

Location Services

- Cisco Hyperlocation, on page 1
- Optimizing RFID Tracking on Access Points, on page 5
- Location Settings, on page 7
- Probe Request Forwarding, on page 12
- CCX Radio Management, on page 13
- Mobile Concierge, on page 17
- CMX Cloud Connector, on page 34

Cisco Hyperlocation

The Cisco Hyperlocation radio module provides the following:

- WSM Radio Module functions that are extended to:
  - 802.11ac
  - Wi-Fi Transmit
  - WSM and RRM channel scanning that is extended to 20-MHz, 40-MHz, and 80-MHz channel bandwidth.
- Expanded location functionality:
  - Low latency location optimized channel scanning
  - 32-antenna angle of arrival (AoA)

Note The download BlockAckReq (BAR)/ Block Ack (BA) uses 1/3 of airtime in the worst case scenario when there is only one AP to do the AoA location.

In a typical AoA location usage, there are 4 to 5 participating APs. These APs send BAR/BA in a round robin fashion and only 5 to 6 percent airtime is used. For each 250 ms of dwell time, the primary AP schedules a 4ms-burst of BAR/BA every 9 ms. Therefore, sufficient airtime is available to support voice and video unless there is a case of extreme overload.

The Cisco Hyperlocation Radio Module is supported on Cisco Aironet 3600 and 3700 Series Access Points.

For more information about Cisco Hyperlocation, see the following documents:

- Cisco Hyperlocation Solution
- Cisco CMX 10.2 Configuration Guide to enable Cisco Hyperlocation
- Cisco CMX 10.2 Release Notes

Guidelines and Restrictions for Cisco Hyperlocation

- Hyperlocation configurations are not supported on Cisco APs in Sniffer mode.
- Cisco Hyperlocation in enabled state has an impact on performance where both radios of APs that do not have Cisco Hyperlocation module go off-channel for about 100 milliseconds every 3 seconds.
- When Hyperlocation is enabled, a burst of BARs are sent for location purposes. This takes about 6 percent to 10 percent of airtime.
- If submode wIPS is in enabled state, it is not possible to enable Hyperlocation or FastLocate.

This section contains the following subsections:

Cisco Hyperlocation in a High Availability Environment

The global and per AP-group Cisco Hyperlocation configuration is mirrored from primary to secondary controller. The secondary controller updates only the internal state and does not forward any configuration information to the APs.

For MSE message encryption, the controller generates an encryption key and sends it to the APs and to the MSE, which uses it for encryption and decryption as end clients. The secondary controller does not generate an encryption key and the AP and MSE use the actual key shared by the primary controller.

Cisco Hyperlocation Client Debug Tracing

The Cisco Hyperlocation Debug Client Tracing feature provides the ability to specify a client MAC address for detailed hyperlocation tracing. Enable this feature using the **test dot11 halo-client-trace client-mac** command. To disable this feature, use the **test dot11 halo-client-trace 0000.0000.0000** command.

Configuring Cisco Hyperlocation

Configuring Cisco Hyperlocation for all APs (GUI)

This section provides instructions to configure Cisco Hyperlocation for all APs, a specific AP, and a group of APs that have the Cisco Hyperlocation radio module and are associated with controller.

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration**.

Step 2 In the **Hyperlocation Config Parameters** section:

a) Check the **Enable Hyperlocation** check box.

Based on AP and installed module, checking the **Enable Hyperlocation** check box enables different location service (PRL-based or AoA-based).

b) Enter the **Packet Detection RSSI Minimum (dBm)** value.

This is the minimum level at which a data packet can be heard by the WSM modules for use in location calculations. The default value is –100 dBm.

We recommend that this value be increased if you want to have only strong signals used in calculating locations.

c) Enter the **Scan Count Threshold for Idle Client Detection** value.

The Scan Count Threshold represents the number of off-channel scan cycles the AP will wait before sending a Block Acknowledgment Request (BAR) to idle clients. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off channel scan cycle.

d) Enter the IPv4 address of the NTP server.

This is the IPv4 address of the NTP server that all APs that are involved in this calculation need to synchronize to.

We recommend that you use the same NTP server as is used by the general controller infrastructure. The scans from multiple AP need to be synchronized for the location to be accurately calculated.

Step 3 Save the configuration.

Configuring Cisco Hyperlocation for an AP (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs**.

Step 2 On the **All APs** page that is displayed, click the name of the access point for which you want to configure Cisco Hyperlocation.

Step 3 Click the **Advanced** tab.

This opens the window.

Step 4 In the **Hyperlocation Configuration** section, from the **Enable Hyperlocation** drop-down list, choose **AP Specific** and then check the check box next to the drop-down list to enable Cisco Hyperlocation for the AP.

Step 5 Save the configuration.

Configuring Cisco Hyperlocation for an AP Group (GUI)

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups**.

Step 2 Click the AP group name.

Step 3 Click the **Location** tab.

Step 4 In the **HyperLocation Config Parameters** section, check the **Enable Hyperlocation** check box to enable Hyperlocation for the AP group.

Step 5 Enter the **Packet Detection RSSI Minimum (dBm)** value.

This is the minimum level at which a data packet can be heard by the WSM modules for use in location calculations. The default value is –100 dDm.

We recommend that this value be increased if you want to have only strong signals used in calculating locations.

Step 6 Enter the **Scan Count Threshold for Idle Client Detection** value.

The Scan Count Threshold represents the number of off-channel scan cycles the APs will wait before sending a Block Acknowledgment Request (BAR) to idle clients. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off channel scan cycle.

Step 7 Enter the IPv4 address of the NTP server.

This is the IPv4 address of the NTP server that all APs that are involved in this calculation need to synchronize to.

We recommend that you use the same NTP server as is used by the general controller infrastructure. The scans from multiple APs need to be synchronized for the location to be accurately calculated.

Step 8 Save the configuration.

Configuring Cisco Hyperlocation for all APs (CLI)

Procedure

- Configure Cisco Hyperlocation for all APs by entering this command:
  config advanced hyperlocation {**enable** | **disable**}
- Configure the IP address of the NTP server by entering this command:
  config advanced hyperlocation ntp *ipv4-addr*
- Reset threshold value in scan cycles after trigger by entering this command:
  config advanced hyperlocation reset-threshold *value*
- Configure the threshold value below which RSSI is ignored while sending to controller by entering this command:
  config advanced hyperlocation threshold *value*
- Configure the number of scan cycles between PAK RSSI location trigger by entering this command:
  config advanced hyperlocation trigger-threshold *value*

- See a summary of Cisco Hyperlocation global configuration by entering this command:
  show advanced hyperlocation summary

Configuring Cisco Hyperlocation for an AP (CLI)

Procedure

- Configure Cisco Hyperlocation for a specific AP by entering this command:
  config advanced hyperlocation {**enable** | **disable**} *ap-name*

Configuring Cisco Hyperlocation for an AP Group (CLI)

Procedure

- Configure Cisco Hyperlocation for an AP group by entering this command:
  config advanced hyperlocation apgroup *group-name* {**enable** | **disable**}

Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

You can use the controller GUI or CLI to configure the access point for monitor mode and to then enable tracking optimization on the access point radio.

