Cisco Webex Wireless Phone 840 and 860
Wireless LAN Deployment Guide

The Cisco Webex Wireless Phone 840 and 860 provide a mobile collaboration platform that allows users to manage tasks and communication easily. The Cisco Webex Wireless Phone 840 and 860 offer the power and performance of a secure, enterprise-grade smartphone, while delivering an easy-to-manage device through Cisco’s collaboration solution. With the flexibility of Wi-Fi, the Cisco Webex Wireless Phone 840 and 860 enable personnel to be productive no matter where they are physically located in the enterprise. The Cisco Webex Wireless Phone 840 is IP65 rated, which is designed to provide protection from dust, liquid splashes, and moisture, where the Cisco Webex Wireless Phone 860 is IP68 rated for complete dust and water protection.

This guide provides information and guidance to help the network administrator deploy the Cisco Webex Wireless Phone 840 and 860 in a wireless LAN environment.
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/08/21</td>
<td>1.1(0) Release</td>
</tr>
<tr>
<td>03/30/21</td>
<td>1.2(0) Release</td>
</tr>
<tr>
<td>08/30/21</td>
<td>1.3(0) Release</td>
</tr>
</tbody>
</table>
Cisco Webex Wireless Phone 840 and 860 Overview

The Cisco Webex Wireless Phone 840 and 860 are the platforms that provide collaboration within enterprises. It brings together the capabilities of Cisco Unified Communication applications, building upon the solid foundations of Cisco Unified Communications devices, both wired and wireless.

Cisco’s implementation of 802.11 permits time sensitive applications such as voice to operate efficiently across campus wide wireless LAN (WLAN) deployments. These extensions provide fast roaming capabilities and an almost seamless flow of multimedia traffic, whilst maintaining security as the end user roams between access points.

It should be understood that WLAN uses unlicensed spectrum, and as a result it may experience interference from other devices using the unlicensed spectrum. The proliferation of devices in the 2.4 GHz spectrum, such as Bluetooth headsets, Microwave ovens, cordless consumer phones, means that the 2.4 GHz spectrum may contain more congestion than other spectrums. The 5 GHz spectrum has far fewer devices operating in this spectrum and is the preferred spectrum to operate the Cisco Webex Wireless Phone 840 and 860 in order to take advantage of the 802.11a/n/ac data rates available.

Despite the optimizations that Cisco has implemented in the Cisco Webex Wireless Phone 840 and 860, the use of unlicensed spectrum means that uninterrupted communication can not be guaranteed, and there may be the possibility of voice gaps of up to several seconds during conversations. Adherence to these deployment guidelines will reduce the likelihood of these voice gaps being present, but there is always this possibility.

Through the use of unlicensed spectrum, and the inability to guarantee the delivery of messages to a WLAN device, the Cisco Webex Wireless Phone 840 and 860 are not intended to be used as a medical device and should not be used to make clinical decisions.

Phone Models

The following Cisco Webex Wireless Phone 840 and 860 models are available.

Below outlines the peak antenna gain and frequency ranges / channels supported by each model.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Peak Antenna Gain</th>
<th>Frequency Ranges</th>
<th>Available Channels</th>
<th>Channel Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-840</td>
<td>Cisco Webex Wireless Phone 840</td>
<td>2.4 GHz = 1.7 dBi</td>
<td>2.412 - 2.472 GHz</td>
<td>13</td>
<td>1-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 GHz = 1.8 dBi</td>
<td>5.180 - 5.240 GHz</td>
<td>4</td>
<td>36,40,44,48</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.260 - 5.320 GHz</td>
<td>4</td>
<td>52,56,60,64</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.500 - 5.720 GHz</td>
<td>12</td>
<td>100-144</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.745 - 5.825 GHz</td>
<td>5</td>
<td>149,153,157,161,165</td>
</tr>
<tr>
<td>CP-840S</td>
<td>Cisco Webex Wireless Phone 840S</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(with barcode scanner)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-860</td>
<td>Cisco Webex Wireless Phone 860</td>
<td>2.4 GHz = 0.6 dBi</td>
<td>2.412 - 2.472 GHz</td>
<td>13</td>
<td>1-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 GHz = 0.8 dBi</td>
<td>5.180 - 5.240 GHz</td>
<td>4</td>
<td>36,40,44,48</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.260 - 5.320 GHz</td>
<td>4</td>
<td>52,56,60,64</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.500 - 5.720 GHz</td>
<td>12</td>
<td>100-144</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.745 - 5.825 GHz</td>
<td>5</td>
<td>149,153,157,161,165</td>
</tr>
<tr>
<td>CP-860S</td>
<td>Cisco Webex Wireless Phone 860S</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(with barcode scanner)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Actual channels utilized is dependent on local regulatory restrictions.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Requirements

The Cisco Webex Wireless Phone 840 and 860 are IEEE 802.11a/b/g/n/ac devices that provide voice communications. The environment must be validated to ensure it meets the requirements to deploy the Cisco Webex Wireless Phone 840 and 860.

Site Survey

Before deploying the Cisco Webex Wireless Phone 840 and 860 into a production environment, a site survey must be completed by a Cisco certified partner with the advanced wireless LAN specialization. During the site survey the RF spectrum can be analyzed to determine which channels are usable in the desired band (5 GHz or 2.4 GHz). Typically, there is less interference in the 5 GHz band as well as more non-overlapping channels, so 5 GHz is the preferred band for operation and even more highly recommended when the Cisco Webex Wireless Phone 840 and 860 are to be used in a mission critical environment. The site survey will include heatmaps showing the intended coverage plan for the location. The site survey will also determine which access point platform type, antenna type, access point configuration (channel and transmit power) to use at the location. It is recommended to select an access point with integrated antennas for non-rugged environments (e.g. office, healthcare, education, hospitality) and an access point platform requiring external antennas for rugged environments (e.g. manufacturing, warehouse, retail).

The wireless LAN must be validated to ensure it meets the requirements to deploy the Cisco Webex Wireless Phone 840 and 860.

Signal
The cell edge should be designed to -67 dBm where there is a 20-30% overlap of adjacent access points at that signal level.

This ensures that the Cisco Webex Wireless Phone 840 and 860 always have adequate signal and can hold a signal long enough in order to roam seamlessly where signal based triggers are utilized vs. packet loss triggers.

Also need to ensure that the upstream signal from the Cisco Webex Wireless Phone 840 and 860 meets the access point’s receiver sensitivity for the transmitted data rate. Rule of thumb is to ensure that the received signal at the access point is -67 dBm or higher.

It is recommended to design the cell size to ensure that the Cisco Webex Wireless Phone 840 and 860 can hold a signal for at least 5 seconds.

Channel Utilization
Channel Utilization levels should be kept under 40%.

Noise
Noise levels should not exceed -92 dBm, which allows for a Signal to Noise Ratio (SNR) of 25 dB where a -67 dBm signal should be maintained.

Also need to ensure that the upstream signal from the Cisco Webex Wireless Phone 840 and 860 meets the access point’s signal to noise ratio for the transmitted data rate.

Packet Loss / Delay
Per voice guidelines, packet loss should not exceed 1% packet loss; otherwise voice quality can be degraded significantly.

Jitter should be kept at a minimal (< 100 ms).
Retries
802.11 retransmissions should be less than 20%.

Multipath
Multipath should be kept to a minimal as this can create nulls and reduce signal levels.

Call Control
The Cisco Webex Wireless Phone 840 and 860 are supported on the following call control platforms.

- Cisco Unified Communications Manager (CUCM)
  Minimum = 11.5(1)
  Recommended = 12.5(1) and later

Note: Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable Cisco Webex Wireless Phone 840 and 860 device support.

Device packages for Cisco Unified Communications Manager are available at the following location.
https://software.cisco.com/download/home/278875240

Wireless LAN
The Cisco Webex Wireless Phone 840 and 860 are supported on the following Cisco Wireless LAN solutions.

- Cisco AireOS Wireless LAN Controller and Cisco Lightweight Access Points
  Minimum = 8.3.143.0
  Recommended = 8.3.150.0, 8.5.171.0, 8.8.130.0, 8.10.151.0

- Cisco Catalyst IOS XE Wireless LAN Controller and Cisco Lightweight Access Points
  Minimum = 16.12.1s
  Recommended = 16.12.5, 17.3.3, 17.5.1

- Cisco Mobility Express and Cisco Lightweight Access Points
  Minimum = 8.3.143.0
  Recommended = 8.3.150.0, 8.5.171.0, 8.8.130.0, 8.10.151.0

- Cisco Autonomous Access Points
  Minimum = 15.2(4)JB6
  Recommended = 15.3(3)JPK1

- Cisco Meraki Access Points
  Minimum = MR 25.9, MX 13.33
  Recommended = MR 27.6, MX 15.42.1

Access Points
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Below are the Cisco access points that are supported. Any access point model that is not listed below is not supported.

The Cisco Webex Wireless Phone 840 and 860 are supported on the following Cisco Aironet access point platforms.
The table below lists the modes that are supported by each Cisco Aironet access point.

<table>
<thead>
<tr>
<th>Cisco AP Series</th>
<th>802.11a</th>
<th>802.11b</th>
<th>802.11g</th>
<th>802.11n</th>
<th>802.11ac</th>
<th>802.11ax</th>
<th>Lightweight</th>
<th>Mobility Express</th>
<th>Autonomous</th>
</tr>
</thead>
<tbody>
<tr>
<td>1540</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1570</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1700</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1810</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1810W</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1815</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes (not 1815t)</td>
<td>No</td>
</tr>
<tr>
<td>1830</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1840</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1850</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>2700</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2800</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>3700</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>3800</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>4800</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>9105</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9115</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9117</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9120</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9124</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
The Cisco Webex Wireless Phone 840 and 860 are supported on the following Cisco Meraki access point platforms.

<table>
<thead>
<tr>
<th>9130</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>No</th>
<th>No</th>
</tr>
</thead>
</table>

MR20  
MR30H  
MR32  
MR33  
MR34  
MR36  
MR42  
MR44  
MR45  
MR46  
MR52  
MR53  
MR55  
MR56
The table below lists the modes that are supported by each Cisco Meraki access point.
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

https://meraki.cisco.com/products/wireless#models
https://meraki.cisco.com/products/appliances#models
<table>
<thead>
<tr>
<th>Meraki AP Series</th>
<th>802.11a</th>
<th>802.11b</th>
<th>802.11g</th>
<th>802.11n</th>
<th>802.11ac</th>
<th>802.11ax</th>
</tr>
</thead>
<tbody>
<tr>
<td>MR20</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR30H</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR33</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR34</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR36</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MR42</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR44</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MR45</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MR46</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MR52</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR53</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR55</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MR56</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MR70</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR74</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR76</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MR84</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MR86</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MX64W</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MX65W</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MX67W</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MX68W</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Z3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** If an access point model is not specifically listed above, then it is not supported.
Support for Cisco Aironet 1500 Series outdoor access points is limited to local access point mode only.
No support for any access point model operating in MESH mode.
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Interoperability with third-party access points can not be guaranteed as there are no interoperability tests performed for third-party access points; however if connected to a Wi-Fi compliant access point, then should have basic functionality.

Some of the key features are the following:

- 5 GHz (802.11a/n/ac)
- Wi-Fi Protected Access v2 (WPA2+AES)
- Wi-Fi Multimedia (WMM)
- Traffic Specification (TSPEC)
- Differentiated Services Code Point (DSCP)
- Class of Service (CoS / 802.1p)

**Antenna Systems**

Some Cisco access points require or allow external antennas. Please refer to the following URL for the list of supported antennas for Cisco Aironet access points and how these external antennas should be mounted.


**Note:** Cisco access points with integrated internal antennas (other than models intended to be wall mounted) are to be mounted on the ceiling as they have omni-directional antennas and are not designed to be wall mounted.

**Protocols**

Supported voice and wireless LAN protocols include the following:

- 802.11a,b,d,e,g,h,i,n,r,ac
- Wi-Fi MultiMedia (WMM)
- Traffic Specification (TSPEC)
- Unscheduled Automatic Power Save Delivery (UAPSD)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
  - Opus, G.722, G.711, G.729
- Dynamic Host Configuration Protocol (DHCP)
- HyperText Transfer Protocol (HTTP/HTTPS)

**Wi-Fi**

The following table lists the maximum tx power and date rates per 802.11 mode utilized by Cisco Webex Wireless Phone 840 and 860.

**Cisco Webex Wireless Phone 840**

**5 GHz Specifications**
### 5 GHz - 802.11a

<table>
<thead>
<tr>
<th>Max Tx Power = 16 dBm (Depends on region)</th>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6 Mbps</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td></td>
<td>9 Mbps</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td></td>
<td>12 Mbps</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>18 Mbps</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>24 Mbps</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>36 Mbps</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>48 Mbps</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>

### 5 GHz - 802.11n (HT20)

<table>
<thead>
<tr>
<th>Max Tx Power = 16 dBm (Depends on region)</th>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td></td>
<td>14 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>21 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>29 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>43 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>58 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>65 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>72 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>14 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td></td>
<td>28 Mbps (MCS 9)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>43 Mbps (MCS 10)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>58 Mbps (MCS 11)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>87 Mbps (MCS 12)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>116 Mbps (MCS 13)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>130 Mbps (MCS 14)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>144 Mbps (MCS 15)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>

### 5 GHz - 802.11n (HT40)

<table>
<thead>
<tr>
<th>Max Tx Power = 15 dBm (Depends on region)</th>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>15 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td></td>
<td>30 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>45 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>60 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>90 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>120 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>135 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>150 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td></td>
<td>30 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td></td>
<td>60 Mbps (MCS 9)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>90 Mbps (MCS 10)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td></td>
<td>120 Mbps (MCS 11)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td></td>
<td>180 Mbps (MCS 12)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>Data Rate</td>
<td>Spatial Streams</td>
<td>Modulation</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>240 Mbps (MCS 13)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
<td></td>
</tr>
<tr>
<td>270 Mbps (MCS 14)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
<td></td>
</tr>
<tr>
<td>300 Mbps (MCS 15)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
<td></td>
</tr>
</tbody>
</table>

### 5 GHz - 802.11ac (VHT20)

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 16 dBM (Depends on region)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>14 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>21 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>29 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>43 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>58 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>65 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>72 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>87 Mbps (MCS 8)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>14 Mbps (MCS 0)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>28 Mbps (MCS 1)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>43 Mbps (MCS 2)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>58 Mbps (MCS 3)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>87 Mbps (MCS 4)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>116 Mbps (MCS 5)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>130 Mbps (MCS 6)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>144 Mbps (MCS 7)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>173 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
</tbody>
</table>

### 5 GHz - 802.11ac (VHT40)

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 15 dBM (Depends on region)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>30 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>45 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>60 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>90 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>120 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>135 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>150 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>180 Mbps (MCS 8)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>200 Mbps (MCS 9)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>30 Mbps (MCS 0)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>60 Mbps (MCS 1)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>90 Mbps (MCS 2)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>120 Mbps (MCS 3)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>180 Mbps (MCS 4)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>240 Mbps (MCS 5)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>270 Mbps (MCS 6)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>300 Mbps (MCS 7)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>
### 5 GHz - 802.11ac (VHT80)

<table>
<thead>
<tr>
<th>Data Rate (Mbps)</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>360 (MCS 8)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>400 (MCS 9)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
</tbody>
</table>

Max Tx Power = 14 dBm (Depends on region)

<table>
<thead>
<tr>
<th>Data Rate (Mbps)</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>33 (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>65 (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>98 (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>130 (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>195 (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>260 (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>293 (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>325 (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>390 (MCS 8)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>433 (MCS 9)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>65 (MCS 0)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>130 (MCS 1)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>195 (MCS 2)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>260 (MCS 3)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>390 (MCS 4)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>520 (MCS 5)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>585 (MCS 6)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>650 (MCS 7)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>780 (MCS 8)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>867 (MCS 9)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
</tbody>
</table>

### 2.4 GHz Specifications

#### 2.4 GHz - 802.11b

<table>
<thead>
<tr>
<th>Data Rate (Mbps)</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>DSSS - BPSK</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>DSSS - QPSK</td>
</tr>
<tr>
<td>5.5</td>
<td>1</td>
<td>DSSS - CCK</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>DSSS - CCK</td>
</tr>
</tbody>
</table>

Max Tx Power = 19 dBm (Depends on region)

#### 2.4 GHz - 802.11g

<table>
<thead>
<tr>
<th>Data Rate (Mbps)</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>36</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>48</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>54</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>

Max Tx Power = 18 dBm (Depends on region)
Cisco Webex Wireless Phone 860

5 GHz Specifications

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Mbps</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>9 Mbps</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>12 Mbps</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>18 Mbps</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>24 Mbps</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>36 Mbps</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>48 Mbps</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>54 Mbps</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>

Max Tx Power = 17 dBm
(Depends on region)
<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>72 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>14 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>28 Mbps (MCS 9)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>43 Mbps (MCS 10)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>58 Mbps (MCS 11)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>87 Mbps (MCS 12)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>116 Mbps (MCS 13)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>130 Mbps (MCS 14)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>144 Mbps (MCS 15)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>

**5 GHz - 802.11n (HT40)**

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 17 dBm (Depends on region)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>30 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>45 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>60 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>90 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>120 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>135 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>150 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>30 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>60 Mbps (MCS 9)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>90 Mbps (MCS 10)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>120 Mbps (MCS 11)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>180 Mbps (MCS 12)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>240 Mbps (MCS 13)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>270 Mbps (MCS 14)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>300 Mbps (MCS 15)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>

**5 GHz - 802.11ac (VHT20)**

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 17 dBm (Depends on region)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>14 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>21 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>29 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>43 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>58 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>65 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>72 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>87 Mbps (MCS 8)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>14 Mbps (MCS 0)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>28 Mbps (MCS 1)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>43 Mbps (MCS 2)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>58 Mbps (MCS 3)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>5 GHz - 802.11ac (VHT40)</td>
<td>Data Rate</td>
<td>Spatial Streams</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Max Tx Power = 17 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Depends on region)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>87 Mbps (MCS 4)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>116 Mbps (MCS 5)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>130 Mbps (MCS 6)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>144 Mbps (MCS 7)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>173 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>5 GHz - 802.11ac (VHT80)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Tx Power = 17 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Depends on region)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>30 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>45 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>60 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>90 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>120 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>135 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>150 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>180 Mbps (MCS 8)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>200 Mbps (MCS 9)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>30 Mbps (MCS 0)</td>
<td>2</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>60 Mbps (MCS 1)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>90 Mbps (MCS 2)</td>
<td>2</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>120 Mbps (MCS 3)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>180 Mbps (MCS 4)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>240 Mbps (MCS 5)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>270 Mbps (MCS 6)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>300 Mbps (MCS 7)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>360 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>400 Mbps (MCS 9)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
</tbody>
</table>
### 2.4 GHz Specifications

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>390 Mbps (MCS 4)</td>
<td>2</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>520 Mbps (MCS 5)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>585 Mbps (MCS 6)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>650 Mbps (MCS 7)</td>
<td>2</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>780 Mbps (MCS 8)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
<tr>
<td>867 Mbps (MCS 9)</td>
<td>2</td>
<td>OFDM - 256 QAM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5 GHz - 802.11ac (VHT160)</th>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 17 dBm (Depends on region)</td>
<td>65 Mbps (MCS 0)</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>130 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
<td></td>
</tr>
<tr>
<td>195 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
<td></td>
</tr>
<tr>
<td>260 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
<td></td>
</tr>
<tr>
<td>390 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
<td></td>
</tr>
<tr>
<td>520 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
<td></td>
</tr>
<tr>
<td>585 Mbps (MCS 6)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
<td></td>
</tr>
<tr>
<td>650 Mbps (MCS 7)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
<td></td>
</tr>
<tr>
<td>780 Mbps (MCS 8)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
<td></td>
</tr>
<tr>
<td>867 Mbps (MCS 9)</td>
<td>1</td>
<td>OFDM - 256 QAM</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4 GHz - 802.11b

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 19 dBm (Depends on region)</td>
<td>1 Mbps</td>
<td>1</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>1</td>
<td>DSSS - QPSK</td>
</tr>
<tr>
<td>5.5 Mbps</td>
<td>1</td>
<td>DSSS - CCK</td>
</tr>
<tr>
<td>11 Mbps</td>
<td>1</td>
<td>DSSS - CCK</td>
</tr>
</tbody>
</table>

### 2.4 GHz - 802.11g

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 17 dBm (Depends on region)</td>
<td>6 Mbps</td>
<td>1</td>
</tr>
<tr>
<td>9 Mbps</td>
<td>1</td>
<td>OFDM - BPSK</td>
</tr>
<tr>
<td>12 Mbps</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>18 Mbps</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>24 Mbps</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>36 Mbps</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>48 Mbps</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
<tr>
<td>54 Mbps</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>

### 2.4 GHz - 802.11n (HT20)

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Spatial Streams</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 16 dBm (Depends on region)</td>
<td>7 Mbps (MCS 0)</td>
<td>1</td>
</tr>
<tr>
<td>14 Mbps (MCS 1)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>21 Mbps (MCS 2)</td>
<td>1</td>
<td>OFDM - QPSK</td>
</tr>
<tr>
<td>29 Mbps (MCS 3)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>43 Mbps (MCS 4)</td>
<td>1</td>
<td>OFDM - 16 QAM</td>
</tr>
<tr>
<td>58 Mbps (MCS 5)</td>
<td>1</td>
<td>OFDM - 64 QAM</td>
</tr>
</tbody>
</table>
Note: To achieve 802.11n/ac connectivity, it is recommended that the Cisco Webex Wireless Phone 840 and 860 be within 100 feet of the access point.

## Regulatory

World Mode (802.11d) allows a client to be used in different regions, where the client can adapt to using the channels and transmit powers advertised by the access point in the local environment.

The Cisco Webex Wireless Phone 840 and 860 operate best when the access point is 802.11d enabled, where it can determine which channels and transmit powers to use per the local region.

Enable World Mode (802.11d) for the corresponding country where the access point is located.

Some 5 GHz channels are also used by radar technology, which requires that the 802.11 client and access point be 802.11h compliant if utilizing those radar frequencies (DFS channels). 802.11h requires 802.11d to be enabled.

The Cisco Webex Wireless Phone 840 and 860 will passively scan DFS channels first before engaging in active scans of those channels.

