment method should be left at the global setting to enable the Cisco WLC to dynamically change the channel number based Radio Resource Management (RRM) directives. For the Cisco 3600 Access Points with the 802.11ac module, channel and transmit power assignments are not supported in the custom mode. The 802.11ac radio inherits the channel and power assignments applied to the 802.11n radio. When the assignment mode is custom, you can configure only the channel width settings on the 802.11ac radio.

1. Statically configuring an access point's radio for the 20-MHz, 40-MHz, or 80-MHz mode overrides the globally configured DCA channel width setting on the DCA page. If you ever change the static RF channel assignment method back to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

Tx Power Level Assignment

Table 5-37 Tx Power Level Assignment Parameters

Parameter	Description
Current Tx Power Level	(Display Only Field) Transmission power level of the access point. Tx Power Level indicates the maximum power. **Note** The power levels and available channels are defined by the Country Code setting and are regulated on a country-by-country basis.
Assignment Method	Assignment method that you can choose: • Global—Use this setting if you set the transmit power of the access point globally by the Cisco WLC. • Custom—Use this setting if the transmit power of the access point is set locally. Choose an option from the drop-down list.
Note The assignment method should be left at the global setting to enable the Cisco WLC to dynamically change the transmit power level based on the Radio Resource Management (RRM).	

Configuring Tx Power Levels

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the product guide or data sheet at http://www.cisco.com for each specific model in order to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example, 2, 3, 4, and so on) represents approximately a 50 percent (or 3 dBm) reduction in the transmit power from the previous power level.

Note The actual power reduction may vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Note Whether you choose the Global or Custom assignment method, the actual conducted transmit power at the access point is verified so that country specific regulations are not exceeded.

Performance Profile

See the Performance Profile of 802.11a/n/ac Access Points topic.

Tracking Optimization

Note If your access point is configured to operate in Monitor mode, you can enable tracking optimization on up to four channels within the 2.4 GHz band (802.11b/g radio) of an access point to enable you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6 and 11).

This table describes the tracking optimization parameters.

Table 5-38 Tracking Optimization Parameters

Parameter	Description
Enable Tracking Optimization	Tracking optimization that you can enable or disable.
Channel 1 Channel 2 Channel 3 Channel 4	Channels on which you want to monitor tags. **Note** To eliminate a channel from monitoring tag, choose **None** from the channel drop-down list.

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.

Configuring 802.11ac Radio in Access Points

Beginning in Cisco WLC Release 7.5 and later, 802.11ac APs are supported by the Cisco WLC. 802.11ac, a 5 GHz-only technology, is a faster and a more scalable version of 802.11n.

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac**, click the blue arrow adjacent the desired 802.11ac slave radio on slot 2, and then click **Configure** to configure the 802.11ac slave radio.

802.11ac radio on slot 2 is a slave radio and you can configure only a few parameters specifically for this Cisco Radio. As 802.11ac is a slave radio, it inherits many properties from the main radio 802.11a/n on slot 1. The only parameters that you can configure for this radio are as follows:

- Admin Status—Interface status of the radio that can be enabled or disabled. The default is enabled. If you disable 802.11n, the 802.11ac radio is also disabled.
- Channel Width—You can choose the RF channel width as 20 MHz, 40 MHz, or 80 MHz. If you choose the channel width as 80 MHz, you must enable 802.11ac mode in the High Throughput page. To enable 802.11ac mode, choose **WIRELESS > 802.11a/n/ac > High Throughput (802.11n/ac)**, and select the **11ac Mode** check box.

The 11ac Supported field is a nonconfigurable parameter that appears for the 802.11ac slave radio on slot 2 and indicates that the radio is 802.11ac capable.

For the Cisco 3600 Access Points with the 802.11ac module, channel and transmit power assignments are not supported in the custom mode. The 802.11ac radio inherits the channel and power assignments applied to the 802.11n radio. When the assignment mode is custom, you can configure only the channel width settings on the 802.11ac radio.

Performance Profile of 802.11a/n/ac Access Points

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n**, click the blue drop-down arrow for an AP name, choose **Configure**, and then click **Performance Profile** to navigate to the Performance Profile page.

This page shows the details of the performance profile of the selected Cisco Radio.

Table 5-39 802.11 General Parameters

Parameter	Description
Interface Type	Cisco Radio type: 802.11a/n/ac or 802.11b/g/n.
AP Name	User-definable name of the access point.
AP ID	Access point identification number that is automatically assigned by the Cisco WLC.
Profile Parameters Globally Controlled	Globally controlled parameters that you can enable or disable. You cannot change the following parameters if the Profile Parameters Globally Controlled check box is selected.
Interference (0 to 100%)	Foreign 802.11a/n or 802.11b/g/n interference threshold between 0 and 100 percent. You can globally set this setting on the RF Grouping pages.
Clients (1 to 75)	Client threshold between 1 and 75 clients. You can globally set this setting on the RF Grouping pages.
Noise (-127 to 0 dBm)	Noise threshold between –127 and 0 dBm. You can globally set this setting on the RF Grouping pages.
Coverage (3 to 50 dBm)	802.11a/n or 802.11b/g/n coverage threshold between 3 and 50 dBm. You can globally set this setting on the RF Grouping pages.
Utilization (0 to 100%)	802.11a/n or 802.11b/g/n RF utilization threshold between 0 and 100 percent. You can globally set this setting on the RF Grouping pages.
Coverage Exception Level (0 to 100%)	Coverage exception level between 0 and 100 percent. You can globally set this setting on the RF Grouping pages.
Data Rate (1 to 1000 Kbps)	802.11a/n or 802.11b/g/n throughput threshold between 1 Kbps and 1000 Kbps. You can globally set this setting on the RF Grouping pages.
Client Min Exception Level (1 to 75)	Client minimum exception level. You can globally set this setting on the RF Grouping pages.

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.

802.11a/n/ac AP Interfaces Details

Choose **WIRELESS > Access Points > Radios > 802.11a/n/ac**, click the blue arrow adjacent the desired access point and choose **Detail** to navigate to the Details page.

This page primarily lists the read-only attributes of the selected Cisco Radio.

AP Details

Note The Monitor Mode parameter is not displayed for ODM access points.

Table 5-40 AP Details Parameters

Parameters	Description
Interface Type	Cisco Radio type 802.11a/n/ac.
AP Name	Name assigned to the access point.
AP ID	Identification number assigned when the access point is configured.
Admin Status	Interface status either enabled or disabled.
Operational Status	Cisco Radio operational status. The value is UP or DOWN.
11n Supported	Support of 11n. The value is Yes or No.
11ac Supported	Support of 802.11ac. The value is Yes or No.
Monitor Mode	Access point monitor mode: Local (normal operation), Cisco 1030 remote edge lightweight access point (Cisco 1030 IEEE 802.11a/b/g remote edge lightweight access point), or Monitor (monitor-only mode).
Location	User-definable location.

Station Configuration Parameters

The following parameters are not displayed for Cisco OEAP 600 Series access points:

- CFP Period
- CFP Max Duration

Table 5-41 Station Configuration Parameters

Parameters	Description
Configuration Type	Configuration type of Automatic or Custom.
Number of WLANs	Number of WLANs. 1 (one) is the default.
Medium Occupancy Limit	Maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	Maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
BSSID	MAC address of the access point.
Beacon Period	Rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds.
Country String	Country in which the station is operating. The first two octets of this string are the two-character country code.

Operation Rate Set

Table 5-42 Operation Rate Set Parameters

Parameter	Range
6000 Kilo Bits	Mandatory, Supported, or Disabled.
9000 Kilo Bits	Mandatory, Supported, or Disabled.
12000 Kilo Bits	Mandatory, Supported, or Disabled.
18000 Kilo Bits	Mandatory, Supported, or Disabled.
24000 Kilo Bits	Mandatory, Supported, or Disabled.
36000 Kilo Bits	Mandatory, Supported, or Disabled.
48000 Kilo Bits	Mandatory, Supported, or Disabled.
54000 Kilo Bits	Mandatory, Supported, or Disabled.

Note The data rates set here are negotiated between the client and the Cisco WLC. If the data rate is set to Mandatory, the client must support it in order to use the network.

If a data rate is set as supported by the Cisco WLC, any associated client that also supports that same rate may communicate with the access point using that rate. It is not required that a client be able to use all the rates marked Supported in order to associate. Each data rate can also be set to Disabled to match client settings.

MAC Operation Parameters

Table 5-43 MAC Operation Parameters

Parameter	Description
Configuration Type	Configuration type. Valid values are automatic or custom.
RTS Threshold	Attribute that indicates the number of octets in an MPDU, below which an RTS/CTS handshake is be performed. An RTS/CTS handshake shall be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size turns off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value is 2347.
Short Retry Limit	Maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that is be made before a failure condition is indicated. The default value is 7.
Long Retry Limit	Maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value is 4.

Table 5-43 MAC Operation Parameters

Parameter	Description
Fragmentation Threshold	Current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU is broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU is fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute is the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute is never less than 256.
Max. Tx MSDU Lifetime	Elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU is terminated. The default value is 512.
Max. Rx Life Time	Elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU. Further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.

Tx Power

The following parameters are not displayed for Cisco OEAP 600 Series access points:

- Supported Power Levels
- Tx Power Configuration
- Current Tx Power Configuration Level

Table 5-44 Tx Power Parameters

Parameter	Description
# Supported Power Levels	Eight or fewer power levels, depending on operator preference.
Tx Power Level 1	Maximum power level that exists across all of the data rates (AP1505 or AP1510 only).
Tx Power Level 2	Tx Power Level 1 minus 3 dBm (AP1505 or AP1510 only).
Tx Power Configuration	Globally controlled or customized for this access point.
Current Tx Power Level	Operating transmit power level from the transmit power table.

Physical Channel Parameters

The following parameters are not displayed for the ODM access point:

- Configuration
- Current CCA Mode
- ED/TI Threshold

Table 5-45 Physical Channel Parameters

Parameter	Description
Current Channel	Current operating frequency channel.
Configuration	Locally customized or globally controlled.
Current CCA Mode	CCA method in operation. Valid values are as follows: • Energy detect only (edonly) = 01 • Carrier sense only (csonly) = 02 • Carrier sense and energy detect (edandcs) = 04 • Carrier sense with timer (cswithtimer) = 08 • High rate carrier sense and energy detect (hrcsanded) = 16
ED/TI Threshold	Energy Detect and Threshold that is used to detect a busy medium (frequency). CCA reports a busy medium upon detecting the RSSI above this threshold.

RF Recommendation Parameters

Table 5-46 RF Recommendation Parameters

Parameter	Description
Channel	802.11a/n Low Band, Medium Band, and High Band. 802.11b/g/n.
Tx Power Level	0 if Radio Resource Management (RRM) is disabled. 1 - 5 if Radio Resource Management (RRM) is enabled.
RTS/CTS Threshold	0 if Radio Resource Management (RRM) is disabled, 1 - 5 if Radio Resource Management (RRM) is enabled. Refer to RTS Threshold in MAC Operation Parameters above.
Fragmentation Threshold	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.
Antenna Pattern	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.
Enhanced Local Mode (ELM) Parameters	
Promiscuous Mode Dwelling	Percentage of time that the access point spent in promiscuous mode. From Release 7.4 and later releases, the ELM can be in promiscuous mode for data frames too. This field appears only if the access point is in ELM mode.

802.11b/g/n Radios

Choose **WIRELESS > Access Points > Radios > 802.11b/g/n** or **MONITOR > Summary** and click **Detail** in the **802.11b/g/n Radios** row under the Access Point Summary section to navigate to the 802.11b/g/n Radios page.

This page displays an overview of your 802.11b/802.11g Cisco Radio network. The status of each 802.11b/g Cisco Radio configured on this Cisco WLC and its profile is detailed in the following table.

- To configure the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Configure** (Configuring 802.11b/g/n Radios).
- To view details about the identified Cisco Radio, click the blue arrow adjacent the desired radio and choose **Details** (802.11b/g/n AP Interfaces Details).

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC addresses or AP names. The current filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address text box.
- AP Name—Access point name text box.
- CleanAir Oper Status—Operational status of the CleanAir capable access point**.**

Note When you enable filtering by the MAC address, the other filters are disabled. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

802.11b/g/n Radio Summary

Table 5-47 802.11 b/g/n Radio Summary Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Radio Slot#	Slot where the radio is installed.
Base Radio MAC	Media Access Control address of the 802.11b/g/n radio.
Admin Status	Interface status of the access point on this radio. The values are enabled or disabled.
Operational Status	Cisco Radio operational status. The values are UP or DOWN.
Channel	Channel number of the access point. **Note** The channels 1, 6, and 11 are nonoverlapping.
CleanAir Admin Status	Administration status of the spectrum sensor for the access point.

Table 5-47 802.11 b/g/n Radio Summary Parameters

Parameter	Description
CleanAir Oper Status	Status of the spectrum sensor for this access point. The CleanAir status is one of the following: • UP—The spectrum sensor for the access point radio is currently operational (error code 0). • DOWN—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio. • ERROR—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable CleanAir functionality on the radio. • N/A—This access point radio cannot support CleanAir functionality. Currently, only Cisco Aironet 3500 series access point radios can be configured for Cisco CleanAir. **Note** You can create a filter to make the 802.11a/n Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP page, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).
Power Level	Transmit power level of the access point where • 1 = Maximum power allowed per Country Code setting • 2 = 50% power • 3 = 25% power • 4 = 6.25 to 12.5% power • 5 = 0.195 to 6.25% power. **Note** The power levels and available channels are defined by the Country Code setting and are regulated on a country by country basis.
Antenna	Internal or external antennas.

Configuring 802.11b/g/n Radios

Choose **WIRELESS > Access Points > Radios > 802.11b/g/n**, and then click the blue arrow adjacent the desired access point and choose **Configure** to navigate to the Configure page.

This page enables you to configure parameters specifically for this Cisco Radio including antenna type, RF channel, and Tx power level assignments. The performance profile for this Cisco Radio is also accessed through this page.

General

Table 5-48 General Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Admin Status	Administration interface status. The default is enabled.
Operational Status	Cisco Radio operational status.
Slot #	Slot where this radio is installed.

11n Parameters

This table describes the 802.11n parameters.

Table 5-49 11n Parameters

Parameter	Description
11n Supported	Indicates whether 11n is supported or not.

CleanAir

Note Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

Table 5-50 CleanAir Parameters

Parameter	Description
CleanAir Capable	Indicates whether the access point is CleanAir capable.
CleanAir Admin Status	Administration status of the spectrum sensor for the access point that you can enable or disable. Set this field to Enable or Disable from the drop-down list.

Antenna Parameters

Table 5-51 Antenna Parameters

Parameter	Description
Antenna Type	Internal or External.
Antenna (Displayed if 11n is supported)	Internal or external antennae: • A—Right antenna port • B—Left antenna port • C—Center antenna port For example, to enable transmissions from antennae ports A and B and receptions from antenna port C, you should select the following check boxes: Tx: A and B and Rx: C.

Table 5-51 Antenna Parameters

Parameter	Description
Diversity (Displayed if 11n is not supported)	Select one of the following: For internal antennas: • Enable—Enables diversity on both Side A and Side B. • Side A—Enables diversity for the front (door) antenna. • Side B—Enable diversity for the rear antenna. For external antennas: • Enable—Enables diversity on both the connectors. • Right—Enables diversity for the Right (Connector B) antenna. • Left—Enables diversity for the Left (Connector A) antenna.
Antenna Gain	Actual—Cannot be set.

Sniffer Channel Assignment

Note This area is displayed if you set the AP Mode on the General Tab to Sniffer.

Table 5-52 Sniffer Channel Assignment Parameters

Parameter	Description
Sniff	Sniffer operation that you can enable or disable. When enabled, the access point begins capturing and forwarding all the packets from the client on a specific channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). The default value is disabled (or unselected).
Channel	Channel on which the access points sniffs for packets. The default value is 1.
Server IP Address	IP address of the remote machine running Airopeek or Wireshark.

RF Channel Assignment

Table 5-53 RF Channel Assignment Parameters

Parameter	Description
Current Channel	Channel number of the access point. **Note** The channels 1, 6, and 11 are nonoverlapping.
Channel Width	RF channel Assignment Method and TX power level Assignment Method that you set to Custom, and choose the channel width. • 20 MHz—Enables the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.

Table 5-53 RF Channel Assignment Parameters

Parameter	Description
Assignment Method	Assignment method that you can choose: • Global—Use this setting if your access point's channel is set globally by the Cisco WLC. • Custom—Use this setting if you set the channel locally.
Note The assignment method should normally be left at the global setting to enable the Cisco WLC to dynamically change the channel number based Radio Resource Management (RRM) directives.	

Tx Power Level Assignment

Table 5-54 Tx Power Level Assignment Parameters

Parameter	Description
Current Tx Power Level	Transmit power level of the access point. Tx Power Level indicates the maximum power. **Note** The power levels and available channels are defined by the Country Code setting and are regulated on a country by country basis.
Assignment Method	Assignment method that you can choose: • Global—Use this setting if your access point's transmit power is set globally by the Cisco WLC. • Custom—Use this setting if your access point's transmit power is set locally. Choose an option from the drop-down list.
Note The assignment method should be left at the global setting to enable the Cisco WLC to dynamically change the transmit power level based on the Radio Resource Management (RRM).	

Configuring Tx Power Levels

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the product guide or data sheet at http://www.cisco.comfor each specific model in order to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example, 2, 3, 4, and so on) represents approximately a 50-percent (or 3 dBm) reduction in the transmit power from the previous power level.

Note The actual power reduction may vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Note Whether you choose the **Global** or **Custom** assignment method, the actual conducted transmit power at the access point is verified so that country specific regulations are not exceeded.

Performance Profile

See the Performance Profile of 802.11a/n/ac Access Points page.

Tracking Optimization

Note If your access point is configured to operate in Monitor mode, you can enable tracking optimization on up to four channels within the 2.4 GHz band (802.11b/g radio) of an access point to enable you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6 and 11).

Table 5-55 Tracking Optimization Parameters

Parameter	Description
Enable Tracking Optimization	Tracking optimization.
Channel 1 Channel 2 Channel 3 Channel 4	Channels on which you want to monitor tags. **Note** To eliminate a channel from monitoring tags, choose **None** from the channel drop-down list.

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.

802.11b/g/n AP Interfaces Details

Choose **WIRELESS > Access Points > Radios > 802.11b/g/n** and then click **Detail** to navigate to the Details page.

This page lists primarily read-only attributes of the selected Cisco Radio.

AP Details

Table 5-56 AP Details Parameters

Parameters	Description
Interface Type	Cisco Radio type as 802.11b/g/n.
AP Name	Name assigned to the access point.
AP ID	Identification number assigned when the access point is configured.
Admin Status	Interface status that you can enable or disable.
Operational Status	Cisco Radio operational status.
11n Supported	Support of 11n.

Table 5-56 AP Details Parameters

Parameters	Description
Monitor Mode	Access point Monitor mode: Local (normal operation), Cisco 1030 remote edge lightweight access point (Cisco 1030 IEEE 802.11a/b/g remote edge lightweight access point), or Monitor (monitor-only mode).
Location	User-definable location.

Station Configuration Parameters

Table 5-57 Station Configuration Parameters

Parameters	Description
Configuration Type	Configuration type of automatic or custom.
Number of WLANs	Number of WLANs. 1 (one) is the default.
Medium Occupancy Limit	Maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	Number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	Maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
BSSID	MAC address of the access point.
Beacon Period	Rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds.
Country String	Country in which the station is operating. The first two octets of this string are the two-character country code.

Operation Rate Set

Table 5-58 Operation Rate Set Parameters

Parameter	Band	Range
1000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
2000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
5500 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
11000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported, or Disabled.
6000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
9000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
12000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
18000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
24000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
36000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.

Table 5-58 Operation Rate Set Parameters

Parameter	Band	Range
48000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.
54000 Kilo Bits	802.11b or 802.11g.	Supported or Disabled.

The data rates set are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it in order to use the network.

If a data rate is set as Supported by the controller, any associated client that also supports that same rate may communicate with the Cisco Aironet 1000 Series IEEE 802.11a/b/g lightweight access point using that rate. It is not required that a client be able to use all the rates marked Supported in order to associate. Each data rate can also be set to Disabled to match Client settings.

MAC Operation Parameters

Table 5-59 MAC Operation Parameters

Parameter	Description
Configuration Type	Configuration type of automatic or custom.
RTS Threshold	Attribute that indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size turns off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default is 2347.
Short Retry Limit	Maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that is made before a failure condition is indicated. The default is 7.
Long Retry Limit	Maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that is made before a failure condition is indicated. The default is 4.
Fragmentation Threshold	Current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU is broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU is fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute is the lesser of 2346 or the aMPDUMaxLength of the attached PHY and will never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute is never be less than 256.

Table 5-59 MAC Operation Parameters

Parameter	Description
Max. Tx MSDU Lifetime	Elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU is terminated. The default value is 512.
Max Rx Life Time	Elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU. Further attempts to reassemble the MMPDU or MSDU are terminated. The default is 512.

Table 5-60 Tx Power Parameters

Parameter	Description
# Supported Power Levels	Eight or fewer power levels, depending on operator preference.
Tx Power Configuration	Globally controlled or Customized for this access point.
Current Tx Power Level	Operating transmit power level from the transmit power table.

Physical Channel Parameters

Table 5-61 Physical Channel Parameters

Parameter	Description
Current Channel	Current operating frequency channel.
Configuration	Locally customized or globally controlled.
Current CCA Mode	CCA method in operation. Valid values are as follows: • Energy detect only (edonly) = 01 • Carrier sense only (csonly) = 02 • Carrier sense and energy detect (edandcs) = 04 • Carrier sense with timer (cswithtimer) = 08 High rate carrier sense and energy detect (hrcsanded) =16.
ED/TI Threshold	Energy Detect and Threshold that is used to detect a busy medium (frequency). CCA reports a busy medium upon detecting the RSSI above this threshold.

RF Recommendation Parameters

Table 5-62 RF Recommendation Parameters

Parameter	Description
Channel	802.11a/n Low Band, Medium Band, and High Band. 802.11b/g/n
Tx Power Level	0 if Radio Resource Management (RRM) is disabled. 1- 5 if Radio Resource Management (RRM)is enabled.

Table 5-62 RF Recommendation Parameters

Parameter	Description
RTS/CTS Threshold	0 if Radio Resource Management (RRM) is disabled. 1 - 5 if Radio Resource Management (RRM) is enabled. See Threshold in MAC Operation Parameters above.
Fragmentation Threshold	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.
Antenna Pattern	0 if Radio Resource Management (RRM) is disabled, or as Radio Resource Management (RRM) recommends.

Enhanced Local Mode (ELM) Parameters

Table 5-63 ELM Parameters

Parameter	Description
Promiscuous Mode Dwelling	Percentage of time that the access point spent in promiscuous mode. Beginning in controller Release 7.4 and later, the ELM can be in promiscuous mode for data frames too. This field appears only if the access point is in the Local mode or the Flexconnect mode, and the submode is WIPS.

CleanAir Parameters

The CleanAir operational status is displayed by the **Operational Status** parameter.

Persistent Devices

Note Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

Table 5-64 Persistent Device Parameters

Parameter	Description
Class Type	Class type of the persistent device.
Channel	Channel that the device is affecting.
DC (%)	Duty cycle (in percentage) of the persistent device.
RSSI(dBm)	Received Strength Signal Indicator of the persistent device.
Last Seen Time	Timestamp when the device was last active.

Dual-Band Radios

Choose **WIRELESS > Access Points > Radios > Dual-Band Radios** or **MONITOR > Summary** and click **Detail** in the **Dual-Band Radios** row under the Access Point Summary section to navigate to this page.

This page displays an overview of your 802.11a/b/g Cisco Radio network. The status of each 802.11a/b/g Cisco Radio configured on this Cisco WLC and its profile is detailed in the following table.

- To configure the identified Cisco Radio, click the blue arrow adjacent the desired access point and choose **Configure** (Configuring Dual-Band Radios).
- To view details about the identified Cisco Radio, click the blue arrow adjacent the desired access point and choose **Details** (Dual-Band Radios Details).

Search AP Filter

Click **Change Filter** to display the Search APs dialog box (see the following figure) and create or change filter parameters. Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of access points by MAC addresses or AP names. The current filter parameters are displayed in the Current Filter field.

- MAC Address—MAC address text box.
- AP Name—Access point name text box.
- CleanAir Oper Status—Operational status of the CleanAir capable access point**.**

Note When you enable filtering by the MAC address, the other filters are disabled. However, you can use a combination of the AP Name and CleanAir Oper Status to filter access points.

Click **Find** to commit your changes. Only the access points that match your search criteria appear on the Dual-Band Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Dual-Band Radios Summary

Table 5-65 Dual-Band Radios Summary Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Radio Slot#	Slot where the radio is installed.
Module Type	The AP module type.
Base Radio MAC	Media Access Control address of the 802.11b/g/n radio.
Admin Status	Interface status of the access point on this radio. The values are enabled or disabled.
Operational Status	Cisco Radio operational status. The values are UP or DOWN.
CleanAir Admin Status	Administration status of the spectrum sensor for the access point.

Table 5-65 Dual-Band Radios Summary Parameters

Parameter	Description
CleanAir Oper Status	Status of the spectrum sensor for this access point. The CleanAir status is one of the following: • UP—The spectrum sensor for the access point radio is currently operational (error code 0). • DOWN—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio. • ERROR—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable CleanAir functionality on the radio. • N/A—This access point radio cannot support CleanAir functionality. Currently, only Cisco Aironet 3500 series access point radios can be configured for Cisco CleanAir. **Note** You can create a filter to make the Dual-Band Radios page show only access point radios that have a specific CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP page, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the Dual-Band Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).
Radio Role	Information about the radio's role
Power Level	Power Level information
Antenna	Internal or external antennas. For Hyperlocation modules—Circular or linear.

Configuring Dual-Band Radios

Choose **WIRELESS > Access Points > Radios > Dual-Band Radios**, and click the blue arrow adjacent the desired access point and choose **Configure** to navigate to the Configure page.

This page enables you to configure parameters specifically for this Cisco Radio including antenna type, RF channel, and Tx power level assignments. The performance profile for this Cisco Radio is also accessed through this page.

General

Table 5-66 General Parameters

Parameter	Description
AP Name	User-definable name of the access point.
Admin Status	Administration interface status. The default is enabled.
Operational Status	Cisco Radio operational status.
Slot #	Slot where this radio is installed.

11n and 11ac Parameters

Table 5-67 11n and 11ac Parameters

Parameter	Description
11n Supported	Whether 11n is supported or not.
11ac Supported	Whether 11ac is supported or not.

CleanAir

Note Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

Table 5-68 CleanAir Parameters

Parameter	Description
CleanAir Capable	Whether the access point is CleanAir capable.
CleanAir Admin Status	CleanAir Administration status of the spectrum sensor for the access point that you can enable or disable. You can set this field to the following options: • Enable—Enables CleanAir for both 2.4-GHz and 5-GHz radios. • Disable—Disables CleanAir for both 2.4-GHz and 5-GHz radios. • 2.4-GHz—Enables CleanAir only for 2.4-GHz radio. • 5-GHz—Enables CleanAir only for 5-GHz radio.

Dual-Band Radios Details

Choose **WIRELESS > Access Points > Radios > Dual-Band Radios** and then click **Detail** to navigate to the Dual-Band Radios page.

This page lists primarily read-only attributes of the selected Cisco Radio.

AP Details

Table 5-69 AP Details Parameters

Parameters	Description
Interface Type	Cisco Radio type as 802.11a/b/g/n.
AP Name	Name assigned to the access point.
AP ID	Identification number assigned when the access point is configured.
Admin Status	Interface status that you can enable or disable.
Operational Status	Cisco Radio operational status.
11n Supported	Support of 11n.
Monitor Mode	Access point Monitor mode: Local (normal operation), Cisco 1030 remote edge lightweight access point (Cisco 1030 IEEE 802.11a/b/g remote edge lightweight access point), or Monitor (monitor-only mode).
Location	User-definable location.

CleanAir Parameters

The CleanAir operational status is displayed by the **Operational Status** parameter.

Global Configuration

Choose **WIRELESS > Access Points > Global Configuration** to navigate to the Global Configuration page. This page enables you to configure the following parameters:

General

LED State—Check box and drop-down list to enable or disable the LED state of the access points. When you have many APs deployed and want to locate a specific AP, you can disable the LED state of all APs and then enable the LED state of the AP you are looking for. Thus, the AP that has its LED state enabled is easily identifiable.

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is used between the network devices to discover properties of the other end of an interface and the device. When CDP is enabled on an interface, the device sends its properties and interface information to the device at the other end of the interface. The controller has an option to enable or disable CDP on all or a specific access point. This configuration is applied to the global CDP state on the access point.

Note CDP over radio interface is applicable only for mesh APs.

Table 5-70 CDP Parameters

Parameter	Description
CDP State	Global CDP that you can enable or disable on Ethernet or radio interfaces for all the access points currently associated to the controller.
Ethernet Interface#	Ethernet interface number.

Table 5-70 CDP Parameters

Parameter	Description
CDP State (Ethernet interface)	CDP that you can enable or disable for all or specific Ethernet interfaces on all or specific access points. **Note** Global CDP for the particular access points should be enabled before enabling or disabling the CDP state.
Radio Slot#	Slot where the radio is installed.
CDP State (radio slot)	CDP that you can enable or disable for all or specific radio interfaces on all or specific access points.

Login Credentials

Cisco IOS access points are shipped from the factory with "Cisco" as the default enable password. This password allows users to log in to the unprivileged mode and execute **show** and **debug** commands, which poses a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the access point's console port.

Note You must keep careful track of the credentials used by the access points. Otherwise, you might not be able to log in to an access point's console port. If you need to return the access points to the default *Cisco*/*Cisco* username and password, you must clear the controller's configuration and the access point's configuration to return them to the default settings. To clear the controller's configuration, choose **Commands** > **Reset to Factory Default** > **Reset** on the controller GUI, or enter the **clear config** command on the controller CLI. To clear the access point's configuration, enter the **clear ap config command** *Cisco_AP* on the controller CLI. After the access point rejoins a controller, it adopts the default *Cisco*/*Cisco* username and password.

You can set a global username, password, and enable password that all access points inherit as they join the controller including access points that are currently joined to the controller and any that join in the future. You can override the global credentials and assign a unique username, password, and enable password for a specific access point. The following are requirements enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain the management username or the reverse of the username.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o, or substituting $ for s.

Table 5-71 Login Credentials Parameters

Parameter	Description
Username	Username that is to be inherited by all access points that join the controller.
Password	Password that is to be inherited by all access points that join the controller.
Enable Password	Enable password that is to be inherited by all access points that join the controller.

Note You can override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point by selecting the **Over-ride Global credentials** check box on the Credentials tab on the All APs Details page.

802.1X Supplicant Credentials

You can configure 8021.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning.

You can set global authentication settings that all access points inherit as they join the controller, which includes all access points that are currently joined to the controller and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

Table 5-72 802.1X Supplicant Credentials Parameters

Parameter	Description
802.1X Authentication	Username, Password, and Confirm Password fields.
Username	Username that is to be inherited by all access points that join the controller.
Password	Password that is to be inherited by all access points that join the controller.
Confirm Password	Confirmed password that is to be inherited by all access points that join the controller.

Note You can override the global authentication settings for a specific access point and assign a unique username and password to this access point by selecting the **Over-ride Global credentials** check box on the Credentials tab on the All APs Details page.

AP Failover Priority

You can configure high-priority access points so that the backup controller recognizes and accepts those access points first, even if it means disassociating a lower-ranked device as a means to provide an available port.

- Global AP Failover Priority—Access point priority assignments.

You can assign priorities to the access points on the High Availability tab on the All APs Details page. By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

AP Image Predownload

You can predownload images for all access points that are associated to your controller on the network.

This table describes the AP image predownload parameters.

Table 5-73 AP Image Predownload Parameters

Parameter	Description
Download Primary	Instruct all access points to download a primary image from the controller.
Download Backup	Instruct all access points to download an image from the controller and store it as a backup.
Interchange Image	Instruct all access points to swap their primary and backup images.
Abort Predownload	Abort the AP Image Predownload process.

High Availability

You can configure primary and secondary backup controllers for all access points (which are used if primary, secondary, or tertiary controllers are not responsive) in this order: primary, secondary, tertiary, primary backup, and secondary backup. In addition, you can configure various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.

Note You can configure the fast heartbeat timer only for access points in local and FlexConnect modes.

- AP Heartbeat Timeout—AP Heartbeat timeout value that you can enter. The valid range is 10 to 30 for the Cisco 7500 Series Controller and 1 to 30 for other platforms.
- Local Mode AP Fast Heartbeat Timer State—Fast heartbeat timer that you can enable or disable for access points in local mode. The default is disable.
- Local Mode AP Fast Heartbeat Timeout—If you enabled Local Mode AP Fast Heartbeat Timer, enter the timeout interval for this parameter. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure. The range for the AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.
- FlexConnect Mode AP Fast Heartbeat Timer State—Fast heartbeat timer for FlexConnect access points that you can enable or disable. The default is disable.
- FlexConnect Mode AP Fast Heartbeat Timeout—If you enabled the FlexConnect mode AP fast heartbeat timer, enter the interval (in seconds) for the fast heartbeat timer for FlexConnect access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure. The range for the FlexConnect Mode AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.
- AP Primary Discovery Timeout—Timeout that you can set. Enter a number between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.
- Back-up Primary Controller IP Address—IPv4/IPv6 address of the primary backup controller. From Release 8.0, controller supports IPv6.

Note The default for the IP address is 0.0.0.0, which disables the primary backup controller.

- Back-up Primary Controller Name—Name of the primary backup controller.
- Back-up Secondary Controller IP Address—IP4/IPv6 address of the secondary backup controller. From Release 8.0, controller supports IPv6.

Note The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

- Back-up Secondary Controller Name—Name of the secondary backup controller.

TCP MSS

If the client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem in controller software release 6.0 or later releases, you can specify the MSS for all access points that are joined to the controller or for a specific access point.

When you enable this feature, the access point selects the MSS for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

- Global TCP Adjust MSS—Enable the check box and set the MSS for all access points that are associated with the controller.

  From Release 8.0, the controller supports IPv6. Use the following Global TCP Adjust MSS values for:

  – IPv4—Specify a value between 536 and 1363.
  – IPv6—Specify a value between 1220 and 1331.

Note Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.

AP Retransmit Config Parameters

When a controller goes out of service, the access point associated with it falls back to the next available controller. Before associating itself to a new controller, the access point first tries to establish a connection with the existing controller that it is associated with. It does so by sending a request (known as a retransmission) at regular intervals to the controller and for a specified number of times (retry count). If the access point does not get an acknowledgement from the controller, it tries to associate itself to the next available controller.

Note Retransmission intervals and retry counts are not applicable for mesh access points.

You can configure the retransmission intervals and retry counts both at a global as well as a specific access point level. A global configuration applies these configuration parameters to all the access points. That is, the retransmission interval and the retry count would be uniform for all access points.

Alternatively, when you configure the retransmission level and retry counts at a specific access point level, the values are applied to that particular access point. Access point specific configurations have higher precedence compared to Cisco WLC global configurations.

This table describes the AP retransmit config parameters.

Table 5-74 AP Retransmit Config Parameters

Parameter	Description
AP Retransmit Count	Number of times that you want the access point to retransmit the request to controller and vice-versa. Valid range is between 3 and 8.
AP Retransmit Interval	Time duration between retransmission of requests. Valid range is between 2 and 5.

OEAP Config Parameters

Table 5-75 OEAP Config Parameters

Parameter	Description
Disable Local Access	Check box that you can select to disable access to the local GUI, LAN ports, and local SSID of the Cisco OEAP.
Disable Split Tunnel	Check box that you can select to disable split tunneling for Cisco OEAP. Selecting the check box disables splitting the tunnel for all WLANs and remote LANs.

FlexConnect Ethernet Fallback

Table 5-76 FlexConnect Ethernet Fallback Parameters

Parameter	Description
Radio Interface Shutdown	Check box that you can select to enable an AP radio interface or disable an AP radio interface. This is disabled by default. When the user selects this checkbox and when AP Ethernet Link goes down, the AP radio interface shuts down.
Delay (0 to 10 Sec)	Delay value, in seconds. The value range is between 0 and 10. The default is 0.

Global Telnet SSH

This table describes the Global Telnet SSH parameter.

h

Table 5-77 Global Telnet SSH Parameters

Parameter	Description
Telnet	Telnet or SSH connectivity on this access point. The default is unselected.
SSH	These protocols make debugging the access point easier, especially when the access point is unable to connect to the controller.

Global IPv6 UDP Lite

This table describes the global IPv6 UDP Lite parameters used to enable or disable an IPv6 CAPWAP UDPLite for CAPWAP AP on the Cisco Wireless LAN Controller.

h

Table 5-78 Global IPv6 UDP Lite Parameters

Parameter	Description
UDP Lite	Check this check box to globally enable IPv6 UDP Lite on APs connecting to the controller using CAPWAP v6 tunnel. **Note** IPv6 UDP Lite is not applicable to APs connected with CAPWAP v4 tunnel.

Hyperlocation Config Parameters

Table 5-79 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 (dBm)	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. **Note** IPv6 address is not supported.

BLE Beacon Config Parameters

Table 5-80 BLE Beacon Config Parameters

Parameter	Description
Interval (1 - 10) Hz	Configures BLE transmission interval
Beacon ID	Five options are available: Beacon1 to Beacon5.
Delete Beacon	Deletes selected beacon.

Table 5-80 BLE Beacon Config Parameters

Parameter	Description
Beacon Status	Enables or disables selected beacon.
UUID	Configures selected beacon's UUID.
TxPower (–52 to 0) dBm	Configures selected beacon's transmission power.

TrustSec Config

Table 5-81 TrustSec Config Parameters

Parameter	Description
Sgacl Enforcement	By default, this check box is enabled, if the global Cisco TrustSec is enabled.
Inline Tagging	Select this check box to enable inline tagging. **Note** You can configure Inline Tagging only if the global Cisco TrustSec is enabled.

Note SGACL Enforcement and Inline Tagging are supported only on Cisco 5520 or 8540 Wireless Controllers. For other Cisco WLCs, these two fields are hidden.

Advanced

This section contains the following topics:

- RF Management, page 5-70
- QoS, page 5-76

RF Management

This section contains the following topics:

- Flexible Radio Assignment, page 5-71
- Load Balancing, page 5-71
- Band Select, page 5-73
- Rx SOP Threshold, page 5-75
- Optimized Roaming, page 5-75
- Network Profile, page 5-76

Flexible Radio Assignment

Use Cisco's Flexible Radio Assignment (FRA) Architecture feature to take advantage of the Cisco Aironet 2800 and 3800 Series AP hardware. FRA is a new core algorithm added to RRM to analyze the NDP measurements and manage the hardware used to determine the role the new Flexible Radio (2.4 GHz, 5 GHz, or Monitor) will play in your network. For more information, see the *Radio Resource Management White Paper*.

Choose **Wireless > Advanced > RF Management > Flexible Radio Assignment** to navigate to the **Flexible Radio Assignment Configuration** page.

The FRA feature is disabled by default. When you enable the feature, you can configure the parameters shown in this table:

Table 5-82 Flexible Radio Assignment Parameters

Parameter	Description
Sensitivity	Adjust the FRA Sensitivity Threshold. This sets the percentage of COF required to consider a radio as redundant. Supported values are: • Low (100%-default) • Medium (95%) • High (90%)
Interval	Set the FRA run interval. Valid range is 1 hour to 24 hours. Default setting is 1 hour. FRA heavily depends on DCA and the FRA interval cannot be lesser than the DCA interval.

Load Balancing

Choose **Wireless > Advanced > RF Management > Load Balancing** to navigate to the Load Balancing page. This page enables you to configure load balancing on the wireless network.

Important Guidelines and Limitations

- Load balancing is configurable only on a per-WLAN basis.
- Load balancing is not supported on the Cisco OEAP 600 Series access point.

This table describes the load balancing parameters.

Table 5-83 Load Balancing Parameters

Parameter	Description
Client Window Size	Threshold that you can set for the client window size. This parameter specifies the threshold for the difference between the number of clients that an access point can have and the client count of the access point that has a minimum number of associated clients. For example, suppose in a network setup there are three access points connected to a controller (AP1, AP2, and AP3). AP1 has 2 clients, AP2 has 3 and AP3 has 4 clients. In this setup, AP1 has a minimum number of clients, that is, 2. If the window size is configured as 2, every AP can have 2 + 2 = 4 clients. So every 5th client is load balanced. If any client tries to join AP3, a denial response is sent from AP3. For a client, the denial message is sent based on the configured value for the maximum denial count. The default is 5.
Maximum Denial Count	Maximum denial count that you can configure. The maximum denial count specifies the maximum number of association rejections that the access point can send to a client for a given sequence of association. When a client tries to associate on a wireless network, it sends an association request to the access point. If the access point is overloaded and load balancing is enabled on the controller, the access point sends a denial to the association request. If there are no other access points in the range of the client, the client tries to associate the same access point again. After the maximum denial count is reached, the client is able to associate. Association attempts on an access point from any client before associating any AP is called a sequence of association. The default is 3.
Load Balancing Statistics	
Total Denial Client Count	Total number of clients denied.
Total Denial Messages Sent	Total number of denial messages sent.
Exceeded Denial Max Limit Count	Total number of messages that exceeded the denial maximum limit count.

Table 5-83 Load Balancing Parameters

Parameter	Description
None 5G Candidate Count	Number of times at the 5G band that there is no AP candidate to load balance off a client.
None 2.4 G Candidate Count	Number of times at the 2.4G band that there is no AP candidate to load balance off a client.

Band Select

Choose **Wireless > Advanced > RF Management > Band Select** to navigate to the Band Select page. This page enables you to configure the band select parameters on the wireless network.

Note Band select is not supported on the Cisco OEAP 600 Series access point.

Table 5-84 Band Select Parameters

Parameter	Description
Probe Cycle Count	Probe cycle count that you can specify. When a client cycle count is reached and if a client still sends a probe request, the access point responds to it with a probe response. For example, we assume at a minimum that a client stays in a channel for 5 milliseconds and there are 11 channels. If the client scans channel 1 and then the other 10 channels, there should be at least a gap of 10x5 milliseconds between the last time the AP hears the client probe and the latest one. The AP only increments the count if the difference of time between the latest and the last probe is more than 50 milliseconds. The default is 2.
Scan Cycle Period Threshold (milliseconds)	Threshold for a new scanning cycle period (in milliseconds) that you can specify. The Client cycle counter is incremented only if the client scans the same channel after any time the value is set for the scan cycle period threshold. For example, if a client is scanning a channel after every 150 milliseconds and a cycle threshold value is configured as 200, the cycle count is incremented after 300 seconds. If the client is scanning after every 250 milliseconds, the cycle count is incremented after 250 milliseconds. The default is 200.

Table 5-84 Band Select Parameters (continued)

Parameter	Description
Age Out Suppression (seconds)	Ageout suppression (in seconds) that you can configure. This parameter specifies the ageout period after which the entry of the client is removed from the suppression table. All entries stay in the suppression table until they are aged out or are replaced when the table is full. If the table is full, and there is no space for a new client, then the access point replaces the oldest entry on the table that had responded already. If there is no empty slot in the table, the access point has to respond to all the new clients until space is available. The default is 20.
Age Out Dual Band (seconds)	Ageout dual band (in seconds) that you can specify. When an access point receives a probe request from any client in both 2.4-GHz and 5-GHz bands, the access point is aware that the client is capable of operating on both bands. Dual-band capable clients are recorded in a dual-band client table. The controller keeps a record of the clients' capabilities to join the 2.4-GHz and 5-GHz bands. The controller ensures that 5-GHz capable clients join the 5-GHz band only. Entries in the table are aged out to make space for new entries. This parameter specifies the time duration after which the client entry is removed. The access point does not respond to the dual band client's 2.4-GHz probe until it is removed from the dual-band client table. The access point fills the dual-band table in the following order until it is full: • Clients with a 5-GHz probe that have associated to 2.4-GHz. • Clients with a 5-GHz probe that also have 2.4-GHz probes. • Clients with just a 5-GHz probe detected and a 5-GHz association. The default is 60.

Table 5-84 Band Select Parameters (continued)

Parameter	Description
Acceptable Client RSSI (dBm)	Acceptable client RSSI (in dBm) that you can set. This parameter specifies the minimum client RSSI threshold. This parameter filters out far away clients with low signal strength to limit the number of clients on the table. The default is –80.
Acceptable Client Mid RSSI (dBm)	Enter a value between –20 dBm and –90 dBm. This parameter sets the mid-RSSI, whose value can be used for toggling 2.4 GHz probe suppression based on the RSSI value. The default value is –60 dBm.

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.