This section contains the following subsections:

Optimizing RFID Tracking on Access Points (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure monitor mode. The All APs > Details for page appears.

Step 3 From the AP Mode drop-down list, choose **Monitor**.

Step 4 Click **Apply**.

Step 5 Click **OK** when warned that the access point will be rebooted.

Step 6 Click **Save Configuration** to save your changes.

Step 7 Choose **Wireless** > **Access Points** > **Radios** > **802.11b/g/n** to open the 802.11b/g/n Radios page.

Step 8 Hover your cursor over the blue drop-down arrow for the desired access point and choose **Configure**. The 802.11b/g/n Cisco APs > Configure page appears.

Step 9 Disable the access point radio by choosing **Disable** from the Admin Status drop-down list and click **Apply**.

Step 10 Enable tracking optimization on the radio by choosing **Enable** from the Enable Tracking Optimization drop-down list.

Step 11 From the four Channel drop-down lists, choose the channels on which you want to monitor RFID tags.

Note
You must configure at least one channel on which the tags will be monitored.

Step 12 Click **Apply**.

Step 13 Click **Save Configuration**.

Step 14 To reenable the access point radio, choose **Enable** from the Admin Status drop-down list and click **Apply**.

Step 15 Click **Save Configuration**.

Optimizing RFID Tracking on Access Points (CLI)

Procedure

Step 1 Configure an access point for monitor mode by entering this command:

config ap mode monitor *Cisco_AP*

Step 2 When warned that the access point will be rebooted and asked if you want to continue, enter **Y**.

Step 3 Save your changes by entering this command:

save config

Step 4 Disable the access point radio by entering this command:

config 802.11b disable *Cisco_AP*

Step 5 Configure the access point to scan only the DCA channels supported by its country of operation by entering this command:

config ap monitor-mode tracking-opt *Cisco_AP*

Note
To specify the exact channels to be scanned, enter the **config ap monitor-mode tracking-opt** *Cisco_AP* command in *Step 6*.

Note
To disable tracking optimization for this access point, enter the **config ap monitor-mode no-optimization** *Cisco_AP* command.

Step 6 After you have entered the command in *Step 5*, you can enter this command to choose up to four specific 802.11b channels to be scanned by the access point:

config ap monitor-mode 802.11b fast-channel *Cisco_AP channel1 channel2 channel3 channel4*

Note
In the United States, you can assign any value between 1 and 11 (inclusive) to the *channel* variable. Other countries support additional channels. You must assign at least one channel.

Step 7 Reenable the access point radio by entering this command:

config 802.11b enable *Cisco_AP*

Step 8 Save your changes by entering this command:

save config

Step 9 See a summary of all access points in monitor mode by entering this command:

show ap monitor-mode summary

Location Settings

Configuring Location Settings (CLI)

The controller determines the location of client devices by gathering received signal strength indication (RSSI) measurements from access points all around the client of interest. The controller can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

Improve location accuracy by configuring the path loss measurement (S60) request for normal clients or calibrating clients by entering this command:

config location plm *?*

where *?* is one of the following:

- **client** {**enable** | **disable**} *burst_interval*—Enables or disables the path loss measurement request for normal, noncalibrating clients. The valid range for the *burst_interval* parameter is 1 to 3600 seconds, and the default value is 60 seconds.
- **calibrating** {**enable** | **disable**} {**uniband** | **multiband**}—Enables or disables the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio.

If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The **config location plm** command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the controller sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1, 6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.

These four additional location CLI commands are available; however, they are set to optimal default values, so we do not recommend that you use or modify them:

- Configure the RSSI timeout value for various devices by entering this command:

  config location expiry *?*

  where*?* is one of the following:

  - **client** *timeout*—Configures the RSSI timeout value for clients. The valid range for the *timeout* parameter is 5 to 3600 seconds, and the default value is 5 seconds.

- **calibrating-client** *timeout*—Configures the RSSI timeout value for calibrating clients. The valid range for the *timeout* parameter is 0 to 3600 seconds, and the default value is 5 seconds.
- **tags** *timeout*—Configures the RSSI timeout value for RFID tags. The valid range for the *timeout* parameter is 5 to 300 seconds, and the default value is 5 seconds.
- **rogue-aps** *timeout*—Configures the RSSI timeout value for rogue access points. The valid range for the *timeout* parameter is 5 to 3600 seconds, and the default value is 5 seconds.

  Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The **config location expiry** command enables you to specify the length of time after which old RSSI averages expire.



Note We recommend that you do not use or modify the **config location expiry** command.

- Configure the RSSI half life for various devices by entering this command:

  config location rssi-half-life *?*

  where *?* is one of the following:

  - **client** *half_life*—Configures the RSSI half life for clients. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
  - **calibrating-client** *half_life*—Configures the RSSI half life for calibrating clients. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
  - **tags** *half_life*—Configures the RSSI half life for RFID tags. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
  - **rogue-aps** *half_life*—Configures the RSSI half life for rogue access points. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

    Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The **config location rssi-half-life** command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life).



Note We recommend that you do not use or modify the **config location rssi-half-life** command.

- Configure the NMSP notification threshold for RSSI measurements by entering this command:

  config location notify-threshold *?*

  where *?* is one of the following:

  - **client** *threshold*—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the *threshold* parameter is 0 to 10 dB, and the default value is 0 dB.

- **tags** *threshold*—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the *threshold* parameter is 0 to 10 dB, and the default value is 0 dB.
- **rogue-aps** *threshold*—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the *threshold* parameter is 0 to 10 dB, and the default value is 0 dB.



Note We recommend that you do not use or modify the **config location notify-threshold** command.

- Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command:

  config location algorithm *?*

  where *?* is one of the following:

  - **simple**—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy.
  - **rssi-average**—Specifies a more accurate algorithm but requires more CPU overhead.



Note We recommend that you do not use or modify the **config location algorithm** command.

Viewing Location Settings (CLI)

To view location information, use these CLI commands:

- View the current location configuration values by entering this command:

  show location summary

- See the RSSI table for a particular client by entering this command:

  show location detail *client_mac_addr*

- See the location-based RFID statistics by entering this command:

  show location statistics rfid

- Clear the location-based RFID statistics by entering this command:

  clear location statistics rfid

- Clear a specific RFID tag or all of the RFID tags in the entire database by entering this command:

  clear location rfid {*mac_address* | **all**}

- See whether location presence (S69) is supported on a client by entering this command:

  show client detail *client_mac*

When location presence is supported by a client and enabled on a location appliance, the location appliance can provide the client with its location upon request. Location presence is enabled automatically on CCXv5 clients.

