Configuring Wireless Technologies

Chokepoints

Chokepoints are low frequency transmitting devices. When a tag passes within range of placed chokepoint, the low-frequency field awakens the tag that in turn sends a message over the Cisco Unified Wireless Network including the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room level accuracy (ranging from few inches to 2 feet depending on the vendor).

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on a the Prime Infrastructure map.

Related Topics

- Adding Chokepoints
- Editing Chokepoints

Adding Chokepoints

To add a chokepoint, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Chokepoints**.

Step 2 From the Select a command drop-down list, choose **Add Chokepoints**, then click **Go**.

Step 3 Enter the MAC address and name for the chokepoint.

Step 4 Select the check box to indicate that it is an Entry/Exit Chokepoint.

Step 5 Enter the coverage range for the chokepoint.

Text Part Number:

Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 6 Click **OK**.

After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.

Removing Chokepoints

To remove a chokepoint, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Chokepoints**.

Step 2 Select the check box of the chokepoint that you want to delete.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**, then click **Go**.

Step 4 Click **OK** to confirm the deletion.

Related Topics

- Editing Chokepoints

Adding Chokepoints to Maps

To add a chokepoint to a map, follow these steps:

Step 1 Choose **Maps > Wireless Maps > Site Maps**.

Step 2 Click the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 4 Click **Go**.

The Add Chokepoints summary page lists all recently-added chokepoints that are in the database but not yet mapped.

Step 5 Select the check box next to the chokepoint that you want to place on the map.

Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top-left hand corner. You are now ready to place the chokepoint on the map.

Step 7 Left-click the chokepoint icon and drag and place it in the proper location.The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8 Click **Save**.

You are returned to the floor map and the added chokepoint appears on the map.

The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse over its map icon

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.

Step 10 You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing Chokepoints from Maps

To remove an chokepoint from the map, follow these steps:

Step 1 Choose **Maps > Wireless Maps > Site Maps**.

Step 2 In the Maps page, choose the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Editing Chokepoints

To edit a current chokepoint, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Chokepoints**. The following information is displayed for each current chokepoint: MAC address, chokepoint name, entry/exit chokepoint, range, static IP address, and map location for the chokepoint.

Step 2 Click the chokepoint you want to edit in the MAC Address column.

Step 3 Edit the following parameters, as necessary:

- Name
- Entry/Exit Chokepoint—Click to enable.
- Range—Coverage range for the chokepoint.

  The chokepoint range is product-specific and is supplied by the chokepoint vendor.
- Static IP Address

Step 4 Click **Save**.

Wi-Fi TDOA Receivers

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

Note

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network. See Adding MSEs to Prime Infrastructure for details on adding a mobility services engine.
2. Add the TDOA receiver to the Prime Infrastructure database and map. See Adding Wi-Fi TDOA Receivers for details on adding the TDOA receiver to the Prime Infrastructure.
3. Activate or start the partner engine service on the MSE using the Prime Infrastructure.
4. Synchronize the Prime Infrastructure and mobility services engines. See Synchronizing Prime Infrastructure and a Mobility Services Engine for details on synchronization.
5. Set up the TDOA receiver using the AeroScout System Manager.

See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* for configuration details at the following URL:
http://support.aeroscout.com.

Related Topics

- Adding Wi-Fi TDOA Receivers
- Editing Wi-Fi TDOA Receivers
- Editing Wi-Fi TDOA Receivers

Adding Wi-Fi TDOA Receivers

After the Wi-Fi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on an Prime Infrastructure map.

After adding TDOA receivers to the Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than the Prime Infrastructure.

For more details on configuration options, see the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide* at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the Prime Infrastructure database and appropriate map, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**, then click **Go**.

Step 3 Enter the MAC address, name and static IP address of the TDOA receiver.

Step 4 Click **OK** to save the TDOA receiver entry to the database.

After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate Prime Infrastructure floor map.

A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Related Topic

- Editing Wi-Fi TDOA Receivers

Adding Wi-Fi TDOA Receivers to Maps

Step 1 To add the TDOA receiver to a map, choose **Maps > Wireless Maps > Site Maps**.

Step 2 In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 3 From the Select a command drop-down list, choose **Add WiFi TDOA receivers**, then click **Go**.

Step 4 Select the check box next to each TDOA receiver to add it to the map.

Step 5 Click **OK**. A map appears with a TDOA receiver icon located in the top-left hand corner. You are now ready to place the TDOA receiver on the map.

Step 6 Left-click the TDOA receiver icon and drag and place it in the proper location on the floor map.

The MAC address and name of the TDOA receiver appear in the left pane when you click the TDOA receiver icon for placement.

Step 7 Click **Save** when the icon is placed correctly on the map. The added TDOA receiver appears on the floor heat map.

The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor.

Step 8 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 9 Select the **WiFi TDOA Receivers** check box. The TDOA receiver appears on the map.

When you place your cursor over a TDOA receiver on a map, configuration details display for that receiver.

Step 10 Click **X** to close the Layers page.

Do not choose **Save Settings** from the Layers menu unless you want to save this display criteria for all maps.

Step 11 You can now download the partner engine software to the mobility services engine.

Related Topics

- Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting
- Editing Wi-Fi TDOA Receivers

Editing Wi-Fi TDOA Receivers

To view a current TDOA receiver to the Prime Infrastructure database, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Step 2 Click the MAC Address link to view the TDOA receiver details including MAC address, name, and static IP address.

Step 3 Make the necessary changes to the receiver name or IP address, then click **Save** to confirm these changes.

A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Removing Wi-Fi TDOA Receivers

You can remove one or multiple WiFi TDOA receivers at a time. If you remove a TDOA receiver from a map it remains in the Prime Infrastructure database but is labeled as unassigned.

To delete a TDOA receiver from the Prime Infrastructure, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > WiFi TDOA Receivers**.

Step 2 Select the check box next to each TDOA receiver to be deleted.

Step 3 From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers**, then click **Go**.

Step 4 To confirm TDOA receiver deletion, click **OK** in the dialog box.

In the **All WiFi TDOA Receivers** page, a message confirms the deletion. The deleted TDOA receiver is no longer listed in the page.

Access Point Radios

- Adding Autonomous Access Points to Prime Infrastructure

Adding Autonomous Access Points to Prime Infrastructure

From Prime Infrastructure, the following methods are available for adding autonomous access points:

- Adding Autonomous Access Points by Device Information, page 27-7 (IP addresses and credentials).
- Adding Autonomous Access Points by CSV File, page 27-8.
- Removing Autonomous Access Points, page 27-10

Adding Autonomous Access Points by Device Information

Autonomous access points can be added to Prime Infrastructure by device information using comma-separated IP addresses and credentials.

Cisco autonomous access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

To add autonomous access points using device information, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios.**

Step 2 From the Select a command drop-down list, choose **Add Autonomous APs**, click **Go**.

Step 3 Choose **Device Info** from the Add Format Type drop-down list.

Step 4 Enter comma-separated IP addresses of autonomous access points.

Step 5 Enter the SNMP Parameters parameters:

- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 10 seconds.
- Community—Public or Private.

Step 6 Enter the Telnet/SSH Parameters:

Default values are used if the Telnet/SSH parameters are left blank.

- Protocol—Select the protocol you want to use (either Telnet or SSH).
- User Name—Enter the username. (The default username is admin.) The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.
- Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
- Enable Password/Confirm Password—Enter and confirm an enable password.
- Telnet Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.

Step 7 Click **Add**.

After the AP is added and its inventory collection is completed, it appears in the Access Point list page (Configure > Access Points). If it is not found in the Access Points list, choose **Configure > Unknown Device** page to check the status.

Note Autonomous access points are not counted towards the total device count for your license.

Adding Autonomous Access Points by CSV File

Autonomous access points can be added to Prime Infrastructure using a CSV file exported from WLSE.

To add autonomous access points using a CSV file, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 From the Select a command drop-down list, choose **Add Autonomous APs**, click **Go**.