If 802.11d is not enabled, then the Cisco Webex Wireless Phone 840 and 860 can attempt to connect to the access point using reduced transmit power.

Below are the countries and their 802.11d codes that are supported by the Cisco Webex Wireless Phone 840 and 860.

<table>
<thead>
<tr>
<th>Country</th>
<th>65 Mbps (MCS 6)</th>
<th>72 Mbps (MCS 7)</th>
<th>14 Mbps (MCS 8)</th>
<th>28 Mbps (MCS 9)</th>
<th>43 Mbps (MCS 10)</th>
<th>58 Mbps (MCS 11)</th>
<th>87 Mbps (MCS 12)</th>
<th>116 Mbps (MCS 13)</th>
<th>130 Mbps (MCS 14)</th>
<th>144 Mbps (MCS 15)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia (AU)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Austria (AT)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Belgium (BE)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Bulgaria (BG)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Canada (CA)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Croatia (HR)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Cyprus (CY)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Czech Republic (CZ)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Denmark (DK)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Estonia (EE)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Finland (FI)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>France (FR)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Germany (DE)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Greece (GR)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Hungary (HU)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Iceland (IS)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Ireland (IE)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Italy (IT)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Latvia (LV)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Liechtenstein (LI)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Lithuania (LT)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Luxembourg (LU)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Malta (MT)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Netherlands (NL)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>New Zealand (NZ)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Norway (NO)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Portugal (PT)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Romania (RO)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Slovakia (SK)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Slovenia (SI)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Spain (ES)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Sweden (SE)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Switzerland (CH)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Turkey (TR)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>United Kingdom (GB)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>United States (US)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Note: Compliance information is available on the Cisco Product Approval Status web site at the following URL:
https://cae-cnc-prd.cisco.com/pdtcnc

Bluetooth

The Cisco Webex Wireless Phone 840 and 860 support Bluetooth technology allowing for wireless headset communications. Bluetooth enables low bandwidth wireless connections within a range of 30 feet, however it is recommended to keep the Bluetooth device within 10 feet of the Cisco Webex Wireless Phone 840 and 860.

The Bluetooth device does not need to be within direct line-of-sight of the phone, but barriers, such as walls, doors, etc. can potentially impact the quality.

Bluetooth utilizes the 2.4 GHz frequency just like 802.11b/g/n and many other devices (e.g. microwave ovens, cordless phones, etc.), so the Bluetooth quality can potentially be interfered with due to using this unlicensed frequency.

Bluetooth Profiles

The Cisco Webex Wireless Phone 840 and 860 support the following Bluetooth profiles.

- Advanced Audio Distribution Profile (A2DP)
- Attribute Profile (ATT)
- Audio/Video Remote Control Profile (AVRCP)
- Device ID Profile (DIP)
- Dial-up Networking Profile (DUN)
- File Transfer Profile (FTP)
- Generic Access Profile (GAP)
- Generic Attribute Profile (GATT)
- Generic Audio/Video Distribution Profile (GAVDP)
- Hands-Free Profile (HFP)
- Headset Profile (HSP)
- Human Interface Device Profile (HID)
- HID over GATT Profile (HOGP)
- Message Access Profile (MAP)
- Object Push Profile (OPP)
- Personal Area Networking Profile (PAN)
- Phone Book Access Profile (PBAP)
- Scan Parameters Profile (ScPP)
- Serial Port Profile (SPP)
- Service Discovery Application Profile (SDAP)
- SIM Access Profile (SAP)

Coexistence (802.11b/g/n + Bluetooth)

If using Coexistence where 802.11b/g/n and Bluetooth are used simultaneously, then there are some limitations and deployment requirements to be considered as they both utilize the 2.4 GHz frequency range.
Capacity
When using Coexistence (802.11b/g/n + Bluetooth), call capacity is reduced due to the utilization of CTS to protect the 802.11g/n and Bluetooth transmissions.

Multicast Audio
Multicast audio from Push to Talk (PTT), Music on Hold (MMOH) and other applications are not supported when using Coexistence.

Voice Quality
Depending on the current data rate configuration, CTS may be sent to protect the Bluetooth transmissions when using Coexistence.
In some environments, 6 Mbps may need to be enabled.

Note: It is recommended to use 802.11a/n/ac if using Bluetooth due to 802.11b/g/n and Bluetooth both utilizing 2.4 GHz, but also due to the above limitations.

Languages
The Cisco Webex Wireless Phone 840 and 860 currently support the following languages.

<table>
<thead>
<tr>
<th>Language</th>
<th>840 / 840S</th>
<th>Call State</th>
<th>Battery Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Danish</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dutch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finnish</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungarian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Norwegian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Russian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slovenian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Swedish</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portuguese</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Battery Life
The Cisco Webex Wireless Phone 840 has a 3040 mAh battery and the Cisco Webex Wireless Phone 860 has a 3000 mAh battery.
The Cisco Webex Wireless Phone 840 and 860 battery’s capacity will be reduced to 80% or less after 500 full charging cycles (charging from empty to full), therefore it is recommended to replace the Cisco Webex Wireless Phone 840 and 860 battery approximately every 2 years.
The Cisco Webex Wireless Phone 860 supports a hot swappable battery, where the Cisco Webex Wireless Phone 840 does not include the hot swappable battery feature.

The table below lists the maximum on call and idle times per phone model.
There are many factors that can influence actual battery life time.

**Usage**

Battery life will be reduced when the Cisco Webex Wireless Phone 840 or 860 user is on call, roaming, turning the display on, using Bluetooth, using applications, receiving messages, or navigating the menus on the phone.

**Coverage**

Ensure the Cisco Webex Wireless Phone 840 and 860 remain in a good RF coverage area and is able to maintain a constant connection to the Cisco Unified Communications Manager.

If the Cisco Webex Wireless Phone 840 or 860 user travels out of range and remains out of range for a significant duration, battery life can be reduced.

**Transmit Power**

It is recommended to utilize an access point that supports the Cisco Compatible Extensions (CCX) Dynamic Transmit Power Control (DTPC) feature. When DTPC is enabled, the access point will advertise its transmit power to all clients, where the Cisco Webex Wireless Phone 840 and 860 can then adjust its transmit power to a minimum level that is only necessary to communicate with the connected access point, therefore also reducing unnecessary noise in other areas.

**Multicast**

If the Cisco Webex Wireless Phone 840 or 860 subscribes to a multicast stream, then the Cisco Webex Wireless Phone 840 or 860 must wake up at each DTIM period to receive the multicast frames, therefore power consumption is increased.

**Power Save Protocol**

The access point must support U-APSD, which is the power save protocol that will be utilized when on call and when in idle.

### 840S and 860S Barcode Scanner

The Cisco Webex Wireless Phone 840S and 860S include a 2D barcode scanner. An Android application is required to invoke the scanner.

The Cisco Webex Wireless Phone 840S and 860S support the following barcode symbologies:

Phone Care

The Cisco Webex Wireless Phone 840 is IP65 rated, which is designed to provide protection from dust, liquid splashes, and moisture, where the Cisco Webex Wireless Phone 860 is IP68 rated for complete dust and water protection.

For standard cleaning, can use a soft, moist cloth to wipe the phone.

For thorough cleaning, it is recommended to use a hydrogen peroxide solution (up to 3%) or an isopropyl alcohol solution (up to 91%).

A bleach solution (up to 10%) can also be used; however should not be used for cleaning any metal charging contacts.

Any cleaning solution containing a higher amount than recommended above, including pure isopropanol, or an alternative alcohol-based liquid could potentially damage the phone.

Carry cases can additionally help protect the phone further and provide drop protection.

For more information, refer to the Cisco Webex Wireless Phone 840 and 860 User Guide at this URL:

Accessories

The following accessories are available for the Cisco Webex Wireless Phone 840 and 860.

- Batteries
- Phone Power Supplies
- Carry Cases
- Belt Clips
- Desktop Chargers
- Multichargers
- Lanyard (840 only)
- Scanner Handle (840 only)

840 Chargers
For more information, refer to the Cisco Webex Wireless Phone 840 and 860 Administration Guide or Cisco Webex Wireless Phone 840 and 860 User Guide.


**Note:** Cisco does not endorse, support, or test third-party cases or covers for the Cisco Webex Wireless Phone 840 or 860. Using the Cisco Webex Wireless Phone 840 or 860 with third-party cases or covers may void the warranty.

**Wireless LAN Design**

The following network design guidelines must be followed in order to accommodate for adequate coverage, call capacity and seamless roaming for the Cisco Webex Wireless Phone 840 and 860.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
802.11 Network

Use the following guidelines to assist with deploying and configuring the wireless LAN.

5 GHz (802.11a/n/ac)

5 GHz is the recommended frequency band to utilize for operation of the Cisco Webex Wireless Phone 840 and 860.

In general, it is recommended for access points to utilize automatic channel selection instead of manually assigning channels to access points.

If there is an intermittent interferer, then the access point or access points serving that area may need to have a channel statically assigned.

The Cisco Webex Wireless Phone 840 and 860 support Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.260 - 5.720 GHz, which are 16 of the 25 possible channels.

Need to ensure there is at least 20 percent overlap with adjacent channels when deploying the Cisco Webex Wireless Phone 840 and 860 in an 802.11a/n/ac environment, which allows for seamless roaming. For critical areas, it is recommended to increase the overlap (30% or more) to ensure that there can be at least 2 access points available with -67 dBm or better, while the Cisco Webex Wireless Phone 840 and 860 also meet the access point’s receiver sensitivity (required signal level for the current data rate).

<table>
<thead>
<tr>
<th>Channel ID</th>
<th>16</th>
<th>18</th>
<th>22</th>
<th>26</th>
<th>30</th>
<th>34</th>
<th>38</th>
<th>42</th>
<th>46</th>
<th>72</th>
<th>74</th>
<th>78</th>
<th>82</th>
<th>86</th>
<th>90</th>
<th>94</th>
<th>98</th>
<th>102</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center Freq. MHz</td>
<td>5180</td>
<td>5220</td>
<td>5260</td>
<td>5300</td>
<td>5340</td>
<td>5380</td>
<td>5420</td>
<td>5460</td>
<td>5500</td>
<td>5540</td>
<td>5580</td>
<td>5620</td>
<td>5660</td>
<td>5700</td>
<td>5740</td>
<td>5780</td>
<td>5820</td>
<td>5860</td>
</tr>
<tr>
<td>Band</td>
<td>UNII-1</td>
<td>UNII-2</td>
<td>UNII-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Dynamic Frequency Selection (DFS)

DFS dynamically instructs a transmitter to switch to another channel whenever radar signal is detected. If the access point detects radar, the radio on the access point goes on hold for at least 60 seconds while the access point passively scans for another usable channel.
TPC allows the client and access point to exchange information, so that the client can dynamically adjust the transmit power. The client uses only enough energy to maintain association to the access point at a given data rate. As a result, the client contributes less to adjacent cell interference, which allows for more densely deployed, high-performance wireless LANs.

If there are repeated radar events detected by the access point (just or falsely), determine if the radar signals are impacting a single channel (narrowband) or multiple channels (wideband), then potentially disable use of that channel or channels in the wireless LAN.

The presence of an access point on a non-DFS channel can help minimize voice interruptions.

In case of radar activity, have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel is available when an access point’s radio is in its hold-off period while scanning for a new usable channel.

A UNII-3 channel (5.745 - 5.825 GHz) can optionally be used if available.

Below is a sample 5 GHz wireless LAN deployment.

For 5 GHz, 25 channels are available in the Americas, 16 channels in Europe, and 19 channels in Japan.

Where UNII-3 is available, it is recommended to use UNII-1, UNII-2, and UNII-3 only to utilize a 12 channel set.

If planning to use UNII-2 extended channels (channels 100 - 144), it is recommended to disable UNII-2 (channels 52-64) on the access point to avoid having so many channels enabled.

Having many 5 GHz channels enabled in the wireless LAN can delay discovery of new access points.

2.4 GHz (802.11b/g/n)

In general, it is recommended for access points to utilize automatic channel selection instead of manually assigning channels to access points.

If there is an intermittent interferer, then the access point or access points serving that area may need to have a channel statically assigned.

In a 2.4 GHz (802.11b/g/n) environment, only non-overlapping channels must be utilized when deploying VoWLAN. Non-overlapping channels have 22 MHz of separation and are at least 5 channels apart.

There are only 3 non-overlapping channels in the 2.4 GHz frequency range (channels 1, 6, 11).
Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying the Cisco Webex Wireless Phone 840 and 860 in an 802.11b/g/n environment, which allows for seamless roaming.

Using an overlapping channel set such as 1, 5, 9, 13 is not a supported configuration.

Below is a sample 2.4 GHz wireless LAN deployment.

Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco Webex Wireless Phone 840 and 860 should always have a signal of -67 dBm or higher when using 5 GHz or 2.4 GHz, while the Cisco Webex Wireless Phone 840 and 860 also meet the access point’s receiver sensitivity required signal level for the transmitted data rate.

Ensure the Packet Error Rate (PER) is no higher than 1%.

A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal should be maintained.

It is recommended to have at least two access points on non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.

To achieve maximum capacity and throughput, the wireless LAN should be designed to 24 Mbps. Higher data rates can optionally be enabled for other applications other than voice only that can take advantage of these higher data rates.
Recommended to set the minimum data rate to 11 Mbps or 12 Mbps for 2.4 GHz (dependent upon 802.11b client support policy) and 12 Mbps for 5 GHz, which should also be the only rate configured as a mandatory / basic rate. In some environments, 6 Mbps may need to be enabled as a mandatory / basic rate. Due to the above requirements, a single channel plan should not be deployed.

When designing the placement of access points, be sure that all key areas have adequate coverage (signal). Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

Microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or other electronic equipment operating in the 2.4 GHz band will interfere with the Wireless LAN.

Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g/n. Some microwaves are shielded more than others and that shielding reduces the spread of the energy. Microwave energy can impact channel 11, and some microwaves can affect the entire frequency range (channels 1 through 11). To avoid microwave interference, select channel 1 for use with access points that are located near microwaves.

Most microwave ovens, Bluetooth, and frequency hopping devices do not have the same effect on the 5 GHz frequency. The 802.11a/n/ac technology provides more non-overlapping channels and typically lower initial RF utilization. For voice deployments, it is suggested to use 802.11a/n/ac for voice and use 802.11b/g/n for data.

However there are products that also utilize the non-licensed 5 GHz frequency (e.g. 5.8 GHz cordless phones, which can impact UNII-3 channels).
The chart below lists the attenuation levels for various materials that may exist in an environment.

<table>
<thead>
<tr>
<th>Material</th>
<th>Attenuation Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wood</td>
<td>Low</td>
</tr>
<tr>
<td>Brick</td>
<td>Medium</td>
</tr>
<tr>
<td>Concrete</td>
<td>High</td>
</tr>
<tr>
<td>Metal</td>
<td>Very High</td>
</tr>
</tbody>
</table>

Cisco Prime Infrastructure can be utilized to verify signal strength and coverage.
Data Rates

It is recommended to disable rates below 12 Mbps for 5 GHz deployments and below 12 Mbps for 2.4 GHz deployments where capacity and range are factored in for best results.

The Cisco Webex Wireless Phone 840 and 860 both have dual antennas, therefore they support up to MCS 15 data rates for 802.11n (up to 300 Mbps).

For 802.11ac, the Cisco Webex Wireless Phone 840 supports up to VHT80 MCS 9 2SS data rates (up to 867 Mbps) and the Cisco Webex Wireless Phone 860 supports up to VHT160 MCS 9 1SS (up to 867 Mbps).

Higher MCS rates can be left enabled for other 802.11n/ac clients, which are utilizing the same band frequency and utilize MIMO (multiple input / multiple output) antenna technology, which can take advantage of those higher rates.

If 802.11b clients are not allowed in the wireless network, then it is strongly recommended to disable the data rates below 12 Mbps. This will eliminate the need to send CTS frames for 802.11g/n protection as 802.11b clients can not detect these OFDM frames.

When 802.11b clients exist in the wireless network, then an 802.11b rate must be enabled and only an 802.11b rate can be configured as a mandatory / basic rate.

The recommended data rate configurations are the following:

<table>
<thead>
<tr>
<th>802.11 Mode</th>
<th>Mandatory Data Rates</th>
<th>Supported Data Rates</th>
<th>Disabled Data Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a/n/ac</td>
<td>12 Mbps</td>
<td>18-54 Mbps,</td>
<td>6, 9 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VHT MCS 0 - MCS 9 1SS,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VHT MCS 0 - MCS 9 2SS,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(VHT MCS 0 - MCS 9 3SS),</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(VHT MCS 0 - MCS 9 4SS)</td>
<td></td>
</tr>
</tbody>
</table>
For a voice only application, data rates higher than 24 Mbps can optionally be enabled or disabled, but there is no advantage from a capacity or throughput perspective and enabling these rates could potentially increase the number of retries for a data frame.

Other applications such as video may be able to benefit from having these higher data rates enabled.

To preserve high capacity and throughput, data rates of 24 Mbps and higher should be enabled.

If deploying in an environment where excessive retries may be a concern, then a limited set of the data rates can be used, where the lowest enabled rate is the mandatory / basic rate.

For rugged environments or deployments requiring maximum range, it is recommended to enable 6 Mbps as a mandatory / basic rate.

Note: Some environments may require that a lower data rate be enabled due to use of legacy clients, environmental factors or maximum range is required.

Set only the lowest data rate enabled as the single mandatory / basic rate. Multicast packets will be sent at the highest mandatory / basic data rate enabled.

Note that capacity and throughput are reduced when lower rates are enabled.

### Rugged Environments

When deploying the Cisco Webex Wireless Phone 840 and 860 in a rugged environment (e.g. manufacturing, warehouse, retail), additional tuning on top of the standard design recommendations may be necessary.

Below are the key items to focus on when deploying a wireless LAN in a rugged environment.

**Access Point and Antenna Selection**

For rugged environments, it is recommended to select an access point platform that requires external antennas. It is also important to ensure an antenna type is selected which can operate well in rugged environments.

**Access Point Placement**
It is crucial that line of sight to the access point’s antennas is maximized by minimizing any obstructions between the Cisco Webex Wireless Phone 840 or 860 and the access point. Ensure that the access point and/or antennas are not mounted behind any obstruction or on or near a metal or glass surface.

If access points with integrated internal antennas are to be used in some areas, then it is recommended to mount those access points on the ceiling as they have omni-directional antennas and are not designed to be wall mounted.

**Frequency Band**
As always, it is recommended to use 5 GHz. Use of 2.4 GHz, especially when 802.11b rates are enabled, may not work well.
For the 5 GHz channel set, it is recommended to use a 8 or 12 channel plan only; disable UNII-2 extended channels if possible.

**Data Rates**
The standard recommended data rate set may not work well if multipath is present at an elevated level.
Therefore, it is recommended to enable lower data rates (e.g. 6 Mbps) to operate better in such an environment.
If using for voice only, then data rates above 24 Mbps can be disabled to increase first transmission success. If the same band is also used for data, video or other applications, then is suggested to keep the higher data rates enabled.

**Transmit Power**
Due to the potential of elevated multipath in rugged environments, the transmit power of the access point and Cisco Webex Wireless Phone 840 and 860 should also be restricted. This is more important if planning to deploy 2.4 GHz in a rugged environment.
If using auto transmit power, the access point transmit power can be configured to use a specified range (maximum and minimum power levels) to prevent the access point from transmitting too hot as well as too weak (e.g. 5 GHz maximum of 16 dBm and minimum of 11 dBm).
The Cisco Webex Wireless Phone 840 and 860 will utilize the access point’s current transmit power setting to determine what transmit power it uses for transmitted frames when DTPC is enabled in the access point’s configuration.

**Fast Roaming**
It is recommended to utilize 802.11r / Fast Transition (FT) for fast roaming. Enabling 802.11r (FT) also reduces the number of frames in the handshake when roaming to only two frames. Reducing the number of frames during a roam, increases the chances of roam success.
When using 802.1x authentication, it is important to use the recommended EAPOL key settings.

**Quality of Service (QoS)**
Need to ensure that DSCP values are preserved throughout the wired network, so that the WMM UP tag for voice and call control frames can be set correctly.

**Beamforming**
If using Cisco 802.11n capable access points, then Beamforming (ClientLink) should be enabled, which can help with client reception.

**Multipath**
Multipath occurs when RF signals take multiple paths from a source to a destination.
A part of the signal goes to the destination while another part bounces off an obstruction, then goes on to the destination. As a result, part of the signal encounters delay and travels a longer path to the destination, which creates signal energy loss.
When the different waveforms combine, they cause distortion and affect the decoding capability of the receiver, as the signal quality is poor.
Multipath can exist in environments where there are reflective surfaces (e.g. metal, glass, etc.). Avoid mounting access points on these surfaces.
Below is a list of multipath effects:

**Data Corruption**  
Occurs when multipath is so severe that the receiver is unable to detect the transmitted information.

**Signal Nulling**  
Occurs when the reflected waves arrive exactly out of phase with the main signal and cancel the main signal completely.

**Increased Signal Amplitude**  
Occurs when the reflected waves arrive in phase with the main signal and add on to the main signal thereby increasing the signal strength.

**Decreased Signal Amplitude**  
Occurs when the reflected waves arrive out of phase to some extent with the main signal thereby reducing the signal amplitude.

Use of Orthogonal Frequency Division Multiplexing (OFDM), which is used by 802.11a/n/ac and 802.11g/n, can help to reduce issues seen in high multipath environments.

If using 802.11b in a high multipath environment, lower data rates should be used in those areas (e.g. 1 and 2 Mbps).

Use of antenna diversity can also help in such environments.

**Security**

When deploying a wireless LAN, security is essential.

The Cisco Webex Wireless Phone 840 and 860 support the following wireless security features.

**WLAN Authentication**

- WPA2 (802.1x authentication)
- WPA2-PSK (Pre-Shared key)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- EAP-TTLS (Extensible Authentication Protocol – Tunneled Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol)
- 802.11r / Fast Transition (FT)
- CCKM (Cisco Centralized Key Management)
- None

**WLAN Encryption**
- AES (Advanced Encryption Standard)

Note: WPA3 is not supported.

802.1x - SHA2 key management is not supported.

CCMP256, GCMP128, and GCMP256 encryption ciphers are not supported.