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI)

NMSP manages communication between the Cisco Connected Mobile Experience (Cisco CMX) and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.



Note The TCP port (16113) that the controller and Cisco CMX communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco CMX for NMSP to function.

Procedure

Step 1 Set the NMSP notification interval value for clients, RFID tags, and rogue clients and access points by entering these commands, where *interval* is a value between 1 and 180 seconds:

- **config nmsp notification interval rssi clients** *interval*
- **config nmsp notification interval rssi rfid** *interval*
- **config nmsp notification interval rssi rogues** *interval*

Step 2 See the NMSP notification intervals by entering this command:

show nmsp notification interval

Information similar to the following appears:

```
NMSP Notification Interval Summary

                                  RSSI Interval:
 Client.......................................... 2 sec
 RFID............................................ 2 sec
 Rogue AP........................................ 2 sec
 Rogue Client.................................... 2 sec

Spectrum Interval:
 Interferer device............................... 2 sec
```

Viewing NMSP Settings (CLI)

To view NMSP information, use these CLI commands:

- See the status of active NMSP connections by entering this command:

  show nmsp status

- See the NMSP capabilities by entering this command:

  show nmsp capability

- See the NMSP counters by entering this command:

  show nmsp statistics {**summary** | **connection**}

  where

  - **summary** shows the common NMSP counters.
  - **connection** shows the connection-specific NMSP counters.

- See the mobility services that are active on the controller by entering this command:

  show nmsp subscription {**summary** | **detail** | **detail** *ip_addr*}

  where

  - **summary** shows all of the mobility services to which the controller is subscribed.
  - **detail** shows details for all of the mobility services to which the controller is subscribed.
  - **detail** *ip_addr* shows details only for the mobility services subscribed to by a specific IP address.

- Clear all NMSP statistics by entering this command:

  clear nmsp statistics

Debugging NMSP Issues

Use these commands if you experience any problems with NMSP:

- Configure NMSP debug options by entering this command:

  debug nmsp *?*

  where *?* is one of the following:

  - **all** {**enable** | **disable**}—Enables or disables debugging for all NMSP messages.
  - **connection** {**enable** | **disable**}—Enables or disables debugging for NMSP connection events.
  - **detail** {**enable** | **disable**}—Enables or disables debugging for NMSP detailed events.
  - **error** {**enable** | **disable**}—Enables or disables debugging for NMSP error messages.
  - **event** {**enable** | **disable**}—Enables or disables debugging for NMSP events.
  - **message** {**tx** | **rx**} {**enable** | **disable**}—Enables or disables debugging for NMSP transmit or receive messages.
  - **packet** {**enable** | **disable**}—Enables or disables debugging for NMSP packet events.

- Enable or disable debugging for NMSP interface events by entering this command:

debug dot11 nmsp {**enable** | **disable**}

- Enable or disable debugging for IAPP NMSP events by entering this command:

  debug iapp nmsp {**enable** | **disable**}

- Enable or disable debugging for RFID NMSP messages by entering this command:

  debug rfid nmsp {**enable** | **disable**}

- Enable or disable debugging for access point monitor NMSP events by entering this command:

  debug service ap-monitor nmsp {**enable** | **disable**}

- Enable or disable debugging for wIPS NMSP events by entering this command:

  debug wips nmsp {**enable** | **disable**}

Probe Request Forwarding

Probe requests are 802.11 management frames sent by clients to request information about the capabilities of SSIDs. By default, access points forward acknowledged probe requests to the controller for processing. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. If desired, you can configure access points to forward both acknowledged and unacknowledged probe requests to the controller. The controller can use the information from unacknowledged probe requests to improve the location accuracy.

Configuring Probe Request Forwarding (CLI)

Procedure

Step 1 Enable or disable the filtering of probe requests forwarded from an access point to the controller by entering this command:

config advanced probe filter {**enable** | **disable**}

- **enable** (default)—Choose this parameter to only forward acknowledged probe requests to the controller.
- **disable**—Choose this parameter to forward both acknowledged and unacknowledged probe requests to the controller.

Step 2 Limit the number of probe requests sent to the controller per client per access point radio in a given interval by entering this command:

config advanced probe limit *num_probes interval*

where

- *num_probes* is the number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
- *interval* is the probe limit interval (from 100 to 64000 milliseconds).

The default value for *num_probes* is 2 probe requests, and the default value for *interval* is 500 milliseconds.

Step 3 Configure the backoff parameters for probe queue in a Cisco AP by entering this command:
config advanced probe backoff {**enable** | **disable**}

- **enable**(default)—Choose this parameter to use increased backoff parameters for probe response.
- **disable**—Choose this parameter to use default backoff parameter value for probe response.

Step 4 Enter the **save config** command to save your changes.

Step 5 See the probe request forwarding configuration by entering this command:

show advanced probe

Information similar to the following appears:

```
Probe request filtering.........................  Enabled
Probes fwd to controller per client per radio....  2
Probe request rate-limiting interval..........  500 msec
```

CCX Radio Management

You can configure two parameters that affect client location calculations:

- Radio measurement requests
- Location calibration

These parameters are supported in Cisco Client Extensions (CCX) v2 and later releases. They are designed to enhance location accuracy and timeliness for participating CCX clients.

For the location features to operate properly, the access points must be configured for Local, Monitor, or FlexConnect mode. Location features will not work on FlexConnect APs that have lost their controller connection and entered Standalone mode.

This section contains the following subsections:

Radio Measurement Requests

When you enable the radio measurement requests feature, lightweight access points issue broadcast radio measurement request messages to clients running CCXv2 or later releases. The access points transmit these messages for every SSID over each enabled radio interface at a configured interval. In the process of performing 802.11 radio measurements, CCX clients send 802.11 broadcast probe requests on all the channels specified in the measurement request. Cisco location appliances use the uplink measurements based on these requests received at the access points to quickly and accurately calculate the client location. You do not need to specify on which channels the clients are to measure. The controller, access point, and client automatically determine which channels to use.

The radio measurement requests feature enables the controller to also obtain information on the radio environment from the client's perspective (rather than from just that of the access point). In this case, the

access points issue unicast radio measurement requests to a particular CCXv4 or v5 client. The client then sends various measurement reports back to the access point and on to the controller. These reports include information about the radio environment and data used to interpret the location of the clients. To prevent the access points and controller from being overwhelmed by radio measurement requests and reports, only two clients per access point and up to 20 clients per controller are supported. You can view the status of radio measurement requests for a particular access point or client as well as radio measurement reports for a particular client from the controller CLI.

The controller software improves the ability of the location appliance to accurately interpret the location of a device through a CCXv4 feature called location-based services. The controller issues a path-loss request to a particular CCXv4 or v5 client. If the client chooses to respond, it sends a path-loss measurement report to the controller. These reports contain the channel and transmit power of the client.



Note Non-CCX and CCXv1 clients ignore the CCX measurement requests and do not participate in the radio measurement activity.