Rx SOP Threshold

Receiver Start of Packet Detection Threshold (Rx SOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. As the Wi-Fi level increases, the radio sensitivity decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network. Rx SOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points.

Choose **WIRELESS > Advanced > RF Management > Rx SOP Threshold** to navigate to the Rx SOP Threshold page. This page enables you to configure the Rx SOP threshold values for each 802.11 band.

This table shows the Rx SOP threshold values for high, medium and low levels for each 802.11 band.

802.11 Band	High Threshold	Medium Threshold	Low Threshold
5 GHz	-76 dBm	-78 dBm	-80 dBm
2.4 GHz	-79 dBm	-82 dBm	-85 dBm

Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection.

This feature disassociates clients based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. Optimized roaming also prevents client association when the client's RSSI is low. This feature checks the RSSI of the incoming client against the RSSI threshold. You can also configure the client coverage reporting interval for a radio.

Choose **WIRELESS > Advanced > RF Management > Optimized Roaming** to navigate to the Rx SOP Threshold page. This page enables you to enable optimized roaming on a radio and configure the parameters.

Table 5-85 Optimized Roaming Parameters

Parameter	Description
Optimized Roaming Mode	Check box that you can select to enable Optimized Roaming.
Optimized Roaming Interval	Client coverage reporting interval for 802.11a/b networks. The range is from 5 to 90 seconds. The default value is 90. **Note** You must disable the 802.11a/b network before you configure the optimized roaming interval.
Optimized Roaming Data Rate Threshold	Threshold data rate for 802.11a/b networks. For 802.11a, the configurable data rates are 6, 9,12,18, 24, 36, 48, and 54. For 802.11b, the configurable data rates are 1, 2, 5.5, 11, 6, 9,12,18, 24, 36, 48, and 54. You can also choose the Disable option to disable the data rate for disassociating clients.

Network Profile

Choose **WIRELESS > Advanced > RF Management > Network Profile** to navigate to the Network Profile page.

Table 5-86 Network Profile Parameters

Parameter	Description
RF Parameter Optimization	Check box that you can select to enable configuration of Client Density and Traffic Type.
Client Density	Options: • Low • Typical • High
Traffic Type	To configure RF parameters for RF traffic type such as: • Data • Data and Voice

QoS

This section contains the following topics:

• Preferred Calls, page 5-77
• SIP Snooping, page 5-77

- Fastlane, page 5-78

Preferred Calls

You can configure a controller to support calls from clients that do not support TSPEC-based calls. This is known as voice prioritization. These calls are given priority over other clients that use the voice pool. Voice prioritization is available only for SIP-based calls, not for TSPEC-based calls. If the bandwidth is available, the controller takes the normal flow and allocates the bandwidth to those calls.

You can configure up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the controller does not check on the maximum call limit. It invokes the CAC to allocate bandwidth for the preferred call. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

Prerequisites for Voice Prioritization

- WLAN QoS should be set to platinum.
- ACM should be enabled for the radio.
- WLAN should have SIP call snooping enabled.

Note The Cisco 5500 Series Controllers and all nonmesh access points do not support the voice prioritization.

Choose **Wireless > Advanced> QoS > Preferred Calls** to navigate to this page. This page enables you to configure voice prioritization parameters on the wireless network.

Click **Add Number** to add a preferred call number.

Table 5-87 Preferred Calls Parameters

Parameter	Description
Call Index	Index to assign to this call number.
Call Number	Call number.

The configured **Call Index** and **Call Numbers** are displayed.

Click **Apply** to add the index and the call number.

Click **Cancel** to return to the Preferred Calls page.

SIP Snooping

Choose **WIRELESS > Advanced > QoS > SIP Snooping** to navigate to the **SIP Snooping** page. This page enables you to configure call snooping ports on the controller. If you need only a single port for call snooping, configure the start and end port with the same number.

The port used by the CIUS tablet is 5060 and the port range used by Facetime is from 16384 to 16402.

This table describes the SIP snooping parameters.

Table 5-88 SIP Snooping Parameters

Parameter	Description
Port Start	Starting port for call snooping. The range is from 0 to 65535.
Port End	Ending port for call snooping. The range is from 0 to 65535.

Fastlane

Choose **WIRELESS > Advanced > QoS > Fastlane** to navigate to the **Fastlane Configuration** page.

Click **Apply** to revert the Fastlane AutoQoS global parameters to default values.

Mesh

Choose **WIRELESS > Mesh** to navigate to the Mesh page.

This page enables you to configure the access point to establish a connection with the controller.

General

Table 5-89 General Parameters

Parameter	Description
Range (Root AP to Mesh AP)	Optimum distance (in feet) that should exist between the root access point and the mesh access point. This global parameter applies to all access points when they join the controller and all existing access points in the network. Values are from 150 to 132000; the default is 12,000.
IDS (Rogue and Signature Detection)	Outdoor mesh access points that you can enable or disable. The default is disable. **Note** IDS reporting is enabled for all indoor mesh access points and cannot be disabled. When you enable this feature, IDS reports are generated for all traffic on the backhaul. These reports can be useful for university or enterprise outdoor campus areas, or for public safety users who want to find out who is operating in 4.9 GHz. When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul.
Backhaul Client Access	Backhaul client access that you can enable or disable. The default status is disabled state. When you enable this feature, both backhaul traffic and client traffic can carry over the same mesh backhaul radio. **Note** After you enable this feature, all mesh access points reboot.

Table 5-89 General Parameters

Parameter	Description
Mesh DCA Channels	Mesh DCA channel that you can enable or disable. The default is disable. Enable this option to enable backhaul channel deselection on the controller using the DCA channel list. Any change to the channels in the controller DCA list is pushed to the associated access points. This option is only applicable for Serial Backhaul mesh access points.
Global Public Safety	Public safety band that you can enable or disable on the mesh access point.
Mesh Backhaul RRM	Check box that you check to enable mesh backhaul RRM.
Outdoor Ext. UNII B Domain Channels	Check box that you check to enable Outdoor Ext. UNII B Domain Channels.

Mesh RAP Downlink Backhaul

Table 5-90 Mesh RAP Downlink Backhaul

Parameter	Description
RAP Downlink Backhaul	To configure Mesh Downlink Backhaul to 2.4 GHz, select the 2.4 GHz option and click **Enable**. This configuration applies to all mesh RAPs. Channel provisioning can also be done on individual RAP. In that case, the channel provisioning applies only to that specific RAP branch of parents and children.

Convergence

Table 5-91 Convergence

Parameter	Description
Mode	Options include: • Standard • Noise Tolerant Fast—Noise-tolerant fast convergence method to handle unstable RF environment • Fast • Very Fast
Channel Change Notification	Check box that you check to enable channel change notification.
Background Scanning	Check box that you can check to enable background scanning.

Ethernet Bridging

Table 5-92 Ethernet Bridging Parameters

Parameter	Description
VLAN Transparent	VLAN transplant that you can enable or disable. This default is disable. When you enable this option, VLAN tags are not handled and packets are bridged as if they are untagged. You should disable this option if you want to enable VLAN-aware Ethernet bridging.

Security

Table 5-93 Security Parameters

Parameter	Description
Security Mode	EAP (Extensible Authentication Protocol) or PSK (Preshared Key); the default option is EAP. **Note** If you enable the External MAC Filter Authorization option, you need to choose the **EAP** option. **Note** If you do not enable the External MAC Filter Authorization option, local EAP or PSK authentication is performed within the controller.
External MAC Filter Authorization	Authorization that you can enable or disable. The default is disable. Enable this option to allow an external RADIUS server to perform MAC filter authorization. This option protects your network against rogue mesh access points by preventing access points that are not defined on the external server from joining. When you enable this option and click **Apply**, the access points reboot and then rejoin the controller if defined in the MAC filter list. Access points that are not defined in the MAC list cannot join the controller. **Note** When this option is not enabled, by default, the controller authorizes and authenticates mesh access points using the MAC address filter. Before you employ external authentication within the mesh network, you must perform the following configuration: • On the controller, configure the RADUIS server to be used as an AAA server. • Configure the controller on the RADIUS server. • Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server. – For remote authorization and authentication, EAP-FAST uses the manufacturer's certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation. – For Cisco IOS-based mesh access points (1240, 1522, 1524), the platform name of the mesh access point is located in front of its Ethernet address within the certificate; therefore, the username for external RADIUS servers is *platform_name_string–Ethernet_MAC_address* such as c1240-001122334455. • Install the certificates and configure EAP-FAST on the RADIUS server.

Table 5-93 Security Parameters

Parameter	Description
Force External Authentication	Force external authentication that you can enable or disable. The default is disable. Enable this option with EAP and External MAC Filter Authorization to allow external authorization and authentication of mesh access points using a RADIUS server.
LSC Only MAP Authentication	LSC Only MAP Authentication that you can enable or disable. The default state is disabled.

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.

ATF

This section describes the Air Time Fairness GUI elements.

Monitor Mode

Choose **WIRELESS > ATF > Monitor Mode** to navigate to **ATF Monitor Mode Configuration** page.

Table 5-94 ATF Monitor Mode Configuration

Parameter	Description
AP Name	Choose an AP Name from the drop-down list for the ATF to be monitored at the AP level.
AP Group Name	Choose an AP group from the drop-down list for the ATF to be monitored at the AP group level.
Network	ATF to be monitored at the network level. Specify the radio type if you choose the ATF to be monitored at the network level.
Radio Type	Radio type that you can choose between 802.11a and 802.11b.

Policy Configuration

Choose **WIRELESS > ATF > Policy Configuration** to navigate to **ATF Policy Configuration** page.

Table 5-95 ATF Policy Configuration

Parameter	Description
ID	An ID for the ATF policy that you can select from the drop-down list.
Name	Name of the ATF Policy that you can specify.

Table 5-95 ATF Policy Configuration

Parameter	Description
Client Fair Sharing	Check box that you can use to enable or disable client fair sharing on the policy.
Weight	Weighted ratio for the policy. **Note** Weighted ratio is used instead of percentages so that the total can exceed 100. The minimum weight that you can set is 10.

Enforcement Mode

Choose **WIRELESS > ATF > Enforcement Mode** to navigate to **ATF Enforcement Mode Configuration** page.

Table 5-96 ATF Enforcement Mode Configuration

Parameter	Description
AP Name	Choose an AP Name from the drop-down list for the ATF to be monitored at the AP level.
AP Group Name	Choose an AP group from the drop-down list for the ATF to be monitored at the AP group level.
Network	ATF to be monitored at the network level. Specify the radio type if you choose the ATF to be monitored at the network level.
Radio Type	Radio type that you can choose between 802.11a and 802.11b.
Enforcement Type	ATF policy enforcement that you can apply as either strict or optimized: • Optimized—The WLAN can share its weighted slot with other WLANs if its own slot is not being used. In optimized mode, the unused airtime (from other under-utilized backhaul nodes and/or clients) can be used by both the over-utilized backhaul or/and client. • Strict—Does not allow sharing of its weighted ratio slot In strict mode, airtime is fixed to airtime percentage, based on mesh node calculation.
Policy Enforcement	Map the WLAN ID with the ATF policy ID to apply the ATF policy to a WLAN.

Mesh Configuration

Choose **WIRELESS > ATF > Mesh Configuration** to navigate to **Mesh Universal Access Client Airtime Allocation** page.

Table 5-97 Mesh Universal Access Client Airtime Allocation

Parameter	Description
AP Name	Choose a mesh AP Name from the drop-down list.
Radio Type	Radio type that you can choose between 802.11a and 802.11b.
Default % Alloc Per Node	Default percentage of allocation per node.
No. of Nodes	Number of backhaul nodes.
Override	Check box that you can check to allow override of ATF Airtime allocation on the mesh AP.
Override allocation on client access Node	Percentage of airtime allocation for client access. Valid range is between 5 and 90. This percentage of airtime allocation impacts both the client and the uplink backhaul percentage.

ATF Statistics

Choose **WIRELESS > ATF > ATF Statistics** to navigate to **ATF Statistics** page.

Table 5-98 ATF Statistics

Parameter	Description
AP Name	Choose an AP Name from the drop-down list to view the ATF statistics of the AP.

RF Profiles

Choose **WIRELESS > RF Profiles** to navigate to the RF Profiles page. This page enables you to create and configure RF profiles in the controller.

Out of Box AP Group

You can select the **Enable Out Of Box** check box to create an Out of Box AP group that consists of newly installed access points that belong to the default AP group. When you enable this feature:

- Newly installed access points that are part of the default AP group will be part of the Out-of-Box AP group and their radios will be switched off. This eliminates any RF instability caused by the new access points.
- All access points that do not have a group name become part of the Out of Box AP group.
- Special RF profiles are created per 802.11 band. These RF profiles have default-settings for all the existing RF parameters and additional new configurations.

When you disable this feature after you enable it, only subscription of new APs to the Out of Box AP group stops. All APs that are subscribed to the Out of Box AP Group remain in this AP group. The network administrators can move such APs to the default-group or a custom AP group upon network convergence.

Click **New** to create a new RF profile.

This table describes the RF profile parameters.

Table 5-99 RF Profile Parameters

Parameter	Description
General Parameters	
Profile Name	Name of the RF profile.
Radio Policy	Whether the RF profile will be applied to the 802.11a or 802.11b/g radios. **Note** According to the selection of the Radio Policy, the other parameters may differ.
Description	Description of the RF profile.
802.11	
Data Rates	Data rate that is Mandatory indicates that the clients that do not support this specific rate will not be able to associate with the AP. Data rate that is Supported indicates that any associated client that also supports this rate can communicate with the AP using this rate. Data rate that is Disabled indicates that clients do not support this specific rate. The following data rates are supported by 802.11a: • 6 Mbps • 9 Mbps • 12 Mbps • 18 Mbps • 24 Mbps • 36 Mbps • 48 Mbps • 54 Mbps The following data rates are supported by 802.11b/g: • 1 Mbps • 2 Mbps • 5.5 Mbps • 6 Mbps • 9 Mbps • 11 Mbps • 12 Mbps • 18 Mbps • 24 Mbps • 36 Mbps • 48 Mbps • 54 Mbps

Table 5-99 RF Profile Parameters

Parameter	Description
MCS Settings	Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available: • 0 (7 Mbps) • 1 (14 Mbps) • 2 (21 Mbps) • 3 (29 Mbps) • 4 (43 Mbps) • 5 (58 Mbps) • 6 (65 Mbps) • 7 (72 Mbps) • 8 (14 Mbps) • 9 (29 Mbps) • 10 (43 Mbps) • 11 (58 Mbps) • 12 (87 Mbps) • 13 (116 Mbps) • 14 (130 Mbps) • 15 (144 Mbps) Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.
RRM > Transmit Power Control (TPC) Parameters	
Maximum Power Level Assignment	Maximum transmit power used by the RRM. The range is from –10 to 30 dBm. The default value is 30 dBm.
Minimum Power Level Assignment	Minimum transmit power used by the RRM. The range is from –10 to 30 dBm. The default value is –10 dBm.
Power Threshold v1	Transmit Power Control v1 threshold value. The range is from –80 to –50 dBm. The default value is –70 dBm. Power Threshold is the cutoff signal level used by the RRM when determining whether to reduce an access point's power.
Power Threshold v2	Configures the Transmit Power Control v2 threshold value. The range is from –80 to –50 dBm. The default value is –67 dBm.
RRM > Coverage Hole Detection Parameters	

Table 5-99 RF Profile Parameters

Parameter	Description
Data RSSI	Minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. The range is from –60 to –90 dBm. The default value is –80 dBm. If the access point receives a packet in the data queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes data RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Voice RSSI	Minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. The range is from –60 to –90 dBm. The default value is –75 dBm. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Coverage Exception	Minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold to trigger a coverage hole exception. The range is from 1 to 75, and the default value is 3.
Coverage Level	Percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. If an access point has more number of such clients than the configured coverage level it triggers a coverage hole event. The range is from 0 to 100%, and the default value is 25%. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.
RRM > DCA	
Avoid AP Foreign AP Interference	Select the **Avoid Foreign AP Interference** check box to cause the Cisco WLC's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or unselect it to disable this feature.
Channel Width	Select the required bandwidth for the AP based on the type of clients available in the RF environment.
RRM > High-Speed Roam	
HSR mode	Check box to enable or disable High-Speed Roam mode. If the check box is selected, the HSR mode is in enabled state.
Neighbor Timeout Factor	Neighbor Timeout factor value.

Table 5-99 RF Profile Parameters

Parameter	Description
RRM > DCA Channel List	
DCA Channels	The DCA Channels text box shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, unselect its check box. The ranges are as follows: • 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153,157, 161, 165, 190, 196 • 802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 The defaults are as follows: • 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153,157, 161 • 802.11b/g—1, 6, 11
Extended UNII-2 channels	100, 104, 108, 112, 116,132, 136, and 140—These extended UNII-2 channels in the 802.11a band do not appear in the channel list. If you have Cisco Aironet 1520 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, select the **Extended UNII-2 Channels** check box.
RRM > Profile Threshold For Traps	
Interference (0 to 100%)	Interference threshold on the RF environment.
Clients (1 to 200)	Number of clients present in the RF profile for which the trap is configured.
Noise (-127 to 0 dBm)	The channel noise level for trap generation.
Utilization (0 to 100 %)	The channel utilization for trap generation.
High Density and Multicast Parameters	
Maximum Clients	Maximum number of clients that can communicate with the AP in a high-density environment. The range is from 1 to 200. The default value is 200.
Client Trap Threshold	Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller and Cisco Prime Infrastructure. The range is from 0 to 200. The default value is 50. Traps are disabled if the threshold value is configured as zero. Client trap threshold value should be less than then maximum clients configuration.

Table 5-99 RF Profile Parameters

Parameter	Description
Multicast Data Rates	Multicast data rate of a client with the AP. The following multicast data rates are supported by 802.11a and 802.11b/g: • 6 Mbps • 9 Mbps • 12 Mbps • 18 Mbps • 24 Mbps • 36 Mbps • 48 Mbps • 54 Mbps If you choose **auto**, the AP automatically adjusts the data rate with the client.
Rx Sop Threshold	Drop-down list from which you can choose the high, medium, or low Rx SOP threshold value for a band. For more details, see Mesh.
Client Distribution > Load Balancing	
Window	The window size is part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations: *load-balancing window + client associations on AP with lightest load = load-balancing threshold* The range is from 0to 20. The default value is 5. In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.
Denial	The denial count sets the maximum number of association denials during load balancing. Enter a value between 1 and 10. The default value is 3.
Client Distribution > Band Select **Note** Band Select configurations are available only for 802.11BG RF profiles.	
Probe Response	Probe responses to clients that you can enable or disable.
Cycle Count	Probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client. The range is from 1 to 10. The default value is 2.

Table 5-99 RF Profile Parameters

Parameter	Description
Cycle Threshold	Time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle. The range is from 1 to 1000 milliseconds. The default value is 200.
Suppression Expire	Expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression. The range is from 10 to 200 seconds. The default value is 20 seconds.
Dual Band Expire	Expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression. The range is from 10 to 300. The default value is 60 seconds.
Client RSSI	Minimum RSSI for a client to respond to a probe. The range is from –90 to –20 dBm. The default value is –80 dBm.

Note Changing the data rates and minimum client count requires explicit network dependencies. You must disable the 802.11a or 802.11b/g network before changing data rates and minimum client count in RF Profiles.

Click **Apply** to send the RF Profile configuration data to the Cisco WLC.

FlexConnect Groups

Choose **WIRELESS > FlexConnect Groups** to navigate to the FlexConnect Groups page. This page lists any FlexConnect groups that have already been created.

All the FlexConnect access points in a group share the same FlexConnect configuration information.

If you want to delete an existing group, click the blue arrow adjacent the group and choose **Remove**.

Cisco Centralized Key Management

FlexConnect groups are required for Cisco Centralized Key Management (CCKM) fast roaming to work with FlexConnect access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can take place when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller.

Note CCKM fast roaming among FlexConnect and non-FlexConnect access points is not supported.

802.1X Authentication

FlexConnect access points support 802.1X authentication. FlexConnect access points forward the client authentication request to a local (backup) RADIUS server when the access point is in standalone mode (for example, when the WAN link is down or when the access point loses connectivity to the controller).

To enable 802.1X authentication, configure backup RADIUS servers on the FlexConnect access points to authenticate the clients when the access point is in standalone mode.

In standalone mode, if the client is connected and the session timeout has expired, the client reauthenticates with the local backup RADIUS server.

Local authentication is useful when you cannot maintain the criteria that a remote office setup has a minimum bandwidth of 128 Kbps with a round trip latency of no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

Note Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.

Local authentication is not supported in the following scenarios:

- Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
- RRM information is not available at the controller for the FlexConnect local authentication-enabled WLAN.
- Local RADIUS is not supported.
- Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information

Note Only the **session timeout** RADIUS attribute is supported in the standalone mode. All other attributes are not supported.

Note RADIUS accounting is not supported in standalone mode.

Click **New** to add a new FlexConnect group.

Creating FlexConnect Groups

Choose **WIRELESS > FlexConnect Groups** and then click **New** to navigate to the FlexConnect Groups > New page.

This page allows you to create an FlexConnect group.

The number of FlexConnect groups and access point support depends on the platform that you are using. You can configure the following:

- Up to 100 FlexConnect groups for a Cisco 5500 Series Wireless Controller.
- Up to 1000 FlexConnect groups for a Cisco Flex 7500 Series Wireless Controller. The Cisco Flex 7500 Series Wireless Controller can accommodate up to 50 access points per group.

- Up to 2000 FlexConnect groups for a Cisco Flex 8500 Series Wireless Controller. The Cisco Flex 8500 Series Wireless Controller can accommodate up to 100 access points per group.
- Up to 20 FlexConnect groups with up to 25 access points per group for the remaining platforms.

You can add up to 20 FlexConnect groups per controller. For the Cisco 5500 Series Wireless Controller, you can add up to 100 FlexConnect groups.

When the FlexConnect Groups > New page appears, enter the name of the new group in the Group Name text box. You can enter up to 32 alphanumeric characters.

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.

Editing FlexConnect Groups

Choose **WIRELESS > FlexConnect Groups** and then click a group name to navigate to the FlexConnect Groups > Edit page.

This page enables you to configure or change the various parameters grouped under different tabs for an existing FlexConnect group. The different tabs are as follows:

- General Tab
- Local Authentication Tab
- Image Upgrade Tab
- ACL Mapping Tab
- Central DHCP Tab
- WLAN to VLAN Mapping Tab
- WLAN AVC Mapping Tab

General Tab

Table 5-100 General Tab Parameters

Parameter	Description
Group Name	Name of the FlexConnect group.
VLAN Template Name	Drop-down list from which you can choose the VLAN template name to be applied. For information about creating FlexConnect VLAN templates, see the FlexConnect VLAN Templates section.
Enable AP Local Authentication	Check box that you can select to enable local AP authentication for a FlexConnect group. The default value is unselected. The FlexConnect AP can be configured as a RADIUS server for LEAP, EAP-FAST, PEAP, or EAP-TLS client authentication. **Note** You can configure LEAP, EAP-FAST, PEAP, or EAP-TLS authentication only if AP local authentication is enabled.
FlexConnect APs	

Table 5-100 General Tab Parameters

Parameter	Description
To add an access point to the group, click **Add AP**. The Add AP area appears. To choose an access point that is connected to this controller, select the **Select APs from Current Controller** check box and then choose the name of the desired access point from the **AP Name** drop-down list. **Note** If you choose an access point on this controller, the MAC address of the access point is automatically entered in the Ethernet MAC field to prevent any mismatches from occurring. To choose an access point that is connected to a different controller, leave the **Select APs from Current Controller** check box unselected and then enter its MAC address in the **Ethernet MAC** text box. **Note** If the FlexConnect access points within a group are connected to different controllers, all controllers must belong to the same mobility group. Click **Add** to add the access point to this FlexConnect group. The access point's MAC address and name appear at the bottom of the page.	
AAA	AAA parameters.
Server IP Address	IP address of the primary or secondary RADIUS server. **Note** IPv6 is not supported for local authentication.
Server Type	Drop-down list from which you can choose a primary or secondary RADIUS server. See the RADIUS Authentication Servers topic for more details.
Shared Secret	RADIUS server login shared secret.
Port Number	Communication port number for the interface protocols. The default port number is 1812. **Note** Do not assign the port number that is used by another application. Use the default port or any other port unused by any other application.

Click **Add** to add the RADIUS server to the list of RADIUS servers.

Local Authentication Tab

Table 5-101 Local Authentication Tab Parameters

Parameter	Description
Local Users Tab	
No of Users	Number of users currently associated.
User Name	Supported local users.

Table 5-101 Local Authentication Tab Parameters

Parameter	Description
Add User	Users that you can add by either entering the username and password or by uploading a comma-separated values (CSV) file. **Note** You can add up to 100 users. • Upload CSV file—Select this option to upload a CSV file that contains user names and passwords. Each line of the file needs to be in the following format: *username*, *password* • File Name—Click **Browse** to browse to the CSV file. • Username—Enter the username of the client that you want to authenticate using LEAP, EAP-FAST, PEAP, or EAP-TLS. • Password—Enter the password of the client. • Confirm Password—Reenter the password of the client. • Add button—Click to add the user or upload the CSV file.
Remove All Users	Click the button to delete all local users.
Protocols Tab	
Enable LEAP Authentication	FlexConnect access point to authenticate clients using LEAP. You can configure LEAP authentication only when AP local authentication is configured.
Enable EAP Fast Authentication	FlexConnect access point to authenticate clients using EAP-FAST. You can configure EAP Fast authentication only when AP local authentication is configured.
Server Key (in hex)	PACs that you can send automatically to clients that do not have one during PAC provisioning. You can select the **Enable Auto key generation** check box to automatically generate the server key. To use manual PAC provisioning, enter the server key used to encrypt and decrypt PACs in the Server Key and Confirm Server Key fields. The key must be 32 hexadecimal characters.
Authority ID (in hex)	Authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
Authority Info	Authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
PAC Timeout (2 to 4095)	PAC timeout value. The default value is unselected. Enter the number of seconds for the PAC to remain viable in the text box. The range is 2 to 4095 seconds.
Enable PEAP Authentication	FlexConnect access point to authenticate clients using PEAP. You can configure PEAP authentication only when AP local authentication is configured.

Table 5-101 Local Authentication Tab Parameters

Parameter	Description
Enable EAP-TLS Authentication	FlexConnect access point to authenticate clients using EAP-TLS. You can configure EAP-TLS authentication only when AP local authentication is configured.
EAP TLS Certificate Download	Check box that you can select to download the EAP root and device certificate to the access point.

Image Upgrade Tab

This table describes the image upgrade parameters.

Table 5-102 Image Upgrade Tab Parameters

Parameter	Description
FlexConnect AP Upgrade	FlexConnect AP upgrade that you can enable.
Slave Maximum Retry Count	Maximum number of retries for the preimage download. This option is available if the FlexConnect AP Upgrade option is enabled.
Upgrade Image	Drop-down list from which you can choose to download the primary image, store the image as backup, or abort the download. The available options are: • Primary—Upgrades the primary image of the controller. • Backup—Upgrades the backup image of the controller. • Abort—Aborts the image upgrade. Click the **FlexConnect Upgrade** button to upgrade the image of the FlexConnect AP.
FlexConnect Master APs	
AP Name	Access point name.
Add Master	Adds a master FlexConnect AP. The following parameters are available: • Master AP Name • AP Model • Manual

ACL Mapping Tab

This tab consists of the following three tabs:

- AAA VLAN-ACL Mapping Tab
- WLAN-ACL Mapping Tab
- Policies Tab

AAA VLAN-ACL Mapping Tab

This table describes the AAA VLAN-ACL mapping tab parameters.

Table 5-103 AAA VLAN-ACL Mapping Tab Parameters

Parameter	Description
VLAN Id	ID of the VLAN for which mapping has to be done.
Ingress ACL	Drop-down list from which you can choose the ingress ACL.
Egress ACL	Drop-down list from which you can choose the egress ACL.

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.

Click **Add** to add a VLAN-ACL mapping.

WLAN-ACL Mapping Tab

Table 5-104 WLAN-ACL Mapping Tab Parameters

Parameter	Description
Web Auth ACL Mapping	
WLAN Id	ID of the WLAN for which the mapping has to be done.
WebAuth ACL	Drop-down list from which you select the WebAuth ACL for external web authentication. Click **Add** to add the WebAuth ACL mapping. For more information about creating FlexConnect ACLs, see the Access Control Lists topic. **Note** You can configure up to 16 WebAuth ACLs for an access point.
Local Split ACL Mapping	
WLAN ID	WLAN ID number.
Local-split ACL	Drop-down list from which you can choose the Local Split ACL to locally switch traffic in centrally switched WLANs. Click **Add** to add the local split ACL mapping. Local-split configuration is applied specific to a WLAN. You can also apply this configuration from a FlexConnect group or from an AP. If the local-split configuration is applied at both the FlexConnect group level and AP level, then the configuration applied at the AP level has higher priority. In other words, the FlexConnect ACL specific to the AP has higher priority.

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.

Click **Add** to add a WLAN FlexConnect ACL mapping.

Policies Tab

Table 5-105 Policies Tab Parameters

Parameter	Description
Policy ACL	Drop-down list from which you can select a device-based Policy AC. Click **Add** to add the Policy ACL. For more information about creating FlexConnect ACLs, see the Access Control Lists topic. **Note** You can configure up to 16 Policy ACLs that are specific to the FlexConnect group.

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.

Click **Add** to add a Policy ACL.

Central DHCP Tab

Table 5-106 Central DHCP Tab Parameters

Parameter	Description
WLAN ID	ID of the WLAN.

WLAN to VLAN Mapping Tab

Until controller Release 7.4, WLAN to VLAN mapping was done per AP. From controller Release 7.5, you can map WLAN to VLAN from the FlexConnect groups. WLAN to VLAN mapping is configured on all the APs in the FlexConnect group and does not override the WLAN to VLAN mapping done on the access points. The order of priority for WLAN to VLAN mappings is highest for AP groups > FlexConnect group > WLAN.

In Release 8.1 VLAN Support/Native VLAN on FlexConnect Group feature is available, which enables you to configure VLAN Support and Native VLAN ID on a FlexConnect Group.

Table 5-107 WLAN to VLAN Mapping Tab Parameters

Parameter	Description
VLAN Support	Enable the VLAN Support check box and enter a Native VLAN ID.
Override Native VLAN on AP	This option overrides the VLAN Support and Native VLAN ID parameters previously configured on the Access points, changes the inheritance level at the AP to “Group-specific”, removes AP Specific WLAN-VLAN Mappings and pushes the group-specific configuration including WLAN-VLAN Mapping configured on the group to all the APs in that group. When the override flag is set at the FlexConnect Group, modification of VLAN Support, Native VLAN ID, WLAN-VLAN Mappings and Inheritance-Level at the AP is not allowed
WLAN ID	ID of the WLAN.
Vlan Id	ID of the VLAN.

Click **Add** to add a WLAN VLAN Mapping.

WLAN AVC Mapping Tab

Table 5-108 WLAN AVC Mapping Tab Parameters

Parameter	Description
WLAN ID	ID of the WLAN.
Application Visibility	Enable the Application Visibility on the FlexConnect Group
Flex AVC Profile	Apply the FlexConnect AVC profile

FlexConnect Groups and OKC

FlexConnect Groups enable Opportunistic Key Caching (OKC) to enable fast roaming of clients. OKC facilitates fast roaming by using PMK Caching in access points that are in the same FlexConnect group.

This feature prevents the need to perform a full authentication as the client roams from one access point to another. Whenever a client roams from one FlexConnect access point to another, the FlexConnect group access point calculates the PMKID using the cached PMK.

To see the PMK cache entries at the FlexConnect access point, use the **show capwap reap pmk** command. This feature is supported on Cisco FlexConnect access points.

Note The FlexConnect access point must be in connected mode when the PMK is derived during WPA2/802.1X authentication.

FlexConnect ACLs

With FlexConnect ACLs, you can control access at the FlexConnect AP for protection and integrity of locally switched data traffic from the AP. Using the controller, you can create FlexConnect ACLs and then configure the FlexConnect ACL with the WLAN using WLAN-ACL mapping. These are then pushed to the AP.

Choose **WIRELESS > FlexConnect Groups > FlexConnect ACLs** to navigate to the **FlexConnect Access Control Lists** page.

This page enables you to list the ACLs configured for FlexConnect access points. To remove a FlexConnect ACL, click the blue arrow adjacent the access point and choose **Remove**.

Click **New** to open the **Access Control Lists > New** page.

Adding FlexConnect ACLs

Choose **WIRELESS > FlexConnect Groups > FlexConnect ACLs** and click **New**. This page enables you to create an ACL. Enter the FlexConnect ACL name in the **Access Control List Name** text box.

Click **Apply** to create a new FlexConnect ACL with the configured name.

Editing Access Control List

Choose **WIRELESS > FlexConnect Groups > FlexConnect ACLs** and click the ACL name of an existing ACL to open the **Access Control List > Edit** page.

Table 5-109 FlexConnect Access Control List Parameters

Parameter	Description
General	
Access List Name	Name of the FlexConnect ACL.
Seq	Up to 64 rules can be defined for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and sequence 5 to 6.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.
Source IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Protocol	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)
Source Port	Any or IP address and netmask.

Table 5-109 FlexConnect Access Control List Parameters

Parameter	Description
Dest Port	Any or IP address and netmask.
DSCP	Any or Specific (from 0 to 63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service (QoS) across the Internet.

Click **Add a New Rule** to add a new rule to an existing ACL.

Adding FlexConnect ACL Rules

Choose **SECURITY > Access Control List > FlexConnect ACLs** to navigate to the FlexConnect Access Control Lists page. Click an ACL name of an existing ACL to open the **Access Control List > Edit** page and click **Add New Rule** button to create a new ACL Rule.

Table 5-110 FlexConnect ACL New Rule Parameters

Parameter	Description
Sequence	Operator that can define up to 64 rules for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5. **Note** If you add or change a sequence number, the Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the Operating System automatically reassigns sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.

Table 5-110 FlexConnect ACL New Rule Parameters

Parameter	Description
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA's Website)
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

FlexConnect VLAN Templates

Choose **WIRELESS > FlexConnect Groups > FlexConnect VLAN Templates** and click **New** to create FlexConnect VLAN templates.

The **FlexConnect VLAN Template List** page displays the VLAN templates and their status.

Editing FlexConnect VLAN Templates

Step 1 On the **FlexConnect VLAN Template List** page, click the name of a template.

The **VLAN Template > Edit** page is displayed.

Step 2 Click **New Mapping**.

Step 3 Enter the VLAN name and VLAN ID.

Valid range of VLAN ID is 1 and 4094.

Step 4 Click **Apply**.

Step 5 On the **VLAN Template > Edit** page, click **Apply All**.

Note For the mapping to be pushed to FlexConnect APs, the FlexConnect VLAN template must be in Applied state. If the template is in Modified state, the template is not pushed to the FlexConnect APs.

Copying FlexConnect VLAN Templates (Optional)

Step 1 On the **FlexConnect VLAN Template List** page, click **Copy**.

Step 2 Enter the FlexConnect VLAN template name.

Step 3 Choose the existing VLAN template name from which the template should be copied.

Step 4 Click **Copy**.

OEAP ACLs

Choose **WIRELESS > OEAP ACLs** to navigate to the **OEAP Access Control Lists** page.

Click **New** to add an OEAP ACL.

OEAP Access Control List > Rules

Step 1 On the **OEAP Access Control Lists** page, click the ACL name.

Step 2 On the **OEAP Access Control List > Rules** page, click **Add New Rule**.

Enter the parameters listed in this table:

Table 5-111 OEAP Access Control List Rules

Parameter	Description
Sequence	Up to 64 rules are supported for each ACL. These rules are listed in order from 1 to 64. Enter a value between 1 and 64 to determine the order of this rule in relation to any other rules defined for this ACL. **Note** If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.
Source	Drop-down list from which you can specify the source of the packets to which the ACL is applicable: • Any—Any source (default value) • IP Address—A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding text boxes.
Destination	Drop-down list from which you can specify the destination of the packets to which this ACL applies: • Any—Any destination (default value) • IP Address—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes. • Network List—A specific network list. If you choose this option, enter the corporate subnets configured in the network list. To create a network list, see the "Network Lists" section on page 5-104.

Table 5-111 OEAP Access Control List Rules

Parameter	Description
Protocol	Drop-down list from which you can choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following: • Any—Any protocol (default value) • TCP • UDP • Other—Any other Internet-Assigned Numbers Authority (IANA) protocol **Note** If you choose Other, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.
Action	Drop-down list from which you can choose an action to be performed: • Deny—Causes this ACL to block packets (default setting) • Permit—Causes this ACL to allow packets • Nat-route—Routes all packets matching the rule to the local network or NAT the packets matching the rule to the Internet.

Step 3 Click **Apply**.

Network Lists

You can create network lists to be used as destination option for the packets to which an OEAP ACL applies.

Step 1 Choose **WIRELESS > Network Lists** to navigate to the **Split Tunnel Network Lists** page.

Step 2 Click **New** to create a Split Tunnel Network List.

Enter the parameters listed in this table:

Table 5-112 Split Tunnel Network List Parameters

Parameter	Description
List Index	Drop-down list from which you can choose the index of the network list.
List Name	Enter a name for the network list.
Gateway IP	Enter the IP address of the gateway.
Subnet Mask	Enter the subnet mask.

Step 3 Click **Apply**.

802.11a/n/ac

This section contains the following topics:

- Network, page 5-105
- RRM, page 5-106
- Client Roaming, page 5-119
- Media, page 5-120
- 802.11 EDCA Parameters, page 5-125
- DFS (802.11h), page 5-126
- High Throughput (802.11n), page 5-127
- CleanAir, page 5-128

Network

Choose **WIRELESS > 802.11a/n/ac > Network** to navigate to the **Global Parameters** page. This page enables you to change the global parameters of your 802.11a/n/ac network.

Table 5-113 802.11a/n/ac Global Parameters

Parameter	Description
802.11a Network Status	802.11a/n/ac network status. **Note** You must enable this option to enable the 802.11a/n/ac network after configuring other 802.11a/n/ac parameters. This option enables only the global Cisco WLAN Solution 802.11a/n/ac network. To disable the 802.11a, 802.11b, 802.11g, 802.11n, and/or 802.11ac networks for an individual WLAN, see the Editing WLANs page.
Beacon Period	Rate (in milliseconds) at which the SSID is broadcast by the access point. Valid values are from 100 to 600; the default is 100.
Fragmentation Threshold	Fragmentation threshold that you can set. Valid values are from 256 to 2346 bytes; the default is 2346.
DTPC Support	DTPC support. Enable this option to advertise the transmit power level of the radio in the beacons and the probe responses.
Maximum Allowed Clients	Maximum clients allowed per radio.
RSSI Low Check	Check box that you can enable to reject a client association request if the Received Signal Strength Indicator (RSSI) is lower than the configured RSSI threshold.
RSSI Threshold	RSSI Threshold that is used to reject the client association request. The range is from –60 to –90 dBm. The default value is –80 dBm.
802.11a Band Status	802.11a/n low-band, mid-band, and high-band statuses.

Table 5-113 802.11a/n/ac Global Parameters

Parameter	Description
Data Rates	Data rates that are negotiated here are negotiated between the client and the Cisco WLC. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Cisco WLC, the client may negotiate for the respective rate. Each data rate can also be set to Disabled to match client settings.
CCX Location Measurement	Mode that enables CAPWAP access points to issue broadcast Radio Measurement Request messages to Cisco Compatible Extensions (V2 and higher) clients. This Measurement Request message is repeated periodically for every SSID over each enabled radio interface based on the specified interval. The response from the client is used to improve accuracy in location measurement. Interval (seconds)—Interval of the broadcast Radio Measurement Request messages.

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.

RRM

This section contains the following topics:

- RF Grouping, page 5-106
- TPC, page 5-109
- DCA, page 5-110
- Coverage, page 5-116
- General, page 5-117

RF Grouping

Choose **WIRELESS > 802.11a/n/ac > RRM > RF Grouping** to navigate to the RF Grouping page.

This page enables you to edit the RF grouping characteristics.

RF Grouping Algorithm

Table 5-114 RF Grouping Algorithm Parameters

Parameter	Description
Group Mode	RF grouping that can be configured in any of these modes: • **leader** **Note** IPv6 is supported for RF grouping in static-leader mode. • **auto** **Note** IPv6 is not supported for RF grouping in auto mode. It supports only IPv4. • **off**. When the group mode is off, no RF grouping occurs. When a controller reboots, it starts by being a standalone leader to itself. In auto mode, the controllers form an RF group and elect an auto leader (group mode is auto mode) if the neighboring APs are in the same RF domain. In static mode, the user can configure the static leader by selecting the leader from the group mode drop-down list. The members' management IP addresses and system name are used to request the member to join the static-leader. **Note** A static leader is not allowed to become a member of another controller until its mode is **auto**. **Note** A controller with a lower priority cannot assume the role of a group leader if a controller with a higher priority is available in the RF group. Click **Restart** to restart the RRM RF grouping.
Group Role	Current role of the controller.
Group Update Interval	Interval (in seconds) that represents the period with which the grouping algorithm is run by the group leader. The Grouping algorithm also runs when the group contents change and automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. This value is set at 600 seconds.

Table 5-114 RF Grouping Algorithm Parameters

Parameter	Description
Group Leader	Name and IPv4/IPv6 address of the group leader for the group that contains the Cisco WLC. The RF Group Leader can be configured in two ways, as follows: • Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes). • Static Mode—In this mode, the user selects a controller as an RF Group leader manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF Group, the reason is indicated. The leader tries to establish a connection with a member every 1 (one) minute if the member has not joined in the previous attempt.
Last Group Update	Elapsed time since the last group update in seconds. This parameter is only valid if this Cisco WLC is a group leader.

RF Group Members

Table 5-115 RF Group Members

Parameter	Description
Controller Name	controller on which the RF Group is created.
IP Address (IPv4/IPv6)	IPv4/IPv6 address of the controller that belong to a RF group. **Note** IPv6 is supported only for leader type (static-leader) of RF grouping.

You can add a controller as a static group member by specifying the controller name and the management IP address. Click **Add** to add the controller as an RF group member.

When adding RF group members, the leader can allow the number of group members based on the following criteria:

- Maximum number of APs supported: The maximum limit for the number of access points in an RF group is 1000 or twice the maximum number APs licensed on the controller.
- Twenty controllers: Only 20 controllers (including the leader) can be part of an RF group if the sum of the access points of all controllers combined is less than or equal to the upper access point limit.

Note If a controller cannot be added as a static RF group member, the reason is indicated in parentheses.

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.

TPC

Choose **WIRELESS > 802.11a/n/ac > RRM > TPC** to navigate to the **Tx Power Control (TPC)** page.

This page enables you to edit the transmit power control (TPC) parameters.

Tx Power-Level Assignment

The TPC algorithm balances RF power in many diverse RF environments. Automatic power control may not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply only to access points that are attached to a controller from which they are configured. The default settings disable this feature, and you should use care when overriding TPC recommendations.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes, enter the maximum and minimum transmit power used by RRM on the Tx Power Control page. The range for these parameters is –10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

Table 5-116 Tx Power Level Assignment Parameters

Parameter	Description
TPC Version	Transmit Power Control version to be chosen from the following options: • Interference Optimal Mode (TPCv2)—For scenarios where voice calls are extensively used. Transmit power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there might be more frequent roaming and coverage hole incidents. • Coverage Optimal Mode (TPCv1)—(Default) Offers strong signal coverage. Power can be kept low to gain extra capacity and reduce interference.
Power Level Assignment Method	Dynamic transmit power assignment has three modes: • Automatic—(Default) The transmit power is periodically updated for all access points that permit this operation. • On Demand—The transmit power is updated when the **Invoke Power Update Now** is clicked. • Fixed—No dynamic transmit power assignments occur and values are set to their global default.

Table 5-116 Tx Power Level Assignment Parameters

Parameter	Description
Maximum Power Level Assignment (–10 to 30 dBm)	Maximum power level assignment on this radio. **Note** If you configure a maximum transmit power, RRM does not allow any access point attached to the controller to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually. The range is from –10 to 30 dBm. The default is 30.
Minimum Power Level Assignment (-10 to 30 dBm)	Minimum power level assignment on this radio. The range is from –10 to 30 dBm. The default is –10.
Power Threshold	Cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value for this parameter varies depending on the TPC version you choose. For TPCv1, the default value is –70 dBm, and for TPCv2, the default value is –67 dBm. The default value can be changed when access points are transmitting at higher (or lower) than desired power levels. The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power levels. Decreasing the value has the opposite effect. **Note** In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.
Power Neighbor Count	Minimum number of neighbors that an access point must have for the transmit power control algorithm to run.
Power Assignment Leader	Name and IP address of the power level assignment leader.
Last Power Level Assignment	Elapsed time since the last transmit power assignment in seconds.