The Cisco Webex Wireless Phone 840 and 860 also support the following additional security features.
- Image authentication
- Device authentication
- File authentication
- Signaling authentication
- Media encryption (SRTP)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)
- Secure profiles
- Encrypted configuration files

**Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)**

Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) is using the TLS protocol with PKI to secure communications to the authentication server.

TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation.

A certificate is required to be installed.

EAP-TLS provides excellent security, but requires client certificate management.

EAP-TLS may also require a user account to be created on the authentication server matching the common name of the certificate imported into the Cisco Webex Wireless Phone 840 or 860.

It is recommended to use a complex password for this user account and that EAP-TLS is the only EAP type enabled on the RADIUS server.


Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends Transport Layer Security (TLS).

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
EAP-TTLS requires that a user account be created on the authentication server.
The authentication server can be validated via importing a certificate into the Cisco Webex Wireless Phone 840 and 860.

**Protected Extensible Authentication Protocol (PEAP)**

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping. PEAP-NONE, PEAP-GTC and PEAP-MSCHAPv2 are supported inner authentication protocols. PEAP requires that a user account be created on the authentication server. The authentication server can be validated via importing a certificate into the Cisco Webex Wireless Phone 840 and 860.

**Quality of Service (QoS)**

Quality of Service enables queuing to ensure high priority for voice traffic. To enable proper queuing for voice and call control traffic use the following guidelines.

- Ensure that **WMM** is enabled on the access point.
- Create a QoS policy on the access point giving priority to voice and call control traffic.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>DSCP</th>
<th>802.1p</th>
<th>WMM UP</th>
<th>Port Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF (46)</td>
<td>5</td>
<td>6</td>
<td>UDP 16384 - 32767</td>
</tr>
<tr>
<td>Call Control</td>
<td>CS3 (24)</td>
<td>3</td>
<td>4</td>
<td>TCP 5060 - 5061</td>
</tr>
</tbody>
</table>

- Be sure that voice and call control packets have the proper QoS markings and other protocols are not using the same QoS markings.
- Enable Differentiated Services Code Point (DSCP) preservation on the Cisco IOS switch.

For more information about TCP and UDP ports used by the Cisco Webex Wireless Phone 840 and 860 and the Cisco Unified Communications Manager, refer to the Cisco Unified Communications Manager TCP and UDP Port Usage document at this URL:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/10_5_x/cucm_b_port-usage-cucm-105x/cucm_b_port-usage-cucm-105x_chapter_00.html

**Call Admission Control (CAC)**

Call Admission Control can be enabled on the access point.

- Enable Call Admission Control (CAC) / Wi-Fi MultiMedia Traffic Specifications (TSPEC) for Voice
- Set the desired maximum RF bandwidth that is allocated for voice traffic (default = 75%)
• Set the bandwidth that is reserved for roaming voice clients (default = 6%)

Pre-Call Admission Control
If Call Admission Control is enabled on the access point, the Cisco Webex Wireless Phone 840 and 860 will send an Add Traffic Stream (ADDTS) to the access point to request bandwidth in order to place or receive a call.
If the AP sends an ADDTS successful message, then the Cisco Webex Wireless Phone 840 or 860 establishes the call.
If the access point rejects the call and the Cisco Webex Wireless Phone 840 or 860 has no other access point to roam to, then the phone will display *Network Busy*.
If the admission is refused for an inbound call there is no messaging from the Cisco Webex Wireless Phone 840 or 860 to inform the remote endpoint that there is insufficient bandwidth to establish the call, so the call can continue to ring out within the system until the remote user terminates the call.

Roaming Admission Control
During a call, the Cisco Webex Wireless Phone 840 and 860 measure Received Signal Strength Indicator (RSSI) and Packet Error Rate (PER) values for the current and all available access points to make roaming decisions.
If the original access point where the call was established had Call Admission Control enabled, then the Cisco Webex Wireless Phone 840 and 860 will send an ADDTS request during the roam to the new access point, which embedded in the reassociation request frame.

Wired QoS
Configure QoS settings and policies for the necessary network devices.

Configuring Cisco Switch Ports for WLAN Devices
Configure the Cisco Wireless LAN Controller and Cisco Access Point switch ports as well as any uplink switch ports.

If utilizing Cisco IOS Switches, use the following switch port configurations.

Enable COS trust for Cisco Wireless LAN Controller

```bash
mls qos
!
interface X
mls qos trust cos
```

Enable DSCP trust for Cisco Access Points

```bash
mls qos
!
interface X
mls qos trust dscp
```
If utilizing Cisco Meraki MS Switches, reference the Cisco Meraki MS Switch VoIP Deployment Guide.

**Note:** When using the Cisco Wireless LAN Controller, DSCP trust must be implemented or must trust the UDP data ports used by the Cisco Wireless LAN Controller (CAPWAP = UDP 5246 and 5247) on all interfaces where wireless packets will traverse to ensure QoS markings are correctly set.

### Configuring Cisco Switch Ports for Wired IP Phones

Enable the Cisco wired IP phone switch ports for Cisco phone trust.

Below is a sample switch configuration:

```plaintext
mls qos
!
Interface X
  mls qos trust device cisco-phone
  mls qos trust dscp
```

### Roaming

The Cisco Webex Wireless Phone 840 and 860 default to Auto for the 802.11 mode, which allows the Cisco Webex Wireless Phone 840 and 860 to connect to either 5 GHz or 2.4 GHz and enables interband roaming support.

802.11r / Fast Transition (FT) is the recommended deployment model for all environment types where frequent roaming occurs. 802.1x authentication is required in order to utilize CCKM.

802.1x without 802.11r (FT) or CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA2 introduces additional transient keys and can lengthen roaming time.

When 802.11r (FT) or CCKM is utilized, roaming times can be reduced to less than 100 ms, where that transition time from one access point to another will not be audible to the user.

The Cisco Webex Wireless Phone 840 and 860 support 802.11r (FT) with WPA2 (AES) or WPA2-PSK (AES) and CCKM with WPA2 (AES).

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Roaming Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2 Personal</td>
<td>150 ms</td>
</tr>
<tr>
<td>WPA2 Enterprise</td>
<td>300 ms</td>
</tr>
<tr>
<td>802.11r (FT)</td>
<td>&lt; 100 ms</td>
</tr>
<tr>
<td>CCKM</td>
<td>&lt; 100 ms</td>
</tr>
</tbody>
</table>

The Cisco Webex Wireless Phone 840 and 860 manage the scanning and roaming events.
The roaming trigger for the majority of roams should be due to meeting the required RSSI differential based on the current RSSI, which results in seamless roaming (no voice interruptions).

For seamless roaming to occur, the Cisco Webex Wireless Phone 840 and 860 must be associated to an access point for at least 3 seconds, otherwise roams can occur based on packet loss (max tx retransmissions or missed beacons).

**Fast Secure Roaming (FSR)**

802.11r / Fast Transition (FT) is the recommended deployment model for all environment types where frequent roaming occurs. Cisco Centralized Key Management (CCKM) is also supported, but requires 802.1x authentication.

802.11r (FT) and CCKM enable fast secure roaming and limits the off-network time to keep audio gaps at a minimum when on call.

802.1x or PSK without 802.11r (FT) and 802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA2 introduces additional transient keys and can lengthen roaming time.

802.11r (FT) and CCKM centralizes the key management and reduces the number of key exchanges.

When 802.11r (FT) or CCKM is utilized, roaming times can be reduced from 400-500 ms to less than 100 ms, where that transition time from one access point to another will not be audible to the user.

There are two methods of 802.11r (FT) roaming.

**Over the Air**

The client communicates directly with the target access point using 802.11 authentication with the FT authentication algorithm.

**Over the Distribution**

The client communicates with the target access point through the current access point. The communication between the client and the target access point is carried in FT action frames between the client and the current access point via the WLAN controller.

802.11r (FT) utilizing the Over the Air method is the recommended fast secure roaming model to deploy.

Since the 802.11r (FT) plus Over the Distribution method requires connectivity to the currently associated access point, this method may not work well if the phone is not always able to communicate with the current access point as well as the target access point, which could occur in non-open environments if line of sight to both the current access point and the target access point can not be retained when a roaming event occurs.

The Cisco Webex Wireless Phone 840 and 860 support 802.11r (FT) with WPA2-PSK or WPA2 and CCKM with WPA2 or WPA.

<table>
<thead>
<tr>
<th>FSR Type</th>
<th>Authentication</th>
<th>Key Management</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11r (FT)</td>
<td>PSK</td>
<td>WPA2</td>
<td>AES</td>
</tr>
<tr>
<td>802.11r (FT)</td>
<td>EAP-TLS</td>
<td>WPA2</td>
<td>AES</td>
</tr>
<tr>
<td>802.11r (FT)</td>
<td>EAP-TTLS</td>
<td>WPA2</td>
<td>AES</td>
</tr>
</tbody>
</table>
### Interband Roaming

The Cisco Webex Wireless Phone 840 and 860 default to Auto for the frequency band mode, which enables interband roaming and currently gives preference to the strongest signal. Typically, this will give preference to 2.4 GHz over 5 GHz due to 2.4 GHz having a stronger signal in general assuming the power levels are the same.

At power on, the Cisco Webex Wireless Phone 840 and 860 will scan all 2.4 and 5 GHz channels when in Auto mode, then attempt to associate to an access point for the configured network if available.

If configured for 5 GHz only or 2.4 GHz only mode, then just those channels are scanned.

It is recommended to perform a spectrum analysis to ensure that the desired bands can be enabled in order to perform interband roaming.

### Power Management

The Cisco Webex Wireless Phone 840 and 860 will utilize U-APSD power save method depending on whether Wi-Fi MultiMedia (WMM) is enabled in the Access Point configuration or not.

The Cisco Webex Wireless Phone 840 and 860 primarily use U-APSD when in idle or on call.

Null Power Save (PS-NULL) frames are utilized for off-channel scanning.

### Delivery Traffic Indicator Message (DTIM)

The Cisco Webex Wireless Phone 840 and 860 can use the DTIM period to schedule wakeup periods to check for broadcast and multicast packets as well as any unicast packets.

It is recommended to set the DTIM period to 2 with a beacon period of **100 ms**.

Broadcast and multicast traffic will be queued until the DTIM period when there are power save enabled clients associated to the access point, so DTIM will determine how quickly these packets can be delivered to the client. If using multicast applications, a shorter DTIM period can be used.

When multiple multicast streams exist on the wireless LAN frequently, then it is recommended to set the DTIM period to 1.

### Dynamic Transmit Power Control (DTPC)

To ensure packets are exchanged successfully between the Cisco Webex Wireless Phone 840 or 860 and the access point, Dynamic Transmit Power Control (DTPC) should be enabled.
DTPC prevents one-way audio when RF traffic is heard in one direction only.

If the access point does not support DTPC, then the Cisco Webex Wireless Phone 840 and 860 will use the highest available transmit power depending on the current channel and data rate.

The access point’s radio transmit power should not have a transmit power greater than what the Cisco Webex Wireless Phone 840 and 860 can support.

**Call Capacity**

Design the network to accommodate the desired call capacity.

The Cisco access point can support up to 27 bi-directional voice streams for both 802.11a/n/ac and 802.11g/n at a data rate of 24 Mbps or higher. To achieve this capacity, there must be minimal wireless LAN background traffic and initial radio frequency (RF) utilization.

The number of calls may vary depending on the data rate, initial channel utilization, and the environment.

**Audio Calls**

Below lists the maximum number of audio calls (single bi-directional voice stream) supported per access point / channel.

<table>
<thead>
<tr>
<th>Max # of Audio Calls</th>
<th>802.11 Mode</th>
<th>Audio Codec</th>
<th>Audio Bit Rate</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>5 GHz or 2.4 GHz</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>6 Mbps</td>
</tr>
<tr>
<td>20</td>
<td>5 GHz or 2.4 GHz</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>12 Mbps</td>
</tr>
<tr>
<td>27</td>
<td>5 GHz or 2.4 GHz</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>24 Mbps or higher</td>
</tr>
</tbody>
</table>

**Multicast**

When enabling multicast in the wireless LAN, performance and capacity must be considered.

If there is an associated client that is in power save mode, then all multicast packets will be queued until the DTIM period.

With multicast, there is no guarantee that the packet will be received by the client.

The multicast traffic will be sent at the highest mandatory / basic data rate enabled on the access point, so will want to ensure that only the lowest enabled rate is configured as the only mandatory / basic rate.

The client will send the IGMP join request to receive that multicast stream. The client will send the IGMP leave when the session is to be ended.

The Cisco Webex Wireless Phone 840 and 860 support the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure that IGMP snooping is also enabled on all switches.

**Note:** If using Coexistence where 802.11b/g/n and Bluetooth are being used simultaneously, then multicast voice is not supported.
Configuring the Cisco Wireless LAN

Cisco AireOS Wireless LAN Controller and Lightweight Access Points

When configuring the Cisco Wireless LAN Controller and Lightweight Access Points, use the following guidelines:

- Ensure 802.11r (FT) or CCKM is Enabled
- Set Quality of Service (QoS) to Platinum
- Set the WMM Policy to Required
- Ensure Session Timeout is enabled and configured correctly
- Ensure Broadcast Key Interval is enabled and configured correctly
- Ensure Aironet IE is Enabled
- Set DTPC Support to Enabled
- Disable P2P (Peer to Peer) Blocking Action
- Ensure Client Exclusion is configured correctly
- Disable DHCP Address Assignment Required
- Set Protected Management Frame (PMF) to Optional or Disabled
- Set MFP Client Protection to Optional or Disabled
- Set the DTIM Period to 2
- Set Client Load Balancing to Disabled
- Set Client Band Select to Disabled
- Set IGMP Snooping to Enabled
- Enable Symmetric Mobile Tunneling Mode if Layer 3 mobility is utilized
- Enable ClientLink if utilizing Cisco 802.11n capable Access Points
- Configure the Data Rates as necessary
- Configure Auto RF as necessary
- Set Admission Control Mandatory for Voice to Enabled
- Set Load Based CAC for Voice to Enabled
- Enable Traffic Stream Metrics for Voice
- Set Admission Control Mandatory for Video to Disabled
- Set EDCA Profile to Voice Optimized or Voice and Video Optimized
- Set Enable Low Latency MAC to Disabled
- Ensure that Power Constraint is Disabled
- Enable Channel Announcement and Channel Quiet Mode
- Configure the High Throughput Data Rates as necessary
- Configure the Frame Aggregation settings
- Enable CleanAir if utilizing Cisco access points with CleanAir technology
- Configure Multicast Direct Feature as necessary
- Set the 802.1p tag to 5 for the Platinum QoS profile
**802.11 Network Settings**

It is recommended to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

If wanting to use 5 GHz, ensure the 802.11a/n/ac network status is **Enabled**.

Set the **Beacon Period** to **100 ms**.

Ensure **DTPC Support** is enabled.

If using Cisco 802.11n capable Access Points, ensure **ClientLink** is enabled.

**Maximum Allowed Clients** can be configured as necessary.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

---

If wanting to use 2.4 GHz, ensure the 802.11b/g/n network status and 802.11g are **Enabled**.

Set the **Beacon Period** to **100 ms**.

**Short Preamble** should be **Enabled** in the 2.4 GHz radio configuration setting on the access point when no legacy clients that require a long preamble are present in the wireless LAN. By using the short preamble instead of long preamble, the wireless network performance is improved.

Ensure **DTPC Support** is enabled.

If using Cisco 802.11n capable Access Points, ensure **ClientLink** is enabled.

**Maximum Allowed Clients** can be configured as necessary.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12 Mbps and higher as supported (optional).
Beamforming (ClientLink)

Enable ClientLink if using Cisco 802.11n capable Access Points.

Use the following commands to enable the beamforming feature globally for all access points or for individual access point radios.

(Cisco Controller) >config 802.11a beamforming global enable  
(Cisco Controller) >config 802.11a beamforming ap <ap_name> enable  
(Cisco Controller) >config 802.11b beamforming global enable  
(Cisco Controller) >config 802.11b beamforming ap <ap_name> enable

The current status of the beamforming feature can be displayed by using the following command.

(Cisco Controller) >show 802.11a  
(Cisco Controller) >show 802.11b

Legacy Tx Beamforming setting.................... Enabled
Auto RF (RRM)

When using the Cisco Wireless LAN Controller it is recommended to enable Auto RF to manage the channel and transmit power settings.

Configure the access point transmit power level assignment method for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

If using automatic power level assignment, a maximum and minimum power level can be specified.
If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

It is recommended to utilize the same channel width for all access points.

If using 2.4 GHz, only channels 1, 6, and 11 should be enabled in the DCA list.

It is recommended to configure the 2.4 GHz channel for 20 MHz even if using Cisco 802.11n Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

This may be necessary if there is an intermittent interferer present in an area.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

It is recommended to use channel bonding only if using 5 GHz.

It is recommended to utilize the same channel width for all access points.
**Client Roaming**

The Cisco Webex Wireless Phone 840 and 860 do not utilize the RF parameters in the Client Roaming section of the Cisco Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

**EDCA Parameters**

Set the EDCA profile to either **Voice Optimized** or **Voice & Video Optimized** and disable **Low Latency MAC** for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

Low Latency MAC (LLM) reduces the number of retransmissions to 2-3 per packet depending on the access point platform, so it can cause issues if multiple data rates are enabled.

LLM is not supported on the Cisco 802.11n/ac Access Points.

**DFS (802.11h)**

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
**Power Constraint** should be left un-configured or set to 0 dB as DTPC will be used by the Cisco Webex Wireless Phone 840 and 860 to control the transmission power.

In later versions of the Cisco Wireless LAN Controller it does not allow both TPC (Power Constraint) and DTPC (Dynamic Transmit Power Control) to be enabled simultaneously.

**Channel Announcement** and **Channel Quiet Mode** should be **Enabled**.

### High Throughput (802.11n/ac)

The 802.11n data rates can be configured per radio (2.4 GHz and 5 GHz).

802.11ac data rates are applicable to 5 GHz only.

Ensure that **WMM** is enabled and **WPA2(AES)** is configured in order to utilize 802.11n/ac data rates.

The Cisco Webex Wireless Phone 840 and 860 support HT MCS 0 – MCS 15 and VHT MCS 0 – MCS 9 1SS and 2SS data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n/ac clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of those higher data rates.
Frame Aggregation

Frame aggregation is a process of packaging multiple MAC Protocol Data Units (MPDUs) or MAC Service Data Units (MSDUs) together to reduce the overheads where in turn throughput and capacity can be optimized.

Aggregation of MAC Protocol Data Unit (A-MPDU) requires the use of block acknowledgements.

It is required to adjust the A-MPDU and A-MSDU settings to the following to optimize the experience with the Cisco Webex Wireless Phone 840 and 860.

**A-MSDU**

User Priority 1, 2 = Enabled
User Priority 0, 3, 4, 5, 6, 7 = Disabled

**A-MPDU**

User Priority 0, 3, 4, 5 = Enabled
User Priority 1, 2, 6, 7 = Disabled

Use the following commands to configure the A-MPDU and A-MSDU settings per the Cisco Webex Wireless Phone 840 and 860 requirements.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
In order to configure the 5 GHz settings, the 802.11a network will need to be disabled first, then re-enabled after the changes are complete.

```
Config 802.11a 11nSupport a-msdu tx priority 1 enable
config 802.11a 11nSupport a-msdu tx priority 2 enable
config 802.11a 11nSupport a-msdu tx priority 0 disable
config 802.11a 11nSupport a-msdu tx priority 3 disable
config 802.11a 11nSupport a-msdu tx priority 4 disable
config 802.11a 11nSupport a-msdu tx priority 5 disable
config 802.11a 11nSupport a-msdu tx priority 6 disable
config 802.11a 11nSupport a-msdu tx priority 7 disable
config 802.11a 11nSupport a-mpdu tx priority 0 enable
config 802.11a 11nSupport a-mpdu tx priority 3 enable
config 802.11a 11nSupport a-mpdu tx priority 4 enable
config 802.11a 11nSupport a-mpdu tx priority 5 enable
config 802.11a 11nSupport a-mpdu tx priority 1 disable
config 802.11a 11nSupport a-mpdu tx priority 2 disable
```

In order to configure the 2.4 GHz settings, the 802.11b/g network will need to be disabled first, then re-enabled after the changes are complete.

```
Config 802.11b 11nSupport a-msdu tx priority 1 enable
config 802.11b 11nSupport a-msdu tx priority 2 enable
config 802.11b 11nSupport a-msdu tx priority 0 disable
config 802.11b 11nSupport a-msdu tx priority 3 disable
config 802.11b 11nSupport a-msdu tx priority 4 disable
config 802.11b 11nSupport a-msdu tx priority 5 disable
config 802.11b 11nSupport a-msdu tx priority 6 disable
config 802.11b 11nSupport a-msdu tx priority 7 disable
config 802.11b 11nSupport a-mpdu tx priority 0 enable
config 802.11b 11nSupport a-mpdu tx priority 3 enable
config 802.11b 11nSupport a-mpdu tx priority 4 enable
config 802.11b 11nSupport a-mpdu tx priority 5 enable
config 802.11b 11nSupport a-mpdu tx priority 1 disable
config 802.11b 11nSupport a-mpdu tx priority 2 disable
```
To view the current A-MPDU and A-MSDU configuration, enter either `show 802.11a` for 5 GHz or `show 802.11b` for 2.4 GHz.