Location Calibration

For CCX clients that need to be tracked more closely (for example, when a client calibration is performed), the controller can be configured to command the access point to send unicast measurement requests to these clients at a configured interval and whenever a CCX client roams to a new access point. These unicast requests can be sent out more often to these specific CCX clients than the broadcast measurement requests, which are sent to all clients. When location calibration is configured for non-CCX and CCXv1 clients, the clients are forced to disassociate at a specified interval to generate location measurements.

Configuring CCX Radio Management

Configuring CCX Radio Management (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the 802.11a/n/ac or 802.11b/g/n **Global Parameters** page.

Step 2 Under CCX Location Measurement, select the **Mode** check box to globally enable CCX radio management. This parameter causes the access points connected to this controller to issue broadcast radio measurement requests to clients running CCX v2 or later releases. The default value is disabled (or unselected).

Step 3 If you selected the Mode check box in the previous step, enter a value in the Interval text box to specify how often the access points are to issue the broadcast radio measurement requests.

The range is 60 to 32400 seconds.

The default is 60 seconds.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 Follow the instructions in *Step 2* of the Configuring CCX Radio Management (CLI) section below to enable access point customization.

Note
To enable CCX radio management for a particular access point, you must enable access point customization, which can be done only through the controller CLI.

Step 7 If desired, repeat this procedure for the other radio band (802.11a/n/ac or 802.11b/g/n).

Configuring CCX Radio Management (CLI)

Procedure

Step 1 Globally enable CCX radio management by entering this command:

config advanced {**802.11a** | **802.11b**} **ccx location-meas global enable** *interval_seconds*

The range for the *interval_seconds* parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes all access points connected to this controller in the 802.11a or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or later releases.

Step 2 Enable access point customization by entering these commands:

- **config advanced** {**802.11a** | **802.11b**} **ccx customize** *Cisco_AP* {**on** | **off**}

  This command enables or disables CCX radio management features for a particular access point in the 802.11a or 802.11b/g network.

- **config advanced** {**802.11a** | **802.11b**} **ccx location-meas ap** *Cisco_AP* **enable** *interval_seconds*

  The range for the *interval_seconds* parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes a particular access point in the 802.11a or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or higher.

Step 3 Save your settings by entering this command:

save config

Viewing CCX Radio Management Information (CLI)

- To see the CCX broadcast location measurement request configuration for all access points connected to this controller in the 802.11a or 802.11b/g network, enter this command:

  show advanced {**802.11a** | **802.11b**} **ccx global**

- To see the CCX broadcast location measurement request configuration for a particular access point in the 802.11a or 802.11b/g network, enter this command:

  show advanced {**802.11a** | **802.11b**} **ccx ap** *Cisco_AP*

- To see the status of radio measurement requests for a particular access point, enter this command:

show ap ccx rm *Cisco_AP* **status**

Information similar to the following appears:

```
A Radio

  Beacon Request.............................. Enabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Disabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration................................... 5

B Radio

  Beacon Request.............................. Disabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Enabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration.................................. 5
```

- To see the status of radio measurement requests for a particular client, enter this command:

  show client ccx rm *client_mac* **status**

  Information similar to the following appears:

```
Client Mac Address.......................... 00:40:96:ae:53:b4
Beacon Request.............................. Enabled
Channel Load Request........................ Disabled
Frame Request............................... Disabled
Noise Histogram Request..................... Disabled
Path Loss Request........................... Disabled
Interval.................................... 5
Iteration................................... 3
```

- To see radio measurement reports for a particular client, enter these commands:

  show client ccx rm *client_mac* **report beacon**—Shows the beacon report for the specified client.

  show client ccx rm *client_mac* **report chan-load**—Shows the channel-load report for the specified client.

  show client ccx rm *client_mac* **report noise-hist**—Shows the noise-histogram report for the specified client.

  show client ccx rm *client_mac* **report frame**—Shows the frame report for the specified client.

- To see the clients configured for location calibration, enter this command:

  show client location-calibration summary

- To see the RSSI reported for both antennas on each access point that heard the client, enter this command:

  show client detail *client_mac*

Debugging CCX Radio Management Issues (CLI)

- Debug CCX broadcast measurement request activity by entering this command:

debug airewave-director message {**enable** | **disable**}

- Debug client location calibration activity by entering this command:

  debug ccxrm [**all** | **error** | **warning** | **message** | **packet** | **detail** {**enable** | **disable**}]

- The CCX radio measurement report packets are encapsulated in Internet Access Point Protocol (IAPP) packets. Therefore, if the previous **debug ccxrm** command does not provide any debugs, enter this command to provide debugs at the IAPP level:

  debug iapp error {**enable** | **disable**}

- Debug the output for forwarded probes and their included RSSI for both antennas by entering this command:

  debug dot11 load-balancing

Mobile Concierge

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

Configuring Mobile Concierge (802.11u) (GUI)

Procedure

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

Step 2 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the 802.11u parameters and select 802.11u. The 802.11u page appears.

Step 3 Check the **802.11u Status** check box to enable 802.11u on the WLAN.

Step 4 In the 802.11u General Parameters area, do the following:

a) Check the **Internet Access** check box to enable this WLAN to provide Internet services.
b) From the **Network Type** drop-down list, choose the network type that best describes the 802.11u you want to configure on this WLAN.
c) From the **Network Auth Type** drop-down list, choose the authentication type that you want to configure for the 802.11u parameters on this network.
d) In the **HESSID** box, enter the homogenous extended service set identifier (HESSID) value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.
e) If the IP address is in the IPv4 format, then from the IPv4 Type drop-down list, choose the IPv4 address type.

f) From the **IPv6 Type** drop-down list, choose whether you want to make the IPv6 address type available or not.

Step 5 In the **OUI List** area, do the following:

a) In the **OUI** field, enter the Organizationally Unique Identifier, which can be a hexadecimal number represented in 3 or 5 bytes (6 or 10 characters). For example, AABBDF.

b) Check the **Is Beacon** check box to enable the OUI beacon responses.

Note
You can have a maximum of 3 OUIs with this field enabled.

c) From the **OUI Index** drop-down list, choose a value from 1 to 32. The default is 1.

d) Click **Add** to add the OUI entry to the WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 6 In the **Domain List** area, do the following:

a) In the **Domain Name** box, enter the domain name that is operating in the WLAN.

b) From the **Domain Index** drop-down list, choose an index for the domain name from 1 to 32. The default is 1.

c) Click **Add** to add the domain entry to the WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 7 In the **Realm List** area, do the following:

a) In the **Realm** field, enter the realm name that you can assign to the WLAN.

b) From the **Realm Index** drop-down list, choose an index for the realm from 1 to 32. The default is 1.

c) Click **Add** to add the domain entry to this WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 8 In the **Cellular Network Information List** area, do the following:

a) In the **Country Code** field, enter the 3-character mobile country code.

b) From the **CellularIndex** drop-down list, choose a value between 1 and 32. The default is 1.

c) In the **Network Code** field, enter the character network code. The network code can be 2 or 3 characters.

d) Click **Add** to add the cellular network information to the WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and select **Remove**.

