Cisco Wireless Phone 840 and 860 Deployment Guide

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

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

Revision History

Date	Comments
01/08/21	1.1(0) Release
03/30/21	1.2(0) Release
08/30/21	1.3(0) Release
10/29/21	1.4(0) Release
04/15/22	1.5(0) Release
07/26/22	1.6(0) Release
10/04/22	1.7(0) Release
04/21/23	1.8(0) Release
07/23/23	1.9(0) Release
10/21/23	1.10(0) Release
12/19/23	1.10(1) Release
03/21/24	1.10(2) Release

Contents

Cisco Wireless Phone 840 and 860 Overview **6**

Phone Models *6*

Requirements *7*
Site Survey 7
Call Control 8
Wireless LAN 8

Protocols *14*

Wi-Fi *15*
Regulatory 22

Bluetooth *23*

Languages *24*

Battery Life *24*

840S and 860S Barcode Scanner *25*

Phone Care *26*

Accessories *26*

Wireless LAN Design **28**

802.11 Network *28*
5 GHz (802.11a/n/ac) 28
2.4 GHz (802.11b/g/n) 29
Signal Strength and Coverage 30
Data Rates 33
Rugged Environments 34

Security *36*
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) 37
Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS) 37
Protected Extensible Authentication Protocol (PEAP) 38

Quality of Service (QoS) *38*
Call Admission Control (CAC) 38
Wired QoS 39

Roaming *40*
Fast Secure Roaming (FSR) 41
Interband Roaming 42

Power Management *42*

Call Capacity *43*

Multicast *43*

Configuring the Cisco Wireless LAN **44**

Cisco AireOS Wireless LAN Controller and Lightweight Access Points *44*
802.11 Network Settings 45
WLAN Settings 56
Controller Settings 65
Call Admission Control (CAC) 67
RF Profiles 70
FlexConnect Groups 73
Multicast Direct 74
QoS Profiles 76
Advanced Settings 80

Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points *84*
802.11 Network Settings 84
WLAN Settings 92
Controller Settings 107
Mobility Settings 108
Call Admission Control (CAC) 109
Multicast 109
Advanced Settings 112
Sample Configuration 114

Cisco Mobility Express and Lightweight Access Points *121*
Controller Settings 122
802.11 Network Settings 123
WLAN Settings 126
RF Profiles 134
Multicast Direct 136

Cisco Autonomous Access Points *137*
802.11 Network Settings 137
WLAN Settings 141
Call Admission Control (CAC) 151
QoS Policies 152
Power Management 155
Sample Configuration 156

Cisco Meraki Access Points *161*
Creating the Wireless Network 161
SSID Configuration 164
Radio Settings 168
Firewall and Traffic Shaping 170

Configuring Cisco Call Control 172

Cisco Unified Communications Manager *172*
Device Enablement 172
Manufacturing Certificate Authority (CA) Certificates 173
Device Pools 173
Phone Button Templates 174
Security Profiles 175
SIP Profiles 177
Common Settings 180
QoS Parameters 180
G.722 and Opus Advertisement 181
Audio Bit Rates 181
Product Specific Configuration Options 182

Webex Calling *186*
Personal Usage 186
Shared Usage 189
Device Settings 192

Configuring the Cisco Wireless Phone 840 and 860 193

Enterprise Mobility Management (EMM) *193*

Cisco Wireless Phone Configuration Management Utility *195*
Creating Configuration Files 195
Configuring Cisco Unified Communications Manager 217
Enrolling the Cisco Wireless Phone 840 and 860 220

Manual Configuration *225*
Wi-Fi Profile Configuration 225
Certificate Management 238
Cisco Phone Application Configuration 243

Bluetooth Settings 247
Upgrading Firmware *250*
Cisco Unified Communications Manager 251
Webex Calling 251
Cisco Wireless Phone Upgrade Tool 251

Using the Cisco Wireless Phone 840 and 860 258

Applications *258*
Cisco Phone 258
Barcode 265
Battery Life 267
Buttons 268
Call Quality Settings 269
Custom Settings 270
Diagnostics 273
Emergency 274
Logging 276
PTT 277
Sound Stage 278
System Updater 283
Web API 284
Application Store *285*

IP Phone Services 287

Troubleshooting 288

Problem Report Tool *288*
Phone Webpages *289*
Device Information 289
Network Information 291
Registration Information 292
Device Logs 294
WLAN Signal Indicator *295*
WLAN Network Information *296*
Restoring Factory Defaults *297*
Capturing a Screenshot of the Phone Display *298*

Additional Documentation 299

Cisco Wireless Phone 840 and 860 Overview

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

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

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

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

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

Phone Models

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

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

Part Number	Description	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
CP-840	Cisco Wireless Phone 840	2.4 GHz = 1.7 dBi 5 GHz = 1.8 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-840S	Cisco Wireless Phone 840S (with barcode scanner)				
CP-860	Cisco Wireless Phone 860	2.4 GHz = 0.6 dBi 5 GHz = 0.8 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-860S	Cisco Wireless Phone 860S (with barcode scanner)				

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

Requirements

The Cisco Wireless Phone 840 and 860 are IEEE 802.11a/b/g/n/ac devices that provide voice communications.

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

Site Survey

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

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

Signal

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

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

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

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

Channel Utilization

Channel Utilization levels should be kept under 40%.

Noise

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

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

Packet Loss / Delay

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

Jitter should be kept at a minimal (< 100 ms).

Retries

802.11 retransmissions should be less than 20%.

Multipath

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

Call Control

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

- Cisco Unified Communications Manager (CUCM)
  - Minimum = 11.5(1)
  - Recommended = 12.5(1), 14.0(1) and later
- Cisco Unified Survivable Remote Site Telephony (SRST)
  - Minimum = 14.1
  - Recommended = 14.3 and later
- Webex Calling

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

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

https://software.cisco.com/download/home/278875240

Wireless LAN

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

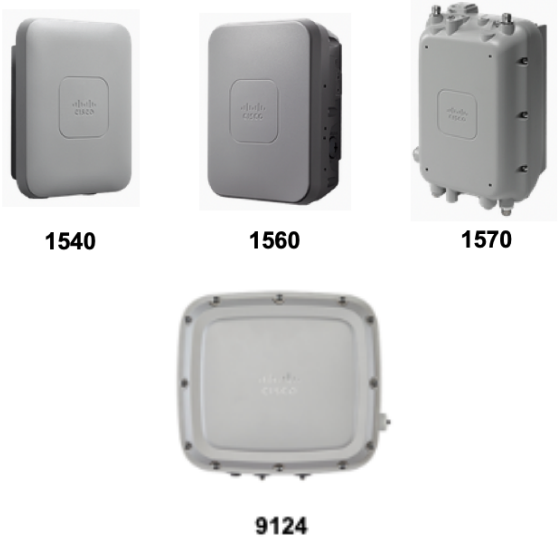
- Cisco AireOS Wireless LAN Controller and Cisco Lightweight Access Points
  - Minimum = 8.3.143.0
  - Recommended = 8.3.150.0, 8.5.182.0, 8.8.130.0, 8.10.190.0
- Cisco Catalyst IOS XE Wireless LAN Controller and Cisco Lightweight Access Points
  - Minimum = 16.12.1s
  - Recommended = 17.3.8a, 17.6.6a, 17.9.4a, 17.12.2, 17.13.1
- Cisco Mobility Express and Cisco Lightweight Access Points
  - Minimum = 8.3.143.0
  - Recommended = 8.3.150.0, 8.5.182.0, 8.8.130.0, 8.10.190.0
- Cisco Autonomous Access Points
  - Minimum = 15.2(4)JB6
  - Recommended = 15.3(3)JPP
- Cisco Meraki Access Points
  - Minimum = MR 25.9, MX 13.33
  - Recommended = MR 30.5, MX 18.107.2

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 Wireless Phone 840 and 860 are supported on the following Cisco Aironet access point platforms.