### 802.11n Status:

**A-MSDU Tx:**
- Priority 0: Disabled
- Priority 1: Enabled
- Priority 2: Enabled
- Priority 3: Disabled
- Priority 4: Disabled
- Priority 5: Disabled
- Priority 6: Disabled
- Priority 7: Disabled

**A-MPDU Tx:**
- Priority 0: Enabled
- Priority 1: Disabled
- Priority 2: Disabled
- Priority 3: Enabled
- Priority 4: Enabled
- Priority 5: Enabled
- Priority 6: Disabled
- Priority 7: Disabled

### CleanAir

**CleanAir** should be **Enabled** when utilizing Cisco access points with CleanAir technology in order to detect any existing interferers.
CleanAir/Spectrum Intelligence Parameters

- CleanAir
- Spectrum Intelligence
- Report Interferers
- Persistent Device Propagation

Interferences to Ignore:
- Canopy
- WiMax Fixed
- 51 FHSS

Interferences to Detect:
- TDD Transmitter
- Jammer
- Continuous Transmitter
- DECT-like Phone
- Video Camera

Trap Configurations

- Enable AQI (Air Quality Index) Trap
- AQI Alarm Threshold (1 to 100)
- Enable trap for Undeclassified Interferences
- Threshold for Undeclassified category trap (1 to 99)
- Enable trap for Classified Interferences
- Threshold for Classified category trap (1 to 99)
- Enable Interference For Security Alarm

Do not trap on these types:
- TDD Transmitter
- Continuous Transmitter
- DECT-like Phone
- Video Camera
- SuperAG

Trap on these types:
- Jammer
- WiFi Inverted
- WiFi Invalid Channel

Event Driven RRM (Change Settings)

- EDRRM
- Sensitivity Threshold (N/A)
- Rogue Contribution (N/A)
- Rogue Duty-Cycle (N/A)

(1) Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled.
(2) AQI value 100 is best and 1 is worst
(3) Spectrum Intelligence does not send traps to Prime Infrastructure and CMX
Rx Sop Threshold

It is recommended to use the default value for Rx Sop Threshold.

WLAN Settings

It is recommended to have a separate SSID for the Cisco Webex Wireless Phone 840 and 860. However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

The SSID to be used by the Cisco Webex Wireless Phone 840 and 860 can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

It is recommended to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.
Ensure that the selected SSID is not utilized by any other wireless LANs as that could lead to failures when powering on or during roaming; especially if a different security type is utilized.

To utilize 802.11r (FT) for fast secure roaming, check the box to enable Fast Transition.

Is recommended to uncheck Over the DS to utilize the Over the Air method instead of the Over the Distribution System method.

**Protected Management Frame** should be set to **Optional** or **Disabled**.

Enable WPA2 policy with AES encryption then either FT 802.1x or FT PSK for authenticated key management type depending on whether 802.1x or PSK is to be utilized.
### Layer 2 Security
- **WPA/WPA2**
- **Security Type**
- **MAC Filtering**

### WPA+PA2 Parameters
- **WPA Policy**
- **WPA2 Policy**
- **WPA2 Encryption**
- **CCMP128 (AES)**
- **TKIP**
- **CCMP256**
- **Mixed Mode**
- **Fast Transition**
- **Fast Transition**
- **Over the DS**
- **Reassociation Timeout**

### Protected Management Frame
- **PMF**
- **Authentication Key Management**
- **802.1X-SHA1**
- **802.1X-SHA2**
- **FT 802.1X**
- **CCKM**

### WPA GTK-randomize State
- **Disabled**

---

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
To utilize CCKM for fast secure roaming, enable WPA2 policy with AES encryption and CCKM for authenticated key management type.
802.1x, CCKM and/or PSK may also be enabled if wanting to utilize the same SSID for various type of voice clients, where some clients do not support 802.11r (FT) depending on whether 802.1x or PSK is being utilized.

RADIUS Authentication and Account Servers can be configured at a per SSID level to override the global list.

If **Enabled** and not specified (set to **None**), then the global list of RADIUS servers defined at **Security > AAA > RADIUS** will be utilized.

EAP parameters can be configured at a per SSID level or at the global level, except for the EAP-Broadcast Key Interval, which can only be configured at the global level.

If wanting to configure the EAP parameters at the per SSID level, check **Enable** in the EAP Parameters section and enter the desired values.
The WMM policy should be set to **Required** only if the Cisco Webex Wireless Phone 840 and 860 or other WMM enabled phones will be using this SSID.

If there are non-WMM clients existing in the WLAN, it is recommended to put those clients on another WLAN.

If non-other WMM clients must utilize the same SSID as the Cisco Webex Wireless Phone 840 and 860, then ensure the WMM policy is set to **Allowed**.

Enabling WMM will enable the 802.11e version of QBSS.
Configure **Enable Session Timeout** as necessary per your requirements. It is recommended to enable the session timeout for 86400 seconds to avoid possible interruptions during audio calls, but also to re-validate client credentials periodically to ensure that the client is using valid credentials.

Enable Aironet Extensions (**Aironet IE**).

**Peer to Peer (P2P) Blocking Action** should be disabled.

Configure **Client Exclusion** as necessary.

The **Maximum Allowed Clients Per AP Radio** can be configured as necessary.

**Off Channel Scanning Defer** can be tuned to defer scanning for certain queues as well as the scan defer time.

If using best effort applications frequently or if DSCP values for priority applications (e.g. voice and call control) are not preserved to the access point, then it is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well as potentially increasing the scan defer time.

For deployments where EAP failures occur frequently, it is recommended to enable priority queue 7 to defer off channel scanning during EAP exchanges.

**DHCP Address Assignment Required** should be disabled.

**Management Frame Protection** should be set to **Optional** or **Disabled**.

Use a **DTIM Period** of 2 with a beacon period of **100 ms**.

Ensure **Client Load Balancing** and **Client Band Select** are disabled.

It is recommended to set **Re-anchor Roamed Voice Clients** to disabled as this can cause brief interruptions with wireless LAN connectivity when a call is terminated after performing an inter-controller roaming.
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

WLANs > Edit 'voice'

General | Security | QoS | Policy-Mapping | Advanced
---|---|---|---|---
Allow AAA Override | Enabled | | | 
Coverage Hole Detection | Enabled | | | 
Enable Session Timeout | Enabled | | | 
Aironet IE | Enabled | | | 
Diagnostic Channel | Enabled | | | 
Override Interface ACL | IPv4: None, IPv6: None | | | 
Layer 2 ACL | None | | | 
P2P Blocking Action | Enabled | | | 
Client Exclusion | Enabled | | | 
Maximum Allowed Clients | 0 | | | 
Static IP Tunneling | Enabled | | | 
Wi-Fi Direct Clients Policy | Disabled | | | 
Maximum Allowed Clients over AR BwCtrl. | 200 | | | 

DHCP
- DHCP Server: Override
- DHCP Addr. Assignment: Required
- Management Frame Protection (MFP)
- MFP Client Protection: Optional
- DTIM Period (in beacon intervals)
- 802.11a/n (1 - 255): 2
- 802.11b/g (1 - 255): 2
- NAC
- NAC State: None
- Load Balancing and Band Select
  - Client Load Balancing
  - Client Band Select

WLANs > Edit 'voice'

General | Security | QoS | Policy-Mapping | Advanced
---|---|---|---|---
Privacy Client
- Passive Client
- Voice
- Media Session Snooping
- Re-anchor Roamed Voice Clients
- KTS based QCI Policy
- Realtime Client Profiling
- DHCP Profiling
- HTTP Profiling
- Local Client Profiling
- DHCP Profiling
- HTTP Profiling
- PMIP
- PMIP Mobility Type
- PMIP NAI Type: unconfigured

WLANs > Edit 'voice'

General | Security | QoS | Policy-Mapping | Advanced
---|---|---|---|---
FlexConnect Local Auth L2 | Enabled | | | 
Learn Client IP Address | Enabled | | | 
VLAN based Central Switching | Enabled | | | 
Central DHCP Processing | Enabled | | | 
 override DNS | Enabled | | | 
RAT-MAP | Enabled | | | 
Central AAI | Enabled | | | 
Lync
- Sync Server: Enabled

11g
- Neighbor list
- Neighbor list Dual Band
- Neighboring BSS Prediction Optimization
- 802.11ax RM Configuration
- Down Link MU-MIMO | Enabled | | | 

PMIPv6
- PMIP Realign
- Universal AP Admin Support
- 802.11ax Transition Support
- BSS Transition
- Disassociation Vici
- Disassociation Time interval
- BSS Max Lifespan
- BSS Max Lifespan:
- Multicast Support
- Tunneling
- Tunneling Profile
- CODEC VLAN Override
- mDNS
- rDNS Snooping | Enabled | | |
AP Groups

AP Groups can be created to specify which WLANs / SSIDs are to be enabled and which interface they should be mapped to as well as what RF Profile parameters should be used for the access points assigned to the AP Group.

On the WLANs tab, select the desired SSIDs and interfaces to map to then select Add.
On the **RF Profile** tab, select the desired 802.11a or 802.11b RF Profile, then select **Apply**.

If changes are made after access points have joined the AP Group, then those access points will reboot once those changes are made.

On the **APs** tab, select the desired access points then select **Add APs**.

Those access points will then reboot.

### Controller Settings

Ensure the Cisco Wireless LAN Controller hostname is configured correctly.

Enable Link Aggregation (LAG) if utilizing multiple ports on the Cisco Wireless LAN Controller.

Configure the desired AP multicast mode.
If utilizing multicast, then **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be enabled.

If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling should be Enabled**. In the recent versions, Symmetric Mobility Tunneling is enabled by default and non-configurable.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
When multiple Cisco Wireless LAN Controllers are to be in the same mobility group, then the IP address and MAC address of each Cisco Wireless LAN Controller should be added to the Static Mobility Group Members configuration.

**Call Admission Control (CAC)**

It is recommended to enable **Admission Control Mandatory** for Voice and configure the maximum bandwidth and reserved roaming bandwidth percentages for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

The maximum bandwidth default setting for voice is **75%** where **6%** of that bandwidth is reserved for roaming clients.

Roaming clients are not limited to using the reserved roaming bandwidth, but roaming bandwidth is to reserve some bandwidth for roaming clients in case all other bandwidth is utilized.

If CAC is to be enabled, will want to ensure **Load-based CAC** is enabled.

**Load-based CAC** will account for all energy on the channel.
Admission Control Mandatory for Video should be disabled.
If Call Admission Control for voice is enabled, then the following configuration should be active, which can be displayed in the `show run-config`.

```
Call Admission Control (CAC) configuration
Voice AC – Admission control (ACM)........ Enabled
Voice max RF bandwidth..................... 75
Voice reserved roaming bandwidth......... 6
Voice load-based CAC mode............... Enabled
Voice tspec inactivity timeout......... Disabled
Video AC – Admission control (ACM)........ Disabled
Voice Stream-Size.......................... 84000
Voice Max-Streams.......................... 2
Video max RF bandwidth..................... 25
Video reserved roaming bandwidth......... 6
```

The voice stream-size and voice max-streams values can be adjusted as necessary by using the following command.
If using SRTP, the Voice Stream-Size may need to be increased.

```
(Cisco Controller) >config 802.11a cac voice stream-size 84000 max-streams 2
```

Ensure QoS is setup correctly under the WLAN configuration, which can be displayed by using the following command.

```
(Cisco Controller) >show wlan <WLAN id>
```
Quality of Service.......................... Platinum (voice)
WMM........................................ Allowed
Dot11-Phone Mode (7920).................. ap-cac-limit
Wired Protocol............................. 802.1P (Tag=5)

Ensure Voice TSPEC Inactivity Timeout is disabled.

(Cisco Controller) > config 802.11a cac voice tspec-inactivity-timeout ignore
(Cisco Controller) > config 802.11b cac voice tspec-inactivity-timeout ignore

In the Media settings, **Unicast Video Redirect** and **Multicast Direct Enable** should be enabled.

### RF Profiles

RF Profiles can be created to specify which frequency bands, data rates, RRM settings, etc. a group of access points should use. It is recommended to have the SSID used by the Cisco Webex Wireless Phone 840 and 860 to be applied to 5 GHz radios only. RF Profiles are applied to an AP group once created.
When creating an RF Profile, the **RF Profile Name** and **Radio Policy** must be defined. Select 802.11a or 802.11b/g for the **Radio Policy**.

On the **802.11** tab, configure the data rates as desired. It is recommended to enable 12 Mbps as **Mandatory** and 18 Mbps and higher as **Supported**; however, some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

On the **RRM** tab, the **Maximum Power Level Assignment** and **Minimum Power Level Assignment** settings as well as other DCA, TPC, and **Coverage Hole Detection** settings can be configured.
On the High Density tab, Maximum Clients, Multicast Data Rates, and Rx Sop Threshold can be configured. It is recommended to use the default value for Rx Sop Threshold.
**FlexConnect Groups**

All access points configured for FlexConnect mode need to be added to a FlexConnect Group.

If utilizing 802.11r (FT) or CCKM, then seamless roams can only occur when roaming to access points within the same FlexConnect Group.

The maximum number of access points allowed per FlexConnect Group is limited, which is WLC model specific.
Multicast Direct

In the Media Stream settings, **Multicast Direct feature** should be enabled.
After **Multicast Direct feature** is enabled, then there will be an option to enable **Multicast Direct** in the QoS menu of the WLAN configuration.

### QoS Profiles

Configure the four QoS profiles (Platinum, Gold, Silver, Bronze), by selecting **802.1p** as the protocol type and set the **802.1p tag** for each profile.

- Platinum = 5
- Gold = 4
- Silver = 2
- Bronze = 1
Edit QoS Profile

QoS Profile Name: platinum

Description: For Voice Applications

Per-User Bandwidth Contracts (kbps) *

<table>
<thead>
<tr>
<th></th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Per-SSID Bandwidth Contracts (kbps) *

<table>
<thead>
<tr>
<th></th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

WLAN QoS Parameters

Maximum Priority: voice
Unicast Default Priority: besteffort
Multicast Default Priority: besteffort

Wired QoS Protocol

Protocol Type: 802.1p
802.1p Tag: 5
Edit QoS Profile

QoS Profile Name: gold

Description: For Video Applications

Per-User Bandwidth Contracts (kbps) *

<table>
<thead>
<tr>
<th>Field</th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Per-SSID Bandwidth Contracts (kbps) *

<table>
<thead>
<tr>
<th>Field</th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

WLAN QoS Parameters

- Maximum Priority: video
- Unicast Default Priority: video
- Multicast Default Priority: video

Wired QoS Protocol

Protocol Type: 802.1p Tag
802.1p Tag: 4
### Edit QoS Profile

**QoS Profile Name**  
silver

**Description**  
For Best Effort

<table>
<thead>
<tr>
<th>Per-User Bandwidth Contracts (kbps) *</th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Per-SSID Bandwidth Contracts (kbps) *</th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### WLAN QoS Parameters

- **Maximum Priority**: besteffort
- **Unicast Default Priority**: besteffort
- **Multicast Default Priority**: besteffort

### Wired QoS Protocol

- **Protocol Type**: 802.1p
- **802.1p Tag**: 0
All EAP parameters can be configured at a per SSID level or at the global level, except for the EAP-Broadcast Key Interval, which can only be configured at the global level.

To view or configure the EAP parameters, select Security > Advanced EAP.
To view the EAP parameters on the Cisco Wireless LAN Controller via command line, enter the following command.

(Cisco Controller) >show advanced eap

EAP-Identity-Request Timeout (seconds)........... 30
EAP-Identity-Request Max Retries................. 2
EAP Key-Index for Dynamic WEP.................... 0
EAP Max-Login Ignore Identity Response.......... enable
EAP-Request Timeout (seconds)..................... 30
EAP-Request Max Retries........................... 2
EAPOL-Key Timeout (milliseconds).................. 400
EAPOL-Key Max Retries......................... 4
EAP-Broadcast Key Interval......................... 3600

If using 802.1x, the **EAP-Request Timeout** on the Cisco Wireless LAN Controller should be set to at least 20 seconds.
In later versions of Cisco Wireless LAN Controller software, the default **EAP-Request Timeout** was changed from 2 to 30 seconds.
For deployments where EAP failures occur frequently, the **EAP-Request Timeout** should be reduced below 30 seconds.
To change the **EAP-Request Timeout** on the Cisco Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >config advanced eap request-timeout 30

If using PSK then it is recommended to reduce the **EAPOL-Key Timeout** to 400 milliseconds from the default of 1000 milliseconds with **EAPOL-Key Max Retries** set to 4 from the default of 2.
If using 802.1x, then using the default values where the **EAPOL-Key Timeout** is set to 1000 milliseconds and **EAPOL-Key Max Retries** are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.
The **EAPOL-Key Timeout** should not exceed 1000 milliseconds (1 second).

To change the **EAPOL-Key Timeout** on the Cisco Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >config advanced eap eapol-key-timeout 400

To change the **EAPOL-Key Max Retries Timeout** on the Cisco Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >config advanced eap eapol-key-retries 4

Ensure **EAP-Broadcast Key Interval** is set to a minimum of 3600 seconds (1 hour).
To change the **EAP-Broadcast Key Interval** on the Cisco Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >config advanced eap bcast-key-interval 3600
Auto-Immune

The Auto-Immune feature can optionally be enabled for protection against denial of service (DoS) attacks. Although when this feature is enabled there can be interruptions introduced with voice over wireless LAN, therefore it is recommended to disable the Auto-Immune feature on the Cisco Wireless LAN Controller.

To view the Auto-Immune configuration on the Cisco Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >show wps summary

Auto-Immune
Auto-Immune................................ Disabled

Client Exclusion Policy
Excessive 802.11-association failures......... Enabled
Excessive 802.11-authentication failures....... Enabled
Excessive 802.1x-authentication............... Enabled
IP-theft......................................... Enabled
Excessive Web authentication failure......... Enabled

Signature Policy
Signature Processing.......................... Enabled

To disable the Auto-Immune feature on the Cisco Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >config wps auto-immune disable

CCKM Timestamp Tolerance

The default CCKM timestamp tolerance is set to 1000 ms. It is recommended to adjust the CCKM timestamp tolerance to 5000 ms to optimize the Cisco Webex Wireless Phone 840 and 860 roaming experience.

(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance ?
<tolerance> Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds; Default tolerance 1000 msecs

Use the following command to configure the CCKM timestamp tolerance per Cisco recommendations.
To confirm the change, enter `show wlan <WLAN id>`, where the following will be displayed.

```
CCKM tsf Tolerance ........................................ 5000
```

**Rogue Policies**

It is recommended to use the default value (**Disable**) for **Rogue Location Discovery Protocol**.

---

**Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points**

When configuring the Cisco Wireless LAN Controller and Lightweight Access Points, use the following guidelines:

- Ensure **802.11r (FT)** or **CCKM** is **Enabled**
- Set **Quality of Service (QoS) SSID Policy** to **Platinum**
- Set the **WMM Policy** to **Required**
- Ensure **Session Timeout** is enabled and configured correctly

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Ensure **Broadcast Key Interval** is enabled and configured correctly
Ensure **Aironet IE** is **Enabled**
Set **DTPC Support** to **Enabled**
Disable **P2P (Peer to Peer) Blocking Action**
Ensure **Client Exclusion Timeout** is configured correctly
Disable **DHCP Required**
Set **Protected Management Frame (PMF)** to **Optional** or **Disabled**
Set the **DTIM Period** to **2**
Set **Load Balance** to **Disabled**
Set **Band Select** to **Disabled**
Set **IGMP Snooping** to **Enabled**
Configure the **Data Rates** as necessary
Configure **RRM** as necessary
Set **Admission Control Mandatory for Voice** to **Enabled**
Set **Load Based CAC for Voice** to **Enabled**
Enable **Traffic Stream Metrics for Voice**
Set **EDCA Profile** to **Voice Optimized** or **Voice and Video Optimized**
Ensure that **Power Constraint** is **Disabled**
Enable **Channel Switch Status** and **Smart DFS**
Set **Channel Switch Announcement Mode** to **Quiet**
Configure the **High Throughput** data rates as necessary
Enable **CleanAir**
Enable **Multicast Direct Enable**

**802.11 Network Settings**

It is recommended to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

If wanting to use 5 GHz, ensure the 5 GHz network status is **Enabled**.
Set the **Beacon Period** to **100 ms**.
Ensure **DTPC Support** is enabled.
Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.
If wanting to use 2.4 GHz, ensure the 2.4 GHz network status and 802.11g network status are **Enabled**.

Set the **Beacon Period** to **100 ms**.

**Short Preamble** should be **Enabled** in the 2.4 GHz radio configuration setting on the access point when no legacy clients that require a long preamble are present in the wireless LAN. By using the short preamble instead of long preamble, the wireless network performance is improved.

Ensure **DTPC Support** is enabled.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12 Mbps and higher as supported (optional).
High Throughput (802.11n/ac)

The 802.11n data rates can be configured per radio (2.4 GHz and 5 GHz).

802.11ac data rates are applicable to 5 GHz only.

Ensure that **WMM** is enabled and **WPA2(AES)** is configured in order to utilize 802.11n/ac data rates.

The Cisco Webex Wireless Phone 840 and 860 support HT MCS 0 – MCS 15 and VHT MCS 0 – MCS 9 1SS and 2SS data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n/ac clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of those higher data rates.
Parameters

In the EDCA Parameters section, set the EDCA profile to **Optimized-voice** or **Optimized-video-voice** for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

In the DFS (802.11h) section, **Power Constraint** should be left un-configured or set to 0 dB as DTPC will be used by the Cisco Webex Wireless Phone 840 and 860 to control the transmission power.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Channel Switch Status and Smart DFS should be Enabled.
Channel Switch Announcement Mode should be set to Quiet.

**RRM**

It is recommended to enable automatic assignment method to manage the channel and transmit power settings.

Configure the access point transmit power level assignment method for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

If using automatic power level assignment, a maximum and minimum power level can be specified.

If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

It is recommended to utilize the same channel width for all access points.

If using 2.4 GHz, only channels 1, 6, and 11 should be enabled in the channel list.
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

This may be necessary if there is an intermittent interferer present in an area.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

It is recommended to utilize the same channel width for all access points.
CleanAir

Enable CleanAir should be Enabled when utilizing Cisco access points with CleanAir technology in order to detect any existing interferers.

WLAN Settings
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
It is recommended to have a separate SSID for the Cisco Webex Wireless Phone 840 and 860. However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

The SSID to be used by the Cisco Webex Wireless Phone 840 and 860 can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

It is recommended to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

Ensure that the selected SSID is not utilized by any other wireless LANs as that could lead to failures when powering on or during roaming; especially if a different security type is utilized.

To utilize 802.11r (FT) for fast secure roaming, set **Fast Transition** to **Enabled**.

Is recommended to uncheck **Over the DS** to utilize the Over the Air method instead of the Over the Distribution System method.

**Protected Management Frame** should be set to **Optional** or **Disabled**.

Enable WPA2 policy with AES(CCMP128) encryption then either FT 802.1x or FT PSK for authenticated key management type depending on whether 802.1x or PSK is to be utilized.
802.1x, CCKM and/or PSK may also be enabled if wanting to utilize the same SSID for various type of voice clients, where some clients do not support 802.11r (FT) depending on whether 802.1x or PSK is being utilized.