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.

DCA

Choose **WIRELESS > 802.11a/n/ac > RRM > DCA** to navigate to the **Dynamic Channel Assignment (DCA)** page.

This page enables you to specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning.

This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Information About the RRM Start-Up Mode

- For a single controller setup, RRM start-up mode will take effect after a controller reboot.
- For a multicontroller setup, RRM start-up mode will take effect after RF Group leader election.
- The RRM start-up mode runs for 100 minutes (10 iterations at a 10-minute interval).
- The duration of the start-up mode is independent of the DCA interval, sensitivity, and network size.
- DCA start-up mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady state channel plan.
- After the start-up mode is finished, DCA continues to run at the interval and sensitivity specified by the user.

Dynamic Channel Assignment Algorithm

Table 5-117 DCA Algorithm Parameters

Parameter	Description
Channel Assignment Method	DCA has three modes: • Automatic—Mode that periodically updates the channel assignments for all access points that permit this operation. – Interval—How often the DCA algorithm has been configured to run. **Note** If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used. – Anchor Time—The time of day when the DCA algorithm has been configured to start. The range is from 0 to 23 (12:00 a.m. to 11:00 p.m.) • Freeze—Mode that causes the controller to evaluate and update the channel assignment for all joined access points, if necessary, but only when you click **Invoke Channel Update Once**. **Note** The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. It waits for the next interval to elapse. • OFF—Mode that turns off DCA and sets all access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios. The default is Automatic.
Avoid Foreign AP Interference	Radio Resource Management (RRM) Foreign 802.11 interference-monitoring parameter that you can enable Radio Resource Management to consider interference from foreign (non-Cisco access point outside the RF/mobility domain) access points when assigning channels to Cisco access points. You can disable this parameter to have Radio Resource Management ignore this interference. In certain circumstances with significant interference energy (dBm) and load (utilization) from Foreign APs, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the Foreign APs to increase capacity and reduce variability for the Cisco WLAN Solution.

Table 5-117 DCA Algorithm Parameters

Parameter	Description
Avoid Cisco AP Load	Radio Resource Management (RRM) bandwidth-sensing parameter that you can enable or disable to have controllers consider the traffic bandwidth used by each access point when the controller assigns channels to the access points. Disable this parameter to have Radio Resource Management ignore this value. The default is enabled. In certain circumstances and with denser deployments, there may not be enough channels to properly create perfect channel reuse. In these circumstances, Radio Resource Management can assign better reuse patterns to those access points that carry more traffic load.
Avoid non-802.11a Noise	Radio Resource Management (RRM) noise-monitoring parameter that you can enable to have access points avoid the channels that have interference from nonaccess point sources, such as microwave ovens or Bluetooth devices. You can disable this parameter to have Radio Resource Management ignore this interference. The default is enabled. In circumstances with significant interference energy (dBm) from non-802.11 noise sources, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability.
Avoid Persistent Non-WiFi Interference	Persistent non-Wi-Fi interference devices that you can enable or disable.
Channel Assignment Leader	Name and IP address of the channel assignment leader. This is the MAC address of the group leader.
Last Auto Channel Iteration	Last time that the Radio Resource Management (RRM) evaluated the current channel assignment on a periodic basis. This parameter does not imply that channels have changed, only that the Radio Resource Management has made an evaluation of the current assignment.
DCA Channel Sensitivity	Configured DCA sensitivity setting. This setting determines how sensitive the DCA algorithm is to environmental changes, such as signal, load, noise, and interference, when determining whether to change channels. **Note** To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

Table 5-117 DCA Algorithm Parameters

Parameter	Description
Channel Width[1]	Channel bandwidth supported for all the 802.11n/ac radios in the 5-GHz band: 20 MHz, 40 MHz, or 80 MHz. 40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels). **Note** If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width. **Note** You cannot pair the following channels together: 116 and 112, 140 and 136, and 165 and 161. 80 MHz channelization allows radios to achieve Very High Throughput (VHT). Adjacent 40-MHz subchannels are grouped into pairs to make 80-MHz channels. • If you choose 80 MHz for 802.11ac capable radios, ensure that you choose four adjacent 20-MHz channels from the DCA Channel List. You can select the primary channel and based on the available channel pairing you can configure appropriate secondary 20-MHz and 40-MHz extension channels for the radio.
Avoid check for non-DFS channel.	Check for non-DFS channels that you can enable or disable. DCA configuration requires at least one non-DFS channel to the list. In the EU countries, outdoor deployments do not support non-DFS channels. Customers based in EU or regions with a similar regulation must enable this option.

1. To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20-MHz, 40-MHz, or 80-MHz mode on the Configuring 802.11a/n APs page. If you change the static RF channel assignment method to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

DCA Channel List

Table 5-118 DCA Channel List Parameters

Parameter	Description	
DCA Channels	DCA channels currently selected.	
Channel list	Channel list you can choose or exclude a channel. **Note** The following extended UNII-2 channels have been removed from the channel list: 100, 104, 108, 112, 116, 132, 136, 140 If you have Cisco Aironet 1520 mesh access points in the -E domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, enable the **Extended UNII-2 channels** option.	
	The channels are as follows: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165,	The default channels are as follows: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
4.9 GHz Channel list	Channel range 1 through 26 that you can choose or include in a channel. These channels are supported on Cisco Aironet 1520 series mesh access points. The 4.9-GHz band is for public safety client access traffic only.	
Extended UNII-2 channels	Extended UNII-2 channels (100, 104, 108, 112, 116, 132, 136, 140) in the channel list that you can enable or disable. The default is unselected.	
India Extended UNII-3 channels	India Extended UNII-3 channels (169 and 173) in the channel list that you can enable or disable. The default is unselected.	

Event Driven RRM

Table 5-119 Event Driven RRM Parameters

Parameter	Description
EDRRM	EDRRM that you can enable or disable. Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference. If enabled, set the sensitivity threshold level (below) at which the RRM is invoked. The default is enabled.
Sensitivity Threshold	Configured sensitivity threshold setting at which the RRM is invoked. The available values are Low, Medium, High, or Custom. When the interference level of the access point raises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity. The default value is Medium.
Custom Sensitivity Threshold	Custom sensitivity threshold that you can enter. This field is displayed if the Sensitivity Threshold is set to custom.
Rogue Contribution	Check box to configure the Rogue Duty Cycle
Rogue Duty-Cycle	Proportion of time (in percentage) during which the interfering device was active. Valid range is 1% to 99%.

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.

Coverage

Choose **WIRELESS > 802.11a/n/ac > RRM > Coverage** to navigate to the **Coverage** page.

This page enables you to configure coverage-hole detection or to specify the Received Signal Strength Indicator (RSSI) parameters.

Coverage Parameters

Table 5-120 RRM Coverage Parameters

Parameter	Description
General	
Enable Coverage Hole Detection	Coverage Hole Detection (CHD) that you can enable or disable. The default is enabled.
Coverage Threshold	
Data RSSI (–60 to –90 dBm)	Data RSSI threshold in dBm. The default is –80.
Voice RSSI (–60 to –90 dBm)	Voice RSSI threshold in dBm. The default is –75.
Min Failed Client Count per AP (1 to 200)	Minimum number of clients on an access point with a RSSI below the coverage threshold. The default is 3.
Coverage exception level per AP (0 to 100%)	Maximum desired percentage of clients on the radio of an access point operating below the desired coverage threshold. The default is 25.
Voice Packet Count (1 to 255 packets)	Specifies the threshold for voice packets.
Data Packet Count (1 to 255 packets)	Specifies the threshold for data packets.
Voice Packet Percentage (1 to 100%)	Failure rate of voice as a percentage. Valid values are from 1 to 100 percent.
Data Packet Percentage (1 to 100%)	Failure rate of data as a percentage. Valid values are from 1 to 100 percent.

General

Choose **WIRELESS > 802.11a/n/ac > RRM > General** to navigate to the **General** page.

This page enables you to specify general radio resource management (RRM) parameters.

Profile Thresholds For Traps

Table 5-121 Profile Threshold Parameters

Parameter	Description
Interference (0 to 100%)	Foreign 802.11a/n/ac interference threshold between 0 and 100 percent. The default is 10.
Clients (1 to 75)	Client threshold between 1 and 75 clients. The default is 12.
Noise (-127 to 0 dBm)	Foreign noise threshold between –127 and 0 dBm. The default is –70.
Utilization (0 to 100%)	802.11a/n/ac RF utilization threshold between 0 and 100 percent. The default is 80.

Noise/Interference/Rogue Monitoring Channels

Table 5-122 Noise/Interference/Rogue Monitoring Channel Parameters

Parameter	Description
Channel List	Country Channels drop-down list. Choose one of the following: • All Channels—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation. • Country Channels (default)—RRM channel scanning occurs only on the data channels in the country of operation. • DCA Channels—RRM channel scanning occurs only on the channel set used by the dynamic channel assignment algorithm, which by default includes all of the nonoverlapping channels allowed in the country of operation. However, you can use the DCA page to specify the channel set to be used by DCA.

Monitor Intervals

Table 5-123 Monitor Interval Parameters

Parameter	Description
Channel Scan Interval	Interval (in seconds) at which the channel scanning occurs. The default is 60. **Note** If your controller supports only OfficeExtend access points, we recommend that you set the channel scan duration to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.
Neighbor Packet Frequency	Interval (in seconds) for how frequently the neighbor packets (messages) are sent, which eventually builds the neighbor list. The default is 60. **Note** If your controller supports only OfficeExtend access points, we recommend that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.
Neighbor Timeout Factor	NDP timeout factor value in minutes. The valid range is 5 minutes to 60 minutes with the default value being 5 minutes. We recommend that you set the timeout factor to 60 minutes. If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes, the Cisco WLC deletes the neighbor from the neighbor list.
Note The range is from 60 to 3600 seconds.	

Click **Set to Factory Default** to set all Auto RF 802.11a parameters to the factory defaults.

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.

Client Roaming

Choose **WIRELESS > 802.11a/n/ac > Client Roaming** to navigate to the **Client Roaming** page.

This page enables you to set seamless client roaming within subnets across access points and virtual LANs (VLANs) under Layer 2 security, and between subnets under Layer 3 security.

CCX-capable clients after association receive a list of neighboring APs, which is used by the clients for selecting the appropriate APs while roaming. This list improves the roaming time. The values for RSSI and Hysteresis are used for fine tuning the roaming behavior and neighbor list.

Table 5-124 802.11a/n/ac Client Roaming Parameters

RF Parameters	Description
Mode	Mode that you can set to either default or custom.
Note The following fields can be changed when you choose Custom mode.	
Minimum RSSI	Minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. The actual value is in dBm (the range is from –50 to –90; the default is –85).
Hysteresis	Signal strength of a neighboring access point to enable a client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points. The actual value is in dB (the range is from 3 to 20; the default is 3).
Scan Threshold	RSSI value from a client's associated access point below which the client must be able to roam to a neighboring access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold. Actual value in dBm (the range is from –50 to –90; the default value is –72).
Transition Time	Maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The actual value is in seconds (the valid range is from 1 to 5; the default value is 5). **Note** For high-speed client roaming applications in outdoor mesh environments, we recommend a setting of 1 second.

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.

Media

This section contains the following topics:

- Voice Parameters, page 5-120
- Video Parameters, page 5-147
- Media Parameters, page 5-124

Voice Parameters

Choose **WIRELESS > 802.11a/n/ac > Media** to navigate to the Media page and click on the **Voice** tab.

This page enables you to set the parameters to adjust the voice quality over the 802.11a/n/ac link.

Guidelines

- Disable all WMM-enabled WLANs before changing voice parameters. Enable the WMM-enabled WLANs again after you have applied the voice settings.
- SIP CAC should only be used for phones that support status code of 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

Table 5-125 802.11a/n/ac Voice CAC Parameters

Parameters	Description
Admission Control (ACM)	Voice CAC that you can enable for this radio band. The default is disable. For more information, see the "Call Admission Control" topic.
CAC Method	CAC method to use. Use **Load Based** to enable channel-based CAC and use **Static** to enable bandwidth-based CAC. The default is load-based CAC. For more information, see the "Load-Based CAC" topic.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for voice applications on this radio band that you can set. Once the client reaches the value specified, the access point rejects new calls on this radio band. The default value is 75%; valid values are from 5% to 85%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming voice clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients. The default value is 6%; valid values are from 0% to 25%.

Table 5-125 802.11a/n/ac Voice CAC Parameters

Parameters	Description
Expedited Bandwidth	Parameter that enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. This setting is disabled by default. For more information, see the "Expedited Bandwidth Request" topic.
SIP CAC Support	SIP CAC support that you can enable. The default is disabled. **Note** To use SIP CAC, you must enable SIP snooping.
Per-call SIP Bandwidth **Note** SIP CAC should only be used for phones that do not support TSPEC-based admission control.	
SIP Codec	Codec name that you want to use on this radio. The available options are G.711, G.729, and User Defined.
SIP Bandwidth (kbps)	Bandwidth in kilobits per second that you want to assign per SIP call on the network. This parameter can be configured only when the SIP Codec selected is User Defined. The default value is 64; valid values are from 8 to 64. **Note** The SIP Bandwidth (Kbps) text box is highlighted only when you select the SIP codec as user-defined. If you choose the SIP codec as G.711, the SIP Bandwidth (Kbps) text box is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (Kbps) text box is set to 8.
SIP Voice Sample Interval (msecs)	Sample interval in milliseconds that the codec must operate. **Note** If SIP CAC is supported and CAC method is static, the Maximum Possible Voice Calls and Maximum Possible Roaming Reserved Calls fields are displayed.
Maximum Possible Voice Calls	Maximum possible voice calls that can be made. This option is displayed if the SIP CAC method is static.
Maximum Possible Roaming Reserved Calls	Maximum possible roaming reserved calls that can be made. This option is displayed if the SIP CAC method is static.
Traffic Streams Metrics	
Metrics Collection	TSM Metrics that you can enable or disable.

Table 5-126 802.11a/n/ac TSM Parameter

Parameters	Description
Metrics collection	TSM collection. For more information, see the "Traffic Stream Metrics" topic.

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion.

CAC enables the client to specify how much bandwidth or shared medium time would be required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

To use CAC with voice applications, follow these steps:

Step 1 Configure the WLAN for Platinum QoS.

Step 2 Enable the Wi-Fi Multimedia (WMM) protocol for the WLAN.

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, CAC does not operate properly.

Unscheduled automatic power save delivery (U-APSD) is enabled automatically when WMM is enabled. U-APSD is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet.

Bandwidth-Based CAC

Bandwidth-based, or static, CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by collocated channel interference. Load-based CAC also covers the additional bandwidth consumption results from PHY and channel impairment.

In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. Load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Expedited Bandwidth Request

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specification (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, the controller attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both static and load-based CAC.

Expedited bandwidth requests are disabled by default. If you configured the WLAN in such a way that it does not support CCX V5 or if you disabled expedited bandwidth requests, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

The following table provides examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 5-127 Expedited Bandwidth Request Parameters

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Static CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	If the voice traffic load is light relative to the data traffic load, then it is admitted. Otherwise, rejected

1. For the static (bandwidth-based) CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.
2. Static CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Traffic Stream Metrics

In a Voice-over-Wireless LAN (VoWLAN) deployment, four variables can affect audio quality: packet latency, packet jitter, packet loss, and roaming time. These variables are referred to as traffic stream metrics (TSM). An administrator can isolate poor voice quality issues by studying these variables.

You can configure TSM on each radio-band (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

Note Access points support TSM in both local and FlexConnect modes.

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.

Video Parameters

Choose **WIRELESS > 802.11a/n/ac > Media** to navigate to the Media page and click the **Video** tab.

This page enables you to set video quality parameters over the 802.11a link.

Note Disable all WMM-enabled WLANs before changing video parameters. Re-enable the WMM-enabled WLANs after you have applied the video settings.

Table 5-128 802.11a/n/ac Video Parameters

Parameters	Description
Admission Control (ACM)	Video CAC for this radio band that you can enable or disable. The default is unselected.
CAC Method	CAC method to use. Use **Load Based** to enable channel-based CAC and use **Static** to enable bandwidth-based CAC. The default is load-based CAC. For more information, see the "Bandwidth-Based CAC" and "Load-Based CAC" topics.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band. The range is from 5 to 85%; however, the maximum RF bandwidth cannot exceed 85% for voice and video. The default value is 0%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming video clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients. The range is from 0 to 25%. The default is 0%.

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.

Media Parameters

Choose **WIRELESS > 802.11a/n/ac > Media** to navigate to the Media page and click the **Media** tab. This page enables you to set voice and video quality parameters over the 802.11a link.

Table 5-129 Media Stream Multicast Direct Parameters

Parameters	Description
Unicast Video Redirect	Unicast video direct that you can enable or disable for this radio. The default is enabled.
Multicast Direct Admission Control	

Table 5-129 Media Stream Multicast Direct Parameters

Parameters	Description
Maximum Media Bandwidth	Percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band. The default value is 85% and the range is from 5 to 85%.
Client Minimum Phy Rate	Minimum transmission data rate in kbps at which the client can operate. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
Maximum Retry Percent	Percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
Media Stream - Multicast Direct Parameters	
Multicast Direct Enable	Multicast direct that you can enable or disable for this radio. The default is enable.
Maximum Streams per Radio	Maximum number of allowed multicast direct streams per radio. The range is from 0 to 20 or you can choose **auto**. The default is **auto**. When the value is **auto**, the controller decides the value based on the radio parameters.
Best Effort QoS Admission	Parameter that you can enable or disable to have the controller admit the media stream in the best radio queue for this radio. The default is disable.

802.11 EDCA Parameters

Choose **WIRELESS > 802.11a/n/ac or 802.11b/g/n > EDCA Parameters** to navigate to the **EDCA Parameters** page.

This page enables you to configure enhanced distributed channel access (EDCA) parameters. EDCA parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

Note You must disable the radio network before configuring the EDCA parameters. To disable the radio network, go to the 802.11a/n/ac page, unselect the **802.11a Network Status** check box, and click **Apply**.

After you configure the EDCA parameter, re-enable the radio network. To re-enable the radio network, go to the 802.11a/n/ac page, select the **802.11a Network Status** check box, and click **Apply**.

Table 5-130 EDCA General Parameters

Parameter	Description
EDCA Profile	Options from the EDCA Profile drop-down box that you can choose: • WMM — (Default) Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network. • Spectralink Voice Priority—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls. • Voice Optimized—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network. • Voice & Video Optimized—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network. **Note** If you deploy video services, admission control (ACM) must be disabled from the Video Parameters page. • Custom Voice—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied. **Note** If you deploy video services, admission control (ACM)must be disabled. • Fastlane—Enables Fastlane EDCA parameters.
Enable Low Latency MAC	MAC optimization for voice that you can choose. This feature enhances voice performance by controlling packet retransmits and aging out voice packets on lightweight access points, improving the number of voice calls serviced for each access point.

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.

DFS (802.11h)

Choose **WIRELESS > 802.11a/n/ac > DFS (802.11h)** to navigate to the 802.11h Global Parameters page. This page enables you to set 802.11h parameters.

Caution Disable the 802.11a/n/ac network before you configure the 802.11h network.

When DFS is enabled, it detects the presence of other devices that use the same radio channel and switches the WLAN operation to another channel if necessary.

Table 5-131 802.11h Parameters

Parameter	Description
Local Power Constraint	Local power constraint (in dBm) that you can specify. This parameter is displayed when Power Constraint is enabled. The range is from 0 to 30 dBm.
Channel Announcement	Channel announcement method in which the access point announces when it is switching to a new channel and the new channel number.
Channel Quite Mode	Channel quite mode that you can enable or disable. This parameter is displayed when Channel Announcement is enabled. The default is unselected.

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.

High Throughput (802.11n)

Choose **WIRELESS > 802.11a/n/ac > High Throughput (802.11n)** to navigate to the **802.11n/ac (5 GHz)/802.11n (2.4 GHz) Throughput** page.

This page enables you to configure 802.11n and 802.11ac support on the network and to enable or disable support of the different modulation coding scheme (MCS) settings. The MCS settings determine the number of spatial streams, modulation, coding rate, and data rate values.

General Parameters

Disabling the 802.11n/ac mode is applicable only to access radios. Backhaul radios always have the 802.11n/ac mode enabled if they are 802.11n capable.

Table 5-132 General Parameters

Parameter	Description
11n Mode	The 802.11n mode that you can enable or disable on the network. The default is enabled. **Note** If you want to disable 802.11n when both 802.11n and 802.11ac are enabled, you must disable 802.11ac first.
11ac Mode	The 802.11ac mode that you can enable or disable on the network. The default is enabled. **Note** You can modify the 802.11ac status only if 802.11n is enabled.

Table 5-132 General Parameters

Parameter	Description
HT MCS Index	Setting for a specific High Throughput (HT) Modulation and Coding Scheme (MCS) index value that you can enable or disable (0 through 23). Data rates are determined according to the MCS index. By default, all are selected.
SS	Signals transmitted by the various antennae are multiplexed by using different spaces within the same spectral channel. These spaces are known as spatial streams. Three spatial streams are available within which you can enable or disable an MCS data rate.
VHT MCS Index (Data Rate)	Setting for a specific Very High Throughput (VHT) MCS that you can enable or disable (0 through 9). By default, all are selected. MCS index 8 and 9 are specific to 802.11ac. Enabling MCS data rate with index 9 automatically enables data rate with MCS index 8. You can enable or disable MCS index 8 only when MCS index 9 is disabled.

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.

CleanAir

To configure the Cisco CleanAir functionality on the 802.11a/n/ac network using the controller GUI, follow these steps:

Step 1 Choose **Wireless** > **802.11a/n/ac > CleanAir** to navigate to the **802.11a/n/ac > CleanAir** page.

Note Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

Step 2 Select the **CleanAir** check box to enable the CleanAir functionality on the 802.11a/n/ac network, or unselect the check box to prevent the controller from detecting spectrum interference. The default is disabled.

Step 3 Select the **Report Interferers** check box to enable the CleanAir system to report any detected sources of interference, or unselect it to prevent the controller from reporting interferers. The default is enabled.

Note Device Security alarms, Event Driven RRM, and Persistence Device Avoidance algorithm will not work if Report Interferers is disabled.

Step 4 Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points associated with the same controller. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5 Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect multiple select text box and any that do not need to be detected appear in the Interferences to Ignore multiple select text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources are detected. The possible sources of interference include the following:

- Canopy—A canopy bridge device
- Continuous Transmitter—A continuous transmitter
- DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
- Jammer—A jamming device
- SuperAG—An 802.11 SuperAG device
- TDD Transmitter—A time division duplex (TDD) transmitter
- Video Camera—A video camera
- WiFi Invalid Channel—A device using nonstandard Wi-Fi channels
- WiFi Inverted Channel—A device using spectrally inverted Wi-Fi signals
- WiMAX Fixed—A WiMAX fixed device (802.11a/n/ac only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n/ac only)

Note Access points associated to the controller send interference reports only for the type of interferer devices that appear in the Interferences to Detect text box. This functionality enables you to filter out a source of interference that you do not want as well as any that may be flooding the network and causing performance problems for the controller or Cisco PI. Filtering allows the system to resume normal performance levels.

Step 6 Configure CleanAir alarms as follows:

- Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselected the check box to disable this feature. The default value is selected.
- If you selected the Enable AQI Trap check box, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default is 35.
- Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality falls below the configured threshold value. The default is 35. The range is from 1 to 100.
- Select the **Enable trap for Unclassified Interferences** check box to enable the traps to be generated for unclassified interferences. Cisco CleanAir can detect and monitor unclassified interferences. Unclassified interferences are interferences that are detected but do not correspond to any of the known interference types.
- Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value between 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.

- Select the **Enable Interference For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect the check box to it to disable this feature. The default value is selected.
- Make sure that any sources of interference that need to trigger interferer alarms appear in the Trap on These Types multiple select text box and any that do not need to trigger interferer alarms appear in the Do Not Trap on These Types text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

  For example, if you want the controller to send an alarm when it detects a jamming device, select the **Enable Interference Type Trap check box** and move the jamming device to the Trap on These Types multiple select box.

Step 7 The Event Driven RRM section displays the current status or the event-driven radio resource management configured on this radio:

- EDRRM—Displays the current status of the spectrum event-driven RRM.
- Sensitivity Threshold—Displays the threshold level at which the event-driven RRM is invoked.

Note If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page appears.

Step 8 Click **Apply** to commit your changes.

802.11b/g/n

This section contains the following topics:

- Network, page 5-130
- RRM, page 5-132
- TPC, page 5-135
- Client Roaming, page 5-143
- Media, page 5-144
- EDCA Parameters, page 5-149
- High Throughput (802.11n), page 5-150
- CleanAir, page 5-151

Network

Choose **WIRELESS > 802.11b/g/n > Network** to navigate to the 802.11b/g/n Global Parameters page.

This page enables you to edit the global parameters of your 802.11b/g/n network.

Table 5-133 802.11 b/g/n Global Parameters

Parameter	Description
General Parameters	
802.11b/g Network Status	802.11b/g/n network parameters that you can enable or disable. The default is enabled.
802.11g Support	802.11g network support. Only available if 802.11b/g network is enabled. The default is enabled. **Note** You must use these commands to enable the 802.11b/g networks after configuring other 802.11b/g parameters. This command only enables the global Cisco WLAN Solution 802.11b/g networks. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, see the Editing WLANs page.
Beacon Period (millisecs)	Rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds. The default is 100 milliseconds.
Short Preamble	Short preamble that you can enable or disable. This parameter must be disabled to optimize this Cisco WLC for some clients, including SpectraLink NetLink Telephones. The default is enabled.
Fragmentation Threshold (bytes)	Fragmentation threshold (in bytes) that you can set in the range 256 to 2346 bytes. The default is 2346.
DTPC Support	DTPC support that you can enable or disable to advertise the transmit power level of the radio in the beacons and the probe responses. The default is unselected.

Table 5-133 802.11 b/g/n Global Parameters

Parameter	Description
Maximum Allowed Clients	Maximum clients allowed per radio. The range is from 1 to 200.
CCX Location Measurement	Mode that enables CAPWAP access points to issue broadcast Radio Measurement Request messages to Cisco Compatible Extensions (V2 and higher) clients. This Measurement Request message is repeated periodically for every SSID over each enabled radio interface based on the specified interval. The response from the client is used to improve accuracy in location measurement. • Mode—Option that you enable if you want CAPWAP access points to issue broadcast Radio Measurement Request messages to Cisco Compatible Extensions (V2 and higher) clients. This Measurement Request message is repeated periodically for every SSID over each enabled radio interface based on the specified interval. The response from the client is used to improve accuracy in the location measurement. The default is unselected. • Interval (seconds)—Specifies the interval of the broadcast Radio Measurement Request messages. • Data Rates—The data rates set here are negotiated between the client and the Cisco WLC. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Cisco WLC, the client may negotiate for the respective rate. Each data rate can also be set to Disabled to match client settings.

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.

RRM

This section contains the following topics:

• RF Grouping, page 5-133

RF Grouping

Choose **WIRELESS > 802.11b/g/n > RRM > RF Grouping** to navigate to the 802.11b > RRM > RF Grouping page.

This page enables you to configure RF grouping characteristics.

Table 5-134 RF Grouping Algorithm Parameters

Parameter	Description
Group Mode	RF grouping that can be configured in any of these modes: • leader **Note** IPv6 is supported for RF grouping in static-leader mode. • auto **Note** IPv6 is not supported for RF grouping in auto mode. It supports only IPv4. • **off**. When the group mode is off, no RF grouping occurs. When a Cisco WLC reboots, it starts by being a standalone leader to itself. In auto mode, the Cisco WLCs form an RF group and elect an auto leader (group mode is auto mode) if the neighboring APs are in the same RF domain. In static mode, the user can configure the static leader by selecting the leader from the group mode drop-down list. The members' management IP addresses and system name are used to request the member to join the static-leader. **Note** A static leader is not allowed to become a member of another Cisco WLC until its mode is **auto**. **Note** A Cisco WLC with a lower priority cannot assume the role of a group leader if a Cisco WLC with a higher priority is available in the RF group. Click **Restart** to restart the RRM RF grouping.
Group Role	Current role of the Cisco WLC.
Group Update Interval	Interval (in seconds) that represent the period with which the grouping algorithm is run by the group leader. The grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. This value is set at 600 seconds.

Table 5-134 RF Grouping Algorithm Parameters

Parameter	Description
Group Leader	Name and IPv4/IPv6 address of the group leader for the group that contains the Cisco WLC. The RF Group Leader can be configured in two ways, as follows: • Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes). • Static Mode—In this mode, the user selects a Cisco WLC as an RF Group leader manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF Group, the reason is indicated. The leader tries to establish a connection with a member every 1 (one) minute if the member has not joined in the previous attempt.
Last Group Update	Elapsed time since the last group update in seconds. This parameter is only valid if this Cisco WLC is a group leader.

Table 5-135 RF Group Member Parameters

Parameter	Description
Controller Name	controller on which the RF group is created.
IP Address (IPv4/IPv6)	IPv4/IPv6 address of the Cisco WLC that belong to a RF group. **Note** IPv6 is supported only for leader type (static-leader) of RF grouping.

You can add a Cisco WLC as a static group member by specifying the Cisco WLC name and the management IP address. Click **Add** to add the Cisco WLC as an RF group member.

When adding RF group members, the leader can allow the number of group members based on the following criteria:

- Maximum number of APs supported: The maximum limit for the number of access points in an RF group is 1000 or twice the maximum number APs licensed on the Cisco WLC.
- Twenty Cisco WLCs: Only 20 Cisco WLCs (including the leader) can be part of an RF group if the sum of the access points of all Cisco WLCs combined is less than or equal to the upper access point limit.

Note If a Cisco WLC cannot be added as a static RF group member, the reason is indicated in parentheses.

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.

TPC

Choose **WIRELESS > 802.11b/g/n > RRM > TPC** to navigate to the **802.11b > RRM > Tx Power Control** page.

This page enables you to edit the transmit power control (TPC) parameters.

Tx Power Level Assignment

The TPC algorithm balances RF power in many diverse RF environments. Automatic power control may not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings only apply to access points that are attached to a controller from which they are configured. The default settings disable this feature, and you should use care when overriding TPC recommendations.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes, enter the maximum and minimum transmit power used by RRM on the Tx Power Control page. The range for these parameters is –10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

This table describes the Tx power level assignment parameters.

Table 5-136 Tx Power Level Assignment Parameters

Parameter	Description
TPC Version	Transmit Power Control version to be chosen from the following options: • Interference Optimal Mode (TPCv2)—For scenarios where voice calls are extensively used. Transmit power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be frequent roaming delays and coverage hole incidents. • Coverage Optimal Mode (TPCv1)—(Default) Offers strong signal coverage and stability. In this mode, power can be kept low to gain extra capacity and reduce interference.
Power Level Assignment Method	Dynamic transmit power assignment has three modes: • Automatic—(Default) The transmit power is periodically updated for all access points that permit this operation. • On Demand—The transmit power is updated when **Invoke Power Update Now** is clicked. • Fixed—No dynamic transmit power assignments occur and values are set to their global default.

Table 5-136 Tx Power Level Assignment Parameters

Parameter	Description
Maximum Power Level Assignment (-10 to 30 dBm)	Maximum power level assignment on this radio. **Note** If you configure a maximum transmit power, RRM does not allow any access point attached to the controller to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually. The range is –10 to 30 dBm. The default is 30.
Minimum Power Level Assignment (–10 to 30 dBm)	Minimum power level assignment on this radio. The range is –10 to 30 dBm. The default is –10.
Power Assignment Leader	Name and IP address of the power level assignment leader.
Last Power Level Assignment	Elapsed time since the last transmit power assignment in seconds.
Power Threshold	Cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value for this parameter varies depending on the TPC version you choose. For TPCv1, the default value is –70 dBm, and for TPCv2, the default value is –67 dBm. The default value can be changed when access points are transmitting at higher (or lower) than desired power levels. The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect. **Note** In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.
Power Neighbor Count	Minimum number of neighbors that an access point must have for the transmit power control algorithm to run.

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.

DCA

Choose **WIRELESS > 802.11b/g/n > RRM > DCA** to navigate to the **802.11b > RRM > Dynamic Channel Assignment** page.

This page enables you to specify the channels that the Dynamic Channel Assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning.

This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Dynamic Channel Assignment Algorithm

Table 5-137 DCA Algorithm Parameters

Parameter	Description
Channel Assignment Method	Dynamic channel assignment has three modes: • Automatic—Mode that periodically updates for all access point that permit this operation. – Interval—How often the DCA algorithm has been configured to run. **Note** If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used. – Anchor Time—The time of day when the DCA algorithm has been configured to start. The range is from 0 to 23 (12:00 a.m. to 11:00 p.m). • Freeze—Mode that causes the controller to update channel assignments when you click **Invoke Channel Update Now**. • OFF—Mode that turns off DCA and sets all access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios. The default is Automatic.
Avoid Foreign AP Interference	Radio Resource Management (RRM) Foreign 802.11 interference-monitoring parameters that you can enable to have Radio Resource Management consider interference from foreign (non-Cisco access point outside the RF/mobility domain) access points when assigning channels to Cisco access points. You can disable this parameter to have Radio Resource Management ignore this interference. The default is unselected. In certain circumstances with significant interference energy (dBm) and load (utilization) from Foreign APs, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the Foreign APs to increase capacity and reduce variability.

Table 5-137 DCA Algorithm Parameters

Parameter	Description
Avoid Cisco AP Load	Radio Resource Management (RRM) Bandwidth-sensing parameter that you can enable controllers to consider the traffic bandwidth used by each access point when assigning channels to access point. You can disable this parameter to have Radio Resource Management ignore this value. The default is unselected. In certain circumstances and with denser deployments, there may not be enough channels to properly create perfect channel reuse. In these circumstances, Radio Resource Management can assign better reuse patterns to those access points that carry more traffic load.
Avoid non-802.11a Noise	Radio Resource Management (RRM) Noise-monitoring parameter that you can enable to have access points avoid channels that have interference from non-Access Point sources, such as microwave ovens or Bluetooth devices. Disable this parameter to have Radio Resource Management ignore this interference. In circumstances with significant interference energy (dBm) from non-802.11 noise sources, Radio Resource Management may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability.
Avoid Persistent Non-WiFi Interference	DCA parameter that you can enable to allow the controller to ignore persistent non-WiFi interference.
Channel Assignment Leader	Name and IP address of the channel assignment leader. Cisco WLAN Solution, mobility groups Cisco WLAN Solution WPS groups. This is the MAC address of the group leader.

Table 5-137 DCA Algorithm Parameters

Parameter	Description
Last Auto Channel Assignment	Last time the Radio Resource Management (RRM) evaluated the current channel assignment on a periodic basis. This parameter does not imply that channels have changed, only that the Radio Resource Management has made an evaluation of the current assignment.
DCA Channel Sensitivity	Configured DCA sensitivity setting. This setting determines how sensitive the DCA algorithm is to environmental changes, such as signal, load, noise, and interference, when determining whether to change channels. The available values are as follows: • Low—The DCA algorithm is not particularly sensitive to environmental changes. • Medium—The DCA algorithm is moderately sensitive to environmental changes. • High—The DCA algorithm is highly sensitive to environmental changes. The default value is Medium. The DCA sensitivity thresholds vary by radio band. **Note** To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

DCA Channel List

Table 5-138 DCA Channel List Parameters

Parameter	Description	
DCA Channels	Channels that are currently selected.	
Select/Channel	Select or exclude a channel.	
	Channels are as follows: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	The default channels are as follows: 1, 6, 11

Event Driven RRM

Table 5-139 Event Driven RRM Parameters

Parameter	Description
EDRRM	Radio Resource Management (RRM) that you can enable or disable to run when a CleanAir enabled access point detects a significant level of interference. The default is unselected. If enabled, set the sensitivity threshold level (below) at which the RRM is invoked.
Sensitivity Threshold	Configured sensitivity threshold setting at which the RRM is invoked. The available values are Low, Medium, High, or Custom. When the interference for the access point rises and the corresponding AQ index falls below the threshold level, RRM initiates a local channel assignment and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity. If you selected the EDRRM sensitivity threshold as custom, you must set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35. The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60. The default value is Medium.
Rogue Contribution	Check box to configure the Rogue Duty Cycle
Rogue Duty-Cycle	Proportion of time (in percentage) during which the interfering device was active. Valid range is 1% to 99%.

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.

Coverage

Choose **WIRELESS > 802.11b/g/n > RRM > Coverage** to navigate to the **802.11b > RRM > Coverage** page.

This page enables you to configure coverage-hole detection or to specify the RSSI parameters.

This table describes the RRM coverage parameters.

Table 5-140 RRM Coverage Parameters

Parameter	Description
General	
Enable Coverage Hole Detection	Coverage Hole Detection (CHD) that you can enable or disable.
Coverage Threshold	
Data RSSI (-60 to -90 dBm)	Minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. The range is from –60 to –90 dBm. The default value is –80 dBm. If the access point receives a packet in the data queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes data RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Voice RSSI (-60 to -90 dBm)	Minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. The range is from –60 to –90 dBm. The default value is –75 dBm. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter, it indicates that a potential coverage hole has been detected. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
Min Failed Client Count per AP (1 to 75)	Minimum number of clients on an access point with a signal-to-noise ratio (SNR) below the coverage threshold. The default value is 3.
Coverage exception level per AP (0 to 100%)	Maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold. The default value is 25.

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.

General

Choose **WIRELESS > 802.11b/g/n > RRM > General** to navigate to the **802.11b > RRM > General** page.

This page enables you to specify general radio resource management (RRM) parameters.

Note The radios for the Cisco OEAP 600 Series access points are controlled through the local GUI on the Cisco OEAP 600 Series access points and not through the controller. It is not possible to control the spectrum channel, power, or disable the radios through the controller because it does not have any effect on the Cisco OEAP 600 Series access points. Therefore, RRM is not supported on the Cisco OEAP 600 Series access points.

Profile Threshold for Traps

Table 5-141 Profile Threshold Parameters

Parameter	Description
Interference (0 to 100%)	Foreign 802.11b/g interference threshold between 0 and 100 percent. The default value is 10.
Clients (1 to 75)	Client threshold between 1 and 75 clients. The default value is 12.
Noise (-127 to 0 dBm)	Foreign noise threshold between –127 and 0 dBm. The default value is –70.
Utilization (0 to 100%)	802.11b/g RF utilization threshold between 0 and 100 percent. The default value is 80.

Noise/Interference/Rogue/CleanAir Monitoring Channels

Table 5-142 Noise/Interference/Rogue/CleanAir Monitoring Channels Parameters

Parameter	Description
Channel List	Country Channels drop-down box that you can choose one of the following: • All Channels—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation. • Country Channels (default)—RRM channel scanning occurs only on the data channels in the country of operation. • DCA Channels—RRM channel scanning occurs only on the channel set used by the dynamic channel assignment (DCA) algorithm, which by default includes all of the nonoverlapping channels allowed in the country of operation. However, you can use the DCA page to specify the channel set to be used by DCA.

Monitor Intervals

Table 5-143 Monitor Interval Parameters

Parameter	Description
Channel Scan Interval	Interval (in seconds) at which the channel scanning occurs. The default value is 180. **Note** If your controller supports only OfficeExtend access points, We recommend that you set the channel scan duration to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.
Neighbor Packet Frequency	Interval (in seconds) for how frequently the access point measures signal strength and how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list. The default value is 60. **Note** If your controller supports only OfficeExtend access points, We recommend that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.
Note The valid interval range is from 60 to 3600 seconds.	

Click **Set to Factory Default** to set all Auto RF 802.11b/g parameters to the factory defaults.

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.

Client Roaming

Choose **WIRELESS > 802.11b/g > Client Roaming** to navigate to the **802.11b > Client Roaming** page. Seamless client roaming within subnets across access points and virtual LANs (VLANs) is supported under Layer 2 security, and between subnets under Layer 3 security.

CCX-capable clients after association receive a list of neighboring APs, which is used by the clients for selecting the appropriate APs while roaming. This improves the roaming time. The values for RSSI and Hysteresis are used for fine tuning the roaming behavior and Neighbor list.

Table 5-144 802.11b/g Client Roaming Parameters

RF Parameters	Description
Mode	Drop-down box: Default or Custom.
Note The following fields can be changed when you select Custom mode.	

Table 5-144 802.11b/g Client Roaming Parameters

RF Parameters	Description
Minimum RSSI	Actual value in dBm (the valid range is from –80 to –90; the default value is –85). This parameter indicates the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.
Hysteresis	Actual value in dB (the valid range is from 2 to 4; the default value is 2). This parameter indicates how strong the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.
Scan Threshold	Actual value in dBm (the valid range is from –70 to –77; the default value is –72). This parameter indicates the RSSI value, from a client's associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
Transition Time	Actual value in seconds (the valid range is from 1 to 10; the default value is 5). **Note** For high-speed client roaming applications in outdoor mesh environments, a setting of 1 second is recommended. This parameter indicates the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.

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.

Media

This section contains the following topics:

- Voice Parameters, page 5-145
- Video Parameters, page 5-147

- Media Parameters, page 5-148

Voice Parameters

Choose **WIRELESS > 802.11b/g > Media** to navigate to the 802.11b (2.4 GHz) > Media pageand click on the **Voice** tab.

This page enables you to set the voice quality parameters over the 802.11 b/g link.

Note Disable all WMM-enabled WLANs prior to changing voice parameters. Reenable the WMM-enabled WLANs after you have applied the voice settings.

CAC Parameters

Table 5-145 802.11b/g/n CAC Parameters

Parameters	Description
Admission Control (ACM)	Voice CAC for this radio band that you can enable or disable. The default value is disabled. For more information, see the "Call Admission Control" topic.
Load-based CAC	Load-based CAC that you can enable or disable. Load-based AC is disabled by default. For more information, see the "Load-Based CAC" topic.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band. Valid values are between 5% to 85%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming voice clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients. The default value is 6%; valid values are between 0% to 25%.
Expedited Bandwidth	Enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. This setting is enabled by default. For more information, see the "Expedited Bandwidth Request" topic.
SIP Codec	Codec name that you want to use on this radio. The available options are G.711, G.729, and User Defined.
SIP Bandwidth (kbps)	Bandwidth in kilobits per second you want to assign per SIP call on the network. This parameter can be configured only when the SIP Codec selected is User Defined.
SIP Voice Sample Interval (msecs)	Sample interval in milliseconds that the codec must operate.

802.11 b/g TSM Parameters

Table 5-146 802.11b/g TSM Parameters

Parameters	Description
Metrics collection	TSM collection that you can enable or disable. The default is unselected. For more information, see the "Traffic Stream Metrics (TSM)" topic.

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion.

CAC enables the client to specify how much bandwidth or shared medium time would be required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

To use CAC with voice applications, do the following:

- Configure the WLAN for Platinum QoS
- Enable the Wi-Fi Multimedia (WMM) protocol for the WLAN

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, CAC does not operate properly.

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Expedited Bandwidth Request

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, the controller attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both static and load-based CAC.

Expedited bandwidth requests are enabled by default. If you configured the WLAN in such a way that it does not support CCX V5 or if you disabled expedited bandwidth requests, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

See the following table for examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 5-147 Expedited Bandwidth Request Parameters

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Static CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

1. For the static (bandwidth-based) CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.
2. Static CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Traffic Stream Metrics (TSM)

In a voice-over-wireless LAN (VoWLAN) deployment, four variables can affect audio quality: packet latency, packet jitter, packet loss, and roaming time. These variables are referred to as TSM. An administrator can isolate poor voice quality issues by studying these variables.

You can configure TSM on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

Note Access points support TSM in both local and FlexConnect modes.

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.

Video Parameters

Choose **WIRELESS > 802.11b/g/n > Media** to navigate to the 802.11b(2.4 GHz) > Media page and click on the **Video** tab.

This page enables you to set the parameters to adjust video quality over an 802.11b/g/n link.

Note Disable all WMM-enabled WLANs prior to changing video parameters. Reenable the WMM-enabled WLANs after you have applied the video settings.

Table 5-148 802.11b/g Video Parameters

Parameters	Description
Admission Control (ACM)	Video CAC for this radio band that you can enable or disable. The default is unselected.
Max RF Bandwidth (%)	Percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band. Valid range is between 5% to 85%; however, the maximum RF bandwidth cannot exceed 100% for voice + video. The default value is 0%.
Reserved Roaming Bandwidth (%)	Percentage of maximum allocated bandwidth reserved for roaming video clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients. The valid range is from 0 to 25%. The default value is 0%.

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.

Media Parameters

Choose **WIRELESS > 802.11b/g/n > Media** to navigate to the 802.11b(2.4 GHz) > Media page and click on the **Media** tab.