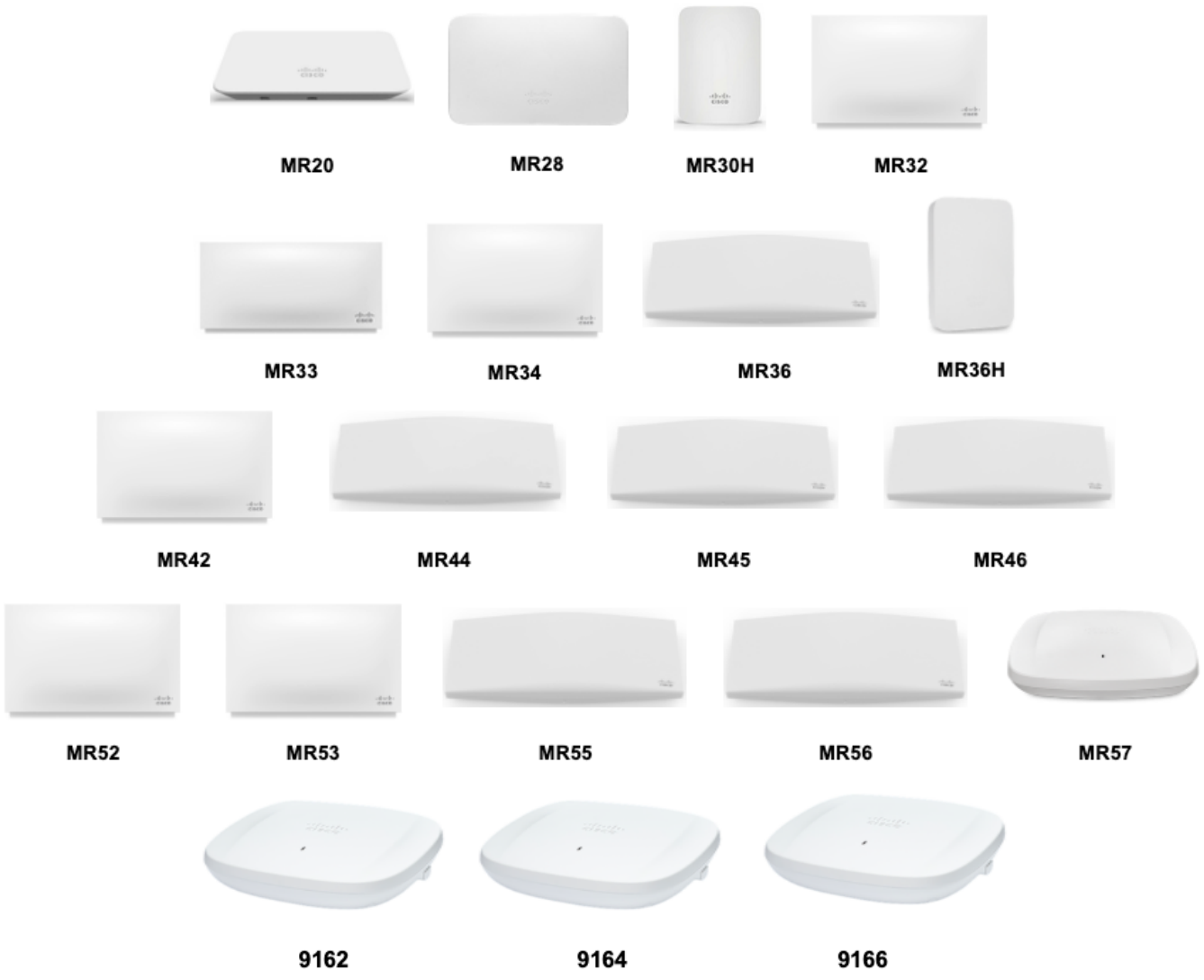


The table below lists the modes that are supported by each Cisco Aironet access point.

Cisco AP Series	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	Lightweight	Mobility Express	Autonomous
1540	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1560	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1570	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
1700	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
1810	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
1810W	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
1815	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (**not 1815t**)	No
1830	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1840	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1850	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
2700	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
2800	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
3700	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
3800	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
4800	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
9105	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

9115	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9117	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9120	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9124	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9130	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9136	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9162	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9164	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9166	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

The Cisco Wireless Phone 840 and 860 are supported on the following Cisco Meraki access point platforms.



https://meraki.cisco.com/products/wireless#models
https://meraki.cisco.com/products/appliances#models

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

Meraki AP Series	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
9162	Yes	Yes	Yes	Yes	Yes	Yes
9164	Yes	Yes	Yes	Yes	Yes	Yes
9166	Yes	Yes	Yes	Yes	Yes	Yes
MR20	Yes	Yes	Yes	Yes	Yes	No
MR28	Yes	Yes	Yes	Yes	Yes	Yes
MR30H	Yes	Yes	Yes	Yes	Yes	No
MR32	Yes	Yes	Yes	Yes	Yes	No
MR33	Yes	Yes	Yes	Yes	Yes	No
MR34	Yes	Yes	Yes	Yes	Yes	No
MR36	Yes	Yes	Yes	Yes	Yes	Yes
MR36H	Yes	Yes	Yes	Yes	Yes	Yes
MR42	Yes	Yes	Yes	Yes	Yes	No
MR44	Yes	Yes	Yes	Yes	Yes	Yes
MR45	Yes	Yes	Yes	Yes	Yes	Yes
MR46	Yes	Yes	Yes	Yes	Yes	Yes
MR52	Yes	Yes	Yes	Yes	Yes	No
MR53	Yes	Yes	Yes	Yes	Yes	No
MR55	Yes	Yes	Yes	Yes	Yes	Yes
MR56	Yes	Yes	Yes	Yes	Yes	Yes
MR57	Yes	Yes	Yes	Yes	Yes	Yes
MR70	Yes	Yes	Yes	Yes	Yes	No
MR74	Yes	Yes	Yes	Yes	Yes	No
MR76	Yes	Yes	Yes	Yes	Yes	Yes
MR78	Yes	Yes	Yes	Yes	Yes	Yes
MR84	Yes	Yes	Yes	Yes	Yes	No
MR86	Yes	Yes	Yes	Yes	Yes	Yes
MX64W	Yes	Yes	Yes	Yes	Yes	No
MX65W	Yes	Yes	Yes	Yes	Yes	No

MX67W	Yes	Yes	Yes	Yes	Yes	No
MX68W	Yes	Yes	Yes	Yes	Yes	No
Z3	Yes	Yes	Yes	Yes	Yes	No

Note: If an access point model is not specifically listed above, then it is not supported.

Support for Cisco Aironet 1500 Series outdoor access points is limited to local access point mode only.

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

Interoperability with third-party access points can not be guaranteed as there are no interoperability tests performed for third-party access points; however if connected to a Wi-Fi compliant access point, then should have basic functionality.

Some of the key features are the following:

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

Antenna Systems

Some Cisco access points require or allow external antennas.

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

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/product_data_sheet09186a008008883b.html

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

Protocols

Supported voice and wireless LAN protocols include the following:

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

Wi-Fi

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

Cisco Wireless Phone 840

5 GHz Specifications

5 GHz - 802.11a	**Data Rate**	**Spatial Streams**	**Modulation**
Max Tx Power = 16 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
5 GHz - 802.11n (HT20)	**Data Rate**	**Spatial Streams**	**Modulation**
Max Tx Power = 16 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK
	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11n (HT40)	**Data Rate**	**Spatial Streams**	**Modulation**
Max Tx Power = 15 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM

	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	30 Mbps (MCS 8)	2	OFDM - BPSK
	60 Mbps (MCS 9)	2	OFDM - QPSK
	90 Mbps (MCS 10)	2	OFDM - QPSK
	120 Mbps (MCS 11)	2	OFDM - 16 QAM
	180 Mbps (MCS 12)	2	OFDM - 16 QAM
	240 Mbps (MCS 13)	2	OFDM - 64 QAM
	270 Mbps (MCS 14)	2	OFDM - 64 QAM
	300 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11ac (VHT20)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 16 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	87 Mbps (MCS 8)	1	OFDM - 256 QAM
	14 Mbps (MCS 0)	2	OFDM - BPSK
	28 Mbps (MCS 1)	2	OFDM - QPSK
	43 Mbps (MCS 2)	2	OFDM - QPSK
	58 Mbps (MCS 3)	2	OFDM - 16 QAM
	87 Mbps (MCS 4)	2	OFDM - 16 QAM
	116 Mbps (MCS 5)	2	OFDM - 64 QAM
	130 Mbps (MCS 6)	2	OFDM - 64 QAM
	144 Mbps (MCS 7)	2	OFDM - 64 QAM
	173 Mbps (MCS 8)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT40)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 15 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	180 Mbps (MCS 8)	1	OFDM - 256 QAM
	200 Mbps (MCS 9)	1	OFDM - 256 QAM