To utilize CCKM for fast secure roaming, enable WPA2 policy with AES encryption and 802.1x + CCKM for authenticated key management type.

The default **CCKM Timestamp Tolerance** is set to 1000 ms.

It is recommended to adjust the **CCKM Timestamp Tolerance** to 5000 ms to optimize the Cisco Webex Wireless Phone 840 and 860 roaming experience.

![Cisco Catalyst 5800-40 Wireless Controller](image)

**Aironet IE** should be **Enabled**.

**Peer to Peer (P2P) Blocking Action** should be **Disabled**.

The **WMM Policy** should be set to **Required** only if the Cisco Webex Wireless Phone 840 and 860 or other WMM enabled phones will be using this SSID.

If there are non-WMM clients existing in the WLAN, it is recommended to put those clients on another WLAN. If non-other WMM clients must utilize the same SSID as the Cisco Webex Wireless Phone 840 and 860, then ensure the WMM policy is set to **Allowed**.

The maximum client connections per WLAN, per AP per WLAN, or per AP radio per WLAN can be configured as necessary.

**Off Channel Scanning Defer** can be tuned to defer scanning for certain queues as well as the scan defer time.

It is recommended to enabled defer priority for queues 4-6.

If using best effort applications frequently or if DSCP values for priority applications (e.g. voice and call control) are not preserved to the access point, then is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well as potentially increasing the scan defer time.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
For deployments where EAP failures occur frequently, it is recommended to enable priority queue 7 to defer off channel scanning during EAP exchanges.

Ensure **Load Balance** and **Band Select** are disabled.

Use a **DTIM Period** of 2 with a beacon period of **100 ms**.

**Policy Profiles**

Policy Profiles are used to define additional settings regarding access, QoS, Mobility, and advanced settings. Policy Profiles are then mapped to a WLAN Profile via a Policy Tag, which then can be applied to an access point.

Ensure the **Status** of the policy profile is **Enabled**.
Select the **VLAN** or **VLAN Group** to be utilized with the policy profile.
Ensure the QoS SSID Policy is set to **Platinum** for egress and **Platinum-up** for ingress.

Configure **Session Timeout** as necessary per your requirements. It is recommended to enable the session timeout for 86400 seconds to avoid possible interruptions during audio calls, but also to re-validate client credentials periodically to ensure that the client is using valid credentials.

Configure **Client Exclusion Timeout** as necessary.

**IPv4 DHCP Required** should be disabled.
RF Profiles

RF Profiles can be created to specify which frequency bands, data rates, RRM settings, and advanced settings a group of access points should use.

It is recommended to have the SSID used by the Cisco Webex Wireless Phone 840 and 860 to be applied to 5 GHz radios only.

RF Profiles are applied to an RF Tag, which then can be applied to an access point.

When creating an RF Profile, the **Name** and **Radio Band** must be defined.

Select **5 GHz Band** or **2.4 GHz Band** for the **Radio Band**.
On the 802.11 tab, configure the data rates as necessary. Is recommended to enable 12 Mbps as **Mandatory** and 18 Mbps and higher as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.
On the **RRM** tab, the **Maximum Power Level** and **Minimum Power Level** settings as well as other DCA, TPC, and Coverage settings can be configured.
On the Advanced tab, Maximum Clients, Multicast Data Rate, Rx Sop Threshold, and other advanced settings can be configured.

It is recommended to use the default value (Auto) for Rx Sop Threshold.
Flex Profiles

Flex Profiles are used to define the settings the access point should use when in Flexconnect mode. Flex Profiles are then mapped to a Site Tag, which then can be applied to an access point.

If utilizing 802.11r (FT) or CCKM, then seamless roams can only occur when roaming to access points within the same Flex Profile.

Configure the Native VLAN ID for the access point to use as well as the allowed VLANs.

Ensure ARP Caching is Enabled.

Enable Local Authentication as necessary.
Tags

**Policy Tag**

Policy Tags define the mapping of WLAN Profiles and Policy Profiles. Policy Tags are then applied to an access point to specify which WLANs / SSIDs are to be enabled, which interface they should be mapped to and which QoS and other settings to use.

When creating a Policy Tag, click Add, select the WLAN Profile to configure then select the Policy Profile to be used.
Site Tag

Site Tags define which AP Join Profile and Flex Profile should be used. Site Tags are then applied to an access point to specify which AP Join Profile and Flex Profile parameters should be used.

When creating a Site Tag, click **Add**, select the **AP Join Profile** to be used.
When creating a Site Tag to include a Flex Profile, ensure **Enable Local Site** is not checked, then select the necessary **Flex Profile**.
**RF Tag**

RF Tags define which RF Profiles should be used for 2.4 GHz and 5 GHz.

RF Tags are then applied to an access point to specify which RF Profile parameters should be used.

When creating a RF Tag, select the **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be used.

Once tags are defined, they can then be applied to an access point.
If a Site Tag is applied including a configured Flex Profile, then the AP Mode will be changed to Flex automatically.
Controller Settings

Ensure the **Default Mobility Domain** is configured correctly.

Enable AP LAG Mode.

Mobility Settings
When multiple Cisco Wireless LAN Controllers are to be in the same mobility group, then the IP address and MAC address of each Cisco Wireless LAN Controller should be added to the Mobility Peer configuration.

Ensure each Cisco Wireless LAN Controller is configured with the same Mobility Group Name.

Ensure the Mobility MAC Address matches the MAC address of the wireless management interface.

Call Admission Control (CAC)
It is recommended to enable **Admission Control Mandatory** for **Voice** and configure the maximum bandwidth and reserved roaming bandwidth percentages for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

The maximum bandwidth default setting for voice is **75%** where **6%** of that bandwidth is reserved for roaming clients.

Roaming clients are not limited to using the reserved roaming bandwidth, but roaming bandwidth is to reserve some bandwidth for roaming clients in case all other bandwidth is utilized.

If CAC is to be enabled, will want to ensure **Load Based CAC** is enabled. **Load Based CAC** will account for all energy on the channel.

The voice stream size and maximum number of voice streams values can be adjusted as necessary.

If using SRTP, the voice stream size may need to be increased.

Ensure the **Inactivity Timeout** is Disabled.

**Unicast Video Redirect** and **Multicast Direct Enable** should be **Enabled**.

**Multicast**

If utilizing multicast, then **Global Wireless Multicast Mode** and **IGMP Snooping** should be **Enabled**.
In the Media Stream settings, **Multicast Direct Enable** should be **Enabled**.

And enable **Multicast Direct** in the WLAN configuration.
Advanced Settings

Advanced EAP Settings
To view or configure the EAP parameters, select Configuration > Security > Advanced EAP.

If using 802.1x, the EAP-Request Timeout on the Cisco Wireless LAN Controller should be set to 30 seconds.
For deployments where EAP failures occur frequently, the EAP-Request Timeout should be reduced below 30 seconds.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
If using PSK then it is recommended to reduce the **EAPOL-Key Timeout** to 400 milliseconds from the default of 1000 milliseconds with **EAPOL-Key Max Retries** set to 4 from the default of 2.

If using 802.1x, then using the default values where the **EAPOL-Key Timeout** is set to 1000 milliseconds and **EAPOL-Key Max Retries** are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively. The **EAPOL-Key Timeout** should not exceed 1000 milliseconds (1 second).

Ensure **EAP-Broadcast Key Interval** is set to a minimum of 3600 seconds (1 hour).

**Rx Sop Threshold**

It is recommended to use the default value (**Auto**) for **Rx Sop Threshold**.

---

**Rogue Policies**

It is recommended to use the default value (**Disable**) for **Rogue Location Discovery Protocol**.
### Sample Configuration

```
version 16.12
service timestamps debug datet ime msec
service timestamps log datet ime msec
service password-encryption
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname RCDN6-21A-WLC5
!
boot-start-marker
boot system flash bootflash:packages.conf
boot-end-marker
!
vrf definition Mgmt-intf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
no logging console
!
aaa new-model
!
!
  aaa group server radius RADIUS_SERVER_GROUP_DAY0
  server name RADIUS_SERVER_DAY0_1
```
server name RADIUS_SERVER_DAY0_2
!
aaa authentication login default local
aaa authentication login authentication_login_day0 group RADIUS_SERVER_GROUP_DAY0
aaa authentication dot1x authentication_dot1x_day0 group RADIUS_SERVER_GROUP_DAY0
aaa authorization exec default local
aaa authorization network default local
!
aaa server radius dynamic-author
!
aaa session-id common
clock timezone CST -6 0
clock summer-time CDT recurring
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH
notifications.
Contact-email-addr sch-smart-licensing@cisco.com
profile “CiscoTAC-1”
active
destination transport-method http
no destination transport-method email
!
ip domain name cisco.com
!
login on-success log
!
subscriber templating
!
parameter-map type webauth global
  virtual-ip ipv4 1.1.1.6
!
flow exporter wireless-local-exporter
destination local wlc
!
flow monitor wireless-avc-basic
exporter wireless-local-exporter
cache timeout active 60
record wireless avc basic
!
no device-tracking logging theft
access-session mac-move deny
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-3110682001
  enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3110682001
revocation-check none
rsakeypair TP-self-signed-3110682001
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
crypto pki certificate chain TP-self-signed-3110682001
  certificate self-signed 01
license udi pid C9800-40-K9 sn TTM231803A3
memory free low-watermark processor 375973

service-template webauth-global-inactive
  inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
  linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
  linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
  diagnostic bootup level minimal

username <REMOVED> privilege 15 password 7 <REMOVED>
redundancy
  mode sso

vlan internal allocation policy ascending

class-map match-any AVC-Reanchor-Class
  match protocol cisco-jabber-audio
  match protocol cisco-jabber-video
  match protocol webex-media
  match protocol webex-app-sharing
  match protocol webex-control
  match protocol webex-meeting
  match protocol webex-meeting

interface Port-channel3
  switchport trunk native vlan 310
  switchport trunk allowed vlan 310,400,500
  switchport mode trunk

interface TenGigabitEthernet0/0/0
  switchport trunk native vlan 310
  switchport trunk allowed vlan 310,400,500
  switchport mode trunk
  no negotiation auto
  channel-group 3 mode active

interface TenGigabitEthernet0/0/1
  switchport trunk native vlan 310
  switchport trunk allowed vlan 310,400,500
  switchport mode trunk
  no negotiation auto
  channel-group 3 mode active

interface TenGigabitEthernet0/0/2
  switchport trunk native vlan 310
  switchport trunk allowed vlan 310,400,500
  switchport mode trunk
  no negotiation auto
  channel-group 3 mode active
!  
interface TenGigabitEthernet0/0/3  
switchport trunk native vlan 310  
switchport trunk allowed vlan 310,400,500  
switchport mode trunk  
no negotiation auto  
channel-group 3 mode active  
!  
interface GigabitEthernet0  
vrf forwarding Mgmt-intf  
ip address 10.201.81.25 255.255.255.240  
negotiation auto  
no cdp enable  
!  
interface Vlan1  
no ip address  
shutdown  
!  
interface Vlan310  
description Management  
ip address 10.201.81.9 255.255.255.240  
!  
interface Vlan400  
description Data  
ip address 10.201.82.14 255.255.255.0  
ip helper-address 72.163.42.112  
ip helper-address 173.37.137.70  
!  
interface Vlan500  
description Voice  
ip address 10.201.83.14 255.255.255.0  
ip helper-address 72.163.42.112  
ip helper-address 173.37.137.70  
!  
ip default-gateway 10.201.81.1  
ip forward-protocol nd  
!  
ip http server  
ip http authentication local  
ip http secure-server  
ip tftp source-interface GigabitEthernet0  
ip tftp blocksize 8192  
ip route 0.0.0.0 0.0.0.0 10.201.81.1  
!  
radius-server attribute wireless accounting mac-delimiter hyphen  
radius-server attribute wireless accounting call-station-id macaddress  
radius-server attribute wireless accounting callStationIdCase lower  
radius-server attribute wireless authentication callStationIdCase lower  
radius-server attribute wireless authentication mac-delimiter hyphen  
radius-server attribute wireless authentication call-station-id ap-macaddress-ssid  
radius-server load-balance method least-outstanding  
!  
radius server RADIUS_SERVER_DAY0_1  
address ipv4 10.42.136.30 auth-port 1812 acct-port 1813  
key 7 <REMOVED>  
!
radius server RADIUS_SERVER_DAY0_2
address ipv4 10.42.3.31 auth-port 1812 acct-port 1813
key 7 <REMOVED>
!
control-plane
!
line con 0
  exec-timeout 60 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
!
ntp server 10.81.254.202
ntp server 10.115.162.212
!
wireless mobility group member mac-address 6c31.0e7b.b8eb ip 10.201.81.10 public-ip 10.201.81.10 group CTG-VoWLAN3
wireless mobility group name CTG-VoWLAN3
wireless mobility mac-address 706d.153d.b50b
wireless cts-sxp profile default-sxp-profile
wireless management interface Vlan310
wireless profile airtime-fairness default-atf-policy 0
wireless profile flex default-flex-profile
description “default flex profile”
wireless profile mesh default-mesh-profile
description “default mesh profile”
wireless profile policy Data
  ipv4 flow monitor wireless-avc-basic input
  ipv4 flow monitor wireless-avc-basic output
  service-policy input silver-up
  service-policy output silver
  session-timeout 86400
  vlan VLAN0400
  no shutdown
wireless profile policy Voice
  ipv4 flow monitor wireless-avc-basic input
  ipv4 flow monitor wireless-avc-basic output
  service-policy input platinum-up
  service-policy output platinum
  session-timeout 86400
  vlan VLAN0500
  no shutdown
wireless profile policy default-policy-profile
  description “default policy profile”
  vlan default
wireless tag site default-site-tag
  description “default site tag”
wireless tag policy default-policy-tag
  description “default policy-tag”
  wlan Data policy Data
  wlan Voice policy Voice
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

wireless tag rf default-rf-tag
description “default RF tag”
wireless rf-network RCDN6-VoWLAN3
wireless security dot1x eapol-key retries 4
wireless security dot1x eapol-key timeout 400
no wireless security dot1x max-login-ignore-identity-response
wireless fabric control-plane default-control-plane
wireless media-stream multicast-direct
wireless multicast
wlan Data 2 data
band-select
ccx aironet-iesupport
load-balance
security dot1x authentication-list authentication_dot1x_day0
no shutdown
wlan Voice 1 voice
no assisted-roaming neighbor-list
no bss-transition
ccx aironet-iesupport
channel-scan defer-priority 4
dtim dot11 24ghz 2
dtim dot11 5ghz 2
media-stream multicast-direct
radio dot11a
security ft
security wpa akm ft dot1x
security dot1x authentication-list authentication_dot1x_day0
wmm require
no shutdown
ap dot11 24ghz rf-profile Low_Client_Density_rf_24gh
coverage data rssi threshold -90
coverage level 2
coverage voice rssi threshold -90
description “pre configured Low Client Density rfprofile for 2.4gh radio”
high-density rx-sop threshold low
tx-power v1 threshold -65
no shutdown
ap dot11 24ghz rf-profile High_Client_Density_rf_24gh
description “pre configured High Client Density rfprofile for 2.4gh radio”
high-density rx-sop threshold medium
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
tx-power min 7
no shutdown
ap dot11 24ghz rf-profile Typical_Client_Density_rf_24gh
description “pre configured Typical Client Density rfprofile for 2.4gh radio”
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
no shutdown
ap dot11 24ghz media-stream multicast-direct
ap dot11 24ghz media-stream video-redirect
no ap dot11 24ghz cac voice tspec-inactivity-timeout
ap dot11 24ghz cac voice tspec-inactivity-timeout ignore
ap dot11 24ghz cac voice acm
ap dot11 24ghz edca-parameters optimized-video-voice
ap dot11 24ghz exp-bwreq
ap dot11 24ghz tsm
ap dot11 24ghz rrm txpower max 14
ap dot11 24ghz rrm txpower min 5
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 5ghz rf-profile Low_Client_Density_rf_5gh
coverage data rssi threshold -90
coverage level 2
description “pre configured Low Client Density rfprofile for 5gh radio”
high-density rx-sop threshold low
tx-power v1 threshold -60
no shutdown
ap dot11 5ghz rf-profile High_Client_Density_rf_5gh
description “pre configured High Client Density rfprofile for 5gh radio”
high-density rx-sop threshold medium
rate RATE_6M disable
rate RATE_9M disable
tx-power min 7
tx-power v1 threshold -65
no shutdown
ap dot11 5ghz rf-profile Typical_Client_Density_rf_5gh
description “pre configured Typical Density rfprofile for 5gh radio”
no shutdown
ap dot11 5ghz media-stream multicast-direct
ap dot11 5ghz media-stream video-redirect
no ap dot11 5ghz cac voice tspec-inactivity-timeout
ap dot11 5ghz cac voice tspec-inactivity-timeout ignore
ap dot11 5ghz cac voice acm
ap dot11 5ghz exp-bwreq
ap dot11 5ghz tsm
ap dot11 5ghz edca-parameters optimized-video-voice
ap dot11 5ghz channelswitch quiet
ap dot11 5ghz rrm channel dca chan-width 40
ap dot11 5ghz rrm channel dca remove 116
ap dot11 5ghz rrm channel dca remove 120
ap dot11 5ghz rrm channel dca remove 124
ap dot11 5ghz rrm channel dca remove 128
ap dot11 5ghz rrm channel dca remove 144
ap dot11 5ghz rrm txpower max 17
ap dot11 5ghz rrm txpower min 11
ap dot11 5ghz rate RATE_24M supported
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap country US
ap lag support
ap tag-source-priority 2 source filter
ap tag-source-priority 3 source ap
ap profile default-ap-profile
capwap backup primary RCDN6-21A-WLC5 10.201.81.9
capwap backup secondary RCDN6-22A-WLC6 10.201.81.10
description “default ap profile”
hyperlocation ble-beacon 0
hyperlocation ble-beacon 1
hyperlocation ble-beacon 2
hyperlocation ble-beacon 3
hyperlocation ble-beacon 4
hyperlocation
lag
mgmtuser username <REMOVED> password 0 <REMOVED> secret 0 <REMOVED>
nntp ip 10.115.162.212
ssh
end

Cisco Mobility Express and Lightweight Access Points

When configuring Cisco Mobility Express and Lightweight Access Points, use the following guidelines:

- Ensure 802.11r (FT) or CCKM is Enabled
- Set Quality of Service (QoS) to Platinum
- Disable P2P (Peer to Peer) Blocking Action
- Set Client Band Select to Disabled
- Set Client Load Balancing to Disabled
- Configure the Data Rates as necessary
- Configure RF Optimization as necessary
- Set Traffic Type to Voice and Data
- Enable CleanAir if utilizing Cisco access points with CleanAir technology
- Configure Multicast Direct as necessary

Controller Settings

Configure one or more of the Mobility Express capable access point’s Operating Mode to include the Controller functionality. Configure the AP Name and IP settings as necessary.
Configure the Cisco Wireless LAN Controller **System Name** and IP settings as necessary.

**802.11 Network Settings**

It is recommended to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

If wanting to use 5 GHz, ensure the **5.0 GHz Band** is **Enabled**.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

If wanting to use 2.4 GHz, ensure the **2.4 GHz Band** is **Enabled**.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.
If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12 Mbps and higher as supported (optional).

If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

It is recommended to utilize the same channel width for all access points.

If using 2.4 GHz, only channels 1, 6, and 11 should be enabled in the DCA list.

**CleanAir detection** should be **Enabled** when utilizing Cisco access points with CleanAir technology in order to detect any existing interferers.

**RF Optimization**

It is recommended to enable **RF Optimization** to manage the channel and transmit power settings.

Set **Traffic Type** to **Voice and Data**.
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

This may be necessary if there is an intermittent interferer present in an area.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

It is recommended to use channel bonding only if using 5 GHz.

It is recommended to utilize the same channel width for all access points.
WLAN Settings

It is recommended to have a separate SSID for the Cisco Webex Wireless Phone 840 and 860. However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

The SSID to be used by the Cisco Webex Wireless Phone 840 and 860 can be configured to only apply to a certain 802.11 radio type (e.g. 5 GHz only).

It is recommended to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band only due to have many channels available and not as many interferers as the 2.4 GHz band has.

Ensure that the selected SSID is not utilized by any other wireless LANs as that could lead to failures when powering on or during roaming; especially if a different security type is utilized.

To utilize 802.11r (FT) for fast secure roaming, set Security Type to either WPA2Enterprise or Personal depending on whether 802.1x or PSK is to be utilized.
Set 802.11r to **Enabled** in the **Advanced** tab of the WLAN configuration.

Ensure **Client Band Select** and **Client Load Balancing** are disabled.
To utilize CCKM for fast secure roaming, set **Security Type** to **WPA2Enterprise**.

Set **CCKM** to **Enabled** in the **Advanced** tab of the WLAN configuration.

Ensure **Client Band Select** and **Client Load Balancing** are disabled.
RADIUS Authentication Servers and Account Servers can be configured at a per WLAN level to override the global list.
Configure the **Native VLAN ID** and **VLAN ID** for the WLAN as necessary. Ensure **Peer to Peer Block** is disabled.
Ensure **Platinum (Voice)** is selected for **QoS**.

The **Maximum Allowed Clients** and **Maximum Allowed Clients Per AP Radio** can be configured as necessary.
**AP Groups**

AP Groups can be created to specify which WLANs are to be enabled and which interface they should be mapped to as well as what RF Profile parameters should be used for the access points assigned to the AP Group.

On the **WLANs** tab, select the desired WLANs and interfaces to map to then select **Add**.
On the **Access Points** tab, select the desired access points then select **Apply**. Those access points will then reboot.

On the **RF Profile** tab, select the desired **2.4GHz** or **5GHz** RF Profile, then select **Apply**.
RF Profiles

RF Profiles can be created to specify which frequency bands, data rates, RRM settings, etc. a group of access points should use. It is recommended to have the SSID used by the Cisco Webex Wireless Phone 840 and 860 to be applied to 5 GHz radios only. RF Profiles are applied to an AP group once created.

When creating an RF Profile, the RF Profile Name and Radio Policy must be defined. Select 5GHz or 2.4GHz for the Radio Policy.

Maximum clients per radio, Multicast data rates, and Rx Sop Threshold can be configured as necessary.

It is recommended to use the default value (Auto) for Rx Sop Threshold.

