The Cisco IP Phone 8861 and 8865 are adaptable for professionals that require the ability to unplug the wired network connection and remain connected. The Wireless LAN and Bluetooth capabilities enable mobility and cord-free communications.

This guide provides information and guidance to help the network administrator deploy these phones in a wireless LAN environment.
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/13/14</td>
<td>10.2(1) Release</td>
</tr>
<tr>
<td>08/17/16</td>
<td>11.0(1) Release</td>
</tr>
<tr>
<td>10/06/16</td>
<td>11.5(1) Release</td>
</tr>
<tr>
<td>08/01/17</td>
<td>11.7(1) Release</td>
</tr>
<tr>
<td>11/02/17</td>
<td>12.0(1) Release</td>
</tr>
<tr>
<td>02/21/18</td>
<td>12.0(1)SR1 Release</td>
</tr>
<tr>
<td>04/02/18</td>
<td>12.1(1) Release</td>
</tr>
<tr>
<td>06/13/18</td>
<td>12.1(1)SR1 Release</td>
</tr>
<tr>
<td>01/15/20</td>
<td>12.6(1) Release</td>
</tr>
<tr>
<td>03/11/20</td>
<td>12.7(1) Release</td>
</tr>
</tbody>
</table>
Cisco IP Phone 8861 and 8865 Overview

The Cisco IP Phone 8861 and 8865 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 and video 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 IP Phone 8861 and 8865 in order to take advantage of the 802.11a/n/ac data rates available.

Despite the optimizations that Cisco has implemented in the Cisco IP Phone 8861 and 8865, 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 IP Phone 8861 and 8865 is not intended to be used as a medical device and should not be used to make clinical decisions.

Phone Models

The following Cisco IP Phone 8861 and 8865 models are available.

Below outlines the modes, frequency ranges and 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>
</table>
| CP-8861-K9= | Cisco IP Phone 8861, Charcoal | 2.4 GHz = 3.2 dBi  
5 GHz = 2.4 dBi | 2.412 - 2.472 GHz  
5.180 - 5.240 GHz  
5.260 - 5.320 GHz  
5.500 - 5.720 GHz  
5.745 - 5.825 GHz | 13  
4  
4  
12  
5 | 1-13  
36,40,44,48  
52,56,60,64  
100-144  
149,153,157,161,165 |
| CP-8861-W-K9= | Cisco IP Phone 8861, White |  |  | | |
| CP-8865-K9= | Cisco IP Phone 8865, Charcoal | 2.4 GHz = 2.1 dBi  
5 GHz = 1.9 dBi | 2.412 - 2.472 GHz  
5.180 - 5.240 GHz  
5.260 - 5.320 GHz  
5.500 - 5.720 GHz  
5.745 - 5.825 GHz | 13  
4  
4  
12  
5 | 1-13  
36,40,44,48  
52,56,60,64  
100-144  
149,153,157,161,165 |
| CP-8865-W-K9= | Cisco IP Phone 8865, White |  |  | | |

A power cube (CP-PWR-CUBE-4=) is required when utilizing the Cisco IP Phone 8861 or 8865 in Wi-Fi mode.

Note: 802.11j (channels 34, 38, 42, 46) are not supported.
Channel 14 for Japan is not supported.
Requirements

The Cisco IP Phone 8861 and 8865 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 IP Phone 8861 and 8865.

Site Survey

Before deploying the Cisco IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 is 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 IP Phone 8861 and 8865.

**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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 can hold a signal for at least 5 seconds.

**Channel Utilization**

Channel Utilization levels should be kept under 40%.

The Cisco IP Phone 8861 and 8865 convert the 0-255 scale value to a percentage, so 105 would equate to around 40% in the Cisco IP Phone 8861 and 8865.

**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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 utilize Session Initiation Protocol (SIP) for call control with the following applications.

- Cisco Unified Communications Manager (CUCM)
  
  Minimum = 8.5(1)
  
  Recommended = 8.6(2), 9.1(2), 10.5(2), 11.0(1), 11.5(1), and later

- Cisco Unified Communications Manager Express (CUCME)
  
  Minimum = 10.0
  
  Recommended = 11.0, 11.5, 11.7, and later

- Cisco Unified Survivable Remote Site Telephony (SRST)
  
  Minimum = 10.0
  
  Recommended = 11.0, 11.5, 11.7, and later

**Note:** Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable Cisco IP Phone 8861 and 8865 device support.

Device packages for Cisco Unified Communications Manager are available at the following location.

http://software.cisco.com/download/navigator.html?mdfid=278875240

Prior to release 11.0 of Cisco Unified Communications Manager Express, the Cisco IP Phone 8861 and 8865 are to utilize the fast track method utilizing the Cisco Unified IP Phone 9971 as the reference model (use 7975 as reference model if needing softkey template support).

With release 11.0 and 11.5 of Cisco Unified Communications Manager Express, the Cisco IP Phone 8865 can utilize the Cisco IP Phone 8861 as the reference model.

With release 11.7 and later of Cisco Unified Communications Manager Express, there is native support for the Cisco IP Phone 8865, therefore can use the Cisco IP Phone 8865 as the model type.


**Wireless LAN**

The Cisco IP Phone 8861 and 8865 are supported on the following Cisco Wireless LAN solutions.

- Cisco AireOS Wireless LAN Controller and Cisco Lightweight Access Points
  
  Minimum = 7.0.252.0
  
  Recommended = 8.0.152.0, 8.2.170.0, 8.3.150.0, 8.5.161.0, 8.8.125.0, 8.10.112.0

- Cisco IOS Wireless LAN Controller and Cisco Lightweight Access Points
  
  Minimum = 16.12.1s
  
  Recommended = 16.12.2s

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
- Cisco Meraki Access Points
  Minimum = MR 25.9, MX 13.33
  Recommended = MR 25.11, MX 13.33

- Cisco Autonomous Access Points
  Minimum = 12.4(21a)JY
  Recommended = 12.4(25d)JA2, 15.2(4)JB6, 15.3(3)JK

Note: Cisco Wireless LAN Controller release 8.0.121.0 or later is required if utilizing Flexconnect + Local Switching mode.

Access Points
Below are the Cisco access points that are supported.
Any access point model that is not listed below is not supported.

The Cisco IP Phone 8861 and 8865 are supported on the following Cisco Aironet access point platforms.
Note: The Cisco IP Phone 8861 and 8865 are supported with the Cisco AP3600 when the internal 802.11a/b/g/n radio is utilized, however is not supported if the 802.11ac module (AIR-RM3000AC) for the Cisco AP3600 is installed.

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>600</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>700</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>700W</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1040</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1130</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1140</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1240</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1250</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1260</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1600</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</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>Model</td>
<td>1810</td>
<td>1810W</td>
<td>1815</td>
<td>1830</td>
<td>1840</td>
<td>1850</td>
<td>2600</td>
<td>2700</td>
<td>2800</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The Cisco IP Phone 8861 and 8865 are supported on the following Cisco Meraki access point platforms.
The Cisco Meraki MR12, MR16, and Z1 access point platforms are not certified for use with Cisco IP Phone 8861 and 8865 deployments.

The table below lists the modes that are supported by each Cisco Meraki access point.

<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>MR18</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

https://meraki.cisco.com/products/wireless/#models
https://meraki.cisco.com/products/appliances/#models
Note: If an access point model is not specifically listed above, then it is not supported.

Currently no support for Cisco Aironet 1500 Series outdoor access points.

No support for any access point model operating in MESH mode.

No support for third-party access points as there are no interoperability tests performed for third-party access points.

However, the user should have basic functionality when connected to a Wi-Fi compliant access point.

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)
- Traffic Classification (TCLAS)
- Differentiated Services Code Point (DSCP)
- Class of Service (CoS / 802.1p)
- QoS Basic Service Set (QBSS)

### 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.

Third-party antennas are not supported, as there is no interoperability testing performed against third-party antennas including Distributed Antenna Systems (DAS) and Leaky Coaxial Systems.

Please refer to the following URL for more info on Cisco Wireless LAN over Distributed Antenna Systems.


**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)
- Traffic Classification (TCLAS)
- Unscheduled Automatic Power Save Delivery (UAPSD)
- Simple Certificate Enrollment Protocol (SCEP)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
  - Opus, G.722, G.711, iSAC, iLBC, G.729
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- HyperText Transfer Protocol (HTTP)
- Cisco Discovery Protocol (CDP)
- Syslog

### Wi-Fi

The following table lists the data rates, ranges, and receiver sensitivity info for Cisco IP Phone 8861 and 8865.

#### 5 GHz Specifications

<table>
<thead>
<tr>
<th>5 GHz - 802.11a</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 14 dBm (Depends on region)</td>
<td>6 Mbps</td>
<td>OFDM - BPSK</td>
<td>-94 dBm</td>
</tr>
<tr>
<td></td>
<td>9 Mbps</td>
<td>OFDM - BPSK</td>
<td>-93 dBm</td>
</tr>
<tr>
<td></td>
<td>12 Mbps</td>
<td>OFDM - QPSK</td>
<td>-92 dBm</td>
</tr>
<tr>
<td></td>
<td>18 Mbps</td>
<td>OFDM - QPSK</td>
<td>-89 dBm</td>
</tr>
<tr>
<td></td>
<td>24 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>-86 dBm</td>
</tr>
<tr>
<td></td>
<td>36 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>-83 dBm</td>
</tr>
<tr>
<td></td>
<td>48 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>-78 dBm</td>
</tr>
<tr>
<td>5 GHz - 802.11n (HT20)</td>
<td>Data Rate</td>
<td>Modulation</td>
<td>Receiver Sensitivity</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Max Tx Power = 13 dBm (Depends on region)</td>
<td>7 Mbps (MCS 0)</td>
<td>OFDM - BPSK</td>
<td>-94 dBm</td>
</tr>
<tr>
<td></td>
<td>14 Mbps (MCS 1)</td>
<td>OFDM - QPSK</td>
<td>-91 dBm</td>
</tr>
<tr>
<td></td>
<td>21 Mbps (MCS 2)</td>
<td>OFDM - QPSK</td>
<td>-89 dBm</td>
</tr>
<tr>
<td></td>
<td>29 Mbps (MCS 3)</td>
<td>OFDM - 16 QAM</td>
<td>-86 dBm</td>
</tr>
<tr>
<td></td>
<td>43 Mbps (MCS 4)</td>
<td>OFDM - 16 QAM</td>
<td>-82 dBm</td>
</tr>
<tr>
<td></td>
<td>58 Mbps (MCS 5)</td>
<td>OFDM - 64 QAM</td>
<td>-77 dBm</td>
</tr>
<tr>
<td></td>
<td>65 Mbps (MCS 6)</td>
<td>OFDM - 64 QAM</td>
<td>-76 dBm</td>
</tr>
<tr>
<td></td>
<td>72 Mbps (MCS 7)</td>
<td>OFDM - 64 QAM</td>
<td>-74 dBm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5 GHz - 802.11n (HT40)</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 13 dBm (Depends on region)</td>
<td>15 Mbps (MCS 0)</td>
<td>OFDM - BPSK</td>
<td>-91 dBm</td>
</tr>
<tr>
<td></td>
<td>30 Mbps (MCS 1)</td>
<td>OFDM - QPSK</td>
<td>-88 dBm</td>
</tr>
<tr>
<td></td>
<td>45 Mbps (MCS 2)</td>
<td>OFDM - QPSK</td>
<td>-86 dBm</td>
</tr>
<tr>
<td></td>
<td>60 Mbps (MCS 3)</td>
<td>OFDM - 16 QAM</td>
<td>-83 dBm</td>
</tr>
<tr>
<td></td>
<td>90 Mbps (MCS 4)</td>
<td>OFDM - 16 QAM</td>
<td>-79 dBm</td>
</tr>
<tr>
<td></td>
<td>120 Mbps (MCS 5)</td>
<td>OFDM - 64 QAM</td>
<td>-75 dBm</td>
</tr>
<tr>
<td></td>
<td>135 Mbps (MCS 6)</td>
<td>OFDM - 64 QAM</td>
<td>-73 dBm</td>
</tr>
<tr>
<td></td>
<td>150 Mbps (MCS 7)</td>
<td>OFDM - 64 QAM</td>
<td>-72 dBm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5 GHz - 802.11ac (VHT20)</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 12 dBm (Depends on region)</td>
<td>7 Mbps (MCS 0)</td>
<td>OFDM - BPSK</td>
<td>-93 dBm</td>
</tr>
<tr>
<td></td>
<td>14 Mbps (MCS 1)</td>
<td>OFDM - QPSK</td>
<td>-90 dBm</td>
</tr>
<tr>
<td></td>
<td>21 Mbps (MCS 2)</td>
<td>OFDM - QPSK</td>
<td>-87 dBm</td>
</tr>
<tr>
<td></td>
<td>29 Mbps (MCS 3)</td>
<td>OFDM - 16 QAM</td>
<td>-84 dBm</td>
</tr>
<tr>
<td></td>
<td>43 Mbps (MCS 4)</td>
<td>OFDM - 16 QAM</td>
<td>-81 dBm</td>
</tr>
<tr>
<td></td>
<td>58 Mbps (MCS 5)</td>
<td>OFDM - 64 QAM</td>
<td>-76 dBm</td>
</tr>
<tr>
<td></td>
<td>65 Mbps (MCS 6)</td>
<td>OFDM - 64 QAM</td>
<td>-75 dBm</td>
</tr>
<tr>
<td></td>
<td>72 Mbps (MCS 7)</td>
<td>OFDM - 64 QAM</td>
<td>-74 dBm</td>
</tr>
<tr>
<td></td>
<td>87 Mbps (MCS 8)</td>
<td>OFDM – 256 QAM</td>
<td>-70 dBm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5 GHz - 802.11ac (VHT40)</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 12 dBm (Depends on region)</td>
<td>15 Mbps (MCS 0)</td>
<td>OFDM - BPSK</td>
<td>-90 dBm</td>
</tr>
<tr>
<td></td>
<td>30 Mbps (MCS 1)</td>
<td>OFDM - QPSK</td>
<td>-87 dBm</td>
</tr>
<tr>
<td></td>
<td>45 Mbps (MCS 2)</td>
<td>OFDM - QPSK</td>
<td>-85 dBm</td>
</tr>
<tr>
<td></td>
<td>60 Mbps (MCS 3)</td>
<td>OFDM - 16 QAM</td>
<td>-82 dBm</td>
</tr>
<tr>
<td></td>
<td>90 Mbps (MCS 4)</td>
<td>OFDM - 16 QAM</td>
<td>-79 dBm</td>
</tr>
<tr>
<td></td>
<td>120 Mbps (MCS 5)</td>
<td>OFDM - 64 QAM</td>
<td>-73 dBm</td>
</tr>
<tr>
<td></td>
<td>135 Mbps (MCS 6)</td>
<td>OFDM - 64 QAM</td>
<td>-72 dBm</td>
</tr>
<tr>
<td></td>
<td>150 Mbps (MCS 7)</td>
<td>OFDM - 64 QAM</td>
<td>-72 dBm</td>
</tr>
<tr>
<td></td>
<td>180 Mbps (MCS 8)</td>
<td>OFDM – 256 QAM</td>
<td>-67 dBm</td>
</tr>
<tr>
<td></td>
<td>200 Mbps (MCS 9)</td>
<td>OFDM – 256 QAM</td>
<td>-66 dBm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5 GHz - 802.11ac (VHT80)</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
</table>
### 2.4 GHz Specifications

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>DSSS - BPSK</td>
<td>-98 dBm</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>DSSS - QPSK</td>
<td>-96 dBm</td>
</tr>
<tr>
<td>5.5 Mbps</td>
<td>DSSS - CCK</td>
<td>-93 dBm</td>
</tr>
<tr>
<td>11 Mbps</td>
<td>DSSS - CCK</td>
<td>-91 dBm</td>
</tr>
</tbody>
</table>

**2.4 GHz - 802.11b**

<table>
<thead>
<tr>
<th>Max Tx Power = 17 dBm (Depends on region)</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>OFDM - BPSK</td>
<td>-95 dBm</td>
<td></td>
</tr>
<tr>
<td>2 Mbps</td>
<td>OFDM - BPSK</td>
<td>-94 dBm</td>
<td></td>
</tr>
<tr>
<td>9 Mbps</td>
<td>OFDM - BPSK</td>
<td>-93 dBm</td>
<td></td>
</tr>
<tr>
<td>12 Mbps</td>
<td>OFDM - QPSK</td>
<td>-90 dBm</td>
<td></td>
</tr>
<tr>
<td>18 Mbps</td>
<td>OFDM - QPSK</td>
<td>-87 dBm</td>
<td></td>
</tr>
<tr>
<td>24 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>-84 dBm</td>
<td></td>
</tr>
<tr>
<td>36 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>-79 dBm</td>
<td></td>
</tr>
<tr>
<td>48 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>-77 dBm</td>
<td></td>
</tr>
<tr>
<td>54 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>-77 dBm</td>
<td></td>
</tr>
</tbody>
</table>

**2.4 GHz - 802.11g**

<table>
<thead>
<tr>
<th>Max Tx Power = 14 dBm (Depends on region)</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Mbps</td>
<td>OFDM - BPSK</td>
<td>-95 dBm</td>
<td></td>
</tr>
<tr>
<td>14 Mbps</td>
<td>OFDM - QPSK</td>
<td>-92 dBm</td>
<td></td>
</tr>
<tr>
<td>21 Mbps</td>
<td>OFDM - QPSK</td>
<td>-90 dBm</td>
<td></td>
</tr>
<tr>
<td>29 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>-87 dBm</td>
<td></td>
</tr>
<tr>
<td>43 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>-83 dBm</td>
<td></td>
</tr>
<tr>
<td>58 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>-78 dBm</td>
<td></td>
</tr>
<tr>
<td>65 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>-77 dBm</td>
<td></td>
</tr>
<tr>
<td>72 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>-75 dBm</td>
<td></td>
</tr>
</tbody>
</table>

**2.4 GHz - 802.11n (HT20)**

<table>
<thead>
<tr>
<th>Max Tx Power = 13 dBm (Depends on region)</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>33 Mbps (MCS 0)</td>
<td>OFDM - BPSK</td>
<td>-87 dBm</td>
<td></td>
</tr>
<tr>
<td>65 Mbps (MCS 1)</td>
<td>OFDM - QPSK</td>
<td>-83 dBm</td>
<td></td>
</tr>
<tr>
<td>98 Mbps (MCS 2)</td>
<td>OFDM - QPSK</td>
<td>-81 dBm</td>
<td></td>
</tr>
<tr>
<td>130 Mbps (MCS 3)</td>
<td>OFDM - 16 QAM</td>
<td>-78 dBm</td>
<td></td>
</tr>
<tr>
<td>195 Mbps (MCS 4)</td>
<td>OFDM - 16 QAM</td>
<td>-75 dBm</td>
<td></td>
</tr>
<tr>
<td>260 Mbps (MCS 5)</td>
<td>OFDM - 64 QAM</td>
<td>-73 dBm</td>
<td></td>
</tr>
<tr>
<td>293 Mbps (MCS 6)</td>
<td>OFDM - 64 QAM</td>
<td>-68 dBm</td>
<td></td>
</tr>
<tr>
<td>325 Mbps (MCS 7)</td>
<td>OFDM - 64 QAM</td>
<td>-68 dBm</td>
<td></td>
</tr>
<tr>
<td>390 Mbps (MCS 8)</td>
<td>OFDM – 256 QAM</td>
<td>-64 dBm</td>
<td></td>
</tr>
<tr>
<td>433 Mbps (MCS 9)</td>
<td>OFDM – 256 QAM</td>
<td>-62 dBm</td>
<td></td>
</tr>
</tbody>
</table>

Note: Receiver sensitivity is the minimum signal needed to decode a packet at a certain data rate.

The above values are pure radio specifications and do not account for the gain of the single integrated antenna.

To achieve 802.11n/ac connectivity, it is recommended that the Cisco IP Phone 8861 and 8865 be within 100 feet of the access point.