This page enables you to set the video quality parameters over an 802.11b/g/n link.

Table 5-149 802.11 b/g/n General Media Parameters

Parameter	Description
Unicast Video Redirect	Enables unicast video redirect. The default value is enabled.

Table 5-150 Multicast Direct Admission Control Parameters

Parameter	Description
Maximum Media Bandwidth (0 - 85%)	Percentage of maximum bandwidth allocated to clients for media applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band. The default value is 85%; valid values are between 0 and 85%.
Client Phy rate	Minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
Maximum Retry Percent	Percentage of the maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

Table 5-151 Media Stream Multicast Direct Parameters

Parameters	Description
Multicast Direct Enable	Multicast direct for this radio. This parameter is enabled by default.
Max Streams per Radio	Maximum number of streams allowed per radio. The range is 0 to 20. The default value is set to auto. If you choose auto, then there is no limit set for the number of client subscriptions.
Max Streams per Client	Maximum number of streams allowed per client. The range is 0 to 20. The default value is set to auto. If you choose auto, then there is no limit set for the number of client subscription.
Best Effort QoS Admission	If enabled, the controller admits the media stream in the best radio queue for this radio. The default is disabled.

EDCA Parameters

Choose **WIRELESS > 802.11b/g/n > EDCA Parameters** to navigate to the **EDCA Parameters** page.

This page enables you to configure enhanced distributed channel access (EDCA) parameters. EDCA parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

Note You must disable the radio network before configuring EDCA parameters. To disable the radio network, go to the 802.11b/g/n page, unselect the **802.11b/g Network Status** check box, and click **Apply**.

After you configure the EDCA parameter, reenable the radio network. To reenable the radio network, go to the 802.11b/g/n page, check the **802.11b/g Network Status** check box, and click **Apply**.

Table 5-152 EDCA General Parameters

Parameter	Description
EDCA Profile	Choose one of the following options from the EDCA Profile drop-down list: • WMM—(Default) Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network. • Spectralink Voice Priority—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls. • Voice Optimized—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network. • Voice & Video Optimized—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network. **Note** If you deploy video services, admission control (ACM) must be disabled.
Enable Low Latency MAC	MAC optimization for voice that you can enable or disable. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, thereby improving the number of voice calls serviced per access point.

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.

High Throughput (802.11n)

Choose **WIRELESS > 802.11b/g/n > High Throughput (802.11n)** to navigate to the **802.11n (2.4 GHz) High Throughput** page.

This page enables you to configure 802.11n support on the network and support of the different Modulation Coding Schemes (MCS) settings. The MCS index determines the number of spatial streams, the modulation, the coding rate, and data rate values.

Table 5-153 802.11n (2.4 GHz) High Throughput Parameters

Parameter	Description
11n Mode	802.11n mode on the network that you can enable or disable. The default is enabled.
MCS (Data Rate) Settings (0 through 23)	Support for a specific MCS that you can enable or disable. By default all MCS data rate settings are enabled.

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.

CleanAir

To configure Cisco CleanAir functionality on the 802.11b/g/n network using the controller GUI, follow these steps:

Step 1 Choose **Wireless > 802.11b/g/n > CleanAir** to navigate to the 802.11b/g/n CleanAir page.

Note Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

Step 2 Select the **CleanAir** check box to enable CleanAir functionality on the 802.11b/g/n network, or unselect it to prevent the controller from detecting spectrum interference. The default is enabled.

Step 3 Select the **Report Interferers** check box to enable the CleanAir system to report any detected sources of interference, or unselect it to prevent the controller from reporting interferers. The default is enabled.

Note Device Security alarms, Event Driven RRM, and Persistence Device Avoidance algorithm will not work if Report Interferers is disabled.

Step 4 Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points associated with the same controller. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times

Step 5 Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect multiple select text box and any that do not need to be detected appear in the Interferences to Ignore multiple select text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources are detected. The possible sources of interference include the following:

- Canopy—A canopy bridge device
- Continuous Transmitter—A continuous transmitter
- DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
- Jammer—A jamming device
- SuperAG—An 802.11 SuperAG device

- TDD Transmitter—A time division duplex (TDD) transmitter
- Video Camera—A video camera
- WiFi Invalid Channel—A device using nonstandard Wi-Fi channels
- WiFi Inverted Channel—A device using spectrally inverted Wi-Fi signals
- WiMAX Fixed—A WiMAX fixed device (802.11a/n/ac only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n/ac only)

Note Access points associated to the controller send interference reports only for the type of interferer devices that appear in the Interferences to Detect text box. This functionality enables you to filter out source of interference that you do not want as well as any that may be flooding the network and causing performance problems for the controller or Cisco PI. Filtering allows the system to resume normal performance levels.

Step 6 Configure CleanAir alarms as follows:

a. Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselect the check box to disable this feature. The default value is selected.

b. If you selected the Enable AQI Trap check box in the step above, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default is 35.

- Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality reaches a threshold value. The default is 35. The valid range is between 1 and 100.
- Select the **Enable trap for Unclassified Interferences** check box to enable the traps to be generated for unclassified interferences. Cisco CleanAir can detect and monitor unclassified interferences. Unclassified interferences are interferences that are detected but do not correspond to any of the known interference types.
- Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value between 1 and 99. The default is 20. This configuration enables traps to be sent at a set threshold.

c. Select the **Enable Interference For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect the check box to disable this feature. The default value is selected.

d. Make sure that any sources of interference that need to trigger interferer alarms appear in the Trap on These Types multiple select text box and any that do not need to trigger interferer alarms appear in the Do Not Trap on These Types text box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

For example, if you want the controller to send an alarm when it detects a jamming device, select the **Enable Interference Type Trap check box** and move the jamming device to the Trap on These Types multiple select box.

Step 7 The Event Driven RRM section displays the current status or the event-driven radio resource management configured on this radio:

- EDRRM—Displays the current status of the spectrum event-driven RRM.
- Sensitivity Threshold—Displays the threshold level at which the event-driven RRM is invoked.

Note If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page appears.

Step 8 Click **Apply** to commit your changes.

Media Stream

This section contains the following topics:

- General, page 5-153
- Media Streams, page 5-154

General

Choose **WIRELESS > Media Stream > General** to navigate to the Media Stream > General page.

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, lost or corrupted packets are not sent and may cause an IP multicast stream to be not viewable.

This page allows you to enable or disable multicast direct support on the network. Additionally, you can also configure an acknowledgment mechanism in which an acknowledgment is sent to clients when the access point receives multicast frames.

Table 5-154 Media Stream General Parameters

Parameter	Description
Multicast Direct Feature	Multicast direct that you can enable or disable. The default is enabled. **Note** Enabling the Multicast feature does not automatically reset the existing client state. You must reset the multicast direct-enabled WLAN and 802.11 networks to clear clients.
Session Message Config	
Session announcement State	Session announcement mechanism to the client. If enabled, clients are informed every time the controller is not able to serve multicast-direct data to the client. The default is unselected.
Session announcement URL	URL where the client can find more information when errors occur during multicast media stream transmission.
Session announcement Email	E-mail ID of the person who can be contacted.

Table 5-154 Media Stream General Parameters

Parameter	Description
Session announcement Phone	Phone number of the person who can be contacted.
Session announcement Note	Reason as to why a particular client cannot be served with a multicast media.

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.

Media Streams

Choose **WIRELESS > Media Stream > Streams** to navigate to the Media Streams page.

This page enables you to list all the multicast media streams configured on the controller.

Table 5-155 Media Stream Parameters

Parameter	Description
Stream Name	Multicast media stream name.
Start IP Address	Starting IP address (IPv4 or IPv6) of the media stream for which the multicast direct feature is enabled.
End IP Address	Ending IP address (IPv4 or IPv6) of the media stream for which the multicast direct feature is enabled.
Operational Status	Operational status of this media stream.

Click **Add New** to configure a new media stream. See the "Configuring a New Media Stream and Enabling the Media Stream" topic.

Click **Delete All** delete the multicast media streams.

Configuring a New Media Stream and Enabling the Media Stream

Step 1 Choose **WIRELESS > Media Stream > Streams** to navugate to the Media Streams page.

Step 2 Click **Add New** to configure a new media stream.

Step 3 Specify the following details for the new stream as follows:

Note The Stream Name, Multicast Destination Start IP Address, and Multicast Destination End IP Address text boxes are mandatory. You must enter information in these text boxes.

- Stream Name—Specifies a unique name to the stream. The stream name can be up to 64 characters.
- Multicast Destination Start IP Address—Specifies the starting IP address (IPv4 or IPv6) of the multicast media stream.

- Multicast Destination End IP Address—Specifies the ending IP address (IPv4 or IPv6) of the multicast media stream.
- Maximum Expected Bandwidth (1 to 35000 Kbps)—Specifies the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 Kbps.

Note We recommend that you use a template to add a media stream to the controller.

Step 4 From the Select from Predefined Templates drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify details about the resource reservation control:

- Very Coarse (below 300 Kbps)
- Coarse (below 500 Kbps)
- Ordinary (below 750 Kbps)
- Low (below 1 Mbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)

Note When you select a template from the drop-down list, the following text boxes under the Resource Reservation Control (RRC) Parameters list their default values that are assigned with the template.

- Average Packet Size (100–1500 bytes)—Specifies the average packet size. The range is 100 to 1500 bytes. The default value is 1200.
- RRC Periodic update—Enables the RRC Periodic update. The RRC Decision message is periodically sent to the access point to update the media stream status. This message is sent at the time of admission and re-RRC calculations. The default is enabled.
- RRC Priority (1–8)—Specifies the priority bit set in the media stream. The priority can be any number from 1 to 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
- Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Select an action from the drop-down list. The possible values are as follows:
  - Drop—Specifies that a stream is dropped on periodic revaluation.
  - Fallback—Specifies that a stream is demoted to best-effort class on periodic reevaluations.

  The default is **Drop**.

Step 5 Click **Apply** to save the configuration changes.

Note To enable the media stream using the controller GUI, perform Step 5 to Step 8.

Note The media stream added needs to be enabled for multicast-direct.

Step 6 Choose **WLANs > WLAN ID** to open the WLANs > Edit page.

Step 7 Choose the **QoS** tab and select **Gold** (Video) from the Quality of Service (QoS) drop-down list.

Step 8 Enable **Multicast Direct**.

Step 9 Click **Apply** to save the configuration changes.

Application Visibility and Control

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1500 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades. AVC recognizes applications and passes this information to other features like QoS, NetFlow, or firewall, which can take action based on the classification

Guidelines

- Only WLANS on local mode access points, or centrally switched on FlexConnect access points can have applications recognized by NBAR.
- Only IPv4 traffic can be analyzed using AVC.

Note AVC is supported only on the Cisco 2500 and 5500 Series Wireless Controllers, Cisco WiSM2, and Cisco Flex 7500 Series Wireless Controllers and Cisco 8500 Series Wireless Controllers,

Choose **WIRELESS > Application Visibility and Control** to navigate to this page. From here, you can choose the following:

- **WIRELESS > Application Visibility and Control > Applications** to view all the supported applications.

  See AVC Applications for more information.
- **WIRELESS > Application Visibility and Control > Profiles** to add new and view existing profiles to the controller.

  See AVC Profiles for more information.

AVC Applications

Choose **WIRELESS > Application Visibility and Control > AVC Applications** to navigate to the **AVC Applications** page, which displays details of all the AVC applications and the Protocol Pack's name, version, and engine version.

Parameter	Description
Application Name	Name of the application.
Application Group	Name of the application group to which the application belongs. The supported application groups are as follows: • Browsing • Business and productivity tools • Email • File sharing • Gaming • Industrial protocols • Instant messaging • Internet privacy • Layer3 over IP • Location-based services • Net admin • Newsgroup • Obsolete • Other • Trojan • Voice and video
Application ID	Unique ID assigned to the application.
Engine ID	Engine ID assigned to each application by the NBAR engine. This ID is used by Prime Assurance Manager (PAM) to display application names.
Selector ID	Selector ID assigned to each application by the NBAR engine. This ID is used by PAM to display application names.

To view all classified applications, choose **Monitor > Applications**, click the WLAN ID to navigate to the **Monitor > Clients** page.

AVC Profiles

Choose **WIRELESS > Application Visibility and Control > AVC Profiles** to navigate to the **AVC Profiles** page.

This page allows you to view the AVC profiles configured on the Cisco WLC.

Guidelines

- You can configure only one AVC profile per WLAN.
- Each AVC profile can have up to 32 rules.
- Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN.
- You can configure up to 16 AVC profiles on a controller.
- You can associate an AVC profile with multiple WLANs.
- AVC profiles do not support AAA Override.
- AVC profiles are applied per WLAN and not per user.

To delete an AVC profile, click the blue arrow adjacent the profile and choose **Remove**.

To add a new AVC profile, click **New**.

Configuring a New AVC Profile and Adding Rules to the Profile

Step 1 Choose **WIRELESS > Application Visibility and Control > AVC Profiles** and click **New** to configure a new AVC profile.

Step 2 Specify the AVC profile name. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Step 3 Click **Apply**. The new AVC profile appears in the list of AVC profiles configured on the Cisco WLC.

Step 4 Click the AVC Profile name to navigate to the AVC Profile > Edit page.

Step 5 Click **Add New Rule** to configure a policy for an application.

Step 6 Specify the following details for the AVC Profile as follows:

Parameter	Description
Application Group	Drop-down list from which you can choose an application group.
Application Name	Drop-down list from which you can choose an application from the chosen application group.

Parameter	Description
Action	Drop-down list from which you can choose the following: • **Drop**—Drops the upstream and downstream packets that correspond to the chosen application. • **Mark**— Marks the upstream and downstream packets that correspond to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you to provide differentiated services based on the QoS levels. If an AVC profile mapped to a WLAN has a rule for MARK action, that application gets precedence according to the QoS profile configured in the AVC rule overriding the QoS profile configured on WLAN. The default action is to permit all applications. NBAR helps identify both high and low priority traffic so that appropriate QoS policy is applied on per WLAN.
DSCP	Packet header code that is used to define QoS across the Internet. The DSCP values are mapped to the following QoS levels: • Platinum (Voice)—Assures a high QoS for Voice over Wireless. • Gold (Video)—Supports the high-quality video applications. • Silver (Best Effort)—Supports the normal bandwidth for clients. • Bronze (Background)— Provides the lowest bandwidth for guest services. You can also choose **Custom** and specify the DSCP value. The range is from 0 to 63.

To edit a rule, click **Add New Rule**, select the application and configure a different action.

Step 7 Click **Apply**.

To apply an AVC profile to all clients in a WLAN, choose **WLANs** and click the profile name to navigate to the **WLANs > Edit** page.

FlexConnect AVC Applications

Choose **WIRELESS > Application Visibility and Control > FlexConnect AVC Applications** to navigate to the **FlexConnect AVC Applications** page, which displays details of all the FlexConnect AVC applications and the Protocol Pack's name, version, and engine version.

Parameter	Description
Application Name	Name of the FlexConnect AVC application.
Application Group	Name of the FlexConnect AVC application group to which the FlexConnect AVC application belongs. The supported FlexConnect AVC application groups are as follows: • Browsing • Business and productivity tools • Email • File sharing • Gaming • Industrial protocols • Instant messaging • Internet privacy • Layer3 over IP • Location-based services • Net admin • Newsgroup • Obsolete • Other • Trojan • Voice and video
Application ID	Unique ID assigned to the FlexConnect AVC application
Engine ID	Engine ID assigned to each application by the NBAR engine. This ID is used by Prime Assurance Manager (PAM) to display FlexConnect AVC application names.
Selector ID	Selector ID assigned to each FlexConnect AVC application by the NBAR engine. This ID is used by PAM to display application names.

To view all classified FlexConnect AVC applications, choose **Monitor > Applications**, click the WLAN ID to navigate to the **Monitor > Clients** page.

FlexConnect AVC Profiles

Choose **WIRELESS > Application Visibility and Control > FlexConnect AVC Profiles** to navigate to the **FlexConnect AVC Profiles** page.

This page allows you to view the FlexConnect AVC profiles configured on the Cisco WLC.

Guidelines

- You can configure only one FlexConnect AVC profile per WLAN.
- Each FlexConnect AVC profile can have up to 32 rules.
- Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN.
- You can configure up to 16 FlexConnect AVC profiles on a controller.
- You can associate an FlexConnect AVC profile with multiple WLANs.
- FlexConnect AVC profiles do not support AAA Override.
- FlexConnect AVC profiles are applied per WLAN and not per user.

To delete a FlexConnect AVC profile, click the blue arrow adjacent the profile and choose **Remove**.

To add a new FlexConnect AVC profile, click **New**.

Configuring a New FlexConnect AVC Profile and Adding Rules to the Profile

Step 1 Choose **WIRELESS > Application Visibility and Control > FlexConnect AVC Profiles** and click **New** to configure a new FlexConnect AVC profile.

Step 2 Specify the FlexConnect AVC profile name. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Step 3 Click **Apply**. The new FlexConnect AVC profile appears in the list of FlexConnect AVC profiles configured on the Cisco WLC.

Step 4 Click the FlexConnect AVC Profile name to navigate to the **FlexConnect AVC Profile > Edit** page.

Step 5 Click **Add New Rule** to configure a policy for an application.

Step 6 Specify the following details for the FlexConnect AVC Profile as follows:

Parameter	Description
Application Group	Drop-down list from which you can choose an application group.

Parameter	Description
Application Name	Drop-down list from which you can choose an application from the chosen application group.
Action	Drop-down list from which you can choose the following: • **Drop**—Drops the upstream and downstream packets that correspond to the chosen application. • **Mark**— Marks the upstream and downstream packets that correspond to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you to provide differentiated services based on the QoS levels. If an AVC profile mapped to a WLAN has a rule for MARK action, that application gets precedence according to the QoS profile configured in the AVC rule overriding the QoS profile configured on WLAN. Packet header code that is used to define QoS across the Internet. The DSCP values are mapped to the following QoS levels: **DSCP (0 to 63)** – **Platinum (Voice)**—Assures a high QoS for Voice over Wireless – **Gold (Video)**—Supports the high-quality video applications – **Silver (Best Effort)**—Supports the normal bandwidth for clients – **Bronze (Background)**—Provides the lowest bandwidth for guest services **Direction**—Bidirectional You can also choose **Custom** and specify the DSCP value. Valid range is 0 to 63. • **Rate-Limit**—Rule to rate-limit packets per application. – **Rate Limit(avg/burst rate)**—To configure the average and burst rates for the application that you want to rate limit. Valid range is 0 to 2147483647 Kbps. The default action is to permit all applications. NBAR helps identify both high and low priority traffic so that appropriate QoS policy is applied on per WLAN.

To edit a rule, click **Add New Rule**, select the application and configure a different action.

Step 7 Click **Apply**.

To apply a FlexConnect AVC profile to all clients in a WLAN, choose **WLANs** and click the profile name to navigate to the **WLANs > Edit** page.

Lync Server

Microsoft Lync server manages services such as voice, video, application sharing and file transfer for clients. Microsoft has an SDN (software-defined network) support, which if subscribed to, sends information with respect to those calls.

The WLC solution subscribes to the Lync messages and apply relevant QoS Policies to active Lync calls for wireless clients, which belong to a given WLC.

For a detailed implementation information, see http://www.cisco.com/c/dam/en/us/products/collateral/wireless/lync.pdf.

Choose **WIRELESS > Lync Server** to navigate to the **Global Lync Server Configuration** page.

Parameter	Description
Lync Server	Check box to enable global Lync SDN.
Port	Text box to specify the port number that the Lync service has to listen to. This number is arbitrary and is not a fixed port. Ensure that the same number is configured on the Lync Server side as well.
Protocol	Two options: • HTTP • HTTPS We recommend that you use HTTPS.

Country

Choose **WIRELESS > Country** to navigate to the Country page.

On this page, select the country code or codes where the Cisco WLC and associated access points are installed and operational. This selection ensures that the listed broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

For more information on configuring country codes, see the Configuring the Country Code topic.

Note Generally, you configure one country code per controller, (the one matching the physical location of the controller and its access points). However, you can configure up to 20 country codes per controller. This multiple-country support enables you to manage access points in various countries from a single controller.

For more information on configuring multiple country codes, see the Multiple Country Codes topic.

Note Both 802.11a/n/ac and 802.11b/g/n networks must be disabled in order to change the country code.

For a complete list of country codes supported per product, refer to this URL:

The currently-supported countries are as follows:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html

- AE (United Arab Emirates)
- AR (Argentina)
- AT (Austria), which allows 802.11a/n/ac and 802.11b/g/n
- AU (Australia), which allows 802.11a and 802.11b
- BE (Belgium), which allows 802.11a and 802.11b/g
- BH (Bahrain)
- BG (Bulgaria)
- BR (Brazil), which allows 802.11a and 802.11b/g
- CA (Canada), which allows 802.11b/g
- CA2 (Canada) DCA excludes UNII-2
- CH (Switzerland and Liechtenstein), which allows 802.11a and 802.11b/g
- CL (Chile)
- CN (China)
- CO (Colombia)
- CY (Cyprus), which allows 802.11a and 802.11b/g
- CZ (Czech Republic), which allows 802.11a and 802.11b
- DE (Germany), which allows 802.11a and 802.11b/g
- DK (Denmark), which allows 802.11a and 802.11b/g
- DO (Dominican Republic)
- EE (Estonia), which allows 802.11a and 802.11b/g
- ES (Spain), which allows 802.11a and 802.11b/g
- FI (Finland), which allows 802.11a and 802.11b/g
- FR (France), which allows 802.11a and 802.11b/g
- GB (United Kingdom), which allows 802.11a and 802.11b/g
- GI (Gibraltar)
- GR (Greece), which allows 802.11b/g
- HK (Hong Kong), which allows 802.11a and 802.11b/g
- HU (Hungary), which allows 802.11a and 802.11b/g
- ID (Indonesia)
- IE (Ireland), which allows 802.11a and 802.11b/g

- IL (Israel), which allows 802.11a and 802.11b/g
- ILO (Israel Outdoors), which allows 802.11a and 802.11b/g
- IN (India), which allows 802.11a and 802.11b
- IQ (Iraq)
- IS (Iceland), which allows 802.11a and 802.11b/g
- IT (Italy), which allows 802.11a and 802.11b/g
- JP (Japan), which allows 802.11a and 802.11b/g
- J2 (Japan 2 P)
- J3 (Japan 3 U)
- KE (Korea Extended K)
- KR (Republic of Korea), which allows 802.11a and 802.11b/g
- KW (Kuwait)
- LI (Liechtenstein)
- LT (Lithuania), which allows 802.11a and 802.11b/g
- LU (Luxembourg), which allows 802.11a and 802.11b/g
- LV (Latvia), which allows 802.11b/g
- MC (Monaco)
- ME (Montenegro)
- MK (Macedonia)
- MT (Malta)
- MX (Mexico)
- MY (Malaysia), which allows 802.11b/g
- NL (Netherlands), which allows 802.11a and 802.11b/g
- NO (Norway), which allows 802.11a and 802.11b/g
- NZ (New Zealand), which allows 802.11a and 802.11b/g
- OM (Oman)
- PA (Panama)
- PE (Peru)
- PH (Philippines), which allows 802.11a and 802.11b
- PH2 (Philippines (DCA excludes UNII))
- PK (Pakistan)
- PL (Poland), which allows 802.11a and 802.11b/g
- PR (Puerto Rico)
- PT (Portugal), which allows 802.11a and 802.11b/g
- PY (Paraguay)
- QA (Qatar)
- RS (Serbia)
- RU (Russian Federation)

- RO (Romania)
- SA (Saudi Arabia)
- SE (Sweden), which allows 802.11a and 802.11b/g
- SG (Singapore), which allows 802.11a and 802.11b/g
- SI (Slovenia), which allows 802.11a and 802.11b/g
- SK (Slovak Republic), which allows 802.11a and 802.11b/g
- TH (Thailand), which allows 802.11b/g
- TN (Tunisia)
- TR (Turkey)
- TW (Taiwan), which allows 802.11a and 802.11b/g
- UA (Ukraine)
- US (United States of America), which allows an 802.11b/g operation, and 802.11a Low, Medium, and High bands
- USE (USA), which allows 802.11a and 802.11b/g
- USL (USA Low), which allows an 802.11b/g operation, and 802.11a Low and Medium bands. (Used for legacy 802.11a interface cards that do not support 802.11a High band)
- USX (USA Extended), which allows 802.11a and 802.11b/g
- VE (Venezuela)
- ZA (South Africa), which allows 802.11a and 802.11b/g

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.

Configuring the Country Code

Note Disable both the 802.11a/n/ac and 802.11b/g/n networks to change the country code.

To configure the country code using the GUI, follow these steps:

Step 1 Disable the 802.11a/n/ac and 802.11b/g/n networks as follows:

a. Click **Wireless > 802.11a/n/ac > Network**.

b. Unselect the **802.11a Network Status Enabled** check box.

c. Click **Apply** to commit your changes.

d. Click **Wireless > 802.11b/g/n > Network**.

e. Unselect the **802.11b/g Network Status Enabled** check box.

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

Step 2 Click **Wireless > Country** to access the Country page.

Step 3 Select the check box for the country where your access point is installed.

Step 4 Click **Apply** to commit your changes.

Step 5 Reenable the 802.11a/n/ac and 802.11b/g/n networks that you disabled in Step 1.

Step 6 Click **Save Configuration** to save your settings.

Multiple Country Codes

You can configure up to 20 country codes for each controller. This multiple-country support enables you to manage access points in various countries from a single controller.

Guidelines

Follow these guidelines when configuring multiple country codes:

- The multiple-country feature is not supported for use with Cisco Aironet 1500 series mesh access points.
- When multiple countries are configured and the radio resource management (RRM) auto-RF feature is enabled, the auto-RF feature is limited to only the channels that are legal in all configured countries and to the lowest power level common to all configured countries. The access points are always able to use all legal frequencies but uncommon channels can only be assigned manually.
- The access point can only operate on the channels for the countries that they are designed for.

Note If an access point is set to a higher legal power level or is configured manually, the power level is limited only by the particular country to which that access point is assigned.

- When multiple countries are configured, the 802.11a/n/ac network is disabled for all the countries if any country does not support the 802.11a radio, or there are no common channels on the 802.11a radio.
- The country list configured on the RF group leader determines what channels the members would operate on. This is independent of what countries have been configured on the RF Group members.

Configuring Multiple Country Codes

Note Disable both the 802.11a/n/ac and 802.11b/g/n networks to change the country code.

To configure country codes using the GUI, follow these steps:

Step 1 Disable the 802.11a/n/ac and 802.11b/g/n networks as follows:

a. Click **Wireless > 802.11a/n/ac > Network**.

b. Unselect the **802.11a Network Status Enabled** check box.

c. Click **Apply** to commit your changes.

d. Click **Wireless > 802.11b/g/n > Network**.

e. Unselect the **802.11b/g Network Status Enabled** check box.

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

Step 2 Choose **Wireless > Country** to access the Country page.

Step 3 Choose the check box for each country where your access points are installed.

Step 4 If you selected more than one check box in Step 3, a message appears indicating that RRM channels and power levels are limited to common channels and power levels. Click **OK** to continue or **Cancel** to cancel the operation.

Step 5 Click **Apply** to commit your changes.

Step 6 Re-enable the 802.11a/n/ac and 802.11b/g/n networks if you did not re-enable them in Step 1.

Step 7 Click **Save Configuration** to save your settings.

Changing Default Country Codes

To see the default country chosen for each access point and to choose a different country if necessary, follow these steps:

Note If you remove a country code from the configuration, any access points that are assigned to the deleted country are reassigned to one of the remaining countries if possible.

Step 1 Click **Wireless > Access Points > All APs** to access the All APs page.

Step 2 Click the link for the desired access point.

The default country for the access point appears in the Country Code drop-down list. The drop-down list contains only those country codes that are compatible with the regulatory domain of at least one of the access point's radios.

Step 3 If the access point is installed in a country other than the one shown, choose the correct country from the drop-down list.

Step 4 Click **Apply** to commit your changes.

Step 5 Repeat Step 2 through Step 4 to assign all the access points that are joined to the controller of a specific country.

Step 6 Re-enable the 802.11a/n/ac and 802.11b/g/n networks.

Step 7 Click **Save Configuration** to save your settings.

Timers

Choose **WIRELESS > Timers** to navigate to the Timers page. This page enables you to view the timeout parameter.

Table 5-156 Timer Parameters

Timer	Description
802.11 Authentication Response Timeout	802.11 authentication response timeout that is between 5 and 60 seconds. The default is 10 seconds.

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.

NetFlow

Choose **WIRELESS > Netflow** to navigate to the Netflow page.

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing. This protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements. NBAR exports traffic data to a NetFlow Collector.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter. Configuring an exporter on the controller enables the collection of application statistics for export to an external monitor.

In the controller you can choose the following:

- **WIRELESS > Netflow > Monitor** to configure or view details of the NetFlow monitor and records.

  See Netflow Monitor for more information.
- **WIRELESS > Netflow > Exporter** to view details of the NetFlow exporters.

  See Netflow Exporter for more information.

Netflow Monitor

Choose **WIRELESS > Netflow > Monitor** to navigate to the Monitor page. NetFlow record monitoring and export are used for integration with Cisco Prime Infrastructure or any NetFlow analysis tool.

This table describes the NetFlow monitor parameters.

Table 5-157 NetFlow Monitor Parameters

Parameter	Description
Monitor Name	Name of the NetFlow monitor. The monitor name can be up to 127 case-sensitive, alphanumeric characters. You cannot include spaces within a monitor name. You can configure only one monitor in the controller.
Record Name	Name of the NetFlow record. A NetFlow record in the controller contains the following information about the traffic in a given flow: • Client MAC address • Client source IP address • WLAN ID • Application ID • Incoming bytes of data • Outgoing bytes of data • Incoming packets • Outgoing packets • Incoming DSCP • Outgoing DSCP • Name of the last AP
Exporter Name	Name of the exporter. You cannot include spaces within an exporter name. You can configure only one monitor in the controller.
Exporter IP	IP address of the collector.
Port	UDP port through which the NetFlow record is exported from the controller.

Click **New** to add a new NetFlow monitor.

Netflow Exporter

Choose **WIRELESS > Netflow > Exporter** to navigate to the Exporter page.

Table 5-158 NetFlow Exporter Parameters

Parameter	Description
Exporter Name	Name of the exporter. You can configure only one exporter on the controller. You cannot include spaces within an exporter name.
Exporter IP	IP address of the exporter.
Port Number	UDP port through which the NetFlow record is exported.

QoS

This section contains the following topics:

- Profiles, page 5-171
- Roles, page 5-173
- QoS Map, page 5-174

Profiles

Choose **WIRELESS > QoS > Profiles** to navigate to the QoS Profiles page. This page enables you to view the quality of service (QoS) settings.

Table 5-159 QoS Profiles

Parameter	Description
Profile Name	Name of the QoS profile.
Description	Platinum (Voice)—Assures a high quality of service for Voice over Wireless. Gold (Video)—Supports high-quality video applications. Silver (Best Effort)—Supports the normal bandwidth for clients. This setting is the default. Bronze (Background)—Provides the lowest bandwidth for guest services. VoIP clients should be set to Platinum while low-bandwidth data clients can be set to Silver or Bronze.

Click the profile name to go to the Editing QoS Profile page and specify how much bandwidth a client is allocated in the network for that QoS profile.

Editing QoS Profile

Choose **WIRELESS > QoS > Profiles** and then click the profile name to navigate to the Edit QoS Profile page.

The top of the main page lists the selected quality of service (QoS) profile name.

Table 5-160 QoS Profile Parameters

Parameter	Description
QoS Profile Name	Name of the QoS profile.
Description	User-defined description for this QoS profile.
Per-User Bandwidth and Per-SSID Bandwidth Contracts	
Note 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.	
Average Data Rate	User-defined average data rate (kbps) for non-UDP traffic. Valid values are from 0 to 60,000; the default is 0 (OFF).

Table 5-160 QoS Profile Parameters

Parameter	Description
Burst Data Rate	User-defined peak data rate (kbps) for non-UDP traffic. Valid values are from 0 to 60,000; the default is 0 (OFF).
Average Real-Time Rate	User-defined average data rate (kbps) for UDP traffic. Valid values are from 0 to 60,000; the default is 0 (OFF).
Burst Real-Time Rate	User-defined peak data rate (kbps) for UDP traffic. Valid values are from 0 to 60,000; the default is 0 (OFF).
WLAN QoS Parameters	
Maximum Priority	Maximum QoS priority for the WLAN of the profile. Available options are as follows: • besteffort • background • video • voice
Unicast Default Priority	Default QoS priority of unicast packet for the WLAN of the profile. Available options are as follows: • besteffort • background • video • voice
Multicast Default Priority	Default QoS priority of multicast packet for the WLAN of the profile. Available options are as follows: • besteffort • background • video • voice
Wired QoS Protocol	
Protocol Type	Protocol type. Choose **802.1P** to activate 802.1P Priority Tags, or choose **None** to deactivate 802.1P Priority Tags (default).
802.1P Tag	802.1P priority tag for the wired connection that is used for traffic and CAPWAP packets. Valid values are from 0 to 7. The default values are 1 for Bronze, 3 for Silver, 4 for Gold, and 6 for Platinum.

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.

Click **Reset to defaults** to reset the parameters to the factory default.

Roles

Choose **WIRELESS > QoS > Roles** to navigate to the QoS Roles for Guest Users page.

This page enables you to view the quality of service (QoS) roles for guest users.

Choose **New** to display the Creating New QoS Roles page and to create a new QoS role.

Click the role name to display the Editing QoS Role Data Rates page and specify how much bandwidth a wired guest user is allocated in the network for that QoS role.

Note After you create the QoS role for guest user, you can assign a role to a guest user from the Local Net Users page.

To delete a role, click the blue arrow adjacent the desired access point and choose **Remove**.

To add a new role, click **New**.

Creating New QoS Roles

Choose **WIRELESS > QoS > Roles** and then click **New** to navigate to the QoS Role Name > New page.

This page enables you to create quality of service roles for guest users. Click the profile name to go to the Editing QoS Role Data Rates page and edit the QoS role parameters.

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.

Editing QoS Role Data Rates

Choose **WIRELESS > QoS > Roles**, and then click the role name to navigate to the Edit QoS Role data rates page.

This page enables you to specify bandwidth limits for guest users of different roles. The top of the main page lists the selected role name.

Table 5-161 QoS Role Parameters

Parameter	Description
Note When you set the Per-User Bandwidth Contracts parameters to 0 (OFF), the traffic allowed is unlimited and is restricted only by other 802.11 limitations.	
Average Data Rate	Operator-defined average data rate (kbps) for non-UDP traffic. Valid values are from 0 to 60,000; the default value is 0 (OFF).
Burst Data Rate	Operator-defined peak data rate (kbps) for non-UDP traffic. Valid values are from 0 to 60,000; the default value is 0 (OFF).
Average Real-Time Rate	Operator-defined average data rate (kbps) for UDP traffic. Valid values are from 0 to 60,000; the default value is 0 (OFF).
Burst Real-Time Rate	Operator-defined peak data rate (kbps) for UDP traffic. Valid values are from 0 to 60,000; the default value is 0 (OFF).

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.

QoS Map

Choose **WIRELESS > QoS > QoS Map** to navigate to the **QoS Map Config** page.

The QoS Mapping feature maintains the QoS policies in situations where appropriate QoS markings that match the application type are not marked by clients or applications. The administrator gets to map the differentiated services code point (DSCP) to user priority (UP) values and also is able to mark from UP to DSCP in a Cisco WLC.

With QoS in enabled state, the QoS feature is advertised by the AP in the frame. The map is propagated through a frame to a compatible device when it associates or re-associates with the network.

With QoS in disabled state, the default map is propagated to the AP and the clients from Cisco WLC.

Table 5-162 QoS Map Parameters

Parameter	Description
QoS Map	Drop-down list from which you can set the status of QoS Map: • Enable • Disable • Default Setting QoS Map to Default resets the UP to DSCP and DSCP to UP table values to default values (255). This also adds DSCP UP exceptions if not present previously.
Trust DSCP Upstream	Check box that you can check to enable marking of the upstream packets using the client DSCP.
UP to DSCP Map To set the DSCP range	
User Priority	Drop-down list from which you can choose the User Priority.
DSCP Default	The default value of DSCP.
DSCP Start	The starting value of the DSCP range
DSCP End	The ending value of the DSCP range
Add DSCP Exception	
DSCP Exception	Set an exception value for DSCP. This is required if a client marks DSCP with an unusual value.
User Priority	Drop-down list from which you can choose the user priority.

Security Tab

The Security tab on the menu bar enables you to configure and set security policies on your Cisco WLC. Use the Selector area to access specific security parameters. Making this selection from the menu bar opens the RADIUS Authentication Servers page.

General (AAA)

Choose **SECURITY > AAA > General** to navigate to the General page.

This page enables you to specify the maximum number of local network users that can exist on the local user database:

- Maximum Local Database entries—Enables you to enter a value for the maximum number of local network users that can be added to the local user database the next time that the Cisco WLC reboots. The currently configured value appears in parentheses to the right of the field. The valid range is from 512 to 2048, and the default setting is 2048.
- Number of entries, already used—Displays the number of entries currently in the database.
- Mgmt User Re-auth Interval—Enables you to enter a value for the time interval in seconds to re-authenticate before the user active session is terminated. The valid range is from 0 to 300 seconds and the default setting is 0.

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.

RADIUS Authentication Servers

Choose **SECURITY > AAA > RADIUS > Authentication** to navigate to the RADIUS Authentication Servers page.

This page displays RADIUS server information for your configured RADIUS server and enables you to edit the Call Station ID Type:

- Auth Called Station ID Type— The Call Station ID Type is applicable only for non-802.1X authentication. The different Call Station ID types are as follows:
  - IP address
  - System MAC address
  - AP MAC address:SSID

  - AP MAC Address
  - AP Name
  - AP Name: SSID
  - AP Group
  - Flex Group
  - AP Location
  - VLAN ID
  - AP Eth MAC Address
  - AP Eth MAC Address:SSID
  - AP Label MAC Address
  - AP Label MAC Address:SSID
- Use AES KeyWrap—RADIUS-to-Cisco WLC key transport using AES KeyWrap protection. The AES KeyWrap is required for FIPS customers. All defined RADIUS must have AES KeyWrap keys defined.
- MAC Delimiter—Delimiter that you can use when you specify the MAC address. The available options are as follows:
  - Colon
  - Hyphen
  - Single Hyphen
  - No Delimiter
- Network User—Network user authentication check box. If this option is enabled, this entry is considered as the network user RADIUS authenticating server entry. If you did not set the RADIUS server entry on the WLAN configuration (**WLANs > Edit > Security > AAA Servers**), you must enable this option for network users.
- Management—Management authentication check box. If this option is enabled, this entry is considered as the management RADIUS authenticating server entry. If you enable this option, authentication requests go to the RADIUS server.
- Server Index—RADIUS server index. The Cisco WLC tries Index 1 first, and then Index 2 and so on, in an ascending order. This value should be 1 if your network is using only one authentication server.
- Server Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—Communication port number for the interface protocols. The default is 1812.
- Tunnel Proxy—Check box to enable or disable AAA proxy on an EoGRE tunnel profile.
- IPSec—Read-only field. Displays the IPsec mechanism. If this option is enabled, the IP Security Parameters fields are also displayed.
- Admin Status—Whether the RADIUS authentication server is enabled or disabled.

Click the server index number to open the Updating RADIUS Authentication Servers page.

To delete an existing RADIUS authentication server, click the blue arrow adjacent the desired access point and choose your cursor over the blue drop-down arrow and choose **Remove**.

To send ping packets to the RADIUS server to verify that you have a working connection between the Cisco WLC and the RADIUS server, click the blue arrow adjacent the desired server and choose **Ping**.

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.

Click **New** to add a new RADIUS authentication server (For more information, see Adding RADIUS Authentication Servers).

Adding RADIUS Authentication Servers

Choose **SECURITY > AAA > RADIUS > Authentication** and then click **New** to navigate to the RADIUS Authentication Servers > New page.

This page enables you to add a new RADIUS server:

- Server Index (Priority)—Index of the RADIUS server. The Cisco WLC tries Index 1 first, and then Index 2 through 17, in an ascending order. Set the server index to 1 if your network is using only one authentication server.

Note You can have a maximum of 17 RADIUS authenticating server entries for a single WLAN.

- Server IP Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.
- Apply Cisco ISE Default settings—Reset to Default Cisco ISE values.
- Key Wrap—Check box that you can select to enable the following AES KeyWrap keys:
  - Key Wrap Format—ASCII or hexadecimal.

  Note FIPS customers must enter keys using hexadecimal notation.

  - Key Encryption Key (KEK)—128-bit (16-byte) AES KeyWrap Key Encryption Key.
  - Message Authentication Code Key (MACK)—160-bit (20-byte) AES KeyWrap Message Authentication Code Key.
- Port Number—Communication port number for the interface protocols.

Note Do not assign the port number that is used by another application. Use the default (1812) or any other port unused by any other application.

- Server Status—RADIUS authentication server that you enable or disable.
- Support for CoA—You can enable or disable Change of Authorization (CoA) which is an extension to the RADIUS protocol. It allows dynamic changes to a user session including support for disconnecting users and changing authorizations applicable to a user session (support for Disconnect and CoA messages). Disconnect messages cause a user session to be terminated immediately; CoA messages modify session authorization attributes such as data filters.
- Server Timeout—Time in seconds after which the RADIUS authentication request times out and a retransmission is taken up by the Cisco WLC. You can specify a value between 2 to 30 seconds.

- Network User—Network user authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user. If you did not set the RADIUS server entry on the WLAN configuration (**WLANs > Edit > Security > AAA Servers**), you must enable this option for network users.
- Management—Management authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user. If you enable this option, authentication requests go to the RADIUS server.
- IPsec—Check box that allows you to enable or disable the IP Security mechanism. If you enable this option, the IP Security Parameters fields are displayed.

Note The IPsec option is displayed only if a crypto card is installed on the Cisco WLC.

Note IPsec does not support IPv6. Use this only if you have used IPv4 for Server IP Address.

- IPsec Authentication: Set the IP security authentication protocol to be used. Options are as follows:
  - HMAC-SHA1
  - HMAC-MD5

    Message Authentication Codes (MACs) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions. HMAC can be used with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA-1 are two constructs of the HMAC using the MD5 hash function and the SHA-1#hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.
- IPsec Encryption—IP security encryption mechanism to be used. Options are as follows:
  - DES —Data Encryption Standard that uses a private data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
  - Triple DES—Data Encryption Standard that applies three keys in succession.
  - AES CBS—Advanced Encryption Standard that uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses 128 bit data path in Cipher Clock Chaining (CBC) mode.
- IKE Phase 1: Internet Key Exchange protocol (IKE). Options are as follows:
  - Aggressive
  - Main

    IKE Phase-1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets, with a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.
- Lifetime (seconds): Set the timeout interval for the session expiry. The default is 28800 seconds.
- IKE Diffie Hellman Group: Set the IKE Diffie Hellman Group. The options are as follows:
  - Group 1 (768 bits)
  - Group 2 (1024 bits)
  - Group 5 (1536 bits)

Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.

Although all the three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 keys might occur slightly faster because of their smaller prime number size.

– Group 14 (2048 bits)

Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.

Although all the four groups provide security from conventional attacks, Group 14 is considered most secure because of its larger key size. However, computations involving Group 1, Group 2, and Group 5 keys might occur slightly faster because of their smaller prime number size. The default value is Group 1.

- Auth Method—IPsec authentication method that can be PSK or Certificate.Shared Secret Format—Format of the shared secret that you set to either ASCII of Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.

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.

Updating RADIUS Authentication Servers

Choose **SECURITY > AAA > RADIUS > Authentication** and click on a link in the Server Index column to update RADIUS authentication servers.

This page enables you to change the RADIUS Authentication parameters on an existing RADIUS server. See Adding RADIUS Authentication Servers.

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.

RADIUS Accounting Servers

Choose **SECURITY > AAA > RADIUS > Accounting** to navigate to the RADIUS Accounting Servers page.

This page displays RADIUS information for your existing RADIUS server.

- Network User—Network user authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user. The default is unselected.
- Server Index—The RADIUS server index. The Cisco WLC tries Index 1 first, and then Index 2 through 17, in an ascending order. Set the server index to 1 if your network is using only one accounting server.

Note You can configure a maximum of 17 RADIUS accounting server entries for a single WLAN.

- Server Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—Controller port number for the interface protocols.

- Tunnel Proxy—Check box to enable or disable AAA proxy on an EoGRE tunnel profile.
- IPsec—Read-only field. Displays the status of the IPsec mechanism. If this option is enabled, the IP Security Parameters fields are also be displayed.
- Admin Status—Whether the RADIUS accounting server is enabled or disabled.