Step 9 Click **Apply**.

Configuring Mobile Concierge (802.11u) (CLI)

Procedure

- To enable or disable 802.11u on a WLAN, enter this command:

  config wlan hotspot dot11u {**enable** | **disable**} *wlan-id*

- To add or delete information about a third generation partnership project's cellular network, enter this command:

config wlan hotspot dot11u 3gpp-info {**add** *index mobile-country-code network-code wlan-id* | **delete** *index wlan-id*}

- To configure the domain name for the entity operating in the 802.11u network, enter this command:

  config wlan hotspot dot11u domain {{{**add** | **modify**} *wlan-id domain-index domain-name*} | {**delete** *wlan-id domain-index*}}

- To configure a homogenous extended service set identifier (HESSID) value for a WLAN, enter this command:

  config wlan hotspot dot11u hessid *hessid wlan-id*

  The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

- To configure the IP address availability type for the IPv4 and IPv6 IP addresses on the WLAN, enter this command:

  config wlan hotspot dot11u ipaddr-type *ipv4-type ipv6-type wlan-id*

- To configure the network authentication type, enter this command:

  config wlan hotspot dot11u auth-type *network-auth wlan-id*

- To configure the Roaming Consortium OI list, enter this command:

  config wlan hotspot dot11u roam-oi {{{**add** | **modify**} *wlan-id oi-index oi is-beacon*} | {**delete** *wlan-id oi-index*}}

- To configure the 802.11u network type and internet access, enter this command:

  config wlan hotspot dot11u network-type *wlan-id network-type internet-access*

- To configure the realm for the WLAN, enter this command:

  config wlan hotspot dot11u nai-realm {{{**add** | **modify**} *realm-name wlan-id realm-index realm-name* | {**delete** *realm-name wlan-id realm-index*}}

- To configure the authentication method for the realm, enter this command:

  config wlan hotspot dot11u nai-realm {**add** | **modify**} **auth-method** *wlan-id realm-index eap-index auth-index auth-method auth-parameter*

- To delete the authentication method for the realm, enter this command:

  config wlan hotspot dot11u nai-realm delete auth-method *wlan-id realm-index eap-index auth-index*

- To configure the extensible authentication protocol (EAP) method for the realm, enter this command:

  config wlan hotpspot dot11u nai-realm {**add** | **modify**} **eap-method** *wlan-id realm-index eap-index eap-method*

- To delete the EAP method for the realm, enter this command:

  config wlan hotspot dot11u nai-realm delete eap-method *wlan-id realm-index eap-index*

Online Sign Up

Online Sign Up (OSU) is a process in which a mobile device is registered with a service provider, enabling users to select a plan to obtain network access. After the sign-up, the device receives the users' credentials to

connect to the network. A network architecture for OSU is given below, which consists of a service provider network and a hotspot:

The service provider network consists of an OSU server, an Authentication, Authorization and Accounting (AAA) server, and (access to) a Certification Authority (CA). These devices may be co-located or separate.

The hotspot has its own OSU, which is optional, and a AAA server. The hotspot is configured to allow only HTTPS traffic to OSU servers. An OSU server registers new customers and provides security credentials to their mobile devices. It can also be used to initially provision devices of existing customers. The AAA server of the service provider is used to authenticate subscribers based on the information received from the OSU server.

The OSU process ensures that:

- A user is communicating with the intended service provider network and OSU server.
- The communication is protected between the mobile device and OSU server.
- Poor security practices of one service provider affecting other service providers are reduced.

The controller should support the following requirements:

- Hotspot 2.0 Indication Element
- OSU Service Provider List
- Icon Request and Response Access Network Query Protocol (ANQP) Element
- OSU Server-Only Authenticated L2 Encryption Network (OSEN)
- Wireless Network Management (WNM) Notification Subscription Remediation Request
- WNM Notification Deauth Imminent Request
- Basic Service Set (BSS) Transition Management Request Frame - Session URL
- QoS Map Set
- Extended Capability Bit Support:
  - WNM Notification
  - QoS Map Set

Hotspot 2.0 Indication Element

This element (using vendor-specific information) enables the controllers and mobile devices to indicate that they are HotSpot (HS) 2.0 capable. All the beacon and probe response frames from HS 2.0 controllers contain this HS 2.0 indication element. For mobile devices, the association and re-association request frames contain the HS 2.0 indication element.

OSU Service Provider List

This element provides information for the entities offering OSU service. The following information is provided for each OSU provider:

- A friendly name (in one or more human languages)-Name of the OSU provider in human language, which matches the name drawn from the OSU server certificate exactly.

- The Network Access Identifier (NAI) used to authenticate to the OSU (if configured for OSEN).
- The icons and Uniform Resource Identifier (URI) of the OSU server.



Note The controller supports a maximum of 16 service providers per OSU-SP list.

The Icon Request or Response ANQP Element

This element provides a filename for the (icon) download request from the mobile device, which is one of the filenames included in the OSU providers list element. The maximum file size for the icon is 65535 octets; the file type should be a valid image type, for example, PNG, JPEG, and so on. The file type restriction is not applicable for controllers and supports a maximum of 16 icons.

OSEN

The OSEN element is used to advertise and select an OSEN-capable network.

WNM Notification Subscription Remediation Request

The WNM notification request is sent from a controller to a mobile device to indicate that subscription remediation is required when the AAA server indicates to controller of this requirement through the RADIUS Access-Accept message. After the authentication is complete, the controller sends WNM notification to the mobile device, using the URL of the Subscription Remediation server as the server URL.

WNM Notification Deauth Imminent Request

A home SP uses the Deauthentication Imminent Notice to inform the mobile device when it is no longer authorized to use the service due to a temporary condition in the network that requires deauthentication, for example, congestion in the Wi-Fi AN or congestion on a mobile core network element. The notice also provides information on the time that must elapse before the AAA server permits the mobile device to reauthenticate again on the same Basic Service Set (BSS) or Extended Service Set (ESS). Following this, the mobile device should not try to reauthenticate to the same BSS or ESS until the expiry of the reauthentication delay.

BSS Transition Management Request Frame - Session URL

The controller uses the BSS Transition Management Request frame to inform the mobile device of the impending session expiry. It also provides an URL to the user detailing on how to extend the session. The controller gets the information about session warning time and URL from the AAA server through the Access-Accept message.

Extended Capability Bit Support

This element has two sections, WNM Notification and QoS Map Set, which are explained in the previous sections.

802.11u MSAP

MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers.

Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.

This section contains the following subsections:

Configuring 802.11u MSAP (GUI)

Procedure

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

Step 2 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the MSAP parameters and select **Service Advertisements**. The Service Advertisement page appears.

Step 3 Enable the service advertisements.

Step 4 Enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.