	30 Mbps (MCS 0)	2	OFDM - BPSK
	60 Mbps (MCS 1)	2	OFDM - QPSK
	90 Mbps (MCS 2)	2	OFDM - QPSK
	120 Mbps (MCS 3)	2	OFDM - 16 QAM
	180 Mbps (MCS 4)	2	OFDM - 16 QAM
	240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM
	300 Mbps (MCS 7)	2	OFDM - 64 QAM
	360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT80)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 14 dBm (Depends on region)	33 Mbps (MCS 0)	1	OFDM - BPSK
	65 Mbps (MCS 1)	1	OFDM - QPSK
	98 Mbps (MCS 2)	1	OFDM - QPSK
	130 Mbps (MCS 3)	1	OFDM - 16 QAM
	195 Mbps (MCS 4)	1	OFDM - 16 QAM
	260 Mbps (MCS 5)	1	OFDM - 64 QAM
	293 Mbps (MCS 6)	1	OFDM - 64 QAM
	325 Mbps (MCS 7)	1	OFDM - 64 QAM
	390 Mbps (MCS 8)	1	OFDM - 256 QAM
	433 Mbps (MCS 9)	1	OFDM - 256 QAM
	65 Mbps (MCS 0)	2	OFDM - BPSK
	130 Mbps (MCS 1)	2	OFDM - QPSK
	195Mbps (MCS 2)	2	OFDM - QPSK
	260 Mbps (MCS 3)	2	OFDM - 16 QAM
	390 Mbps (MCS 4)	2	OFDM - 16 QAM
	520 Mbps (MCS 5)	2	OFDM - 64 QAM
	585 Mbps (MCS 6)	2	OFDM - 64 QAM
	650 Mbps (MCS 7)	2	OFDM - 64 QAM
	780 Mbps (MCS 8)	2	OFDM - 256 QAM
	867 Mbps (MCS 9)	2	OFDM - 256 QAM

2.4 GHz Specifications

2.4 GHz - 802.11b	Data Rate	Spatial Streams	Modulation
Max Tx Power = 19 dBm (Depends on region)	1 Mbps	1	DSSS - BPSK
	2 Mbps	1	DSSS - QPSK
	5.5 Mbps	1	DSSS - CCK
	11 Mbps	1	DSSS - CCK
2.4 GHz - 802.11g	Data Rate	Spatial Streams	Modulation

Max Tx Power = 18 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
2.4 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 18 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK
	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM

Cisco Wireless Phone 860

5 GHz Specifications

5 GHz - 802.11a	**Data Rate**	**Spatial Streams**	**Modulation**
Max Tx Power = 17 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
5 GHz - 802.11n (HT20)	**Data Rate**	**Spatial Streams**	**Modulation**

Max Tx Power = 17 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK
	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK
	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11n (HT40)	**Data Rate**	**Spatial Streams**	**Modulation**
Max Tx Power = 17 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	30 Mbps (MCS 8)	2	OFDM - BPSK
	60 Mbps (MCS 9)	2	OFDM - QPSK
	90 Mbps (MCS 10)	2	OFDM - QPSK
	120 Mbps (MCS 11)	2	OFDM - 16 QAM
	180 Mbps (MCS 12)	2	OFDM - 16 QAM
	240 Mbps (MCS 13)	2	OFDM - 64 QAM
	270 Mbps (MCS 14)	2	OFDM - 64 QAM
	300 Mbps (MCS 15)	2	OFDM - 64 QAM
5 GHz - 802.11ac (VHT20)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 17 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM

	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	87 Mbps (MCS 8)	1	OFDM - 256 QAM
	14 Mbps (MCS 0)	2	OFDM - BPSK
	28 Mbps (MCS 1)	2	OFDM - QPSK
	43 Mbps (MCS 2)	2	OFDM - QPSK
	58 Mbps (MCS 3)	2	OFDM - 16 QAM
	87 Mbps (MCS 4)	2	OFDM - 16 QAM
	116 Mbps (MCS 5)	2	OFDM - 64 QAM
	130 Mbps (MCS 6)	2	OFDM - 64 QAM
	144 Mbps (MCS 7)	2	OFDM - 64 QAM
	173 Mbps (MCS 8)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT40)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 17 dBm (Depends on region)	15 Mbps (MCS 0)	1	OFDM - BPSK
	30 Mbps (MCS 1)	1	OFDM - QPSK
	45 Mbps (MCS 2)	1	OFDM - QPSK
	60 Mbps (MCS 3)	1	OFDM - 16 QAM
	90 Mbps (MCS 4)	1	OFDM - 16 QAM
	120 Mbps (MCS 5)	1	OFDM - 64 QAM
	135 Mbps (MCS 6)	1	OFDM - 64 QAM
	150 Mbps (MCS 7)	1	OFDM - 64 QAM
	180 Mbps (MCS 8)	1	OFDM - 256 QAM
	200 Mbps (MCS 9)	1	OFDM - 256 QAM
	30 Mbps (MCS 0)	2	OFDM - BPSK
	60 Mbps (MCS 1)	2	OFDM - QPSK
	90 Mbps (MCS 2)	2	OFDM - QPSK
	120 Mbps (MCS 3)	2	OFDM - 16 QAM
	180 Mbps (MCS 4)	2	OFDM - 16 QAM
	240 Mbps (MCS 5)	2	OFDM - 64 QAM
	270 Mbps (MCS 6)	2	OFDM - 64 QAM
	300 Mbps (MCS 7)	2	OFDM - 64 QAM
	360 Mbps (MCS 8)	2	OFDM - 256 QAM
	400 Mbps (MCS 9)	2	OFDM - 256 QAM
5 GHz - 802.11ac (VHT80)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 17 dBm (Depends on region)	33 Mbps (MCS 0)	1	OFDM - BPSK
	65 Mbps (MCS 1)	1	OFDM - QPSK
	98 Mbps (MCS 2)	1	OFDM - QPSK
	130 Mbps (MCS 3)	1	OFDM - 16 QAM
	195 Mbps (MCS 4)	1	OFDM - 16 QAM
	260 Mbps (MCS 5)	1	OFDM - 64 QAM
	293 Mbps (MCS 6)	1	OFDM - 64 QAM
	325 Mbps (MCS 7)	1	OFDM - 64 QAM

	390 Mbps (MCS 8)	1	OFDM - 256 QAM
	433 Mbps (MCS 9)	1	OFDM - 256 QAM
	65 Mbps (MCS 0)	2	OFDM - BPSK
	130 Mbps (MCS 1)	2	OFDM - QPSK
	195Mbps (MCS 2)	2	OFDM - QPSK
	260 Mbps (MCS 3)	2	OFDM - 16 QAM
	390 Mbps (MCS 4)	2	OFDM - 16 QAM
	520 Mbps (MCS 5)	2	OFDM - 64 QAM
	585 Mbps (MCS 6)	2	OFDM - 64 QAM
	650 Mbps (MCS 7)	2	OFDM - 64 QAM
	780 Mbps (MCS 8)	2	OFDM - 256 QAM
	867 Mbps (MCS 9)	2	OFDM - 256 QAM

2.4 GHz Specifications

2.4 GHz - 802.11b	Data Rate	Spatial Streams	Modulation
Max Tx Power = 19 dBm (Depends on region)	1 Mbps	1	DSSS - BPSK
	2 Mbps	1	DSSS - QPSK
	5.5 Mbps	1	DSSS - CCK
	11 Mbps	1	DSSS - CCK
2.4 GHz - 802.11g	Data Rate	Spatial Streams	Modulation
Max Tx Power = 17 dBm (Depends on region)	6 Mbps	1	OFDM - BPSK
	9 Mbps	1	OFDM - BPSK
	12 Mbps	1	OFDM - QPSK
	18 Mbps	1	OFDM - QPSK
	24 Mbps	1	OFDM - 16 QAM
	36 Mbps	1	OFDM - 16 QAM
	48 Mbps	1	OFDM - 64 QAM
	54 Mbps	1	OFDM - 64 QAM
2.4 GHz - 802.11n (HT20)	Data Rate	Spatial Streams	Modulation
Max Tx Power = 16 dBm (Depends on region)	7 Mbps (MCS 0)	1	OFDM - BPSK
	14 Mbps (MCS 1)	1	OFDM - QPSK
	21 Mbps (MCS 2)	1	OFDM - QPSK
	29 Mbps (MCS 3)	1	OFDM - 16 QAM
	43 Mbps (MCS 4)	1	OFDM - 16 QAM
	58 Mbps (MCS 5)	1	OFDM - 64 QAM
	65 Mbps (MCS 6)	1	OFDM - 64 QAM
	72 Mbps (MCS 7)	1	OFDM - 64 QAM
	14 Mbps (MCS 8)	2	OFDM - BPSK
	28 Mbps (MCS 9)	2	OFDM - QPSK
	43 Mbps (MCS 10)	2	OFDM - QPSK