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
### 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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 will passively scan DFS channels first before engaging in active scans of those channels. If 802.11d is not enabled, then the Cisco IP Phone 8861 and 8865 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 IP Phone 8861 and 8865.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>AR</td>
<td>Iceland</td>
<td>IS</td>
<td>Philippines</td>
<td>PH</td>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Austria</td>
<td>AT</td>
<td>India</td>
<td>IN</td>
<td>Poland</td>
<td>PL</td>
<td>Austria</td>
<td>AT</td>
</tr>
<tr>
<td>Bahrain</td>
<td>BH</td>
<td>Ireland</td>
<td>IE</td>
<td>Portugal</td>
<td>PT</td>
<td>Belgium</td>
<td>BE</td>
</tr>
<tr>
<td>Belgium</td>
<td>BE</td>
<td>Israel</td>
<td>IL</td>
<td>Puerto Rico</td>
<td>PR</td>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
<td>Japan</td>
<td>JP</td>
<td>Russian Federation</td>
<td>RU</td>
<td>Bulgaria</td>
<td>BG</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>BG</td>
<td>Korea</td>
<td>KR</td>
<td>Saudi Arabia</td>
<td>SA</td>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
<td>Latvia</td>
<td>LV</td>
<td>Serbia</td>
<td>RS</td>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
<td>Liechtenstein</td>
<td>LI</td>
<td>Singapore</td>
<td>SG</td>
<td>Colombia</td>
<td>CO</td>
</tr>
<tr>
<td>Colombia</td>
<td>CO</td>
<td>Lithuania</td>
<td>LT</td>
<td>Slovakia</td>
<td>SK</td>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
<td>Luxembourg</td>
<td>LU</td>
<td>Slovenia</td>
<td>SI</td>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
<td>Macau</td>
<td>MO</td>
<td>South Africa</td>
<td>ZA</td>
<td>Cyprus</td>
<td>CY</td>
</tr>
<tr>
<td>Cyprus</td>
<td>CY</td>
<td>Macedonia</td>
<td>MK</td>
<td>Spain</td>
<td>ES</td>
<td>Czech Republic</td>
<td>CZ</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>CZ</td>
<td>Malaysia</td>
<td>MY</td>
<td>Sweden</td>
<td>SE</td>
<td>Denmark</td>
<td>DK</td>
</tr>
<tr>
<td>Denmark</td>
<td>DK</td>
<td>Malta</td>
<td>MT</td>
<td>Switzerland</td>
<td>CH</td>
<td>Dominican Republic</td>
<td>DO</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>DO</td>
<td>Mexico</td>
<td>MX</td>
<td>Taiwan</td>
<td>TW</td>
<td>Ecuador</td>
<td>EC</td>
</tr>
<tr>
<td>Ecuador</td>
<td>EC</td>
<td>Monaco</td>
<td>MC</td>
<td>Thailand</td>
<td>TH</td>
<td>Egypt</td>
<td>EG</td>
</tr>
<tr>
<td>Egypt</td>
<td>EG</td>
<td>Montenegro</td>
<td>ME</td>
<td>Turkey</td>
<td>TR</td>
<td>Estonia</td>
<td>EE</td>
</tr>
<tr>
<td>Estonia</td>
<td>EE</td>
<td>Netherlands</td>
<td>NL</td>
<td>Ukraine</td>
<td>UA</td>
<td>Finland</td>
<td>FI</td>
</tr>
<tr>
<td>Finland</td>
<td>FI</td>
<td>New Zealand</td>
<td>NZ</td>
<td>United Arab Emirates</td>
<td>AE</td>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
<td>Nigeria</td>
<td>NG</td>
<td>United Kingdom</td>
<td>GB</td>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
<td>Norway</td>
<td>NO</td>
<td>United States</td>
<td>US</td>
<td>Gibraltar</td>
<td>GI</td>
</tr>
<tr>
<td>Gibraltar</td>
<td>GI</td>
<td>Oman</td>
<td>OM</td>
<td>Uruguay</td>
<td>UY</td>
<td>Greece</td>
<td>GR</td>
</tr>
<tr>
<td>Greece</td>
<td>GR</td>
<td>Panama</td>
<td>PA</td>
<td>Venezuela</td>
<td>VE</td>
<td>Hong Kong</td>
<td>HK</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>HK</td>
<td>Paraguay</td>
<td>PY</td>
<td>Vietnam</td>
<td>VN</td>
<td>Hungary</td>
<td>HU</td>
</tr>
</tbody>
</table>

**Note:** Compliance information is available on the Cisco Product Approval Status web site at the following URL: [http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH](http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH)
Bluetooth

The Cisco IP Phone 8861 and 8865 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 IP Phone 8861 and 8865.

Up to ten headsets can be paired, where the previously connected headset is given priority.

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 IP Phone 8861 and 8865 support the following Bluetooth profiles.

Hands-Free Profile (HFP)

With Bluetooth Hands-Free Profile (HFP) support, the following features can be available if supported by the Bluetooth headset.

- Ring
- Answer a call
- End a call
- Volume Control
- Last Number Redial
- Call Waiting
- Divert / Reject
- 3 way calling (Hold & Accept and Release & Accept)
- Speed Dialing

Phone Book Access Profile (PBAP)

Phone Book Access Profile (PBAP) support enables the exchange of phone book objects between devices.

For more information, refer to the documentation from the Bluetooth headset manufacturer.

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 IP Phone 8861 and 8865 currently support the following languages.

<table>
<thead>
<tr>
<th>Arabic</th>
<th>French</th>
<th>Polish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgarian</td>
<td>German</td>
<td>Portuguese</td>
</tr>
<tr>
<td>Catalan</td>
<td>Greek</td>
<td>Romanian</td>
</tr>
<tr>
<td>Chinese</td>
<td>Hebrew</td>
<td>Russian</td>
</tr>
<tr>
<td>Croatian</td>
<td>Hungarian</td>
<td>Serbian</td>
</tr>
<tr>
<td>Czech</td>
<td>Italian</td>
<td>Slovak</td>
</tr>
<tr>
<td>Danish</td>
<td>Japanese</td>
<td>Slovenian</td>
</tr>
<tr>
<td>Dutch</td>
<td>Korean</td>
<td>Spanish</td>
</tr>
<tr>
<td>English</td>
<td>Latvian</td>
<td>Swedish</td>
</tr>
<tr>
<td>Estonian</td>
<td>Lithuanian</td>
<td>Thai</td>
</tr>
<tr>
<td>Finnish</td>
<td>Norwegian</td>
<td>Turkish</td>
</tr>
</tbody>
</table>

The corresponding locale package must be installed to enable support for that language. English is the default language on the phone.

Download the locale packages from the Localization page at the following URL:
http://software.cisco.com/download/navigator.html?mdfid=278875240

Cisco 8865 Video Calls

The Cisco IP Phone 8865 supports video calling via a high-resolution color LCD and an integrated camera.

The Video Capabilities feature within Cisco Unified Communications Manager must be enabled for each Cisco IP Phone 8865 if wanting to participate in video calls.

The Cisco IP Phone 8865 is able to establish video calls with other Cisco 8865 endpoints, Cisco TelePresence Systems, and other video enabled endpoints.

WVGA 480p or HD 720p is the recommended video format to utilize unless higher-grade video is required when communicating with other capable endpoints.

For remote users, WVGA 480p or HD 720p should be the maximum video resolution enabled in the Cisco IP Phone 8865 configuration within Cisco Unified Communications Manager.

A Videoconferencing System with MCU running version 5.7 or later is required to provide videoconferencing capabilities.

H.264 is the protocol used for the video stream, where up to 30 fps (frames per second) are supported.
There is a separate stream for the audio session that utilizes one of the support audio codecs. The Cisco IP Phone 8865 supports video bandwidth adaption, where the video bit rate can be adjusted as necessary if the current network connection can not support higher video resolutions.

The following video formats are supported:

- QCIF (176 x 144)
- SIF (352 x 240)
- CIF (352 x 288)
- VGA (640 x 480)
- 240p (432 x 240)
- nHD 360p (640 x 360)
- WVGA 480p (800 x 480)
- HD 720p (1280 x 720)

**Accessories**

The following accessories are available for the Cisco IP Phone 8861 and 8865.

- Cisco IP Color Key Expansion Module for Cisco 8861 and 8865
- Headsets (Cisco 521, 522, 531, 532, 561, 562, 730)

**Other Accessories**

- Headsets
  - Jabra ([www.jabra.com](http://www.jabra.com))
  - Motorola ([www.motorola.com](http://www.motorola.com))
  - Plantronics ([www.plantronics.com](http://www.plantronics.com))

**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 IP Phone 8861 and 8865.

**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 IP Phone 8861 and 8865. 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 IP Phone 8861 and 8865 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 15 of the 24 possible channels.

Need to ensure there is at least 20 percent overlap with adjacent channels when deploying the Cisco IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 also meet the access point’s receiver sensitivity (required signal level for the current data rate).

<table>
<thead>
<tr>
<th>Channel ID</th>
<th>26</th>
<th>36</th>
<th>40</th>
<th>44</th>
<th>48</th>
<th>52</th>
<th>56</th>
<th>60</th>
<th>64</th>
<th>100</th>
<th>104</th>
<th>108</th>
<th>112</th>
<th>116</th>
<th>120</th>
<th>124</th>
<th>128</th>
<th>132</th>
<th>136</th>
<th>140</th>
<th>144</th>
<th>148</th>
<th>152</th>
<th>156</th>
<th>160</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center Freq. MHz</td>
<td>5180</td>
<td>5200</td>
<td>5220</td>
<td>5240</td>
<td>5260</td>
<td>5280</td>
<td>5300</td>
<td>5320</td>
<td>5340</td>
<td>5360</td>
<td>5380</td>
<td>5400</td>
<td>5420</td>
<td>5440</td>
<td>5460</td>
<td>5480</td>
<td>5500</td>
<td>5520</td>
<td>5540</td>
<td>5560</td>
<td>5580</td>
<td>5600</td>
<td>5620</td>
<td>5640</td>
<td>5660</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 IP Phone 8861 and 8865 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.
Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco IP Phone 8861 and 8865 should always have a signal of -67 dBm or higher when using 5 GHz or 2.4 GHz, while the Cisco IP Phone 8861 and 8865 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).

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

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
### 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 IP Phone 8861 and 8865 both have a single antenna, therefore it supports up to MCS 7 data rates for 802.11n (up to 150 Mbps) and up to MCS 9 data rates for 802.11ac (up to 433 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, VHT MCS 1 - MCS 9</td>
<td>6, 9 Mbps, VHT MCS 0</td>
</tr>
<tr>
<td>802.11a/n</td>
<td>12 Mbps</td>
<td>18-54 Mbps, HT MCS 1 - MCS 7 (HT MCS 8 - MCS 23)</td>
<td>6, 9 Mbps, HT MCS 0</td>
</tr>
</tbody>
</table>
802.11g/n    12 Mbps    18-54 Mbps, HT MCS 1 - MCS 7 (HT MCS 8 - MCS 23)    1, 2, 5.5, 6, 9, 11 Mbps, HT MCS 0
802.11b/g/n  11 Mbps    12-54 Mbps, HT MCS 1 - MCS 7 (HT MCS 8 - MCS 23)    1, 2, 5.5, 6, 9 Mbps, HT MCS 0
802.11a      12 Mbps    18-54 Mbps    6, 9 Mbps
802.11g      12 Mbps    18-54 Mbps    1, 2, 5.5, 6, 9, 11 Mbps
802.11b/g    11 Mbps    12-54 Mbps    1, 2, 5.5, 6, 9 Mbps
802.11b      11 Mbps    None    1, 2, 5.5 Mbps

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 (e.g. 12, 24, 54, MCS 1, MCS 4, MCS 7), 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 IP Phone 8861 and 8865 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 (e.g. Cisco 1602e, 2602e, 3502e, 3602e, and 3702e Series Access Points). 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 IP Phone 8861 or 8865 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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 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, video, 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 IP Phone 8861 and 8865 support the following wireless security features.

**WLAN Authentication**

- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- PEAP-GTC (Protected Extensible Authentication Protocol - Generic Token Card)
- PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2)
Cisco IP Phone 8861 and 8865

Wireless LAN Deployment Guide

- 802.11r / Fast Transition (FT)
- CCKM (Cisco Centralized Key Management)
- None

WLAN Encryption

- AES (Advanced Encryption Standard)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
- WEP (Wired Equivalent Protocol) 40/64 and 104/128 bit

Note: WPA3 is not supported.

802.1x-SHA2 key management is not supported.
CCMP256, GCMP128, and GCMP256 encryption ciphers are not supported.
Shared Key authentication is not supported.

The Cisco IP Phone 8861 and 8865 also support the following additional security features.

- Image authentication
- Device authentication
- File authentication
- Signaling authentication
- Secure Cisco Unified SRST
- Media encryption (SRTP)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)
- Secure profiles
- Encrypted configuration files
- Settings Access (can limit user access to configuration menus)

Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)

Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST) encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the access point and the Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS) or Cisco Identity Services Engine (ISE).

The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (the Cisco IP Phone 8861 and 8865) and the RADIUS server. The server sends an Authority ID (AID) to the client, which in turn selects the appropriate PAC. The client returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both endpoints now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must enable don the RADIUS server.

To enable EAP-FAST, a certificate must be installed on to the RADIUS server.

The Cisco IP Phone 8861 and 8865 currently support automatic provisioning of the PAC only, so enable Allow anonymous in-band PAC provisioning on the RADIUS server as shown below.

Both EAP-GTC and EAP-MSCHAPv2 must be enabled when Allow anonymous in-band PAC provisioning is enabled.

EAP-FAST requires that a user account be created on the authentication server.

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
If anonymous PAC provisioning is not allowed in the production wireless LAN environment then a staging RADIUS server can be setup for initial PAC provisioning of the Cisco IP Phone 8861 and 8865. This requires that the staging RADIUS server be setup as a slave EAP-FAST server and components are replicated from the product master EAP-FAST server, which include user and group database and EAP-FAST master key and policy info. Ensure the production master EAP-FAST RADIUS server is setup to send the EAP-FAST master keys and policies to the staging slave EAP-FAST RADIUS server, which will then allow the Cisco IP Phone 8861 and 8865 to use the provisioned PAC in the production environment where Allow anonymous in-band PAC provisioning is disabled. When it is time to renew the PAC, then authenticated in-band PAC provisioning will be used, so ensure that Allow authenticated in-band PAC provisioning is enabled. Ensure that the Cisco IP Phone 8861 and 8865 has connected to the network during the grace period to ensure it can use its existing PAC created either using the active or retired master key in order to get issued a new PAC. Is recommended to only have the staging wireless LAN pointed to the staging RADIUS server and to disable the staging access point radios when not being used.

**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 IP Phone 8861 or 8865.

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.
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-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 IP Phone 8861 and 8865.

For more information on Cisco Secure Access Control System (ACS) and Cisco Identity Services Engine (ISE), refer to the following links.


EAP and User Database Compatibility

The following chart displays the EAP and database configurations supported by the Cisco IP Phone 8861 and 8865.

<table>
<thead>
<tr>
<th>Database Type</th>
<th>EAP-FAST (Phase Zero)</th>
<th>EAP-TLS</th>
<th>PEAP-GTC</th>
<th>PEAP-MSCHAPv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ACS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows SAM</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows AD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LDAP</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ODBC (ACS for Windows Only)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LEAP Proxy RADIUS Server</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>All Token Servers</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
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>Interactive Video &amp; Audio for Video Calls</td>
<td>AF41 (34)</td>
<td>4</td>
<td>5</td>
<td>UDP 16384 - 32767</td>
</tr>
<tr>
<td>Call Control</td>
<td>CS3 (24)</td>
<td>3</td>
<td>4</td>
<td>TCP/UDP 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.

Note: Voice and interactive video frames will be marked with DSCP AF41 and WMM UP 5 for video calls.

For more information about TCP and UDP ports used by the Cisco IP Phone 8861 and 8865 and the Cisco Unified Communications Manager, refer to the Cisco Unified Communications Manager TCP and UDP Port Usage document at this URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/10_0_1/CUCM_BK_T537717B_00_tcp-port-usage-guide-100.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 IP Phone 8861 and 8865 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 IP Phone 8861 or 8865 establishes the call.

If the access point rejects the call and the Cisco IP Phone 8861 or 8865 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 IP Phone 8861 or 8865 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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 will send an ADDTS request during the roam to the new access point, which embedded in the reassociation request frame.

Traffic Classification (TCLAS)
Traffic Classification (TCLAS) helps to ensure that the access point properly classifies voice packets.
Without proper classification, voice packets will be treated as best effort, which will defeat the purpose of TSPEC and QoS in general.
TCP and UDP port information will be used to set the UP (User Priority) value.
The previous method of classification depends upon preservation of DSCP value throughout the network, where the DSCP value maps to a particular queue (BE, BK, VI, VO).
However, the DSCP values are not always preserved as this can be viewed as a security risk.
Using port based QoS policies is inadequate for CAPWAP based wireless LAN solutions as all data packets use the same UDP port (CAPWAP = UDP 5246) and the access point uses the outside QoS marking to determine which queue the packets should be placed in.
With TCLAS, DSCP preservation is not a requirement.
Call Admission Control must be enabled on the access point in order to enable TCLAS.
TCLAS will be negotiated within the ADDTS packets, which are used to request bandwidth in order to place or receive a call.

QoS Basic Service Set (QBSS)
There are three different versions of QoS Basic Service Set (QBSS) that the Cisco IP Phone 8861 and 8865 support.
The first version from Cisco was on a 0-100 scale and was not based on clear channel assessment (CCA), so it does not account for channel utilization, but only the 802.11 traffic traversing that individual access point’s radio. So it does not account for other 802.11 energy or interferers using the same frequencies.
QBSS is also a part of 802.11e, which is on a 0-255 scale and is CCA based. So this gives a true representation on how busy the channel is. The max threshold is also defined on the client side, which is set to 105.
The second version from Cisco is based on the 802.11e version, but allows the default max threshold of 105 to be optionally configured.
Each version of QBSS can be optionally be configured on the access point.

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**

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

**Enable DSCP trust for Cisco Access Points**

```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:

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

**Roaming**

The Cisco IP Phone 8861 and 8865 default to Auto for the 802.11 mode, which allows the Cisco IP Phone 8861 and 8865 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. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.
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.

The Cisco IP Phone 8861 and 8865 support 802.11r (FT) with WPA2 (AES) or WPA2-PSK (AES) and CCKM with WPA2 (AES or TKIP) and WPA (TKIP or AES).

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Roaming Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA/WPA2 Personal</td>
<td>150 ms</td>
</tr>
<tr>
<td>WPA/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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 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).

Roaming based on RSSI may not occur if the current signal has met the strong RSSI threshold.

**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. WPA and WPA2 introduce 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 IP Phone 8861 and 8865 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-FAST</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>PEAP-GTC</td>
<td>WPA2</td>
<td>AES</td>
</tr>
<tr>
<td>802.11r (FT)</td>
<td>PEAP-MSCHAPv2</td>
<td>WPA2</td>
<td>AES</td>
</tr>
<tr>
<td>CCKM</td>
<td>EAP-FAST</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
<tr>
<td>CCKM</td>
<td>EAP-TLS</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
<tr>
<td>CCKM</td>
<td>PEAP-GTC</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
<tr>
<td>CCKM</td>
<td>PEAP-MSCHAPv2</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
</tbody>
</table>

**Note:** If deploying the Cisco IP Phone 8861 or 8865 into an environment where other Wi-Fi phone models exist but those Wi-Fi phone models do not support 802.11r (FT), then should be able to use that same pre-existing SSID for the Cisco IP Phone 8861 or 8865, but is recommended to enable 802.11r (FT) utilizing the Over the Air method on top of the other pre-existing key management types (e.g. 802.1x, CCKM, or 802.1x + CCKM); assuming the other Wi-Fi phone models can interoperate in an 802.11r (FT) enabled network while not utilizing 802.11r (FT).

**Interband Roaming**

The Cisco IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 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 power supply (CP-PWR-CUBE-4=) is required to enable the Cisco IP Phone 8861 or 8865 for wireless LAN mode, as there is no internal battery.
Wireless LAN is automatically disabled temporarily when Ethernet is connected to the Cisco IP Phone 8861 or 8865, but will be automatically re-enabled once Ethernet is disconnected if Wireless LAN was enabled previously.

The Cisco IP Phone 8861 and 8865 primarily use active mode (no Wi-Fi power save) when in idle or on call.

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

**Delivery Traffic Indicator Message (DTIM)**

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

Since the Cisco IP Phone 8861 and 8865 use active mode, the DTIM period will not be used to schedule wake up periods to check for broadcast and multicast packets as well as any unicast packets.

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 IP Phone 8861 or 8865 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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 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 Only Calls**

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

<table>
<thead>
<tr>
<th>Max # of Streams</th>
<th>Audio Codec</th>
<th>Audio Bit Rate</th>
<th>802.11 Mode</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>6 Mbps</td>
</tr>
<tr>
<td>20</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>12 Mbps</td>
</tr>
<tr>
<td>27</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>802.11a/n/ac or 802.11g/n + Bluetooth Disabled</td>
<td>24 Mbps or higher</td>
</tr>
</tbody>
</table>
Video Calls

Video calls over Wireless LAN will significantly reduce the potential call capacity.

Below lists the maximum number of video calls (single bi-directional voice and video stream) supported per access point / channel for each video bit rate.

If there are two Cisco 8865 endpoints communicating with each other, then that is two bi-directional voice and video streams.

<table>
<thead>
<tr>
<th>Max # of Video Calls</th>
<th>802.11 Mode</th>
<th>802.11 Data Rate</th>
<th>Audio Codec</th>
<th>Audio Bit Rate</th>
<th>Video Type</th>
<th>Video Resolution</th>
<th>Video Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-13</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12-54 Mbps</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>nHD 360p</td>
<td>640 x 360</td>
<td>400 Kbps</td>
</tr>
<tr>
<td>5-13</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>MCS 1 - MCS 7 (20 MHz Channels)</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>nHD 360p</td>
<td>640 x 360</td>
<td>400 Kbps</td>
</tr>
<tr>
<td>8-16</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>MCS 1 - MCS 7 (40 MHz Channels)</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>nHD 360p</td>
<td>640 x 360</td>
<td>400 Kbps</td>
</tr>
<tr>
<td>3-9</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12-54 Mbps</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>VGA</td>
<td>640 x 480</td>
<td>700 Kbps</td>
</tr>
<tr>
<td>3-9</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>MCS 1 - MCS 7 (20 MHz Channels)</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>VGA</td>
<td>640 x 480</td>
<td>700 Kbps</td>
</tr>
<tr>
<td>4-12</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>MCS 1 - MCS 7 (40 MHz Channels)</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>VGA</td>
<td>640 x 480</td>
<td>700 Kbps</td>
</tr>
<tr>
<td>2-8</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12-54 Mbps</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>HD 720p</td>
<td>1280 x 720</td>
<td>1000 Kbps</td>
</tr>
<tr>
<td>2-8</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>MCS 1 - MCS 7 (20 MHz Channels)</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>HD 720p</td>
<td>1280 x 720</td>
<td>1000 Kbps</td>
</tr>
<tr>
<td>3-11</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>MCS 1 - MCS 7 (40 MHz Channels)</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>HD 720p</td>
<td>1280 x 720</td>
<td>1000 Kbps</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.
The Cisco IP Phone 8861 and 8865 utilize active mode primarily, but 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 IP Phone 8861 and 8865 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 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**

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
• 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 IP Phone 8861 and 8865 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.

With the current releases, Maximum Allowed Clients can be configured.

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.

With the current releases, **Maximum Allowed Clients** can be configured.

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.

For releases prior to 7.2.103.0, **ClientLink** can be enabled globally via the 802.11 Global Parameters section or on individual access points via the access point’s 802.11 radio configuration page.

As of release 7.2.103.0, **ClientLink** is no longer configurable via the Cisco Wireless LAN Controller’s web interface and is only configurable via command line.

With releases 7.2.103.0 and later 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 IP Phone 8861 and 8865 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)**

Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets. Low latency MAC feature is not supported for 1148/1160/1530 platforms if more than 3 data rates are enabled.
**Power Constraint** should be left un-configured or set to 0 dB as DTPC will be used by the Cisco IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 support HT MCS 0 - MCS 7 and VHT MCS 0 - MCS 9 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.

It is recommended to disable MCS 0.
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 IP Phone 8861 and 8865.

**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 IP Phone 8861 and 8865 requirements.

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.