On the 802.11 tab, configure the data rates as necessary.

Is recommended to enable 12 Mbps as Mandatory and 18 Mbps and higher as Supported; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.
On the RRM tab, the Channel Width settings and DCA Channels can be configured.

**Multicast Direct**

In the Media Stream settings, enable Global Multicast and Multicast Direct.
After Multicast Direct is enabled in the Media Stream settings, then there will be an option to enable Multicast Direct in the Advanced tab of the WLAN configuration.

Cisco Autonomous Access Points

When configuring Cisco Autonomous Access Points, use the following guidelines:

- Ensure 802.11r (FT) or CCKM is Enabled
- Configure the Data Rates as necessary
• Enable DTPC
• Configure Quality of Service (QoS)
• Set the WMM Policy to Required
• Ensure Aironet Extensions is Enabled
• Disable Public Secure Packet Forwarding (PSPF)
• Set IGMP Snooping to Enabled

802.11 Network Settings

It is recommended to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

If wanting to use 5 GHz, ensure the 802.11a/n/ac network status is Enabled.

Is recommended to enable 11r over air to enable fast secure roaming.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.

For Cisco Autonomous Access Points, select Dynamic Frequency Selection (DFS) to use auto channel selection. When DFS is enabled, enable at least one band (bands 1-4).

Can select band 1 only for the access point to use a UNII-1 channel (channel 36, 40, 44, or 48).

Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

This may be necessary if there is an intermittent interferer present in an area.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

It is recommended to utilize the same channel width for all access points.
Ensure **Client Power** is configured properly. Do not use default setting of **Max** power for client power on Cisco Autonomous Access Points as that will not advertise DTPC to the client.

Enable **Dot11d** for **World Mode** and configure the proper **Country Code**.

Ensure **Aironet Extensions** is enabled.

Set the **Beacon Period** to **100 ms** and **DTIM** to 2.
### Network Configuration

#### NETWORK MAP
- Summary
- Adjacent Nodes

#### NETWORK INTERFACE
- Summary
- IP Address
- GigabitEthernet0
- Radio0-802.11n 2.4GHz
- Radio0-802.11ac 5GHz

#### Hostname: ap-1
- Uptime is 1 day, 4 hours, 56 minutes

### Network Interfaces: Radio1-802.11ac Settings

<table>
<thead>
<tr>
<th>Enable Radio:</th>
<th>○ Enable</th>
<th>○ Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Status (Software/Hardware):</td>
<td>Enabled</td>
<td>Up</td>
</tr>
</tbody>
</table>

#### Role in Radio Network:
- ○ Access Point
- ○ Access Point (Fallback to Radio Shutdown)
- ○ Access Point (Fallback to Repeater)
- ○ Repeater
- ○ Root Bridge
- ○ Non-Root Bridge
- ○ Root Bridge with Wireless Clients
- ○ Non-Root Bridge with Wireless Clients

#### Max-Clients:
- ○ enable
- ○ disable
- (1-255)

#### 11r Configuration:
- ○ enable
- ○ disable
- ○ over-air
- ○ over-ds
- Reassociation-time: (20-1200 ms)

#### Data Rates:

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>○ Require</th>
<th>○ Enable</th>
<th>○ Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>9.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>12.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>18.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>24.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>36.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>48.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>54.0Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>90.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>114.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>171.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>238.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>322.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>378.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>462.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>552.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>642.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>732.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>842.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>942.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1042.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1142.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1242.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1342.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1442.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1542.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1642.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1742.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1842.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>1942.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2042.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2142.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2242.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2342.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2442.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2542.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2642.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2742.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2842.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
<tr>
<td>2942.2Mb/sec</td>
<td>○ Require</td>
<td>○ Enable</td>
<td>○ Disable</td>
</tr>
</tbody>
</table>

**Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide** 138
If wanting to use 2.4 GHz, ensure the 802.11b/g/n network status and 802.11g is enabled. Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps and higher as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12 Mbps and higher as supported (optional).
**WLAN Settings**

It is recommended to have a separate SSID for the Cisco Webex Wireless Phone 840 and 860. However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

The SSID to be used by the Cisco Webex Wireless Phone 840 and 860 can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

Enable **WPA2** key management.

Ensure either **11r** or **CCKM** is enabled, where 11r is recommended.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA Pre-shared Key</td>
<td></td>
<td>ASCII</td>
</tr>
<tr>
<td>11w Configuration</td>
<td>Disable</td>
<td></td>
</tr>
<tr>
<td>11w Association-comboack</td>
<td>1000 (100-30000)</td>
<td></td>
</tr>
<tr>
<td>11w Squerry-retry</td>
<td>100 (100-500)</td>
<td></td>
</tr>
<tr>
<td>IOS Client MFP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Client MFP on this SSID</td>
<td>Optimal</td>
<td></td>
</tr>
<tr>
<td>AP Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credentials</td>
<td>&lt;NONE&gt;</td>
<td>Define Credentials</td>
</tr>
<tr>
<td>Authentication Methods Profile</td>
<td>&lt;NONE&gt;</td>
<td>Define Authentication Methods Profile</td>
</tr>
<tr>
<td>Accounting Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Accounting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounting Server Priorities</td>
<td>Use Defaults</td>
<td>Define Defaults</td>
</tr>
<tr>
<td>Customize</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority 1</td>
<td>&lt;NONE&gt;</td>
<td></td>
</tr>
<tr>
<td>Priority 2</td>
<td>&lt;NONE&gt;</td>
<td></td>
</tr>
<tr>
<td>Priority 3</td>
<td>&lt;NONE&gt;</td>
<td></td>
</tr>
<tr>
<td>Rate Limit Parameters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limit TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input</td>
<td>Rate:</td>
<td>Burst-Size:</td>
</tr>
<tr>
<td>Output</td>
<td>Rate:</td>
<td>Burst-Size:</td>
</tr>
<tr>
<td>Limit UDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input</td>
<td>Rate:</td>
<td>Burst-Size:</td>
</tr>
<tr>
<td>Output</td>
<td>Rate:</td>
<td>Burst-Size:</td>
</tr>
<tr>
<td>General Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertise Extended Capabilities of this SSID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertise Wireless Provisioning Services (WPS) Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertise this SSID as a Secondary Broadcast SSID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable IP Redirection on this SSID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>DISABLED</td>
<td></td>
</tr>
</tbody>
</table>
Segment wireless voice and data into separate VLANs.

Ensure that Public Secure Packet Forwarding (PSPF) is not enabled for the voice VLAN as this will prevent clients from communicating directly when associated to the same access point. If PSPF is enabled, then the result will be no way audio.
Ensure **AES** is selected for encryption type.
Configure the RADIUS servers to be used for authentication and accounting.
**Wireless Domain Services (WDS)**

Wireless Domain Services should be utilized in the Cisco Autonomous Access Point environment, which is also required for fast secure roaming.

Select one access point to be the primary WDS server and another to be the backup WDS server.

Configure the primary WDS server with the highest priority (e.g. 255) and the backup WDS server with a lower priority (e.g. 254).
The Cisco Autonomous Access Points utilize Inter-Access Point Protocol (IAPP), which is a multicast protocol, therefore should use a dedicated native VLAN for Cisco Autonomous Access Points.

For the native VLAN, it is recommended to not use VLAN 1 to ensure that IAPP packets are exchanged successfully. Port security should be disabled on switch ports that Cisco Autonomous Access Points are directly connected to.

Server groups for Wireless Domain Services must be defined.
First, define the server group to be used for infrastructure authentication. Is recommended to use local RADIUS for infrastructure authentication. If not using local RADIUS for infrastructure authentication, then need to ensure that all access points with Wireless Domain Services enabled are configured in the RADIUS server.

Then, define the server group to be used for client authentication. Will need to ensure that all access points with Wireless Domain Services enabled are configured in the RADIUS server.
To utilize local RADIUS for infrastructure authentication, enable all authentication protocols.

Create a Network Access Server entry for the local access point.

Define the user account in which access points will be configured for to authenticate to the Wireless Domain Services enabled access point.

Configure local RADIUS on each access point participating in Wireless Domain Services.
Once the desired access points have been configured successfully to enable Wireless Domain Services, then all access points including those serving as WDS servers need to be configured to be able to authenticate to the WDS servers.

Enable **Participate in SWAN Infrastructure**.

If using a single WDS server, then can specify the IP address of the WDS server; otherwise enable **Auto Discovery**.
Enter the **Username** and **Password** to be used to authenticate to the WDS server.

Once the access point has been configured to authenticate to the WDS server, can check WDS Status to see the WDS server state as well as how many access points are registered to the WDS server.

**Call Admission Control (CAC)**

Load-based CAC and support for multiple streams are not present on the Cisco Autonomous Access Points therefore it is not recommended to enable CAC on Cisco Autonomous Access points.
The Cisco Autonomous Access Point only allows for 1 stream and the stream size is not customizable, therefore SRTP, Barge, Silent Monitoring, and Call Recording will not work if CAC is enabled.

If enabling Admission Control for Voice or for Video on the Cisco Autonomous Access Point, the admission must be unblocked on the SSID as well. In recent releases, the admission is unblocked by default.

```plaintext
Dot11 ssid voice
  vlan 3
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2 dot11r
      admit-traffic
```

**QoS Policies**

Configure the following QoS policy on the Cisco Autonomous Access Point to enable DSCP to CoS (WMM UP) mapping. This allows packets to be placed into the proper queue as long as those packets are marked correctly when received at the access point level.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
To enable QBSS, select **Enable** and check **Dot11e**.

If **Dot11e** is checked, then both CCA versions (802.11e and Cisco version 2) will be enabled.

Ensure **IGMP Snooping** is enabled.

Ensure **Wi-Fi MultiMedia (WMM)** is enabled.
If enabling the **Stream** feature either directly or via selecting **Optimized Voice** for the radio access category in the QoS configuration section, then use the defaults, where 5.5, 6, 11, 12 and 24 Mbps are enabled as nominal rates for 802.11b/g, 6, 12, and 24 Mbps enabled for 802.11a and 6.5, 13, and 26 Mbps enabled for 802.11n.

If the **Stream** feature is enabled, ensure that only voice packets are being put into the voice queue. Signaling packets should be put into a separate queue. This can be ensured by setting up a QoS policy mapping the DSCP to the correct queue.
Power Management

To enable Proxy ARP, set **Client ARP Caching** to **Enable**.

Also ensure that **Forward ARP Requests to Radio Interfaces When Not All Client IP Addresses Are Known** is checked.
Sample Configuration

version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap-1
!
logging rate-limit console 9
!
aaa new-model
!
aaa group server radius rad_eap
   server name 10.0.0.20
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
   server name 10.0.0.20
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius WDS
   server name 10.9.0.9
!
aaa group server radius Clients
   server name 10.0.0.20
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login method_WDS group WDS
aaa authentication login method_Clients group Clients
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
clock timezone -0500 -5 0
clock summer-time -0400 recurring
no ip source-route
no ip cef
ip domain name cisco.com
ip name-server 10.0.0.30
ip name-server 10.0.0.31
!
dot11 pause-time 100
dot11 syslog
!
dot11 ssid data
  vlan 2
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2
!
dot11 ssid voice
  vlan 3
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2 dot11r
!
dot11 arp-cache optional
dot11 phone dot11e
!
no ipv6 cef
!
crypto pki trustpoint TP-self-signed-672874324
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-672874324
  revocation-check none
  rsakeypair TP-self-signed-672874324
!
crypto pki certificate chain TP-self-signed-672874324
  certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 050F0030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 35657274
  69666666 6174652D 36373238 37343332 343301E7 0D313630 38330332 33303533
  3851370D 32030331 30310300 30303030 5A303031 2E030C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3637 32387334
  33233430 819F300D 06092A86 4886F70D 01010105 003818D0 03081890 02818100
  CB155DD1 3421B13F CD121F42 7A62D9F5 38EBC966 4420F38A 38DFAFF2 D43CD3B9
  5F5A1877 7910F9F5 6E9EDE4F 730942C7 17DC4CBC E5AE3E49 0AF79419 0BEF34BC
  5DECBE42 FF2978CB C34D5AEF ED17DB58 C7BF6592 61C1AD25 3E8F7205 15EA58C2
  0A5E3B15 7F08F9EA 5DA2BFA7 95E6C60 22C229C7 02A919D7 A4FEB50B 5425357F
  02030100 01A35330 51300F06 03551D13 01010F04 05300301 01FF301F 0603551D
  23041830 1680145C 2FEE6CF0E 0E380A40 11381459 5D596E3E A684A030 1D603555
  1D0E0416 0414FCF2 E6CF0EE0 380A4011 3814595D 596E3EA6 84DA300D 06092A86
  4886F70D 01010505 00381818 0053F55B 5EBB1FE2 C849BC45 47D0E710 0200404E
  A8B174BC A46E1B5A 857166C3 B9FD71DF 72645F91F 7204A676 16BD35A2 4F39ADF7
  0BD24F71 BAF916AC E984343C A5473B95 E5D15237 8897D346 A150BFB2 DC23E8D3
  AFF0A51C B6253153 C4E2C022 66F1E361 B2EE49E2 763FCBC7 6381E7F7 61B6E14D
  60CD9F47 2C046417 37211E5F CE
  quit

username <REMOVED> privilege 15 password 7 <REMOVED>
!
class-map match-all classVoice0
  match ip dscp cs3

class-map match-all classVoice1
  match ip dscp af41

class-map match-all classVoice2
  match ip dscp ef
!
policy-map Voice
  class classVoice0
    set cos 4
class classVoice1
  set cos 5
class classVoice2
  set cos 6
policy-map Data
class class-default
  set cos 0
!
bridge irb
!
interface Dot11Radio0
  no ip address
  shutdown
  antenna gain 0
  traffic-metrics aggregate-report
  stbc
  mbssid
Power client local
channel 2412
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
  no ip address
  !
  encryption vlan 2 mode ciphers aes-ccm
  !
  encryption vlan 3 mode ciphers aes-ccm
  !
  ssid data
  !
  ssid voice
  !
  antenna gain 0
  peakdetect
  dfs band 3 block
  stbc
  mbssid
  power client local
  channel width 40-below
  channel 5180
  station-role root
  dot11 dot11r pre-authentication over-air
  dot11 dot11r reassociation-time value 1000
  dot11 qos class voice local
    admission-control
    admit-traffic narrowband max-channel 75 roam-channel 6
! dot11 qos class voice cell
    admission-control
!
world-mode dot11d country-code US both
!
interface Dot11Radio1.2
    encapsulation dot1Q 2
    bridge-group 2
    bridge-group 2 subscriber-loop-control
    bridge-group 2 spanning-disabled
    bridge-group 2 block-unknown-source
    no bridge-group 2 source-learning
    no bridge-group 2 unicast-flooding
    service-policy input Data
    service-policy output Data
!
interface Dot11Radio1.3
    encapsulation dot1Q 3
    bridge-group 3
    bridge-group 3 subscriber-loop-control
    bridge-group 3 spanning-disabled
    bridge-group 3 block-unknown-source
    no bridge-group 3 source-learning
    no bridge-group 3 unicast-flooding
    service-policy input Voice
!
interface Dot11Radio1.10
    encapsulation dot1Q 10 native
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 spanning-disabled
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
    no ip address
duplex auto
    speed auto
!
interface GigabitEthernet0.2
    encapsulation dot1Q 2
    bridge-group 2
    bridge-group 2 spanning-disabled
    no bridge-group 2 source-learning
    service-policy input Data
    service-policy output Data
!
interface GigabitEthernet0.3
    encapsulation dot1Q 3
    bridge-group 3
    bridge-group 3 spanning-disabled
    no bridge-group 3 source-learning
    service-policy input Voice
!
interface GigabitEthernet0.10
  encapsulation dot1Q 10 native
  bridge-group 1
  bridge-group 1 spanning-disabled
  no bridge-group 1 source-learning

interface BVI1
  mac-address 18e7.281b.3f54
  ip address 10.9.0.9 255.255.255.0
  ipv6 address dhcp
  ipv6 address autoconfig
  ipv6 enable

  ip default-gateway 10.9.0.2
  ip forward-protocol nd
  no ip http server
  ip http authentication aaa
  ip http secure-server
  ip radius source-interface BVI1

  radius-server local
    nas 10.9.0.9 key 7 <REMOVED>
  user wds nthash 7 <REMOVED>

  radius-server attribute 32 include-in-access-req format %h

  radius server 10.0.0.20
  address ipv4 10.0.0.20 auth-port 1812 acct-port 1813
  key 7 <REMOVED>

  radius server 10.9.0.9
  address ipv4 10.9.0.9 auth-port 1812 acct-port 1813
  key 7 <REMOVED>

  access-list 111 permit tcp any any neq telnet
  bridge 1 route ip

  wlc cp ap username wds password 7 <REMOVED>
  wlc cp ap wds ip address 10.9.0.9
  wlc cp authentication-server infrastructure method_WDS
  wlc cp authentication-server client eap method_Clients
  wlc cp authentication-server client leap method_Clients
  wlc cp wds priority 255 interface BVI1

  line con 0
  access-class 111 in
  line vty 0 4
  access-class 111 in
  transport input all

  snntp server 10.0.0.2
  snntp broadcast client
end
Cisco Meraki Access Points

When configuring Cisco Meraki access points, use the following guidelines:

- Enable 802.11r for WPA2-Enterprise or Pre-shared key
- Set Splash page to None
- Enable Bridge mode
- Enable VLAN tagging
- Set Band selection to 5 GHz band only
- Configure the Data Rates as necessary
- Configure Quality of Service (QoS)

Creating the Wireless Network

A wireless network must be created prior to adding any Cisco Meraki access points to provide WLAN service. Select Create a new network from the drop-down menu.
Select Wireless for Network type then click Create.
Cisco Meraki access points can be claimed either by specifying the serial number or order number. Once claimed, those Cisco Meraki access points will then be listed in the available inventory.

Cisco Meraki access points can be claimed either by selecting **Add Devices** on the **Create network** or **Organization > Configure > Inventory** pages.

Access points can also be claimed by selecting **Add APs** on the **Wireless > Monitor > Access points** page, then selecting **Claim**.
Once claimed, Cisco Meraki access points can be added to the desired wireless network via the **Organization > Configure > Inventory** page.

Claimed access points can also be added to a wireless network by selecting **Add APs** on the **Wireless > Monitor > Access points** page.
SSID Configuration

To create a SSID, select the desired network from the drop-down menu then select **Wireless > Configure > SSIDs**.

It is recommended to have a separate SSID for the Cisco Webex Wireless Phone 840 and 860; data clients and other type of clients should utilize a different SSID and VLAN.

However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized.

To set the SSID name, select **Rename**.

To enable the SSID, select **Enabled** from the drop-down menu.

On the **Wireless > Configure > Access control** page, select **WPA2-Enterprise** to enable 802.1x authentication.

The Cisco Meraki authentication server or an external RADIUS server can be utilized when selecting **WPA2-Enterprise**.

The Cisco Meraki authentication server supports PEAP authentication and requires a valid email address.

Other authentication types (e.g. Pre-Shared Key) are available as well.

Ensure **802.11r** is enabled.

Ensure Splash page is set to **None** to enable direct access.
Note: Cisco Meraki access points support 802.11r (FT) for fast secure roaming, but do not support Cisco Centralized Key Management (CCKM).

If WPA2-Enterprise is enabled where the Cisco Meraki authentication server will be utilized as the RADIUS server, then a user account must be created on the Network-wide > Configure > Users page, which the Cisco Webex Wireless Phone 840 and 860 will be configured to use for 802.1x authentication.
On the **Wireless > Configure > Access control** page, recommend to enable **Bridge mode**, where the Cisco Webex Wireless Phone 840 and 860 will obtain DHCP from the local LAN instead of the Cisco Meraki network; unless call control, other endpoints, etc. are cloud-based.

Once **Bridge mode** is enabled, the VLAN tagging option will be available.

It is recommended to enable **VLAN tagging** for the SSID.

If VLAN tagging is utilized, ensure that the Cisco Meraki access point is connected to a switch port configured for trunk mode allowing that VLAN.


If utilizing Cisco IOS Switches, use the following switch port configuration for ports that have Cisco Meraki access points connected to enable 802.1q trunking.

```
Interface GigabitEthernet X
    switchport trunk encapsulation dot1q
    switchport mode trunk
    mls qos trust dscp
```
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

On the **Wireless > Configure > Access control** page, the frequency band for the SSID to be used by the Cisco Webex Wireless Phone 840 and 860 can be configured as necessary. It is recommended to select **5 GHz band only** to have the Cisco Webex Wireless Phone 840 and 860 operate on the 5 GHz band due to having many channels available and not as many interferers as the 2.4 GHz band has.

If the 2.4 GHz band needs to be used due to increased distance, then **Dual band operation (2.4 GHz and 5 GHz)** should be selected. Do not utilize the **Dual band operation with Band Steering** option.

Is recommended to disable data rates below 12 Mbps unless a legacy 2.4 GHz client needs to be able to connect to the Wireless LAN.

Cisco Meraki access points currently utilize a DTIM period of 1 with a beacon period of **100 ms**; which both are non-configurable.

On the **Wireless > Configure > SSID availability** page, the SSID can be broadcasted by setting **Visibility** to **Advertise this SSID publicly**.

Is recommended to set **Per-AP Availability** to **This SSID is enabled on all APs**.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
A schedule for SSID availability can be configured as necessary, however it is recommended to set **Scheduled Availability** to **Disabled**.

### Radio Settings

On the **Wireless > Configure > Radio settings** page, access points can be configured in bulk or by individual access point to define the automatic or manual channel and transmit power settings.

When using Cisco Meraki access points it is recommended to select **Auto** for the channel and transmit power to utilize what is defined in the RF Profile. However, individual access points can be configured with static channel and transmit power for either 5 or 2.4 GHz radios, which may be necessary if there is an intermittent interferer present in an area. While other access points can be enabled for **Auto** and work around the access points that are have static channel assignments.

It is recommended to either modify the standard **Basic Indoor Profile** or create a new RF Profile with **Band selection** set to **Per SSID** and **Client balancing** set to **Off**.
In the RF Profile, the **Channel width** for 5 GHz radios can be set to use 20 MHz, 40 MHz, or 80 MHz channels. 2.4 GHz radios utilize 20 MHz channel width and can not be configured for any other channel width. It is recommended to utilize the same channel width for all access points.