	58 Mbps (MCS 11)	2	OFDM - 16 QAM
	87 Mbps (MCS 12)	2	OFDM - 16 QAM
	116 Mbps (MCS 13)	2	OFDM - 64 QAM
	130 Mbps (MCS 14)	2	OFDM - 64 QAM
	144 Mbps (MCS 15)	2	OFDM - 64 QAM

Note: To achieve 802.11n/ac connectivity, it is recommended that the Cisco Wireless Phone 840 and 860 be within 100 feet of the access point.

Regulatory

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

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

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

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

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

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

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

Australia (AU)
Austria (AT)
Belgium (BE)
Bulgaria (BG)
Canada (CA)
Croatia (HR)
Cyprus (CY)
Czech Republic (CZ)
Denmark (DK)
Estonia (EE)
Finland (FI)
France (FR)
Germany (DE)
Greece (GR)
Hungary (HU)
Iceland (IS)
Ireland (IE)
Italy (IT)
Latvia (LV)
Liechtenstein (LI)
Lithuania (LT)
Luxembourg (LU)
Malta (MT)
Netherlands (NL)
New Zealand (NZ)
Norway (NO)
Poland (PL)
Portugal (PT)
Romania (RO)
Slovakia (SK)
Slovenia (SI)
Spain (ES)
Sweden (SE)
Switzerland (CH)
Turkey (TR)
United Kingdom (GB)
United States (US)

Note: Compliance information is available on the Cisco Product Approval Status web site at the following URL:

https://cae-cnc-prd.cisco.com/pdtcnc

Bluetooth

The Cisco Wireless Phone 840 and 860 support Bluetooth technology allowing for wireless headset communications.

Bluetooth enables low bandwidth wireless connections within a range of 30 feet, however it is recommended to keep the Bluetooth device within 10 feet of the Cisco Wireless Phone 840 and 860.

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

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

Bluetooth Profiles

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

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

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 Wireless Phone 840 and 860 currently support the following languages.

Danish	German	Portuguese
Dutch	Hungarian	Russian
English	Italian	Slovenian
Finnish	Japanese	Spanish
French	Norwegian	Swedish

Battery Life

The Cisco Wireless Phone 840 has a 3040 mAh battery and the Cisco Wireless Phone 860 has a 3000 mAh battery.

The Cisco Wireless Phone 840 and 860 battery's capacity will be reduced to 80% or less after 500 full charging cycles (charging from empty to full), therefore it is recommended to replace the Cisco Wireless Phone 840 and 860 battery approximately every 2 years.

The Cisco Wireless Phone 860 supports a hot swappable battery feature, which allows up to 60 seconds to swap the battery; where the Cisco Wireless Phone 840 does not include the hot swappable battery feature.

The table below lists the maximum on call and idle times per phone model.

Phone Model	Call State	Battery Time
840 / 840S	On Call	Up to 17 hours
	Idle	Up to 168 hours
860 / 860S	On Call	Up to 12 hours
	Idle	Up to 120 hours

There are many factors that can influence actual battery life time.

Usage

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

Coverage

Ensure the Cisco Wireless Phone 840 and 860 remain in a good RF coverage area and is able to maintain a constant connection to the call server.

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

Proxy ARP

For optimal idle battery life, it is recommended to utilize an access point that supports the Proxy ARP feature. Proxy ARP allows the Cisco Wireless Phone 840 and 860 to remain in suspend mode longer versus having to wake up at each DTIM period, therefore reducing power consumption.

If the access point does not support Proxy ARP, then the Cisco Wireless Phone 840 and 860 must wake up at each DTIM period, which can reduce idle battery life as much as 50%.

Transmit Power

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

Multicast

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

Power Save Protocol

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

840S and 860S Barcode Scanner

The Cisco Wireless Phone 840S and 860S include a 2D barcode scanner.

An Android application is required to invoke the scanner.

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

- Aztec, CCA EAN-128, CCA EAN-13, CCA EAN-8, CCA GS1 DataBar Expanded, CCA GS1 DataBar Limited, CCA GS1 DataBar-14, CCA UPC-A, CCA UPC-E, CCB EAN-128, CCB EAN-13, CCB EAN-8, CCB GS1 DataBar Expanded, CCB GS1 DataBar Limited, CCB GS1 DataBar-14, CCB UPC-A, CCB UPC-E, CCC EAN-128, Codabar, Code 11, Code 128, Code 32, Code 39 Full ASCII, Code 39 Trioptic, Code 93, DataMatrix, Discrete (Standard) 2 of 5, EAN-128, EAN-13, EAN-13 + 2 Supplemental, EAN-13 + 5 supplemental, EAN-8, EAN-8 + 2 Supplemental, EAN-8 + 5 supplemental, GS1 DataBar Expanded, GS1 DataBar Limited, GS1 DataBar-14, Han Xin, Interleaved 2 of 5, ISBT-128, ISBT-128 Con, Macro Micro PDF, Macro PDF, Macro QR, Matrix 2 of 5, Micro PDF, Micro QR, MSI, PDF-417, QR Code, UPC-A, UPC-A + 2 Supplemental, UPC-A + 5 supplemental, UPC-E0, UPC-E0 + 2 Supplemental, UPC-E0 + 5 supplemental

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

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Phone Care

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

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

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

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

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

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

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

https://www.cisco.com/content/en/us/td/docs/voice_ip_comm/cuipph/800-series/userguide/w800_b_wireless-800-user-guide.html

Accessories

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

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

840 Chargers

860 Chargers

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

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

https://www.cisco.com/content/en/us/td/docs/voice_ip_comm/cuipph/800-series/userguide/w800_b_wireless-800-user-guide.html

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

Wireless LAN Design

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

802.11 Network

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

5 GHz (802.11a/n/ac)

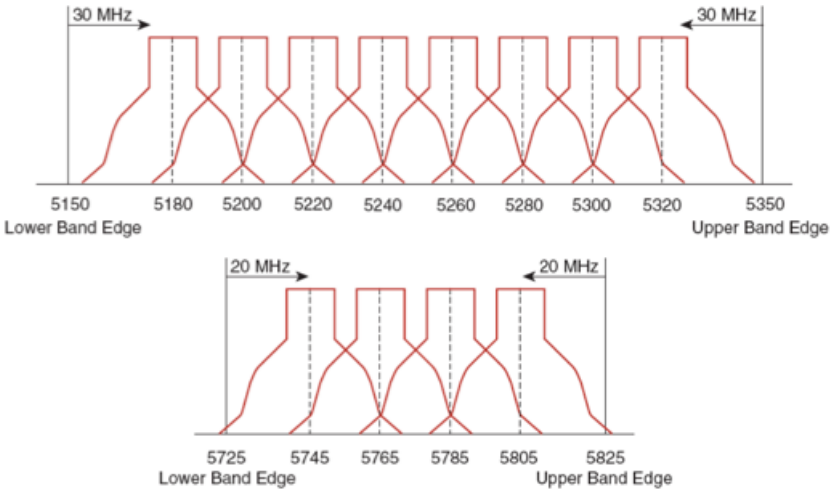
5 GHz is the recommended frequency band to utilize for operation of the Cisco Wireless Phone 840 and 860.

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

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

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

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



Channel ID	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161
Center Freq. MHz	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805
Band	UNII-1				UNII-2															UNNII-3			

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.