```bash
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
config 802.11a 11nSupport a-mpdu tx priority 6 disable
config 802.11a 11nSupport a-mpdu tx priority 7 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
config 802.11b 11nSupport a-mpdu tx priority 6 disable
config 802.11b 11nSupport a-mpdu tx priority 7 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.
Rx Sop Threshold

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

WLAN Settings

It is recommended to have a separate SSID for the Cisco IP Phone 8861 and 8865.

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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 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, 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.
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.

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.
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 IP Phone 8861 and 8865 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-WMM clients must utilize the same SSID as the Cisco IP Phone 8861 and 8865, then ensure the WMM policy is set to **Allowed**.

Enabling WMM will enable the 802.11e version of QBSS. There are also the **7920 Client CAC** and **7920 AP CAC** options, where **7920 Client CAC** will enable Cisco version 1 and **7920 AP CAC** enables Cisco version 2.
Configure **Enable Session Timeout** as necessary per your requirements. It is recommended to either disable the session timeout or extend the timeout (e.g. 24 hours / 86400 seconds) to avoid possible interruptions during audio calls. If disabled it will avoid any potential interruptions altogether, but enabling session timeout can help 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, video, 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.

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.

**Media Session Snooping** can be enabled to utilize SIP CAC when the access point is in local mode.

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.

802.11k and 802.11v are not supported, therefore should be disabled.
### Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide

#### WLANs

**General**
- Allow AAA Override: Enabled
- Coverage Hole Detection: Enabled
- Enable Session Timeout: 3600 (Session Timeout (secs))
- Arisen IE: Enabled
- Diagnostic Channel: Enabled
- Override Interface ACL: IPv4 None, IPv6 None
- Layer2 ACL: None
- URL ACL: None
- P2P Blocking Action: Disabled
- Client Exclusion: Enabled
- Maximum Allowed Clients: 200
- Static IP Tunneling: Enabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients: 200

**Advanced**

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

#### WLANs

**General**
- Maximum Allowed Clients: 200
- Clear HotSpot Configuration: Enabled
- Client user life time (1-1000000): Enabled
- Client user life threshold (1-1000000): 0
- Kalahari HotSpot: Enabled
- 11ac MU-MIMO: Enabled
- WGB MIB: Enabled

**Advanced**

- **Off Channel Scanning Deny**
  - Scan Defor Priority: 0 1 3 4 5 6 7
  - Scan Defor Time (milliseconds): 1000

- **FlexConnect**
  - FlexConnect Local Switching: Enabled

- **Voice**
  - Media Session Snapback: Enabled
  - Re-anchor Roamed Voice Clients: Enabled
  - QoS based CAC Policy: Enabled

- **Radio Client Profiling**
  - DHCP Profiling: Enabled
  - HTTP Profiling: Enabled

- **Local Client Profiling**
  - DHCP Profiling: Enabled
  - HTTP Profiling: Enabled

- **Universal AP Admin**
  - 11v BSS Transition Support
    - BSS Transition: Enabled
    - Optimized Roaming Bisassociation (0 to 40 TTIE): 40
    - BSS Max MM Service: Enabled
    - Directly Multicast Service: Enabled

- **Tunneling**
  - Tunnel Profile: None
  - 802.1x: None

---

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide

57
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.

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.

SIP CAC can help ensure that downstream voice frames are prioritized correctly when a client does not support TSPEC.

Load based CAC logic is utilized with SIP CAC, so all 802.11 traffic and energy on the channel is accounted for to determine available bandwidth.

The access point has different methods for Call Admission Control when using SIP CAC depending on whether the client uses TCP or UDP for SIP communications.

If the client uses TCP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN and will not forward the SIP frames upstream or downstream if there is not bandwidth available for the new voice stream. This could potentially result in loss of registration to the Cisco Unified Communications Manager.

If the client uses UDP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN and will sent a 486 busy message to the client, which in turn can be interpreted as a **Network Busy** message and the client could either roam to another access point or simply terminate the call setup for that session.

If the Cisco IP Phone 8861 and 8865 uses TCP for SIP communications and the channel is busy where another call can not be allowed, then the Cisco IP Phone 8861 and 8865 could potentially lose registration to the Cisco Unified Communications Manager if SIP CAC is enabled.

---

**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 IP Phone 8861 and 8865 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. 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 (Auto) 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

<table>
<thead>
<tr>
<th>QoS Profile Name</th>
<th>platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>For Voice Applications</td>
</tr>
</tbody>
</table>

#### 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 2
- Unicast Default Priority: voice 2
- Multicast Default Priority: voice 2

### Wired QoS Protocol

- Protocol Type: 802.1p 1
- 802.1Q Tag: 5

* The value zero (0) indicates the feature is disabled.
Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide

Wireless

- Access Points
  - All APs
  - Radios
  - 802.11a/n/ac
  - 802.11b/g/n
  - Dual-Band Radios
  - Global Configuration

- Advanced
  - Mesh
  - RF Profiles
  - FlexConnect Groups
  - FlexConnect ACLs
  - 802.11a/n/ac
  - 802.11b/g/n
  - Media Stream
  - Application Visibility
  - And Control
  - Country
  - Timers
  - Netflow

- QoS
  - Profiles
  - Roles

Edit QoS Profile

QoS Profile Name: B22

Description: For Video 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: video 1
- Unicast Default Priority: video 2
- Multicast Default Priority: video 3

Wired QoS Protocol

- Protocol Type: 802.1p
- 802.1p Tag: 4

* The value zero (0) indicates the feature is disabled
## Edit QoS Profile

### QoS Profile Name
- **Profile Name**: diver

### Description
- Description: For Best Effort

### 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

<table>
<thead>
<tr>
<th>QoS Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Priority</td>
<td>besteffort</td>
</tr>
<tr>
<td>Unicast Default Priority</td>
<td>besteffort</td>
</tr>
<tr>
<td>Multicast Default Priority</td>
<td>besteffort</td>
</tr>
</tbody>
</table>

### Wired QoS Protocol

<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1p Tag</td>
<td>2</td>
</tr>
</tbody>
</table>

* The value zero (0) indicates the feature is disabled
Note: The 802.1p tag mappings were changed with the 7.5.102.0 release.
Prior to the 7.5.102.0 release, Platinum = 6, Gold = 5, Silver = 3, Bronze = 1.

Advanced Settings

Advanced EAP Settings

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 or WPA/WPA2, 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.
If using WPA/WPA2 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 WPA/WPA2, 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

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

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
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 IP Phone 8861 and 8865 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.

(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id>

To confirm the change, enter `show wlan <WLAN id>`, where the following will be displayed.

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

**TKIP Countermeasure Holdoff Time**
TKIP countermeasure mode can occur if the access point receives two Message Integrity Check (MIC) errors within a 60 second period. When this occurs, the access point will de-authenticate all TKIP clients associated to that 802.11 radio and holdoff any clients for the countermeasure holdoff time (default = 60 seconds).

To change the TKIP countermeasure holdoff time on the Cisco Wireless LAN Controller, telnet or SSH to the controller and enter the following command specifying the number of seconds and WLAN ID.

(Cisco Controller) >config wlan security tkip hold-down <nseconds> <wlan-id>

To confirm the change, enter `show wlan <WLAN id>`, where the following will be displayed.

Tkip MIC Countermeasure Hold-down Timer...... 60

**Rogue Policies**
Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
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
- 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 IP Phone 8861 and 8865 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.

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 IP Phone 8861 and 8865 support HT MCS 0 - MCS 7 and VHT MCS 0 - MCS 9 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 IP Phone 8861 and 8865 to control the transmission power.

**Channel Switch Status** and **Smart DFS** should be **Enabled**.

---

### 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 IP Phone 8861 and 8865 to control the transmission power.

**Channel Switch Status** and **Smart DFS** should be **Enabled**.

---

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
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.

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
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**
It is recommended to have a separate SSID for the Cisco IP Phone 8861 and 8865. 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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865 roaming experience.

---

**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 IP Phone 8861 and 8865 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 IP Phone 8861 and 8865, 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.
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**.

802.11k and 802.11v are not supported, therefore should be disabled.

**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.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Edit Policy Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td><strong>Access Policies</strong></td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td><strong>Switching Policy</strong></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Voice</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td><strong>Enter Description</strong></td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td><strong>ENABLED</strong></td>
</tr>
<tr>
<td><strong>Passive Client</strong></td>
<td><strong>DISABLED</strong></td>
</tr>
<tr>
<td><strong>EAP</strong></td>
<td><strong>DISABLED</strong></td>
</tr>
<tr>
<td><strong>CTS Policy</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Inline Tagging</strong></td>
<td></td>
</tr>
<tr>
<td><strong>802.11 Enforcement</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Default SID</strong></td>
<td><strong>2-85519</strong></td>
</tr>
<tr>
<td><strong>WLAN Local Profiling</strong></td>
<td></td>
</tr>
<tr>
<td><strong>WLAN ACL</strong></td>
<td><strong>IPv4 ACL</strong></td>
</tr>
<tr>
<td><strong>IPv6 ACL</strong></td>
<td><strong>Search or Select</strong></td>
</tr>
<tr>
<td><strong>URL Filters</strong></td>
<td><strong>Search or Select</strong></td>
</tr>
<tr>
<td><strong>Pre Auth</strong></td>
<td><strong>Search or Select</strong></td>
</tr>
<tr>
<td><strong>Post Auth</strong></td>
<td><strong>Search or Select</strong></td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td></td>
</tr>
<tr>
<td><strong>VLAN Group</strong></td>
<td><strong>VLAN1000</strong></td>
</tr>
<tr>
<td><strong>Multicast VLAN</strong></td>
<td><strong>Enter Multicast VLAN</strong></td>
</tr>
</tbody>
</table>

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
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 either disable the session timeout (set to 0) or extend the timeout (e.g. 24 hours / 86400 seconds) to avoid possible interruptions during audio calls. If disabled it will avoid any potential interruptions altogether, but enabling session timeout can help 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 IP Phone 8861 and 8865 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.

SIP CAC can help ensure that downstream voice frames are prioritized correctly when a client does not support TSPEC.

Load Based CAC logic is utilized with SIP CAC, so all 802.11 traffic and energy on the channel is accounted for to determine available bandwidth.

The access point has different methods for Call Admission Control when using SIP CAC depending on whether the client uses TCP or UDP for SIP communications.

If the client uses TCP for SIP, then the access point will snoop the SIP packets when call snooping is enabled on the WLAN and will not forward the SIP frames upstream or downstream if there is not bandwidth available for the new voice stream. This could potentially result in loss of registration to the Cisco Unified Communications Manager.

If the client uses UDP for SIP, then the access point will snoop the SIP packets when call snooping is enabled on the WLAN and will sent a 486 busy message to the client, which in turn can be interpreted as a Network Busy message and the client could either roam to another access point or simply terminate the call setup for that session.

If the Cisco IP Phone 8861 and 8865 uses TCP for SIP communications and the channel is busy where another call can not be allowed, then the Cisco IP Phone 8861 and 8865 could potentially lose registration to the Cisco Unified Communications Manager if SIP CAC is enabled.

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 EAP Settings

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

If using 802.1x or WPA/WPA2, 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.
If using WPA/WPA2 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 WPA/WPA2, 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 datetime msec
service timestamps log datetime 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 selfsigned 01
03B20330 30B20218 A0030201 02020101 300D0609 2A864886 F70D0101 05050003
3112F30 2D060355 04031326 494F532D 53656C66 C2D536976 6E65642D 43656774
69666963 61746565 2D3331330 36383320 30313301E 170D3139 303733130 30343236
35375A17 0D323030 30313310 30373030 303A3031 312F302D 06035504 03132649
4F532D35 65C662D 5369676E 65642D43 65727069 6E656365 74655233 31313303
38323030 31308201 22300D06 092A8648 86F70D01 01010590 0382010F 00308201
0A028201 0100B74F D6A0DE5D DBF2C2DD 25196AAB1 86C8BD48 3AAAF455 C4E7D559
41A10FE1 87EC742C C5014113 9A0FD83A F490EA64 DF68A513 AA690C4 810A9FED
870309EA 781EB999 882F737E EC79D592 DEC6C126 A5FB5666 905C24D8 B204CD4
68B236D6 7E9A07F3 B043D632 EEDF4CAF D306C303 843493AA F44126E3 A07DE905
6B6C5BB B C8E6C9E6 45D79F62 B81FF68C B44FA7A C AEDB8A9E 55B75096 E476BC3
D5B90090 1A0C7CD0 910B6C63 920E9666 39EC3702 387757F1 C26F0BB5 89D4733D
FED71CF4 33020C77 0F721B21 5578C850 590BC846 7CB79469 A51CEBA5 96EA876D
DDB8244A 96EDA13 DD83B0FA 3221A839 5F985C86 F2C57B78 8E6608B6 18A346D2
03D3B68 26BF0203 010001A3 53305130 0F603555 1D130101 FF040530 030101FF
301F0603 551D2304 18301660 141B4651 019E0AEC 86E4EB65 C0E023ED 60F6062C
0F301D06 03551DOE 04160414 1B465101 9E0AEC8E 64EB65C0 E023ED60 F6062C0F
300D0609 AB864886 F70D0101 05050003 82010100 3319F2A7 3E85859F 85C08F28
67553F93 408DCC6E EFE2704E C142766C 5FEE0E97 0AFD0EAE 816CBE42 60FFBC26
6E411C57 3F1AB3F8 2F1E9959 AED26C86 2C0B59B9 692C72C B5859A15 999916F8
699587DC 9440E77C FF685698 2F9A5CEC 9315F1AA 357E8777 7AE1E37C 5FCD7E46
EB3ADC4 3F22A9E0 EA35EBB8 E55B8721 0E8756A1 6A6E3A6A C7FD8E64 6C3722C
F90919C9 DE675E5C 301FF83A 0593ACE6 4A469209 CAAEC53F 5102FDD3 AE378090
46282E00 BCF65EB7 4C257EFD 57986F82 B6DD8336 CEA82E27 63B4C6C5 F92945E8
2A9F9A95 2AD21793 50FF7987 F4A79079 6FE92AE5 66DFC8B8 14021984 0B1E3F6E
45D57889 B04883C5 114D79AD FBB2CAFF 587ECF9D
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 3697363 6F312030 0E060355 04031317 43697363
6F204C69 63656E73 696E6762 526F6F74 20434130 1E170D31 33035333 30319343
3834375 A170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
3697363 6F312030 0E060355 04031317 43697363 6F204C69 63656E73 696E6762
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212A147 C6558D7D 947113830D 8711441E 1AAFF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5B85C5BD 0CFEBEA3 7009A87F 0B256EE
4AAEAE80D DB6FD13C 90B1F0D8 FFC69C96 6FA68957 A2617DE7 104F43E5 EA2956AC
73903AE3 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 9B871886
5E69491 20F320E7 94EB71D7 AE3BCCSS F10684CF 4BC8E00F 539BA42B 42C68B7
C7479096 B4CB2D62 EA2F505D C7B062A4 68119958 E8250FC4 5D5F5FB8 8F72D191
C55FD761 6F9A44CD 3D992327 ABBB03BD 4E6D0709 7CBADF80 DF5F4368 9513E5E4
DFC7C6CF 04DD77FD 02030100 01A3423D 40300E06 03551DF0 010FF04 0430201
6300F06 03551D13 010FF04 05300301 01FF301D 0630551D 0E041604 144DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 09A26848 86F7D001 010B0500
03820100 050702F4 D9392A66 8602519F E838AE5C 6D4DF6B0 49631C78 240DA905
6D4EDCDE FF4FD2E2B 77FC460E CD636FDB DD490B3E 3A05673AB 0903D3B1 6C9E3D8B
D9898787F4 E040CB9E 1AEC0C32 2189BB5C 8FA85686 C98B646 5575B146 8D6C66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF746F 152E99B7 B10CBF98 E973DE7F 5BDDE8B6 C71E3B49 1675308B
5FB0DA06 B92AFAF9 49E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80D8C61D6 B6ACECA EEBB77F9 8428787B 35202CDC 60E4616A B623C3BD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 93E235B5 8862F8AE 0275156F 719BB2F0
D697DF7F 28
quit
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 wifi-calling
!
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 aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile
wireless management interface Vlan310
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
service-policy input silver-up
session-timeout 86400
vlan VLAN0400
no shutdown
wireless profile policy Voice
ipv4 flow monitor wireless-avc-basic input
service-policy input platinum-up
session-timeout 86400
vlan VLAN0500
no shutdown
wireless profile policy default-policy-profile
description "default policy profile"
vlan default
no shutdown
wireless tag site default-site-tag
description "default site tag"
wireless tag policy default-policy-tag
description "default policy-tag"
wireless tag rf default-rf-tag
description "default RF tag"
wireless rf-network RCDN6-VoWLAN3
media-stream multicast-direct
wireless multicast
wlan Data 2 data
load-balance
security dot1x authentication-list authentication_dot1x_day0
no shutdown
wireless Voice 1 voice
no assisted-roaming neighbor-list
no bss-transition
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
coverage voice rssi threshold -90
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
tax-power min 7
tax-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>
ntp ip 10.115.162.212
ssh
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 Claim 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.

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

SSID Configuration
Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
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 IP Phone 8861 and 8865; 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 IP Phone 8861 and 8865 will be configured to use for 802.1x authentication.

Note: Cisco Meraki access points do not support EAP-FAST.

On the Wireless > Configure > Access control page, recommend to enable Bridge mode, where the Cisco IP Phone 8861 and 8865 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 Meraki MS Switches, reference the Cisco Meraki MS Switch VoIP Deployment Guide.