Click the server index number to update the RADIUS accounting servers (see Editing RADIUS Accounting Servers).

Click the blue arrow adjacent the desired server and choose **Remove** to delete an existing RADIUS accounting server.

Click the blue arrow adjacent the desired server and choose **Ping** to send ping packets to the RADIUS server to verify that you have a working connection between the Cisco WLC and the RADIUS server.

Click **New** to add a new RADIUS accounting server (For more information, see Adding RADIUS Accounting Servers).

Adding RADIUS Accounting Servers

Choose **SECURITY > AAA > RADIUS > Accounting** and then click **New** to navigate to the RADIUS Accounting Servers > New page.

This page enables you to add a new RADIUS server:

- Server Index (Priority)—Index of the RADIUS server. The Cisco WLC tries Index 1 first, and then Index 2 through 17, in an ascending order. Set to 1 if your network is using only one accounting server.
- Server IP Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII of Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.
- Port Number—Port number for the interface protocols.

Note Do not assign the port number to one that is used by another application. Use the default (1813) or any other port unused by any other application.

- Server Status—RADIUS accounting server that you enable or disable.
- Server Timeout—Time in seconds after which the RADIUS authentication request times out and a retransmission is taken up by the Cisco WLC. You can specify a value between 2 to 30 seconds.
- Network User—Network user authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
- IPSec—Check box that you can select to enable or disable the IP Security mechanism. If you enable this option, the IP Security Parameters fields are displayed.

Note IPSec does not support IPv6. Use this only if you have used IPv4 for Server IP Address.

- IPSec Authentication: Set the IP security authentication protocol to be used. Options are as follows:
  - HMAC-SHA1

  - MAC-MD5
  - None

    Message Authentication Codes (MACs) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions. HMAC can be used with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA-1 are two constructs of the HMAC using the MD5 hash function and the SHA-1#hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

- IPsec Encryption—IP security encryption mechanism. Options are as follows:
  - DES—Data Encryption Standard that uses a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
  - Triple DES—Data Encryption Standard that applies three keys in succession.
  - AES 128 CBC—Advanced Encryption Standard that uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses 128-bit data path in Cipher Clock Chaining (CBC) mode.
- IKE Authentication: (Display Only Field).
- IKE (Internet Key Exchange protocol) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.
- IKE Phase 1: Set the Internet Key Exchange protocol (IKE). Options are as follows:
  - Aggressive
  - Main

    IKE Phase-1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets, with a slightly faster connection establishment, at the cost of transmitting the identities of the security gateways in the clear.
- Lifetime (seconds): Timeout interval for the session expiry. The default is 28800 seconds.
- IKE Diffie Hellman Group—Options are as follows:
  - Group 1 (768 bits)
  - Group 2 (1024 bits)
  - Group 5 (1536 bits)
  - Group 14 (2048 bits)

    Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.

    Although all the four groups provide security from conventional attacks, Group 14 is considered most secure because of its larger key size. However, computations involving Group 1, Group 2, and Group 5 keys might occur slightly faster because of their smaller prime number size.
- Auth Method—IPsec authentication method that can be PSK or Certificate.
- Shared Secret Format—Format of the shared secret that you set to either ASCII of Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.

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.

Editing RADIUS Accounting Servers

Choose **SECURITY > AAA > RADIUS > Accounting** and then click **Edit** to navigate to the RADIUS Accounting Servers > Edit page.

This page enables you to change the RADIUS accounting parameters on an existing RADIUS server. for more information about the parameters, see Adding RADIUS Accounting Servers:

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.

RADIUS Fallback Parameters

Choose **SECURITY > AAA > RADIUS > Fallback** to navigate to the RADIUS > Fallback Parameters page.

If the primary RADIUS server (for example, Index 1) is unavailable, the Cisco WLC switches to the next RADIUS server (for example, Index 2). By default, when the RADIUS server configured as Index 1 becomes available again, the current RADIUS server remains the primary server.

You can configure the RADIUS server fallback behavior to specify which RADIUS server is the primary server. This table describes the RADIUS fallback parameters.

Table 6-1 RADIUS Fallback Parameters

Parameter	Description
Fallback Mode	Specify the RADIUS server fallback mode: • Active—Specifies that the Cisco WLC will revert to a server with a lower server index from the backup servers by sending RADIUS probe messages to determine whether a server that has been marked as inactive is back online. The Cisco WLC ignores all inactive servers for all active RADIUS requests. • Passive—Specifies that the Cisco WLC will revert to a server with a lower server index from the backup servers without using probe messages. The Cisco WLC ignores all inactive servers for a period of time and then retries later when a RADIUS message needs to be sent. • Off—(Default) Disable server fallback.
Username	Enter the name to be sent in the inactive server probes, up to 16 alphanumeric characters. The default value is cisco-probe.
Interval in sec	Enter the probe interval (when using Active mode) or inactive time (when using Passive mode) in seconds. Valid values are from 180 to 3600; the default value is 300.

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.

RADIUS DNS Parameters

Choose **SECURITY > AAA > RADIUS > DNS** to navigate to the RADIUS DNS Parameters page.

This page allows Cisco WLC to retrieve the RADIUS IP information from a DNS server. The DNS server is queried at regular intervals for updates. The Cisco WLC also runs the query if you manually change the DNS server list, or if one of the servers timeouts. As the DNS list overrides the static list, all manual AAA configurations on the WLAN will stop functioning as soon as the global server list gets populated from the DNS server. DNS AAA is also valid for FlexConnect AP clients using central authentication.

Note RADIUS DNS is not supported for FlexConnect AP groups and FlexConnect clients with local switching.

Note DNS does not support IPv6.

Table 6-2 DNS Parameters

Parameter	Description
DNS Query	Check box to enable the Cisco WLC to retrieve the RADIUS IP information from a DNS server. The default is disabled state. **Note** When you enable the DNS query, the static configurations will be overridden. The DNS list overrides the static AAA list.
Port Number	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port. **Note** The accounting port is derived from the authentication port.
Secret Format	Format of the shared secret that you set to either ASCII or Hex.
Secret/Confirm Secret	RADIUS server login secret. **Note** All the DNS servers should use the same secret.
DNS Timeout	Maximum time, in seconds, that the Cisco WLC waits before timing out the request and resending it. The range is from 1 to 180 days.
URL	Fully qualified domain name (FQDN) of the RADIUS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
Server IP Address	DNS server IP address. **Note** IPv6 is not supported for DNS.

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.

TACACS+ Authentication Servers

Choose **SECURITY > AAA > TACACS+ > Authentication** to navigate to the TACACS+ Authentication Servers page.

This page displays a summary of the existing TACACS+ authentication servers.

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the Cisco WLC automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

This page displays the following information about the configured TACACS+ servers:

- Server Index—Index of the TACACS+ server.
- Server Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TACACS+ server TCP port number.
- Admin Status—TACACS+ server status.

You can perform the following actions:

- To edit an existing TACACS+ authentication server, click the index number for that server.
- To remove an existing TACACS+ authentication server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the TACACS+ authentication server, click the blue arrow adjacent the desired server and choose **Ping**.
- Click **New** to add a new TACACS+ Authentication server.

Adding TACACS+ Authentication Servers

Choose **SECURITY > AAA > TACACS+ > Authentication** and then click **New** to navigate to the TACACS+ Authentication Servers > New page.

This page enables you to configure a TACACS+ authentication server:

Note You must configure TACACS+ on both your Cisco Secure Access Control Server (ACS) and your Cisco WLC. For information on configuring the ACS, refer to the *Cisco Wireless Controller Configuration Guide* or the *Cisco Secure ACS Configuration Guide*.

- Server Index (Priority)—Index of the TACACS+ server. Choose a number to specify the priority order of this server in relation to any other configured TACACS+ servers. You can configure up to three servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Port Number—TACACS+ server TCP port number. The valid range is 1 to 65535; the default value is 49.

Note Do not assign a port number that is used by another application. Use the default (49) or any other port unused by any other application.

- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

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.

Editing TACACS+ Authentication Servers

Choose **SECURITY > AAA > TACACS+ > Authentication** and then click a Server Index number to navigate to the TACACS+ Authentication Servers > Edit page.

This page enables you to change the settings for an existing TACACS+ authentication server.

- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

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.

TACACS+ Accounting Servers

Choose **SECURITY > AAA > TACACS+ > Accounting** to navigate to the TACACS+ Accounting Servers page.

This page displays a summary of the existing Terminal Access Controller Access Control System Plus (TACACS+) Accounting servers.

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the Cisco WLC automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

This page displays the following information about the configured TACACS+ servers:

- Server Index—Index of the TACACS+ server.
- Server Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TACACS+ server TCP port number.

- Admin Status—TACACS+ server status.

To edit an existing TACACS+ accounting server, click the index number for that server.

- To remove an existing TACACS+ accounting server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the TACACS+ accounting server, click the blue arrow adjacent the desired server and choose **Ping**.
- Click **New** to add a new TACACS+ accounting server.

Adding TACACS+ Accounting Servers

Choose **SECURITY > AAA > TACACS+ > Accounting** and then click **New** to navigate to the TACACS+ Accounting Servers > New page.

This page enables you to configure a TACACS+ accounting server:

Note You must configure TACACS+ on both your Cisco Secure Access Control Server (ACS) and your Cisco WLC. For information on configuring the ACS, refer to the *Cisco Wireless Controller Configuration Guide* or the *Cisco Secure ACS Configuration Guide*.

- Server Index (Priority)—Index of the TACACS server. Choose a number to specify the priority order of this server in relation to any other configured TACACS+ servers. You can configure up to three servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Port Number—Enter the TACACS+ server TCP port number. The valid range is 1 to 65535; the default value is 49.

Note Do not assign a port number that is used by another application. Use the default (49) or any other port unused by any other application.

- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

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.

Editing TACACS+ Accounting Servers

Choose **SECURITY > AAA > TACACS+ > Accounting** and then click a Server Index number to navigate to the TACACS+ Accounting Servers > Edit page.

This page enables you to change the settings for an existing TACACS+ accounting server.

- Shared Secret Format—Shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Server Status—TACACS+ server that you enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

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.

TACACS+ Authorization Servers

Choose **SECURITY > AAA > TACACS+ > Authorization** to navigate to the TACACS+ Authorization Servers page.

This page displays a summary of the existing TACACS+ authorization servers:

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the Cisco WLC automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

This page displays the following information about the configured TACACS+ servers:

- Server Index—Index of the TACACS+ server.
- Server Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TACACS+ server TCP port number.
- Admin Status—TACACS+ server status.

You can perform the following actions:

- To edit an existing TACACS+ Authorization server, click the index number for that server.
- To remove an existing TACACS+ Authorization server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the TACACS+ Authorization server, click the blue arrow adjacent the desired server and choose **Ping**.
- Click **New** to add a new TACACS+ Authorization server.

Adding TACACS+ Authorization Servers

Choose **SECURITY > AAA > TACACS+ > Authorization** and then click **New** to navigate to the TACACS+ Authorization Servers > New page.

This page enables you to configure a TACACS+ authorization server:

Note You must configure TACACS+ on both your Cisco Secure Access Control Server (ACS) and your Cisco WLC. For information on configuring the ACS, refer to the *Cisco Wireless Controller Configuration Guide* or the *Cisco Secure ACS Configuration Guide*.

- Server Index (Priority)—Index of the TACACS+ server. Choose a number to specify the priority order of this server in relation to any other configured TACACS+ servers. You can configure up to three servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Port Number—TACACS+ server TCP port number. The valid range is 1 to 65535; the default value is 49.

Note Do not assign a port number that is used by another application. Use the default (49) or any other port unused by any other application.

- Server Status—Enable or disable this TACACS+ server.
- Server Timeout—Enter the number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

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.

Editing TACACS+ Authorization Servers

Choose **SECURITY > AAA > TACACS+ > Authorization** and then click a Server Index number to navigate to the TACACS+ Authorization Servers > Edit page.

This page enables you to change the settings for an existing TACACS+ authorization server:

- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

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.

TACACS+ DNS Parameters

Choose **SECURITY > AAA > TACACS+ > DNS** to navigate to the TACACS+ DNS Parameters page.

This page allows Cisco WLC to retrieve the TACACS+ IP information from a DNS server. The DNS server is queried at regular intervals for updates. The Cisco WLC also runs the query if you manually change the DNS server list, or if one of the servers timeouts. As the DNS list overrides the static list, all manual AAA configurations on the WLAN will stop functioning as soon as the global server list gets populated from the DNS server. DNS AAA is also valid for FlexConnect AP clients using central authentication.

Note TACACS+ DNS is not supported for FlexConnect AP groups and FlexConnect clients with local switching.

Note DNS does not support IPv6.

Table 6-3 TACACS+ DNS Parameters

Parameter	Description
DNS Query	Check box to enable the Cisco WLC to retrieve the TACACS+ IP information from a DNS server. The default is disabled state. **Note** When you enable the DNS query, the static configurations will be overridden. The DNS list overrides the static AAA list.
Port Number	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port. **Note** The accounting port is derived from the authentication port.
Secret Format	Format of the shared secret that you set to either ASCII or Hex.
Secret/Confirm Secret	TACACS+ server login secret. **Note** All the DNS servers should use the same secret.
DNS Timeout	Maximum time, in seconds, that the Cisco WLC waits before timing out the request and resending it. The range is from 1 to 180 days.
URL	Fully qualified domain name (FQDN) of the TACACS+ server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
Server IP Address	DNS server IP address. **Note** IPv6 is not supported for DNS.

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.

TACACS+ Fallback Parameters

Choose **SECURITY > AAA > TACACS+ > Fallback** to navigate to the **TACACS+** > Fallback Parameters page.

You can configure the TACACS+ server fallback behavior to specify if the TACACS+ server should be enabled or disabled. This table describes the **TACACS+** fallback parameters.

Table 6-4 RADIUS Fallback Parameters

Parameter	Description
Fallback Mode	Specify the TACACS+ server fallback mode: • Enable—Activates the TACACS+ server. • Disable—Deactivates the TACACS+ server.
Interval in sec	Enter the probe interval in seconds. Valid values are from 180 to 3600. Enter 0 to disable the feature.

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.

LDAP Servers

Choose **SECURITY > AAA > LDAP** to navigate to the LDAP Servers page.

This page displays a summary of the existing Lightweight Directory Access Protocol (LDAP) servers:

- Server Index—Index of the LDAP server.
- Server Address (IPv4/IPv6)—IP address of the LDAP server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TCP port number of the LDAP server.
- Server State—Current status of the server.
- Bind—Local authentication bind method for the LDAP server.

You can perform the following actions:

- To edit an existing LDAP server, click the index number for that server.
- To remove an existing LDAP server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the LDAP server, click the blue arrow adjacent the desired server and choose **Ping**.

Click **New** to add a new LDAP server.

Adding LDAP Servers

Choose **SECURITY > AAA > LDAP** and then click **New** to navigate to the LDAP Servers > New page.

This page enables you to configure a Lightweight Directory Access Protocol (LDAP) server as a back-end database, which is similar to a RADIUS or local user database. An LDAP back-end database allows the Cisco WLC to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP may use an LDAP server as its back-end database to retrieve user credentials.

Note The LDAP back-end database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC.

LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password. For example, Microsoft Active Directory is not supported because it does not return a clear-text password.

If the LDAP server cannot be configured to return a clear-text password, LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are not supported.

- Server Index (Priority)—Index of the LDAP server. Choose a number to specify the priority order of this server in relation to any other configured LDAP servers. You can configure up to 17 servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the LDAP server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port Number—LDAP server TCP port number. The valid range is 1 to 65535; the default value is 389.
- Simple Bind—Local authentication bind method for the LDAP server that you can specify: either Anonymous or Authenticated. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password be entered to secure access.
- Bind Username—(for Authenticated bind method) Username to be used for local authentication to the LDAP server. The username can contain up to 80 characters.

Note If the username starts with "cn=" (in lowercase letters), the Cisco WLC assumes that the username includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.

- Bind Password—(for Authenticated bind method) Password to be used for local authentication to the LDAP server.
- Confirm Bind Password—(for Authenticated bind method) Password to be used for local authentication to the LDAP server.
- User Base DN—Distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, ou=next organizational unit, and o=corporation.com. If the tree that contains users is the base DN, type **o=***corporation***.com** or **dc=***corporation***,dc=com**.
- User Attribute—Name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.
- User Object Type—Value of the LDAP objectType attribute that identifies the record as a user.
- Server Timeout—Number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.
- Enable Server Status—LDAP server that you can enable or disable.

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.

Editing LDAP Servers

Choose **SECURITY > AAA > LDAP** and then click a Server Index number to navigate to the LDAP Servers > Edit page.

This page enables you to change the settings for an existing Lightweight Directory Access Protocol (LDAP) server:

- Enable Server Status—LDAP server that you can enable or disable.
- Simple Bind—Local authentication bind method for the LDAP server that you can specify: either Anonymous or Authenticated. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password be entered to secure access.
- Bind Username—Username to be used for local authentication to the LDAP server.
- Bind Password—Password to be used for local authentication to the LDAP server.
- Confirm Bind Password—Password to be used for local authentication to the LDAP server.
- User Base DN—Distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, ou=next organizational unit, and o=corporation.com. If the tree that contains users is the base DN, type **o=***corporation***.com** or **dc=***corporation***,dc=com**.
- User Attribute—Name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.
- User Object Type—Value of the LDAP objectType attribute that identifies the record as a user.
- Server Timeout—Number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

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.

Local Net Users

Choose **SECURITY > AAA > Local Net Users** to navigate to the Local Net Users page.

This page displays a summary of the existing local network clients who are allowed to access a specific Cisco WLAN Solution WLAN sorted by the username. You must enable Layer 3 Web Authentication located on the Adding Local Net Users page must be enabled.

Table 6-5 Local Net User Parameters

Parameter	Description
User Name	Username of the local net user.
WLAN Profile	WLAN profile of the local net user.
Guest User	Whether the user is a guest user.
Role	Role of the local net user.
Description	Short description about the configured local net user.

Client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

- Click the username to edit a local network user definition on the Editing Local Net Users page.

- Click the blue arrow adjacent the desired client and choose **Remove** to remove an existing local network client.

Click **New** to add a new local network client (Adding Local Net Users).

Adding Local Net Users

Choose **SECURITY > AAA > Local Net Users** and then click **New** to navigate to the Local Net Users > New page.

This page enables you to add a local network user. You must enable Layer 3 Web Authentication located on Editing WLANs page.

- User Name—Username of the local network user.
- Password—Password of the local network user.
- Confirm Password—Password for the local network user.
- Guest User—Guest User check box that you can select to limit the amount of time that the user has access to the local network. The default setting is unselected.
- Lifetime—If you selected the Guest User check box, enter the amount of time (in seconds) that the guest user account is to remain active in the Lifetime text box. The valid range is 60 to 2592000 seconds, and the default setting is 86400 seconds.
- Guest User Role—If you created a QoS role for guest users (QoS Roles for Guest Users), select the Guest User Role check box and select a Role from the drop-down list.
- WLAN Profile—Select WLAN profile that the user is allowed to access. If you choose **Any WLAN**, which is the default setting, the user can access any of the configured WLANs.
- Description—User description that you can enter.

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.

Editing Local Net Users

Choose **SECURITY > AAA > Local Net Users** and then click the username to navigate to the Local Net Users > Edit page.

This page enables you to edit a local network user definition. You must enable Layer 3 Web Authentication located on Editing WLANs page.

- User Name—Read-only field that displays the username of the local network user.
- Password—Password that you can specify.
- Confirm Password—Password that you can specify.
- Lifetime (seconds)—Lifetime of the user in seconds.
- Guest User Role—Guest User parameter that you can confirm or change if you want to limit the amount of time that the user has access to the local network. The default setting is unselected. If you selected the Guest User check box, confirm or change the amount of time (in seconds) that the guest user account is to remain active in the Lifetime text box. The valid range is 60 to 2592000 seconds, and the default setting is 86400 seconds.
- Guest User Role—If you created a QoS role for guest users (QoS Roles for Guest Users), confirm or change the Guest User Role check box and select a Role from the drop-down list.

- WLAN Profile—WLAN profile that you can select from the drop-down list.
- Description—User description that you can enter.

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.

MAC Filtering

Choose **SECURITY > AAA > MAC Filtering** to navigate to the MAC Filtering page.

This page displays the RADIUS Compatibility Mode, MAC delimiters for MAC Filtering, and the client MAC addresses that you entered into the Cisco WLC's local database.

You can configure each client MAC address to access network services through a specific Cisco WLAN and interface, or you can configure the WLAN as “Any WLAN” and the interface as “None” so that the client is not limited to that single WLAN or interface.

If MAC filtering is configured, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local MAC filtering is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured.

- Radius Compatibility Mode—Select the required RADIUS Compatibility Mode for MAC filtering:
  - Cisco ACS—In the RADIUS access-request packet, the username and password are the client MAC address.
  - Free RADIUS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the shared secret between the Cisco WLC and that RADIUS server.

Note The shared secret is the phrase that you entered when configuring the RADIUS server on the Cisco WLC.

Note Cisco ACS supports the free RADIUS compatibility mode.

  - Other—In the RADIUS access-request packet, the username is the client MAC address, but the password is not sent in the RADIUS access-request packet.
- Choose the required MAC delimiters for MAC filtering. The MAC delimiters can be a colon (xx:xx:xx:xx:xx:xx), hyphen (xx-xx-xx-xx-xx-xx), single hyphen (xxxxxx-xxxxxx), or none (xxxxxxxxxxxx), as required by the RADIUS server.

This page lists the current local MAC filters:

- MAC Address—Client MAC address.
- Profile Name—Profile name to which the client has access.
- Interface—Interface name as defined in the Interfaces page.
- IP Address—IP address.
- Description—Description of the local MAC filter.

You can perform the following actions:

- Click the MAC address to change a current local MAC filter definition on the Editing MAC Filters page.

- Click the blue arrow adjacent the desired filter and choose **Remove** to remove a current local MAC filter.

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.

Click **New** to add a new client by the MAC address (Adding MAC Filters).

Adding MAC Filters

Choose **SECURITY > AAA > MAC Filtering** and then click **New** to navigate to the MAC Filtering > New page.

This page enables you to add a client by the MAC address:

- MAC Address—Client MAC address that you can specify.
- Profile Name—Profile name to which the client has access.
- Description—Client description that you can specify.
- IP Address—IP address of the client.
- Interface Name—Associated interface name, as defined in the Interfaces page.

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.

Editing MAC Filters

Choose **SECURITY > AAA > MAC Filtering** and then click a MAC address to navigate to the MAC Filtering > Edit page.

This page enables you to change a MAC filter definition for an existing client MAC address.

- MAC Address—Read-only field that displays the client MAC address.
- Profile Name—Profile name to which the client has access from the drop-down list.
- IP Address—Client IP address that you can specify.
- Interface Name—Associated Interface Name, as defined in the Interfaces page.

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.

Disabled Clients

Choose **SECURITY > AAA > Disabled Clients** to navigate to the Disabled Clients page.

This page presents a summary of the clients who are prevented (manually barred by the MAC address) from accessing to network services.

This page displays the following information:

- Search by MAC Address—MAC address that you can specify to search for a disabled client. Click **Search** to search for a disabled client.
- MAC Address—Disabled client MAC address.

- Description—Description of the disabled client.

You can perform the following actions:

- Click the MAC address to open the Disabled Client > Edit page.
- Click the blue arrow adjacent the desired client and choose **Remove** to enable a client that was formerly disabled.

Click **New** to manually disable a client (see Adding Disabled Clients for more information).

Adding Disabled Clients

Choose **SECURITY > AAA > Disabled Client** and then click **New** or **MONITOR > Clients** then click **Disable** to navigate to the Disabled Client > New page.

This page enables you to disable a client by its MAC address.

- MAC Address—Disabled client MAC address.
- Description— Client description of the client you want to disable.

Note When you enter a client MAC address to be disabled, the operating system checks that the MAC address is not one of the known Local Net clients (Local Net Users), Authorized clients (MAC Filtering), or Local Management users (Local Management Users) MAC addresses. If the entered MAC address is on one of these three lists, the operating system does not allow the MAC address to be manually disabled.

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.

Editing Disabled Clients

Choose **SECURITY > AAA > Disabled Clients** and then click **Edit** to navigate to the Disabled Client > Edit page.

This page enables you to change the client description, based on the client MAC address that prevents a client from accessing the network.

- MAC Address—Disabled client MAC address.
- Description—Description of the disabled client.

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.

User Policies

Choose **SECURITY > AAA > User Login Policies** to navigate to the User Policies page.

This page enables you to specify the maximum number of concurrent logins for a single username, 0 (unlimited) through eight.

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 Policies

Choose **SECURITY > AAA > AP Policies** to navigate to the AP Policies page.

This page enables you to set policies that help in the authorization of access points. Access points are authorized against AAA and/or a certificate.

Table 6-6 Policy Configuration Parameters

Parameter	Description
Accept Self Signed Certificate (SSC)	Check box that you can select if you want the access point to accept self-signed certificates (SSCs).
Accept Manufactured Installed Certificate (MIC)	Check box that you can select if you want the access point to accept manufactured installed certificates (MICs).
Accept Local Significant Certificate (LSC)	Check box that you can select if you want the access point to accept local significant certificate (LSC).
Authorize MIC APs against auth-list or AAA	Check box that you can select if you want the access points to be authorized against AAA.
Authorize LSC APs against auth-list	Check box that you can select if you want the access points to be authorized against a local significant certificate.

Note Before you can accept an LSC, you must enable LSC on the Cisco WLC. See the Local Significant Certificates page for information on enabling LSC on the Cisco WLC.

To delete an access point from the authorization list, click the blue arrow adjacent the desired access point and choose **Remove**.

Search by MAC

You can search the AP Authorization List by MAC address.

Enter the MAC address as six two-digit hexadecimal numbers separated by colons (for example, 01:23:45:67:89:AB) and click **Search**. The AP Authorization Details page is displayed.

Adding an AP to Authorization List

To add an access point to the authorization list of a Cisco 4100 Series Wireless LAN Controller, follow these steps:

Step 1 Click **Add** to display the Add AP to Authorization List area.

Step 2 In the MAC Address text box, enter the MAC address of the AP.

Step 3 From the Certificate Type drop-down list, choose **MIC**.

Step 4 Click **Add**.

To add an AP to the authorization list of a Cisco 2000 Series Wireless LAN Controller or Cisco 4400 Series Wireless LAN Controller, follow these steps:

Step 1 Click **Add** to display the Add AP to Authorization List area.

Step 2 In the MAC Address field, enter the MAC address of the AP.

Step 3 From the Certificate Type drop-down list, choose **MIC**, **SSC**, or **LSC**.

Step 4 In the SHA1 Key Hash **text box,** enter the SHA1 key hash in hexadecimal format**.**

Note **The SHA1 Key Hash option is displayed only if you have chosen** SSC **as the certificate type in the previous step.**

Step 5 Click **Add AP to AuthList**.

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.

Password Policies

Choose **SECURITY > AAA > Password Policies** to navigate to the Password Policies page.

This page enables you to enforce strong password checks on newly created passwords for additional management users of Cisco WLC and access point. The following are the requirements enforced on the new password:

- When the Cisco WLC is upgraded from old version, all the old passwords are maintained as it is, even though the passwords are weak. After the system upgrade, if strong password checks are enabled, the same is enforced from that time and the strength of previously added passwords will not be checked or altered.
- Depending on the settings done in the Password Policy page, the local management and access point user configuration is affected.

Table 6-7 Password Policy Parameters

Parameter	Description
Password Policies —Local Management User and AP	
Password must contain characters from at least three different classes	Check box that you can select if you want your password to contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
No character can be repeated more than three times consecutively	Check box that you enable if you do not want any character in the new password to be repeated more than three times consecutively.

Table 6-7 Password Policy Parameters

Parameter	Description
Password cannot be default words such as cisco, admin	Check box that you can select if you do not want the password to contain words such as Cisco, ocsic, admin, nimda, or any variant obtained by changing the capitalization of letters or by substituting 1, |, or ! or substituting 0 for o, or substituting $ for s.
Password cannot contain username or reverse of username	Check box that you can enable if you do not want the password to contain a username or the reverse letters of a username.
Password position check	Check box that you can enable to verify a four-character change from the old password.
Password case digit check	Check box that you can enable to verify if all four combinations (lower, upper, digits) or special characters are there in the password.
Strong password minimum length	Minimum length of the password.
Strong password minimum upper case characters	Minimum number of upper-case characters that are required in the password.
Strong password minimum lower case characters	Minimum number of lower-case characters that are required in the password.
Strong password minimum digits	Minimum number of digits that are required in the password.
Strong password minimum special characters	Minimum number of special characters that are required in the password.
Management User	
Management User Lockout Enable	Check box that you can select to lock out a management user when the number of successive failed attempts exceeds the Management User Lockout Attempts. When disabled, this option unlocks the management user who was locked out.
Management User Lockout Attempts	Number of successive incorrect password attempts after which the management user is locked.
Management User Lockout Time	Amount of time, in seconds, after lockout attempts when the management user is locked.
Management User Password Lifetime	Number of days before the management user requires a change of password due to the age of the password.
SNMPv3 User	
SNMP User Lockout Enable	Check box that you can select to lock out an SNMP user when the number of successive failed attempts exceeds the SNMP User Lockout Attempts. When disabled, this option unlocks the SNMP user who is locked out.
SNMP User Lockout Attempts	Number of successive incorrect password attempts after which an SNMP user is locked.

Table 6-7 Password Policy Parameters

Parameter	Description
SNMP User Lockout Time	Amount of time, in seconds, after lockout attempts when an SNMP user is locked.
SNMP User Password Lifetime	Number of days before an SNMP user requires a change of password due to the age of the password.

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.

Local EAP

This section contains the following topics:

- General, page 6-26
- Profiles, page 6-26
- EAP-FAST Method Parameters, page 6-28
- Authentication Priority, page 6-28

General

Choose **SECURITY > Local EAP > General** to navigate to the **General** page. This page enables you to specify timeout values for local EAP.

This table describes the local EAP parameters.

Table 6-8 Local EAP Parameters

Parameter	Description
Local Auth Active Timeout (in secs)	Amount of time (in seconds) that the Cisco WLC attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fail. The valid range is 1 to 3600 seconds, and the default setting is 100 seconds.

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.

Profiles

Choose **SECURITY > Local EAP > Profiles** to navigate to the **Local EAP Profiles** page.

Note Local EAP Profiles is not supported on AP602 OEAP.

This page lists any local EAP profiles that you have configured and specifies their EAP types. You can create up to 24 local EAP profiles. To remove an existing profile, click the blue arrow adjacent the desired profile and choose **Remove**.

This page displays the following information:

- Profile Name—Profile name.
- LEAP—Check box indicating if Local EAP is enabled. The default is disabled state.
- EAP-FAST—Check box indicating if EAP-FAST is enabled. The default is disabled state.
- EAP-TLS—Check box indicating if EAP-TLS is enabled. The default is disabled state.
- PEAP—Check box indicating if PEAP is enabled. The default is disabled state.

Click **New** to create a new local EAP profile.

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.

Adding Local EAP Profiles

Choose **SECURITY > Local EAP > Profiles** and then click **New** to navigate to the Local EAP Profiles > New page.

This page enables you to create a local EAP profile, which specifies the EAP authentication types that are supported on the wireless clients. This page allows you to modify the following settings:

- Profile Name—Name (up to 63 alphanumeric characters; do not include spaces) for your new profile.

After you create a profile, you can edit the parameters from the Editing Local EAP Profiles page.

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.

Editing Local EAP Profiles

Choose **SECURITY > Local EAP > Profiles** and then click on the profile name to navigate to the Local EAP Profiles > Edit page.

This page enables you to edit a local EAP profile used for authentication:

- LEAP.
- EAP-FAST.
- EAP-TLS.
- PEAP—EAP type used for local authentication. Both PEAPv0/EAP-MSCHAPv2 and PEAPv1/EAP-GTC are enabled on the Cisco WLC.
- Local Certificate Required—Setting if you use EAP-FAST and want the device certificate on the Cisco WLC to be used for authentication. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.
- Client Certificate Required—Setting if you use EAP-FAST and want the wireless clients to send their device certificates to the Cisco WLC in order to authenticate or if you chose EAP-TLS and the client is using a certificate that is generated by a CA. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected. The default is disabled state.
- Certificate Issuer—Certificates that will be sent to the client, either from Cisco or from another Vendor. The default setting is Cisco.

- Check Against CA Certificates—Setting that you use if you want the incoming certificate from the client to be validated against the CA certificates on the Cisco WLC. The default is enabled.
- Verify Certificate CN Identity—Setting that you use if you want the common name (CN) in the incoming certificate to be validated against the CA certificates' CN on the Cisco WLC. You must enable this setting when you use an LDAP server as backup database. The default is disabled state
- Check Certificate Date Validity—Setting that you use if you want the Cisco WLC to verify that the incoming device certificate is still valid and has not expired. The default is enabled.

Note Certificate date validity is checked against the current UTC (GMT) time that is configured on the Cisco WLC. The time zone offset will be ignored.

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.

EAP-FAST Method Parameters

Choose **SECURITY > Local EAP > EAP-FAST Parameters** to navigate to the EAP-FAST Method Parameters page.

This page enables you to configure the following EAP-FAST settings if you configured an EAP-FAST profile from the Adding Local EAP Profiles page:

- Server Key (in hex)—Key (in hexadecimal characters) used to encrypt and decrypt PACs.
- Confirm Server Key—Key that you reenter (in hexadecimal characters).
- Time to Live for the PAC—Number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.
- Authority ID (in hex)—Authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.
- Authority ID Information—Authority identifier of the local EAP-FAST server in text format.
- Anonymous Provision—Setting if you want to enable anonymous provisioning. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned. Disable this feature when you use EAP-FAST with certificates. The default is enabled.

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.

Authentication Priority

Choose **SECURITY > Local EAP > Authentication Priority** to navigate to the Priority Order > Local-Auth page.

This page enables you to specify the order in which user credentials are retrieved from the back-end database servers.

Highlight the desired database from the left User Credentials box.

Use the left and right arrows and the Up and Down buttons to move the desired database to the top of the right User Credentials box.

Note If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP back-end database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If LOCAL is on the top, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP back-end database.

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.

Advanced EAP

Choose **Security > Advanced EAP** to navigate to the **Advanced EAP** page.

Table 6-9 Advanced EAP Parameters

Parameter	Description
Identity Request Timeout (in secs)	Amount of time (in seconds) in which the Cisco WLC attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 1 second.
Identity request Max Retries	Maximum number of times that the Cisco WLC attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 20 retries.
Dynamic WEP Key Index	Key index used for dynamic wired equivalent privacy (WEP). The default setting is 0.
Request Timeout (in secs)	Amount of time (in seconds) in which the Cisco WLC attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 1 second.
Request Max Retries	Maximum number of times that the Cisco WLC attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 20 retries.
Max-Login Ignore Identity Response	Number of devices that you can be connected to the Cisco WLC with the same username. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same Cisco WLC. The default value is enabled.
EAPOL-Key Timeout	Amount of time (in seconds) in which the Cisco WLC attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.

Table 6-9 Advanced EAP Parameters

Parameter	Description
EAPOL-Key Max Retries	Maximum number of times that the Cisco WLC attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.
EAP-Broadcast Key Interval (in secs)	EAP-broadcast key renew interval time in seconds.

Priority Order of Management Users

Choose **Security > Priority Order > Management User** to navigate to the Priority Order > Management User page.

This page enables you to specify the order of authentication when multiple databases are configured:

- Authentication Priority—Choose either **Radius** or **TACACS+** to specify which server has priority over the other when the Cisco WLC attempts to authenticate.

  By default, the local database is always queried first. If the username is not found, the Cisco WLC switches to the TACACS+ server if configured for TACACS+ or to the RADIUS server if configured for RADIUS. The default setting is local and then RADIUS.

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.

Local Significant Certificates

Choose **SECURITY > Certificate > LSC** to navigate to the Local Significant Certificates page.

This page enables you to enable local significant certificates (LSCs) on the Cisco WLC.

Prior to release Cisco WLC 7.0, MAPs supported only the Manufactured Installed Certificate (MIC) for authentication and association with the Cisco WLC. Starting with this release, you can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, validity periods, restrictions, and usages on the generated certificates. After these customer-generated or locally significant certificates (LSCs) are present on the APs and Cisco WLCs, the devices start using these LSCs, to join, authenticate, and derive a session key. Cisco supported normal APs from the Cisco WLC 5.2 release and later releases and extended the support for mesh APs as well from the Cisco WLC 7.0 release.

The LSC is installed on access points and Cisco WLCs. You need to provision the LSC first on the Cisco WLC, which should be configured to communicate with a CA server.

Note Only external dedicated CA servers are supported in this release.

The access point gets a signed X.509 certificate by sending a certRequest to the Cisco WLC. The Cisco WLC acts as a CA proxy and receives the certRequest signed by the CA for the access point.

General Tab

Table 6-10 General Tab Parameters

Parameter	Description
Certificate Type	Certificates that are added to the Cisco WLC's CA certificate database. To add the CA certificate or device certificate into the Cisco WLC's CA certificate database, click the blue arrow adjacent the desired certificate type and choose **Add**. To remove a certificate, click the blue arrow adjacent the desired certificate type and choose **Remove**.
Enable LSC on Controller	Check box to enable LSC on the Cisco WLC. The default is disabled state.
CA Server URL	URL of the CA server in the following format: **http://***url***:***port***/***path* The *url* can be either a domain name or an IP address.
Params	Parameters for the device certificate. The keysize is a value from 384 to 2048 (in bits); the default value is 2048. The following parameters are available: • Country Code—Enter the country code. The country code is a three byte string. • State—Enter the state. This value can be up to 64 bytes. • City—Enter the city. The value can be up to 64 bytes. • Organization—Enter the organization. The value can be up to 64 bytes. • Department—Enter the department. The value can be up to 64 bytes. • Email—Enter a valid e-mail address. • Key Size—Enter the key size. The range includes 360 to 2048 bits. The default is 2048.

AP Provisioning Tab

Table 6-11 AP Provisioning Tab Parameters

Parameter	Description
Enable	Parameter that enables you to provision the LSC on the access point. Click **Update** to enable an LSC on the access point. The default is disabled state.
Number of attempts to LSC	Number of times that the access point attempts to join the Cisco WLC using an LSC before the access point reverts to the default certificate (MIC or SSC). The valid range is 0 to 255, and the default value is 3. If you set the number of retries to a nonzero value and the access point fails to join the Cisco WLC using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the Cisco WLC using an LSC, the access point does not attempt to join the Cisco WLC using the default certificate. **Note** If you are configuring an LSC for the first time, we recommend that you configure a nonzero value.
AP Ethernet MAC Addresses	Ethernet MAC address of the access point.
MAC Address	Access point MAC addresses.

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.

Self Significant Certificates

Choose **SECURITY > Certificate > SSC** to navigate to the Self Signed Certificates page.

This page enables you to view the Self Signed Certificate of the virtual Cisco WLC and enable hash validation of the SSC certificate by the access points.

Virtual Cisco WLCs use SSC certificates instead of Manufacturing Installed Certificates (MIC) used by physical Cisco WLCs.

You can select the **Enable SSC Hash Validation** check box to allow an AP to validate the SSC certificate of the virtual Cisco WLC. When an AP validates the SSC certificate, it checks if the hash key of the virtual Cisco WLC matches the hash key stored in its flash. If a match is found, the validation passes and the AP moves to the Run state. If a match is not found, the validation fails and the AP disconnects from the Cisco WLC and restarts the discovery process.

By default, hash validation is enabled. Therefore, an AP must have the virtual Cisco WLC hash key in its flash before associating with the virtual Cisco WLC. If you disable hash validation of the SSC certificate, the AP bypasses the hash validation and directly moves to the run state.

To configure the hash key of the virtual Cisco WLC, choose **CONTROLLER > Mobility Management > Mobility Groups**, click **New** and enter the IP address, MAC address, mobility group name, and hash key of the virtual Cisco WLC.

APs can associate with a physical Cisco WLC, download the hash keys and then associate with a virtual Cisco WLC. If the AP is associated to a physical Cisco WLC, if hash validation is disabled, it joins any virtual Cisco WLC without hash validation.

Access Control Lists

Choose **SECURITY > Access Control Lists > Access Control Lists** to navigate to the Access Control Lists page.

This page enables you to view current access control lists (ACLs) that are similar to standard firewall access control lists.

Note You can define up to 64 ACLs with up to 64 rules (filters) per ACL.

- Enable Counters—Check box that you can select to see if packets are hitting any of the ACLs that are configured on your Cisco WLC. The default is unselected.

  Note ACL counters are available only on the following Cisco WLCs: Cisco 5500 Series Controller, Cisco 4400 Series Controller, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

- Name—ACL name to open the Editing Access Control Lists page.
- Type—IPv4 or IPv6 ACL.

To remove an existing ACL, click the blue arrow adjacent the desired ACL and choose **Remove**.

To clear the counters for an ACL, click the blue arrow adjacent the desired ACL and choose **Clear Counters**.

Guidelines

- Pre-auth ACL must have the following two rules for proper operation:
  - One allowing traffic to the DNS server.
  - One allowing traffic from the DNS server.
- Beginning in Cisco WLC Release 7.4 and later, DNS traffic is handled based on deny rules defined in the WLAN Pre-Auth ACL.
  - If no Pre-Auth ACL is configured and applied, then all DNS packets are allowed to pass to any server.
  - If Pre-Auth ACL is configured, but no matching deny rule is configured, then allow all DNS packets to pass to any server.
  - If Pre-Auth ACL is configured with a rule to allow DNS traffic to a given server and a rule configured to drop all traffic based on protocol/IP address, then allow DNS to one server only and block all other DNS traffic.

Click **New** to add a new ACL (see the Adding Access Control Lists topic).

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.

Adding Access Control Lists

Choose **SECURITY > Access Control Lists > Access Control Lists** and then click **New** to navigate to the Access Control Lists > New page.

- Access Control List Name— ACL name that you can specify.
- Access Control List Type—ACL type as either IPv4 or IPv6.

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.

Editing Access Control Lists

Choose **SECURITY > Access Control Lists > Access Control Lists** and then click on the ACL name to navigate to the Access Control Lists > Edit page.

This page enables you to view and/or change an ACL definition, which is similar to standard firewall ACLs.

Note You can define up to 64 ACLs with up to 64 rules (filters) per ACL.

To remove a rule, click the blue arrow adjacent the desired ACL and choose **Remove**.

Table 6-12 Current Rule Parameters

Parameter	Description
Access List Name	Name of the ACL.
Deny Counters	Number of times that packets have matched the explicit deny ACL rule. **Note** You must enable ACL counters on the Access Control Lists page to enable the Deny Counters.
Sequence	Up to 64 rules can be defined for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and sequence 5 to 6. **Note** Click the sequence number to modify the rule (See the Editing Access Control Lists Rules topic).
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

Table 6-12 Current Rule Parameters

Parameter	Description
Source IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.
Destination IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.
Protocol	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)
Source Port	Any or IP address and netmask.
Dest Port	Any or IP address and netmask.
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Direction	Any, Inbound (from client), or Outbound (to client).
Number of Hits	Number of times that packets have matched an ACL rule. **Note** This field appears only if you enabled ACL counters on the Access Control Lists page.

When the ACL contains one or more ACL rule, click the sequence number to modify the rule on the Editing Access Control Lists Rules page.

Click **Add New Rule** to add a new rule to an existing ACL.

Editing Access Control Lists Rules

Choose **SECURITY > Access Control Lists > Access Control Lists,** click the ACL name. Click the sequence number of the rule that you want to change to navigate to the Access Control Lists > Rules > Edit page.

This page enables you to change an ACL rule definition.

Note The operating system enables you to define up to 64 ACLs with up to 64 rules (filters) per ACL.

Table 6-13 Rule Edit Parameters

Parameter	Description
Sequence	Up to 64 rules can be defined for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns Sequence 6 to 7 and sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)

Table 6-13 Rule Edit Parameters

Parameter	Description
Source Port/Destination Port	Source/Destination Ports for this ACL: • Any • HTTP • HTTPS • Telnet • RADIUS • DHCP Server • DHCP Client • DNS • L2TP • PPTF Control • SMTP • SNMP • LDAP • Kerberos • NetBIOS NS • NetBIOS DS • NetBIOS SS • MS Dir Server • Other • Port Range
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Direction	Any, Inbound (from client), or Outbound (to client).
Action **Note** The default filter is to deny all access unless a rule explicitly permits it.	Deny or Permit.

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.

Adding Access Control Lists Rules

Choose **SECURITY > Access Control Lists > Access Control Lists,** click the ACL name of an existing ACL, and then click **Add New Rule** to navigate to the Access Control Lists > Rules > New page.

This table describes the new rule parameters.

Table 6-14 New Rule Parameters

Parameter	Description
Sequence	Operator that can define up to 64 rules for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA's Website)
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.