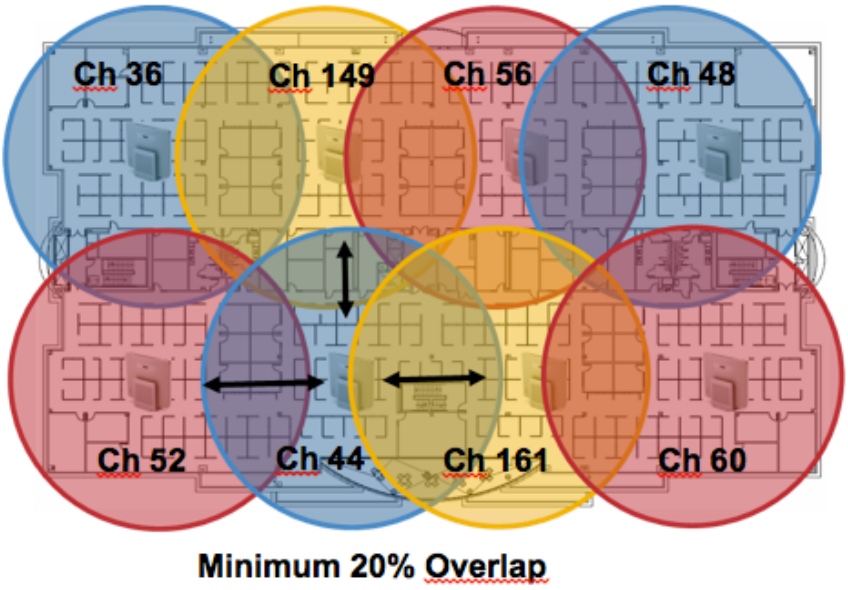
If there are repeated radar events detected by the access point (just or falsely), determine if the radar signals are impacting a single channel (narrowband) or multiple channels (wideband), then potentially disable use of that channel or channels in the wireless LAN.

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.

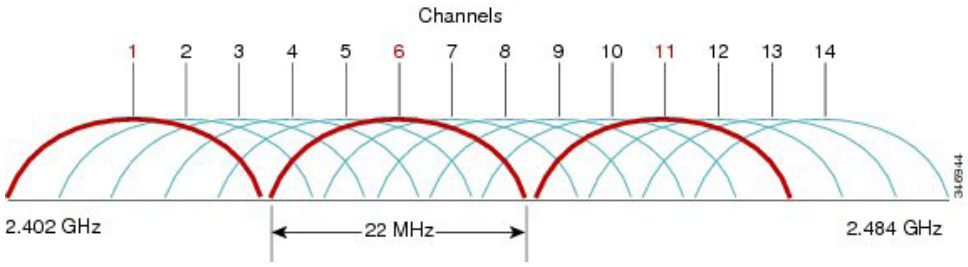
If there is an intermittent interferer, then the access point or access points serving that area may need to have a channel statically assigned.

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.

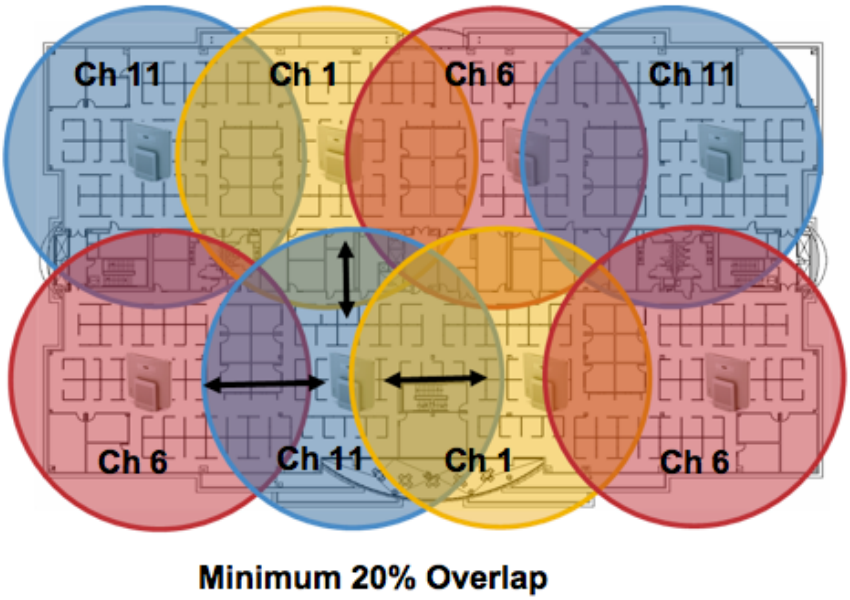
There are only 3 non-overlapping channels in the 2.4 GHz frequency range (channels 1, 6, 11).

Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying the Cisco Wireless Phone 840 and 860 in an 802.11b/g/n environment, which allows for seamless roaming.

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



Below is a sample 2.4 GHz wireless LAN deployment.



Signal Strength and Coverage

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

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

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

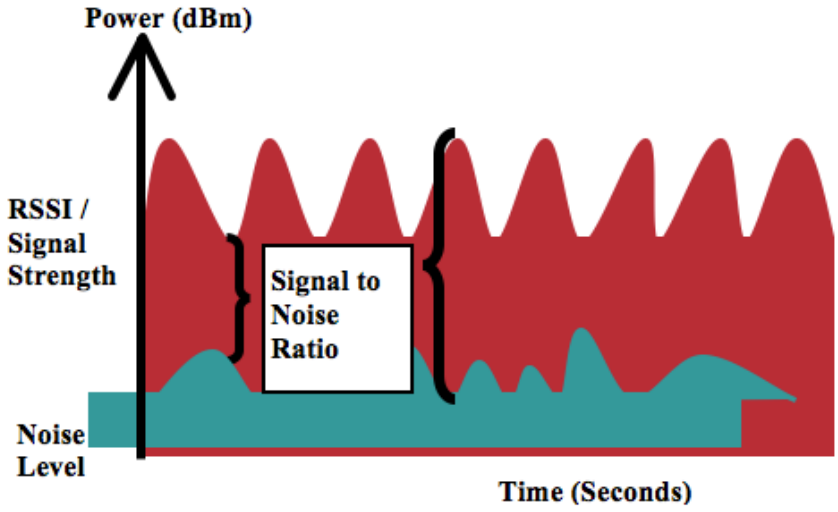
It is recommended to have at least two access points on non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.

To achieve maximum capacity and throughput, the wireless LAN should be designed to 24 Mbps. Higher data rates can optionally be enabled for other applications other than voice only that can take advantage of these higher data rates.

Recommended to set the minimum data rate to 11 Mbps or 12 Mbps for 2.4 GHz (dependent upon 802.11b client support policy) and 12 Mbps for 5 GHz, which should also be the only rate configured as a mandatory / basic rate.

In some environments, 6 Mbps may need to be enabled as a mandatory / basic rate.

Due to the above requirements, a single channel plan should not be deployed.



When designing the placement of access points, be sure that all key areas have adequate coverage (signal).

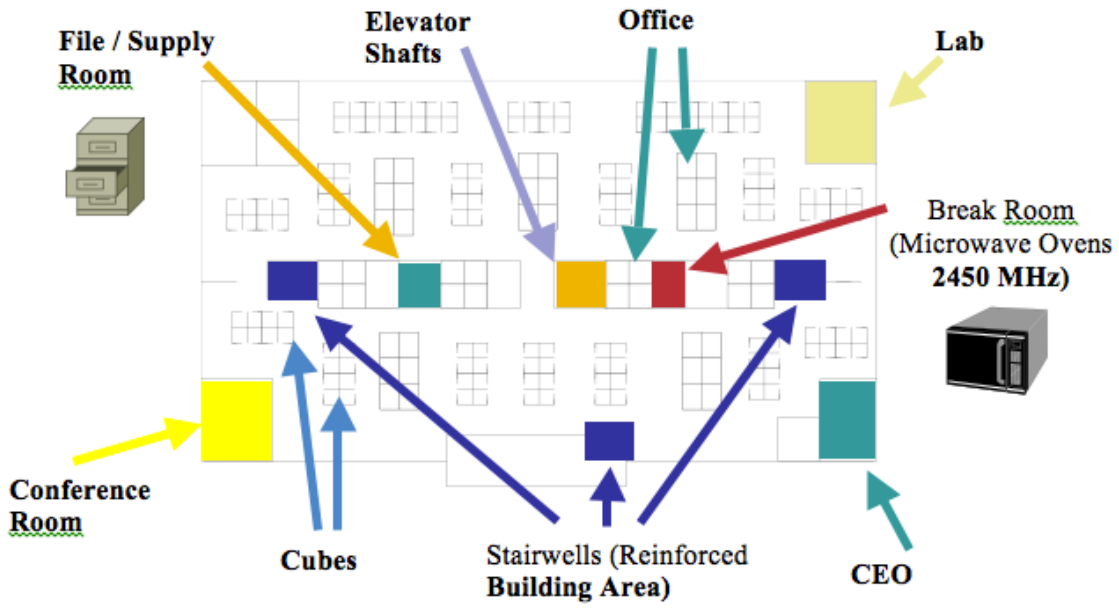
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