Step 5 Click **Apply**.

Configuring MSAP (CLI)

Procedure

- To enable or disable MSAP on a WLAN, enter this command:

  config wlan hotspot msap {**enable** | **disable**} *wlan-id*

- To assign a server ID, enter this command:

  config wlan hotspot msap server-id *server-id wlan-id*

Configuring 802.11u HotSpot

Information About 802.11u HotSpot

This feature, which enables IEEE 802.11 devices to interwork with external networks, is typically found in hotspots or other public networks irrespective of whether the service is subscription based or free.

The interworking service aids network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks prior to association. Interworking not only helps users within the home, enterprise, and public access, but also assists manufacturers and operators to provide common components and services for IEEE 802.11 customers. These services are configured on a per WLAN basis on the controller.



Note The Downstream Group-Addressed Forwarding (DGAF) bit in the Hotspot 2.0 IE will not be updated automatically until you disable and enable the WLAN.

Configuring 802.11u HotSpot (GUI)

Procedure

Step 1 Choose **WLAN** to open the **WLANs** window.

Step 2 Hover your mouse over the blue drop-down arrow that corresponds to the desired WLAN on which you want to configure the HotSpot parameters and choose **HotSpot**. The **WLAN > HotSpot 2.0** page is displayed.

Step 3 On the **WLAN > HotSpot 2.0** window, enable HotSpot2.

Step 4 In the **Domain ID** field, enter the domain identifier.

Step 5 In the **OSU SSID** field, enter the OSU SSID.

Step 6 To set the WAN link parameters, perform the following tasks:

a) From the **WAN Link Status** drop-down list, choose the status. The default is the Not Configured status.
b) From the **WAN Symmetric Link Status** drop-down list, choose the status as either **Different** or **Same**.
c) Enter the **WAN Downlink and Uplink** speeds. The maximum value is 4,294,967,295 kbps.

Step 7 In the **Online Sign Up List** area, perform the following tasks:

a) From the **OSU Index** drop-down list, choose the OSU index you want to use.
b) From the **Lang Code** drop-down list, choose the language code you want to use, and select whether its in ASCII or HEX format from the next drop down list.
c) In the **SP Name** field, enter the service provider name.
d) In the **Description** field, enter the description.
e) Click **Add** to add the parameters to the list.

Step 8 In the **Operator Name List** area, perform the following tasks:

a) In the **Operator Name** text box, enter the name of the 802.11 operator.
b) From the **Operator index** drop-down list, choose an index value between 1 and 32 for the operator.
c) In the **Language Code** field, enter an ISO-14962-1997-encoded string defining the language. This string is a three-character language code.
d) Click **Add** to add the operator details.

The operator details are displayed in a tabular form. To remove an operator, hover your mouse pointer over the blue drop-down arrow and choose **Remove**.

Step 9 In the **Port Config List** area, perform the following tasks:

a) From the **IP Protocol** drop-down list, choose the IP protocol that you want to enable.
b) From the **Port No** drop-down list, choose the port number that is enabled on the WLAN.
c) From the **Status** drop-down list, choose the status of the port.
d) From the **Index** drop-down list, choose an index value for the port configuration.
e) Click **Add** to add the port configuration parameters.

To remove a port configuration list, hover your mouse over the blue drop-down arrow and choose **Remove**.

Step 10 Click **Apply**.

Configuring HotSpot 2.0 (CLI)

Note The character '?' is not supported in the value part of the commands.

Procedure

- To enable or disable HotSpot2 on a WLAN, enter this command:

  config wlan hotspot hs2 {**enable** | **disable**}

- To configure the operator name on a WLAN, enter this command:

  config wlan hotspot hs2 operator-name {**add** | **modify**} *wlan-id index operator-name lang-code*

  The following options are available:

  - *wlan-id*—The WLAN ID on which you want to configure the operator-name.
  - *index*—The operator index of the operator. The range is 1 to 32.
  - *operator-name*—The name of the 802.11an operator.
  - *lang-code*—The language used. An ISO-14962-1997 encoded string defining the language. This string is a three character language code. Enter the first three letters of the language in English (For example: eng for English).

Tip Press the **tab** key after entering a keyword or argument to get a list of valid values for the command.

- To delete the operator name, enter this command:

  config wlan hotspot hs2 operator-name delete *wlan-id index*

- To configure the port configuration parameters, enter this command:

  config wlan hotspot hs2 port-config {**add** | **modify**} *wlan-id index ip-protocol port-number*

- To delete a port configuration, enter this command:

  config wlan hotspot hs2 port-config delete *wlan-id index*

- To configure the WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics *wlan-id link-status symet-link downlink-speed uplink-speed*

  The values are as follows:

  - *link-status*—The link status. The valid range is 1 to 3.
  - *symet-link*—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
  - *downlink-speed*—The downlink speed. The maximum value is 4,194,304 kbps.
  - *uplink-speed*—The uplink speed. The maximum value is 4,194,304 kbps.

- To clear all HotSpot configurations, enter this command:

  config wlan hotspot clear-all *wlan-id*

- To configure the Access Network Query Protocol (ANQP) 4-way messaging, enter this command:

  config advanced hotspot anqp-4way {**enable** | **disable** | **threshold** *value*}

- To configure the ANQP comeback delay value in terms of TUs, enter this command:

  config advanced hotspot cmbk-delay *value*

- To limit the number of GAS request action frames to be sent to the controller by an AP in a given interval, enter this command:

  config advanced hotspot gas-limit {**enable** *num-of-GAS-required interval* | **disable**}

Configuring Access Points for HotSpot2 (GUI)

When HotSpot2 is configured, the access points that are part of the network must be configured to support HotSpot2.

Procedure

Step 1 Click **Wireless** > **All APs** to open the All APs page.

Step 2 Click the **AP Name** link to configure the HotSpot parameters on the desired access point. The AP Details page appears.

Step 3 Under the General Tab, configure the following parameters:

- **Venue Group**—The venue category that this access point belongs to. The following options are available:
  - **Unspecified**
  - **Assembly**
  - **Business**
  - **Educational**
  - **Factory and Industrial**
  - **Institutional**
  - **Mercantile**
  - **Residential**
  - **Storage**
  - **Utility and Misc**
  - **Vehicular**
  - **Outdoor**
- **Venue Type**—Depending on the venue category selected above, the venue type drop-down list displays options for the venue type.

- **Venue Name**—Venue name that you can provide to the access point. This name is associated with the BSS. This is used in cases where the SSID does not provide enough information about the venue.
- **Language**—The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (For example, eng for English).

Step 4 Click **Apply**.

Configuring Access Points for HotSpot2 (CLI)

- **config ap venue add** *venue-name venue-group venue-type lang-code ap-name*–Adds the venue details to the access point indicating support for HotSpot2.