5 GHz channels to be used by **AutoChannel** can also be configured in the RF Profile. 2.4 GHz channels used by **AutoChannel** are limited to channels 1, 6, and 11 only.

The **Radio transmit power range** is also be configured in the RF Profile.

If the **Minimum bitrate configuration** is set to Per band, then it will override what is defined in the SSID configuration. It is recommended to disable data rates below 12 Mbps unless a legacy 2.4 GHz client needs to be able to connect to the Wireless LAN.
Cisco Meraki access points do not support Dynamic Transmit Power Control (DTPC), therefore the Cisco Webex Wireless Phone 840 and 860 will utilize the maximum transmit power supported for the current channel and data rate.

**Firewall and Traffic Shaping**
On the **Wireless > Configure > Firewall & traffic shaping** page, firewall and traffic shaping rules can be defined. Ensure a **Layer 3 firewall rule** is configured to allow local LAN access for wireless clients. To allow traffic shaping rules to be defined select **Shape traffic on this SSID** in the drop-down menu for **Shape traffic**. Once **Shape traffic on this SSID** has been applied, then select **Create a new rule** to define **Traffic shaping rules**.

By default, Cisco Meraki access points currently tag voice frames marked with DSCP EF (46) as WMM UP 5 instead of WMM UP 6 and call control frames marked with DSCP CS3 (24) as WMM UP 3 instead of WMM UP 4.

---

**Note:** Cisco Meraki access points do not support Call Admission Control / Traffic Specification (TSPEC).

---

### Configuring Cisco Call Control

#### Cisco Unified Communications Manager

Cisco Unified Communications Manager offers many different phone, call and security features.

#### Device Enablement

To enable the Cisco Webex Wireless Phone 840 or 860 device type in the Cisco Unified Communications Manager, the corresponding device enabler (QED) COP file for each phone model must be installed via the Cisco Unified Operating System Administration webpage for each Cisco Unified Communications Manager server.
Each Cisco Unified Communication Manager node may not have to be restarted after the device enabler (QED) COP file has been installed.

Perform the following, which is dependent on the Cisco Unified Communications Manager version.

**11.5(1)SU4 and lower**

- Reboot all Cisco Unified Communications Manager nodes.

**11.5(1)SU5 and higher or 12.5(1) and higher**

- Restart the Cisco Tomcat service on all Cisco Unified Communications Manager nodes.
- If running the Cisco CallManager service on the publisher node, restart the service on the publisher node only.

**Note:** The Cisco CallManager service on subscriber nodes do not need to be restarted.

For information on how to install the COP file, refer to the Cisco Unified Communications Manager Operating System Administration Guide at this URL:


When adding the Cisco Webex Wireless Phone 840 or 860 to the Cisco Unified Communications Manager it must be provisioned using the Wi-Fi MAC address.

The Wi-Fi MAC address of the Cisco Webex Wireless Phone 840 or 860 can be found by navigating to **Settings > About phone > Wi-Fi MAC address**.

As of the 1.3(0) release, the Cisco Webex Wireless Phone 840 and 860 support multiple lines (up to 6), shared lines, and privacy.

The Cisco Webex Wireless Phone 840 and 860 do not support auto registration.

---

**Manufacturing Certificate Authority (CA) Certificates**

A new manufacturing certificate authority (CA) is being utilized for the Cisco Webex Wireless Phone 860.

Until the new root and intermediate certificates are natively included in Cisco Unified Communications Manager, additional steps are required in order to trust the new Manufacturing Installed Certificate (MIC), which includes manually adding the root and intermediate certificates to the certificate chain.

1. To install the new Cisco Manufacturing CA certificates, first download the missing root and intermediate certificates from the externally available Cisco PKI website.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
The missing certificates to complete the chain of trust up to and including the root for the new MICs are below:

- **Cisco Manufacturing CA III (cmca3)** – Intermediate

- **Cisco Basic Assurance Root CA 2099 (cbarc2099)** - Root for Cisco Manufacturing CA III

2. Using your web browser, login to the Cisco Unified Operating System Administration web page.
3. Under the **Security** menu, select **Certificate Management**.
4. Select **Upload Certificate/Certificate Chain**.
5. Select **CallManager-trust** for the **Certificate Purpose**, browse to the certificate, then select **Upload**.
   
   **Note:** Repeat this step for all certificates on the Cisco Unified Communication Manager publisher only as the certificate will replicate to all other Cisco Unified Communication Manager nodes.

6. Select **CAPF-trust** for the **Certificate Purpose**, browse to the certificate, then select **Upload**.

   **Note:** Repeat this step for all certificates on all Cisco Unified Communication Manager nodes as the certificate will not replicate to all other Cisco Unified Communication Manager nodes automatically.

### Device Pools

When creating a new Cisco Webex Wireless Phone 840 or 860, a **Device Pool** must be configured.

The device pool defines common settings (e.g. Cisco Unified Communications Manager Group, etc.), roaming sensitive settings (e.g. Date/Time Group, Region, etc.), local route group settings, device mobility related information settings, and other group settings.

Device Pools can be used to either group devices per location, per model type, etc.
Phone Button Templates

When creating a new Cisco Webex Wireless Phone 840 or 860, a Phone Button Template must be configured. Custom phone button templates can be created with the option for many different features.
Security Profiles

When creating a new Cisco Webex Wireless Phone 840 or 860, a Device Security Profile must be configured. Security profiles can be utilized to enable authenticated mode or encrypted mode, where signaling, media and configuration file encryption is then enabled.

The Certificate Authority Proxy Function (CAPF) must be operational in order to utilize a Locally Signed Certificate (LSC) with a security profile.

The Cisco Webex Wireless Phone 840 and 860 have a Manufacturing Installed Certificate (MIC), which can be utilized with a security profile as well.

The default device security profile is the model specific Standard SIP Non-Secure Profile, which does not utilize encryption.
### Phone Security Profile Information

<table>
<thead>
<tr>
<th>Product Type:</th>
<th>Cisco 840</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Protocol:</td>
<td>SIP</td>
</tr>
<tr>
<td>Name*:</td>
<td>Cisco 840 - Standard SIP Non-Secure Profile</td>
</tr>
<tr>
<td>Description</td>
<td>Cisco 840 - Standard SIP Non-Secure Profile</td>
</tr>
<tr>
<td>Nonce Validity Time*:</td>
<td>600</td>
</tr>
<tr>
<td>Device Security Mode</td>
<td>Non Secure</td>
</tr>
<tr>
<td>Transport Type*:</td>
<td>TCP+UDP</td>
</tr>
</tbody>
</table>

Enable Digest Authentication

TFTP Encrypted Config

### Phone Security Profile CAPF Information

| Authentication Mode* | By Null String |
| Key Order* | RSA Only |
| RSA Key Size (Bits)* | 2048 |
| EC Key Size (Bits) | < None > |

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

### Parameters used in Phone

| SIP Phone Port* | 5060 |

### Phone Security Profile Information

| Product Type: | Cisco 860 |
| Device Protocol: | SIP |
| Name*: | Cisco 860 - Standard SIP Non-Secure Profile |
| Description | Cisco 860 - Standard SIP Non-Secure Profile |
| Nonce Validity Time*: | 600 |
| Device Security Mode | Non Secure |
| Transport Type*: | TCP+UDP |

Enable Digest Authentication

TFTP Encrypted Config

### Phone Security Profile CAPF Information

| Authentication Mode* | By Null String |
| Key Order* | RSA Only |
| RSA Key Size (Bits)* | 2048 |
| EC Key Size (Bits) | < None > |

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

### Parameters used in Phone

| SIP Phone Port* | 5060 |

Note: Transport type must be set as TCP+UDP or TCP as UDP is not supported.
SIP Profiles

When creating a new Cisco Webex Wireless Phone 840 or 860, a SIP Profile must be configured.

It is recommended to create a custom SIP Profile for the Cisco Webex Wireless Phone 840 and 860 (do not use the Standard SIP Profile or Standard SIP Profile for Mobile Device).

To create a custom SIP Profile for the Cisco Webex Wireless Phone 840 or 860, use the Standard SIP Profile as the reference template.

Copy the Standard SIP Profile, then change the following parameters.

**Timer Register Delta (seconds)** = 30  (default = 5)
**Timer Keep Alive Expires (seconds)** = 300  (default = 120)
**Timer Subscribe Expires (seconds)** = 300  (default = 120)
**Timer Subscribe Delta (seconds)** = 15  (default = 5)

Ensure SIP Station KeepAlive Interval at System > Service Parameters > Cisco CallManager remains configured for 120 seconds.

**Custom SIP Profile Example**
### SIP Profile Information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name*</td>
<td>Custom 860 SIP Profile</td>
</tr>
<tr>
<td>Description</td>
<td>Custom 860 SIP Profile</td>
</tr>
<tr>
<td>Default MTP Telephony Event Payload Type*</td>
<td>101</td>
</tr>
<tr>
<td>Early Offer for G.Clear Calls*</td>
<td>Disabled</td>
</tr>
<tr>
<td>User-Agent and Server header information*</td>
<td>Send Unified CM Version Information as User-Agent</td>
</tr>
<tr>
<td>Version in User Agent and Server Header*</td>
<td>Major And Minor</td>
</tr>
<tr>
<td>Dial String Interpretation*</td>
<td>Phone number consists of characters 0-9, *, #, or x</td>
</tr>
<tr>
<td>Confidential Access Level Headers*</td>
<td>Disabled</td>
</tr>
<tr>
<td>Redirect by Application</td>
<td></td>
</tr>
<tr>
<td>Disable Early Media on 180</td>
<td></td>
</tr>
<tr>
<td>Outgoing T.38 INVITE include audio mline</td>
<td></td>
</tr>
<tr>
<td>Offer valid IP and Send/Receive mode only for T.38 Fax Relay</td>
<td></td>
</tr>
<tr>
<td>Use Fully Qualified Domain Name in SIP Requests</td>
<td></td>
</tr>
<tr>
<td>Assured Services SIP conformance</td>
<td></td>
</tr>
<tr>
<td>Enable External QoS**</td>
<td></td>
</tr>
</tbody>
</table>

### SDP Information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*</td>
<td>TIAS and AS</td>
</tr>
<tr>
<td>SDP Transparency Profile</td>
<td>Pass all unknown SDP attributes</td>
</tr>
<tr>
<td>Accept Audio Codec Preferences in Received Offer*</td>
<td>Default</td>
</tr>
<tr>
<td>Require SDP Inactive Exchange for Mid-Call Media Change</td>
<td></td>
</tr>
<tr>
<td>Allow RR/RS bandwidth modifier (RFC 3556)</td>
<td></td>
</tr>
</tbody>
</table>

### Parameters used in Phone

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer Invite Expires (seconds)*</td>
<td>180</td>
</tr>
<tr>
<td>Timer Register Delta (seconds)*</td>
<td>30</td>
</tr>
<tr>
<td>Timer Register Expires (seconds)*</td>
<td>3600</td>
</tr>
<tr>
<td>Timer T1 (msec)*</td>
<td>500</td>
</tr>
<tr>
<td>Timer T2 (msec)*</td>
<td>4000</td>
</tr>
<tr>
<td>Retry INVITE*</td>
<td>6</td>
</tr>
<tr>
<td>Retry Non-INVITE*</td>
<td>10</td>
</tr>
<tr>
<td>Media Port Ranges</td>
<td>Common Port Range for Audio and Video</td>
</tr>
<tr>
<td>Start Media Port*</td>
<td>16384</td>
</tr>
<tr>
<td>Configuration Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Stop Media Port</td>
<td>32766</td>
</tr>
<tr>
<td>DSCP for Audio Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for Video Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for Audio Portion of Video Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for TelePresence Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>DSCP for Audio Portion of TelePresence Calls</td>
<td>Use System Default</td>
</tr>
<tr>
<td>Call Pickup URI</td>
<td>x-cisco-serviceuri-pickup</td>
</tr>
<tr>
<td>Call Pickup Group Other URI</td>
<td>x-cisco-serviceuri-opickup</td>
</tr>
<tr>
<td>Call Pickup Group URI</td>
<td>x-cisco-serviceuri-gpickup</td>
</tr>
<tr>
<td>Meet Me Service URI</td>
<td>x-cisco-serviceuri-meetme</td>
</tr>
<tr>
<td>User Info</td>
<td>None</td>
</tr>
<tr>
<td>DTMF DB Level</td>
<td>Nominal</td>
</tr>
<tr>
<td>Call Hold Ring Back</td>
<td>Off</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Off</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Off</td>
</tr>
<tr>
<td>Do Not Disturb Control</td>
<td>Off</td>
</tr>
<tr>
<td>Telnet Level for 7940 and 7960</td>
<td>Disabled</td>
</tr>
<tr>
<td>Resource Priority Namespace</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Timer Keep Alive Expires (seconds)</td>
<td>300</td>
</tr>
<tr>
<td>Timer Subscribe Expires (seconds)</td>
<td>300</td>
</tr>
<tr>
<td>Timer Subscribe Delta (seconds)</td>
<td>15</td>
</tr>
<tr>
<td>Maximum Redirections</td>
<td>70</td>
</tr>
<tr>
<td>Off Hook To First Digit Timer (milliseconds)</td>
<td>15000</td>
</tr>
<tr>
<td>Call Forward URI</td>
<td>x-cisco-serviceuri-cfwdial</td>
</tr>
<tr>
<td>Speed Dial (Abbreviated Dial) URI</td>
<td>x-cisco-serviceuri-abbrevdial</td>
</tr>
<tr>
<td>Conference Join Enabled</td>
<td>☑</td>
</tr>
<tr>
<td>RFC 2543 Hold</td>
<td>☐</td>
</tr>
<tr>
<td>Semi Attended Transfer</td>
<td>☑</td>
</tr>
<tr>
<td>Enable VAD</td>
<td>☐</td>
</tr>
<tr>
<td>Slutter Message Waiting</td>
<td>☐</td>
</tr>
<tr>
<td>MLPP User Authentication</td>
<td>☐</td>
</tr>
</tbody>
</table>

**Normalization Script**

| Normalization Script                          | < None > |
Common Settings

Some settings such as Web Access can be configured on an enterprise phone, common phone profile or individual phone level. Web Access is disabled by default for the Cisco Webex Wireless Phone 840 and 860. Override common settings can be enabled at either configuration level.

QoS Parameters

The DSCP values to be used for SIP communications, phone configuration, and phone based services to be used by the phone are defined in the Cisco Unified Communications Manager’s Enterprise Parameters.
The default DSCP value for SIP communications and phone configuration is set to CS3.

Phone based services are configured to be best effort traffic by default.

---

<table>
<thead>
<tr>
<th>Enterprise Parameters Configuration</th>
<th>Parameter Name</th>
<th>Parameter Value</th>
<th>Suggested Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster ID</td>
<td>Cluster ID</td>
<td>Stand Alone Cluster</td>
<td>Stand Alone Cluster</td>
</tr>
<tr>
<td>Max Number of Device Level Trace</td>
<td></td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>DSCP for Phone-based Services</td>
<td></td>
<td>default DSCP (000000)</td>
<td>default DSCP (000000)</td>
</tr>
<tr>
<td>DSCP for Phone Configuration</td>
<td></td>
<td>CS3 (precedence 3) DSCP (011000)</td>
<td>CS3 (precedence 3) DSCP (011000)</td>
</tr>
<tr>
<td>DSCP for Cisco CallManager to Device Interface</td>
<td></td>
<td>CS3 (precedence 3) DSCP (011000)</td>
<td>CS3 (precedence 3) DSCP (011000)</td>
</tr>
<tr>
<td>Connection Monitor Duration</td>
<td></td>
<td>120</td>
<td>120</td>
</tr>
<tr>
<td>Auto Registration Phone Protocol</td>
<td></td>
<td>SCCP</td>
<td>SCCP</td>
</tr>
<tr>
<td>Auto Registration Legacy Mode</td>
<td></td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>BLF For Call Lists</td>
<td></td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Advertise G.722 Codec</td>
<td></td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Phone Personalization</td>
<td></td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Services Provisioning</td>
<td></td>
<td>Internal</td>
<td>Internal</td>
</tr>
<tr>
<td>Feature Control Policy</td>
<td></td>
<td>&lt; None &gt;</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Wi-Fi Hotspot Profile</td>
<td></td>
<td>IMS Inter Operator Id</td>
<td>IMS Inter Operator Id</td>
</tr>
<tr>
<td>IMS Inter Operator Id</td>
<td></td>
<td>IMS Inter Operator Id</td>
<td>IMS Inter Operator Id</td>
</tr>
<tr>
<td>URL Lookup Policy</td>
<td></td>
<td>Case Sensitive</td>
<td>Case Sensitive</td>
</tr>
</tbody>
</table>

---

**G.722 and Opus Advertisement**

Cisco Unified Communications Manager supports the ability to configure whether G.722 and Opus are to be a supported codec system wide or not.

G.722 and Opus codecs can be disabled at the enterprise phone, common phone profile or individual phone level by setting **Advertise G.722 and Opus Codecs to Disabled**.

---

**Audio Bit Rates**

The audio bit rate can be configured by creating or editing existing Regions in the Cisco Unified Communications Manager.

---

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Use the following information to configure the audio bit rate to be used for audio calls.

<table>
<thead>
<tr>
<th>Audio Codec</th>
<th>Audio Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opus</td>
<td>6-510 Kbps</td>
</tr>
<tr>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
</tr>
<tr>
<td>G.729</td>
<td>8 Kbps</td>
</tr>
</tbody>
</table>

**Product Specific Configuration Options**

In Cisco Unified Communications Manager Administration, the following configuration options are available for the Cisco Webex Wireless Phone 840 and 860.

For a description of these options, click ? at the top of the configuration page.

Product specific configuration options can be configured in bulk via the Bulk Admin Tool if using Cisco Unified Communications Manager.

Some of the product specific configuration options can be configured on an enterprise phone, common phone profile or individual phone configuration level.

**Cisco Webex Wireless Phone 840 and 860 Configuration Options**
### Field Name | Description
--- | ---
**Web Access** | This parameter specifies whether the phone will accept connections from a web browser or other HTTP client. Disabling the web server functionality of the phone will block access to the phones internal web pages. These pages provide statistics and configuration information.

**Web Password** | This parameter specifies the password to access the phone’s Web interface. Enter a 8-127 character password.

**Reboot immediately after downloading software updates** | This parameter specifies whether the phone will reboot immediately after downloading a software update or if it will notify the user to manually reboot. The phone must be rebooted to apply software updates.

**Emergency Numbers** | This parameter specifies the emergency numbers that can be dialed without unlocking the phone keypad. For example, in the United States, the 911 emergency number is a good candidate so that it can be dialed without unlocking the phone. To specify more than one number, use a comma as a separator. For example, if you want to enter 411, 511, and 911 as emergency numbers, then enter 411,511,911 in the field without spaces.

**Visual Voicemail Access** | This parameter enables or disables access to Visual Voicemail.

**Voicemail Server (Primary)** | This parameter contains the address of the primary voicemail server for Visual Voicemail.
<table>
<thead>
<tr>
<th><strong>Voicemail Server (Backup)</strong></th>
<th>This parameter contains the address of the backup voicemail server for Visual Voicemail.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Load Server</strong></td>
<td>This parameter specifies that the phone will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IP address (using standard IP addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades.</td>
</tr>
<tr>
<td><strong>Advertise G.722 and Opus Codecs</strong></td>
<td>This parameter specifies whether the phone will advertise the G.722 and Opus codecs or not. Codec negotiation involves two steps: first, the phone must advertise the supported codec(s) to the Cisco Unified CallManager (not all endpoints support the same set of codecs). Second, when the Cisco Unified CallManager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. The options are Use System Default (this phone will defer to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (this phone will not advertise G.722 or Opus support), and Enabled (this phone will advertise G.722 and Opus support).</td>
</tr>
<tr>
<td><strong>Customer support upload URL</strong></td>
<td>This URL is used to upload problem report files when the user has run the “Problem Reporting Tool” on the endpoint.</td>
</tr>
<tr>
<td><strong>Secondary SIP Server</strong></td>
<td>This parameter contains the address of the server for the optional second registration.</td>
</tr>
<tr>
<td><strong>Secondary SIP Server Port</strong></td>
<td>This parameter contains the far-end port number for the optional second registration.</td>
</tr>
<tr>
<td><strong>Secondary SIP Transport</strong></td>
<td>This parameter contains the transport type for the optional second registration.</td>
</tr>
<tr>
<td><strong>Secondary SIP Extension</strong></td>
<td>This parameter contains the SIP extension for the optional second registration.</td>
</tr>
<tr>
<td><strong>Secondary SIP Username</strong></td>
<td>This parameter contains the SIP username for the optional second registration.</td>
</tr>
<tr>
<td><strong>Secondary SIP Password</strong></td>
<td>This parameter contains the SIP password for the optional second registration.</td>
</tr>
</tbody>
</table>

**Note:** If wanting to keep the web password or secondary SIP password enabled long-term, then should utilize a secure profile with TFTP encryption enabled.

For more information on these features, see the Cisco Webex Wireless Phone 840 and 860 Administration Guide or the Cisco Webex Wireless Phone 840 and 860 Release Notes.


Configuring the Cisco Webex Wireless Phone 840 and 860

To configure the Cisco Webex Wireless Phone 840 and 860, either use an Enterprise Mobility Management (EMM) application for provisioning or use the local user interface for manual configuration.

Enterprise Mobility Management (EMM) Configuration

Use the following guidelines to manually configure the Cisco Webex Wireless Phone 840 and 860 via an Enterprise Mobility Management (EMM) application.

On the startup screen, quickly tap the display 6 times and then can scan a QR code to enroll the Cisco Webex Wireless Phone 840 or 860 to the EMM via the device owner method.

The following applications will need to be added as allowed applications to ensure they will be available on the Cisco Webex Wireless Phone 840 and 860 when enrolling the phone using the device owner method as these applications will not be available in the Google Play Store.

- **Cisco Phone** = com.cisco.phone
- **Application URLs** = com.cisco.appurl
- **Logging** = com.cisco.logging
- **Port Manager** = com.cisco.portmanager
- **System Updater** = com.cisco.sysupdater
- **UCM Client** = com.cisco.ucmclient
Below is the list of Cisco applications specific to the Cisco Webex Wireless Phone 840 and 860 that will be available in the Google Play Store and can optionally be added when enrolling the phone using the device owner method.