Table 6-14 New Rule Parameters

Parameter	Description
Direction	Any, Inbound (from client), or Outbound (to client).
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

CPU Access Control Lists

Choose **SECURITY > Access Control Lists > CPU Access Control Lists** to navigate to the CPU Access Control Lists page.

This page enables you to configure and apply an Access Control List (ACL) to the Cisco WLC CPU to control traffic to the CPU.

Table 6-15 CPU ACL Parameters

Parameter	Description	Default
Enable CPU ACL	Designated ACL that you can enable to control the IPv4 traffic to the Cisco WLC CPU.	Unselected (disabled)
ACL Name	Previously configured ACL. To configure an ACL, see Adding Access Control Lists. If you choose **none** while the CPU ACL feature is enabled, an error message appears.	none
Enable CPU IPv6 ACL	Designated ACL that you can enable to control the IPv6 traffic to the Cisco WLC CPU.	Unselected (disabled)
IPv6 ACL Name	Previously configured ACL. To configure an ACL, see Adding Access Control Lists. If you choose **none** while the CPU ACL feature is enabled, an error message appears.	none

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.

FlexConnect ACLs

With FlexConnect ACLs, you can control access at the FlexConnect AP for protection and integrity of locally switched data traffic from the AP. Using the Cisco WLC, you can create FlexConnect ACLs and then configure the FlexConnect ACL with the WLAN using WLAN-ACL mapping. These are then pushed to the AP.

Choose **SECURITY > Access Control Lists > FlexConnect ACLs** to navigate to the FlexConnect ACLs page.

This page enables you to list the ACLs configured for FlexConnect access points. To remove a FlexConnect ACL, click the blue arrow adjacent the desired ACL and choose **Remove**.

Click **New** to add a new FlexConnect ACL.

Adding FlexConnect ACLs

Choose **SECURITY > Access Control Lists > FlexConnect ACLs** and click **New**. The FlexConnect ACL > New page enables you to create an ACL. Enter the FlexConnect ACL name in the Access Control List Name text box.

Click **Apply** to create the new FlexConnect ACL with the configured name.

Editing Access Control List

Choose **SECURITY > FlexConnect ACLs** and click the ACL name of an existing ACL to open the Access Control List > Edit page.

Table 6-16 FlexConnect Access Control List Parameters

Parameter	Description
General	
Access List Name	Name of the FlexConnect ACL.
Seq	Up to 64 rules can be defined for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and sequence 5 to 6.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.
Source IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.

Table 6-16 FlexConnect Access Control List Parameters

Parameter	Description
Protocol	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)
Source Port	Any or IP address and netmask.
Dest Port	Any or IP address and netmask.
DSCP	Any or Specific (from 0 to 63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service (QoS) across the Internet.

Click **Add a New Rule** to add a new rule to an existing ACL .

Adding FlexConnect ACL Rules

Choose **SECURITY > Access Control List > FlexConnect ACLs** to navigate to the FlexConnect Access Control Lists page. Click an ACL name to open the **Access Control List > Edit** page and click **Add New Rule** button to create a new ACL Rule.

Table 6-17 FlexConnect ACL New Rule Parameters

Parameter	Description
Sequence	Operator that can define up to 64 rules for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)

Table 6-17 FlexConnect ACL New Rule Parameters

Parameter	Description
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

Layer2 ACLs

You can configure rules for Layer 2 access control lists (ACLs) based on the Ethertype associated with the packets. Using this feature, if a WLAN with central switching is required to support only PPPoE clients, you can apply Layer 2 ACL rules on the WLAN to allow only PPPoE packets after the client is authenticated and the rest of the packets are dropped. Similarly, if the WLAN is required to support only IPv4 clients or only IPv6 clients, you can apply Layer 2 ACL rules on the WLAN to allow only IPv4 or IPv6 packets after the client is authenticated and the rest of the packets are dropped. For a locally-switched WLAN, you can apply the same Layer 2 ACL either for the WLAN or a FlexConnect AP. AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs. The Layer 2 ACL that is applied to the FlexConnect AP takes precedence over the Layer 2 ACL that is applied to the WLAN.

Table 6-18 Layer2 ACL New Rule Parameters

Parameter	Description
Sequence	Enter a value between 1 and 16 to determine the order of this rule in relation to any other rules defined for this ACL. Up to 16 rules are supported for each ACL. **Note** If rules 1 through 4 are already defined and you add rule 15, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

Table 6-18 Layer2 ACL New Rule Parameters

Parameter	Description
Ether Type	Drop-down list from which you can choose the Ether type. You can select any predefined Ether Types from the Ether Type drop-down list or enter your own Ether type value using the custom option from the Ether Type drop-down list.
Action	Drop-down list from which you can specify the action to be taken: • Deny—Causes the ACL to block packets • Permit—Causes the ACL to allow packets

URL ACLs

Choose **SECURITY > Access Control Lists > URL ACLs to navigate to the URL Access Control Lists page.**

This page enables you to configure URL ACL list.

- Enable URL ACL—Check box that you can select to enable or disable the URL filtering feature. The default is unselected.

To remove an existing ACL, click the blue arrow adjacent the desired URL ACL and choose **Remove**.

To clear the counters for an ACL, click the blue arrow adjacent the desired URL ACL and choose **Clear Counters**.

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.

Adding URL ACL List

Choose **SECURITY > Access Control Lists > URL ACLs,** and then click **New** to navigate to the URL Access Control Lists > New page.

- URL ACL Name—you can specify the URL ACL name.

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.

Adding URL ACL Rules

Choose **SECURITY > Access Control Lists > URL ACLs,** and then click on the URL Acl name to navigate to the URL Access Control Lists > Edit page. Click **Add New Rule** to create a new definition.

This page enables you to add parameter values to an URL ACL definition.

This table describes the rule parameters.

Table 6-19 Current Rule Parameters

Parameter	Description
Rule Index	The Enter a value of range supported by the Cisco WLC: • Cisco 5508 WLC, WiSM2 support 64 rules in one ACL • Cisco 5520, 8510, 8540 WLCs support 100 rules in one ACL
URL	URL address that you want to add in this list.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

Editing URL ACL Rules

Choose **SECURITY > Access Control Lists > URL ACLs,** and then click on the URL Acl name to navigate to the URL Access Control Lists > Edit page. Click the Rule Index number of the rule that you want to change to navigate to the URL ACLs > URL Access Control Lists > Rules > Edit page.

This page enables you to view and/or change an URL ACL definition..

Table 6-20 Editing Rule Parameters

Parameter	Description
Rule Index	The Enter a value of range supported by the Cisco WLC: • Cisco 5508 WLC, WiSM2 support 64 rules in one ACL • Cisco 5520, 8510, 8540 WLCs support 100 rules in one ACL
URL	URL address that you want to add in this list.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

Activating URL Filtering ACL (Global)

Choose **SECURITY** > **Local Policies** > and click on the policy name to navigate to the Policy > Edit page.

- **Match Role String**–enter the match role string as entered in the Cisco AV pair
- **URL ACL**–choose the URL ACL list from the drop down menu

Rogue Policy

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > General** to navigate to the Rogue Policies page.

This page enables you to select global parameters for rogue access point detection.

Note The Cisco 5500 Series Wireless Controllers support up to 2000 rogues (including acknowledged rogues); the Cisco 4400 Series Wireless Controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues, and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each Cisco WLC limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

Rogue Location Discovery Protocol

The Cisco WLC continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the Cisco WLC discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

You can configure the Cisco WLC to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The later option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure the Cisco WLC to use RLDP on all access points, the Cisco WLC always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue.

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS) on a monitor mode access point.

Rogue Policies

Table 6-21 Rogue Policy Parameters

Parameter	Description
Rogue Detection Security Level	Rogue detection security level that you can select: • Low—Basic rogue detection for small-scale deployments. Auto containment is not supported for this security level. • High—Basic rogue detection and auto containment for medium-scale or less critical deployments. RLDP is disabled for this security level. • Critical—Basic rogue detection, auto containment, and RLDP for highly critical deployments. • Custom—You can configure the rogue policy parameters. Each security level has preset configurations for each rogue detection security level.
Rogue Location Discovery Protocol	RLDP options that you can specify: • Disable—Disables RLDP. This is the default value. If the rogue detection security level is Low, RLDP is disabled. • Monitor Mode APs—Enables RLDP only on monitor mode access points. If the rogue detection security level is High, the RLDP mode is set to Monitor Mode APs mode. • All APs—Enables RLDP on all the access points (monitor mode and data). If the rogue detection security level is Critical, the RLDP mode is All APs. **Note** If you configure the Cisco WLC to use RLDP on all the access points, the Cisco WLC always chooses the monitor access point for the RLDP operation if a monitor access point and a local (data) access point are both nearby.
Expiration Timeout for Rogue AP and rogue Client Entries	Number of seconds after which the rogue access point will be taken off the list. The range is from 240 to 3600 and the default value is 1200. The expiration timeout for rogue AP and client entries for each rogue detection security levels are as follows: • Low—240 • High—1200 • Critical—3600 • Custom—Any value between 240 and 3600
Validate rogue clients against AAA	Validation that you can enable using the AAA server or local database to validate if rogue clients are valid clients. The default is disabled state. If DNS query is enabled (**SECURITY > AAA > RADIUS > DNS**), the validation occurs using the RADIUS list from the DNS server.

Table 6-21 Rogue Policy Parameters

Parameter	Description
Validate rogue clients against MSE	Validation that you can enable using MSE to validate if rogue clients are valid clients. The default is disabled state. You cannot validate rogue clients against MSE and AAA at the same time.
Detect and report Ad-Hoc Networks	Ad-hoc rogue detection and reporting that you can enable or disable. The default value is enabled.
Rogue Detection Report Interval (10 to 300 Sec)	Time interval, in seconds, at which the APs should send the rogue detection report to the Cisco WLC. The default value is 10. The rogue detection report interval for each rogue detection security levels are as follows: • Low—60 • High—30 • Critical—10 **Note** This feature is applicable to APs that are in monitor mode only.
Rogue Detection Minimum RSSI (–70 dBm to –128 dBm)	Minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. The default value is –128 dBm. The rogue detection minimum RSSI for each rogue detection security levels are as follows: • Low— –80 dBm • High— –128 dBm • Critical— –128 dBm **Note** This feature is applicable to all the AP modes.
Rogue Detection Transient Interval	Time interval, in seconds, at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. After the rogue is scanned for consistently, updates are sent periodically to the Cisco WLC. The APs filter the transient rogues that are active for a very short period and are then silent. The range is from 120 to 1800. The rogue detection transient interval for each rogue detection security level is as follows: • Low—120 • High—300 • Critical—600 **Note** This feature applies to APs that are in monitor mode only.
Rogue Client Threshold	Threshold rogue client count after which a trap is sent from the Cisco WLC. Enter 0 to disable the feature. The range is from 1 to 256. The default is disabled state. The rogue client threshold for each rogue detection security levels is 0.
Rogue Containment Automatic Rate Selection	Check box that you can select to enable automatic rate selection for rogue containment.

RSSI (dBm)	802.11b/g Tx Rate (Mbps)	802.11a Tx Rate (Mbps)
–74	1	6
–70	2	12
–55	5.5	12
< –40	5.5	18

Auto Contain

If you want the Cisco WLC to automatically contain certain rogue devices, check the following check boxes. Otherwise, leave the check boxes unselected, which is the default value.

Caution When you enable any of these parameters, the following warning appears:

"Using this feature may have legal consequences. Do you want to continue?"

The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Table 6-22 Auto Contain Parameters

Parameter	Description
Auto Containment Level	Drop-down list from which you can choose the rogue auto containment level from 1 to 4. You can choose up to four APs for auto containment when a rogue is moved to a contained state through any of the auto containment policies. You can also choose Auto for automatic selection of the number of APs used for auto containment. The Cisco WLC chooses the required number of APs based on the RSSI for effective containment. The RSSI value associated with each containment level is as follows: • 1—0 to –55 dBm • 2— –75 to –55 dBm • 3— –85 to –75 dBm • 4—Less than –85 dBm
Auto Containment only for Monitor mode APs	Check box that you can select to enable the monitor mode APs for auto containment. The default is disabled state.

Table 6-22 Auto Contain Parameters

Parameter	Description
Auto Containment on FlexConnect Standalone	Check box that you can select to enable auto containment on FlexConnect APs in the standalone mode. The default is disabled state. When the FlexConnect APs are in the standalone mode, you can enable only the Using our SSID or AdHoc Rogue AP auto containment policies. The containment stops after the standalone AP connects back to the Cisco WLC.
Rogue on Wire	Check box that you enable to automatically contain the rogues that are detected on the wired network. The default is disabled state.
Using our SSID	Check box that you enable to automatically contain those rogues that are advertising your network's SSID. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a rogue is detected. The default is disabled state.
Valid client on Rogue AP	Check box that you enable to automatically contain a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a rogue is detected. The default is disabled state.
AdHoc Rogue AP	Check box that you enable to automatically contain ad-hoc networks detected by the Cisco WLC. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a network is detected. The default is disabled state.

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.

Rogue Rules

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Rogue Rules** to navigate to the Rogue Rules page.

This page enables you to add new rogue rules and to change the priority of the rogue rules.

Note Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

Table 6-23 Rogue Rules Parameters

Parameter	Description
Rule Name	Name of the rogue rule. You can configure a maximum of 64 rogue rules.
Type	Whether the rule is Friendly, Malicious, or Custom.
Status	Status of the rule: enabled or disabled.

Table 6-23 Rogue Rules Parameters

Parameter	Description
Notify	Type of notification upon rule match that is one of the following: • All—Notifies the Cisco WLC and a trap receiver such as Cisco Prime Infrastructure. • Global—Notifies only a trap receiver such as Cisco Prime Infrastructure. • Local—Notifies only the Cisco WLC. • None—No notifications are sent.
State	State of the rogue access point after a rule match. It can be one of the following: • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. The Cisco WLC forwards an immediate alert to the system administrator for further action. • Contain—The Cisco WLC contains the offending device so that its signals no longer interfere with authorized clients. • Internal—The unknown access point is inside the network and poses no threat to WLAN security. The Cisco WLC trusts this rogue access point. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. The Cisco WLC acknowledges the presence of this rogue access point. For example, the access points that belongs to a neighboring coffee shop are external rogue access points. • Delete—The rogue access point is deleted from the database when the rogue rule is applied to the rogue access point.
Match Operation	Click the **Match All** radio button to enable the rogue rule only when a detected rogue access point meets all the conditions of the rule. Click the **Match Any** radio button to enable the rule when any of the conditions are met.

Table 6-23 Rogue Rules Parameters

Parameter	Description
Enable Rule	Check box that you can select to enable a rogue rule.
Condition	Drop-down list from which you can choose one or more of the following rogue rule conditions: • SSID—Requires that a rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User-Configured SSID text box, and click **Add SSID**. You can configure up to 25 SSIDs per rogue rule. • RSSI—Requires that a rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, the access point is classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI text box. The range is from –95 to –50 dBm (inclusive), and the default value is 0 dBm. • Duration—Requires that a rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration text box. The range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds. • Client Count—Requires that a minimum number of clients be associated to a rogue access point. For example, if the number of clients associated to a rogue access point is greater than or equal to the configured value, the access point is classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients text box. The range is from 1 to 10 (inclusive), and the default value is 0. • No Encrytion—Requires that a rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option. • Managed SSID—Requires that a rogue access point's managed SSID (the SSID configured for the WLAN) be known to the Cisco WLC. No further configuration is required for this option. • Substring SSID—Requires that a rogue access point have a substring of a user-configured SSID. If you choose this option, enter the substring of the SSID in the User-Configured SSID text box. For example, if you have an SSID as ABCDE, you can specify the substring as ABCD or ABC. You can classify multiple SSIDs with matching patterns. You can configure up to 25 SSID substrings per rogue rule.

- Click **Add Rule** to add a new rogue rule:
  a. Enter a rule name. The rule name cannot contain any spaces.
  b. Choose the rule type (**Friendly** or **Malicious**) to classify rogue access points that match this rule as friendly or malicious.
  c. Click **Add**.
- Click the rule name to open the Editing Rogue Rules page.

Click **Add Rule** to add a new rogue rule.

Click **Change Priority** to change the order in which rogue classification rules are applied.

Editing Rogue Rules

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Rogue Rules** and click the rule name to navigate to the Rogue Rule > Edit page.

Note Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

This page enables you to edit the rogue rule settings.

Table 6-24 Rogue Rule Parameters

Parameter	Description
Rule Name	Name of the rogue rule.
Type	Whether the rule is Friendly, Malicious, or Custom.
Notify	Type of notification upon rule match that is one of the following: • All—Notifies the Cisco WLC and a trap receiver such as Cisco Prime Infrastructure. • Global—Notifies only a trap receiver such as Cisco Prime Infrastructure. • Local—Notifies only the Cisco WLC. • None—No notifications are sent.

Table 6-24 Rogue Rule Parameters

Parameter	Description
State	State of the rogue access point after a rule match. It can be one of the following: • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. The Cisco WLC forwards an immediate alert to the system administrator for further action. • Contain—The Cisco WLC contains the offending device so that its signals no longer interfere with authorized clients. • Internal—The unknown access point is inside the network and poses no threat to WLAN security. The Cisco WLC trusts this rogue access point. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. The Cisco WLC acknowledges the presence of this rogue access point. For example, the access points that belongs to a neighboring coffee shop are external rogue access points. • Delete—The rogue access point is deleted from the database when the rogue rule is applied to the rogue access point.
Match Operation	Rule that you choose: • Match All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. • Match Any—(Default) If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.
Enable Rule	Rule that you enable or disable. The default is disabled state.
Severity Score	Custom classification severity score. The range is from 1 to 100. This field appears only when you choose Custom rule type.
Classification Name	Custom classification name. The name can be up to 32 case-sensitive, alphanumeric characters.This field appears only when you choose Custom rule type.

Conditions

To add conditions to the rogue rule, select the condition from the drop-down list and click **Add Condition**.

Table 6-25 Rogue Rules Condition Parameters

Parameter	Description
Time Duration (0 to 3600)	Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration field. The range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
Minimum RSSI (-95 to -50)	Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI field. The range is from –95 to –50 dBm (inclusive), and the default value is 0 dBm.
Minimum number of Rogue client (1-10)	Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients field. The range is from 1 to 10 (inclusive), and the default value is 0.
No Encryption	Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option. **Note** Prime Infrastructure refers to this option as "Open Authentication."
Managed SSID[1]	Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the Cisco WLC. No further configuration is required for this option.
User configured SSID[1]	Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID field, and click **Add SSID**. You can add multiple SSIDs. To remove an SSID, select the SSID and click **Remove**.

1. The SSID and Managed SSID conditions cannot be used with the Match All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

To remove a condition, click the blue arrow adjacent the desired condition and choose the **Remove** link.

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.

Priority of Rogue Rules

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Rogue Rules** and click **Change Priority** to navigate to the Rogue Rules > Priority page.

This page enables you to change the order in which rogue classification rules are applied.

Highlight the rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.

Continue to move the rules up or down until the rules are in the desired order.

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.

Friendly Rogues

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Friendly Rogue** to navigate to the Friendly Rogue page.

This page enables you to classify any rogue access points as friendly and add them to the friendly MAC address list.

To classify a rogue rule, follow these steps:

Step 1 In the MAC Address text box, enter the MAC address of the friendly rogue access point.

Step 2 Click **Apply** to commit your changes.

Step 3 Click **Save Configuration** to save your changes.

This access point is added to the Cisco WLC's list of friendly access points and appears on the **Friendly Rogue APs** page.

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.

Standard Signatures

Choose **SECURITY > Wireless Protection Policies > Standard Signatures** to access the Standard Signatures page.

This page enables you to view standard signature information:

- Enable Check for All Standard and Custom Signatures—Check box to enable if you want to allow all signatures (both standard and custom) whose individual states are set to Enabled to remain enabled. The default is enabled. When the signatures are enabled, the access points joined to the Cisco WLC perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the Cisco WLC.

  If you unselect this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.

- Precedence—Precedence Order Number.

- Name—Name of the signature.
- Frame Type—Type of frame, such as Management or Data.
- Action—Type of action to take, such as report.
- State—Whether the state is enabled or disabled.
- Description—Text description of the signature, such as “Broadcast Deauthentication Frame.”

Click the precedence order number to view more detailed information. See the Standard Signature Details topic.

Standard Signature Details

Choose **SECURITY > Wireless Protection Policies > Standard Signatures** to navigate to the Standard Signatures page. Click the precedence order number to access the Standard Signature > Detail page. This page enables you to view detailed signature information:

- Precedence—Precedence order number.
- Name—Name of the signature, such as Bcast deauth.
- Description—Text description of the signature, such as “Broadcast Deauthentication Frame.”
- Frame Type—Management or Data.
- Action—None or Report.
- Measurement Interval (sec)—Number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value varies per signature.
- Tracking—Tracking method used by the access points to perform signature analysis and report the results to the Cisco WLC. The possible values are as follows:
  - Per Signature—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis.
  - Per MAC—Signature analysis and pattern matching are tracked and reported separately for individual client MAC addresses on a per-channel basis.
  - Per Signature and MAC—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis as well as on a per-MAC-address and per-channel basis.
- Signature Frequency—Number of matching packets per interval that must be identified at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.
- Signature MAC Frequency—Number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.
- Quiet Time (secs)—Length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds, and the default value varies per signature.
- State—Whether this signature to detect security attacks is enabled or disabled. The default value is enabled (or checked).

Patterns

- Offset—Offset, in bytes, from the start of the packet header or body based on the value of the preceding <offsetStart> where the pattern match operation is to be performed.

- Pattern—Hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.
- Mask—Mask is a hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.

Custom Signatures

Choose **SECURITY > Wireless Protection Policies > Custom Signatures** to access the Custom Signatures page.

- Enable Check for All Standard and Custom Signatures—Check box to enable or disable signatures (both standard and custom) whose individual states are set to Enabled to remain enabled. The default is enabled. When the signatures are enabled, the access points joined to the Cisco WLC perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the Cisco WLC.

  If you unselect this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.
- Precedence—Precedence Order Number.
- Name—Name of the custom signature.
- Frame Type—Frame type, such as Management, or data.
- Action—Type of action to take, such as report.
- State—Whether the state is enabled or disabled.
- Description—Text description of the signature.

Custom Signature Details

Choose **SECURITY > Wireless Protection Policies > Custom Signatures,** and then click **Detail** to access this page. This page enables you to view detailed signature information:

- Precedence—Precedence Order Number.
- Name—Name of the signature, such as Bcast deauth.
- Description—Text description of the signature, such as “Broadcast Deauthentication Frame.”
- Frame Type—Management or Data.
- Action—None or Report.
- Measurement Interval (sec)—Interval in seconds.
- Signature Frequency—Packet match frequency in packets/interval.
- Signature MAC Frequency—Packet match frequency in packets/interval.
- Quiet Time (secs)—Interval in seconds.
- State—Whether the state is enabled or disabled.

Signature Patterns

- Offset—Offset, in bytes, from the start of the packet header or body based on the value of the preceding <offsetStart> where the pattern match operation is to be performed.

- Pattern—Hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.
- Mask—Hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.

Signature Events Summary

Choose **SECURITY > Wireless Protection Policies > Signature Events Summary** to access the Signature Events Summary page.

Table 6-26 Signature Events Summary Parameters

Parameter	Description
Signature Type	Management or data.
Precedence	Precedence order number.
Signature Name	Name of the standard or custom signature.
# Events	Number of attack event occurrences for that particular signature.

Click the signature type to view more detailed information. See the Signature Events Summary Details topic.

Signature Events Summary Details

Choose **SECURITY > Wireless Protection Policies > Signature Events Summary**, and click the signature type to access the Signature Events Summary Details page.

Table 6-27 Signature Events Summary Parameters

Parameter	Description
Signature Type	Management or data.
Precedence	Precedence order number.
Signature Name	Name of the standard or custom signature.
Source MAC Address	MAC address of the attacking client radio.
Track Method	Tracking method AP used to track the signature attacks per signature, source MAC, or both.
Frequency	Packet match frequency in packets/interval (50 per signature and 30 Per MAC tracking method).
# APs	Number of radio interfaces/APs on the channel that detected the attack.
Last Heard	Latest time stamp at which the radio interface/AP detected the attack.

Click **Detail** to view more detailed information. See the Signature Event Track Details topic.

Signature Event Track Details

Choose **SECURITY > Wireless Protection Policies > Signature Events Summary** and then click the Signature Type to access the Signature Event Track Details page.

Table 6-28 Signature Event Detail Parameters

Parameter	Description
Signature Type	Management or data.
Precedence	Precedence order number.
Signature Name	Name of the standard or custom signature.
Source MAC Address	MAC address of the attacking client radio.
Track Method	Tracking method AP used to track the signature attacks per signature, source MAC, or both.
Frequency	Packet match frequency in packets/interval (50 per signature and 30 per MAC tracking method).
# APs	Number of radio interfaces/APs on the channel that detected the attack.
AP MAC Address	Radio MAC address of the AP that detected the attack.
AP Name	Hostname of the AP.
Radio Type	802.11a or 802.11g.
Channel	Radio channel number.
Last Reported by this AP	Time stamp at which the AP reported the attack earlier.

Client Exclusion Policies

Choose **SECURITY > Wireless Protection Policies > Client Exclusion Policies** to access the Client Exclusion Policies page.

This page enables you to configure the Cisco WLC to exclude clients under certain conditions:

- Excessive 802.11 Association Failures—Clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11 Authentication Failures—Clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11X Authentication Failures—Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—Clients are excluded if the IP address is already assigned to another device.
- Excessive Web Authentication Failures—Clients are excluded on the fourth web authentication attempt, after three consecutive failures.

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 Authentication

Choose **SECURITY > Wireless Protection Policies > AP Authentication** to access the AP Authentication Policy page.

This page enables you to set access point authentication policies:

When you enable the AP authentication feature, the access points sending RRM neighbor packets with different RF network names are reported as rogues.

When you enable Infrastructure Management Frame Protection (MFP), it is enabled globally for the Cisco WLC. You can enable or disable Infrastructure MFP validation for a particular access point (All APs Details) or protection for a particular WLAN (Editing WLANs) if MFP is enabled globally for the Cisco WLC.

- Protection Type—None, AP Authentication, or Management Frame Protection. Management Frame Protection is the default if AP Authentication was not previously configured and is the preferred method for authenticating access points.

Note This setting does not affect Client MFP, which is configured per WLAN.

- Alarm Trigger Threshold—AP Authentication sets the number of hits to be ignored from a foreign access point before an alarm is raised. The valid range is from 1 to 255; the default value is 255.

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.

Management Frame Protection Settings

Choose **SECURITY > Wireless Protection Policies > Management Frame Protection** to navigate to the Management Frame Protection page.

General Parameters

Click **General** from the left navigation pane to access the Management Frame Protection Settings > General page.

Table 6-29 General Parameters

Parameter	Description
Management Frame Protection	Disabled/Enabled (globally). **Note** This MFP status represents the status of the Cisco MFP and not the status of 802.11w, introduced in Release 7.4
Controller Time Source Valid	True (time is set externally [for example, NTP]). False (time is set locally).

WLAN Parameters

Click **WLAN** from the left navigation pane to access the Management Frame Protection Settings > WLANs page.

Table 6-30 WLAN Parameters

Parameter	Description
WLAN-ID	Unique identifier.
WLAN Name	Unique identifier.
WLAN Status	Enabled/Disabled.
Infrastructure Protection	Enabled/Disabled. Shows if MFP infrastructure protection is enabled for individual WLANs.

Web Login Page

Choose **SECURITY > Web Auth > Web Login** to navigate to the Web Login page.

This page enables you to customize the content and appearance of the Login page for guest users and all others. It allows you to personalize the login page with a company logo, graphics, colors, type styles, a welcome message, any terms and conditions, and so on.

The login page is shown the first time that you access the WLAN if Web Authentication is turned on (under WLAN Security Policies). Cisco provides a default web login page that can be modified with any text-based HTML editor. However, the User Name and Password fields should not be changed, and the Submit method should be retained. After you create the customized web login page, you must make it into a tar file that contains the page code and any images desired, and then upload to the Cisco WLC through the TFTP server as a Webauth Bundle (see the Download File to Controller page).

Note For Cisco 5508 Wireless Controllers, and Cisco WLC network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under **Security Policies > Web Policy** on the Editing WLANs page.

Table 6-31 Web Login Page Parameters

Parameter	Description
Web Authentication Type	Internal (Default); Customize (Downloaded); External (Redirect to external server). Enable this last option and enter the URL if you want to use a customized login page configured on your web server for web authentication, instead of the default web authentication page provided by the Cisco WLC. The maximum length is 254 characters. **Note** Your web server should be on a different network from the Cisco WLC service port network. If you are using a custom web-auth bundle that is served by the internal Cisco WLC web server, the page should not contain more than 5 elements (including HTML, CSS, and Images) because the internal Cisco WLC web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time (For example Firefox 4) if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection. If you have a complex custom web authentication module, we recommend that you use an external web-auth config on the Cisco WLC, where the full login page is hosted at an external web server. For more information, see the External Web Authentication topic.
Redirect URL after login	URL that you want the user to be redirected after a login. For example, you may enter your company's URL here and the users will be directed to that URL after login. The maximum length is 254 characters. By default, the user is redirected to the URL that was entered in the user's browser before the login page was served.
Headline	Login page headline. For example, "Welcome to Cisco Wireless Network." The maximum length is 127 characters.
Message	Login page message. For example, "Please enter your user name and password" or "This page will not be available from 1:00 Hrs to 2:00 today due to maintenance." The maximum length is 2047 characters.
External Web Server	IP address of the external web server if used.
Preview button	Ability to view either the default page, the customized web login page you created, or the landing page on the external server if that Web Auth option is chosen.
Apply button	Button that you click after previewing your web login page selection. If you have selected a customized (downloaded) page, you will be prompted to ensure that you have downloaded a customized web authentication bundle to the system (Cisco WLC) before applying the setting. If not, this selection fails.

Commands

- Preview—Views either the default page, the customized web login page you created, or the landing page on the external server if that Web Auth option is chosen.

- Apply—Selects a Customized (Downloaded) page, and displays a message asking you to make sure that you have downloaded a customized web authentication bundle to the system (Cisco WLC) before applying the setting. If you do not save, this selection fails.

External Web Authentication

The following steps describe how external web authentication works.

Step 1 When you open a web browser with a URL, it is verified for authentication. If it is not authenticated, the Cisco WLC forwards the request to the Cisco WLC web server to collect authentication details.

Step 2 The Cisco WLC web server then redirects you to the external web server URL that leads you to a login page. At this point, you are also allowed to access the Walled Garden sites (Walled Garden sites are a group of websites that users can browse before they are authenticated on to your wireless network).

Note If you are using an external web server with a Cisco 5500 Series Controller or a Cisco WLC network module, you must configure a preauthentication ACL on the WLAN for the external web server. This ACL should then be set as a WLAN preauthentication ACL under the Web Policy.

Step 3 The login request is sent back to the action URL of the Cisco WLC web server. The Cisco WLC web server submits the username and password for authentication.

Step 4 The Cisco WLC application initiates the RADIUS server request and authenticates you.

Step 5 If successful, the Cisco WLC web connects the client and the Cisco WLC web server forwards you to the configured redirect URL or to the initially requested URL.

Step 6 If user authentication fails, the Cisco WLC web server redirects you to the URL of the user login page.

Cisco Support for External Web Authentication

The Cisco support for external web authentication is as follows:

- External Web Authentication login URL—The Cisco WLC allows you to configure the login URL by using a flag to turn on the External Web Authentication mode. If this flag is configured, you are redirected to the customized login page instead of Cisco's default Web Authentication page.
- CLI commands for External Web Authentication—The following commands are available for configuring external web authentication:

```
custom-web ext-webauth-url <url>
custom-web ext-webauth-mode enable
```

- Provide AP MAC address—The Cisco WLC web server appends the MAC address of the AP with which you are associated with the external webauth URL.
- Provide the connect back URL—The external webauth URL is appended with the Cisco WLC web server URL that can be used by you to connect back and forward the user credentials.

Template for Customer Login Page

You can use the login page template provided by Cisco to develop your own login screen. The template contains the following:

- Hidden attribute names that enable the Cisco WLC to authenticate the user.
- A JavaScript function that extracts the AP MAC address and the redirected URL from the query string.
- A function that sets your web auth page's action URL.

Based on the AP MAC address, you can change your login page using scripts or display a message to the user.

The HTML code for the customer login page template is as follows:

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
      var link = document.location.href;
      var searchString = "redirect=";
      var equalIndex = link.indexOf(searchString);
      var redirectUrl = "";
      if(equalIndex >= 0) {
            equalIndex += searchString.length;
            redirectUrl = "http://";
            redirectUrl += link.substring(equalIndex);
      }
      if(redirectUrl.length > 255)
      redirectUrl = redirectUrl.substring(0,255);
      document.forms[0].redirect_url.value = redirectUrl;

      document.forms[0].buttonClicked.value = 4;
      document.forms[0].submit();
}

function loadAction(){
      var url = window.location.href;
      var args = new Object();
      var query = location.search.substring(1);
      var pairs = query.split("&");
      for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
      }
      //alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The controller URL is " + args.switch_url);
      document.forms[0].action = args.switch_url;
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
```

```
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username" SIZE="25"
MAXLENGTH="63" VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password"
name="password" SIZE="25" MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

Web Authentication Certificate

Choose **SECURITY > Web Auth > Certificate** to navigate to the Web Authentication Certificate page.

This page enables you to view the current web authentication certificate type, download an SSL certificate, or regenerate a new locally generated web auth certificate.

Note The operating system automatically generates a fully functional web authentication certificate as it is loaded onto your Cisco WLC, which means that you do not have to do anything to use certificates with Layer 3 web authentication.

However, if you would like to use a new operating system-generated web authentication certificate, click **Regenerate Certificate**. The operating system generates a new web auth certificate and displays a "Successfully generated Web Authentication Certificate" message. Reboot the Cisco WLC to register the new certificate.

If you prefer to use an externally generated web authentication certificate, verify that the Cisco WLC can ping the TFTP server, check the **Download SSL Certificate** check box, and fill in the following parameters:

- Server IP address.
- Maximum Retries—Maximum number of times each download can be attempted.

- Timeout—Amount of time allowed for each download.
- Certificate File Path—Usually "/" so the TFTP software can use its default directory.
- Certificate File Name—Web authentication certificate filename in encrypted .PEM (Privacy Enhanced Mail) format.
- Certificate Password.

Note The TFTP server cannot run on the same computer as the Cisco WCS, because the Cisco WCS and the TFTP server use the same communication port.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

When you have filled in the required information, click **Apply** and the operating system collects the new certificate from the TFTP server. Reboot the Cisco WLC to register the new certificate.

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.

Click **Regenerate Certificate** to direct the operating system to internally generate a new Web Authentication certificate.

TrustSec

Cisco TrustSec (CTS) enables organizations to secure their networks and services through identity-based access control to anyone, anywhere, anytime. The solution also offers data integrity and confidentiality services, policy-based governance, and centralized monitoring, troubleshooting, and reporting services. CTS can be combined with personalized, professional service offerings to simplify solution deployment and management, and is a foundational security component to Cisco Borderless Networks.

The CTS security architecture builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms. CTS uses the device and user credentials acquired during authentication for classifying the packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on ingress to the CTS network so that they can be correctly identified to apply security and other policy criteria along the data path. The tag, called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. CTS security group tag is applied only when you enable AAA override on a WLAN.

General Configuration

Choose **SECURITY > TrustSec > General** to navigate to the **General** page.

Table 6-32 TrustSec General Parameters

Parameter	Description
CTS	Check box to enable Cisco TrustSec. Only if the CTS check box is enabled, you will be able to configure the Device Id, Password, and Inline Tagging for the controller.
Device ID	The Cisco ISE device ID that can be used to authenticate with other ISE devices.
Password	The Cisco ISE password for this device that can be used to authenticate with other ISE devices.
Inline Tagging	Check box to enable Inline Tagging.
Environment Data	
Current State	Displays the current state of the environment data. Current state can be either complete or not complete.
Last Status	Displays the last state of the environment data. For example, Last status = WAITING_RESPONSE.

Click **Apply** to commit your changes.

Click **Refresh Env Data** to refresh the environment data.

SXP Configuration

Choose **SECURITY > TrustSec > SXP Config** to navigate to the SXP Configuration page.

Table 6-33 TrustSec SXP Parameters

Parameter	Description
Total SXP Connections	Total number of SXP connections configured.
SXP State	Status of SXP connections as either disabled or enabled.
SXP Mode	SXP mode of the Cisco WLC. The Cisco WLC is always set to the Speaker mode in SXP connections.
Default Password	Password for MD5 authentication of SXP messages We recommend that the password contain a minimum of 6 characters.
Default Source IP	IP address of the management interface. The default source IP address for all SXP connections is the management IP address of the Cisco WLC. The source IP address cannot be configured.

Table 6-33 TrustSec SXP Parameters

Parameter	Description
Retry Period	The SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000. The SXP retry period determines how often the Cisco TrustSec software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco TrustSec software makes a new attempt to set up the connection after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.
Peer IP Address	The IP address of the peer, that is the IP address of the next hop switch to which the Cisco WLC is connected.

Click **Add** to create a new SXP connection.

This page also displays the following SXP Connection information:

- **Peer IP Address**—The IP address of the peer, that is the IP address of the next hop switch to which the Cisco WLC is connected.
- **Source IP Address**—The IP address of the source, that is the management IP address of the Cisco WLC.
- **Connection Status**—Status of the SXP connection.

Click **Apply** to commit your changes.

Policy Details

Choose **SECURITY > TrustSec > Policy** to navigate to the Policy details page.

This page displays the Security Group Access Control Lists (SGACLs) for Destination Security Group Tag (D-SGT).

Table 6-34 TrustSec Policy Details

Policy Details	Description
Total SGT Authorization Policy count	The overall SGT authorization policy count.
D-SGT	The destination SGTs applied.
Generation Id	The generation Id of the SGT.
Policy Download Status	The status of the downloaded policy.
Number of clients with this SGT	The clients linked to that SGT.

Table 6-34 TrustSec Policy Details

Policy Details	Description
Refresh period (seconds)	The refresh period describes how often the Cisco TrustSec software refreshes the SGACLs for D-SGT. The valid range is from one second to a week. You can configure this value from a Cisco ISE.
Number of RBACLs for D-SGT	The number of Access Control Entities (ACE) for a given SGACL.

- Click **Refresh All** to refresh all SGTs.
- Click the D-SGT to open the SGT Detail page.

SGT Detail

Choose **SECURITY > TrustSec > Policy** and click the D-SGT to navigate to the SGT Detail page.

This page enables you to view the details of the SGT.

Table 6-35 SGT Details

SGT Details	Description
Policy Matrix for SGT	Name of the D-SGT.
Generation Id	Generation Id of the SGT.
SGACL Name	Lists the SGACL names.
S-SGT	Lists the Source Security Group Tag (S-SGT).
D-SGT	Lists the Destination Security Group Tag (D-SGT).

- Click **Refresh** to refresh a specific SGT.
- Click **Back** to revert back to the Policy details page.
- Click the SGACL Name to open the SGACL Detail page.

SGACL Detail

Choose **SECURITY > TrustSec > Policy** and click the D-SGT to navigate to the SGT Detail page.

In the SGT Detail page, click the SGACL Name to navigate to the SGACL Detail page.

This page enables you to view the details of the SGACL.

This table describes the SGACL details.

Table 6-36 SGACL Details

SGACL Details	Description
SGACL Name	Name of the SGACL
Generation Id	Generation Id of the SGACL
SGACL Policy Capability	Lists the SGACL policy, such as IPv4, IPv6, or IPv4v6
Number of ACEs Associated	Lists the number of associated Access Control Entities (ACEs)
ACEs List Info	List of ACEs associated

Click **Back** to revert back to the SGT Detail page.

Local Policies

Choose **SECURITY > Local Policies** to navigate to the Policy List page.

This page enables you to configure the device-based policies on the Cisco WLC. You can configure policies for a user or a device on the network. The maximum number of policies that you can configure is 64. Click the name of the policy to navigate to the Edit page and update the parameters. For more information, see Configuring Policies.

Click **New** to add a new policy.

Configuring Policies

Choose **SECURITY > Local Policies** and click the name of the policy to navigate to the Edit page. You can define parameters under Match Criteria and specify the policy action for the client. Policies applied on AP groups have more priority than those applied on WLANs.

Note Policies are not applied on WLANs and AP groups if AAA Override is configured on the Cisco WLC.

To apply the configured policies on a WLAN, choose **WLAN**, click the WLAN ID to navigate to the Edit page, and click the **Policy-Mapping** tab. You can configure up to 16 policies on a WLAN.

To apply the configured policies on an AP group, choose **WLAN > Advanced > AP Groups** , click the AP Group name to navigate to the Edit page, and click the **WLAN** tab. You can configure up to 16 policies on an AP group.

Table 6-37 Policy Parameters

Parameter	Description
Policy Name	Name of the policy.
Policy ID	Unique identifier of the policy
Match Criteria	

Table 6-37 Policy Parameters

Parameter	Description
Match Role String	User type or user group of the user, for example, student, employee, and so on.
Match EAP Type	EAP authentication method used by the client. The available methods are as follows: • LEAP • EAP-FAST • EAP-TLS • PEAP
Device Type	Drop-down list from which you can choose a type of device. Click **Add** to add the device to the policy device list.
Device List	Devices configured for the policy.
Action	
IPv4 ACL	Drop-down list from which you can choose an IPv4 ACL for the policy.
VLAN ID	VLAN associated with the policy.
QoS Policy	Drop-down list from which you can choose the QoS policy that can be one of the following: • Platinum (Voice)—Assures a high QoS for Voice over Wireless. • Gold (Video)—Supports high-quality video applications. • Silver (Best Effort)—Supports the normal bandwidth for clients. • Bronze (Background)—Provides the lowest bandwidth for guest services.
Session Timeout	Maximum amount of time, in seconds, before a client is forced to reauthenticate. The default value is 0.
Sleeping Client Timeout	Maximum amount of time, in hours, after the idle timeout before a guest client is forced to reauthenticate. The default value is 12. The range is from 1 to 720.
Flexconnect ACL	Drop down list from which you can choose the Fexconnect ACL for the policy.
AVC Profile	Drop down box lists all the configured AVC profiles on the controller for selection.
Active Hours	
Day	Day of the week on which the policy is active.
Start Time	Start time of the policy.
End Time	End time of the policy.

OpenDNS

Choose **SECURITY > OpenDNS** to navigate to the Open DNS global configuration page.

The Cisco Umbrella WLAN provides a cloud-delivered network security service at the Domain Name System (DNS) level, with automatic detection of both known and emergent threats.

Configuring OpenDNS

Choose **SECURITY > OpenDNS** and select the OpenDNS Global Status check box to enable Open DNS. Paste the API token received from Cisco Umbrella at the OpenDNS-ApiToken field and enter a name at the Profile Name text box and click Add button, to create an OpenDNS profile. All the previously added profiles are listed in the screen.

Click on the Profile Mapped Summary link to see the WLAN, AP Group, and Local Policy mapping for each OpenDNS profile.

This table describes the OpenDNS parameters.

Table 6-38 Open DNS Parameters

Parameter	Description
OpenDNS Global Status	Enables or disables the OpenDNS.
OpenDNS-Api token	API token received from Cisco Umbrella (formerly Open DNS site)
Profile	
Profile Name	Cisco Umbrella profile that can be applied over a WLAN.

Cisco Intrusion Detection System

Cisco WLCs are equipped with sensors to detect intrusion attempts by unauthorized clients. These intruders are added to a shun list, which is forwarded to all Cisco mobility groups. A Renew flag is used to indicate that the Cisco WLC receiving the shun list should remove all entries from the sending Cisco WLC before processing the received list.

In a scenario where the primary Cisco WLC that has a connection to a Cisco Intrusion Detection System sensor is rebooted and some entries on this Cisco Intrusion Detection System sensor have expired, the first query after a reboot should renew and synchronize the newly acquired shun list from this Cisco Intrusion Detection System sensor in the mobility group.

The querying Cisco WLC compares the newly acquired shun list with its local list every time. If a new entry is found, it should be included in the next mmCidsUpdate. If an entry is removed in the new list, it sends this entry in the next mmCidsUpdate with Remaining Minutes set to zero. If the Remaining Minutes are set to zero, the receiving Cisco WLC removes this entry from the shun list.

Cisco Intrusion Detection System Sensors List

Choose **SECURITY > Advanced > CIDS > Sensors** to navigate to the Cisco Intrusion Detection System Sensors List page.