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
```

On the **Wireless > Configure > Access control** page, the frequency band for the SSID to be used by the Cisco IP Phone 8861 and 8865 can be configured as necessary.

It is recommended to select **5 GHz band only** to have the Cisco IP Phone 8861 and 8865 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-Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
configurable.

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

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

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, configure what radio transmit power and channel settings to use.

For the Radio power setting, it is recommended to select Enable power reduction on nearby APs as co-channel interference can be potentially reduced. If wanting to use maximum radio power, then select Always use 100% power.

Can select whether to enable use of DFS channels or not via the Auto channel option.

The Default 5 GHz channel width is set to 80 MHz by default and that channel width will be utilized if the access point is 802.11ac capable. The Default 5 GHz channel width can also be set to use 20 MHz or 40 MHz.

It is recommended to utilize the same channel width for all access points.
If **Channel width** is set to **Auto** for an access point, then that access point will use the value specified for **Default 5 GHz channel width** if applicable for that access point model.

The channel width can also be configured on a per access point basis overriding the default.

2.4 GHz radios utilize 20 MHz channel width and can not be configured for 40 MHz channels.

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

When using Cisco Meraki access points it is recommended to select **Auto** for the channel and transmit power.

When **Auto** is selected for 2.4 GHz channels, only channels 1, 6, and 11 will be utilized.

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.

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 account for the access points that have static channel assignments.

---

**Note:** Cisco Meraki access points do not support Dynamic Transmit Power Control (DTPC), therefore the Cisco IP Phone 8861 and 8865 will utilize the maximum transmit power supported for the current channel and data rate.
Traffic Shaping

On the **Wireless > Configure > Firewall & traffic shaping** page, traffic shaping rules can be defined.

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).

Monitoring Clients

On the **Network-wide > Monitor > Clients** page, client information and statistics can be displayed.
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 IP Phone 8861 and 8865 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.

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**.
**Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide**

### Network Interfaces: Radio1-802.11ac Settings

- **Enable Radio:**
  - Enable
  - Disable

- **Current Status (Software/Hardware):**
  - Enabled

- **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-Client:**
  - Enable
  - Disable (1-255)

- **11r Configuration:**
  - Enable
  - Disable
  - Over-air
  - Over-ds
  - Reassociation-time: (20-1200 ms)

- **Data Rates:**
  - 6.0Mbit/sec
  - 9.0Mbit/sec
  - 12.0Mbit/sec
  - 18.0Mbit/sec
  - 24.0Mbit/sec
  - 36.0Mbit/sec
  - 48.0Mbit/sec
  - 54.0Mbit/sec
  - 80.1-2Mbit/sec
  - 11.1-2Mbit/sec
  - 12.1-2Mbit/sec
  - 18.1-2Mbit/sec
  - 24.1-2Mbit/sec
  - 36.1-2Mbit/sec
  - 48.1-2Mbit/sec
  - 54.1-2Mbit/sec
  - 80.2-2Mbit/sec
  - 11.2-2Mbit/sec
  - 12.2-2Mbit/sec
  - 18.2-2Mbit/sec
  - 24.2-2Mbit/sec
  - 36.2-2Mbit/sec
  - 48.2-2Mbit/sec
  - 54.2-2Mbit/sec
  - 80.3-2Mbit/sec
  - 11.3-2Mbit/sec
  - 12.3-2Mbit/sec
  - 18.3-2Mbit/sec
  - 24.3-2Mbit/sec
  - 36.3-2Mbit/sec
  - 48.3-2Mbit/sec
  - 54.3-2Mbit/sec
  - 80.4-2Mbit/sec
  - 11.4-2Mbit/sec
  - 12.4-2Mbit/sec
  - 18.4-2Mbit/sec
  - 24.4-2Mbit/sec
  - 36.4-2Mbit/sec
  - 48.4-2Mbit/sec
  - 54.4-2Mbit/sec

---

*Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide*
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 IP Phone 8861 and 8865. 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 IP Phone 8861 and 8865 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><strong>WPA Pre-shared Key:</strong></th>
<th></th>
<th>ASCII</th>
<th>Hexadecimal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>11w Configuration:</strong></td>
<td>Disable</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11w Association-comeback:</strong></td>
<td>1900</td>
<td>(1000-20000)</td>
<td></td>
</tr>
<tr>
<td><strong>11w Saquery-retry:</strong></td>
<td>100</td>
<td>(100-500)</td>
<td></td>
</tr>
</tbody>
</table>

**IOS Client MFP**

- **Enable Client MFP on this SSID:** Optional

**AP Authentication**

- **Credentials:** <NONE>  Define Credentials
- **Authentication Methods Profile:** <NONE>  Define Authentication Methods Profiles

**Accounting Settings**

- **Enable Accounting**
  - Use Defaults  Define Defaults
  - Customize
    - Priority 1: <NONE>
    - Priority 2: <NONE>
    - Priority 3: <NONE>

**Rate Limit Parameters**

- **Limit TCP:**
  - Input: Rate:  Burst-Size: (0-50000)
  - Output: Rate:  Burst-Size: (0-50000)

- **Limit UDP:**
  - Input: Rate:  Burst-Size: (0-50000)
  - Output: Rate:  Burst-Size: (0-50000)

**General Settings**

- **Advertise Extended Capabilities of this SSID**
- **Advertise Wireless Provisioning Services (WPS) Support**
- **Advertise this SSID as a Secondary Broadcast SSID**

- **Enable IP Redirection on this SSID**

  **IP Address:** DISABLED
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.

```
dot11 ssid voice
  vlan 3
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2 dot1 lr
  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.
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 (SIP) 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

Proxy ARP can optimize idle battery life, by answering any ARP requests on behalf of the phone.

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.
Advanced Settings

TKIP Countermeasure Holdoff Time

TKIP countermeasure mode can occur if the access point receives two Message Integrity Check (MIC) errors within a 60 second period. When this occurs, the access point will de-authenticate all TKIP clients associated to that 802.11 radio and holdoff any clients for the countermeasure holdoff time (default = 60 seconds).

To change the TKIP countermeasure holdoff time on the Cisco Autonomous Access Point, telnet or SSH to the access point and enter the following command specifying the number of seconds and WLAN ID.

```
Interface dot11radio X
    countermeasure tkip hold-time <nseconds>
```

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 05050030
    30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
    69666966 6174652D 30333031 313233343234303817 0D3136303830333233385A170D
    32303031 30303030 5A303031 2E302C06 03550403 1325494F
    532D5365 6C666965 66643038333233303533385A170D 32303031 30303030 5A303031 2E302C06
    03550403 1325494F
    33323430 81F930F0D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
    CB155DD1 3421B13F CD121F42 7A62D9F5 38EBC966 4420F38A 38DFAFF2 D43CD3B9
    5F5A1B75 7910F9F5 6E9EDEFA 730942C7 17DC4C8C E5AE3E49 0AF79419 0BEF34BC
    5DEB4E2 FF2978CB C34D5AAE ED1DFB58 C7BF6592 61C1AD25 3EF87205 15E58C2
    05A32B1A 7F08FAEA 5DA2BFA7 95E56C60 2C2229C7 024A91D7 A4FEB50B 5425357F
    02030100 01A35330 51300F06 03551D13 01010004 05300301 01FF301F 0603551D
    23041830 16A0184FC 2F66CF0E E0380A40 11381459 5D596E3E A684DA30 1D060355
    1D0E0416 0414FC2E 66CF0EE0 380A4011 3814595D 596E3EA6 84DA300D 06092A86
    4886F70D 01010505 00038181 0053F55B 5EBB1FE2 C849BC45 47D0E710 0200404E
    A8B174BC A46EB56A 857166C3 B9FD71DF 726F5AFD C804A671 16BD35A2 4F39AFD7
    0BD24F71 BAF916AC E984343C A54B7395 E5D15237 8897D436 A150BFB2 DC23E8D3
username <REMOVED> privilege 15 password <REMOVED>
!
class-map match-all _class_Voice0
  match ip dscp cs3
class-map match-all _class_Voice1
  match ip dscp af41
class-map match-all _class_Voice2
  match ip dscp ef
!
policy-map Voice
  class _class_Voice0
    set cos 4
  class _class_Voice1
    set cos 5
  class _class_Voice2
    set cos 6
!
bridge irb
!
interface Dot11Radio0
  no ip address
  shutdown
  antenna gain 0
  traffic-metrics aggregate-report
  stbc
  mbssid
  speed  basic-12.0 18.0 24.0 36.0 48.0 54.0 m1. m2. m3. m4. m5. m6. m7. m8. m9. m10. m11. m12. m13. m14. m15. m16. m17. m18. m19. m20. m21. m22. m23.
  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
speed basic-12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9. m10. m11. m12. m13. m14. m15. m16. m17. m18. m19. m20. m21. m22. m23. a1ss9 a2ss8 a3ss9
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 ntlhash 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
!
wlccep ap username wds password 7 <REMOVED>
wlccep ap wds ip address 10.9.0.9
wlccep authentication-server infrastructure method_WDS
wlccep authentication-server client eap method_Clients
wlccep authentication-server client leap method_Clients
wlccep wds priority 255 interface BVI1
Configuring Cisco Call Control

Cisco Unified Communications Manager

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

When adding the Cisco IP Phone 8861 or 8865 to the Cisco Unified Communications Manager it must be provisioned using the Ethernet MAC address as the Wireless LAN MAC is used for Wi-Fi connectivity only.

The Ethernet MAC address of the Cisco IP Phone 8861 or 8865 can be found by navigating to Applications > Admin settings > Network setup > Ethernet setup.

Device Pools

When creating a new Cisco IP Phone 8861 or 8865, 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 IP Phone 8861 or 8865, a **Phone Button Template** must be configured. Custom phone button templates can be created with the option for many different features, which can then be applied on a device or group level.
Security Profiles

When creating a new Cisco IP Phone 8861 or 8865, 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 IP Phone 8861 and 8865 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.
SIP Profiles

When creating a new Cisco IP Phone 8861 or 8865, a **SIP Profile** must be configured.

It is recommended to create a custom SIP Profile for the Cisco IP Phone 8861 and 8865 EX (do not use the **Standard SIP Profile** or **Standard SIP Profile for Mobile Device**).

To create a custom SIP Profile for the Cisco IP Phone 8861 or 8865, 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)

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
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 8861 SIP Profile
<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<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 URL</td>
<td>x-cisco-serviceurl-pickup</td>
</tr>
<tr>
<td>Call Pickup Group URL</td>
<td>x-cisco-serviceurl-pickup</td>
</tr>
<tr>
<td>Call Pickup Group Other URL</td>
<td>x-cisco-serviceurl-pickup</td>
</tr>
<tr>
<td>Meet Me Service URL</td>
<td>x-cisco-serviceurl-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>User</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>25000</td>
</tr>
<tr>
<td>Call Forward URI</td>
<td>x-cisco-serviceurl-fwrdial</td>
</tr>
<tr>
<td>Speed Dial (Abbreviated Dial) URI</td>
<td>x-cisco-serviceurl-abbrevdial</td>
</tr>
</tbody>
</table>

**Normalization Script**

Normalization Script: < None >
Some settings such as Wireless LAN and Bluetooth can be configured on an enterprise phone, common phone profile or individual phone level.

Wireless LAN and Bluetooth are enabled by default for the Cisco IP Phone 8861 and 8865.

Wireless LAN is automatically disabled temporarily when Ethernet is connected to the Cisco IP Phone 8861 or 8865, but will be automatically re-enabled once Ethernet is disconnected if Wireless LAN was enabled previously.

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>Parameter Name</th>
<th>Parameter Value</th>
<th>Suggested Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP for Phone-based Services</td>
<td>default DSCP (000000)</td>
<td>CS3(precedence 3) DSCP (011000)</td>
</tr>
<tr>
<td>DSCP for Phone Configuration</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>CS3(precedence 3) DSCP (011000)</td>
<td>CS3(precedence 3) DSCP (011000)</td>
</tr>
</tbody>
</table>

G.722 and iSAC Advertisement

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

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

Audio and Video Bit Rates

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

It is recommended to select G.722 or G.711 for the audio codec.

By default the video call bit rate is set to 384 Kbps.

For typical deployments, it is recommended to utilize 600p (1100-2000 Kbps) or HD 720p (1000-1599 Kbps) for the video stream.

For enhanced video quality, set the video call bit rate to 1 Mbps to utilize HD 720p (total 1064 Kbps including G.722 audio).
Use the following information to configure the audio bit rate to be used for audio or audio + video 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>iSAC</td>
<td>32 Kbps</td>
</tr>
<tr>
<td>iLBC</td>
<td>16 Kbps</td>
</tr>
<tr>
<td>G.729</td>
<td>8 Kbps</td>
</tr>
</tbody>
</table>

Use the following information to configure the video bit rate to be used for video calls.

The value configured will determine the resolution of the transmitted video stream from the Cisco IP Phone 8865. The Cisco IP Phone 8865 can receive up to HD 720p video depending on the remote device’s capabilities, where the region settings configuration is factored in.

The Cisco IP Phone 8865 supports video bandwidth adaption, where the video bit rate can be adjusted as necessary if the current network connection can not support higher video resolutions.

<table>
<thead>
<tr>
<th>Video Type</th>
<th>Video Resolution</th>
<th>Frames per Second (fps)</th>
<th>Video Bit Rate Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>QCIF</td>
<td>176 x 144</td>
<td>15</td>
<td>64-93 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>94-119 Kbps</td>
</tr>
<tr>
<td>SIF</td>
<td>352 x 240</td>
<td>15</td>
<td>120-199 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>200-279 Kbps</td>
</tr>
<tr>
<td>CIF</td>
<td>352 x 288</td>
<td>15</td>
<td>120-199 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>200-279 Kbps</td>
</tr>
<tr>
<td>VGA</td>
<td>640 x 480</td>
<td>15</td>
<td>280-519 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>520-1500 Kbps</td>
</tr>
<tr>
<td>240p</td>
<td>432 x 240</td>
<td>15</td>
<td>64-179 Kbps</td>
</tr>
</tbody>
</table>
**Video Capabilities**

In order for the Cisco IP Phone 8865 to send and receive video, that capability must be enabled in the Cisco Unified Communications Manager.

The **Video Capabilities** option is set to **Enabled** by default, but ensure it remains enabled in the phone’s configuration within the Product Specific Configuration Layout section.

<table>
<thead>
<tr>
<th>Video Capability</th>
<th>Resolution</th>
<th>Frame Rate</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>nHD 360p</td>
<td>640 x 360</td>
<td>30</td>
<td>180-209 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>210-349 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>400-659 Kbps</td>
</tr>
<tr>
<td>WVGA 480p</td>
<td>800 x 480</td>
<td>15</td>
<td>350-399 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>660-789 Kbps</td>
</tr>
<tr>
<td>HD 720p</td>
<td>1280 x 720</td>
<td>15</td>
<td>790-1359 Kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>1360-2500 Kbps</td>
</tr>
</tbody>
</table>

**VPN Configuration**

VPN configuration information can be pushed down from the administrator via Cisco Unified Communications Manager. A VPN gateway must be created, where the name and VPN gateway URL are defined.

<table>
<thead>
<tr>
<th>VPN Gateway Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Gateway Name*</td>
<td>Corporate_VPN_GW</td>
</tr>
<tr>
<td>VPN Gateway Description</td>
<td></td>
</tr>
<tr>
<td>VPN Gateway URL*</td>
<td><a href="https://vpn.cisco.com">https://vpn.cisco.com</a></td>
</tr>
</tbody>
</table>

A VPN group must also be created, which contains information about which VPN gateway will be utilized.
A VPN profile must be configured, which specifies which type of client authentication will be utilized as well as other parameters.

Once the VPN group and profile have been configured, they can then be applied to a Common Phone Profile, which in turn can be applied to a specific device.

If the Cisco IP Phone 8861 or 8865 is currently connected to a network and is unable to connect to the Cisco Unified Communications Manager then it can attempt to establish a VPN session automatically if a VPN profile is configured.
**Wireless LAN Profiles**

With Cisco Unified Communications Manager 10.0 release and later, the Cisco IP Phone 8861 and 8865 can be provisioned with Wireless LAN Profiles via the Cisco Unified Communications Manager.

With Cisco Unified Communications Manager 11.0 and later, EAP-TLS support is included.

Use the following guidelines to configure a Wireless LAN profile within Cisco Unified Communications Manager to then apply to a Cisco IP Phone 8861 or 8865.

- Prior to creating a Wireless LAN Profile and associating it to a Cisco IP Phone 8861 and 8865, the Cisco IP Phone 8861 and 8865 should be configured to utilize a security profile in which TFTP encryption is enabled so Wireless LAN Profile data is not passed down to the Cisco IP Phone 8861 and 8865 in clear text via TFTP.

- Once the security profile has been created, it then needs to be applied to the Cisco IP Phone 8861 and 8865 to enable TFTP encryption for that Cisco IP Phone 8861’s and 8865’s configuration files.
- Select the configured security profile from the **Device Security Profile** drop-down menu.
• To create a Wireless LAN Profile, navigate to **Device > Device Settings > Wireless LAN Profile** within the Cisco Unified Communications Manager’s Administration interface.
• From the Wireless LAN Profile page, select **Add New**.

![Cisco Unified CM Administration](image)

• A Wireless LAN Profile can then be created where the **Name**, **Description**, **Wireless Settings** (SSID, Frequency Band, User Modifiable), and **Authentication Settings** are specified.

• Below are Wireless LAN Profile defaults:
  • **Frequency Band** = Auto
  • **User Modifiable** = Allowed
  • **Authentication Method** = EAP-FAST
• Enter a **Name** for the Wireless LAN Profile containing up to 50 characters.
• A **Description** containing up to 63 characters can optionally be configured.

• Select the desired **User Modifiable** option.
  - **Allowed** - The user has the capability to change any Wireless LAN settings (e.g. Enable/Disable, SSID, Frequency Band, Authentication Method, Username and Password, PSK Passphrase, WEP Key) locally on the endpoint.
  - **Disallowed** - The user is unable to change any Wireless LAN settings.
  - **Restricted** - The user is only able to change certain Wireless LAN settings (e.g. Username and Password).
- Enter an **SSID** containing up to 32 ASCII characters.

- Select the desired **Frequency Band** option.
  - **Auto** = Give preference to 5 GHz channels, but operates on both 5 GHz and 2.4 GHz channels
  - **2.4 GHz** = Operates on 2.4 GHz channels only
  - **5 GHz** = Operates on 5 GHz channels only

- Select the desired **Authentication Method** option.

- If **EAP-FAST**, **PEAP-MSCHAPv2**, or **PEAP-GTC** is selected then the option to enter shared credentials (Username and Password) is available.
- If **Provide Shared Credentials** is not checked, then the Username and Password will need to be configured locally on the Cisco IP Phone 8861 and 8865 by the admin or user.
- If **Provide Shared Credentials** is checked, then the specified **Username** and **Password** will be utilized for all Cisco IP Phone 8861 and 8865 that utilize this Wireless LAN Profile.
- Up to 64 characters can be entered for the Username and Password.
- A **Password Description** can optionally be entered.

![Authentication Method](EAP-FAST)

- **Provide Shared Credentials**
  - **Username**
  - **Password**
  - **show password**
  - **Password Description**

- **Authentication Method**
  - **EAP-FAST**

- If **EAP-TLS** is selected then **User Certificate** must be configured to specify the type of user certificate to utilize for EAP-TLS authentication.
- Can set **User Certificate** to **MIC** (Manufacturing Installed Certificate) or **User Installed**.

![Authentication Method](EAP-TLS)

- **Authentication Method**
  - **EAP-TLS**

- **User Certificate**
  - **MIC**
  - **User Installed**

- If **PSK** is selected to utilize Pre-Shared Key authentication, then a **PSK Passphrase** must be entered.
- The **PSK Passphrase** must be in one of the following formats:
  - 8-63 ASCII character string
  - 64 HEX character string
- A **Password Description** can optionally be entered.

![Authentication Method](PSK)

- **Authentication Method**
  - **PSK**

- **PSK Passphrase**
  - **show passphrase**
  - **Password Description**

- If **WEP** is selected to utilize static WEP (Wired Equivalent Privacy) authentication, then a **WEP Key** must be entered.
- Only WEP key 1 is supported, so need to ensure that the entered key matches transmit key on the access point side.
- The **WEP Key** must be in one of the following formats:
  - 40/64 Bit Key = 5 digit ASCII or 10 digit HEX character string
  - 104/128 Bit Key = 13 digit ASCII or 26 digit HEX character string
- A **Password Description** can optionally be entered.
- If **None** is selected, then no authentication is required and no encryption will be utilized.

- Select **Save** once the Wireless LAN Profile configuration is complete.
- The Cisco IP Phone 8861 and 8865 do not support the **Network Access Profile** option.

To create a Wireless LAN Profile Group, navigate to **Device > Device Settings > Wireless LAN Profile Group** within the Cisco Unified Communications Manager’s Administration interface.
- From the Wireless LAN Profile Group page, select **Add New**.
- A Wireless LAN Profile Group can then be created where the Name, Description, and Wireless LAN Profiles are specified.
- Only 1 Wireless LAN Profile should be added to a Wireless LAN Profile Group.
- Select **Save** once the Wireless LAN Profile Group configuration is complete.

- Once the Wireless LAN Profile Group has been created, it can be applied to a Device Pool or an individual Cisco IP Phone 8861 and 8865.
- To apply a Wireless LAN Profile Group to a device pool, navigate to **System > Device Pool** within the Cisco Unified Communications Manager’s Administration interface.
- Create a Device Pool as necessary and put the desired Cisco IP Phone 8861 and 8865 into this Device Pool.
- Once the Device Pool has been created, configure the Wireless LAN Profile Group then select **Save**.
- Once the Wireless LAN Profile Group has been applied to the Device Pool, select **Apply Config** for the Cisco IP Phone 8861 and 8865 to download the Wireless LAN Profile Group configuration.
To apply a Wireless LAN Profile Group to an individual Cisco IP Phone 8861 and 8865, navigate to Device > Phone within the Cisco Unified Communications Manager’s Administration interface.

Navigate to the desired Cisco IP Phone 8861 and 8865, configure the Wireless LAN Profile Group then select Save.

Once the Wireless LAN Profile Group has been applied to the individual Cisco IP Phone 8861 and 8865, select Apply Config for the Cisco IP Phone 8861 and 8865 to download the Wireless LAN Profile Group configuration.
Note: The Cisco IP Phone 8861 and 8865 currently do not support use of the LSC (Locally Significant Certificate) as the User Certificate for EAP-TLS.

Cisco Unified Communications Manager Express

Prior to release 11.0 of Cisco Unified Communications Manager Express, the Cisco IP Phone 8861 and 8865 are to utilize the fast track method utilizing the Cisco Unified IP Phone 9971 as the reference model (use 7975 as reference model if needing softkey template support).

With release 11.0 and 11.5 of Cisco Unified Communications Manager Express, the Cisco IP Phone 8865 can utilize the Cisco IP Phone 8861 as the reference model.

With release 11.7 and later of Cisco Unified Communications Manager Express, there is native support for the Cisco IP Phone 8865, therefore can use the Cisco IP Phone 8861 as the model type.