Step 3 Choose **File** from the Add Format Type drop-down list.

Step 4 Enter or browse to the applicable CSV file.

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username

- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Step 5 Click **OK**.

Bulk Update of Autonomous Access Points

You can update multiple autonomous access points credentials by importing a CSV file.

To update autonomous access point(s) information in a bulk, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios.**

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Bulk Update APs**. The Bulk Update Autonomous Access Points page appears.

Step 4 Click **Choose File** to select a CSV file, and then find the location of the CSV file you want to import.

Step 5 Click **Update and Sync**.

Related Topics

- Sample CSV File for the Bulk Update of Autonomous Access Points

Sample CSV File for the Bulk Update of Autonomous Access Points

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask

- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Removing Autonomous Access Points

Note If you replace Autonomous Access Points because of some reason, remove the Autonomous Access Points from Prime Infrastructure before you install the replacement access points on the network.

To remove an autonomous access point from Prime Infrastructure, follow these steps:

Step 1 Select the check boxes of the access points you want to remove. Select the APs that are not associated.

Step 2 Choose **Remove APs** from the Select a command drop-down list.

Viewing Autonomous Access Points in Prime Infrastructure

Once added, the autonomous access points can be viewed on the **Monitor > Access Points** page.

Click the autonomous access point to view more detailed information such as the following:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in Monitor > Maps.

They can be added to a floor area by choosing **Monitor Maps >** *floor area* and choosing **Add Access Points** from the Select a command drop-down list.

Downloading Images to Autonomous Access Points (TFTP)

Lightweight access point images are bundled with controller images and managed by the controller. Autonomous access point images must be handled by a NMS system such as WLSE, CiscoWorks, or Prime Infrastructure.

To download images to autonomous access points using TFTP, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios.**

Step 2 Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 From the Select a command drop-down list, choose **Download Autonomous AP Image (TFTP)**. The Download images to Autonomous APs page appears.

Step 4 Configure the following parameters:

- File is located on—Choose **Local machine** or **TFTP server**.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the TFTP server IP address. This is automatically populated if the default server is selected.
- Prime Infrastructure Server Files In—Specify where Prime Infrastructure server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the server filename.

Step 5 Click **Download**.

Tip Some TFTP servers might not support files larger than 32 MB.

Downloading Images to Autonomous Access Points (FTP)

To download images to autonomous access points (using FTP), follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**

Step 2 Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 From the Select a command drop-down list, choose **Download Autonomous AP Image (FTP)**. The Download images to Autonomous APs page appears.

Step 4 Enter the FTP credentials including username and password.

Step 5 Configure the following parameters:

- File is located on—Choose **Local machine** or **FTP server**.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the FTP server IP address. This is automatically populated if the default server is selected.

- Prime Infrastructure Server Files In—Specify where Prime Infrastructure server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the server filename.

Step 6 Click **Download**.

Supporting Autonomous Access Points in Work Group Bridge (WGB) mode

Workgroup Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as clients in Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all Prime Infrastructure clients that are WGBs, choose **Monitor > Clients**. From the Show drop-down list, choose **WGB Clients**, and click **Go**. The Clients (detected as WGBs) page appears. Click a user to view detailed information regarding a specific WGB and its wired clients.

Note Prime Infrastructure provides WGB client information for the autonomous access point whether or not it is managed by Prime Infrastructure. If the WGB access point is also managed by Prime Infrastructure, Prime Infrastructure provides basic monitoring functions for the access point similar to other autonomous access points.

Configuring Access Point Details

Choose **Configuration > Wireless Technologies > Access Point Radios** to see a summary of all access points in Prime Infrastructure database. The summary information includes the following:

- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

Note If you hover your mouse cursor over the Audit Status value, the time of the last audit is displayed.

Note You can click the **Edit View** link to add, remove or reorder columns such as AP Mode, Channel Width, Client Count, and so on.

Step 1 Click the link in the AP Name column to see detailed information about that access point name. The Access Point Detail page appears.

Note The operating system software automatically detects and adds an access point to Prime Infrastructure database as it associates with existing controllers in Prime Infrastructure database.

Note Access point parameters might vary depending on the access point type.

Some of the parameters on the page are automatically populated.

- The General group box displays the AP Name, Ethernet MAC, Base Radio MAC, IP Address, Admin Status, AP Static IPv4/IPv6, AP Mode, AP Sub Mode, AP Failover Priority, Registered Controller, Primary Controller Name, Secondary Controller Name, Tertiary Controller Name, Primary Controller Management IP, Secondary Controller Management IP, Tertiary Controller Management IP, AP Group Name, Location, Statistics Timer.
- The Versions group box of the page displays the software and boot version.
- The Inventory Information group box displays the model, AP type, AP certificate type, serial number, and REAP mode support, FlexConnect mode support.
- The Ethernet Interfaces group box provides information such as interface name, slot ID, admin status, and CDP state.
- The Radio Interfaces group box provides the current status of 802.11a/n, 802.11ac, 802.11b/g/n, and XOR (2.4 GHz), XOR (5GHz), or XOR (Monitor Mode) radios with the information such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

To set the configurable parameters, follow these steps:

Note Changing access point parameters causes the access point to be temporarily disabled and this might cause some clients to lose connectivity.

Step 2 Enter the name assigned to the access point.

Step 3 Use the drop-down list to choose a country code to establish multiple country support. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that the access point complies with the regulations of your country. Consider the following when setting the country code:

- You can configure up to 20 countries per controller.
- Because only one auto-RF engine and one list of available channels exist, configuring multiple countries limits the channels available to auto-RF in the common channels. A common channel is one that is legal in each and every configured country.
- When you configure access points for multiple countries, the auto-RF channels are limited to the highest power level available in every configured country. A particular access point might be set to exceed these limitations (or you might manually set the levels in excess of these limitations), but auto-RF does not automatically choose a non-common channel or raise the power level beyond that available in all countries.

Note Access points might not operate properly if they are not designed for use in your country of operation. For example, an (-A) access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Europe (-E). Always be sure to purchase access points that match the regulatory domain of your country. For a complete list of country codes supported per product, see this URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Step 4 If you want to enable the access point for administrative purposes, select the **Enable** check box.

Step 5 If you click **Enable** at the AP Static IP check box, a static IP address is always assigned to the access point rather than getting an IP address dynamically upon reboot.

Step 6 Choose the role of the access point from the AP Mode drop-down list. No reboot is required after the mode is changed *except* when monitor mode is selected. You are notified of the reboot when you click **Save**. The available modes are as follows:

- Local—This is the normal operation of the access point and the default AP Mode choice. With this mode, data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.

  AP Sub Mode—When the AP Mode is set to Local, you can set the AP Sub Mode to WIPS.

- FlexConnect—Choose **FlexConnect** from the AP Mode drop-down list to enable FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

  Note To configure Local or FlexConnect access points for Cisco Adaptive wIPS feature, choose Local or FlexConnect, and select the **Enhanced wIPS Engine Enabled** check box.

  AP Sub Mode - When the AP Mode is set to FlexConnect, you can set the AP Sub Mode to any one of the following:

  – WIPS

  – PPPOE—To configure the Point-to-Point Protocol over Ethernet (PPPoE) submode on the access point.

  – PPPOE-WIPS—To configure both Point Protocol over Ethernet (PPPoE) and wIPS submodes on the access point.

- Monitor—This is radio receive only mode and allows the access point to scan all configured channels every 12 seconds. Only deauthentication packets are sent in the air with an access point configured this way. A monitor mode access point detects rogues, but it cannot connect to a suspicious rogue as a client to prepare for the sending of RLDP packets.

  AP Sub Mode—When the AP Mode is set to Monitor, you can set the AP Sub Mode to WIPS.