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

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

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

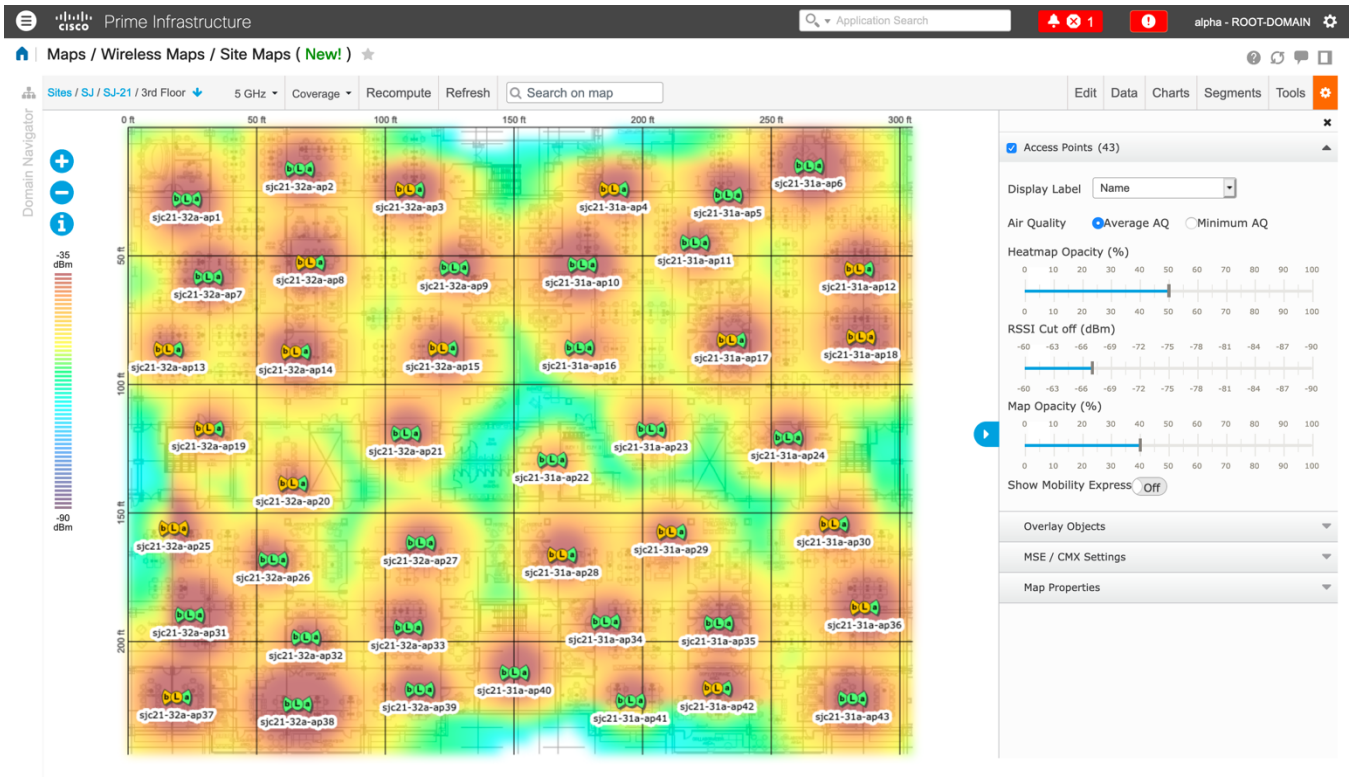
However there are products that also utilize the non-licensed 5 GHz frequency (e.g. 5.8 GHz cordless phones, which can impact UNII-3 channels).



The chart below lists the attenuation levels for various materials that may exist in an environment.

Material	Attenuation Level
Wood	Low
Brick	Medium
Concrete	High
Metal	Very High

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



Data Rates

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

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

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

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

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

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

The recommended data rate configurations are the following:

802.11 Mode	Mandatory Data Rates	Supported Data Rates	Disabled Data Rates
802.11a/n/ac	12 Mbps	18-54 Mbps, VHT MCS 0 - MCS 9 1SS, VHT MCS 0 - MCS 9 2SS, (VHT MCS 0 - MCS 9 3SS), (VHT MCS 0 - MCS 9 4SS)	6, 9 Mbps
802.11a/n	12 Mbps	18-54 Mbps,	6, 9 Mbps

		HT MCS 0 - MCS 15, (HT MCS 16 - MCS 31)	
802.11g/n	12 Mbps	18-54 Mbps, HT MCS 0 - MCS 15, (HT MCS 16 - MCS 31)	1, 2, 5.5, 6, 9, 11 Mbps
802.11b/g/n	11 Mbps	12-54 Mbps, HT MCS 0 - MCS 15, (HT MCS 16 - MCS 31)	1, 2, 5.5, 6, 9 Mbps
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, 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 Wireless Phone 840 and 860 in a rugged environment (e.g. manufacturing, warehouse, retail), additional tuning on top of the standard design recommendations may be necessary.

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

Access Point and Antenna Selection

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

Access Point Placement

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

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

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

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

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

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

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

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

Multipath

Multipath occurs when RF signals take multiple paths from a source to a destination.

A part of the signal goes to the destination while another part bounces off an obstruction, then goes on to the destination. As a result, part of the signal encounters delay and travels a longer path to the destination, which creates signal energy loss.

When the different waveforms combine, they cause distortion and affect the decoding capability of the receiver, as the signal quality is poor.

Multipath can exist in environments where there are reflective surfaces (e.g. metal, glass, etc.). Avoid mounting access points on these surfaces.

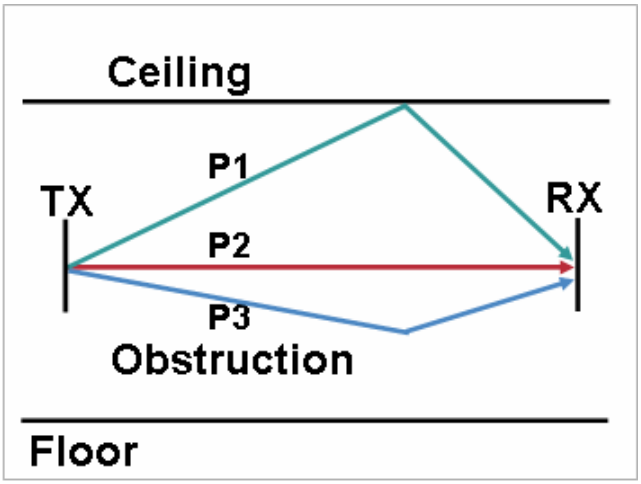
Below is a list of multipath effects:

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

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

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

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



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

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

Use of antenna diversity can also help in such environments.

Security

When deploying a wireless LAN, security is essential.

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

WLAN Authentication

- WPA2 (802.1x authentication)
- WPA2-PSK (Pre-Shared key)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- EAP-TTLS (Extensible Authentication Protocol – Tunneled Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol)
- 802.11r / Fast Transition (FT)
- CCKM (Cisco Centralized Key Management)

- None

WLAN Encryption

- AES (Advanced Encryption Standard)

Note: WPA3 is not supported.

802.1x-SHA2 key management is not supported.

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

The Cisco Wireless Phone 840 and 860 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

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 Wireless Phone 840 or 860.

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

Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS)

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

EAP-TTLS-GTC, EAP-TTLS-MSCHAP, EAP-TTLS-MSCHAPv2, and EAP-TTLS-PAP are supported inner authentication protocols.