Sample Configuration

```
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname CME
!
```

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
boot-start-marker
boot system flash:c2900-universalk9-mz.SPA.156-1.T0a.bin
boot-end-marker

aqm-register-fnf

logging buffered 51200 warnings

aaa new-model

aaa authentication login default local
aaa authorization exec default local

aaa session-id common

ethernet lmi ce

clock timezone EST -5 0

clock summer-time EST recurring

ip domain name cisco.com

ip cef

no ipv6 cef

multi-link bundle-name-authenticated

cts logging verbose

crypto pki trustpoint TP-self-signed-2915022231

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-2915022231

revocation-check none

rsakeypair TP-self-signed-2915022231

! crypto pki certificate chain TP-self-signed-2915022231

certificate self-signed 01

3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 35656C66 2D536967 6E65642D 43657274
69666663 67146252 32393135 30323232 33313031E 170D3132 30373033 30333039
35395A17 0D323030 31303130 30303030 304A3031 312F302D 06035504 03132649
4F532D53 656C6662 5369676E 65642D43 65727469 66963631 74652D32 39313530
32323233 3130819F 300D0609 2A864886 F70D0101 01000003 8180D003 8190281
8100ABC4 D23F5B00 36665DCC 86171E19 CE92D3E5 A0576068 3AADCD26 89C3B795
1B4518BE 2B173A5C 60A82125 80935C29 1027DE28 FCF05E62 18A07C10 C59D34ED
9A1A4CCD7 3981E1BB 20445CFC 99686D13 D84C6B03 4D84B448 1102A0CF AE333B48
CBBF588F 6842A40B C9555A0B 0C283E66 0341D00C D0B8EB8D DCA8AE00 0DAF3083
8E170203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
551D2304 18301680 1D4B81B2 7EF36719 1D028ED 84384303 685250E6 6E301D06
03551D0E 04160414 D81B27E F367191D C08ED84 384A3068 525E6E6 300D0609
2A864886 F70D0101 05050003 81801001 2DB8E5AC 2D588D18 1CB78EE2 0EFAE777
716B441C 9389C987 612BBE9A 7B9E30CB 4B4F41A7 0F0DB51D E4F45FB2 F8A139B3
70DF1E94 A7EE4F81 B08E3F21 C0743E56 59D42988 D7FAB957 FADBFBFE A77F404F
634BD39D 87559D1D CCA93B3A 87899A98 C151CF62 EF183C8E CB2C9DFC 71F45AE0
92A26F8B CBA7FA2B F9C5DB6D EEC936

quit

voice-card 0

voice service voip

no ip address trusted authenticate
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
no supplementary-service sip moved-temporarily sip
bind control source-interface GigabitEthernet0/0
bind media source-interface GigabitEthernet0/0
registrar server expires max 1000 min 800
no call service stop
!
voice register global
mode cme
source-address 10.0.0.10 port 5060
max-dn 40
max-pool 42
load 8861 sip88xx.12-7-1-0001-393
load 8865 sip8845_65.12-7-1-0001-393
authenticate register
olsontimezone America/New_York version 2010
timezone 12
create profile sync 0089201122844265
camera
video
!
voice register dn  1
data 1101
name 8861
label 1101
mwi
!
voice register dn  2
data 1102
name 8865
label 1102
mwi
!
voice register pool  1
busy-trigger-per-button 2
id mac 6C99.8984.B7E5
session-transport tcp
type 8861
number 1 dn 1
dtmf-relay rtp-nte
username 8861 password <REMOVED>
codec g711ulaw
no vad
!
voice register pool  2
busy-trigger-per-button 2
id mac AC7E.8AB7.63B6
session-transport tcp
type 8865
number 1 dn 2
dtmf-relay rtp-nte
username 8865 password <REMOVED>
codec g711ulaw
no vad
! license udi pid CISCO2901/K9 sn <REMOVED>
!
username <REMOVED> privilege 15 password 7 <REMOVED>
!
redundancy
!
interface Embedded-Service-Engine0/0
   no ip address
shutdown
!
interface GigabitEthernet0/0
   ip address 10.0.0.10 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
   no ip address
shutdown
duplex auto
speed auto
!
ip forward
!
interface GigabitEthernet0/0
   shutdown
no ip address
   speed auto
duplex auto

! interface GigabitEthernet0/1
   shutdown
duplex auto
speed auto
!
ip http protocol nd
!
ip http secure
ip http authentication local
!
ip http server
ip http timeout
policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
!
tftp-server flash://8861/sip88xx.12-7-1-0001-393.loads alias sip88xx.12-7-1-0001-393.loads
tftp-server flash://8861/boot1288xx.BE-01-007.sbn alias boot1288xx.BE-01-007.sbn
tftp-server flash://8861/fbi88xx.BE-01-012.sbn alias fbi88xx.BE-01-012.sbn
tftp-server flash://8861/kern88xx.12-7-1-0001-393.sbn alias kern88xx.12-7-1-0001-393.sbn
tftp-server flash://8861/kern288xx.12-7-1-0001-393.sbn alias kern288xx.12-7-1-0001-393.sbn
tftp-server flash://8861/kern388xx.12-7-1-0001-393.sbn alias kern388xx.12-7-1-0001-393.sbn
tftp-server flash://8861/m0patch288xx.BE-01-001.sbn alias m0patch288xx.BE-01-001.sbn
tftp-server flash://8861/preloader88xx.BE-01-002.sbn alias preloader88xx.BE-01-002.sbn
tftp-server flash://8861/rootfs88xx.12-7-1-0001-393.sbn alias rootfs88xx.12-7-1-0001-393.sbn
tftp-server flash://8861/rootfs288xx.12-7-1-0001-393.sbn alias rootfs288xx.12-7-1-0001-393.sbn
tftp-server flash://8861/rootfs388xx.12-7-1-0001-393.sbn alias rootfs388xx.12-7-1-0001-393.sbn
tftp-server flash://8861/sb288xx.BE-01-026.sbn alias sb288xx.BE-01-026.sbn
tftp-server flash://8861/sb2388xx.BE-01-027.sbn alias sb2388xx.BE-01-027.sbn
tftp-server flash://8861/ssb288xx.BE-01-007.sbn alias ssb288xx.BE-01-007.sbn
tftp-server flash://8861/vc488xx.12-7-1-0001-393.sbn alias vc488xx.12-7-1-0001-393.sbn
!
tftp-server flash://8865/sip8845_65.12-7-1-0001-393.loads alias sip8845_65.12-7-1-0001-393.loads
tftp-server flash://8865/fbi8845_65.BEV-01-006.sbn alias fbi8845_65.BEV-01-006.sbn
tftp-server flash://8865/kern8845_65.12-7-1-0001-393.sbn alias kern8845_65.12-7-1-0001-393.sbn
tftp-server flash://8865/rootfs8845_65.12-7-1-0001-393.sbn alias rootfs8845_65.12-7-1-0001-393.sbn
tftp-server flash://8865/sb28845_65.BEV-01-015.sbn alias sb28845_65.BEV-01-015.sbn
tftp-server flash://8865/vc48845_65.12-7-1-0001-393.sbn alias vc48845_65.12-7-1-0001-393.sbn
!
control-plane
!
Product Specific Configuration Options

In Cisco Unified Communications Manager Administration, the following configuration options are available for the Cisco IP Phone 8861 and 8865.

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 IP Phone 8861 and 8865 Common Configuration Options

<table>
<thead>
<tr>
<th>Parameter Specific Configuration Layout</th>
<th>Parameter Value</th>
<th>Override Enterprise/Common Phone Profile Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Speakerphone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable Speakerphone and Headset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable Handset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC Port</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Settings Access</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>PC Voice VLAN Access</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Video Capabilities</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Web Access</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Disable TLS 1.0 and TLS 1.1 for Web Access</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Enbloc Dialing</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Days Display Not Active</td>
<td>Sunday</td>
<td></td>
</tr>
<tr>
<td>Display On Time</td>
<td>07:30</td>
<td></td>
</tr>
<tr>
<td>Display On Duration</td>
<td>10:30</td>
<td></td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>01:00</td>
<td></td>
</tr>
<tr>
<td>Display On When Incoming Call</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Enable Power Save Plus</td>
<td>Sunday</td>
<td></td>
</tr>
<tr>
<td>Phone On Time</td>
<td>00:00</td>
<td></td>
</tr>
<tr>
<td>Phone Off Time</td>
<td>24:00</td>
<td></td>
</tr>
<tr>
<td>Phone Off Idle Timeout</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Enable Audible Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EnergyWise Domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EnergyWise Secret</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow EnergyWise Overrides</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Join And Direct Transfer Policy</td>
<td>Same line, across line enable</td>
<td></td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Recording Tone</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Recording Tone Local Volume</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Setting</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Recording Tone Remote Volume*</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Recording Tone Duration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP): Switch Port*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP): PC Port*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP): PC Port*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>LLDP Asset ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LLDP Power Priority*</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>802.1x Authentication*</td>
<td>User Controlled</td>
<td></td>
</tr>
<tr>
<td>Automatic Port Synchronization*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Switch Port Remote Configuration*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>PC Port Remote Configuration*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>SSH Access*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Incoming Call Toast Timer*</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Ring Locale*</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>TLS Resumption Timer*</td>
<td>3600</td>
<td></td>
</tr>
<tr>
<td>FIPS Mode*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Record Call Log from Shared Line*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Minimum Ring Volume*</td>
<td>0-Silent</td>
<td></td>
</tr>
<tr>
<td>Peer Firmware Sharing*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Load Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Load Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Headset Hookswitch Control*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Wideband Headset UI Control*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Wideband Headset*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Back USB Port*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Side USB Port*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Console Access*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Bluetooth*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Allow Bluetooth Contacts Import*</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Disable Speakerphone</td>
<td>Disable only the speakerphone functionality. Disabling speakerphone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>functionality will not affect the headset. You can use lines and speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dials with headset/handset.</td>
<td></td>
</tr>
<tr>
<td>Disable Speakerphone and Headset</td>
<td>Disable all speakerphone functions and headset microphone.</td>
<td></td>
</tr>
<tr>
<td>Disable Handset</td>
<td>Disable handset.</td>
<td></td>
</tr>
<tr>
<td>PC Port</td>
<td>Indicates whether the PC port on the phone is enabled or disabled. The port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>labeled “10/100 PC” on the back of the phone connects a PC or workstation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to the phone so they can share a single network connection.</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Settings Access</td>
<td>Indicates whether the Settings button on the phone is functional. When Settings Access is enabled, you can change the phone network configuration, ring type, and volume on the phone. When Settings Access is disabled, the Settings button is completely disabled; no options appear when you press the button. Also, you cannot adjust the ringer volume or save any volume settings. By default, Settings Access is enabled.</td>
<td></td>
</tr>
<tr>
<td>PC Voice VLAN Access</td>
<td>Indicates whether the phone will allow a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the phone. Set this setting to Enabled if an application is being run on the PC that requires monitoring of the phones traffic. These could include monitoring and recording applications and use of network monitoring software for analysis purposes.</td>
<td></td>
</tr>
<tr>
<td>Video Capabilities</td>
<td>When enabled, indicates that the phone will participate in video calls when connected to an appropriately equipped PC.</td>
<td></td>
</tr>
<tr>
<td>Web Access</td>
<td>This parameter indicates 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. Features, such as QRT ( Quality Report Tool ), will not function properly without access to the phones web pages. This setting will also affect any serviceability application such as CiscoWorks 2000 that relies on web access.</td>
<td></td>
</tr>
<tr>
<td>Disable TLS 1.0 and TLS 1.1 for Web Access</td>
<td>This parameter indicates to disable TLS 1.0 and TLS 1.1 when using https for web access.</td>
<td></td>
</tr>
<tr>
<td>Enbloc Dialing</td>
<td>This parameter indicates to enable enblocDialing.</td>
<td></td>
</tr>
<tr>
<td>Days Display Not Active</td>
<td>This field allows the user to specify the days that the display is to remain off by default. Typically this would be Saturday and Sunday for US corporate customers. Saturday and Sunday should be the default. The list contains all of the days of the week. To turn off display on Saturday and Sunday the User would hold down Control and select Saturday and Sunday.</td>
<td></td>
</tr>
<tr>
<td>Display On Time</td>
<td>This field indicates the time of day the display is to automatically turn itself on for days listed in the off schedule. The value should be in a 24 hour format. Where 0:00 is the beginning of the day and 23:59 is the end of the day. Leaving this field blank will activate the display at the default time of the day (e.g. – “7:30”). To set the display to turn on at 7:00AM the user would enter “07:00” without the quotes. To have the display to turn on at 2:00PM enter “14:00” without the quotes.</td>
<td></td>
</tr>
<tr>
<td>Display On Duration</td>
<td>This field indicates the amount of time the display is to be active for when it is turned on by the programmed schedule. No value indicates the end of the day. Maximum value is 24 hours. This value is in free form hours and minutes. “1:30” would activate the display for one hour and 30 minutes.</td>
<td></td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>This field indicates how long to wait before the display is turned off when it was turned on by user activity. This inactivity timer will continually reset itself during user activity. Leaving this field blank will make the phone use a pre-determined default value of one hour. Maximum value is 24 hours. This value can be in free form hours and minutes. “1:30” would turn off the display after one hour and 30 minutes of inactivity.</td>
<td></td>
</tr>
<tr>
<td>Display On When Incoming Call</td>
<td>This field indicates whether LCD display is on when there is an incoming call. If</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Enable Power Save Plus</td>
<td>To enable the Power Save Plus feature, select the day(s) that you want the phone to power off on schedule. You can select multiple days by pressing and holding the Control key while clicking on the days that you want Power Save Plus to operate. The default is disabled (no days selected). In Power Save Plus mode, enough power is maintained to illuminate one key. All other functions of the phone are turned off in Power Save Plus mode. Power Save Plus mode turns off the phone for the time period specified in the Phone On Time and Phone Off Time fields. This time period is usually outside of your organization’s regular operating hours. The illuminated key allows a user to press it to restore full power to the phone. After pressing the illuminated key, the phone power-cycles and reregisters with Unified CM before it becomes fully operational. Power Save Plus is disabled by default. When you select day(s) in this field, the following notice displays to indicate e911 concerns. By enabling Power Save Plus, you are agreeing to the terms specified in this Notice. Notice: WHILE POWER SAVE PLUS MODE (THE &quot;MODE&quot;) IS IN EFFECT, ENDPOINTS CONFIGURED FOR THE MODE ARE DISABLED FOR EMERGENCY CALLING AND FROM RECEIVING INBOUND CALLS. BY SELECTING THIS MODE, YOU AGREE TO THE FOLLOWING: (I) YOU ARE TAKING FULL RESPONSIBILITY FOR PROVIDING ALTERNATE METHODS FOR EMERGENCY CALLING AND RECEIVING CALLS WHILE THE MODE IS IN EFFECT; (II) CISCO HAS NO LIABILITY IN CONNECTION WITH YOUR SELECTION OF THE MODE AND ALL LIABILITY IN CONNECTION WITH ENABLING THE MODE IS YOUR RESPONSIBILITY; AND (III) YOU WILL FULLY INFORM USERS OF THE EFFECTS OF THE MODE ON CALLS, CALLING AND OTHERWISE.</td>
<td></td>
</tr>
<tr>
<td>Phone On Time</td>
<td>This field determines the time that the phone turns on automatically on the days that are selected in the Enable Power Save Plus list box. Enter the time in 24 hour format, where 00:00 represents midnight. For example, to automatically turn the phone on at 7:00 a.m., (0700), enter 07:00. To turn the phone on at 2:00 p.m. (1400), enter 14:00. If this field is blank, the phone automatically turns on at 00:00. The default is blank.</td>
<td></td>
</tr>
<tr>
<td>Phone Off Time</td>
<td>This field determines the time of day that the phone will turn itself off on the days that are selected in the Enable Power Save Plus list box. Enter the time in the following format hours:minutes. If this field is blank, the phone automatically turns off at midnight (00:00). The default is blank. Note: If Phone On Time is blank (or 00:00) and Phone Off Time is blank (or 24:00), the phone will remain on continuously, effectively disabling the Power Save Plus feature unless you allow EnergyWise to send overrides.</td>
<td></td>
</tr>
<tr>
<td>Phone Off Idle Timeout</td>
<td>This field represents the number of minutes that the device must be idle before the device will request the power sourcing equipment (PSE) to power down the device. The value in this field takes effect: - When the device was in Power Save Plus mode as scheduled and was taken out of Power Save Plus mode because the phone user pressed the select key – When the phone is repowered by the attached switch – When the Phone Off Time is met but the phone is in use The unit is minutes. The default is 60. The range is 20 to 1440.</td>
<td></td>
</tr>
<tr>
<td>Enable Audible Alert</td>
<td>This checkbox, when enabled, instructs the phone to play an audible alert ten minutes prior to the time specified in the field, Phone Off Time. The select key on the phone will quickly flash to visually alert the user to the impending phone state change (powering off as a result of the Power Save Plus feature). To also audibly alert the user, enable this checkbox. The default is disabled. This field is set to Enabled (default), the LCD display will turn on (if off) when a call is received. If Disabled, the LCD display will not turn on when a call is received.</td>
<td></td>
</tr>
<tr>
<td>Field Label</td>
<td>Help Text</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Allow EnergyWise Overrides</td>
<td>This checkbox determines whether you will allow the EnergyWise domain controller policy to send power level updates to the phones. A few conditions apply; first, one or more days must be selected in the Enable Power Save Plus field. If the Enable Power Save Plus list box does not have any days selected, the phone will ignore the EnergyWise directive to turn off the phone. Second, the settings in Unified CM Administration will take effect on schedule even if EnergyWise sends an override. For example, assume the Display Off Time is set to 22:00 (10 p.m.), the value in the Display On Time field is 06:00 (6 a.m.), and the Enable Power Save Plus has one or more days selected. If EnergyWise directs the phone to turn off at 20:00 (8 p.m.), that directive will remain in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6 a.m. At 6 a.m., the phone will turn on and resume receiving its power level changes from the settings in Unified CM Administration. To change the power level on the phone again, EnergyWise must reissue a new power level change command. Also, any user interaction will take effect so if a user presses the select softkey after EnergyWise has directed the phone to power off, the phone will power on as a result of the user action. The default is unchecked.</td>
<td></td>
</tr>
<tr>
<td>Join And Direct Transfer Policy</td>
<td>This field indicates join and direct transfer policy for same line and across line.</td>
<td></td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Indicates whether the phone will forward packets transmitted and received on the Phone Port to the PC Port. Select Enabled if an application is being run on the PC Port that requires monitoring of the IP Phone’s traffic such as monitoring and recording applications (common in call center environments) or network packet capture tools used for diagnostic purposes. To use this feature PC Voice VLAN access must be enabled.</td>
<td></td>
</tr>
<tr>
<td>Recording Tone</td>
<td>This can be used to configure whether the recording tone is enabled or disabled on the phone. If enabled, the phone mixes the recording tone into both directions for every call.</td>
<td></td>
</tr>
<tr>
<td>Recording Tone Local Volume</td>
<td>This can be used to configure the loudness setting of the recording tone that the local party hears. This loudness setting applies regardless of the actual device used for hearing (handset, speakerphone, headset). The loudness setting should be in the range of 0% to 100%, with 0% being no tone and 100% being at the same level as the current volume setting. The default value is 100%.</td>
<td></td>
</tr>
<tr>
<td>Recording Tone Remote Volume</td>
<td>This can be used to configure the loudness setting of the recording tone that the...</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Recording Tone Duration</td>
<td>Indicates the length of time in milliseconds for which the recording tone is inserted in the audio stream. The default for this parameter is set to the value in the Network locale file for this field. The valid range for this parameter is a value between 1 and 3000 milliseconds.</td>
<td></td>
</tr>
<tr>
<td>Log Server</td>
<td>Specifies an IP address and port of a remote system where log messages are sent. The format is:xxx.xxx.xxx.xxx:ppppp@@options. Options will be format as base=x;pfs=y; base value range is 0<del>7,pfs value range is 0</del>1. And the two parameters are optional. Absence of pfs or base, pfs will be set to the default value 0 and base will be set to the default value 7.</td>
<td></td>
</tr>
<tr>
<td>Cisco Discover Protocol (CDP): Switch Port</td>
<td>Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the switch port.</td>
<td></td>
</tr>
<tr>
<td>Cisco Discover Protocol (CDP): PC Port</td>
<td>Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the PC port.</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port</td>
<td>Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the switch port.</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol – (LLDP): PC Port</td>
<td>Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the PC port.</td>
<td></td>
</tr>
<tr>
<td>LLDP Asset ID</td>
<td>Allows administrator to set Asset ID for Link Layer Discovery Protocol.</td>
<td></td>
</tr>
<tr>
<td>LLDP Power Priority</td>
<td>Allows administrator to set Power Priority for Link Layer Discovery Protocol.</td>
<td></td>
</tr>
<tr>
<td>802.1x Authentication</td>
<td>Specifies the 802.1x authentication feature status.</td>
<td></td>
</tr>
<tr>
<td>Automatic Port Synchronization</td>
<td>Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds.</td>
<td></td>
</tr>
<tr>
<td>Switch Port Remote Configuration</td>
<td>Allows remote configuration of the speed and duplex for the switch port of the phone, which overrides any manual configuration at the phone. Be aware that configuring this port may cause the phone to lose network connectivity.</td>
<td></td>
</tr>
<tr>
<td>PC Port Remote Configuration</td>
<td>Allows remote configuration of the speed and duplex for the PC port of the phone, which overrides any manual configuration at the phone.</td>
<td></td>
</tr>
<tr>
<td>SSH Access</td>
<td>This parameter indicates whether the phone will accept ssh connections. Disabling the ssh server functionality of the phone will block access to the phone.</td>
<td></td>
</tr>
<tr>
<td>Incoming Call Toast Timer</td>
<td>This parameter specifies the maximum time in seconds that the toast displays a new incoming call notification.</td>
<td></td>
</tr>
<tr>
<td>Ring Locale</td>
<td>IP Phone has distinctive ring for On-net/Off-net or line based, but its ring cadence is fixed, and it is based on US standard only. Ring cadence in US standard is opposite to Japan standard. To support Japan ring cadence, the ring cadence should be configurable according to Ring Locale.</td>
<td></td>
</tr>
<tr>
<td>TLS Resumption Timer</td>
<td>The current TLS session to support TLS session resumption is HTTPS client. The HTTPS client sessions support configurable session resumption timer. The timer specifies the maximum session resumption time allowed. If the value is set to 0, TLS session resumption will be disabled.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>FIPS Mode</td>
<td>This parameter specifies if the fips mode is enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>Record Call Log From Shared Line</td>
<td>This field indicates whether or not to record call log from shared line.</td>
<td></td>
</tr>
<tr>
<td>Minimum Ring Volume</td>
<td>This parameter controls the minimum ring volume on an IP phone. This value is set by the administrator, and can not be changed by an end user. The end user can increase the ring volume, but may not decrease the ring volume below the level defined. The minimum ring volume range is from 0 to 15, with 0 (silent) being the default value.</td>
<td></td>
</tr>
<tr>
<td>Peer Firmware Sharing</td>
<td>Enables or disables Peer to Peer image distribution in order to allow a single phone in a subnet to retrieve an image firmware file then distribute it to its peers – thus reducing TFTP bandwidth and providing for a faster firmware upgrade time.</td>
<td></td>
</tr>
<tr>
<td>Load Server</td>
<td>Indicates 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>
<td></td>
</tr>
<tr>
<td>IPv6 Load Server</td>
<td>Indicates that the phone will use an alternative IPv6 server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local IPv6 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 IPv6 address (using standard IPv6 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>
<td></td>
</tr>
<tr>
<td>Wireless Headset Hookswitch Control</td>
<td>Allows administrator to enable or disable Wireless Headset Hookswitch Control.</td>
<td></td>
</tr>
<tr>
<td>Wideband Headset UI Control</td>
<td>Allows users to enable or disable Wideband Headset option on phone UI.</td>
<td></td>
</tr>
<tr>
<td>Wideband Headset</td>
<td>Enable or disable the use of a Wideband Headset on the phone. Used in conjunction with User Control Wideband Headset.</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Indicates whether the Wi-Fi on the device is enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>Back USB Port</td>
<td>Indicates whether the back usb port on the phone is enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>Side USB Port</td>
<td>Indicates whether the side usb port on the phone is enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>Console Access</td>
<td>Indicates whether the serial console is enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Indicates whether the Bluetooth device on the phone is enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>Allow Bluetooth Contacts Import</td>
<td>Indicates whether the Bluetooth device on the phone is allowed to sync the contacts from the phone.</td>
<td></td>
</tr>
<tr>
<td>Allow Bluetooth Mobile Handsfree Mode</td>
<td>Indicates whether the user is allowed to enable or disable 2 way audio between devices with HFP.</td>
<td></td>
</tr>
<tr>
<td>Bluetooth Profiles</td>
<td>Indicates which Bluetooth profiles on the phone are enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>Indicates whether the phone will learn MAC addresses from Gratuitous ARP responses. Disabling the phones ability to accept Gratuitous ARP will prevent applications, which use this mechanism for monitoring and recording of voice streams from working. If monitoring capability is not desired, change this setting to Disabled.</td>
<td></td>
</tr>
<tr>
<td>Show All Calls On Primary Line</td>
<td>When enabled, indicates that all calls presented to this device will be shown when the Primary line is selected.</td>
<td></td>
</tr>
<tr>
<td>HTTPS Server</td>
<td>Allows Administrator to permit http and https or https only connections if Web Access is enabled.</td>
<td></td>
</tr>
<tr>
<td>IPv6 Log Server</td>
<td>Specifies an IPv6 address and port of a remote system where log messages are sent. The format is: [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]:ppppp@@options. Options will be format as base=x:pfs=y; base value range is 0<del>7, pfs value range is 0</del>1. And the two parameters are optional. Absence of pfs or base, pfs will be set to the default value 0 and base will be set to the default value 7.</td>
<td></td>
</tr>
<tr>
<td>Remote Log</td>
<td>This parameter specifies where to send the log data by serviceability. If enabled, the log data will be copied by serviceability to the place specified by Log Server/IPV6 Log Server. If disabled, the log data will not be copied by serviceability to the place specified by Log Server/IPV6 Log Server.</td>
<td></td>
</tr>
<tr>
<td>Log Profile</td>
<td>Run the pre-defined debug command remotely.</td>
<td></td>
</tr>
<tr>
<td>Advertise G.722 and iSAC Codecs</td>
<td>Indicates whether Cisco IP Phones will advertise the G.722 codec to Cisco Unified CallManager. Codec negotiation involves two steps: first, the phone must advertise the supported codec(s) to Cisco Unified CallManager (not all endpoints support the same set of codecs). Second, when 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. Valid values specify 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 to Cisco Unified CallManager) or Enabled (this phone will advertise G.722 to Cisco Unified CallManager).</td>
<td></td>
</tr>
<tr>
<td>Detect Unified CM Connection Failure</td>
<td>This field determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. Note that the precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing. This only applies to the wired Ethernet connection. Default = Normal</td>
<td></td>
</tr>
<tr>
<td>Power Negotiation</td>
<td>You should enable the Power Negotiation feature when connected to a switch that supports power negotiation. However, if a switch does not support power negotiation, then you should disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the phone can power up accessories up to 12.9W</td>
<td></td>
</tr>
<tr>
<td><strong>Provide Dial Tone from Release Button</strong></td>
<td>Indicates whether Dial Tone is provided when Release Button is pressed. If the value is true, then in “Off Hook Dialing/RingingOut/Connected” state, a new Call Windows will be brought out after Release Button is pressed. If “Revert To All Calls” feature was enabled, it should be active first before “Dial Tone” feature.</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Background Image</strong></td>
<td>This parameter specifies the default wallpaper file. Only the administrator disables end user access to phone wallpaper list, could this parameter take effect.</td>
<td></td>
</tr>
<tr>
<td><strong>Simplified New Call UI</strong></td>
<td>This parameter specifies if use simplified call UI style when the phone is Off-hook. Those who like the New Call Window can continue to use that at the same time that those who prefer the Simplified New Call Session can use that method.</td>
<td></td>
</tr>
<tr>
<td><strong>Revert to All Calls</strong></td>
<td>When enabled, phone will revert to All Calls after any call is ended if the call is on a filter other than Primary line, All Calls or Alerting Calls.</td>
<td></td>
</tr>
<tr>
<td><strong>Show Call History for Selected Line Only</strong></td>
<td>When enabled, the phone shows call history for selected line only.</td>
<td></td>
</tr>
<tr>
<td><strong>Actionable Incoming Call Alert</strong></td>
<td>Show an Alert with Answer, Divert and Ignore softkeys when there is an incoming call alerting for user to act.</td>
<td></td>
</tr>
<tr>
<td><strong>DF Bit</strong></td>
<td>Configure the DF bit in IP header.</td>
<td></td>
</tr>
<tr>
<td><strong>Default Line Filter</strong></td>
<td>Indicates that the phone will use an alternative line filter, rather than all lines as default filter on the phone. This option enables you to configure the lines you want to get notified with alert or toast when there’s incoming calls. Enter the line numbers separated by comma. If this field is left blank, the phone will use all lines as the default filter.</td>
<td></td>
</tr>
<tr>
<td><strong>Lowest Alerting Line State Priority</strong></td>
<td>When disabled, if there is an incoming call alerting on the shared line, the LED/Line state icon will reflect the alerting state instead of Remote-In-Use. When enabled, customer see the Remote-In-Use state when there is call alerting on the shared line.</td>
<td></td>
</tr>
<tr>
<td><strong>One Column Display for KEM</strong></td>
<td>When disabled. The KEM will display 18 Line/Button configured. Each line item will use half of the KEM screen width. When enabled, each line item will occupy entire KEM screen width for being able to show more characters. Total 9 Line/Button configured will be display on one KEM.</td>
<td></td>
</tr>
<tr>
<td><strong>Energy Efficient Ethernet(EEE): PC Port</strong></td>
<td>This parameter indicates enable or disable Energy Efficient Ethernet(EEE) on PC port. Default is Enable.</td>
<td></td>
</tr>
<tr>
<td><strong>Energy Efficient Ethernet(EEE): SW Port</strong></td>
<td>This parameter indicates enable or disable Energy Efficient Ethernet(EEE) on switch port. Default is Enable.</td>
<td></td>
</tr>
<tr>
<td><strong>User Credentials Persistent for Expressway Sign in</strong></td>
<td>This parameter enables phone to persistently store user credentials used for authentication with Expressway Sign in.</td>
<td></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 Report Tool” on the endpoint.</td>
<td></td>
</tr>
<tr>
<td><strong>Web Admin</strong></td>
<td>This field controls the accessibility of the Web Admin interface, which operates independently from the ‘Web Access’ parameter. If disabled then the Web Admin interface is not available. If enabled then Web Admin interface is available.</td>
<td></td>
</tr>
<tr>
<td><strong>Admin Password</strong></td>
<td>Specifies the password to access the phone’s Web Admin interface. Enter a 8-127 character password.</td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>WLAN SCEP Server</td>
<td>Indicates the SCEP Server the phone will use to obtain certificates for WLAN authentication. Enter the hostname or the IP address (using standard IP addressing format) of the server.</td>
<td></td>
</tr>
<tr>
<td>WLAN Root CA Fingerprint (SHA256 or SHA1)</td>
<td>Indicates the SHA256 or SHA1 fingerprint of the Root CA to use for validation during the SCEP process when issuing certificates for WLAN authentication. It is recommended to utilize the SHA256 fingerprint, which can be obtained via OpenSSL (i.e. openssl x509 -in rootca.cer -noout -sha256 -fingerprint) or using a Web Browser to inspect the certificate details. Enter the 64 hexadecimal character value for the SHA256 fingerprint or the 40 hexadecimal character value for the SHA1 fingerprint with a common separator (colon, dash, period, space) or without a separator. If using a separator, then the separator should be consistently placed after every 2, 4, 8, 16, or 32 hexadecimal characters for a SHA256 fingerprint or every 2, 4, or 8 hexadecimal characters for a SHA1 fingerprint.</td>
<td></td>
</tr>
<tr>
<td>WLAN Authentication Attempts</td>
<td>This parameter specifies the number of authentication attempts when there is explicit failure due to invalid credentials.</td>
<td></td>
</tr>
<tr>
<td>WLAN Profile 1 Prompt Mode</td>
<td>This parameter enables or disables WLAN prompt mode, where user is prompted to re-enter password on device start up or reboot.</td>
<td></td>
</tr>
<tr>
<td>Line Mode</td>
<td>This parameter allows admin to switch between Session Line Mode and Enhanced Line Mode. While in Session Line Mode, the buttons on the left of the screen can be configured as programmable line keys and the buttons on the right of the screen are always session keys. While in Enhanced Line Mode, all the buttons can be configured as programmable line keys.</td>
<td></td>
</tr>
<tr>
<td>Admin Configurable Ringer</td>
<td>This parameter is used to config ringtone on phone. Once config, phone can not change ringtone anymore.</td>
<td></td>
</tr>
<tr>
<td>Customer Support Use</td>
<td>This parameter specifies some special issue. Please split the special issue ID with &quot;;&quot;.</td>
<td></td>
</tr>
<tr>
<td>Disable TLS Ciphers</td>
<td>This parameter is used to disable TLS cipher list, the default value is None, and you can choose one or use “CTRL” choose several ciphers from the list, if you choose all of the ciphers, phone TLS service will be impacted.</td>
<td></td>
</tr>
</tbody>
</table>