Note You can expand the monitor mode for tags to include location calculation by enabling the tracking optimized monitor mode (TOMM) feature. When TOMM is enabled, you can specify which four channels within the 2.4 GHz band (802.11b/g radio) of an access point to use to monitor tags. This allows you to focus channel scans on only those channels for which tags are traditionally found (such as channels 1, 6, and 11) in your network. To enable TOMM, you must also make additional edits on the 802.11b/g radio of the access point. See the "Configuring Access Point Radios for Tracking Optimized Monitor Mode" section on page 27-35 for configuration details.

Note You cannot enable both TOMM and wIPS at the same time. TOMM can be enabled only when wIPS is disabled.

Note To configure access points for Cisco Adaptive wIPS feature, choose **Monitor** and select the **Enhanced wIPS Engine Enabled** check box, and select **wIPS** from the Monitor Mode Optimization drop-down list.

- Rogue Detector—In this mode, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
- Sniffer—Operating in sniffer mode, the access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com.
- Bridge—Bridge mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.
- SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

Note This option is displayed only if the access point is CleanAir-capable.

Note Changing the AP mode reboots the access point.

Step 7 Disable any access point radios.

Step 8 From the AP Failover Priority drop-down list, choose **Low**, **Medium**, **High**, or **Critical** to indicate the failover priority of the access point. The default priority is low.

Step 9 In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

Step 10 The AP Group Name drop-down shows all access point group names that have been defined using WLANs > AP Group VLANs, and you can specify whether this access point is tied to any group.

Note An access point group name to 31 characters for WLC versions earlier than 4.2.132.0 and 5.0.159.0.

Step 11 Enter a description of the physical location where the access point was placed.

Step 12 In the Stats Collection Period field, enter the time in which the access point sends .11 statistics to the controller. The valid range is 0 to 65535 seconds. A value of 0 means statistics should not be sent.

Step 13 Choose **Enable** for Mirror Mode if you want to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point. Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port since any connections to this port become unresponsive.

Step 14 You can globally configure MFP on a controller. When you do, management frame protection and validation are enabled by default for each joined access point, and access point authentication is automatically disabled. After MFP is globally enabled on a controller, you can disable and re-enable it for individual WLANs and access points.

If you click to enable MFP Frame Validation, three main functions are performed:

- Management frame protection—When management frame protection is enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing those receiving access points which were configured to detect MFP frames to report the discrepancy.
- Management frame validation—When management frame validation is enabled, the access point validates every management frame it receives from other access points in the network. When the originator is configured to transmit MFP frames, the access point ensures that the MIC IE is present and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE, it reports the discrepancy to the network management system. To report this discrepancy, the access point must have been configured to transmit MFP frames. Likewise, for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.
- Event reporting—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to alert the network manager.

Step 15 Select the **Cisco Discovery Protocol** check box if you want to enable it. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment, such as routers, bridges, and communication servers. Each device sends periodic messages to a multicast address and listens to the messages that others send to learn about neighboring devices. When the device boots, it sends a CDP packet specifying whether the device is inline power enabled so that the requested power can be supplied.

Note Changing access point parameters temporarily disables an access point and might result in loss of connectivity to some clients.

Step 16 Select the check box to enable rogue detection.

Note Rogue detection is disabled automatically 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. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.

Step 17 Select the **Encryption** check box to enable encryption.

Note Enabling or disabling encryption functionality causes the access point to reboot, which then causes clients to lose connectivity.

Note DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security, but disabled by default for all other access points.

Note Cisco 5500 controllers can be loaded with one of the two types of images, AS_5500_LDPE_x_x_x_x.aes or AS_5500_x_x_x_x.aes. For the 5500 controller loaded with former image, you need to have DTLS License to show encryption.

Note For WiSM2 and 2500 controllers, it is mandatory to have DTLS license to show encryption.

Step 18 If rogue detection is enabled, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.

Step 19 Select the **SSH Access** check box to enable SSH access.

Step 20 Select the **Telnet Access** check box to enable Telnet access.

Note An OfficeExtend access point might be connected directly to the WAN which allows external access if the default password is used by the access point. Therefore, Telnet and SSH access are disabled automatically for OfficeExtend access points.

Step 21 If you want to override credentials for this access point, select the **Override Global Username Password** check box. You can then enter a new supplicant AP username, AP password, and Enable password that you want to assign for this access point.

Note In the System > AP Username Password page, you can set global credentials for all access points to inherit as they join a controller. These established credentials appear in the lower right of the AP Parameters tab page.

The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

Step 22 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received.

Step 23 You can now manipulate power injector settings through Prime Infrastructure without having to go directly to the controllers. In the Power Over Ethernet Settings section, select the check box to enable pre-standard or power injector state.

Pre-standard is chosen if the access point is powered by a high power Cisco switch; otherwise, it is disabled. If power injector state is selected, power injector options appear. The possible values are installed or override. If you choose override, you can either enter a MAC address or leave it empty so that it is supplied by WLC.

Note To determine which source of power is running Prime Infrastructure, choose **Monitor > Access Points**, click **Edit View**, and then choose and move POE Status to the View Information box. After you click **Submit**, the POE status appears in the last column. If the device is powered by an injector, the POE status appears as Not Applicable.

Step 24 Select the **Enable** check box to enable the following FlexConnect configurations:

Note FlexConnect settings cannot be changed when the access point is enabled.

- OfficeExtend AP—The default is Enabled.

  Note Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point, but it does put the access point at risk because it becomes remotely deployed. If you want to clear the configuration of an access point and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the personal SSID of the access point, click **Reset Personal SSID** at the bottom of the access point details page.

When you select Enabled for the OfficeExtend AP, a warning message provides the following information:

- Configuration changes that automatically occur. Encryption and Link Latency are enabled. Rogue Detection, SSH Access, and Telnet Access are disabled.
- A reminder to configure at least one primary, secondary, and tertiary controller (including name and IP address).

  Note Typically, an access point first looks for the primary controller to join. After that, the controller tries the secondary and then the tertiary controller. If none of these controllers are configured, the access point switches to a default discovery mode in an attempt to join whatever controller it might find.

  An OfficeExtend access point searches only for a primary, secondary, or tertiary controller to join. It does not look any further for a configured controller. Because of this, it is important that you configure at least one primary, secondary, or tertiary controller name and IP address.

  - A warning the enabling encryption causes the access point to reboot and causes clients to lose connectivity.

- Least Latency Controller Join—When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

Note The access point only performs this search once when it initially joins the controller. It does not recalculate the primary, secondary, and tertiary controllers latency measurements once joined to see if the measurements have changed.

- VLAN Support—When selected, enter the Native VLAN identifier.

  When Enable VLAN is selected, Prime Infrastructure displays locally switched VLANs. You can only edit a VLAN ID that is mapped to a WLAN ID.

- AP level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled.You can only edit the Ingress and Egress ACLs mapped to a VLAN ID.

Note The AP level VLAN ACL Mapping configuration is pushed to the access point, only when the VLAN IDs entered in Prime Infrastructure is available in the AP Level VLAN ACL Mapping section of the access point in the associated controller.

- Group level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled.You can view the Group level VLAN ACL mapping that you have specified under the ACL tab of the FlexConnect ACL groups.
- PreAuthentication ACL Mappings
  - Web-Authentication and Web-Policy ACLs—Click the **External WebAuthentication ACLs** link to view the WebAuth and Web Policy ACL mappings at access point level. The ACL Mappings page lists details of the WLAN ACL mappings and web policy ACLs.

Step 25 Select the role of the mesh access point from the Role drop-down list. The default setting is MAP.

Note An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

Step 26 Enter the name of the bridge group to which the access point belongs. The name can have up to 10 characters.

Note Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.

Note For mesh access points to communicate, they must have the same bridge group name.

Note For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.

Note For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

The Type field appears whether the mesh access point is an indoor or outdoor access point, and the Backhaul Interface field displays the access point radio that is being used as the backhaul for the access point.

Step 27 Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

Note This data rate is shared between the mesh access points and is fixed for the whole mesh network.

Note Do NOT change the data rate for a deployed mesh networking solution.