  The values are as follows:

  - *venue-name*—Name of the venue where this access point is located.
  - *venue-group*—Category of the venue. See the following table.
  - *venue-type*—Type of the venue. Depending on the venue-group chosen, select the venue type. See the following table.
  - *lang-code*—The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (For example: eng for English)
  - *ap-name*—Access point name.

Tip Press the **tab** key after entering a keyword or argument to get a list of valid values for the command.

- **config ap venue delete** *ap-name*—Deletes the venue related information from the access point.

Table 1: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	

Venue Group Name	Value	Venue Type for Group
ASSEMBLY	1	• 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 4—AMPHITHEATER • 5—AMUSEMENT PARK • 6—PLACE OF WORSHIP • 7—CONVENTION CENTER • 8—LIBRARY • 9—MUSEUM • 10—RESTAURANT • 11—THEATER • 12—BAR • 13—COFFEE SHOP • 14—ZOO OR AQUARIUM • 15—EMERGENCY COORDINATION CENTER
BUSINESS	2	• 0—UNSPECIFIED BUSINESS • 1—DOCTOR OR DENTIST OFFICE • 2—BANK • 3—FIRE STATION • 4—POLICE STATION • 6—POST OFFICE • 7—PROFESSIONAL OFFICE • 8—RESEARCH AND DEVELOPMENT FACILITY • 9—ATTORNEY OFFICE
EDUCATIONAL	3	• 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE

Venue Group Name	Value	Venue Type for Group
FACTORY-INDUSTRIAL	4	• 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY
INSTITUTIONAL	5	• 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL
MERCANTILE	6	• 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION
RESIDENTIAL	7	• 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE
STORAGE	8	UNSPECIFIED STORAGE
UTILITY-MISC	9	0—UNSPECIFIED UTILITY AND MISCELLANEOUS

Venue Group Name	Value	Venue Type for Group
VEHICULAR	10	• 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE
OUTDOOR	11	• 0—UNSPECIFIED OUTDOOR • 1—MUNI-MESH NETWORK • 2—CITY PARK • 3—REST AREA • 4—TRAFFIC CONTROL • 5—BUS STOP • 6—KIOSK

Downloading the Icon File (CLI)

You can configure unique icons of the service providers to be displayed on the client devices. You can download these icon files to the controller for the icon files to be sent through a gas message and displayed on the client devices. This feature enhances the user interface on the client devices wherein users can differentiate between service providers based on the icons displayed.

Procedure

Step 1 Save the icon file on an TFTP, SFTP, or an FTP server.

Step 2 Download the icon file to the controller by entering these commands:

a) **transfer download datatype icon**

b) **transfer download start**

Configuring ICONs

Note The character '?' is not supported in the command values.

- To download an icon from the TFTP server or FTP server into the controller, enter this command:

  configure icon parameters

- To configure icon parameters, enter this command:

  config icons file-info *filename file-type lang-code width height*

- To delete an icon from flash, enter this command:

  config icons delete {*filename* | **all**}

- To display icon parameters, enter this command:

  show icons summary

This section contains the following subsections:

Downloading an ICON File (GUI)

Procedure

Step 1 Copy the **ICON** file to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.

The **Download File to Controller** window is displayed.

Step 3 From the **File Type** drop-down list, choose ICON.

Step 4 From the **Transfer Mode** drop-down list, choose from one of the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 5 In the **IP Address** field, enter the IP address of the server type you chose in Step 4. If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times the TFTP server can attempt to download the certificate in the Maximum Retries field, and the amount of time (in seconds) that the TFTP server can attempt to download the certificate in the **Timeout** field.

Step 7 In the **File Path** field, enter the directory path of the icon file.

Step 8 In the **File Name** field, enter the name of the icon file.

Step 9 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log in to the FTP server.

b) In the **Server Login Password** field, enter the password to log in to the FTP server.

c) In the **Server Port Number** field, enter the port number in the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the login ICON file to the controller.

A message is displayed indicating the status of the download.

Step 11 Click **Apply**.

Configuring an ICON (GUI)

Procedure

Step 1 Choose **Controller** > **Icons**.

The **Icon Configuration** window is displayed.

Step 2 In the **Filename** field, enter the filename for the icon.

Step 3 In the **File Type** field, enter the file type of the icon.

Step 4 In the **Lang Code** field, enter the language code.

Step 5 In the **Width** field, enter the width of the icon.

Step 6 In the **Height** field, enter the height of the icon.

Step 7 Click **Add**.

Step 8 Click **Apply**.

Configuring OSEN Support (CLI)

Note The character '?' is not supported in the command values.

- To enable or disable OSEN on a given WLAN, enter this command:

  config wlan security wpa osen {**enable** | **disable**} *wlan-id*

- To display OSEN details on a given WLAN, enter this command:

  show wlan *wlan-id*

This section contains the following subsection:

Configuring OSEN Details (GUI)

Procedure

Step 1 Choose **WLAN** to open the **WLANs** window.

Step 2 Click the WLAN ID to open the Edit page pertaining to the selected WLAN.

Step 3 Click the **Security** tab and then the **Layer 2** tab.

Step 4 From the **Layer 2 Security** drop-down list, choose **WPA+WPA2**.

Step 5 Under **WPA+WPA2 Parameters**, check the **OSEN Policy** check box to enable OSEN.

Step 6 Check the **OSEN Encryption** check box to enable OSEN encryption, and check the **TKIP** check box to enable TKIP.

Step 7 Click **Apply**.

Configuring OSU (CLI)



Note The character '?' is not supported in the command values.

- To configure an (OSU) Service Set Identifier (SSID) name, enter this command:

  config wlan hotspot hs2 osu legacy-ssid {**wlan-id** | **ssid-name**}

- To create an OSU service provider name, enter this command:

  config wlan hotspot hs2 osu sp create *wlan-id osu-index lang-code ascii/hex friendly-name*[*description*]

  The following options are available:

  - *wlan-id*—The WLAN ID on which you want to configure the operator-name.
  - *osu-index*—The osu index of the operator. The range is 1 to 32.
  - *lang-code*—The language used.
  - *ascii/hex*—.
  - *friendly-name*—The name of the 802.11an operator.
  - *description*—The language used.

- To delete an OSU service provider, enter this command:

  config wlan hotspot hs2 osu sp delete *wlan-id osu-index lang-code*

- To configure a domain ID, enter this command:

  config wlan hotspot hs2 domain-id {**wland** | **domain-id**}

- To create an OSU URL, enter this command:

  config wlan hotspot hs2 osu sp uri add *wlan-id osu-index uri*

- To delete an OSU URL, enter this command:

  config wlan hotspot hs2 osu sp uri delete *wlan-id osu-index*

- To configure an OSU method list, enter this command:

  config wlan hotspot hs2 osu sp method add *wlan-id osu-index method-pri* [*method-sec*]

- To delete an OSU method list, enter this command:

config wlan hotspot hs2 osu sp method delete *wlan-id osu-index method*

- To configure an OSU icon file on a given WLAN, enter this command:

  config wlan hotspot hs2 osu sp icon-file add *wlan-id osu-index icon-filename*

Note Yous should first configure icon parameters using the **config icon** *icon-filename* command.