### 8865 Specific Configuration Options

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Video Port</td>
<td>This is to set the video start port.</td>
</tr>
<tr>
<td>Stop Video Port</td>
<td>This is to set the video stop port.</td>
</tr>
</tbody>
</table>

### XML Syntax

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide 180
To configure product specific configuration options for the Cisco IP Phone 8861 and 8865 with Cisco Unified Communications Manager Express, add the necessary options under `telephony-service`.

**Service phone <module> <value>**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Module</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Speakerphone</td>
<td>disableSpeaker</td>
<td>false = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true = Enabled</td>
</tr>
<tr>
<td>Disable Speakerphone and Headset</td>
<td>disableSpeakerAndHeadset</td>
<td>false = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true = Enabled</td>
</tr>
<tr>
<td>Disable Handset</td>
<td>disableHandset</td>
<td>false = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true = Enabled</td>
</tr>
<tr>
<td>PC Port</td>
<td>pcPort</td>
<td>0 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td>Settings Access</td>
<td>settingsAccess</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Restricted</td>
</tr>
<tr>
<td>PC Voice VLAN Access</td>
<td>voiceVlanAccess</td>
<td>0 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td>Video Capabilities</td>
<td>videoCapability</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Web Access</td>
<td>webAccess</td>
<td>0 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td>Disable TLS 1.0 and TLS 1.1 for Web Access</td>
<td>tls12Only</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Enbloc Dialing</td>
<td>useEnblocDialing</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Days Display Not Active</td>
<td>daysDisplayNotActive</td>
<td>1 = Sunday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Monday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 = Tuesday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 = Wednesday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 = Thursday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 = Friday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 = Saturday</td>
</tr>
<tr>
<td>Display On Time</td>
<td>displayOnTime</td>
<td>Time in 24 hour format</td>
</tr>
<tr>
<td>Setting</td>
<td>Configuration</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display On Duration</td>
<td>displayOnDuration</td>
<td>Time in 24 hour format</td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>displayIdleTimeout</td>
<td>Time in 24 hour format</td>
</tr>
</tbody>
</table>
| Display On When Incoming Call               | displayOnWhenIncomingCall | 0 = Disabled  
1 = Enabled                                                   |
| Enable Power Save Plus                       | enablePowerSavePlus | 1 = Sunday  
2 = Monday  
3 = Tuesday  
4 = Wednesday  
5 = Thursday  
6 = Friday  
7 = Saturday                                      |
| Phone On Time                                | phoneOnTime    | Time in 24 hour format                                                      |
| Phone Off Time                               | phoneOffTime    | Time in 24 hour format                                                      |
| Phone Off Idle Timeout                       | phoneOffIdleTimeout    | 20-1440  
(Default = 60)                                  |
| Enable Audible Alert                         | enableAudibleAlert | false = Disabled  
true = Enabled                                             |
| EnergyWise Domain                            | energyWiseDomain | Up to 127 character string                                                   |
| EnergyWise Secret                            | energyWiseSecret | Up to 127 character string                                                   |
| Allow EnergyWise Overrides                   | allowEnergyWiseOverrides | false = Disabled  
true = Enabled                                             |
| Join and Direct Transfer Policy              | joinAndDirectTransferPolicy | 0 = Same line, across line enable  
1 = Same line enable only  
2 = Same line, across line enable |
| Span to PC Port                              | spanToPCPort    | 0 = Enabled  
1 = Disabled                                            |
| Recording Tone                               | recordingTone    | 0 = Disabled  
1 = Enabled                                            |
| Recording Tone Local Volume                 | recordingToneLocalVolume | 0-100  
(Default = 100)                                 |
<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Python Variable</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Tone Remote Volume</td>
<td>recordingToneRemoteVolume</td>
<td>0-100 (Default = 50)</td>
</tr>
<tr>
<td>Recording Tone Duration</td>
<td>recordingToneDuration</td>
<td>1-3000</td>
</tr>
<tr>
<td>Log Server</td>
<td>logServer</td>
<td>Up to 256 character string</td>
</tr>
<tr>
<td>Cisco Discover Protocol (CDP): Switch Port</td>
<td>enableCdpSwPort</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Cisco Discover Protocol (CDP): PC Port</td>
<td>enableCdpPcPort</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port</td>
<td>enableLldpSwPort</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol - (LLDP): PC Port</td>
<td>enableLldpPcPort</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>LLDP Asset ID</td>
<td>lldpAssetId</td>
<td>Up to 32 character string</td>
</tr>
<tr>
<td>LLDP Power Priority</td>
<td>powerPriority</td>
<td>0 = Unknown, 1 = Low, 2 = High, 3 = Critical</td>
</tr>
<tr>
<td>802.1x Authentication</td>
<td>eapAuthentication</td>
<td>0 = User Controlled, 1 = Disabled, 2 = Enabled</td>
</tr>
<tr>
<td>Automatic Port Synchronization</td>
<td>PortAutoLinkSync</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Switch Port Remote Configuration</td>
<td>SWRemoteConfig</td>
<td>0 = Disabled, 1 = Auto Negotiate, 2 = 10 Half, 3 = 10 Full, 4 = 100 Half, 5 = 100 Full, 6 = 1000 Full</td>
</tr>
<tr>
<td>PC Port Remote Configuration</td>
<td>PCRemoteConfig</td>
<td>0 = Disabled, 1 = Auto Negotiate, 2 = 10 Half</td>
</tr>
<tr>
<td>Setting</td>
<td>System Variable</td>
<td>Values</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| SSH Access                      | sshAccess                   | 0 = Enabled  
1 = Disabled  |
| Incoming Call Toast Timer       | incomingCallToastTimer      | 0 = 0  
3 = 3  
4 = 4  
5 = 5  
6 = 6  
7 = 7  
8 = 8  
9 = 9  
10 = 10  
15 = 15  
30 = 30  
60 = 60 |
| Ring Locale                     | RingLocale                  | 0 = Default  
1 = Japan |
| TLS Resumption Timer            | TLSResumptionTimer          | 0-3600  
( Default = 3600 ) |
| FIPS Mode                       | fipsMode                    | 0 = Disabled  
1 = Enabled |
| Record Call Log From Shared Line| logCallFromSharedLine       | 0 = Disabled  
1 = Enabled |
| Minimum Ring Volume             | minimumRingVolume           | 0 = Silent  
1 = Volume Level 1  
2 = Volume Level 2  
3 = Volume Level 3  
4 = Volume Level 4  
5 = Volume Level 5  
6 = Volume Level 6  
7 = Volume Level 7  
8 = Volume Level 8  
9 = Volume Level 9  
10 = Volume Level 10  
11 = Volume Level 11 |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Firmware Sharing</td>
<td>peerFirmwareSharing</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Load Server</td>
<td>loadServer</td>
<td>Up to 256 character string</td>
</tr>
<tr>
<td>IPv6 Load Server</td>
<td>ipv6LoadServer</td>
<td>Up to 256 character string</td>
</tr>
<tr>
<td>Wireless Headset Hookswitch Control</td>
<td>ehookEnable</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Wideband Headset UI Control</td>
<td>headsetWidebandUIControl</td>
<td>0 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td>Wideband Headset</td>
<td>headsetWidebandEnable</td>
<td>0 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>wifi</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Back USB Port</td>
<td>usb1</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Side USB Port</td>
<td>usb2</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Console Access</td>
<td>ConsoleAccess</td>
<td>0 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>bluetooth</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Allow Bluetooth Contacts Import</td>
<td>btpbap</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Allow Bluetooth Mobile Handsfree Mode</td>
<td>bthfu</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Bluetooth Profiles</td>
<td>bluetoothProfile</td>
<td>0 = Handsfree</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Human Interface Device</td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>garp</td>
<td>0 = Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td>Show All Calls On Primary Line</td>
<td>allCallsOnPrimary</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
</tbody>
</table>

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
<table>
<thead>
<tr>
<th>Feature</th>
<th>Variable</th>
<th>Default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Server</td>
<td>webProtocol</td>
<td>0 = http and https Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = https only</td>
</tr>
<tr>
<td>IPv6 Log Server</td>
<td>ipv6LogServer</td>
<td>Up to 256 character string</td>
</tr>
<tr>
<td>Remote Log</td>
<td>remoteLog</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Log Profile</td>
<td>logProfile</td>
<td>0 = Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Preset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Telephony</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 = SIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 = UI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 = Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 = Media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 = Upgrade</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 = Accessory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 = Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 = Wi-Fi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 = VPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 = Energywise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13 = MobileRemoteAccess</td>
</tr>
<tr>
<td>Advertise G.722 and iSAC Codecs</td>
<td>g722CodecSupport</td>
<td>0 = Use System Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Enabled</td>
</tr>
<tr>
<td>Detect Unified CM Connection Failure</td>
<td>detectCMConnectionFailure</td>
<td>0 = Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Delayed</td>
</tr>
<tr>
<td>Power Negotiation</td>
<td>powerNegotiation</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Provide Dial Tone from Release Button</td>
<td>dialToneFromReleaseKey</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Background Image</td>
<td>defaultWallpaperFile</td>
<td>Up to 64 character string</td>
</tr>
<tr>
<td>Simplified New Call UI</td>
<td>simplifiedNewCall</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Revert to All Calls</td>
<td>revertToAllCalls</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Show Call History for Selected Line Only</td>
<td>showCallHistoryForSelectedLine</td>
<td>0 = Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Enabled</td>
</tr>
<tr>
<td>Actionable</td>
<td>actionableAlert</td>
<td>0 = Disabled</td>
</tr>
</tbody>
</table>

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Incoming Call Alert                         |                    | 1 = Show for all Incoming Call  
2 = Show for Invisible Incoming Call |
| DF Bit                                       | dfBit              | 0 = 0  
1 = 1                                                                         |
| Default Line Filter                         | defaultLineFilter  | Up to 5000 characters                                                       |
| Lowest Alerting Line State Priority         | lowAlertState      | 0 = Disabled  
1 = Enabled                                                                   |
| One Column Display for KEM                  | kemOneColumn       | 0 = Disabled  
1 = Enabled                                                                   |
| Energy Efficient Ethernet (EEE): PC Port    | EnableEEEPcPort    | 0 = Disabled  
1 = Enabled                                                                   |
| Energy Efficient Ethernet (EEE): SW Port    | EnableEEESwPort    | 0 = Disabled  
1 = Enabled                                                                   |
| User Credentials Persistent for Expressway Sign in | PasswordPersistenceForCollaborationEdge | 0 = Disabled  
1 = Enabled                                                                   |
| Customer support upload URL                 | problemReportUploadURL | Up to 256 character string                                               |
| Web Admin                                   | webAdmin           | 0 = Disabled  
1 = Enabled                                                                   |
| Admin Password                              | adminPassword      | 8 to 127 character string                                                  |
| WLAN SCEP Server                            | wlanScepServer     | Up to 256 character string                                                 |
| WLAN Root CA Fingerprint (SHA256 or SHA1)   | wlanRootCaFingerprint | Up to 95 character string                                                |
| WLAN Authentication Attempts                | wlanAuthAttempts   | 1 = 1  
2 = 2  
3 = 3                                                                         |
| WLAN Profile 1 Prompt Mode                  | promptMode1        | 0 = Disabled  
1 = Enabled                                                                   |
| Line Mode                                   | lineMode           | 0 = Session Line Mode  
1 = Enhanced Line Mode                                                         |
| Admin Configurable Ringer                   | adminConfigurableRinger | 0 = Disabled  
1 = Sunrise  
2 = Chirp1                                                                      |
For more information on these features, see the Cisco IP Phone 8800 Series Administration Guide or the Cisco IP Phone 8800 Series Release Notes.