Step 28 Choose **Enable** from the Ethernet Bridging drop-down list to enable Ethernet bridging for the mesh access point.

Step 29 Click **Save** to save the configuration.

Step 30 Re-enable the access point radios.

Step 31 If you need to reset this access point, click **Reset AP Now**.

Step 32 Click **Reset Personal SSID** to reset the OfficeExtend access point personal SSID to the factory default.

Step 33 If you need to clear the access point configuration and reset all values to the factory default, click **Clear Config**.

Configuring an Ethernet Interface

Note The 152x mesh access points are configured on any one of these four ports: port 0-PoE in, port 1-PoE out, Port 2 - cable, and port 3- fiber. Other APs (such as 1130,1140,1240,1250) are configured on Port 2 - cable.

To configure an Ethernet interface, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears.

Note The Access Point Details page displays the list of Ethernet interfaces.

Step 3 Click the link under Interface to see detailed information about that interface. The Ethernet Interface page appears.

This page displays the following parameters:

- AP Name—The name of the access point.
- Slot Id—Indicates the slot number.
- Admin Status—Indicates the administration state of the access point.
- CDP State—Select the **CDP State** check box to enable the CDP state.

Step 4 Click **Save**.

Importing AP Configuration

To import a current access point configuration file, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 From the **Select a command** drop-down list, choose **Import AP Config**.

A pop-up aleart box appears stating All Unified AP(s) are imported from CSV file only. Unified AP(s) from Excel and XML file are not imported.

Step 3 Click **OK** to close the pop-up alert box.

Step 4 Click **Go**.

Step 5 Enter the CSV file path in the text box or click **Browse** to navigate to the CSV file on your computer.

The first row of the CSV file is used to describe the columns included. The AP Ethernet Mac Address column is mandatory. The parameters on this page are used for columns not defined in the CSV file.

Sample File Header:

```
AP Name,Ethernet MAC,Location,Primary Controller,Secondary Controller,Tertiary Controller
ap-1, 00:1c:58:74:8c:22, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3
```

The CSV file can contain following fields.

- AP Ethernet MAC Address—Mandatory
- AP Name—Optional
- Location—Optional
- Primary Controller—Optional
- Secondary Controller—Optional
- Tertiary Controller—Optional

Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

- Ethernet MAC—AP Ethernet MAC Address
- AP Name—AP Name
- Location—AP Location
- Primary Controller—Primary Controller Name
- Secondary Controller—Secondary Controller Name
- Tertiary Controller—Tertiary Controller Name

Note Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

Step 6 When the appropriate CSV file path appears in the Select CSV File text box, click **OK**.

Related Topics

- Configuring Access Point Details
- Configuring Access Points 802.11n Antenna
- Viewing Audit Status (for Access Points)
- Searching Access Points
- Copying and Replacing Access Points
- Removing Access Points
- Scheduling Radio Status
- Exporting AP Configuration
- Downloading Images to Autonomous Access Points (TFTP)

Exporting AP Configuration

To export current access point configuration files, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 From the Select a command drop-down list, choose **Export AP Config**.

A pop-up alert box appears stating All Unified AP(s) are exported to CSV/EXCEL/XML file.

Step 3 Click **OK** to close the pop-up alert box.

Step 4 Click **Go** to view the current AP configurations including:

- AP Name
- Ethernet MAC
- Location
- Primary Controller
- Secondary Controller
- Tertiary Controller

Step 5 Select the file option (CSV, Excel, XML) to export the access point configurations.

Step 6 In the File Download window, click **Save** to save the file.

Configuring Access Points 802.11n Antenna

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

If you choose **Configuration > Wireless Technologies > Access Point Radios**. and select an **802.11n** item from the Radio column, the following page appears.

This page contains the following fields:.

Note Changing any of the fields causes the radio to be temporarily disabled and thus might result in loss of connectivity for some clients.

General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the **CDP State** check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—Select the check box to enable CleanAir.

Antenna

- Antenna Type—Indicates an external or internal antenna.
- Antenna Diversity—Select **Right**, **Left**, or **Enabled**.

  Note Antenna diversity refers to the Cisco Aironet access point feature where an access point samples the radio signal from two integrated antenna ports and choose the preferred antenna. This diversity option is designed to create robustness in areas with multi-path distortion.

  For external antenna, select one of the following:

  – Enabled—Use this setting to enable diversity on both the left and right connectors of the access point.

  – Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the left connector of the access point.

  – Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the right connector of the access point.

  For internal antennas, select one of the following:

  - Enabled—Use this setting to enable diversity on both Side A and Side B.
  - Side A—Use this setting to enable diversity on Side A (front antenna) only.
  - Side B—Use this setting to enable diversity on Side B (rear antenna) only.
- External Antenna—Choose the **external antenna** or **Other** from the drop-down list.
- Antenna Gain—Enter the desired antenna gain in the text box.

Note The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

- Current Gain (dBm)—Indicates the current gain in dBm.

Table 27-1 lists the antenna names, gain, and descriptions.

Table 27-1 Antenna Names, Gain, and Descriptions

Antenna Name	Gain (dBi)	Description
AIR-ANT2524DB-R=	2/4	Dipole antenna
AIR-ANT2524DG-R=	2/4	Dipole antenna
AIR-ANT2524DW-R=	2/4	Dipole antenna
AIR-ANT2535SDW-R=	3/5	Dipole antenna
AIR-ANT2524V4C-R=	2/4	Omni ceiling antenna
AIR-ANT2566P4W-R=	6/6	Patch wall mount antenna
AIR-ANT2544V4M-R=	4/4	Omni wall mount antenna
AIR-ANT2544V4M-R8=	3/2	Omni wall mount antenna
AIR-ANT2566D4M-R=	6/6	Directional wall mount antenna
AIR-ANT2513P4M-N=	13/13	Patch wall mount antenna
AIR-ANT-LOC-01=		Omni antenna
AIR-ANT1000	0.00	AP 1000 Integrated antenna
CUSH-S5157WP	3.00	5.15-5.87 GHz diversity wideband panel antenna (side gain and back attenuation)
KODIAK-DIRECTIONAL	8.00	Integrated Kodiak directional antenna
KODIAK-OMNI	5.00	Kodiak omni antenna
AIR-ANT1728	5.20	Omni ceiling mount antenna
AIR-ANT1729	6.00	Patch wall mount antenna
AIR-ANT2012	6.50	Diversity patch wall mount antenna
AIR-ANT2410Y-R	10.00	Yagi master or wall mount antenna
AIR-ANT5959	2.00	Omni diversity ceiling mount antenna
AJAX-OMNI	5.00	Integrated Ajax omni antenna
AIR-ANT5135D-R	3.50	Omni dipole antenna
AIR-ANT5135DW-R	3.50	3.5-dBi white dipole antenna
AIR-ANT5135DG-R	3.50	3.5 dB5 gray non-articulating dipole antenna