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

The authentication server can be validated via importing a certificate into the Cisco Wireless Phone 840 and 860.

Protected Extensible Authentication Protocol (PEAP)

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server.

The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping.

PEAP-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 Wireless Phone 840 and 860.

Quality of Service (QoS)

Quality of Service enables queuing to ensure high priority for voice traffic.

To enable proper queuing for voice and call control traffic use the following guidelines.

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

Traffic Type	Call Server	DSCP	802.1p	WMM UP	Protocol
Voice	CUCM	EF (46)	5	6	RTP (UDP 16384 - 32767)
	Webex Calling	EF (46)	5	6	RTP (UDP 19560 - 65535)
Call Control	CUCM	CS3 (24)	3	4	SIP (TCP 5060 - 5061)
	Webex Calling	CS3 (24)	3	4	SIP (TCP 8934)

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

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

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

For information on network requirements for Webex Calling, refer to the **Port Reference Information for Webex Calling** document at this URL:

https://help.webex.com/en-us/article/b2exve/Port-Reference-Information-for-Webex-Calling

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 Wireless Phone 840 and 860 will send an Add Traffic Stream (ADDTS) to the access point to request bandwidth in order to place or receive a call.

If the AP sends an ADDTS successful message, then the Cisco Wireless Phone 840 or 860 establishes the call.

If the access point rejects the call and the Cisco Wireless Phone 840 or 860 has no other access point to roam to, then the phone will display **Network Busy**.

If the admission is refused for an inbound call there is no messaging from the Cisco Wireless Phone 840 or 860 to inform the remote endpoint that there is insufficient bandwidth to establish the call, so the call can continue to ring out within the system until the remote user terminates the call.

Roaming Admission Control

During a call, the Cisco Wireless Phone 840 and 860 measure Received Signal Strength Indicator (RSSI) and Packet Error Rate (PER) values for the current and all available access points to make roaming decisions.

If the original access point where the call was established had Call Admission Control enabled, then the Cisco Wireless Phone 840 and 860 will send an ADDTS request during the roam to the new access point, which embedded in the reassociation request frame.

Wired QoS

Configure QoS settings and policies for the necessary network devices.

Configuring Cisco Switch Ports for WLAN Devices

Configure the Cisco Wireless LAN Controller and Cisco Access Point switch ports as well as any uplink switch ports.