- To delete an OSU icon file from a given WLAN, enter this command:

  config wlan hotspot hs2 osu sp icon-file delete *wlan-id osu-index icon-filename*

- To configure an OSU NAI, enter this command:

  config wlan hotspot hs2 osu sp nai add *wlan-id osu-index nai*

- To delete an OSU NAI, enter this command:

  config wlan hotspot hs2 osu sp nai delete *wlan-id osu-index*

- To display the OSU details configured on a given WLAN, enter this command:

  show wlan *wlan-id*

Configuring OSU Details (GUI)

Procedure

Step 1 Choose **WLAN**.

It opens the WLANs window.

Step 2 Hover your mouse over the blue drop-down arrow corresponding to the desired WLAN on which you want to configure the OSU parameters and choose **802.11u**.

The **802.11u Parameters** window appears.

Step 3 In the **WLAN > 802.11u Parameters** window, enable 802.11u.

Step 4 In the Service Provider Name field, enter the name of the service provider.

The **OSU Index** field displays the OSU index that you are editing.

The **Language Code** field displays the language code associated with the OSU Index.

Step 5 In the **Description** field, enter the description for the OSU.

Step 6 In the **URI** field, enter the URI details.

Step 7 In the **NAI** field, enter the NAI details.

Step 8 In the **Icon Filename** field, enter the filename for the icon associated with the service provider.

Step 9 From the **Method** drop-down list, choose the association method.

Step 10 Click **Apply**.

Configuring WAN Metrics



Note The character '?' is not supported in the command values.

- To configure downlink WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics downlink *wlan-id dlink-speed dlink-load*

- To configure uplink WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics uplink *wlan-id ulink-speed ulink-load*

- To configure the link status of WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics link-status *wlan-id link-status*

- To configure the load measurement duration WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics lmd *wlan-id ilmd-val*

CMX Cloud Connector

Cisco CMX Cloud Connector is a Software-as-a-Service (SaaS) product aimed to provide in-venue analytics which seamlessly integrates with the Cisco wireless infrastructure. This product provides secured guest-access solutions to visitors through custom portal. To list some of the features of Cisco CMX Cloud, it analyzes guest activity to provide better engagement, and track assets.

The Cisco CMX Cloud Connector comprises the following packages:

- Cisco CMX Connect
- Cisco CMX Connect with Cisco CMX Presence Analytics

Cisco CMX Connect provides a customizable, seamless, location-aware guest-captive portal that on-boards customers with free Wi-Fi internet access.

Cisco CMX Presence Analytics is a comprehensive analytics and engagement platform that detects the presence of visitors through their mobile devices, using Cisco access points. It eliminates the need for maps, thus enabling faster deployment, easy-to-use and quicker insights.

Cisco CMX Presence Analytics provides customer insights to customer-facing enterprises like retail, hospitality, education, sports, and entertainment, healthcare, airport sectors, and so on. This caters to the needs of businesses with smaller sites and wireless deployments that are not designed for location accuracy.

The incoming connections from Mobility Service Engine (MSE) or CMX to controller are restricted to four TCP/TLS connections. One outgoing HTTPS connection is used to connect controller to CMX cloud, with the controller acting as HTTPs client. The controller uses the preinstalled GeoTrust CA certificate to authenticate CMX Cloud server.

In the controller, when an HTTP proxy server is configured, it can send the NMSP data over this proxy server to the CMX Cloud as the fifth data consumer.

When multiple MSE or CMX devices are used, we recommend you to distribute the subscriptions for services like client measurements, Intrusion Detection System (IDS), RFID, and so on, across different NMSP connections.

As an example, four NMSP connections are distributed among the following services:

- WIPS Server
- Client and Rogues
- RFID
- Halo Traffic Control

The NMSP protocol is used to export the following data from controller to CMX server:

- Client Information
- Client RSSI measurements
- Client traffic stats
- RFID Tag information and measurements
- AP Radio information
- Rogue AP
- Client information
- RSSI measurements

This section contains the following subsections:

Prerequisites for CMX Cloud Connector

- You must have a CMX account at http://www.cmxcisco.com.
- Configure the DNS name in the controller.

  For more information, see https://support.cmxcisco.com/hc/en-us.
- Configure the IP address of the DNS server on the controller to allow it to resolve the configured cloud URL.

Restrictions for CMX Cloud Connector

- Incoming TCP/TLS connections from MSE are limited to four to reduce duplication of NMSP data.
- One CMX cloud URL can be configured in a controller.
- wIPS service is not supported on HTTPS connection.

Configuring CMX Cloud Connector (GUI)

Configure the CMX cloud server in a controller.



Note To change either the ID token or the URL, you need to disable the CMX service, update the fields, and enable the service.

Procedure

Step 1 Choose **Management** > **Cloud Services** > **CMX**.
Step 2 Set the Service Status as **Disabled**.
Step 3 Click **Apply**.
Step 4 Choose **Cloud Services** > **Server**.
Step 5 Enter the server URL in the **URL** box.
Step 6 Enter the **ID-Token** in the Id-token box.
Step 7 Click **Apply**.
Step 8 Choose **Cloud Services** > **CMX**.
Step 9 Set the Service Status as **Enabled**.
Step 10 Click **Apply**

Configuring CMX Cloud Connector (CLI)

Procedure

Step 1 Configure the CMX Cloud Services by entering this command:
config cloud-services cmx {**enabled | disabled**}

Note
To apply any changes that are made to the cloud URL or dependant configurations, disable and re-enable the CMX cloud-service. The following are the dependent configurations:

- Cloud URL
- Cloud Id-token
- DNS server IP
- HTTP proxy

Step 2 Configure the Cloud Server URL by entering this command:
config cloud-services server url *url*

Step 3 Configure the Cloud Server Id-Token by entering this command:
config cloud-services server id-token *id-token*

Step 4 View CMX Cloud Services summary by entering this command:
show cloud-services cmx summary

Step 5 View the CMX cloud services statistics by entering this command:
show cloud-services cmx statistics

Step 6 View the status of active NMSP connections by entering this command:
show nmsp status

Step 7 View the mobility services summary by entering this command:
show nmsp subscription summary

Installing CMX-Serv CA Certificate on a Controller (CLI)

Procedure

Step 1 Download the CMX server CA certificate by entering this command:
transfer download datatype cmx-serv-ca-cert

Step 2 Specify the transfer mode that is used to download the config file by entering this command:
transfer download mode {**ftp** | **tftp**| **http**| **stftp**}

Step 3 Specify the name of the certificate file to be downloaded by entering this command:
transfer download filename*cert-file-name*

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 5 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note
The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 6 Begin the certificate transfer by entering this command:
transfer download start

Enter **Y** to confirm upload.

Step 7 Reboot the device by entering this command:

reset system