Table 27-1 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dBi)	Description
AIR-ANT2413P2M-N	13.00	Dual polarized patch antenna for 2.4 GHz.
AIR-ANT2422DW-R	2.20	2.2-dBi white dipole antenna
AIR-ANT2422DB-R	2.20	Omni dipole antenna
AIR-ANT2422DG-R	2.20	2.2 dBi gray non-articulating dipole antenna
AIR-ANT5145V-R	4.50	Omni diversity antenna
AIR-ANT5160V-R	6.00	Omni antenna
AIR-ANT3549	9.00	Patch wall mount antenna
AIR-ANT4941	2.20	Omni dipole antenna
AIR-ANT2506	0.00	Omni mass mount antenna
AIR-ANT3213	5.20	Omni diversity pillar antenna
CUSH-S24516DBP	3.00	Integrated 2.4/5 GHz hemispheric pattern
CUSH-S5153WBPX	6.00	Ceiling mount 6-dBi omni
AIR-ANT5170V-R	7.00	Wall mount diversity patch antenna
AIR-ANT5175V	7.50	Omni antenna for Wireless Bridge
AIR-ANT5195V-R	9.50	Wall mount patch antenna
AIR-ANT58G10SSA	9.50	Sector antenna for Wireless Bridge
AIR-ANT2455V	5.50	Omni antenna for Wireless Bridge
CUSH-S54717P	17.00	Patch array antenna for Wireless Bridge
CUSH-S49014WP	14.00	Patch array antenna for Wireless Bridge
CUSH-S2406BP	8.00	Omni antenna for Wireless Bridge
AIR-ANT1100	2.20	Default antenna for AP1100
BR1310	13.00	Integrated patch directional antenna
AIR-ANT2460	6.00	Patch wall mount antenna
AIR-ANT2465	6.50	Diversity patch wall mount antenna
AIR-ANT2485	9.00	Patch wall mount antenna
AIR-ANT2480V-N	8.00	2.4 GHz omni antenna for mesh
AIR-ANT5114P2M-N	14.00	5 GHz patch for mesh
AIR-ANT5117S-N	17.00	5 GHz sector for mesh
AIR-ANT2450V-N	5.00	2.4 GHz omni antenna
AIR-ANT5180V-N	8.00	5 GHz omni antenna
AIR-ANT2450S-R	5.50	2.4 GHz 135-degree sector antenna
AIR-ANT2451V-R	2.4 GHz—2.0 5 GHz—3.0	2.4 GHz and 5 GHz four-element dual band antenna. **Note** Two elements for the 2.4 GHz band and two elements for the 5 GHz band.
AIR-ANT2460NP-R	6.00	2.4 GHz MIMO (3-Element) Patch Antenna
AIR-ANT5160NP-R	6.00	5 GHz MIMO (3-Element) Patch Antenna

Table 27-1 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dBi)	Description
AIR-ANT2420V-N	2.2	Omni dipole antenna
AIR-ANT2422SDW-R	2.20	2.4 GHz “Stubby” white monopole antenna
AIR-ANT5135SDW-R	3.50	5 GHz “Stubby” white monopole antenna
AIR-ANT2451NV-R	2.4 GHz—2.5 5 GHz—3.5	2.4 GHz and 5 GHz “6-pack” ceiling mount omni antenna
AIR-ANT2452V-R	5.2	2.4 GHz Diversity Wall Mount Omni-directional Antenna **Note** This is a replacement antenna to the existing AIR-ANT3213.
AIR-ANT24020V-R	2.0	External omni diversity ceiling mount antenna **Note** This is a replacement antenna to the existing antenna AIR-ANT5959.
AIR-ANT5140V-R	4.0	Omni antenna w/RP-TNC connectors(3)
AIR-ANT2430V-R	3.0	Omni antenna w/RP-TNC connectors(3)
AIR-ANT1949	2.4 GHz—13.5	External antenna
AIR-ANT2440NV-R	4.0	2.4 GHz MIMO Wall Mount Antenna
AIR-ANT5140NV-R	4.0	5 GHz MIMO Wall Mount Antenna
AIR-ANT2460P-R	6.0	Grayling Patch Antenna
AIR-ANT2485P-R	8.5	Grayling Patch Antenna
AIR-ANT2547V-N	2.4 GHz—4.0 5 GHz—7.0	2.4 GHz and 5 GHz dual band Omni-directional Antenna.
AIR-ANT2588P3M-N	8.0	Dual-band patch antenna for both 2.4 GHz and 5 GHz.
Internal-802.11	2	Internal AP802 Antenna
Internal-602i	2.4 GHz—4	Internal omni antenna
Internal-602i	5.0 GHz—4	Internal omni antenna

Table 27-2 lists the default values of some of the attributes of an access point when it is added to Prime Infrastructure for the first time.

Table 27-2 Supported Antennas

AP Type	Radio Type	Supported Antennas
AP 2800i		AIR-ANT2524V4C-R=, AIR-ANT2566P4W-R=, AIR-ANT2544V4M-R=, AIR-ANT2544V4M-R8=, AIR-ANT2566D4M-R=
AP 2800e		AIR-ANT2524DB-R=, AIR-ANT2524DG-R=, AIR-ANT2524DW-R=, AIR-ANT2535SDW-R=, AIR-ANT2524V4C-R=, AIR-ANT2566P4W-R=, AIR-ANT2544V4M-R=, AIR-ANT2544V4M-R8=, AIR-ANT2566D4M-R=, AIR-ANT2513P4M-N=
AP 3800i		AIR-ANT2524V4C-R=, AIR-ANT2566P4W-R=, AIR-ANT2544V4M-R=, AIR-ANT2544V4M-R8=, AIR-ANT2566D4M-R=, AIR-ANT-LOC-01=
AP 3800e		AIR-ANT2524DB-R=, AIR-ANT2524DG-R=, AIR-ANT2524DW-R=, AIR-ANT2535SDW-R=, AIR-ANT2524V4C-R=, AIR-ANT2566P4W-R=, AIR-ANT2544V4M-R=, AIR-ANT2544V4M-R8=, AIR-ANT2566D4M-R=, AIR-ANT-LOC-01=
AP 3800p		AIR-ANT2524DB-R=, AIR-ANT2524DG-R=, AIR-ANT2524DW-R=, AIR-ANT2535SDW-R=, AIR-ANT2524V4C-R=, AIR-ANT2566P4W-R=, AIR-ANT2544V4M-R=, AIR-ANT2544V4M-R8=, AIR-ANT2566D4M-R=, AIR-ANT2513P4M-N=, AIR-ANT-LOC-01=
AP 1200	802.11a	KODIAC-OMNI, KODIAK-DIRECTIONAL, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1240	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1131	802.11a	AJAX-OMNI
	802.11b/g	AJAX-OMNI
AP 1100	802.11b/g (only b/g)	AIR-ANT1100
AP 1310	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R

Table 27-2 Supported Antennas (continued)

AP Type	Radio Type	Supported Antennas
	802.11b/g	BR1310, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1250	802.11a	AIR-ANT5135D-R, AIR-ANT5135SDW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5160NP-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT2451NV-R-5GHz
	802.11b/g	AIR-ANT2460, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT2465, AIR-ANT2485, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1000	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1030	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1500	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP
AP 1505	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP
AP 1260	802.11a	AIR-ANT5135DG-R, AIR-ANT5135D-R, AIR-ANT5135DB-R, AIR-ANT5135DW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT5140V-R, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT5135SDW-R, AIR-ANT2451NV-R-5GHz, AIR-ANT5160NP-R

Table 27-2 Supported Antennas (continued)