### Configuring the Cisco IP Phone 8861 and 8865

**Wi-Fi Profile Configuration**

To configure the Wi-Fi settings on the Cisco IP Phone 8861 and 8865, either use an Ethernet network to connect to a Cisco Unified Communications Manager or use the local user interface and keypad.

**Automatic Provisioning**

For automatic provisioning of the Wi-Fi Profiles, the Cisco IP Phone 8861 and 8865 needs to be connected to a network via Ethernet or via Wi-Fi, which has connectivity to the Cisco Unified Communications Manager.

With connectivity to a Cisco Unified Communications Manager 10.0 or later, Wi-Fi profile configuration data can be downloaded and applied to the Cisco IP Phone 8861 and 8865.

Cisco Unified Communications Manager 11.0 or later is required if wanting to download and apply a Wi-Fi profile including EAP-TLS authentication.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Support Use</td>
<td>customerSupportUse</td>
</tr>
<tr>
<td></td>
<td>Up to 64 character string</td>
</tr>
<tr>
<td>Disable TLS Ciphers</td>
<td>disableTLSCiphers</td>
</tr>
<tr>
<td></td>
<td>0 = None</td>
</tr>
<tr>
<td></td>
<td>1 = TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td></td>
<td>2 = TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td></td>
<td>3 = TLS_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td></td>
<td>4 = TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td></td>
<td>5 = TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td></td>
<td>6 = TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td></td>
<td>7 = TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>Start Video Port</td>
<td>startVideoPort</td>
</tr>
<tr>
<td></td>
<td>2048-65535</td>
</tr>
<tr>
<td>Stop Video Port</td>
<td>stopVideoPort</td>
</tr>
<tr>
<td></td>
<td>2048-65535</td>
</tr>
</tbody>
</table>
For more information, see the Cisco Unified Communications Manager > Wireless LAN Profiles section.

Certificates can also be automatically installed utilizing a network connection.
For more information, see the Simplified Certificate Enrollment Protocol (SCEP) section.

**Local User Interface**

Use the following guidelines to configure the Wi-Fi Profiles via the local keypad.

- Navigate to Applications > Admin settings > Network setup > Wi-Fi client setup.
- Ensure that Wireless is set to On (default = Off).
  Ensure Wi-Fi is enabled in the Cisco Unified Communications Manager.
  If there is an active Ethernet connection, then Wi-Fi will be disabled and Ethernet must be disconnected before Wi-Fi can be enabled.
- **Wi-Fi sign in access** can be set to On to enable shortcut access in the Applications menu in order to update the username or password if using 802.1x authentication.
- **Wi-Fi sign in access** must be set to On in order for the phone to prompt the user to enter the password when WLAN Profile 1 Prompt Mode is Enabled or to prompt the user to enter the password when there are authentication failures using the configured WLAN Authentication Attempts setting.

Configure the Wi-Fi settings either manually or use the configuration wizard, which is available as of the 11.5(1)SR1 release.

**Wi-Fi Profile Configuration Wizard**

- If the SSID is broadcasted, then can utilize the Wi-Fi profile configuration wizard by selecting Applications > Admin settings > Network setup > Wi-Fi client setup > Network name.
- The **Security mode** and **802.11 mode** will be learned automatically, which is determined based on the SSID’s configuration.
- Enter the additional credentials depending on the security mode selected.
- If the SSID is enabled either on 5 GHz only or on 2.4 GHz only, then **802.11 mode** will not be configurable.

- If the SSID is 802.1x enabled, then Cisco IP Phone 8861 and 8865 will dynamically select the EAP type if set to **Auto**, which is determined based on the RADIUS server’s configuration.

- Select **Connect** once the configuration has been completed.
Manual Wi-Fi Profile Configuration

- Enter Applications > Admin settings > Network setup > Wi-Fi client setup > Network name, then select Other. Select Connect after making the necessary changes or Cancel to discard the changes.

- Below lists the available security modes supported and the key management and encryption types that can be used for each mode.

  The key management and encryption type (cipher) will be auto-configured based on the access point’s current configuration, where precedence is giving to the strongest key management type enabled (e.g. WPA2) then the strongest cipher enabled (e.g. AES).

<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>
<tr>
<td>WEP</td>
<td>N/A</td>
<td>Static</td>
<td>WEP</td>
</tr>
<tr>
<td>PSK</td>
<td>N/A</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>EAP-FAST</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>EAP-TLS</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
</tbody>
</table>
• If wanting to configure a wireless network profile without security (open security), then simply enter the **SSID** and select **None** for the security type.

  Select **Connect** after making the necessary changes.

• If selecting **WEP** as the security mode, then a **static WEP key (password)** must be entered. Only key index 1 is supported, so will want to ensure that only key index 1 is configured on the access point. Select **Connect** after making the necessary changes.

<table>
<thead>
<tr>
<th>Key Style</th>
<th>Key Size</th>
<th>Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>40/64 bit</td>
<td>5</td>
</tr>
<tr>
<td>ASCII</td>
<td>104/128 bit</td>
<td>13</td>
</tr>
<tr>
<td>HEX</td>
<td>40/64 bit</td>
<td>10 (0-9, A-F)</td>
</tr>
<tr>
<td>HEX</td>
<td>104/128 bit</td>
<td>26 (0-9, A-F)</td>
</tr>
</tbody>
</table>

• If selecting **PSK** as the security mode, then a Pre-Shared Key (passphrase) must be configured.
Enter the ASCII or hexadecimal formatted password. Select Connect after making the necessary changes.

<table>
<thead>
<tr>
<th>Key Style</th>
<th>Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>8-63</td>
</tr>
<tr>
<td>HEX</td>
<td>64 (0-9,A-F)</td>
</tr>
</tbody>
</table>

- If selecting EAP-FAST, PEAP-GTC, or PEAP-MSCHAPv2 as the security mode, then a username and password must be configured.
  Select Connect after making the necessary changes.

- The root CA certificate of the CA chain that issues the RADIUS server certificates can optionally be installed either via SCEP or manually via the admin webpage if wanting to enable server validation for PEAP-GTC or PEAP-MSCHAPV2. Server validation is automatically enabled once a server certificate is installed.
• If selecting EAP-TLS as the security mode, then must configure the type of user certificate to use. If **User installed** is selected, then will need to have a user certificate installed either manually via the admin webpage or via SCEP. Select **Connect** after making the necessary changes.

• The root CA certificate of the CA chain that issues the RADIUS server certificates must be installed to enable server validation when using EAP-TLS. Server validation is automatically enabled once a server certificate is installed.
• Select one of the following 802.11 modes to set the frequency band, then **Save**.
  
  - **Auto**
  - **2.4 GHz**
  - **5 GHz**

  **Auto** mode will scan both 2.4 GHz and 5 GHz channels and attempt to associate to the access point with the strongest signal.

  **2.4 GHz** mode will only scan 2.4 GHz channels and **5 GHz** mode will only scan 5 GHz channels, then will attempt to associate to an available access point.

  It is recommended to set the frequency band on the Cisco IP Phone 8861 and 8865 to 5 GHz when wanting to utilize the 5 GHz frequency band only, which prevents scanning and potentially roaming to the 2.4 GHz frequency band.

• In the **IPv4 setup** or **IPv6 setup**, Dynamic Host Configuration Protocol (DHCP) or static IP settings can be configured. Select **Apply** after making the necessary changes or **Revert** to discard the changes.
If option 150 or 66 is not configured to provide the TFTP Server’s IP address via the network’s DHCP scope, then set Alternate TFTP to On and enter the IP address for the TFTP Server.

Select Apply after making the necessary changes or Revert to discard the changes.

The current network settings can be cleared by selecting Applications > Admin settings > Reset settings > Network settings.

Note: The Cisco IP Phone 8861 and 8865 only support a single wireless LAN profile.

802.11r (FT) or CCKM will be negotiated if enabled on the access point when using EAP-FAST, EAP-TLS, PEAP-GTC, or PEAP-MSCHAPv2, where preference is given to 802.11r (FT).
WPA3 is not supported.

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
802.1x-SHA2 key management is not supported.
CCMP256, GCMP128, and GCMP256 encryption ciphers are not supported.
WEP128 is listed as WEP104 on the Cisco Wireless LAN Controllers.

For more information, refer to the Configuring Settings on the Cisco IP Phone 8800 Series in the Cisco IP Phone 8800 Series Administration Guide at this URL:

Certificate Management
The Cisco IP Phone 8861 and 8865 can utilize X.509 digital certificates for EAP-TLS or to enable Server Validation when using PEAP-GTC or PEAP-MSCHAPV2.
A User Certificate can be installed either automatically via Simple Certificate Enrollment Protocol (SCEP) or manually via the phone’s admin webpage interface (https://x.x.x.x:8443).
A Server Certificate can be installed either automatically via Simple Certificate Enrollment Protocol (SCEP) or manually via the phone’s admin webpage interface (https://x.x.x.x:8443).
Only 1 certificate per certificate type is allowed; 1 User Certificate and 1 Server Certificate (either via SCEP or manual method).
Once a certificate is installed, Server Validation is automatically enabled if configured for EAP-TLS, PEAP-GTC, or PEAP-MSCHAPV2.
Microsoft® Certificate Authority (CA) servers are recommended. Other CA server types may not be completely interoperable with the Cisco IP Phone 8861 and 8865.
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-256 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.

Manual Installation
For out of box (factory reset) manual installation, the admin webpage interface is Enabled, the username is fixed to admin, and the password is temporarily set to Cisco.
The temporary password will no longer be available once the phone registers to Cisco Unified Communications Manager.
The admin webpage interface will be Disabled on the phone once it registers to Cisco Unified Communications Manager regardless if it contains support for the Web Admin and Admin Password options.
Once the phone has registered to CUCM, set **Web Admin** to **Enabled** in CUCM to enable the admin webpage interface. Then configure **Admin Password** by specifying a 8-127 character string.

If wanting to keep the admin webpage interface access enabled long-term, then should utilize a secure profile with TFTP encryption enabled.

For out of box (factory reset), will need to ensure the date and time is configured correctly. Can set the **Date & Time** by syncing to the local machine or setting the **Date & Time** manually.
Can utilize either the internal Manufacturing Installed Certificate (MIC) or a custom User Installed certificate to be used as the User Certificate for EAP-TLS.

**Manufacturing Installed Certificate (MIC)**

The pre-installed Manufacturing Installed Certificate (MIC) can be used as the User Certificate for EAP-TLS. The MIC’s CA chain must be exported and added to the RADIUS server’s trust list if wanting to use the MIC as the User Certificate for EAP-TLS.

Click **Export** to download the root and sub CA certificates from the admin webpage interface.

**User Installed Certificate**

To manually install a user certificate for EAP-TLS, select **Install** for **User Installed** on the main certificates webpage. Select **Browse** to point to the user certificate in PKCS #12 format (.p12 or .pfx).

Enter the **Extract password** (up to 12 characters), then select **Upload**.

Ensure the CA chain that issued the user certificate is added to the RADIUS server’s trust list.

Will need to restart the Cisco IP Phone 8861 or 8865 after all certificates are installed.

**Server Certificate**
The root CA certificate that issued the RADIUS server’s certificate must be installed for **EAP-TLS** or to enable **Server Validation** for **PEAP-GTC** or **PEAP-MSCHAPV2**.

To manually install a server certificate, select **Install** for **Authentication Server CA** on the main certificates webpage. Select **Browse** to point to the server certificate with **PEM (Base-64)** or **DER** encoding.

Will need to restart the Cisco IP Phone 8861 or 8865 after all certificates are installed.

**Simple Certificate Enrollment Protocol (SCEP)**

SCEP is the standard for automatically provisioning and renewing certificates avoiding manual installation and re-installation of certificates on clients.

A Cisco IOS Registration Agent (RA) (e.g. Cisco IOS router) can serve as a proxy (e.g. SCEP RA) to the SCEP enabled CA that is to issue certificates.

Need to ensure that the same CA chain is used for issuing certificates to the phones as well as for the RADIUS servers; otherwise server validation could fail.

For initial certificate enrollment via SCEP, the Cisco IP Phone 8861 and 8865 needs to be connected to an Ethernet network which has connectivity to the Cisco Unified Communications Manager.

The Cisco IP Phone 8861 & 8865 utilizes the following parameters defined in Cisco Unified Communications Manager for SCEP requests.

The **WLAN SCEP Server** must be configured to include either the IP address or hostname of the SCEP RA.

The **WLAN Root CA Fingerprint (SHA256 or SHA1)** must be configured to include the fingerprint of the CA that issuing the certificates. If the issuing CA in which the SCEP RA is enrolled to is a subordinate CA, then enter its fingerprint and not the fingerprint of the root CA. The defined fingerprint is used to validate the received certificate.

Removing these parameters will disable SCEP.
The Cisco IP Phone 8861 & 8865 then sends a SCEP enroll request to the SCEP RA including the phone’s Manufacturing Installed Certificate (MIC) as the Proof of Identity (POI).

The SCEP RA validates the phone’s MIC using the certificate of the subordinate CA that issued the phone’s MIC, then passes it to the RADIUS server for further device authentication.

The RADIUS server validates the device and sends a response to the SCEP RA.

The SCEP RA then forwards the enroll request to the CA if RADIUS authentication was successful.

The SCEP RA receives the user certificate from the CA and sends it to the phone after it receives a poll request from the phone.

The Cisco IP Phone 8861 and 8865 will periodically check the user and server certificate expiration periods.

Certificate renewal will occur every 24 hours until successful when the expiration date is within 50 days.

If the CA certificate used to define the WLAN Root CA Fingerprint (SHA256 or SHA1) has expired, then the phone will send a SCEP getca request for a new CA certificate, but the admin would need to update the fingerprint in the phone’s configuration within Cisco Unified Communication Manager to match the new CA certificate prior so it can be successfully validated. The old CA certificate will then be removed if the new one is successfully received from the CA.

If the user certificate has expired, the phone will send a new SCEP enroll request to update the user certificate. The old user certificate will then be removed if a new user certificate is successfully received from the CA.

If the WLAN SCEP Server or WLAN Root CA Fingerprint (SHA256 or SHA1) has been modified, then the Cisco IP Phone 8861 and 8865 will attempt to update the CA and user certs immediately.

Certificate Authority (CA) Configuration

Is recommended to use Microsoft® Certificate Authority (CA) servers.

Use the following guidelines to configure the Microsoft CA.

- Create Certificate Authority and Active Directory Domain Service on Microsoft Windows server.
- Enable Network Device Enrollment Service.

- Make Administrator a member of IIS_IUSERS group by going to MemberOf tab of user property screen.

- Launch Server Manager, then click Add roles.
• On the Select Server Role page, select the Active Directory Certificate Services role, then click Next.

• Add the Network Device Enrollment Service role service.
• In the Add Roles Wizard, on the Select Role Services page, select the Network Device Enrollment Service check box, then click Next.

![Add Role Services](image)

• The wizard will detect whether all the required dependencies are installed. If any dependencies are missing, you will be prompted with a dialog box explaining what is missing and requesting your permission to install the dependencies. Click Yes to continue the installation.

• Click User Account under Role Services and then click Select User....
• Type in **Administrator** as the user name, then enter the password.

• Enter the Registration Authority information.
- Select **Microsoft Strong Cryptographic Provider** for Signature Key CSP and Encryption key CSP.
- Select **2048** for Key character length.
Select **Install**.

**Active Directory Certificate Services**

- **Network Device Enrollment Service**
  - Account: YD-MSCA\Administrator
  - RA Information:
    - Name: YD-MSCA-W2K8-MSCP-RA
    - Country: US
    - Email: <None>
    - Company: <None>
    - Department: <None>
    - City: <None>
    - State: <None>
  - Signature Key CSP: Microsoft Strong Cryptographic Provider
  - Signature Key Length: 2048
  - Exchange Key CSP: Microsoft Strong Cryptographic Provider
  - Challenge Phrase URL: https://YD-MSCA-W2K8/certenv/mscp_admin

Print, email, or save this information.
A confirmation page will be displayed if the installation was successful.

- Disable SCEP enrollment challenge password requirement via `regedit` by setting `EnforcePassword` to 0.  
  (`HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword`)

- SCEP uses the certificate template that is set in the registry for issuing certificates.  
  (`HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP`
• Typically the RA will have a longer period (same as that of the CA certificate).
• The default template used for RA to be enrolled to the SCP server is **IPSECIntermediateOffline** as highlighted above.
• Make sure a correct template is set to the above registries before enrolling the RA to the SCEP server.
• After the Cisco RA is enrolled to the SCEP server, admin needs to change the template in the registry (if the user certificate period needs to be shorter than that of the root CA).

  • Right click **Certificate Templates** then select **Manage**.

  • Right click **User template** then select **Duplicate Template**.
  • Select **Windows Server 2003 2008 Template**.
  • Under the **General** tab, change template name and validity period.
  • Under the **Extensions** tab, ensure the following:
    • **Client Authentication** is set as one of the application policies
    • **Key Usage** has **Digital Signature** attribute
Configure the **Validity Period** on the **General** tab as necessary.
- Configure **Subject Name** tab as shown below.
• Configure **Extensions** tab as shown below.
- Configure **Algorithm Name**, **Minimum Key Size**, and **Request Hash** as necessary on the **Cryptography** tab.
- Enable the newly created template by right clicking **Certificate Templates** then selecting **New > Certificate Template to Issue**.

- Select **SCEP User** template.
Associate the newly created template to SCEP via `regedit`.

Go to IIS > Application Pools to stop then start the SCEP service for the new template to take effect.

RADIUS Configuration
Use the following guidelines to configure the RADIUS server.

- Add the SCEP RA under **Network Device and AAA Clients**.
- Configure the RADIUS shared secret that the SCEP RA is currently configured for.
• Create a user account matching the common name of the phone’s Manufacturing Installed Certificate (MIC) with the password set to `cisco` (e.g. CP-8861-SEPxxxxxxxxxxx or CP-8865-SEPxxxxxxxxxxx).

• Add the Cisco Manufacturing CA chain to the RADIUS trust list as well as any other CA chains utilized for authentication.
- Create a **Certificate Authentication Profile**.

- Create an **Identity Store Sequence** to be used for EAP-TLS authentication.
- Check **Certificate Based**, select the newly created **Certificate Authentication Profile**, and select **Internal Users** as the additional identity store.
• Create an **Identity Store Sequence** to be used for SCEP authentication.
• Check **Password Based**, select the newly created **Certificate Authentication Profile**, and select **Internal Users** as the identity store.
• Create an **Authorization Profile** to be used for SCEP authorization.
Under the RADIUS Attributes tab, add the **cisco-av-pair** attribute where the **Type** is set to **String** and **Value** is set to `pki:cert-application=all`. 
- Create an **Access Policy** to be used for EAP-TLS authentication.
For the **Access Service** for EAP-TLS authentication, need to ensure that **EAP-TLS** is enabled.
• Under **Identity**, rules can be defined to match EAP type then determine which identity source to use for authentication.
- Under **Identity**, rules can be defined to match various conditions then determine which authorization profile to use.

- Create an **Access Policy** to be used for SCEP authentication.
For the **Access Service** for SCEP authentication, need to ensure that **PAP/ASCII** is enabled.
• Under **Identity**, rules can be defined to match various conditions then determine which identity source to use for authentication.
Under **Identity**, rules can be defined to match various conditions then determine which authorization profile to use.

---

**SCEP RA Configuration**

Currently only a Cisco IOS router running IOS version 15.1(4)M10 or later is supported as the SCEP RA.

Use the following guidelines to configure a Cisco IOS router as a SCEP RA.

- Enable HTTP server on the Cisco IOS router.

  ```
  ISR_RA# configure terminal
  ISR_RA(config)# ip http server
  ISR_RA(config)# exit
  ```

- Configure a RADIUS server for device authentication.

  ```
  ISR_RA# configure terminal
  ISR_RA(config)# radius server MyRadius
  ISR_RA(config-radius-server)# address ipv4 10.195.19.63 auth-port 1812 acct-port 1813
  ISR_RA(config-radius-server)# key <REMOVED>
  ISR_RA(config-radius-server)# exit
  ISR_RA(config)# aaa authorization network PhoneList group radius
  ISR_RA(config)# exit
  ```

- Configure a PKI trustpoint for the MIC’s CA chain to validate the phone’s MIC.
ISR_RA# configure terminal
ISR_RA(config)# crypto pki trustpoint MIC_trustpoint
ISR_RA(ca-trustpoint)# authorization list PhoneList
ISR_RA(ca-trustpoint)# authorization username subjectname commonname
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# crypto pki trustpoint MIC_trustpoint
ISR_RA(ca-trustpoint)# enrollment terminal
ISR_RA(ca-trustpoint)# revocation-check none
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# crypto pki authenticate MIC_trustpoint

Enter the base 64 encoded Manufacturing CA certificate. End with a blank line or the word quit on a line by itself.