Table 6-39 Cisco Intrusion Detection System Sensors List Parameters

Parameter	Description
Index	Typically 1.
Server Address	URL of the CIDS sensor server.
Port	Typically 443.
State	State that is either enabled or disabled
Query Interval	To be specified in seconds.

Adding Cisco Intrusion Detection System Sensors

Choose **SECURITY > Advanced > CIDS > Sensors > New** to navigate to the Cisco Intrusion Detection System Sensor Add page.

Table 6-40 Cisco Intrusion Detection System Sensor Add Parameters

Parameter	Description
Index	Index value from the drop-down list.
Server Address	URL of the Cisco Intrusion Detection System sensor server.
Port	SNMP port number. The default is 443.
Username	Name that the Cisco WLC uses to authenticate to the IDS sensor. **Note** This username must be configured on the IDS sensor and have at least a read-only privilege.
Password	Password that the Cisco WLC uses to authenticate to the IDS sensor.
Confirm Password	Password that you reenter so that the Cisco WLC can authenticate to the IDS sensor.
Query Interval	Interval in seconds.
State	State that allows you to enable to register the Cisco WLC with this IDS sensor. The default is disabled state.
Fingerprint (SHA1 hash)	40 hexadecimal characters.

Editing Cisco Intrusion Detection System Sensors

Choose **SECURITY > Advanced > CIDS > Sensors** and then click the index number to navigate to the Cisco Intrusion Detection System Sensor Edit page.

Table 6-41 Cisco Intrusion Detection System Sensor Edit Parameters

Parameter	Description
Index	Configured index number.
Server Address	URL of the CIDS sensor server.
Port	SNMP port number. The default is 443.
Username	Name that the Cisco WLC uses to authenticate to the IDS sensor.
Password	Password that the Cisco WLC uses to authenticate to the IDS sensor.
State	Check box that enables you to enable or disable the state. The default is disabled state.
Query Interval	Interval in seconds.
Fingerprint (SHA1 hash)	40 hexadecimal characters.
Last Query (count)	Unknown (0) when disabled.

Cisco Intrusion Detection System Shun List

Choose **SECURITY > Advanced > CIDS > Sensors > Shunned Clients** to navigate to the Cisco Intrusion Detection System Shun List page.

Table 6-42 CIDS Shun List Parameters

Parameter	Description
IP Address	URL of the Cisco WLC Shun List sensor.
Last MAC Address	MAC address of the Shun List sensor.
Expire	Time remaining until expiration of the current list.
Sensor IP/Index	Cisco WLC sensor IP and index number.

Re-sync—Purges and resets the list.

CA Certification

Choose **SECURITY > Advanced > Vendor Certs > CA Certificate** to navigate to the CA Certification page.

This page contains the current CA certificate information. If you choose to add an operator-generated or purchased CA Certificate, paste the new CA certificate ASCII text into the certificate box and click **Apply**.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

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.

Click **Delete Certificate** to delete the current CA Certification. You are prompted to confirm if you select this option.

ID Certificate

Choose **SECURITY > Advanced > Vendor Certs > ID Certificate** to navigate to this page.

This page summarizes existing network ID certificates by the ID certificate name and valid period. An ID certificate can be used by web server operators to ensure secure server operation.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

Click **New** to add a new ID certificate.

Adding ID Certificates

Choose **SECURITY > Advanced > Vendor Certs > ID Certificate** and then click **New** to navigate to the New ID Certificate page.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

This page enables you to add new ID certificates, in addition to the factory-supplied ID certificate. For each new ID certificate, add the following:

- Certificate Name—Certificate name that you can specify.
- Certificate Password—Certificate password (private key).
- Certificate—New ID certificate ASCII text into the Certificate 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.

Management Tab

This tab on the menu bar enables you to access the Cisco WLC management details. Use the left navigation pane to access specific management parameters. Making this selection from the menu bar opens the Summary page.

Summary

Choose **MANAGEMENT > Summary** to navigate to the Summary page. This page displays the network summary.

Table 7-1 Summary Parameters

Parameter	Description
SNMP Protocols	SNMP protocols supported.
Syslog	Log of system events.
HTTP Mode	Access mode for web and secure web.
HTTPS Mode	Status of the HTTPS Secure Shell (SSL) interface that uses secure certificate authentication.
New Telnet Sessions Allowed	Whether or not additional Telnet sessions are permitted.
New SSH Sessions Allowed	Whether or not additional SSH-enabled sessions are permitted.
Management via Wireless	Whether Cisco WLC management from a wireless client is enabled or disabled.

SNMP System Summary

Choose **MANAGEMENT > SNMP > General** to navigate to the SNMP System Summary page. This page enables you to change some of the SNMP system parameters.

Table 7-2 SNMP System Parameters

Parameter	Description
Name	Customer-definable name of the Cisco WLC.
Location	Customer-definable Cisco WLC location.

Table 7-2 SNMP System Parameters

Parameter	Description
Contact	Customer-definable contact details.
System Description	Read-only Cisco WLC description.
System Object ID	Read-only object ID.
SNMP Port Number	Read-only SNMP port number.
Trap Port Number	Definable trap port number; the default value is 162.
SNMP v1 Mode	SNMP v1 mode that you can enable or disable; The default is disabled state.
SNMP v2c Mode	SNMP v2c mode that you can enable or disable; the default is enabled. This parameter should be modified if remote management is desired.
SNMP v3 Mode	SNMP v3 mode that you can enable or disable; the default is enabled. This parameter should be modified if remote management is desired.

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.

SNMP V3 Users

Choose **MANAGEMENT > SNMP > SNMP V3 Users** to navigate to the SNMP V3 Users page. This page provides a summary of the SNMP users.

Table 7-3 SNMP User Summary Parameters

Parameter	Range
User Name	Name of the user profile.
Access Level	Read-only or read-write.
Auth Protocol	None, HMAC-MD5, or HMAC-SHA.
Privacy Protocol	None, CBC-DES, or CFB-AES-128.

To remove a user profile, click the blue arrow adjacent the desired profile and choose **Remove**. You are prompted for confirmation of the user removal.

Click **New** to add a new SNMP user (see the Adding SNMP V3 Users topic).

Adding SNMP V3 Users

Choose **MANAGEMENT > SNMP > SNMP V3 Users** and then click **New** to navigate to the SNMP V3 Users > New page. This page provides a summary of the SNMP users.

Table 7-4 SNMP User Details Parameters

Parameter	Range
User Profile Name	Name of the user profile.
Access Mode	Read-only or read-write.

Table 7-4 SNMP User Details Parameters

Parameter	Range
Authentication Protocol	None, HMAC-MD5, or HMAC-SHA (default). For HMAC-MD5 or HMAC-SHA, enter and confirm an authentication password.
Privacy Protocol	None, CBC-DES, or CFB-AES-128 (default). For CBC-DES, enter and confirm a Privacy Password.

If you select an authentication or privacy protocol, you must enter a password for each.

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.

SNMP Communities

Choose **MANAGEMENT > SNMP > Communities** to navigate to the **SNMP v1 / v2c Community** page.

Edit a user profile by choosing **Edit** (see the Editing SNMP v1/v2c Community topic).

To remove a community, click the blue arrow adjacent the desired community and choose **Remove**. You are prompted to confirm the removal of the community. This page provides a summary of the SNMP community.

Table 7-5 SNMP Community Summary Parameters

Parameter	Range
Community Name	Community string to which this entry grants access. A valid entry is a case-sensitive, alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address (IPv4/IPv6)	IP address from which this device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. From Release 8.0, SNMP community supports IPv4 and IPv6. **Note** If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
IP Mask/Prefix Length	The subnet mask/ prefix length assigned to IPv4/IPv6 address Mask that must be an operand in the AND operation with the requesting entity's IP address before the IP addresses are compared. If the IP addresses match, then the address is an authenticated IP address. For example, if the IP address is 9.47.128.0 and the corresponding subnet mask is 255.255.255.0, a range of incoming IP addresses would match. The incoming IP address could equal 9.47.128.0 to 9.47.128.255. The default value is 0.0.0.0.

Table 7-5 SNMP Community Summary Parameters

Parameter	Range
Access Mode	Access level for this community string. This mode may be specified by choosing read/write or read only from the drop-down list.
Status	Status of this community access entry. When this object is set to enabled, if the community name for this row is not unique among all valid rows, the set request is rejected.

Click **New** to add a new community user profile (see the Adding SNMP v1/v2c Community topic).

Adding SNMP v1/v2c Community

Choose **MANAGEMENT > SNMP > Communities** and then click **New** to navigate to the **SNMP v1 / v2c Community > New** page. This page enables you to add a new SNMP community profile.

Note There is no IPSec support for IPv6.

Table 7-6 SNMP Community Summary Parameters

Parameter	Range
Community Name	Community string to which this entry grants access. A valid entry is a case-sensitive, alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address (IPv4/IPv6)	IP address from which this device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. From Release 8.0, SNMP community supports IPv4 and IPv6. **Note** If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
IP Mask/Prefix Length	The subnet mask/ prefix length assigned to IPv4/IPv6 address. Mask that must be the AND operand with the requesting entity's IP address before the IP addresses are compared. If the IP addresses match, then the address is an authenticated IP address. For example, if the IP address is 9.47.128.0 and the corresponding subnet mask is 255.255.255.0, a range of incoming IP addresses would match, that is, the incoming IP address could equal 9.47.128.0 to 9.47.128.255. The default value is 0.0.0.0. **Note** For IPv6 input, enter Prefix Length.
Access Mode	Access level for this community string. This mode, may be specified by selecting read/write or read-only from the drop-down list.

Table 7-6 SNMP Community Summary Parameters

Parameter	Range
Status	Status of this community access entry. When this object is set to enabled, if the community name for this row is not unique among all valid rows, the set request is rejected. Community names may be made invalid by choosing disable.
IPSec Parameters	
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see "IPSEC" section on page 7-14.

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.

Editing SNMP v1/v2c Community

Choose **MANAGEMENT > SNMP > Communities** and then click **Edit** to navigate to the **SNMP v1 / v2c Community > Edit** page.

This page allows you to enable or disable an SNMP community profile. All fields are read-only except the Status text box.

Note There is no IPSec support for IPv6.

Table 7-7 SNMP Community Summary Parameters

Parameter	Range
Community Name	Community string to which this entry grants access. A valid entry is a case-sensitive, alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address (IPv4/IPv6)	IP address from which this device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. From Release 8.0, SNMP community supports IPv4 and IPv6. **Note** If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.

Table 7-7 SNMP Community Summary Parameters

Parameter	Range
IP Mask/Prefix Length	The subnet mask/ prefix length assigned to IPv4/IPv6 address. Mask that must be the AND operand with the requesting entity's IP address before the IP addresses are compared. If the IP addresses match, then the address is an authenticated IP address. For example, if the IP address is 9.47.128.0 and the corresponding subnet mask is 255.255.255.0, a range of incoming IP addresses would match, that is, the incoming IP address could equal 9.47.128.0 to 9.47.128.255. The default value is 0.0.0.0. **Note** For IPv6 input, enter Prefix Length.
Access Mode	Access level for this community string. This mode may be specified by selecting read/write or read-only from the drop-down list.
Status	Status of this community access entry. When this object is set to enabled, if the community name for this row is not unique among all valid rows, the set request is rejected. Community names may be made invalid by choosing disable.
IPSec Parameters	
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see "IPSEC" section on page 7-14.

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.

SNMP Trap Receiver

Choose **MANAGEMENT > SNMP > Trap Receivers** to navigate to the **SNMP Trap Receiver** page.

Edit a user profile by choosing **Edit** (see the Editing SNMP Trap Receivers topic).

Remove a user profile by choosing **Remove**. You are prompted for confirmation of the trap removal. This page provides a summary of existing SNMP trap receivers.

Table 7-8 SNMP Trap Receiver Summary Parameters

Parameter	Range
Community Name	Name of the server where the traps are sent.
IP Address (IPv4/IPv6)	IP address of the server. From Release 8.0, SNMP trap receiver support IPv4 and IPv6.
Status	Status that must be enabled for the SNMP traps to be sent to the server.
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see "IPSEC" section on page 7-14.

Click **New** to add a new trap receiver (see the Adding SNMP Trap Receivers topic).

Adding SNMP Trap Receivers

Choose **MANAGEMENT > SNMP > Trap Receivers** and then click **New** to navigate to the **SNMP Trap Receiver > New** page.

This page enables you to add a server to receive SNMP traps from this Cisco WLC.

Table 7-9 SNMP Trap Receiver Detail Parameters

Parameter	Range
Community Name	Name of the server where the traps are sent.
IP Address (IPv4/IPv6)	IP address of the server. From Release 8.0, SNMP trap receiver support IPv4 and IPv6.
Status	Status that you must enable for the SNMP traps to be sent to the receiver. The default is enabled.
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see "IPSEC" section on page 7-14.

Note There is no IPSec support for IPv6.

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.

Editing SNMP Trap Receivers

Choose **MANAGEMENT > SNMP > Trap Receivers** and then click the Community Name to edit an SNMP trap receivers and its IPSec details.

Note There is no IPSec support for IPv6.

This page enables you to configure sending traps to a particular server. Only the Status text box can be modified.

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.

SNMP Trap Controls

Choose **MANAGEMENT > SNMP > Trap Controls** to navigate to the SNMP Trap Controls page.

This page enables you to select which traps logs should be captured. Choose the applicable logs and choose **Apply**.

Note Select the **Select All** check box to enable all traps on a tab. Unselect the **Select All** check box to disable all traps on a tab.

General Tab

Table 7-10 General Tab Parameters

Trap Name	Description
Link (Port) Up/Down	Port changes status from up or down.
Spanning Tree[1]	Spanning tree traps. Refer to the STP specifications for descriptions of individual parameters.
Config Save	Notification sent when the configuration is modified.
RFID Limit Reached	Notification sent when the number of RFID tags on the Cisco WLC exceeds the threshold limit defined in the Threshold field.
Threshold	Threshold number of the RFID tags on the Cisco WLC to trigger a trap.

1. The Cisco 5500 Series Controllers do not support the Spanning Tree Protocol.

Client Tab

Table 7-11 Client Tab Parameters

Trap Name	Description
802.11 Association	Associate notification sent when the client sends an association frame.
802.11 Disassociation	Disassociate notification sent when the client sends a disassociation frame.
802.11 Deauthentication	Deauthenticate notification sent when the client sends a deauthentication frame.
802.11 Failed Authentication	Authenticate failure notification sent when the client sends an authentication frame with a status code other than successful.
802.11 Failed Association	Associate failure notification sent when the client sends an association frame with a status code other than successful.
Exclusion	Associate failure notification sent when a client is Exclusion Listed (blacklisted).
Authentication	Authentication notification sent when a client is successfully authenticated.
Max Clients Limit Reached	Notification sent when the maximum number of clients, defined in the **Threshold** field, have been associated with the Cisco WLC.
NAC Alert	Alert that is sent when a client joins an SNMP NAC-enabled WLAN. This notification is generated when clients on NAC-enabled SSIDs complete Layer 2 authentication. This trap is to inform the NAC appliance about the client's presence.
Association with Stats	Associate notification sent with data statistics when a client associates with the Cisco WLC or roams. The data statistics include transmitted and received bytes and packets.
Disassociation with Stats	Disassociate notification sent with data statistics when a client disassociates from the Cisco WLC. The data statistics include transmitted and received bytes and packets, SSID, and session ID.

AP Tab

Table 7-12 AP Tab Parameters

Trap Name	Description
AP Register	Notification sent when the access point associates or disassociates with the Cisco WLC.
AP Interface Up/Down	Notification sent when the access point interface (802.11a/n or 802.11b/g/n) status changes to up or down.
AP Authorization	AP authorization that you can enable or disable. The default is enabled.
AP SSID Key Conflict	Notification sent when two SSIDs on an AP have the same cipher key.
AP Mode Change	Notification sent when the access point mode changes.
AP Time Sync Failure	Notification sent when the heartbeat (for example, 60s) between the Cisco WLC and the AP is lost or the connection breaks.

Security Tab

Table 7-13 Security Tab Parameters

Trap Name	Description
AAA Traps	
User Authentication	Trap to inform that a client RADIUS authentication failure has occurred.
RADIUS Servers Not Responding	Trap to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
802.11 Security Traps	
WEP/WPA Decrypt Error	Trap to inform that an error has occurred while a WEP/WPA entity is being decrypted.
IDS Signature Attack	IDS Signature attack that you can enable or disable. The default is enabled.
Rogues	
Rogue AP	Trap that is sent with its MAC address whenever a rogue access point is detected. When a rogue access point that was detected earlier no longer exists, this trap is sent.
Adjacent Channel Rogue	Notification sent when a rogue AP is detected in the adjacent channels and if it has been removed from the network.
Management Traps	
SNMP Authentication	SNMPv2 entity that has received a protocol message that is not properly authenticated.
Multiple Users	Two users that log in with the same login ID.
Strong Password	Strong password check that you enable or disable.

Auto RF Tab

Table 7-14 Auto RF Tab Parameters

Trap Name	Description
Auto RF Profile	
Load Profile	Notification sent when the Load Profile state changes between PASS and FAIL.
Noise Profile	Notification sent when the Noise Profile state changes between PASS and FAIL.
Interference Profile	Notification sent when the Interference Profile state changes between PASS and FAIL.
Coverage Profile	Notification sent when the Coverage Profile state changes between PASS and FAIL.
Auto RF Update Traps	
Channel Update	Notification sent when the access point's dynamic channel algorithm is updated.
Tx Power Update	Notification sent when the access point's dynamic transmit power algorithm is updated.

Mesh Tab

Table 7-15 Mesh Tab Parameters

Trap Name	Description
Child Excluded Parent	Notification sent when the child access point marks a parent access point for exclusion. When the child fails to authenticate at the Cisco WLC after a fixed number of times, the child marks the parent for exclusion. The child remembers the excluded MAC address and informs the Cisco WLC when it joins the network. The child access point marks the MAC address and excludes it for the time determined by MAP node so that it does not try to join this excluded node. The child MAC address is sent as part of the index.
Parent Change	Notification sent when a child moves to another parent. The alarm includes the MAC addresses of the former and current parents.
Authfailure Mesh	Notification sent when the access point tries to join the mesh but fails to authenticate because it is not in the MAC filter list. The trap contains the MAC address of the AP that failed authorization.
Child Moved	Notification sent when the parent access point loses connection with its child.
Excessive Parent Change	Notification sent when the number of parent changes for a given mesh access point exceeds the threshold. Each access point keeps count of the number of parent changes within a fixed time. If the count exceeds the threshold defined by c1MeshExcessiveParentChangeThreshold, then the child access point informs the Cisco WLC.
Excessive Children	Notification sent when the child count of an access point exceeds 10 (default) children. RAP and MAP need to be handled separately. RAP allows more than 10 (default) children up to 20 (default) children.

Table 7-15 Mesh Tab Parameters

Trap Name	Description
Poor SNR	Notification sent when the child access point detects a signal-to-noise ratio (SNR) below 12 dB on the backhaul link. The alarm includes the SNR value and the MAC addresses of the parent and child.
Console Login	Notification sent when a login on the MAP console is successful or when a failure occurs after three attempts.
Excessive Association	Notification sent when the MAP access point associates more than 5 times within 60 minutes.
Default Bridge Group Name	Notification sent when a MAP mesh node joins parent using the “default” bridge group name.
Excessive Hopcount	Notification sent when the number of hops from the Mesh access point (MAP) node to the root access point (RAP) exceeds the threshold defined by clMeshExcessiveHopCountThreshold.
Secondary Backhaul Change	Notification sent when the MAP changes the backhaul from primary to secondary.
PSK Auth Failure	Notification sent when WPA/WPA2-PSK authentication failure occurs.

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.

SNMP Trap Logs

Choose **MANAGEMENT > SNMP > Trap Logs** to navigate to the **Trap Logs** page.

This page enables you to view the trap logs that have been captured by the Cisco WLC. Each trap entry includes the log number, system time, and trap description.

This page also displays the number of traps since the last reset and number of traps since log last viewed.

Note Review the following client reason and status codes. You are likely to encounter them when reviewing the trap logs.

Client Reason Code Descriptions

Table 7-16 Client Reason Code Parameters

Client Reason Code	Description	Meaning
0	noReasonCode	Normal operation.
1	unspecifiedReason	Client associated but no longer authorized.
2	previousAuthNotValid	Client associated but not authorized.
3	deauthenticationLeaving	Access point went offline; deauthenticating the client.

Table 7-16 Client Reason Code Parameters

Client Reason Code	Description	Meaning
4	disassociationDueToInactivity	Client session timeout exceeded.
5	disassociationAPBusy	Access point is busy.
6	class2FrameFromNonAuthStation	Client attempted to transfer data before it was authenticated.
7	class2FrameFromNonAssStation	Client attempted to transfer data before it was associated.
8	disassociationStaHasLeft	Operating system moved the client to another access point using nonaggressive load balancing.
9	staReqAssociationWithoutAuth	Client not authorized yet; still attempting to associate with an access point.
99	missingReasonCode	Client momentarily in an unknown state.

Client Status Code Descriptions

Table 7-17 Client Status Code Parameters

Client Status Code	Description	Meaning
0	idle	Normal operation; no rejections of client association requests.
1	aaaPending	Completing an AAA transaction.
2	authenticated	802.11 authentication is completed.
3	associated	802.11 association is completed.
4	powersave	Client is in powersave mode.
5	disassociated	802.11 disassociation is completed.
6	tobedeleted	Client is deleted after disassociation.
7	probing	Client not associated or authorized yet.
8	disabled	Automatically disabled by the operating system for an operator-defined time.

Click **Clear Log** to delete all log entries. You are prompted for confirmation to delete the logs.

HTTP-HTTPS Configuration

Choose **MANAGEMENT > HTTP-HTTPS** to navigate to the HTTP-HTTPS Configuration page.

This page enables you to configure the following settings for Web Mode or Secure Web Mode:

- HTTP Access—HTTP Web User Interface that is accessible using a login and password. If you disable HTTP Web Mode, you must enable Secure Web Mode or you must use the CLI or Cisco Wireless Control System interface to configure the Cisco WLC. If you disable Web Mode and Secure Web Mode, you must use the CLI interface to configure the Cisco WLC.
- HTTPS Access—HTTPS Secure Shell (SSL) interface that is accessible using secure certificate authentication (configured below). This is the default access. If you disable HTTPS Secure Web Mode, you must enable Web Mode or you must use the CLI or Cisco Wireless Control System interface to configure the Cisco WLC.
- Web Session Timeout—Amount of inactivity (in minutes) before the session times out.
- Current Certificate**—**Name, Type, Serial Number, Valid, Subject Name, Issuer Name, MD5 Fingerpoint, and SHA1 Fingerpoint.
- Download SSL Certificate**—**Certificate that you use to download an SSL Web Admin Certificate from a local TFTP server. Select the **Download SSL Certificate** check box to display the following entries:
  - Server IP Address—IP address of the local TFTP server.
  - Maximum Retries—Maximum number of times each download can be attempted.
  - Timeout—Amount of time allowed for each download.
  - Certificate File Path—Usually either \ or /, as most TFTP servers automatically determine the path to their default file location. Otherwise, use the TFTP server absolute file path.
  - Certificate File Name—Web Administration Certificate filename in encrypted PEM (Privacy Enhanced Mail) format.
  - Certificate Password—SSL certificate password that is used to decrypt the SSL Web Admin Certificate.

Note The TFTP server cannot run on the same computer because the Cisco Prime Infrastructure and the TFTP server use the same communication port.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

Click **Apply** and **Yes** to download the SSL Web Admin Certificate. The operating system informs you of the file transfer and the certificate installation progress.

The SSL password decrypts the certificate, and the certificate is used for Secure Web Mode access when activated.

Note You must save the configuration changes and reboot the Cisco WLC after changing the SSL certificate.

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

Click **Delete Certificate** to instruct the operating system to delete the current SSL certificate.

Click **Regenerate Certificate** to instruct the operating system to generate a new SSL certificate to replace any existing certificate; the Web User Interface displays the "Successfully Generated SSL Web Admin Certificate" message when done.

IPSEC

Choose **MANAGEMENT > IPSEC** to navigate to the **IPSEC Profile Name** page.

Click **New** to create a new IPSEC profile.

On the **IPSEC Profile Name** page, click an IPSEC profile name to edit the profile.

Table 7-18 IPSEC Profile Parameters

Parameter	Range
IPSec Profile Name	Name of the IPSec profile that you created.
IKE Version	IKE version: 1 or 2.
Encryption	IP security encryption mechanism used.
Authentication	IP security authentication protocol used.
IKE DH Group	Set the IKE Diffie-Hellman Group. The options are as follows: • Group 14 (2048 bits) • Group 19 (256 bits) • Group 20 (384 bits) Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.
IKE Lifetime	IKE lifetime in seconds. Valid range is between 1800 and 57600. Default value is 28800 seconds.
IPSec Lifetime	IPSec lifetime in seconds. Valid range is between 1800 and 57600. Default value is 1800 seconds.
IKE Phase1	Internet Key Exchange protocol (IKE). Options are as follows: • Aggressive • Main IKE Phase1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets, with a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.
IKE Peer Identification	IKE peer identification mode. Options include: • FQDN • User FQDN • CN • IP
IKE Peer Value	Peer value for IKE that you can specify.

Table 7-18 IPSEC Profile Parameters

Parameter	Range
IKE Authentication Mode	IKE authentication method as either PSK or Certificate.
Shared Secret Format	Format of the shared secret that you set to either ASCII of Hex.
Shared Secret	RADIUS Server login Shared Secret.
Confirm Shared Secret	RADIUS Server login Shared Secret.

Telnet-SSH Configuration

Choose **MANAGEMENT > Telnet-SSH** to navigate to the Telnet-SSH Configuration page.

Note Only FIPS approved algorithm 128-cbc is supported when using SSH to control WLANs.

This page enables you to modify the following settings for Telnet accessibility to the Cisco WLC:

- Session Timeout (minutes)—Number of minutes that a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The timeout may be specified as a number from 0 to 160. The default is 5 minutes.
- Maximum Number of Telnet Sessions—Values from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed. The default is 5.
- Allow New Telnet Sessions—Whether new Telnet sessions are not allowed on the DS port when set to no. The default is no.

Note New Telnet sessions are allowed or disallowed on both the DS (network) port and the Service port using the Allow New Telnet Sessions parameter.

- Allow New SSH Sessions—Whether new Secure Shell Telnet sessions are not allowed when set to no. The default value is yes.

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.

Serial Port Configuration

Choose **MANAGEMENT > Serial Port** to navigate to the Serial Port Configuration page. This page enables you to modify configurable serial session properties.

This table describes the serial port configuration parameters.

Table 7-19 Serial Port Configuration Parameters

Parameter	Description	Range
Serial Port Login Timeout (Seconds)	Time, in minutes, of inactivity on a serial port connection, after which the Cisco WLC closes the connection.	Any numeric value between 0 and 9600 is allowed. The default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	Default baud rate at which the serial port tries to connect.	The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The default is 9600 baud.
Character Size (bits)	Number of bits in a character.	8 (read-only).
Flow Control	Whether hardware flow control is enabled or disabled.	Disabled (read-only).
Stop Bits	Number of stop bits per character.	1 (read-only).
Parity	Parity method used on the serial port.	None (read-only).

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.

Local Management Users

Choose **MANAGEMENT > Local Management Users** to navigate to the Local Management Users page.

This page lists current management user logins on the Cisco WLC and the users' access privileges.

You may remove a user account by click the blue arrow adjacent the desired account and choose **Remove**.

Caution Removing the default admin user prohibits both web and CLI access to the Cisco WLC. Therefore, you must create a user with administrative (read/write) privileges before you remove the default user.

- Click **New** to add a new management user. For more information, see the Adding Local Management Users topic.

Adding Local Management Users

Choose **MANAGEMENT > Local Management Users** and then click **New** to navigate to the **Local Management Users > New** page.

This page enables you to add management user accounts on the Cisco WLC and the user's access privileges.

The settings for the Management User Details parameters depends on the settings that you make in the Password Policy page. The following requirements are enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain a management username or the reverse letters of a username.
- The password should not contain words like Cisco, oscic, admin, nimda, or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

This table describes the management user details parameters.

Table 7-20 Management User Details Parameters

Parameter	Description
User Name	Login username.
Password	User password. The default is admin.
Confirm Password	User password that you confirm. The default is admin.
User Access Mode	User privilege assignment (Read-Only, Read-Write, or Lobby Admin) that you create for Guest User Accounts.
Telnet Capable	Check box that you can select to enable local management users to Telnet to the Cisco WLC. By default, this feature is enabled. You must enable global Telnet to enable this feature. SSH connection is not affected when you enable this option.

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.

Guest User Accounts

The first step in creating guest user accounts is for the system administrator to set up a lobby administrator account, also known as a Lobby Ambassador account. A Lobby Ambassador account has limited configuration privileges and has access only to the pages that are used to configure and manage guest user accounts. This feature enables a nontechnical person to create and manage guest user accounts on the Cisco WLC.

A guest user account can provide a user account for a limited amount of time. The Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires.

To create a guest user account, log out of the Cisco WLC and log back in again as Lobby Administrator. You will view the guest user accounts you create on the Cisco WLC (and all others) on the local net user's page (see the Local Net Users topic).

Lobby Ambassador Account Setup

Step 1 Go to **Management > Local Management Users > New**.

Step 2 Create a username for the Lobby Ambassador account and enter it in the User Name text box.

Step 3 Create a password for the Lobby Ambassador account and enter it in the Password text box.

Step 4 Reenter the Lobby Ambassador account password in the Confirm Password text box.

Step 5 Select **LobbyAdmin** in the User Access Mode box.

Step 6 Click **Apply**. The Local Management Users page opens and displays all registered users, including the new username that you just created, identified as LobbyAdmin. You may create additional new users from this page, or remove any except the admin user.

Adding Guest User Accounts

Step 1 Log into the Cisco WLC user as Lobby Ambassador.

Step 2 Click **Configure > Controller Templates** to display the NTP Server Templates page.

Step 3 From the left navigation, choose **Security**, and then choose **Guest Users** to display the Guest Users page.

Step 4 From the Select a Command drop-down list, choose **Add Template** and click **GO**.

Step 5 On the Guest User > New Template page, follow these steps to add a new guest user account:

a. Enter the guest username. The maximum is 24 characters.

b. Select the check box to generate an automatic password or enter a password. If you enter a password, enter it twice to confirm. The generated password is automatically entered into the password text box.

Note Passwords are case sensitive.

c. From the drop-down list, choose an SSID (WLAN Service Set Identifier). The SSID that this guest user applies must be a WLAN that has a Layer 3 web authentication policy configured. Your administrator can advise which SSID to use.

d. Enter a description of the guest user account.

e. From the drop-down list, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 30 days. A value of zero (0) implies infinity and will be a permanent account.

Step 6 Click **Save** to save your changes or click **Cancel** to leave the settings unchanged. When you click Save, the screen refreshes and includes the following:

- Save—Save your changes.
- Apply to Controllers—The Apply to Controller page appears. Select the check box for the Cisco WLC or Config Group name that the guest user account applies to and click **OK**. If you do not want to apply to Cisco WLCs, click **Cancel**. If you click OK, the Apply to Controllers page refreshes and shows the operation status. If the operation status shows as successful, the guest user account has been completed and can be used immediately.
- The Account Expiry page displays the Cisco WLC to which the guest user account was applied and the seconds remaining before the guest user account expires.
- Delete—Deletes the displayed guest user template.
- Cancel—Disregards any settings or changes.

User Sessions

Choose **MANAGEMENT > User Sessions** to navigate to the **CLI Sessions** page. This page provides a list of open CLI sessions.

Table 7-21 CLI Session Details Parameters

Parameter	Description
ID	Session identification.
User Name	Login username.
Login Type	Telnet or serial session.
Connection From	Name of the client computer system or the physical port.
Idle time	Elapsed inactive session time.
Session Time	Elapsed active session time.

To stop an existing Telnet session, click the blue arrow adjacent the desired session and choose **Close**.

Syslog Configuration

Choose **MANAGEMENT > Logs > Config** to navigate to the Syslog Configuration page.

This page enables you to configure system logs.

If you enable system logs, enter the IP address of the server to which to send the syslog messages and click **Add**. You can add up to three syslog servers to the Cisco WLC. The list of syslog servers that have already been added to the Cisco WLC appears below this field.

Syslog Server

Table 7-22 Syslog Server Parameters

Parameter	Description
Syslog Server IP Address (IPv4/IPv6)	Enter the IPv4/ IPv6 address of the Syslog server address. **Note** You can only add a maximum of 3 Syslog servers.

Table 7-22 Syslog Server Parameters

Parameter	Description
Syslog Level	Severity level for filtering syslog messages to the syslog servers: • Emergencies—Severity level 0 • Alerts—Severity level 1 (default value) • Critical—Severity level 2 • Errors—Severity level 3 • Warnings—Severity level 4 • Notifications—Severity level 5 • Informational—Severity level 6 • Debugging—Severity level 7 **Note** If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the Cisco WLC. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.
Syslog Facility	Facility for outgoing syslog messages to the syslog servers: • Kernel—Facility level 0 • User Process—Facility level 1 • Mail—Facility level 2 • System Daemons—Facility level 3 • Authorization—Facility level 4 • Syslog—Facility level 5 (default value) • Line Printer—Facility level 6 • USENET—Facility level 7 • Unix-to-Unix Copy—Facility level 8 • Cron—Facility level 9 • FTP Daemon—Facility level 11 • System Use 1—Facility level 12 • System Use 2—Facility level 13 • System Use 3—Facility level 14 • System Use 4—Facility level 15 • Local Use 0—Facility level 16 • Local Use 1—Facility level 17 • Local Use 2—Facility level 18 • Local Use 3—Facility level 19 • Local Use 4—Facility level 20 • Local Use 5—Facility level 21 • Local Use 6—Facility level 22 • Local Use 7—Facility level 23

Msg Log Configuration

Table 7-23 Msg Log Configuration Parameters

Parameter	Description
Buffered Log Level	Severity level for logging messages to the Cisco WLC buffer and console: • Emergencies—Severity level 0 • Alerts—Severity level 1 • Critical—Severity level 2 • Errors—Severity level 3 (default value) • Warnings—Severity level 4 • Notifications—Severity level 5 • Informational—Severity level 6 • Debugging—Severity level 7 • Disable—Disable console logging
Console Log Level	
File Info	Information about the source file.The default is enabled.
Trace Info	Traceback information. The default is disabled state.

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.

Message Logs

Choose **MANAGEMENT > Logs > Message logs** to navigate to the Message Logs page.

This page enables you to view the message logs that have been captured by the Cisco WLC, by the last to the first message. Each trap entry includes the system time, filename and line, message type and message.

Click **Clear** to purge the existing message log..

Management Via Wireless

Choose **MANAGEMENT > Mgmt Via Wireless** to navigate to the Management Via Wireless page. This page enables you to configure access to the Cisco WLC management interface from wireless clients using IPv4 and IPv6 methods. The default is disabled state.

Note Due to IPsec limitations, the Management Via Wireless feature is available only if you log in across WPA, Static WEP, or VPN Pass Through WLANs. The Management feature is not available if you attempt to log on through an IPsec 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.

Cloud Services

Choose **MANAGEMENT > Cloud Services** to navigate to the **Cloud Services** page. This page enables you to configure the CMX Cloud in the Cisco WLC. HTTPS protocol is used to connect the Cisco WLC and the CMX cloud.

Server

Table 7-24 Cloud Server Configuration Parameters

Parameter	Description
URL	The CMX server URL.
Id-Token	Cloud server Id-token issued for Cisco WLC.

CMX

Table 7-25 Cloud CMX Configuration Parameters

Parameter	Description
Service Status	CMX service that you can enable or disable.
Connectivity Mode	Communication protocol used to connect the Cisco WLC with the CMX server (read-only).
Link Status	The current status of the link (read-only).

Installing and Configuring Licenses

You can order Cisco 5508 Wireless Controllers with support for 12, 25, 50, 100, 250 or 500 access points as the Cisco WLC's base capacity. You can add additional access point capacity through capacity adder licenses available at 25, 50, 100, and 250 access point capacities. You can add the capacity adder licenses to any base license in any combination to arrive at the maximum capacity of 500 access points. The base and adder licenses are supported through both rehosting and RMAs.

The base license supports the standard base software set and, for 6.0196.0 and later releases, the premium software set is included as part of the base feature set, which includes this functionality:

- Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links.

About the availability of data DTLS for the 7.0.116.0 release:

  – Cisco 5500 Series Controller—The Cisco 5500 Series Controller will be available with two licensing options: one with data DTLS capabilities and another image without data DTLS.

  - Cisco 7500, 2500, WiSM2—These platforms by default will not contain DTLS. To turn on data DTLS, a license must be installed. That is, these platforms will have a single image with data DTLS turned off. To use data DTLS you must have a license.

- Support for OfficeExtend Access Points, which are used for secure mobile telecommuting. For more information about OfficeExtend access points, see OfficeExtend Access Points.

All features included in a Wireless LAN Controller WPLUS license are now included in the base license; this change is introduced in release 6.0.196.0. There are no changes to WCS BASE and PLUS licensing. These WPLUS license features are included in the base license:

- OfficeExtend AP
- Enterprise Mesh
- CAPWAP Data Encryption

The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:

- If you have a WPLUS license and you upgrade from 6.0.x.x to 7.0.98.0, your license file contains both Basic and WPLUS license features. You will not see any disruption in feature availability and operation.
- If you have a WPLUS license and you downgrade from 7.0.98.0 to 6.0.196.0 or 6.0.188 or 6.0.182, your license file contains only base license, and you will lose all WPLUS features.
- If you have a base license and downgrade from 6.0.196.0 to 6.0.188 or 6.0.182, when you downgrade, you lose all WPLUS features.

To view the Cisco WLC trap log, choose **Monitor** and click **View All** under "Most Recent Traps" on the Cisco WLC GUI.

Note You can also view traps by using SNMP-based management tools.

The ap-count licenses and their corresponding image-based licenses are installed together. The Cisco WLC keeps track of the licensed access point count and does not allow more than the number of access points to associate to it.

The Cisco 5500 Series Controller is shipped with both permanent and evaluation base and base-ap-count licenses. If desired, you can activate the evaluation licenses, which are designed for temporary use and set to expire after 60 days.

No licensing steps are required after you receive your Cisco 5500 Series Controller because the licenses you ordered are installed at the factory. In addition, licenses and product authorization keys (PAKs) are preregistered to serial numbers. However, as your wireless network evolves, you might want to add support for additional access points or upgrade from the standard software set to the base software set. To do so, you need to obtain and install an upgrade license.

Obtaining an Upgrade License

A certificate with a product authorization key (PAK) is required before you can obtain an upgrade license.

You can use the capacity adder licenses to increase the number of access points supported by the Cisco WLC up to a maximum of 500 access points. The capacity adder licenses are available in access point capacities of 10, 25, 50, 100 and 250 access points. You can add these licenses to any of the base capacity licenses of 12, 25, 50, 100 and 250 access points.

For example, if your Cisco WLC was initially ordered with support for 100 access points (base license AIR-CT5508-100-K9), you could increase the capacity to 500 access points by purchasing a 250 access point, 100 access point, and a 50 access point additive capacity license (LIC-CT5508-250A, LIC-CT5508-100A, and LIC-CT5508-50A).

You can find more information on ordering capacity adder licenses at this URL: http://www.cisco.com/c/en/us/products/wireless/5500-series-wireless-controllers/datasheet-listing.html

If you skip any tiers when upgrading (for example, if you do not install the -25U and -50U licenses along with the -100U), the license registration fails.

For a single Cisco WLC, you can order different upgrade licenses in one transaction (for example, -25U, -50U, -100U, and -250U), for which you receive one PAK with one license. Then you have only one license (instead of four) to install on your Cisco WLC.

If you have multiple Cisco WLCs and want to upgrade all of them, you can order multiple quantities of each upgrade license in one transaction (for example, you can order 10 each of the -25U, -50U, -100U, and -250 upgrade licenses), for which you receive one PAK with one license. You can continue to register the PAK for multiple Cisco WLCs until it is exhausted.

Base license SKUs for the Cisco Flex 7500 Series Controllers are as follows:

- AIR-CT7510-300-K9
- AIR-CT7510-500-K9
- AIR-CT7510-1K-K9
- AIR-CT7510-2K-K9

Base license SKUs for the Cisco 5500 Series Controllers are as follows:

- AIR-CT5508-12-K9
- AIR-CT5508-25-K9
- AIR-CT5508-50-K9
- AIR-CT5508-100-K9
- AIR-CT5508-250-K9
- AIR-CT5508-500-K9

The capacity adder SKUs are as follows:

- LIC-CT5508-10A
- LIC-CT5508-25A
- LIC-CT5508-50A
- LIC-CT5508-100A
- LIC-CT5508-250A

Base license SKUs for the Cisco 2500 Series Controllers are as follows:

- AIR-CT2504-5-K9
- AIR-CT2504-15-K9
- AIR-CT2504-25-K9
- AIR-CT2504-50-K9

Base license SKUs for the Cisco WiSM2 Controllers are as follows:

- WS-SVC-WISM2-1-K9—WiSM2 with 100 AP support

- WS-SVC-WISM2-3-K9—WiSM2 with 300 AP support
- WS-SVC-WISM2-5-K9—WiSM2

To obtain and register a PAK certificate, follow these steps:

Step 1 Order the PAK certificate for an upgrade license through your Cisco channel partner or your Cisco sales representative, or order it online at this URL:

http://www.cisco.com/web/ordering/root/index.html

Step 2 If you are ordering online, begin by choosing the primary upgrade SKU L-LIC-CT5508-UPG or LIC CT5508-UPG. Then, choose any number of the following options to upgrade one or more Cisco WLCs under one PAK.

This table describes the controller configuration parameters.

Table 7-26 License Agent Configuration Parameters

Type	Part Number	Description
email	L-LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many Cisco WLCs under one product authorization key
	L-LIC-CT5508-25A	25 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT5508-50A	50 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT5508-100A	100 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT5508-250A	250 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT2504-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many Cisco WLCs under one product authorization key
	L-LIC-CT2504-5A	5 AP Adder License for Cisco 2504 Wireless Controller (e-Delivery)
	L-LiC-CT2504-25A	25 AP Adder License for Cisco 2504 Wireless Controller (E-Delivery)

Table 7-26 License Agent Configuration Parameters

Type	Part Number	Description
paper	LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU, to upgrade one or many Cisco WLCs under one product authorization key
	LIC-CT5508-25A	25 AP Adder License for the Cisco 5508 Controller
	LIC-CT5508-50A	50 AP Adder License for the Cisco 5508 Controller
	LIC-CT5508-100A	100 AP Adder License for the Cisco 5508 Controller
	LIC-CT5508-250A	250 AP Adder License for the Cisco 5508 Controller
	LIC-CT2504-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this sku to upgrade one or many Cisco WLCs under one product authorization key
	LIC-CT2504-5A	5 AP Adder License for Cisco 2504 Controller (Paper Certificate -US Mail)
	LIC-CT2504-25A	25 AP Adder License for Cisco 2504 Controller (Paper Certificate - US Mail)

Note If you require a paper certificate for Customs, order it without the "L-" in the SKU (for example, LIC-CT5508-250A) and choose to ship it using the U.S. mail.

Step 3 After you receive the certificate, use one of two methods to register the PAK:

- Cisco License Manager (CLM)—This method automates the process of obtaining licenses and deploying them on Cisco devices. For deployments with more than five Cisco WLCs, we recommend using CLM to register PAKs and install licenses. You can also use CLM to rehost or RMA a license.

Note You can download the CLM software and access user documentation at http://www.cisco.com/c/en/us/products/cloud-systems-management/license-manager/index.html

- Licensing portal—This alternative method enables you to manually obtain and install licenses on your Cisco WLC. If you want to use the licensing portal to register the PAK, follow the instructions in Step 4.

Step 4 Use the licensing portal to register the PAK as follows:

a. Go to http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet

b. On the main Product License Registration page, enter the PAK mailed with the certificate in the Product Authorization Key (PAK) text box and click **Submit**.

c. On the Validate Features page, enter the number of licenses that you want to register in the Qty text box and click **Update**.

d. To determine the Cisco WLC's product ID and serial number, choose **Controller > Inventory** on the Cisco WLC GUI or enter the **show license udi** command on the Cisco WLC CLI.

Note To determine the Cisco WLC's product ID and serial number, see the Inventory page.

e. On the Designate Licensee page, enter the product ID and serial number of the Cisco WLC on which you plan to install the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Submit**.

f. On the Finish and Submit page, verify that all information is correct and click **Submit**.

g. When a message appears indicating that the registration is complete, click **Download License**. The license is emailed within 1 hour to the address that you specified.

h. When the e-mail arrives, follow the instructions provided.

i. Copy the license file to your TFTP server.

j. Follow the instructions in the "Installing a License" section below to install the license on your Cisco WLC.