AP Type	Radio Type	Supported Antennas
	802.11b/g	AIR-ANT2422DG-R, AIR-ANT4941, AIR-ANT2422DB-R, AIR-ANT2422DW-R, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2430V-R, AIR-ANT24120, AIR-ANT2414S-R, AIR-ANT1949, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT24020V-R, AIR-ANT2452V-R
AP 1040	802.11a	Internal-1040-5.0 GHz
	802.11b/g	Internal-1040-2.4 GHz
AP 1140	802.11a	Internal-1140-5.0 GHz
	802.11b/g	Internal-1140-2.4 GHz
AP 1550	802.11a	AIR-ANT2547V-N-5.0GHz, Internal-1550-5.0 GHz
	802.11b/g	AIR-ANT2547V-N-2.4GHz,Internal-1550-2.4GHz
AP2600E	802.11 a/n	AIR-ANT2524DB-R-5GHz
AP2600E	802.11b/g/n	AIR-ANT2524DB-R-2.4GHz
AP2600I	802.11 a/n	Internal-2600-5GHz
AP2600I	802.11b/g/n	Internal-2600-2.4GHz_
AP 3500e	802.11a	AIR-ANT5135DG-R,AIR-ANT5135D-R,AIR-ANT5135DB-R,AIR-ANT5135DW-R,AIR-ANT5145V-R,AIR-ANT5160V-R,AIR-ANT5170V-R,AIR-ANT5195V-R,AIR-ANT5140V-R,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT5135SDW-R,AIR-ANT2451NV-R-5GHz,AIR-ANT5160NP-R
AP 3500e	802.11b/g	AIR-ANT2422DG-R,AIR-ANT4941,AIR-ANT2422DB-R,AIR-ANT2422DW-R,AIR-ANT2460,AIR-ANT2465,AIR-ANT2485,AIR-ANT1728,AIR-ANT2012,AIR-ANT1729,AIR-ANT2410Y-R,AIR-ANT5959,AIR-ANT3549,AIR-ANT2506,AIR-ANT3213,AIR-ANT2430V-R,AIR-ANT24120,AIR-ANT2414S-R,AIR-ANT1949,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT2460NP-R,AIR-ANT2422SDW-R,AIR-ANT2451NV-R-2.4GHz,AIR-ANT24020V-R,AIR-ANT2452V-R
AP 3500i	802.11a	Internal-3500i-5 GHz
AP 3500i	802.11b/g	Internal-3500i-2.4 GHz
AP 3600e	802.11a	AIR-ANT2524DB-R, AIR-ANT2524DW-R, AIR-ANT2524DG-R, AIR-ANT2566P4W-R, AIR-ANT2524V4C-R.
AP 3600e	802.11b/g	AIR-ANT2524DB-R, AIR-ANT2524DW-R, AIR-ANT2524DG-R, AIR-ANT2566P4W-R, AIR-ANT2524V4C-R.
AP 3600i	802.11a	Internal-3600i-5 GHz
AP 3600i	802.11b/g	Internal-3600i-2.4 GHz
AP 3500p	802.11a	AIR-ANT5135DG-R, AIR-ANT5135D-R, AIR-ANT5135DW-R, AIR-ANT5140V-R, AIR-ANT5135SDW-R, AIR-ANT5160NP-R

Table 27-2 Supported Antennas (continued)

AP Type	Radio Type	Supported Antennas
AP 3500p	802.11b/g	AIR-ANT2422DG-R, AIR-ANT2422DB-R, AIR-ANT2422DW-R, AIR-ANT1728, AIR-ANT2410Y-R, AIR-ANT2506, AIR-ANT2430V-R, AIR-ANT1949, AIR-ANT2450S-R, AIR-ANT2460NP-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT2440NV-R, AIR-ANT2460P-R, AIR-ANT2485P-R
801GN	802.11a	Not Applicable
	802.11b/g	AIR-ANT4941, AIR-ANT2422DB-R
801AGN	802.11a	AIR-ANTM2050D-R
	802.11b/g	AIR-ANTM2050D-R
802GN	802.11a	Not Applicable
	802.11b/g	Internal-802.11
802AGN	802.11a	AIR-ANTM2050D-R
	802.11b/g	AIR-ANTM2050D-R
1552CU	802.11a	AIR-ANT2413P2M-N
	802.11b/g	AIR-ANT5114P2M-N
	802.11n	AIR-ANT2588P3M-N
1552EU	802.11a	AIR-ANT2413P2M-N
	802.11b/g	AIR-ANT5114P2M-N
	802.11n	AIR-ANT2588P3M-N
1552E	802.11b/g	AIR-ANT2420V-N

WLAN Override

The following 802.11a WLAN Override field appears:

- WLAN Override—Choose **Enable** or **Disable** from the drop-down list.

Note When you enable WLAN Override, operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a Cisco Radio.

Note WLAN override does not apply to access points that support the 512 WLAN feature.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

Note The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear:

- Current Channel—Channel number of the access point.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the channel of the access point is set globally by the controller.
  - Custom—Use this setting if the channel of the access point is set locally. Select a channel from the drop-down list.

    For example, if you select 2(17 dBm) as the custom power, 2 corresponds to the Power Level and 17 is the Absolute Power (dBm).
- Channel width—Select the channel width from the drop-down list. The selections include 20, above 40, and below 40.

  RF Channel assignment supports 802.11n 40 MHz channel width in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates.

Note Selecting a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

Note The power level and channel numbers of an access point are not audited.

Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following. When the XOR radio is in 5GHz, you can configure only **Global** assignment method.
  - Global—Use this setting if the power level is set globally by the controller.
  - Custom—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

Select any of the 11n Antenna Selection parameters:

- Antenna A

- Antenna B
- Antenna C
- Antenna D

11n Parameters

The following 11n fields appear:

- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose **Enable**, **Disable**, or **Not Applicable** from the drop-down list.

Configuring CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the Ethernet and radio ports of the bridge by default.

Configuring CDP on Access Points

To configure CDP on Radio or Ethernet interfaces, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 Choose an access point associated with software release 5.0 or later.

Step 3 Click the slots of radio or an Ethernet interface for which you want to enable CDP.

Step 4 Select the **CDP State** check box to enable CDP on the interface.

Step 5 Click **Save**.

Configuring Access Points XOR Antenna

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

If you choose **Configuration > Wireless Technologies > Access Point Radios**. and select an **XOR (2.4GHz) or XOR(5GHz)** from the Radio column, the following page appears.

This page contains the following fields:

Note Changing any of the fields causes the radio to be temporarily disabled and thus might result in loss of connectivity for some clients.

General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Slot ID—Slot ID.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the **CDP State** check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—From the drop-down choose any of the options: Both Disabled, 5GHz Enabled, 2.4 GHz Enabled, and Both Enabled.

Radio Assignment

- Assignment Method—The assignment methods are: **Auto**, **Serving**, or **Monitor**.

Note Band Selection, RF Channel Assignment, and Tx Power Level Assignment appears only for Serving assignment method.

- Band Selection— You can either choose 2.4 GHz or 5 GHz radio.

Antenna

Depending on the Radio Assignment selection, the following parameters appear:

- Antenna Type—Indicates the antenna type: External or Internal.
- XOR A Antenna—(Displayed only for Auto assignment method). Choose the external antenna or **Other** from the drop-down list.
- XOR B Antenna—(Displayed only for Auto assignment method). Choose the external antenna or **Other** from the drop-down list.
- External Antenna—(Displayed for Serving and Monitor assignment method). Choose the **external antenna** or **Other** from the drop-down list. The values in the drop-down varies for 2.4 GHz and 5GHz radio.
- Antenna Gain—(Displayed for Serving and Monitor assignment method.) Enter the desired antenna gain in the text box. To configure the custom antenna gain, select **Others** for the External Antenna option.

Note The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear only if you have selected Radio Assignment method as Serving.

- Current Channel—Channel number of the access point.
- Channel Width—Only radios with 20 MHz is supported for a 2.4 GHz radio. For a 5 GHZ radio, from the Channel Width drop-down list, choose 20 MHz, 40 MHz, 80 MHz or 160 MHZ.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the channel of the access point is set globally by the controller.
  - Custom—Use this setting if the channel of the access point is set locally. Select a channel from the **Custom** drop-down list. The values in the drop-down varies for 2.4 GHz and 5 GHz radios.

11n and 11ac Parameters

- 11n Supported—Indicates whether or not 11n radio is supported.
- 11ac Supported—Indicates whether or not 11ac radio is supported.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

Note The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following. When the XOR radio is in 5GHz, you can configure only **Global** assignment method.
  - Global—Use this setting if the power level is set globally by the controller.
  - Custom—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

Select any of the 11n Antenna Selection parameters:

- Antenna A
- Antenna B
- Antenna C

- Antenna D

11n Parameters

The following 11n fields appear:

- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose **Enable**, **Disable**, or **Not Applicable** from the drop-down list.

Configuring Access Point Radios for Tracking Optimized Monitor Mode

To optimize monitoring and location calculation of tags, you can enable Tracking Optimized Monitor Mode (TOMM) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11b/g radio of the access point.

Note For details on enabling Monitor mode on an access point, see Step 6 in the "Configuring Access Point Details" section on page 27-12.