-----BEGIN CERTIFICATE-----
MIIEZTCCA02gAwIBAgIBAwJAbAgMEAOggjxftoMG0GCSqGSIb3DEQjBgAAHj0cCwAwYD
QJBiQHMA0GCSqGSIb3DEQjBAogIBAgIAKghOjB2mV1qIdUL7A7LbH1oW5U2J+wC5yG
xXJ5A0f7HlY1C7cBdFJDZpEyQFh8hknz/B71w5pGCTGMCiEwOQYDVR0PBBxOgAwRyw
BIJh5EO0jx67zMa5m0Qfj1P5XzCGxfTy2s37OvYxZ5MNrTt0T6H7zSgPuOvFt60Kw0
-----END CERTIFICATE-----

Trustpoint 'MIC_trustpoint' is a subordinate CA and holds a non self-signed cert.
Certificate has the following attributes:
Fingerprint MD5: AC14F08F C3780F8F D9EEE6C9 39111280
Fingerprint SHA1: 90B2E06B 7AD5DAFF CDF43187 2909F381 37471BF8

-----END CERTIFICATE-----

Trustpoint 'MIC_trustpoint' is a subordinate CA and holds a non self-signed cert.
Certificate has the following attributes:
Fingerprint MD5: AC14F08F C3780F8F D9EEE6C9 39111280
Fingerprint SHA1: 90B2E06B 7AD5DAFF CDF43187 2909F381 37471BF8
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
ISR_RA(config)# exit

- Configure a PKI trustpoint and PKI server to enroll to the CA server.

ISR_RA# configure terminal
ISR_RA(config)# crypto pki trustpoint MSCA
ISR_RA(config)# enrollment mode ra
ISR_RA(config)# enrollment url http://10.81.116.249/certsrv/mscep/mscep.dll
ISR_RA(config)# serial-number
ISR_RA(config)# fingerprint 81512B43164290925C6891701B374EBD254447
ISR_RA(config)# revocation-check none
ISR_RA(config)# rsakeypair MSCA_Key 2048
ISR_RA(config)# exit
ISR_RA(config)# crypto pki server MSCA
ISR_RA(config)# grant auto trustpoint MIC_trustpoint
ISR_RA(config)# hash sha1
ISR_RA(config)# mode ra transparent
ISR_RA(config)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Re-enter password:
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 22 seconds)
Certificate has the following attributes:
Fingerprint MD5: CDE40276 04A28DA8 BDE5DF48 0BC1A8F7
Fingerprint SHA1: 81512B43 16429092 925C6891 701B374 EBD254447
Trustpoint Fingerprint: AE5CDEF2 A633DEF4 1D5A5104 7D6A8BD7 E08B576C
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: ISR_RA
% The serial number in the certificate will be: <REMOVED>
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose MSCA' command will show the fingerprint.
% Enrollment in progress...
ISR_RA(config)#% Exporting Certificate Server signing certificate and keys...
Feb 17 15:21:42: CRYPTO_PKI: Certificate Request Fingerprint MD5: CDE40276 04A28DA8 BDE5DF48 0BC1A8F7
Feb 17 15:21:42: CRYPTO_PKI: Certificate Request Fingerprint SHA1: AE5CDEF2 A633DEF4 1D5A5104 7D6A8BD7 E08B576C
Feb 17 15:21:43: %PKI-6-CERTRET: Certificate received from Certificate Authority
Sample Configuration

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SCEP-RA
!
boot-start-marker
boot system flash c3845-advsecurityk9-mz.151-4.M10.bin
boot-end-marker
!
enable password <REMOVED>
!
aaa new-model
!
aaa authentication login default local
aaa authorization network PhoneList group radius
!
aaa session-id common
!
dot11 syslog
ip source-route
!
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
crypto pki server MSCA
  grant auto trustpoint MIC_trustpoint
  hash sha1
  mode ra transparent
crypto pki token default removal timeout 0
!
crypto pki trustpoint MIC_trustpoint
  enrollment terminal
  revocation-check none
  authorization list PhoneList
  authorization username subjectname commonname
!
crypto pki trustpoint MSCA
  enrollment mode ra
  serial-number
  fingerprint 81512B4316429092925C6891701B374EBD254447
  revocation-check none
  rsakeypair MSCA_Key 2048
!
crypto pki certificate chain MIC_trustpoint
  certificate ca 02
```
![ansi]

AE4949D1 97B6A380 08AC4ABB 23A30B34 27A0A112 C63D6BFD 476C4F4B 2DBBB200
D5BDF499 F5068067 85123637 E3EBF106 7D2AF2D0 87DCF856 34E937BF 246C41BD
C0781E14 A22BCC66 2151F46B 5AD4314C 345E8871 41830E80 5D5A8416 21C5220D
409449E6 E2161582 2113833C 982B68AE 1B5E206E BC535C5B A28E1210 E7FB5296
27DB54AF 20A3FA02 5A

!  
license udi pid CISCO3845-MB sn <REMOVED>
archive
log config
hidekeys
username <REMOVED> privilege 15 password 0 <REMOVED>
!
redundancy
!
interface GigabitEthernet0/0
ip address 10.195.19.65 255.255.255.128
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
media-type rj45
!
ip default-gateway 10.195.19.1
ip forward-protocol nd
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.195.19.1
!
radius server MyRadius
address ipv4 10.195.19.63 auth-port 1812 acct-port 1813
key <REMOVED>
!
control-plane
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
transport input all
line vty 5 15
exec-timeout 0 0
transport input all
!
scheduler allocate 20000 1000
end

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide 231
Certificate Removal

Certificates can be removed either via the admin webpage interface or via the local user interface. To remove a certificate via the admin webpage, select **Delete** for the corresponding certificate, then restart the phone once a certificate has been removed.

![Certificate Removal](image)

Bluetooth Settings

The Cisco IP Phone 8861 and 8865 have Bluetooth support, which enables hands-free communications. To pair a Bluetooth headset to the Cisco IP Phone 8861 and 8865, follow the instructions below.

- Navigate to Applications > Bluetooth.
- Ensure that **Bluetooth** is set to **On**.
  - Ensure **Bluetooth** is enabled in the Cisco Unified Communications Manager; otherwise the option will not be visible in the settings menu.
- Select **Add Bluetooth device**.
  - Ensure the Bluetooth device is in pairing mode.

  ![Bluetooth Settings](image)

- Select the Bluetooth device after it is displayed in the list.
- The Cisco IP Phone 8861 and 8865 will then attempt to pair will attempt to use the pin code **0000**. If unsuccessful, enter the pin code when prompted.
- Once paired, then the Cisco IP Phone 8861 and 8865 will attempt to connect to the Bluetooth device.
• Selecting the Bluetooth device then selecting **Disconnect** will disconnect that currently connected Bluetooth device.

• Select **Delete** to unpair the selected Bluetooth device.

• Selecting **Show detail** will display additional details of the Bluetooth device.
Mobile Phone Sharing

The Cisco IP Phone 8861 and 8865 support mobile phone sharing where a mobile phone can be paired to it.

- Ensure **Hand-free-2-way audio** is set to **On**.
- Ensure the Bluetooth enabled mobile phone is in pairing mode, then select the device in the list.
- A security prompt will then be displayed to authorize and initiate pairing.
- Select **Pair** once the passkey has been confirmed.
• Once paired, then the Cisco IP Phone 8861 or 8865 will attempt to connect to the Bluetooth enabled mobile phone.
• A prompt then will be displayed to select whether the contacts and call history from the Bluetooth enabled mobile phone should be stored locally in the Cisco IP Phone 8861 or 8865 or not.
  Need to ensure that **Allow Bluetooth Contacts Import** is enabled in the Cisco Unified Communications Manager.

• Contacts access can be disabled if previously enabled by selecting **Disable** in the **Settings** menu.

• Selecting **Show detail** within the **Settings** menu will display additional details of the Bluetooth device.
• The Cisco IP Phone 8861 and 8865 can answer calls bound for the Bluetooth enabled mobile phone and make outbound calls utilizing the mobile phone’s line.

  Need to ensure that **Allow Bluetooth Mobile Handsfree Mode** is enabled in the Cisco Unified Communications Manager.

• Calls can easily be moved between the Cisco IP Phone 8861 or 8865 and the Bluetooth enabled mobile phone.

• To move a call from the Bluetooth enabled mobile phone to the Cisco IP Phone 8861 or 8865, simply select the **Move audio** softkey on the Cisco IP Phone 8861 or 8865.

• The call will then be directed to the Cisco IP Phone 8861 or 8865 via the Bluetooth enabled mobile phone.

• Select **Move audio** to switch the call back to the Bluetooth enabled mobile phone.
Video Call Settings

Video call settings for the Cisco IP Phone 8865 can be configured by selecting Applications > Settings > Video.

Brightness can be configured to accommodate for the current working environment by selecting Exposure within the phone settings.

The video bandwidth can be configured as necessary depending on the current working environment. This is set to Auto by default, which enables video bandwidth adaptation.

Upgrading Firmware

Cisco Unified Communications Manager

To upgrade the firmware, install the signed COP file for Cisco Unified Communications Manager.

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 IP Phone 8861 or 8865 then downloads the firmware files to flash if it is not running the specified image already.

The Load Server can be specified as an alternate TFTP server to retrieve firmware files, which is located in the product specific configuration section of Cisco IP Phone 8861 and 8865 within Cisco Unified Communications Manager Administration.
Cisco IP Phone 8861 and 8865

Cisco Unifi Communications Manager Express

To install the firmware on Cisco Unified Communications Manager Express, extract the contents of the TAR file and upload into the router’s flash. Each file will need to be enabled for TFTP download. Configure the phone load and reset the phones to upgrade the firmware.

8861 Example:

tftp-server flash:/8861/sip88xx.12-7-1-0001-393.loads alias sip88xx.12-7-1-0001-393.loads
tftp-server flash:/8861/boot1288xx.BE-01-007.sbn alias boot1288xx.BE-01-007.sbn
tftp-server flash:/8861/fbi88xx.BE-01-012.sbn alias fbi88xx.BE-01-012.sbn
tftp-server flash:/8861/kern88xx.12-7-1-0001-393.sbn alias kern88xx.12-7-1-0001-393.sbn
tftp-server flash:/8861/kern288xx.12-7-1-0001-393.sbn alias kern288xx.12-7-1-0001-393.sbn
tftp-server flash:/8861/kern388xx.12-7-1-0001-393.sbn alias kern388xx.12-7-1-0001-393.sbn
tftp-server flash:/8861/m0patch288xx.BE-01-001.sbn alias m0patch288xx.BE-01-001.sbn
tftp-server flash:/8861/preloader88xx.BE-01-002.sbn alias preloader88xx.BE-01-002.sbn
tftp-server flash:/8861/rootfs88xx.12-7-1-0001-393.sbn alias rootfs88xx.12-7-1-0001-393.sbn
tftp-server flash:/8861/rootfs288xx.12-7-1-0001-393.sbn alias rootfs288xx.12-7-1-0001-393.sbn
tftp-server flash:/8861/rootfs388xx.12-7-1-0001-393.sbn alias rootfs388xx.12-7-1-0001-393.sbn
tftp-server flash:/8861/sb288xx.BE-01-026.sbn alias sb288xx.BE-01-026.sbn
tftp-server flash:/8861/sb2288xx.BE-01-013.sbn alias sb2288xx.BE-01-013.sbn
tftp-server flash:/8861/sb2388xx.BE-01-027.sbn alias sb2388xx.BE-01-027.sbn
tftp-server flash:/8861/ssb288xx.BE-01-007.sbn alias ssb288xx.BE-01-007.sbn
tftp-server flash:/8861/ve488xx.12-7-1-0001-393.sbn alias ve488xx.12-7-1-0001-393.sbn

voice register global
load 8861 sip88xx.12-7-1-0001-393

8865 Example:

tftp-server flash:/8865/sip8845_65.12-7-1-0001-393.loads alias sip8845_65.12-7-1-0001-393.loads
tftp-server flash:/8865/fbi8845_65.BEV-01-006.sbn alias fbi8845_65.BEV-01-006.sbn
tftp-server flash:/8865/kern8845_65.12-7-1-0001-393.sbn alias kern8845_65.12-7-1-0001-393.sbn
tftp-server flash:/8865/rootfs8845_65.12-7-1-0001-393.sbn alias rootfs8845_65.12-7-1-0001-393.sbn
tftp-server flash:/8865/rootfs28845_65.12-7-1-0001-393.sbn alias rootfs28845_65.12-7-1-0001-393.sbn
tftp-server flash:/8865/rootfs38845_65.12-7-1-0001-393.sbn alias rootfs38845_65.12-7-1-0001-393.sbn
tftp-server flash:/8865/sb28845_65.BEV-01-015.sbn alias sb28845_65.BEV-01-015.sbn
tftp-server flash:/8865/ve48845_65.12-7-1-0001-393.sbn alias ve48845_65.12-7-1-0001-393.sbn

voice register global
load 8865 sip8845_65.12-7-1-0001-393

IP Phone Services

The Cisco IP Phone 8861 and 8865 are capable of supporting Extensible Markup Language (XML) applications.

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
For information on IP phone services configuration, refer to the following URL.

**Extensible Markup Language (XML)**

The following document provides the information needed for eXtensible Markup Language (XML) and X/Open System Interface (XSI) programmers and system administrators to develop and deploy IP phone services.


**Troubleshooting**

**Problem Report Tool**

A problem report can be created via the Problem Report Tool by selecting the **Report Problem** softkey at **Applications > Phone information**.

The date and time and problem description can be defined.

The **Customer support upload URL** option in Cisco Unified Communications Manager can be configured per phone to obtain the logs or manually download the logs from the phone’s webpage under **Console Logs**.

![Problem reporting tool](image)

**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**

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
<?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.");
}

?type>
The admin webpage interface ([https://x.x.x.x:8443](https://x.x.x.x:8443)) contains all of the info as the standard read-only page plus a few extra configurable pages (i.e. Certificates, Date and time, and Phone restart). To access the admin webpage interface, **Web Admin** must be enabled and **Admin Password** must be configured in Cisco Unified Communications Manager.

**Device Information**

The Cisco IP Phone 8861 and 8865 provide device information, where network status, MAC address and version information is displayed.

Browse to the standard web interface ([https://x.x.x.x](https://x.x.x.x)) of the Cisco IP Phone 8861 or 8865 select **Device information** to view this information.

![Device Information Table]

**Network Setup**

Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide
The Cisco IP Phone 8861 and 8865 provide network setup information, where network and Cisco Unified Communications Manager information is displayed.

Browse to the standard web interface (https://x.x.x.x) of the Cisco IP Phone 8861 or 8865 then select **Network setup** to view this information.

---

![Network setup table](image)

**Streaming Statistics**

The Cisco IP Phone 8861 and 8865 provide call statistic information, where codec type, jitter and packet count info, etc. is displayed.

Browse to the standard web interface (https://x.x.x.x) of Cisco IP Phone 8861 or 8865 then select the necessary menu item under **Streaming statistics** to view this information.
**Device Logs**

Console logs, core dumps, status messages, and debug display can be obtained from the web interface of Cisco IP Phone 8861 or 8865 for troubleshooting purposes.

**Console Logs**

Browse to the standard web interface (https://x.x.x.x) of Cisco IP Phone 8861 or 8865 then select **Console Logs** to view this information.

---

### Streaming statistics

**Cisco IP Phone CP-8865 (SEPAC7E8AB763B6)**

<table>
<thead>
<tr>
<th>Device Information</th>
<th>Network setup</th>
<th>Network statistics</th>
<th>Ethernet Information</th>
<th>Access</th>
<th>Network</th>
<th>Device logs</th>
<th>Console logs</th>
<th>Core dumps</th>
<th>Status messages</th>
<th>Debug display</th>
<th>Streaming statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote address</td>
<td>10.81.12.27/22280</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local address</td>
<td>10.81.12.32/29120</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start time</td>
<td>7:21:39pm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream status</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host name</td>
<td>SEPAC7E8AB763B6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender packets</td>
<td>1030</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender octets</td>
<td>51500</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender codec</td>
<td>OPUS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender reports sent</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender report time sent</td>
<td>7:21:55pm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rxr lost packets</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg jitter</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver codec</td>
<td>OPUS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver reports sent</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver report time sent</td>
<td>00:00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rcvr packets</td>
<td>1025</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rcvr octets</td>
<td>102471</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cumulative conceal ratio</td>
<td>0.0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interval conceal ratio</td>
<td>0.0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max conceal ratio</td>
<td>0.0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conceal seconds</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severely conceal seconds</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latency</td>
<td>55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max jitter</td>
<td>70</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender size</td>
<td>20 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender reports received</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender report time received</td>
<td>7:22:00pm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver size</td>
<td>20 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver discarded</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A Problem Report Tool (PRT) log can be generated from Device logs > Console logs by selecting Report problem.

**PRT Status: collecting** will be displayed after Report problem has been selected.

**PRT Status: completed** will be displayed when the PRT log collection has completed and the file is available for download.
The PRT log will remain (even if the phone is rebooted) until the PRT log collection process is invoked again.

Problem Report Tool Logs:
prt-20200203-190420-AC7E8AB763B6.tar.gz

Core Dumps
Browse to the standard web interface (https://x.x.x.x) of Cisco IP Phone 8861 or 8865 then select Core dumps to view this information.

A Java core dump can be generated from Device logs > Core dumps by selecting Generate java core&heapdump.
The Java core dump log will remain until the phone is rebooted or the Java core dump log collection process is invoked again.
**Status Messages**

Browse to the standard web interface ([https://x.x.x.x](https://x.x.x.x)) of Cisco IP Phone 8861 or 8865 then **Status messages** to view this information.

**Debug Display**

Browse to the standard web interface ([https://x.x.x.x](https://x.x.x.x)) of Cisco IP Phone 8861 or 8865 then select **Debug display** to view this information.
### WLAN Signal Indicator

The WLAN signal indicator is displayed in the upper right hand corner of the main screen when the Cisco IP Phone 8861 and 8865 is connected to an access point.

### Current Access Point

The Cisco IP Phone 8861 and 8865 only show the current access point (no neighbor list). To view current access point details go to Applications > Admin settings > Status > Current access point.
The Cisco IP Phone 8861 and 8865 are constantly scanning regardless of current signal or call state to discover new access points.

WLAN Statistics

Wireless statistic information can be viewed locally on the phone under Applications > Admin settings > Status > Wireless statistics.

Call Statistics

Call statistic information can be viewed locally on the phone under Applications > Admin settings > Status > Call statistics.
Status Messages

Status messages can be viewed locally on the phone under Applications > Admin settings > Status > Status messages.

Restoring Factory Defaults

The configuration of the Cisco IP Phone 8861 and 8865 can be reset to factory defaults by selecting Applications > Admin settings > Reset settings > All settings.

A confirmation screen will appear where Reset must be selected to proceed with the factory data reset.
If the Cisco IP Phone 8861 or 8865 is not able to boot properly, a factory reset can also be initiated via the following procedure:

- Turn the phone off by disconnecting the power.
- Press and hold the # key, then power on the phone.
- Keep the # key held until the Mute LED turns off.
- Once the Mute LED turns off, release the # key.
- Then press 1 2 3 4 5 6 7 8 9 * 0 #.
- The Mute LED will turn on to indicate the factory reset sequence has been accepted.
- The Cisco IP Phone 8861 or 8865 will then continue the normal boot process and have the factory settings restored.

To boot the alternate image, perform the following procedure.

- Turn the phone off by disconnecting the power.
- Press and hold the * key, then power on the phone.
- Keep the * key held until the Mute LED turns off.
- Once the Mute LED turns off, release the * key.
- The Cisco IP Phone 8861 or 8865 will then boot using the alternate image.

Capturing a Screenshot of the Phone Display

The current display of the Cisco IP Phone 8861 or 8865 can be captured by browsing to http://x.x.x.x/CGI/Screenshot, where x.x.x.x is the IP address of the Cisco IP Phone 8861 or 8865. At the prompt enter the username and password for the account that the Cisco IP Phone is associated to in Cisco Unified Communications Manager.
Additional Documentation

Cisco IP Phone 8861 and 8865 Data Sheets

Cisco IP Phone 8800 Series Administration Guide

Cisco IP Phone 8800 Series User Guide

Cisco IP Phone 8800 Series Quick Start Guide

Cisco IP Phone 8800 Series Accessory Guide

Cisco IP Phone 8800 Series Release Notes

Cisco IP Phone 8800 Series Software
http://software.cisco.com/download/navigator.html?mdfid=284729655

Cisco Unified Communications Manager

Cisco Unified Communications Manager Express

Cisco Voice Software
http://software.cisco.com/download/navigator.html?mdfid=278875240

Cisco IP Phone Services Application Development Notes

Real-Time Traffic over Wireless LAN SRND
Cisco IP Phone 8861 and 8865 Wireless LAN Deployment Guide

Cisco Unified Communications SRND

Cisco Wireless LAN Controller Documentation

Cisco Meraki Wireless LAN Documentation
https://meraki.cisco.com/products

Cisco Autonomous Access Point Documentation