Installing a License

For installation instructions, see the Install License section on the License Commands page.

Licenses

Note To use Cisco Smart Software License supported on certain supported models, see License Type and Smart-License sections.

Choose **MANAGEMENT > Software Activation > Licenses** to navigate to the Licenses page.

This page enables you to view all of the following types of information about the licenses installed on the Cisco WLC:

- License—Name of the license.
- Type—Permanent, evaluation, or extension.
- Time (expires)—How long until the license expires.
- HBL Count—Maximum number of access points allowed for the adder license. This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers.
- Non HBL Count—Maximum number of access points allowed for the CDK license. This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers.

- Count—Maximum number of access points allowed for this license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.
- Priority—Low, medium, or high.
- Status—In use, not in use, inactive, or End User License Agreement (EULA) not accepted.

If you ever want to remove a license from the Cisco WLC, click the blue arrow adjacent the desired license and choose **Remove**. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the Cisco WLC.

For Cisco Flex 7500 Series and 8500 Series Controllers, honor-based licensing also called Right to Use licensing was introduced in Cisco WLC Release 7.3. This feature allows you to add and activate an AP-count license on the Cisco WLC without using any external tools after accepting an End User License Agreement (EULA).

To add an AP-count license for Cisco Flex 7500 Series and 8500 Series Controllers follow these steps:

Step 1 Enter the count in the License Count text box.

Step 2 Choose **Add** from the License Count drop-down list.

Step 3 Click **Set Count**.

Step 4 When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.

The ap-count permanent license is active now.

To delete an AP-count license or reduce the count for Cisco Flex 7500 Series and 8500 Series Controllers follow these steps:

Step 1 Enter the count in the License Count text box.

Step 2 Choose **Delete** from the License Count drop-down list.

Step 3 Click **Set Count**.

Step 4 When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.

If the count is equal to the HBL count of the license, the license is removed from the list. If the count is less than the HBL count, the license appears with the decremented count.

To view more details for a particular license, click the link for the desired license. The License Detail page appears.

License Detail

Choose **MANAGEMENT > Software Activation > License** and then click a license name to navigate to the License Detail page.

This page shows the following additional information for the license:

- License name

- License type

  The license type can be permanent, evaluation, or extension.

- License version
- Comment

  You can enter a comment for this license in the Comment text box and click **Apply**.

- Status

  Status of the license. It can be one of the following:

  – In use
  – Not in use
  – Inactive
  – End user license agreement not accepted

- Current Status

  This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers. It indicates the current status of the license. It can be one of the following:

  – In use
  – Not in use
  – Inactive
  – End user license agreement not accepted

- Expires

  Length of time before the license expires

Note Permanent licenses never expire.

- License Status

  This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers.You can activate or deactivate the license by choosing **Activate** or **Deactivate** from the drop-down list.

- Built-in License

  Whether the license is a built-in license.

- Maximum Count

  Maximum number of access points allowed for this license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.

- Counts Used

  Number of access points currently using this license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.

- Priority

  To activate an ap-count evaluation license, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

Activating an AP-Count Evaluation License

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50 access point count and want to try an evaluation license with a 100 access point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the Cisco WLC uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, forcing the Cisco WLC to use the permanent license.

Note If the ap-count evaluation license is a wplus license and the ap-count permanent license is a base license, you must also change the feature set to wplus. See the License Level page for instructions.

Note To prevent disruptions in operation, the Cisco WLC does not switch licenses when an evaluation license expires. You must reboot the Cisco WLC in order to return to a permanent license. Following a reboot, the Cisco WLC defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the Cisco WLC uses a permanent license at another level or an unexpired evaluation license.

To activate an ap-count evaluation license, follow these steps:

Step 1 Choose **High** from the Priority drop-down list and click **Set Priority**.

Step 2 Click **OK** when prompted to confirm your decision about changing the priority of the license.

Step 3 When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.

Step 4 When prompted to reboot the Cisco WLC, click **OK**.

Step 5 Reboot the Cisco WLC in order for the priority change to take effect.

Step 6 Click Licenses to open the Licenses page and verify that the ap-count evaluation license now has a high priority and is in use. You can use the evaluation license until it expires.

If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

Step 1 Choose **Low** from the Priority drop-down list and click **Set Priority**.

Step 2 Click **OK** when prompted to confirm your decision about changing the priority of the license.

Step 3 When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.

Step 4 When prompted to reboot the Cisco WLC, click **OK**.

Step 5 Reboot the Cisco WLC in order for the priority change to take effect.

Step 6 Click Licenses to open the Licenses page and verify that the ap-count evaluation license now has a low priority and is not in use. Instead, the ap-count permanent license should be in use.

License Level

Choose **MANAGEMENT > Software Activation > License Usage** to navigate to the License Level page.

This page enables you to configure the Cisco WLC to specify which feature set it uses (base or wplus). Only the base or wplus license can be active at a time. The currently active license determines the feature set and number of access points supported on the Cisco WLC.

This page shows the current license level (base or wplus) and the level to be used after the next Cisco WLC reboot. It also shows the maximum number of access points allowed by the license on the Cisco WLC, the number of access points currently joined to the Cisco WLC, and the number of access points that can still join the Cisco WLC.

Note To learn more about the available license levels, click the **base** or **wplus** license level link to open the Licenses page. This page shows the licenses applicable to this level and the list of features supported. Click **Back** to return to the License Level page.

To change the license level, follow these steps:

Step 1 Choose the license level to be used on the next reboot: **base**, **wplus**, or **auto**. If you choose auto, the licensing software automatically chooses the license level to use on the next reboot. It chooses permanent licenses over evaluation licenses and wplus licenses over base licenses.

Note If you are considering upgrading from a base license to a wplus license, you can try an evaluation wplus license before upgrading to a permanent wplus license. To activate the evaluation license, you need to set the image level to **wplus** in order for the Cisco WLC to use the wplus evaluation license instead of the base permanent license. If no valid licenses are installed, the Cisco WLC can always operate in base level.

Note To prevent disruptions in operation, the Cisco WLC does not switch licenses when an evaluation license expires. You must reboot the Cisco WLC in order to return to a permanent license. Following a reboot, the Cisco WLC defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the Cisco WLC uses a permanent license at another level or an unexpired evaluation license.

Step 2 Click **Activate**.

Step 3 Click **OK** when prompted to confirm your decision to change the license level on the next reboot.

Step 4 If the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**. The Next Boot Level text box now shows the license level that you specified as the level to be used after the next Cisco WLC reboot.

Step 5 Reboot the Cisco WLC for the specified license level to take effect.

License Commands

Choose > **Software Activation** > **Commands** to navigate to the License Commands page.

From this page, you can install, save, or rehost licenses, and save device credentials.

Install License

Note For information about obtaining an upgrade license, see the Obtaining an Upgrade License topic.

Step 1 From the Action drop-down list, choose **Install License**. The Install license from a file section appears.

Step 2 In the File Name to Install text box, enter the path to the license (*.lic) on the TFTP server.

Step 3 Click **Install License**. A message appears to show whether the license was installed successfully. If the installation fails, the message provides the reason for the failure, such as the license is an existing license, the path was not found, the license does not belong to this device, you do not have correct permissions for the license, and so on.

Step 4 If the end-user license agreement (EULA) acceptance window appears, read the agreement and click **Accept** to accept the terms of the agreement.

Note Typically you are prompted to accept the end-user license agreement (EULA) for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

Step 5 Reboot the Cisco WLC.

Save License

Step 1 From the Action drop-down list, choose **Save License**. This saves all the licenses to a file, except the evaluation license section that appears.

Step 2 In the File Name to Save text box, enter the path on the TFTP server where you want the licenses to be saved.

Note You cannot save evaluation licenses.

Step 3 Click **Save Licenses**.

Step 4 Reboot the Cisco WLC.

Save Credentials

To save device credential information to a file, enter the path on the TFTP server where you want the device credentials to be saved and click **Save Credentials**. You need to save the device credentials to rehost a license.

Rehost

Revoking a license from one Cisco WLC and installing it on another is called *rehosting*. You might want to rehost a license to change the purpose of a Cisco WLC. For example, if you want to move your OfficeExtend or indoor mesh access points to a different Cisco WLC, you could transfer the wplus license from one Cisco WLC to another.

In order to rehost a license, you must generate credential information from the Cisco WLC and use it to obtain a permission ticket to revoke the license from the Cisco licensing site. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the Cisco WLC on which you want to install the license.

Evaluation licenses and the permanent base image license cannot be rehosted.

Note A revoked license cannot be reinstalled on the same Cisco WLC.

To rehost a license, follow these steps:

Step 1 In the File Name to Save Credentials text box, enter the path on the TFTP server where you want the device credentials to be saved and click **Save Credentials**.

Step 2 Obtain a permission ticket to revoke the license as follows:

a. Click **Cisco Licensing** (https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet). The Product License Registration page appears.

b. Under Manage Licenses, click **Look Up a License**.

c. Enter the product ID and serial number for your Cisco WLC.

Note To determine the Cisco WLC's product ID and serial number, see the Inventory page.

d. Open the device credential information file that you saved in Step 1 and copy and paste the contents of the file into the Device Credentials text box.

e. Enter the security code in the blank box and click **Continue**.

f. Choose the licenses that you want to revoke from this Cisco WLC and click **Start License Transfer**.

g. On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost box and click **Continue**.

h. On the Designate Licensee page, enter the product ID and serial number of the Cisco WLC for which you plan to revoke the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.

i. On the Review and Submit page, verify that all information is correct and click **Submit**.

j. When a message appears indicating that the registration is complete, click **Download Permission Ticket**. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.

k. After the e-mail arrives, copy the rehost permission ticket to your TFTP server.

Step 3 Use the rehost permission ticket to revoke the license from this Cisco WLC and generate a rehost ticket as follows:

a. In the Cisco WLC GUI Enter Saved Permission Ticket File Name text box, enter the TFTP path and filename (*.lic) for the rehost permission ticket that you generated in Step 2.

b. In the Rehost Ticket File Name text box, enter the TFTP path and filename (*.lic) for the ticket that will be used to rehost this license on another Cisco WLC.

c. Click **Generate Rehost Ticket**.

d. When the EULA acceptance page appears, read the agreement and click **Accept** to accept the terms of the agreement.

Step 4 Use the rehost ticket that you generated in Step 3 to obtain a license installation file, which can then be installed on another Cisco WLC as follows:

a. Click **Cisco Licensing** (http://www.cisco.com/go/license)

b. On the Product License Registration page, click **Upload Rehost Ticket** under Manage Licenses.

c. On the Upload Ticket page, enter the rehost ticket that you generated in Step 3 in the Enter Rehost Ticket text box and click **Continue**.

d. On the Validate Features page, verify that the license information for your Cisco WLC is correct, enter the rehost quantity, and click **Continue**.

e. On the Designate Licensee page, enter the product ID and serial number of the Cisco WLC on which you plan to use the license, read and accept the conditions of the EULA, complete the rest of the text boxes on this page, and click **Continue**.

f. On the Review and Submit page, verify that all information is correct and click **Submit**.

g. When a message appears indicating that the registration is complete, click **Download License**. The rehost license key is e-mailed within 1 hour to the address you specified.

h. After the e-mail arrives, copy the rehost license key to your TFTP server.

i. Follow the instructions from the Install License page to install this license on another Cisco WLC.

License Type

This section is applicable to platforms that support both **RTU** and **Smart Licensing** mechanisms.

To choose the license type that should be used, follow these steps:

Note The device must be rebooted to activate the changed license mechanism.

Step 1 Choose **Management > Software Activation > License Type**.

Step 2 From the **Licensing Type** drop-down list, choose from the following options:

- **RTU**
- **Smart-Licensing**

Step 3 Enter the **DNS Server IP address** in IPv4 format.

Step 4 Click **Apply**.

Step 5 Reboot Cisco WLC to activate the selected license mechanism.

Smart-License

Cisco Smart Software Licensing is a secured mechanism designed to provide flexible licensing of next generation Cisco software products in your network.

Cisco Smart Software Licensing feature is currently supported only on the following Cisco WLC models:

- Cisco 5520 WLC (AIR-CT5520-K9)
- Cisco 8540 WLC (AIR-CT8540-K9)
- Cisco vWLC (L-AIR-CTVM-5-K9)

Device Registration

Step 1 Choose **Management > Smart-License > Device registration** to open the **Device Registration** page.

Step 2 To register a new device, follow these steps:

a. From the **Action** drop-down list, choose **Registration** to register a new device.

b. In the **Smart License registration in the field** area, enter the token ID of the device in the **Token-id** box.

c. Check the **Force** check box to push for the registration of this device token ID with the central system for activation.

Note To de-register the device, choose **De-registration** from the **Action** drop-down list to remove the registered device.

Step 3 Click **Apply**.

Status

Step 1 Choose **Management** > **Smart-license** > **Status** to open the **Status** page

Step 2 To view the **Smart-Licensing Parameters**, choose from the following options in the drop-down list:

- Status—displays the license status
- Summary—displays a brief summary of all licenses
- all—displays the information on all the licenses
- Udi—displays the unique device identifier (UDI) for the licenses
- Usage—displays entitled licenses in use
- Tech-support—displays information to help troubleshoot issues

Call-home Configuration

Choose **Management > Smart-License > Call-home > Configuration** to open the **Call-Home Configuration** page.

Table 7-27 Call-Home Configuration Parameters

Parameter	Description
Events	Options: • Enabled—enables the Call-home reporting • Disabled—disables the Call-home reporting
Reporting Data-privacy-level	Options: • Normal—scrubs normal level commands • High—scrubs all normal level commands, IP domain name and IP address commands
Reporting Hostname	Enter the Hostname
HTTP-Proxy	To enable proxy, enter the IP-address and port number.
TAC Profile Name	Displays the TAC profile name
TAC Profile Status	Options: • Enabled—enables the TAC profile • Disabled—disables the TAC profile
Contact person's email address	Enter the contact person’s email address
Profile	
Name	Name of the new profile
Status	Options: • Enabled—enables the new profile • Disabled—disables the profile
Module	Options: • sm-license-data—reporting of smart license data • all—reporting of smart license and call-home data • call-home-data—reporting of call-home data
Reporting Format	Options: • short-text—data reporting in short-text format • long-text—data reporting in long-text format • xml—data reporting in XML format **Note** Currently, only XML format is supported.
URL	Enter the URL, depending on your preference either the Cisco URL or your custom satellite URL.

System Resource Information

Choose **MANAGEMENT > Tech Support > System Resource Information** to navigate to the System Resource Information page.

This page enables you to view the settings for the current Cisco WLC CPU usage, system buffers, and web server buffers.

For Cisco 5500 Series Controllers, the System Resource Information page also shows the Individual CPU usage, which is the percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level.

Controller Crash Information

Choose **MANAGEMENT > Tech Support > Controller Crash** to navigate to the Controller Crash Information page.

This page displays the most recent Cisco WLC CPU crash files from most to least recent.

Core Dump

Choose **MANAGEMENT > Tech Support > Core Dump** to navigate to the Core Dump page.

You can configure the following settings so that the Cisco WLC can automatically upload a core dump file of the Cisco WLC:

- Core Dump Transfer—Setting to enable or disable the Cisco WLC to generate a core dump file following a crash.
- Transfer Mode—Transfer mode type. Choose FTP. The default is FTP.
- IP Address—IP address of the FTP server to which the core dump file is uploaded.
- File Name—Name that the Cisco WLC uses to label the core dump file.
- User Name—Username to log on to FTP.
- Password—Password to log on to FTP.

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 Crash Logs

Choose **MANAGEMENT > Tech Support > AP Crash Log** to navigate to the AP Crash Logs page.

This page enables you to view the following settings for the most recent access point log:

- AP Name—Access point name
- AP ID—Access point ID
- MAC Address—MAC address of the access point
- Admin Status—Admin status of the access point
- Operational Status—Operational status of the access point

- Port—Port number
- FileName—Name of the crash log file
- FileSize—Size of the crash log file
- TimeStamp—Crash Timestamp

Commands Tab

This tab on the menu bar enables you to access the controller operating system software management commands. Use the left navigation pane to access the operating system software management parameters.

You can access the following pages from the Commands tab:

- Download File to Controller
- Upload File from Controller
- System Reboot
- Config Boot
- Scheduled Reboot
- Reset to Factory Default
- Set Time
- Login Banner
- Redundancy

You can find controller configuration information in the following sections:

- Using the Configuration Wizard
- Collect the Initial Configuration Settings
- Connecting Your Web Browser to a Controller
- Configuration Wizard System Information
- Service Interface Configuration
- Management Interface Configuration
- Miscellaneous Configuration
- Virtual Interface Configuration
- WLAN Policy Configuration
- RADIUS Server Configuration
- 802.11 Configuration
- Completing the Configuration Wizard

Download File to Controller

Choose **COMMANDS > Download File** to navigate to this page.

This page enables you to download and install new controller operating system software (code), a signature file, or a configuration file to your controller from a local TFTP (trivial file transfer protocol), FTP server, SFTP server, or over HTTP.

Note Follow these guidelines when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as Cisco Prime Infrastructure, because the Cisco Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

To download a file to the controller, follow these steps:

Step 1 From the File Type drop-down list, choose the kind of file that you want to download from the following options:

- Code—You can download an executable image.
- File Type—File type of the icon. For example, JPEG, PNG, etc.
- Configuration—If you choose Configuration, also enter the configuration file encryption key that enables the data in the file to be encrypted when the file is downloaded.
- Signature File—A standard signature file exists on the controller by default. You can upload this signature file from the controller, or you can create a custom signature file and download it to the controller or modify the standard signature file to create a custom signature.

  If you are downloading a custom signature file (*.sig), copy it to the default directory on your TFTP server.
- Webauth Bundle—You can download a custom webauth bundle.
- Vendor Device Certificate—When you choose Vendor Device Certificate, also enter the certificate password that is used to protect the certificate.
- Vendor CA Certificate—You can download a vendor CA certificate.
- Login Banner—The login banner is the text that appears in the window before user authentication when you access the controller CLI using Telnet, SSH, or a console port connection. You save the login banner information as a text file (*.txt). The text file cannot be larger than 1296 characters and cannot have more than 16 lines of text.

  Note The ACSII character set consists of printable and nonprintable characters. The login banner supports only printable characters.

Note Clearing the controller configuration does not remove the login banner. See the Login Banner topic for information about clearing the login banner file.

Note The controller can have only one login banner file. If you download another login banner file to the controller, the first login banner file is overwritten.

Step 2 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**
- **HTTP**

Step 3 If you selected **TFTP** from the **Transfer Mode** drop-down list, do the following:

a. In the IP Address (IPv4/IPv6) text box, enter the IPv4/IPv6 address of the TFTP server.

b. In the Maximum Retries text box, enter the maximum number of times the controller should attempt to download the signature file. The valid range is from 1 to 254; the default value is 10.

c. In the Timeout text box, enter the amount of time in seconds before the controller times out while attempting to download the signature file. The valid range is from 1 to 254; the default value is 6.

d. In the File Path text box, enter the file path on the server (default = /).

e. In the File Name text box, enter the name of the file to be transferred.

Note You cannot use special characters such as \ : * ? " < > | for the file path or a filename.

Step 4 If you selected **FTP** or **SFTP** from the **Transfer Mode** drop-down list, do the following:

a. In the IP Address (IPv4/IPv6) text box, enter the IPv4/IPv6 address of the FTP or SFTP server.

b. In the File Path text box, enter the file path on the server (default = /).

c. In the File Name text box, enter the name of the file to be transferred.

d. In the Server Login Username text box, enter the username to log in to the FTP or SFTP server.

e. In the Server Login Password text box, enter the password to log in to the FTP or SFTP server.

f. In the Server Port Number text box, enter the port number on the FTP or SFTP server through which the download occurs. The default value for the FTP server port is 21. The default value for the SFTP server port is 22.

Note The SFTP server must support SSHv2, else the file transfer will fail.

Step 5 If you selected **HTTP** from the **Transfer Mode** drop-down list, do the following:

a. Click **Choose File** and browse to the *.aes* file on the local computer to send to WLC.

Step 6 Click the **Download** button.

The controller downloads and installs the new controller operating system software. This process takes at least three minutes and overwrites your existing code and configuration.

Note You must reboot the controller after the new operating system software is installed.

Buttons

- Clear: Deletes the entries in the data fields.
- Download: Begins the download from the SFTP , FTP or TFTP server; you are prompted to continue.

Upload File from Controller

Choose **COMMANDS > Upload File** to navigate to this page.

This page enables you to upload files from your controller to a local SFTP , FTP or, TFTP server.

Note The SFTP server must support SSHv2, else the file transfer will fail.

You can upload the following files:

- Configuration file—See the Editing Configuration Files topic for information about editing configuration files. The following options are available:
  - Configuration
  - Event Log
  - Message Log
  - Trap Log
  - Crash File
  - Debug-File
  - Signature File
  - PAC (Protected Access Credential)—In the User text box, enter the name of the user who will use the PAC. In the Validity text box, enter the number days for the PAC to remain valid. The default setting is zero (0). In the Password and Confirm Password text boxes, enter a password to protect the PAC.
  - Radio Core Dump
  - Invalid Config—See the Configuration Files with Invalid CLI Commands topic for information about uploading the invalid configuration for analysis.
  - Packet Capture—When a Cisco 5500 Series Controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash. When a crash occurs, the controller generates a new packet capture file (*.pcap) file. You can upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file.

Note Only Cisco 5500 Series Controllers generate packet capture files. This feature is not available on other controller platforms.

  - Watchdog Crash File
  - Panic Crash File

- Configuration File Encryption—Enable the Configuration File Encryption option and enter the encryption key. File encryption ensures that data is encrypted while uploading or downloading the controller configuration file through a TFTP, SFTP, or FTP server.
- Transfer Mode—Choose the transfer mode from the drop-down list. Available options include FTP, SFTP, and TFTP.

  If you chose TFTP from the Transfer Mode drop-down list, enter the IPv4/IPv6 address of the TFTP server, the file path on the server (default = /), and a name for the file you have selected for upload.

Note The TFTP server cannot run on the same computer as the Cisco Wireless Control System because the Cisco WCS or Cisco Prime Infrastructure and the TFTP server use the same communication port.

  If you chose FTP or SFTP from the Transfer Mode drop-down list, enter the IPv4/IPv6 address of the FTP or SFTP server, the file path on the server (default = /), a name for the file you have selected for upload, the username to log in to the SFTP or FTP server, the password to log in to the SFTP or FTP server, and the port number on the SFTP or FTP server through which the download occurs (the default value for the FTP server port is 21, and the default value for the SFTP server port is 22).

When you click Upload, the selected file is uploaded to your TFTP, SFTP, or FTP server and is saved with the same name that you entered in the File Name field.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. When you upload the configuration file to a TFTP, SFTP, or FTP server, the controller converts the file from XML to CLI. You can then read, modify, delete, or add CLI commands to the configuration file in CLI format on the server.

Note To edit the configuration file, you can use either Notepad on Windows or the VI editor on Linux.

When you are finished, save your changes to the configuration file on the server and download the file back to the controller, where it is reconverted to XML format and saved.

Configuration Files with Invalid CLI Commands

CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter the **show invalid-config** command on the controller CLI.

Note You can enter this command only before the **clear config** or **save config** command.

If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP, SFTP, or FTP server for analysis.

Buttons

- Clear: Deletes the entries in the data fields are deleted.
- Upload: Begins the file upload to the TFTP, SFTP, or FTP server; you are prompted to continue.

System Reboot

Choose **COMMANDS > Reboot** to navigate to this page.

This page enables you to restart the controller. You are prompted to save your configuration changes in the next page if you have not already saved configuration changes using the Save Configuration Administrative toolbar at the top right of your window.

Buttons

- Reboot: Restarts the controller. You are prompted for confirmation. See the System Reboot > Save? topic.

System Reboot > Save?

Choose **COMMANDS > Reboot** and then click **Reboot** to navigate to this page.

This page prompts you to restart the controller after saving your configuration changes or restart without saving.

Buttons

- Reboot: Restarts the controller after saving your existing applied changes. See the System Reboot > Confirm topic.

System Reboot > Confirm

Choose **COMMANDS > Reboot** and then click **Reboot** to navigate to this page.

This page enables you to confirm the restart of your controller after saving your configuration changes. All system connections are lost so you must open a new session and log back in to the controller.

Buttons

- Reboot: Restarts the controller.

Config Boot

Choose **Commands > Config Boot** to navigate to this page.

This page enables you to configure the primary and backup boot image for the controller.

General

The primary image uses the primary image version on the controller. The primary image is the active image. The backup image uses the backup image version on the controller.

Config Boot Image

Boot enables you to select the image that you want the controller to use while rebooting. You can choose one of the two options provided from the drop-down list: Primary or Backup. Depending on the option that you choose from the drop-down list, the controller takes that image as the active image while rebooting.

Buttons

- Apply: Saves the config boot input to the controller.

Scheduled Reboot

This topic describes how to schedule a reboot of the controller.

Reboot At

Choose **COMMANDS > Scheduled Reboot >Reboot At** and then click the **Reboot** button to navigate to this page.

This page enables you to schedule a reboot of the controller at a specific time. All system connections are lost so you must open a new session and log back into the controller.

You can schedule the following settings for a reboot:

- Current Time—Current time on the controller.
- Date—Date on which you want to schedule the reboot. You can choose the month by using the drop-down lists for the month and the year in the Year text box.
- Time—Time at which you want to schedule the reboot. You can choose the hour from the Hour drop-down list and enter the minutes and seconds in the text boxes provided.
- Image—Type of image that the controller must use when rebooting. The following options are available:
  - Normal—The controller reboots with the current available software image.
  - Interchange—The controller interchanges the software image with the backup image when rebooting.

Buttons

- Save and Reboot: Saves the controller configuration and reboot.
- Reboot without Save: Reboots the controller without saving the configuration.

Reboot In

Choose **COMMANDS > Scheduled Reboot >Reboot In** and click **Reboot** to navigate to this page.

This page enables you to schedule a reboot of the controller in a specific time duration from the current time. All system connections are lost so you must open a new session and log back into the controller.

- Time—Time configured here adds to the current time configured in the controller. For example, if the current time in the controller is 10:15:00 a.m. and the time you configure here in the **Reboot In** page is 2:00:00, the reboot time will be 12:15:00 p.m.
- Image—Type of image that the controller must use when rebooting. The following options are available:
  - Normal—The controller reboots with the current available software image.
  - Interchange—The controller interchanges the software image with the backup image when rebooting.

Buttons

- Save and Reboot: Saves the controller configuration and reboot.
- Reboot without Save: Reboots the controller without saving the configuration.

Clear Reboot

Choose **COMMANDS > Scheduled Reboot > Clear Reboot** to navigate to this page.

This page enables you to cancel the scheduled reboot. The following information appears:

- Scheduled Reset Information—Scheduled reset information.
  - Current Time—Current time on the controller.
  - System Reset Time—System reset time.
- Reset System Notify-time—Reset system notification time.
  - Current reset system notify-time—Scheduled notification time (in minutes) before the traps are sent.
  - Notify Time—Notification time (in minutes) before the traps should be sent.

Buttons

- Clear: Clears the scheduled reset information.
- Apply: Applies the current settings.

Reset to Factory Default

Choose **COMMANDS > Reset to Factory Default** to navigate to this page.

This page enables you to reset the controller configuration to the factory default. Resetting the configuration overwrites all applied and saved configuration parameters. You are prompted for confirmation to reset the configuration.

All configuration data files are deleted, and upon reboot, the controller is restored to its original unconfigured state. Resetting the configuration removes all IP configuration and you need a serial connection to restore the base configuration.

Note After confirming the configuration removal, you must reboot the controller and choose **Reboot Without Saving**.

Buttons

- Reset: Returns the configuration to the factory default.

Set Time

Choose **COMMANDS > Set Time** to navigate to this page. This page enables you to configure the following settings for the time and date on the controller:

- Current Time—Current timestamp on the controller.
- Date—The date on the controller
  - Month
  - Day
  - Year
- Time
  - Hour
  - Minutes
  - Seconds
- Timezone
  - Delta—You cannot use this option on the controller GUI. However, if you do so on the controller CLI, the change is reflected in the Delta Hours and Mins fields on the controller GUI.
  - Location—When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

Login Banner

Choose **COMMANDS > Login Banner** to navigate to this page.

To clear the login banner from the controller, click **Clear**. At the prompt, click **OK** to clear the banner.

Redundancy

Choose **COMMANDS > Redundancy to configure the redundancy parameters and peer network routes:**

- To upload files from the peer controller to a local TFTP server, choose **COMMANDS > Redundancy > Upload Peer**.
- To reset the peer controller, choose **COMMANDS > Redundancy > Reset Peer**.

Redundancy > Upload Peer

Choose **COMMANDS > Redundancy > Upload Peer** to navigate to this page.

This page enables you to upload files from the peer controller to a local TFTP server.

You can upload the following files:

- Configuration file—See the Editing Configuration Files topic for information about editing configuration files. The following options are available:
  - Configuration
  - Event Log
  - Message Log
  - Trap Log
  - Crash File
  - Debug-File
  - Signature File
  - PAC (Protected Access Credential)—In the User text box, enter the name of the user who will use the PAC. In the Validity text box, enter the number days for the PAC to remain valid. The default setting is zero (0). In the Password and Confirm Password text boxes, enter a password to protect the PAC.
  - Radio Core Dump
  - Invalid Config—See the Configuration Files with Invalid CLI Commands topic for information about uploading the invalid configuration for analysis.
  - Packet Capture—When a Cisco 5500 Series Controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash. When a crash occurs, the controller generates a new packet capture file (*.pcap) file. You can upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file.

Note Only Cisco 5500 Series Controllers generate packet capture files. This feature is not available on other controller platforms.

  - Watchdog Crash File
  - Panic Crash File
- Configuration File Encryption—Enable the Configuration File Encryption option and enter the encryption key. File encryption ensures that data is encrypted while uploading or downloading the controller configuration file through a TFTP, SFTP, or FTP server.
- Transfer Mode—Choose the transfer mode from the drop-down list. Available options include FTP, SFTP, and TFTP. If you chose TFTP from the Transfer Mode drop-down list, enter the IP address of the TFTP server, the file path on the server (default = /), and a name for the file you have selected for upload.

Note The TFTP server cannot run on the same computer as the Cisco Wireless Control System because the Cisco WCS or Cisco Prime Infrastructure and the TFTP server use the same communication port.

If you chose FTP or SFTP from the Transfer Mode drop-down list, enter the IP address of the FTP or SFTP server, the file path on the server (default = /), a name for the file you have selected for upload, the username to log in to the FTP or SFTP server, the password to log in to the FTP or SFTP server, and the port number on the FTP or SFTP server through which the download occurs (the default value for the server port is 21 and the default value for the SFTP server port is 22).

When you click Upload, the selected file is uploaded to your TFTP, SFTP, or FTP server and is saved with the same name that you entered in the File Name field.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. When you upload the configuration file to a TFTP, SFTP, or FTP server, the controller converts the file from XML to CLI. You can then read, modify, delete, or add CLI commands to the configuration file in CLI format on the server.

Note To edit the configuration file, you can use either Notepad on Windows or the VI editor on Linux.

When you are finished, save your changes to the configuration file on the server and download the file back to the controller, where it is reconverted to XML format and saved.

Configuration Files with Invalid CLI Commands

CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter the **show invalid-config** command on the controller CLI.

Note You can enter this command only before the **clear config** or **save config** command.

If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP, SFTP, or FTP server for analysis.

Buttons

- Clear: Deletes the entries in the data fields are deleted.
- Upload: Begins the file upload to the TFTP, SFTP, or FTP server; you are prompted to continue.

Redundancy > Reset Peer

Choose **COMMANDS > Redundancy > Reset Peer** to navigate to this page.

This page enables you to reset the peer controller.

Buttons

- Reboot: Resets the peer controller.

Using the Configuration Wizard

When the controller is activated for the first time from the factory, or when it has been rebooted after a Reset to Factory Default, the Web User Interface displays the Web Configuration Wizard. Use the web Configuration Wizard to configure the controller for initial operation.

Complete the following wizard screens to enter the initial controller configuration:

- Collect the Initial Configuration Settings
- Connecting Your Web Browser to a Controller
- Configuration Wizard System Information
- Service Interface Configuration
- Management Interface Configuration
- Miscellaneous Configuration
- Virtual Interface Configuration
- WLAN Policy Configuration
- RADIUS Server Configuration
- 802.11 Configuration
- Redundancy Configuration
- Completing the Configuration Wizard

Collect the Initial Configuration Settings

Collect the following high-level controller parameters.

System Parameters

The system parameters are as follows:

- Controller name
- Supported protocols: 802.11a/n and/or 802.11b/g/n
- New usernames and passwords (optional)

Network (Distribution System) Parameters

The network parameters are as follows:

- Distribution System (network) port static IP address, netmask, and optional default gateway IP address from the network planner.
- Service port static IP address and netmask from the network planner (optional).
- Distribution System physical port (1000Base-T, 1000BASE-SX, or 10/100BASE-T). The 1000Base-SX (UNUSED PRODUCT) provides a 100/1000 Mbps wired connection to a network through an 850nM (SX) fiber-optic link using an LC physical connector.
- Distribution System port VLAN assignment (optional).
- Distribution System port Web and Secure Web mode settings, enabled or disabled.

- Distribution System port Spanning Tree Protocol: enabled/disabled, 802.1D/fast/off mode per port, path cost per port, priority per port, bridge priority, forward delay, hello time, maximum age.

WLAN Parameters

The WLAN parameters are as follows:

- VLAN assignments
- Layer 2 Security settings
- Layer 3 Security settings
- QoS assignments

Mobility Parameters

Specify the Mobility Settings for the controller by providing a mobility group name. This step is optional.

RADIUS Parameters

Specify the RADIUS parameters.

SNMP Parameters

Specify the SNMP parameters.

Other Parameters

Other Port and Parameter Settings: Service port, Radio Resource Management (RRM), third-party APs, Serial/CLI Console port, 802.3x Flow Control, and System Logging.

Other Actions

Collect all files that may need uploading or downloading to the controller, including the latest operating system code.

Connecting Your Web Browser to a Controller

To connect your web browser to the controller, follow these steps:

Note For the Initial GUI Configuration Wizard only, you cannot access the controller using IPv6 address.

Step 1 Temporarily configure your web browser device with a 192.168.1.2 IP address. Connect your web browser to the controller front panel service port, either using a crossover Ethernet cable or through an Ethernet hub or controller.

Note In case of Cisco WLC 2500, connect your PC to the port 2 on the controller and configure to use the same subnet.

Step 2 Type 192.168.1.1 into the address line of your web browser to log into the web user interface as described in the Commands Tab topic. The web server built into the controller responds with the login prompt.

Step 3 Enter admin and admin as the login and password, respectively. The controller displays the Configuration Wizard System Information page, in which you will configure the controller name and administrative user login.

Configuration Wizard System Information

To configure the wizard, follow these steps:

Step 1 On the Configuration Wizard System Information page, enter the controller name.

Step 2 Also in the Configuration Wizard page, enter a new administrative username and password. The default is admin and admin, respectively.)

Step 3 Click **Next** to have the controller save your inputs and display the Service Interface Configuration page, in which you will configure the Service Port Interface.

Service Interface Configuration

To configure the service interface, follow these steps:

Step 1 Click the DHCP Protocol **Enable** box when the Service Port Interface is to obtain an IP address from a DHCP server. When the Service Port Interface is to use a fixed IP address, leave this box unselected.

Step 2 The IP Address box contains the current Service Port Interface IP address. If desired, enter a different Service Port Interface IP address.

Step 3 The Netmask box contains the current Service Port IP netmask. If desired, enter a different Service Port Interface IP netmask.

Step 4 Click **Next** to have the controller save your inputs and display the Management Interface Configuration page, in which you will configure the Management Interface.

Management Interface Configuration

To configure the management interface, follow these steps:

Caution Do not configure wired clients in the same VLAN or subnet of the service port on the network. If you configure wired clients on the same subnet or VLAN as the service port, you will not be able to access the management interface.

Step 1 Enter a Management Interface VLAN assignment.

The VLAN Identifier box contains the current VLAN assignment (0 if untagged). If desired, enter a different Management Interface VLAN assignment (or 0 if untagged).

Step 2 Enter the Management Interface IP address.

The IP Address text box contains the current Management Interface IP address. If desired, enter a different Management Interface IP address.

Step 3 Enter a Management Interface netmask.

The Netmask text box contains the current Management Interface netmask. If desired, enter a different management interface netmask.

Step 4 Enter the Management Interface Gateway in the Gateway text box.

The Gateway text box contains the default Management Interface gateway. If desired, enter a different Management Interface gateway.

Step 5 Enter the Management Interface Physical Port in the Port Number text box text box.

The Port Number text box contains the current Management Interface physical port. If desired, enter a different Management Interface physical port.

Step 6 Enter the Primary DHCP Server IP address.

The Primary DHCP Server text box contains the default Management Interface primary DHCP server IP address. If necessary, enter a valid primary DHCP server IP address for the Management Interface.

Step 7 Enter the secondary DHCP server box.

The Secondary DHCP Server text box contains the default Management Interface secondary DHCP server IP address. If necessary, enter a valid secondary DHCP server IP address for the Management Interface.

Step 8 Click **Next** to have the controller save your inputs and display the Miscellaneous Configuration page, in which you will configure some Cisco WLAN Solution parameters.

Redundancy Configuration

To configure High Availabilty between two controllers, follow these steps:

Step 1 Configure the management IP address of both the controllers.

Note Before enabling redundancy, ensure that the management IP address of both the controllers are in the same subnet.

Step 2 Enter yes to enable HA.

Step 3 Configure the primary and secondary unit.

Step 4 Configure the Redundant Management and Peer Redundant Management IP address.

Note Both the interfaces should be in same subnet as the Management interface.

Miscellaneous Configuration

To perform the miscellaneous configuration, follow these steps:

Step 1 Enter the RF Mobility Domain Name.

The RF Mobility Domain Name text box contains the default RF Mobility Domain Name. If desired, enter a different RF mobility domain name.

Step 2 Enter the country code in the Country Code text box.

The Country Code text box contains the current country code. If desired, enter a different country code.

Step 3 Click **Next** to have the controller save your inputs and display the Virtual Interface Configuration page, in which you will configure the Virtual Interface parameters.

Virtual Interface Configuration

To configure the virtual interface, follow these steps:

Step 1 Enter the IP address.

The IP Address text box contains the default Virtual Interface IP address. Enter a different virtual interface IP address. Note that the Virtual Interface uses any fictitious, unassigned IP address (such as 192.0.2.1), to be used by Layer 3 Security and Mobility managers.

Step 2 Enter the DNS host name.

The DNS Host Name text box contains a space for a Web Auth ID Certificate DNS Host Name. If the controller uses an externally-generated Web Auth ID Certificate that includes a DNS Host Name, enter the DNS Host Name here.

Step 3 Click **Next** to have the controller save your inputs and display the WLAN Policy Configuration page, in which you will configure the WLAN 1 parameters.

WLAN Policy Configuration

To configure the WLAN policy, follow these steps:

Note Refer to the Editing WLANs page for a description of these parameters.

Step 1 Enter the WLAN SSID in the WLAN SSID text box.

The WLAN SSID text box contains the current WLAN 1 SSID. If desired, enter a different SSID.

Step 2 Enter the radio policy you want to adopt in the Radio Policy text box.

The Radio Policy text box contains the default bands controlled by the WLAN 1 policy. If desired, enter a different WLAN 1 policy: 802.11a only, 802.11g only, 802.11b/g only, 802.11a/g only, or All.

Step 3 Enter the admin status in the Admin Status text box.

The Admin Status text box contains the default administrative status (unselected, or disabled). If desired, enable the WLAN 1 policy by selecting the **Admin Status** box.

Step 4 Enter the session timeout value in the Session Timeout text box.

The Session Timeout text box contains the default 802.11 session timeout (0, or no timeout). If desired, enter a different 802.11 session timeout in minutes.

Step 5 Enter the QoS value in the Quality of Service text box.

The Quality of Service (QoS) text box contains the default QoS status (Silver, or Best Effort QoS). If desired, enter a different QoS: Platinum = Voice, Gold = Video, Bronze = Background, or leave as Silver = Best Effort. VoIP clients should be set to Platinum, Gold or Silver, while low-bandwidth clients can be set to Bronze.

Step 6 Set the AAA Override status.

The Allow AAA Override text box contains the default AAA Override status (unselected, or disabled). If desired, enable AAA Override by selecting the **AAA Override** box.

Step 7 Set the Blacklist Exclusion List Timeout.

The Blacklist Exclusion List Timeout text box contains the default client Exclusion List (blacklist) timeout status (selected, or enabled). If desired, disable Exclusion List (Blacklist) Timeout by unselecting the **Blacklist Timeout** box.

Step 8 Enter the number of seconds a client is added to the Exclusion List (blacklisted) after you fail to authenticate three consecutive times.

Step 9 Set the DHCP Server Override.

The DHCP Server Override text box contains the current status (unselected or disabled). If desired, enable DHCP Server Override by selecting the Override box.

Step 10 Set the DHCP Addr. Assignment.

The DHCP Addr. Assignment Required text box contains the current status (unselected or not required). If desired, enable DHCP Address Assignment Required parameter by selecting the **Required** box.

Step 11 Enter the Interface Name.

The Interface Name text box contains the current WLAN 1 Interface (management). Leave this setting unchanged.

Step 12 Enter the Layer 2 Security.

The Layer 2 Security text box contains the default Layer 2 Security setting (802.1X). If desired, select a different Layer 2 Security setting: None, WPA, 802.1X, Static WEP, Cranite, or Fortress. Refer to the Editing WLANs page for a description of these parameters and the related parameters that can be set for Layer 2 Security.

Step 13 Enter the Layer 3 Security.

The Layer 3 Security text box contains the default Layer 3 Security setting (None). If desired, select a different Layer 3 Security setting: None, IPSec, or VPN Pass Through. Refer to the Editing WLANs page for a description of these parameters and the related parameters that can be set for Layer 3 Security.

Step 14 Click **Next** to have the controller save your inputs and display the RADIUS Server Configuration page, in which you will configure the RADIUS server parameters.

RADIUS Server Configuration

If you do not want to configure a RADIUS server at this time, click **Skip** to ignore this section, and continue with the 802.11 Configuration section. If you do want to configure a RADIUS server, continue with this section.

To configure a RADIUS server, follow these steps:

Step 1 Enter the RADIUS server IP.

If required, enter a RADIUS server IP address.

Step 2 Enter the RADIUS Server Shared Secret password in the Shared Secret and Confirm Shared Secret text box.

Step 3 Enter the communication port number in the Port Number text box.

The Port Number text box contains the default communication port number (1812). If required, enter a different, unused communication port number.

Step 4 Set the RADIUS server status.

The Server Status text box contains the default RADIUS server status (Disabled). If desired, enable the RADIUS configuration by choosing **Enabled**.

Step 5 Click **Apply** to have the controller save your inputs and display the 802.11 Configuration page, in which you will activate or deactivate the different 802.11 bands and the Radio Resource Management (RRM) (RRM software).

802.11 Configuration

To configure 802.11 parameters, follow these steps:

Step 1 Set the 802.11a network status by selecting the **Network Status** check box.

The 802.11a Network Status check box contains the current status (unselected = disabled). If desired, select the box to activate the 802.11a Network in the Cisco WLAN Solution.

Step 2 Set the 802.11b network status by selecting the **Network Status** check box.

The 802.11b Network Status check box contains the current status (unselected = disabled). If desired, select the **Network Status** check box to activate the 802.11b Network in the Cisco WLAN Solution.

Step 3 Set the 802.11g network status by selecting the **Network Status** check box.

The 802.11g Network Status check box contains the current status (unselected = disabled). If desired, select the **Network Status** check box to activate the 802.11g Network in the Cisco WLAN Solution.

Step 4 Select the **Radio Resource Management** check box to enable RRM.

The Radio Resource Management check box contains the current Radio Resource Management, or Radio Resource Management, status (selected = enabled). If desired, unselect the box to disable the Radio Resource Management dynamic channel number and transmit power level assignment functions.

Step 5 Click **Next** to have the controller save your inputs and display the Configuration Wizard Completed page, in which the controller saves your changes in nonvolatile RAM and reboots the controller.

Completing the Configuration Wizard

To complete the configuration, follow these steps:

Step 1 Click the **Save and Reboot** button to have the controller save your changes in nonvolatile RAM and reboot. The operating system prompts you to confirm the operation.

Step 2 Click **OK** to continue. You have configured the controller using the Web User Interface.

Notices and Disclaimers

This topic contains notices and disclaimers that pertain to the Cisco Wireless Controller.

Notices

The following notices pertain to this software license:

- OpenSSL/Open SSL Project
- License Issues

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and noncommercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Disclaimers

All third party trademarks are the property of their respective owners.