To set enable TOMM and assign monitoring channels on the access point radio, follow these steps:

Step 1 After enabling Monitor mode at the access point level, choose Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 In the Access Points page, click the **802.11 b/g Radio** link for the appropriate access point.

Step 3 In the General group box, disable **Admin Status** by unselecting the check box. This disables the radio.

Step 4 Select the **TOMM** check box. This check box only appears for Monitor Mode APs. The drop-down lists for each of the four configurable channels are displayed.

Step 5 Choose the four channels on which you want the access point to monitor tags.

Note You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, choose **None** from the channel drop-down list.

Step 6 Click **Save**. Channel selection is saved.

Step 7 In the Radio parameters page, reenable the radio by selecting the **Admin Status** check box.

Step 8 Click **Save**. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM in the Monitor > Access Points page.

Copying and Replacing Access Points

The Copy and Replace AP feature is useful if you need to remove an access point from the network and replace it with a new access point. All of the access point information, such as AP mode, name, and map location needs to be copied from the old access point to the new access point.

To access the **Copy and Replace AP** function, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 Select the check box for the applicable access point.

Step 3 From the Select a command drop-down list, choose **Copy and Replace AP**.

Step 4 Click **Go**.

The old access point needs to be removed from the network first. This access point then becomes unassociated to any controller.When you plug in the new access point, it is associated with the controller and Prime Infrastructure refreshes the information. At that point, select the old unassociated access point and choose to copy and replace the configuration to the new access point.

Note If a different access point type is used to replace an older access point, only the configuration parameters that apply are copied.

Bulk Copy and Replacing the Access Points

Using the Bulk Copy and Replace AP feature, you can remove hundreds of access points from the network and replace them with the new access points. The access point information such as, AP Mode, AP Name, and MAC Address is copied from the old access points to the new access points.

1. Physically replacing the APs:
   - Ensure that the access points that were associated with the Cisco WLC is already managed by the Cisco Prime Infrastructure.
   - Identify the APs that need to be replaced.
   - Older 802.11n APs are physically replaced with the newer 802.11ac APs.
   - Note down the Name and MAC address of the 802.11n and 802.11ac APs.
   - Update the CSV file with the new Name and MAC Address.
2. Refresh the Cisco WLC configurations on Cisco Prime Infrastructure:
   - After replacing the APs physically, refresh the WLC configurations on the Cisco Prime Infrastructure.
   - Ensure the Lightweight Operational Status Background task is running or enabled.
   - Go to **Configure > Controller > Access Points** to check if the new 802.11ac APs are displaying and the old 802.111n APs status is displayed as **Not Associated.**
3. Perform Bulk Copy Replace on the Cisco Prime Infrastructure. To perform bulk copy and replace AP, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 From the Select a command drop-down list, choose **bulk Copy and Replace AP**, click **Go**.

Step 3 Click Choose File to select CSV file, and then find the location of the CSV file that you want to import.

Step 4 Click **OK**.

Removing Access Points

To remove access points that are not associated, follow these steps:

Step 1 Choose **Configuration > Wireless Technologies > Access Point Radios**.

Step 2 From the Select a command drop-down list, choose **Remove APs**.

Step 3 Click **Go**.

Step 4 Click **OK** to confirm the removal.

Scheduling and Viewing Radio Status

This section contains the following topics;

Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box for the applicable access point(s).

Step 3 From the Select a command drop-down list, choose **Schedule Radio Status**.

Step 4 Click **Go**.

Step 5 Choose **Enable** or **Disable** from the Admin Status drop-down list.

Step 6 Use the Hours and Minutes drop-down lists to determine the scheduled time.

Step 7 Click the calendar icon to select the scheduled date for the status change.

Step 8 If the scheduled task is recurring, choose **Daily** or **Weekly**, as applicable. If the scheduled task is a one-time event, choose **No Recurrence**.

Step 9 Choose **Save** to confirm the scheduled task.

Viewing Scheduled Tasks

To view currently scheduled radio status tasks, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box for the applicable access point(s).

Step 3 From the Select a command drop-down list, choose **View Scheduled Radio Task(s)**.

Step 4 Click **Go**.

The Scheduled Task(s) information includes:

- Scheduled Task(s)—Choose the task to view its access points and access point radios.
- Scheduled Radio adminStatus—Indicates the status change (Enable or Disable).
- Schedule Time—Indicates the time the schedule task occurs.
- Execution status—Indicates whether or not the task is scheduled.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.
- Next Execution—Indicates the time and date of the next task occurrence.
- Last Execution—Indicates the time and date of the last task occurrence.
- Unschedule—Click **Unschedule** to cancel the scheduled task. Click **OK** to confirm the cancellation.

Viewing Audit Status (for Access Points)

An Audit Status column in the Configure > Access Points page shows an audit status for each of the access points. You can also view the audit report for the selected access points. The report shows the time of the audit, the IP address of the selected access point, and the synchronization status.

To view the audit status, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Click the **Audit Status** column value to go to the latest audit details page for the selected access point. This report is interactive and per access point.

Note If you hover your mouse cursor over the Audit Status column value, the time of the last audit is displayed.

To run an access point on-demand audit report, select the desired access point for which you want to run the report and choose **Audit Now** from the Select a command drop-down list. In versions prior to 4.1, the audit only spanned the parameters present in the AP Details and AP Interface Details page. In Release 4.1, this audit report covers complete access point level auditing. The audit results are stored in the database so that you can view the latest audit reports without having to run another audit.

Note The audit can only be run on an access point that is associated to a controller.

Filtering Alarms for Maintenance Mode Access Points

Prime Infrastructure uses critical alarms to track if the managed access points are down. The controller sends three different alarms when the following occurs:

- The Access point is down
- Radio A of the access point is down
- Radio B/G of the access point is down

In Release 7.0.172.0 and later, these 3 alarms are grouped into a single alarm.

When an access point is under technical maintenance, the critical alarms need to be deprioritized. You can deprioritize the severity of an alarm of an access point using the Configure > Access Points page. When you move an access point to maintenance state, the alarm status for that access point appears in black color.

This section contains of the following topics:

- Placing an Access Point in Maintenance State, page 27-39
- Removing an Access Point from Maintenance State, page 27-39

Placing an Access Point in Maintenance State

To move an access point to the maintenance state, follow these steps:

Step 1 Choose **Prime Infrastructure > Configure > Access Points**.

The Access Points page appears.

Step 2 From the drop-down list, choose **Place in Maintenance State**, and click **Go**.

The access point is moved to maintenance state.

Once the access point is moved to maintenance state, the access point down alarms are processed with lower severity instead of critical.

Removing an Access Point from Maintenance State

To remove an access point from the maintenance state, follow these steps:

Step 1 Choose **Prime Infrastructure > Configure > Access Points**.

The Access Points page appears.

Step 2 From the drop-down list, choose **Remove from Maintenance State**, and click **Go**.

The access point is removed from the maintenance state.

Searching Access Points

Use the search options in the uppermost right corner of the page to create and save custom searches:

- New Search: Enter an IP address, name, SSID, or MAC, and click **Search**.
- Saved Searches: Click **Saved Search** to choose a category, a saved custom search, or choose other criteria for a search from the drop-down lists.
- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.

After you click **Go**, the access point search results appear (see Table 27-3).

Table 27-3 Access Point Search Results

Field	Options
IP Address	IP address of the access point.
Ethernet MAC	MAC address of the access point.
AP Name	Name assigned to the access point. Click the access point name item to display details.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.
Controller	IP address of the controller.
AP Type	Access point radio frequency type.
Operational Status	Displays the operational status of the Cisco radios (Up or Down).
Alarm Status	Alarms are color coded as follows: • Clear = No Alarm • Red = Critical Alarm • Orange = Major Alarm • Yellow = Minor Alarm
Audit Status	The audit status of the access point.
Serial Number	The serial number of the access point.
AP Mode	Describes the role of the access point modes such as Local, FlexConnect, Monitor, Rogue Detector, Sniffer, Bridge, or SE-Connect.