- **Battery Life** = com.cisco.batterylife
- **Buttons** = com.cisco.buttons
- **Call Quality Settings** = com.cisco.callquality
- **Custom Settings** = com.cisco.customsettings
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- **Web API** = com.cisco.webapi
- **Barcode** (840s and 860s models only) = com.cisco.barcode.service

Depending on the EMM platform utilized, the **Gboard - the Google Keyboard** application may also need to be added when enrolling the phone using the device owner method.
Please see the EMM application documentation for additional information.

**Manual Configuration**

Use the following guidelines to manually configure the Cisco Webex Wireless Phone 840 and 860 via the local user interface.

**Wi-Fi Profile Configuration**

Use the following guidelines to manually configure a Wi-Fi network via the local user interface.

- For an out of box (factory reset) phone, configure the Wi-Fi network via the startup wizard or select **Set up offline**.
- Configuration options will be determined by whether a broadcasted Wi-Fi network is being configured or a Wi-Fi network is being manually configured.
- Below lists the available security modes supported and the key management and encryption types that can be used for each mode.

<table>
<thead>
<tr>
<th>Security Mode</th>
<th>802.1x Type</th>
<th>Key Management</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>N/A</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
### Configuring a Broadcasted Wi-Fi Network

- If the Wi-Fi network is broadcasted, select the desired Wi-Fi network from the list via the startup wizard, then enter the required credentials depending on the Wi-Fi network’s security settings.
- If configuring the broadcasted Wi-Fi network offline (not via the startup wizard), swipe up from the bottom of the phone’s display to show the installed applications, then select **Settings > Network & internet > Wi-Fi** to configure the Wi-Fi network.

- To connect to an open Wi-Fi network, simply click on the Wi-Fi network name.

- To connect to a PSK enabled Wi-Fi network, click on the Wi-Fi network name, then enter the 8-63 ASCII or 64 HEX Password.
• To connect to an EAP enabled Wi-Fi network, click on the Wi-Fi network name, then select the EAP method.
• If configuring a PEAP or EAP-TTLS (TTLS) Wi-Fi network, select the Phase 2 authentication method and CA certificate option to utilize, then enter the Identity and Password.
• If configuring an EAP-TLS (TLS) Wi-Fi network, select the User certificate and CA certificate options to utilize.
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Configuring a Non-Broadcasted Wi-Fi Network

- If manually configuring a non-broadcasted (hidden) Wi-Fi network, swipe up from the bottom of the phone’s display to show the installed applications, select Settings > Network & internet > Wi-Fi.
- At the bottom of Wi-Fi settings, select Add Network, then configure the network name (SSID), security type, and enter the required credentials depending on the Wi-Fi network’s security settings.
- A non-broadcasted Wi-Fi network must also be marked as a Hidden network in the Advanced options section of the Wi-Fi network settings; otherwise the Wi-Fi network will show as not in range.
• To connect to an open Wi-Fi network, enter the **Network name**, then set **Security** to **None**.

• To connect to a PSK enabled Wi-Fi network, enter the **Network name**, set **Security** to **WPA/WPA2-Personal**, then enter the 8-63 ASCII or 64 HEX **Password**.
• To connect to an EAP enabled Wi-Fi network, enter the Network name, set Security to WPA/WPA2-Enterprise, then select the **EAP method**.

• If configuring a PEAP or EAP-TTLS (TTLS) Wi-Fi network, select the **Phase 2 authentication** method and **CA certificate** option to utilize, then enter the **Identity** and **Password**.

• If configuring an EAP-TLS (TLS) Wi-Fi network, select the **User certificate** and **CA certificate** options to utilize.
Configuring Advanced Options for the Wi-Fi Network

- A non-broadcasted Wi-Fi network must be configured as a **Hidden network** in the **Advanced options** section of the Wi-Fi network settings; otherwise the Wi-Fi network will show as not in range.
- Set **Hidden network** to **Yes** to connect to a non-broadcasted Wi-Fi network.

- IP settings (Static or DHCP config) can be configured in the **Advanced options** section of the Wi-Fi network settings.
• Proxy settings can also be configured in the Advanced options section of the Wi-Fi network settings.

Configuring the Call Quality Settings

• The Wi-Fi band selection (Auto, 2.4 GHz, 5 GHz) including enabled channels, fast secure roaming preferences (FT and CCKM), and the Wi-Fi low RSSI threshold can be configured in the Call Quality Settings application.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
• If wanting to utilize a single Wi-Fi frequency band or to limit the channels to be enabled per Wi-Fi frequency band, select **Wi-Fi band selection**, then uncheck **Auto** and either select **2.4 GHz Wi-Fi band** only, **5 GHz Wi-Fi band** only, or both if wanting to utilize both 2.4 GHz and 5 GHz.

• If **Auto** is unchecked, then the channels to enable per Wi-Fi frequency band can be configured by simply clicking on the desired channel set.
2.4 GHz: channels 1 - 14
- Ch:1 (2412 MHz)
- Ch:2 (2417 MHz)
- Ch:3 (2422 MHz)
- Ch:4 (2427 MHz)
- Ch:5 (2432 MHz)
- Ch:6 (2437 MHz)
- Ch:7 (2442 MHz)
- Ch:8 (2447 MHz)
- Ch:9 (2452 MHz)

5.0 GHz: channels 36 - 48
- Subband 1: channels 36 - 48
  - Ch:36 (5180 MHz)
  - Ch:40 (5200 MHz)
  - Ch:44 (5220 MHz)
  - Ch:48 (5240 MHz)
- Subband 2: channels 52 - 64
  - Ch:52 (5260 MHz)
  - Ch:56 (5280 MHz)
  - Ch:60 (5300 MHz)
  - Ch:64 (5320 MHz)
• If wanting to utilize 802.11r (FT) for fast secure roaming, ensure the slider for FT is to the right to be set as Preferred.
• If wanting to utilize CCKM for fast secure roaming, ensure the slider for CCKM is to the right to be set as Preferred.
• If both FT and CCKM are set as Preferred, then 802.11r (FT) will be given preference over CCKM.

Note: 802.11r (FT) or CCKM will be negotiated if enabled on the access point when using EAP-TLS, EAP-TTLS, or PEAP, where preference is given to 802.11r (FT) when enabled.

WPA3 is not supported.

802.1x-SHA2 key management is not supported.
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
CCMP256, GCMP128, and GCMP256 encryption ciphers are not supported.

For more information, refer to the Cisco Webex Wireless Phone 840 and 860 Administration Guide at this URL:

Certificate Management

The Cisco Webex Wireless Phone 840 and 860 can utilize X.509 digital certificates for EAP-TLS or to enable server validation when using EAP-TTLS or PEAP.

When using EAP-TLS, need to ensure the date and time is configured correctly.

Both DER and Base-64 (PEM) encoding are acceptable for the client and server certificates.

Certificates with a key size of 1024, 2048, and 4096 are supported.

Ensure the client and server certificates are signed using either the SHA-1 or SHA-2 algorithm, as the SHA-3 signature algorithms are not supported.

Ensure Client Authentication is listed in the Enhanced Key Usage section of the user certificate details.

Microsoft® Certificate Authority (CA) servers are recommended. Other CA server types may not be completely interoperable with the Cisco Webex Wireless Phone 840 and 860.

Installing Certificates

Certificates can be automatically installed via an Enterprise Mobility Management (EMM) application if supported. Certificates can also be manually installed within Wi-Fi settings or Security settings.

To install certificates via Wi-Fi settings, select Settings > Network & internet > Wi-Fi > Wi-Fi Preferences > Advanced, then select Install certificates.

The certificate downloaded or copied to the phone’s storage prior can then be selected to be installed.
To install certificates via Security settings, select **Settings > Security > Encryption & credentials**, then select **Install from storage**.

The certificate downloaded or copied to the phone’s storage prior can then be selected to be installed.
A user certificate must be installed to utilize EAP-TLS. A password may need to be entered to extract the certificates and keys. A certificate name can then be entered. Ensure the CA chain that issued the user certificate is added to the RADIUS server’s trust list.

The root CA certificate that issued the RADIUS server’s certificate must be installed to enable server validation for EAP-TLS, EAP-TTLS, or PEAP.
Configuring Certificates

Once the certificates are installed, they can then be selected for use in the Wi-Fi profile configuration.

For **PEAP** and **EAP-TTLS**, the **CA certificate** can optionally be configured to enable server validation.
For **EAP-TLS**, the **User certificate** must be configured and the **CA certificate** can optionally be configured to enable server validation.

**Removing Certificates**

Certificates can be removed individually or in bulk.

To remove an individual certificate, select the certificate under **System > Encryption & credentials > User credentials**, then select **Remove**.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
To remove all certificates, select **Clear credentials** under **System > Encryption & credentials**, then select **OK** to confirm the removal.

**Cisco Phone Application Configuration**
Use the following guidelines to configure the **Cisco Phone** application.

- **Cisco Phone** settings can be configured by selecting the three lines in the upper left hand corner while in the **Cisco Phone** application.

  ![Cisco Phone interface](image)

- **User settings** such as ringtone can be configured as necessary.

  ![User settings](image)

- Trust lists and TFTP servers can be managed by selecting **Phone information > Security**.
• Once **Phone information > Security** is selected, the **Local Phone Unlock Password** must be entered (default = **##**).

• If needing to configure a TFTP server as the network is not providing DHCP option 150 or DHCP option 66 for the Cisco Unified Communications Manager you want to register to, enable **Alternate TFTP**, then enter the TFTP server addresses.

• Select the back arrow in the upper left hand corner twice to exit the **Settings** menu and save the settings.

For more information, refer to the Cisco Webex Wireless Phone 840 and 860 Administration Guide at this URL:
Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
Note: DHCP option 66 is now supported as of the 1.2(0) release.

Bluetooth Settings

The Cisco Webex Wireless Phone 840 and 860 include Bluetooth support, which enables hands-free communications. To pair a Bluetooth headset to the Cisco Webex Wireless Phone 840 and 860, follow the instructions below.

- Navigate to Settings > Connected devices.

- Ensure that Bluetooth is set to On in Settings > Connected devices > Connection Preferences > Bluetooth.
- The Bluetooth device name can also be changed as necessary.
• Ensure the Bluetooth device is in pairing mode, then select **Pair new device**.
• Select the Bluetooth device after it is displayed in the list.
• The Cisco Webex Wireless Phone 840 and 860 will then attempt to pair automatically with the Bluetooth device. If unsuccessful, enter the pin code when prompted.

• Once paired, the Cisco Webex Wireless Phone 840 and 860 will attempt to connect to the Bluetooth device.
• The Bluetooth device name can be changed in the device details.
• Selecting the Bluetooth device then selecting **Disconnect** will disconnect that currently connected Bluetooth device.
• Select **Forget** to unpair the selected Bluetooth device.

**Upgrading Firmware**

**Cisco Unified Communications Manager**

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
To upgrade the firmware, install the signed COP file for Cisco Unified Communications Manager then restart the Cisco TFTP service for all nodes running the Cisco TFTP service.

For information on how to install the COP file, refer to the Cisco Unified Communications Manager Operating System Administration Guide at this URL:


The downloaded phone configuration file is parsed and the device load is identified. The Cisco Webex Wireless Phone 840 or 860 then downloads the firmware files to flash if it is not running the specified image already.

A Load Server can be specified as an alternate server to retrieve firmware files via HTTP on TCP port 6970 (as TFTP on UDP port 69 is not supported), which is located in the product specific configuration section of Cisco Webex Wireless Phone 840 and 860 within Cisco Unified Communications Manager Administration. Download the firmware in ZIP file format, extract the contents, then copy those files to the load server.

The user will be prompted to confirm to reboot and apply the new firmware unless the Reboot immediately after downloading software updates option is enabled in Cisco Unified Communications Manager.

The current Build number can be viewed at Settings > About phone > Build number.

Using the Cisco Webex Wireless Phone 840 and 860

Applications

The Cisco Webex Wireless Phone 840 and 860 have the following pre-installed custom applications.
- **Cisco Phone** - Voice and video calling
- **Battery Life** - Battery monitoring
- **Buttons** - Button customizations
- **Call Quality Settings** - Wi-Fi customizations
- **Custom Settings** - User restrictions and device settings
- **Emergency** - Panic button feature
- **Logging** - Advanced debugging
- **PTT** - Push to talk feature
- **System Updater** - Firmware update notifications
- **Web API** – Web API settings
- **Barcode** - Barcode scanning feature (840s and 860s models only)

**Cisco Phone**

To launch the phone application, select the **Cisco Phone** icon on the main page or from the applications menu.

The Cisco Webex Wireless Phone 840 and 860 will attempt to register to Cisco Unified Communications Manager after power on, so the application does not have to be launched manually in order to make or receive calls.

The Cisco Webex Wireless Phone 840 and 860 is registered to Cisco Unified Communications Manager when there is a check mark icon in the notification status bar and the extension is displayed in the Cisco Phone application.
Call history is accessible via the **Calls** tab.

Contacts and favorites are accessible via the **Contacts** tab.

Manual calls can be made via the **Keypad** tab.

Voicemail is accessible via the **Voicemail** tab if **Visual Voicemail Access** is **Enabled** in Cisco Unified Communications Manager.

Features such as **Speed dial**, **Call forward**, **Privacy (if enabled)**, and **Applications (if configured)** are accessible by selecting the three lines in the upper left hand corner then **Features**.

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide
To configure speed dials, select **Features > Call forward**.

Once a speed dial is configured by mapping to an existing contact entry’s number, simply press and hold the associated number when on the **Keypad** tab.

To enable call forward, select **Features > Call forward**, tap the slider so it moves to the right, then enter the destination number to forward all calls to.
To disable call forward, simply tap the slider so it moves to the left. Select the back arrow in the upper left hand corner to exit the Settings menu and save the settings.

To utilize the privacy feature, a custom phone button template with privacy configured for one of the buttons must be created first then apply it to the phone. Then to enable privacy, simply tap on Privacy under Features. A check mark will be displayed to the right of Privacy to indicate if the feature is enabled.
To access configured applications, select **Features > Applications**.

Battery Life

Battery life monitoring can be enabled by selecting the three dots in the upper right hand corner while in the **Battery Life** application, then selecting **Settings**.

To enable battery life monitoring, ensure the slider for **Enable battery monitoring** is to the right to be set as **On**.
Buttons

The hard buttons on the Cisco Webex Wireless Phone 840 and 860 can be custom configured in the Buttons application.

Note: The Fingerprint button is only available on the Cisco Webex Wireless Phone 860.
Call Quality Settings

The Wi-Fi band selection (Auto, 2.4 GHz, 5 GHz) including enabled channels, fast secure roaming preferences (FT and CCKM), and the Wi-Fi low RSSI threshold can be configured in the Call Quality Settings application.

Custom Settings

Various settings including user restrictions, time configuration, etc. can be custom configured in the Custom Settings application.
Emergency settings including motion sensor, panic button, emergency call and tone configuration can be configured by selecting the three dots in the upper right hand corner while in the Emergency application, then selecting Settings.
Emergency settings

- Motion sensor configuration
- Panic button configuration
- Emergency call configuration
- Emergency tone configuration
**Note:** The Emergency button (red button) is located on the top right of the Cisco Webex Wireless Phone 840 and the Cisco Webex Wireless Phone 860.

**Logging**

Various debug options are available in the **Logging** application.

Enter the **Local Phone Unlock Password** when prompted (default = **#**).
PTT

Push to Talk (PTT) settings can be configured by selecting the three dots in the upper right hand corner while in the PTT application, then selecting Settings.
System Updater

The Cisco Unified Communications Manager administrator will manage and push down firmware updates to the Cisco Webex Wireless Phone 840 and 860. The user will then be prompted to confirm to reboot and apply the new firmware unless the **Reboot immediately after downloading software updates** option is enabled in Cisco Unified Communications Manager.
Web API

Web API settings can be configured by selecting the three dots in the upper right hand corner while in the Web API application, then selecting Settings.
Barcode

The barcode scanner is available on the Cisco Webex Wireless Phone 840S and 860S models only.

Barcode scanner settings can be configured by selecting the three dots in the upper right hand corner while in the Barcode application, then selecting Settings.
Application Store

Various types of applications are available for download from Google Play.

Google Play is an application market developed by Google™ for Android OS. The Play Store application allows users to browse and download applications published by third-party developers.

A Google account is necessary to download applications.

When first launching Google Play, you will be prompted to sign in with your credentials or register if you do not have an account already.

Google Play can also be accessed at this URL.

https://play.google.com/store

Troubleshooting

Problem Report Tool

A problem report can be created by selecting the three lines in the upper left hand corner while in the Cisco Phone application, then selecting Report problem.

The Customer support upload URL option in Cisco Unified Communications Manager can be configured per phone to obtain the logs automatically or manually downloaded the logs from the phone’s webpage under Device Logs.
Configure a Customer Support Upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: "SEP001122334455")
- serialno (example: "FCH12345ABC")
- username (the username configured in Cisco Unified Communications Manager, the device owner)
- prt_file (example: "probrep-20141021-162840.tar.gz")

Sample Script

```php
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used: upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $POST['devicename'];

```
$devicename = trim($devicename, "'\"\");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"\");

$username = $_POST['username'];
$username = trim($username, "'\"\");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
    header("HTTP/1.0 500 Internal Server Error");
    die("Error: You must select a file to upload.");
}

?>

Phone Webpages

Cisco Webex Wireless Phone 840 and 860 information can be gathered remotely by accessing the phone’s webpage interfaces. The webpage interface (https://x.x.x.x) contains read-only information regarding device information, network information, registration information, and device logs. To access the webpage interface, Web Access must be enabled in Cisco Unified Communications Manager.

Device Information

The Cisco Webex Wireless Phone 840 and 860 provide device information, where MAC address and version information is displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco Webex Wireless Phone 840 or 860 then select Device information to view this information.
Network Information

The Cisco Webex Wireless Phone 840 and 860 provide network information, where wireless LAN and network information is displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco Webex Wireless Phone 840 or 860 then select Network information to view this information.
Registration Information

The Cisco Webex Wireless Phone 840 and 860 provide registration information, where phone DN and registration status information is displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco Webex Wireless Phone 840 or 860 then select Registration information to view this information.
Device Logs

Device logs can be obtained from the web interface of Cisco Webex Wireless Phone 840 or 860 for troubleshooting purposes. Browse to the web interface (https://x.x.x.x) of the Cisco Webex Wireless Phone 840 or 860 then select Device Logs to view this information.

Click the + sign to the right of the log file type (Problem reports, Device logs, Android reports, Wlan) to list those log files, which can then be downloaded.

WLAN Signal Indicator

The WLAN signal indicator for the Cisco Webex Wireless Phone 840 and 860 is displayed in the upper right hand corner of the display.

When the Cisco Webex Wireless Phone 840 and 860 is connected to an access point, the icon will be grey in color as shown below.
**WLAN Network Information**

The current WLAN network information for the Cisco Webex Wireless Phone 840 and 860 can be viewed by selecting **Settings > Network & internet > Wi-Fi**, then selecting the connected Wi-Fi network.

A configured Wi-Fi network can be removed by selecting **Forget**.
Restoring Factory Defaults

The configuration of the Cisco Webex Wireless Phone 840 and 860 can be reset to factory defaults by selecting **Settings > System > Advanced > Reset options > Erase all data (factory reset)**.

An informational screen will be displayed indicating all of the data that will be erased, where **Erase all data** must be selected to continue with the factory reset.

Then a confirmation screen will be displayed, where **Erase all data** must be selected to proceed with the factory data reset. The phone will then restart and boot with factory settings restored.
If the Cisco Webex Wireless Phone 840 or 860 is not able to boot properly, a factory reset can also be initiated via the following procedure:

- Power the phone off by pressing the **Power** button (button on the top left for the Cisco Webex Wireless Phone 840 and second button from the top on the right side for the Cisco Webex Wireless Phone 860), then select **Power off**.
- Press and hold the **Emergency** button (red button located on the top right of the Cisco Webex Wireless Phone 840 and the Cisco Webex Wireless Phone 860), then power the phone on.
- Keep the **Power** button pressed until the phone vibrates, then release the **Power** button, while continuing to keep the **Emergency** button pressed.
- Once the bootloader screen is displayed, release the **Emergency** button.
- Press the **Volume Down** button until **Recovery mode** is displayed, then press the **Power** button to select that option.
- The phone will restart and return to a new screen that displays the Android icon.
- From this screen, press and hold the **Power** button, then quickly press and release the **Volume Up** button to enter the **Recovery Menu** screen.
- Release the **Power** button once the **Recovery Menu** is displayed.
- Press the **Volume Down** button to highlight **Wipe data/factory reset**, then press the **Power** button to select that option.
- Press the **Volume Down** button to highlight **Factory data reset**, then press the **Power** button to select that option.
- Press the **Power** button again when **Reboot system now** is highlighted.
- The Cisco Webex Wireless Phone 840 or 860 will then restart and have the factory settings restored.

**Note:** If the Cisco Webex Wireless Phone 840 or 860 have been signed into a Google account or have other device ownership, then they will have factory wipe protection enabled, which will prevent the device from being fully wiped and require you to have the Google account information in order to access the device even after the restoring factory defaults.

**Capturing a Screenshot of the Phone Display**

The current display of the Cisco Webex Wireless Phone 840 or 860 can be captured by pressing the power button, then selecting **Screenshot**.
Additional Documentation

Cisco Webex Wireless Phone 840 and 860 Data Sheet

Cisco Webex Wireless Phone 840 and 860 Administration Guide

Cisco Webex Wireless Phone 840 and 860 User Guide

Cisco Webex Wireless Phone 840 and 860 Quick Reference Guides

Cisco Webex Wireless Phone 840 and 860 Release Notes

Cisco Webex Wireless Phone 840 and 860 Software
https://software.cisco.com/download/home/286327931

Cisco Unified Communications Manager

Cisco Voice Software
https://software.cisco.com/download/home/278875240

Real-Time Traffic over Wireless LAN Design Guide

Cisco Unified Communications Design Guides

Cisco AireOS Wireless LAN Controller Documentation

Cisco Catalyst IOS XE Wireless LAN Controller Documentation

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

Cisco Mobility Express Documentation

Cisco Autonomous Access Point Documentation

Cisco Meraki Wireless LAN Documentation
https://documentation.meraki.com