Viewing Mesh Link Details

You can access mesh link details in several ways:

- Click the **Mesh** dashboard in Prime Infrastructure home page
- Choose **Monitor > Access Points**, click the **Mesh Links** tab and then click the **Details** link
- After you import a KML file from Google Earth, click the **AP Mesh** link

The current statistics are displayed at the top of the page followed by diagrams for certain statistics.

- SNR Graph—SNR Up and Down graphs are combined into one graph. Each set of data is represented by different colors.

- Link Metrics Graph—The Adjusted Link Metric and Unadjusted Link Metric is combined into one graph. Each set of data is represented by different colors.
- Packet Error Rate Graph—Displays the packet error rates in a graph.
- Link Events—The last five events for the link are displayed.
- Mesh Worst SNR Links—Displays the worst signal-to-noise ratio (SNR) links.
- AP Uptime—These statistics help determine if an access point is rebooting frequently.
- LWAPP Join Taken Time—These statistics determine how long it takes an access point to join.
- Location Links—Allows you to navigate to Prime Infrastructure map or the Google Earth location.

Viewing or Editing Rogue Access Point Rules

You can view or edit current rogue access point rules on a single WLC.

To access the rogue access point rules, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **Security > Rogue AP Rules**. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.

Step 4 Choose a Rogue AP Rule to view or edit its details.

Wireless Configuration Groups [Beta]

Wireless Configuration Groups [Beta] workflow is the improved workflow of WLAN Controller Configuration Groups feature, which is available in the Prime Infrastructure. With the improved Wireless Configuration workflow, you can:

- Select device specific templates.
- Deploy multiple templates on multiple devices.
- Audit multiple wireless templates from PI.

Note Dependency templates do not work in this workflow.

Related Topic

- Creating a New Configuration Group
- Adding or Removing Templates from Wireless Configuration Group
- Auditing Wireless Configuration Groups

Creating a New Configuration Group

Step 1 Choose **Configuration > Wireless Technologies > Wireless Configuration Groups [Beta]**.

Step 2 Click **Create** to create a new configuration group.

The Configuration Group Workflow wizard appears.

Step 3 In the **General Configuration** tab, enter the configuration group name, and click **Next**.

The Select Template tab appears.

Step 4 In the Select Template tab, select the Device Type: **CUWN** or **CUWN-IOS**.

Step 5 Drag and drop a template or a group from **Templates** tree view > **My Templates** to the **Selected Template(s)** group box.

The Selected Template(s) group box lists templates or groups, which were added from the Templates tree view.

Step 6 Click **Save and Quit** to save the configuration group and quit the work flow.

Step 7 Click **Next** to save the configuration group and to deploy the templates selected.

The Select Devices tab appears.

Step 8 The Select Devices tab lists Controllers based on the device type selected.

Step 9 Select the **Device Name** check box and click **Deploy**.

Once the deploy is successful, the Wireless Configuration Groups list page appears.

The Wireless Configuration Groups page contains the following details for the deployed device:

- Group Name
- Deployed Devices Count
- Templates Count
- Last Modified On
- Last Applied On
- Deploy Status
  - Not Initiated —Indicates if the device is deployed on any of the devices or not.
  - Success—Indicates the number of successful templates associated with the applicable IP address.
  - Partial Success / Failure—Indicates the number of failures with provisioning of templates to the applicable controller. Click on **Partial Success / Failure** link to know the reason for failure.

Auditing Wireless Configuration Groups

The Config Groups Audit page allows you to verify if the controllers configuration complies with the group template. During the audit, you can leave this screen or logout of Cisco Prime Infrastructure. The process continues, and you can return to this page later to view the report.

Note Do not perform any other configuration group functions during the audit verification.

Step 1 Choose **Configuration > Wireless Technologies > Wireless Configuration Groups [Beta].**

Step 2 Select the Group Name check box, and click **Audit**.

The Select Devices page appears.

Step 3 Select a **Device Name** check box and click Audit.

A report is generated and the current configuration on each controller is compared with that in the configuration group template. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

- Audit Status
  - Not Initiated
  - Success—Indicates whether the number of templates associated with the applicable IP address are in sync or not.
  - Not In Sync—Indicates the number of failures with provisioning of templates to the applicable controller. Click **Not In Sync** to know more details.

Adding or Removing Templates from Wireless Configuration Group

Step 1 Choose **Configuration > Wireless Technologies > Wireless Configuration Groups [Beta].**

Step 2 Select the Group Name check box, and click **Edit**.

Step 3 In the Config Group Workflow wizard, click **Select Templates** tab.

Step 4 Choose **CUWN** or **CUWN-IOS**.

- Drag and drop a template or a group from the Templates Tree view to the Selected Template(s) group box.

The Selected Template(s) group box will list the selected template or groups which were added from the Templates Tree view.

Configuring WLAN Controller Auto Provisioning

Prime Infrastructure simplifies WLAN deployments with support for auto-provisioning. Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current Cisco Wireless LAN Controller (WLC). Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

For Auto Provision to complete successfully so that Cisco Prime Infrastructure manages Cisco WLC, the Cisco WLC needs to send a COLD_START trap to the trap receiver (Prime Infrastructure). Prime infrastructure on receiving this trap checks if the device is marked for auto provision. If the device is marked for auto provision, it adds that device to Prime infrastructure and manages it.

Note The controller radio and b/g networks are initially disabled by the Prime Infrastructure startup configuration file. You can turn on those radio networks by using a template, which should be included as one of the automated templates.

Related Topics

- Adding an Auto Provisioning Filter
- Auto Provisioning Primary Search Key Settings

The Auto Provision Filters page allows you to create and edit auto provisioning filters that define the list of allowable devices to be auto provisioned or auto monitored by Prime Infrastructure.

For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status. To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using **Administration > Users, Roles, & AAA > User Groups >** ***group name*** **> List of Tasks Permitted** in Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

Filter parameters include:

Parameter	Description
Filter Name	Identifies the name of the filter.
Filter Enable	Indicates whether or not the filter is enabled. Only enabled filters can participate in the Auto Provisioning process.
Monitor Only	If selected, the Cisco WLC defined in this filter is managed by Prime Infrastructure but not configured by Prime Infrastructure if the Cisco WLC contacts Prime Infrastructure during the auto provisioning process.
Filter Mode	Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).
Config Group Name	Indicates the Configuration Group name. All Config-Groups used by auto provision filters should not have any controller defined in them.

Adding an Auto Provisioning Filter

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To add an Auto Provisioning Filter:

Step 1 Choose **Configuration >Wireless Technologies > WLAN Controller Auto Provisioning**.

Step 2 Choose **Add Filter** from the **Select a command** drop-down list, then click **Go**.

Step 3 Enter the required parameters.

You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the graphical user interface.

Step 4 Click **Save**.

To change the default username and password, you need to delete and then recreate the admin user and explained in Steps 5 through Step 8.

Step 5 To change the default username and password, you need to create a new read/write user on the controller using the Local Management User Template.You must create this new user so that you can delete the default admin user as shown in Step 6.

Step 6 Choose **Inventory > Device Management > Network Devices > All Devices**, click on the controller name, click the **Configuration** tab, then select **Management > Local Management User**, select the admin user, then from the **Select a command** drop-down list, select **Delete Local Management User** and click **Go**.

Step 7 Create a new admin user on the controller using the Local Management User Template.

Step 8 Delete the user you created in Step 5.

Related Topic

- Controller > Management > Local Management User

Auto Provisioning Primary Search Key Settings

Use the Primary Search Key Setting to set the matching criteria search order.

Step 1 Choose **Configuration > Plug and Play > Controller Auto Provisioning**, then from the left sidebar menu, choose **Setting**.

Step 2 Click to highlight the applicable search key, then use the **Move Up** or **Move Down** buttons to move the search key to a higher or lower priority.

Step 3 Click **Save** to confirm the changes.