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

Enable COS trust for Cisco Wireless LAN Controller

```
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**.

https://meraki.cisco.com/lib/pdf/meraki_whitepaper_msvoip.pdf

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

802.11r / Fast Transition (FT) is the recommended deployment model for all environment types where frequent roaming occurs.

802.1x authentication is required in order to utilize CCKM.

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

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

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

Authentication	Roaming Time
WPA2 Personal	150 ms
WPA2 Enterprise	300 ms
802.11r (FT)	< 100 ms
CCKM	< 100 ms

The Cisco Wireless Phone 840 and 860 manage the scanning and roaming events.

The roaming trigger for the majority of roams should be due to meeting the required RSSI differential based on the current RSSI, which results in seamless roaming (no voice interruptions).

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

Fast Secure Roaming (FSR)

802.11r / Fast Transition (FT) is the recommended deployment model for all environment types where frequent roaming occurs.

Cisco Centralized Key Management (CCKM) is also supported, but requires 802.1x authentication.

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

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

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

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

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

Over the Air

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

Over the Distribution

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

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

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

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

FSR Type	Authentication	Key Management	Encryption
802.11r (FT)	PSK	WPA2	AES
802.11r (FT)	EAP-TLS	WPA2	AES
802.11r (FT)	EAP-TTLS	WPA2	AES
802.11r (FT)	PEAP	WPA2	AES

CCKM	EAP-TLS	WPA2	AES
CCKM	EAP-TTLS	WPA2	AES
CCKM	PEAP	WPA2	AES

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

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

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

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

Power Management

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

If the access point does not support Proxy ARP, then the idle battery life will be up to fifty percent less.

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

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

Delivery Traffic Indicator Message (DTIM)

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

If Proxy ARP is enabled, then the Cisco Wireless Phone 840 and 860 do not have to wake up at DTIM.

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

The DTIM period is a tradeoff between battery life and multicast performance.

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 Wireless Phone 840 or 860 and the access point, Dynamic Transmit Power Control (DTPC) should be enabled.

DTPC prevents one-way audio when RF traffic is heard in one direction only.

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

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

Call Capacity

Design the network to accommodate the desired call capacity.

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

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

Audio Calls

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

Max # of Audio Calls	802.11 Mode	Audio Codec	Audio Bit Rate	Data Rate
13	5 GHz or 2.4 GHz	G.722 / G.711	64 Kbps	6 Mbps
20	5 GHz or 2.4 GHz	G.722 / G.711	64 Kbps	12 Mbps
27	5 GHz or 2.4 GHz	G.722 / G.711	64 Kbps	24 Mbps or higher

Multicast

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

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

With multicast, there is no guarantee that the packet will be received the 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 Wireless Phone 840 and 860 support the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure that IGMP snooping is also enabled on all switches.

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

Configuring the Cisco Wireless LAN

Cisco AireOS Wireless LAN Controller and Lightweight Access Points

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

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

- Set the **Protocol Type** to **None** for the **Platinum** QoS profile

802.11 Network Settings

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

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

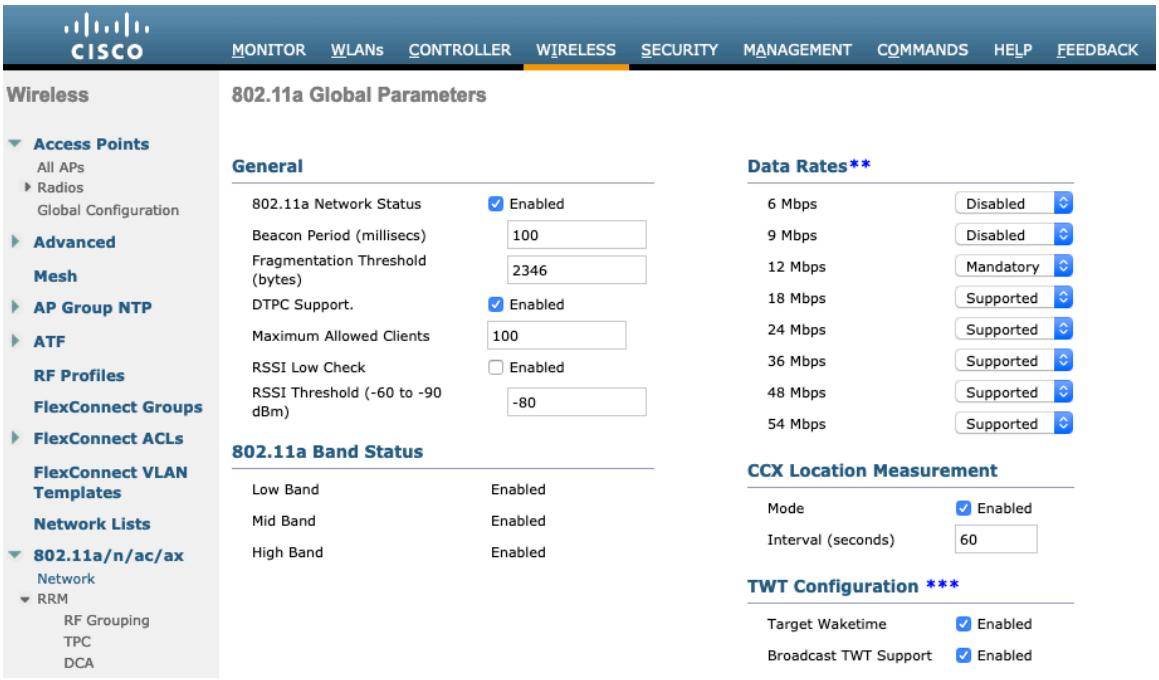
Set the **Beacon Period** to **100 ms**.

Ensure **DTPC Support** is enabled.

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

Maximum Allowed Clients can be configured as necessary.

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



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

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

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

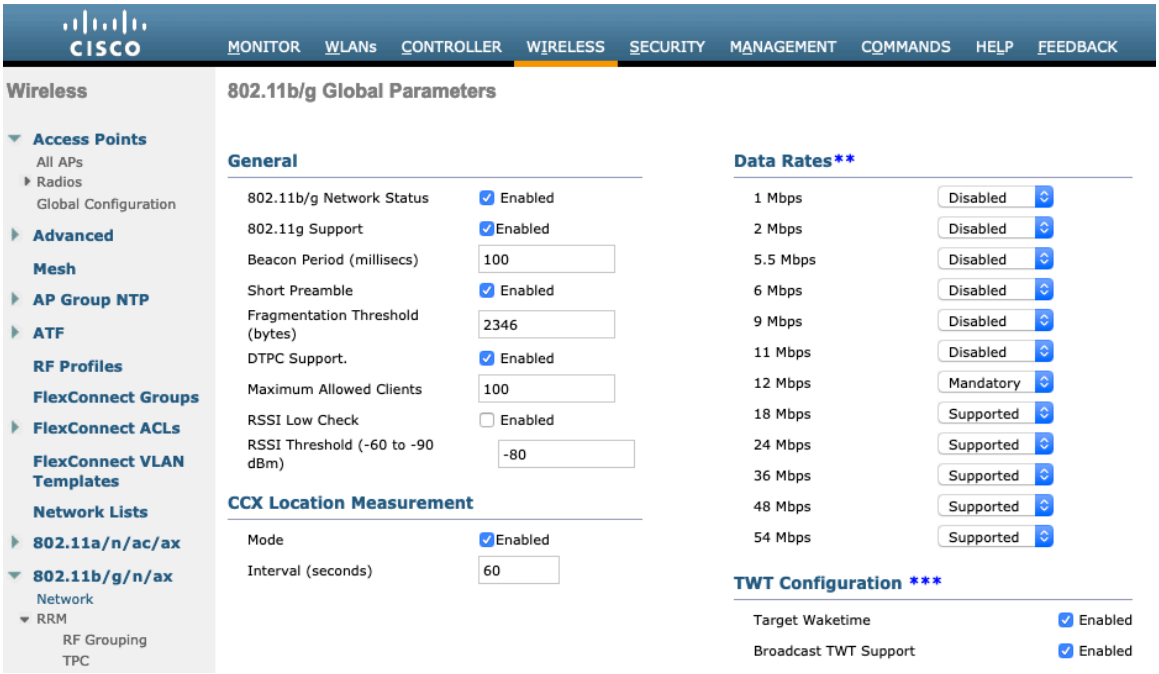
Ensure **DTPC Support** is enabled.

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

Maximum Allowed Clients can be configured as necessary.

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

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



Beamforming (ClientLink)

Enable **ClientLink** if using Cisco 802.11n capable Access Points.

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

(Cisco Controller) >config 802.11a beamforming global enable

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

(Cisco Controller) >config 802.11b beamforming global enable

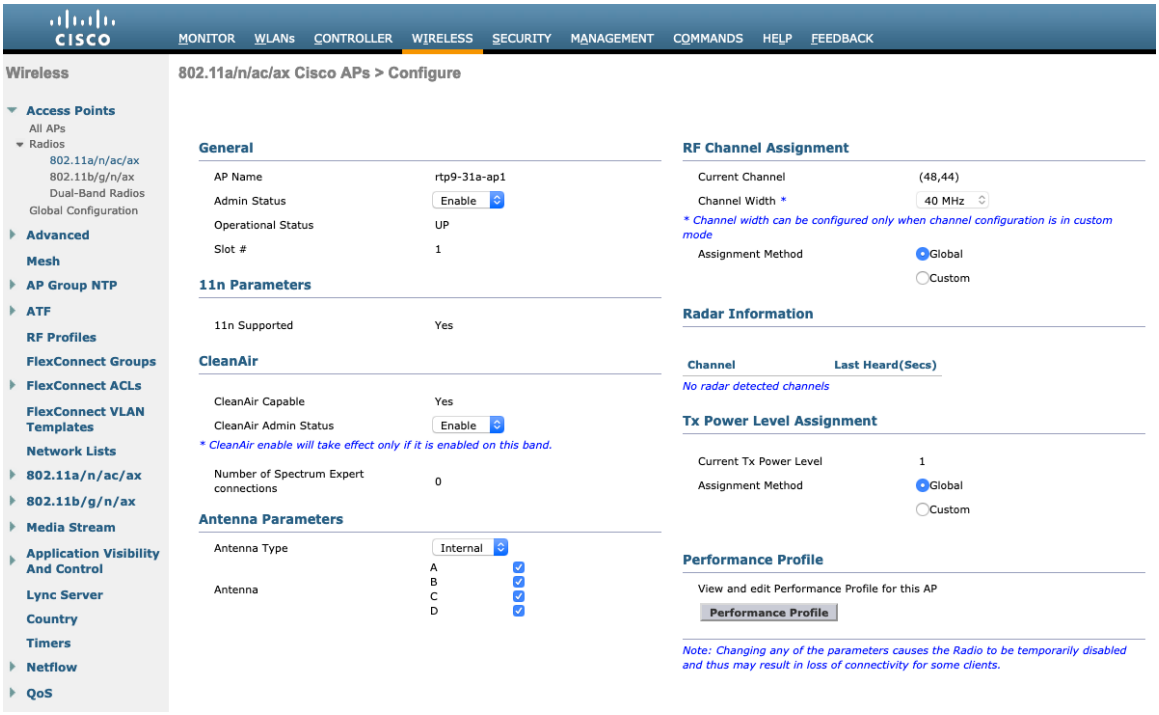
(Cisco Controller) >config 802.11b beamforming ap <ap_name> enable

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

(Cisco Controller) >show 802.11a

(Cisco Controller) >show 802.11b

Legacy Tx Beamforming setting……. **Enabled**

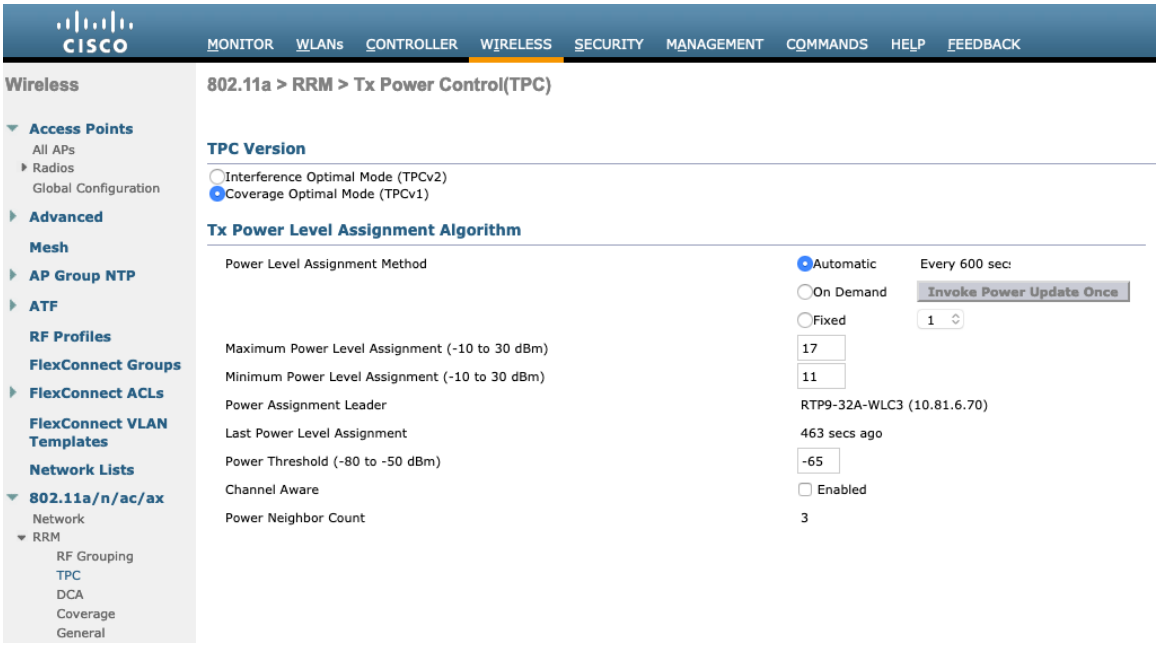


Auto RF (RRM)

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

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

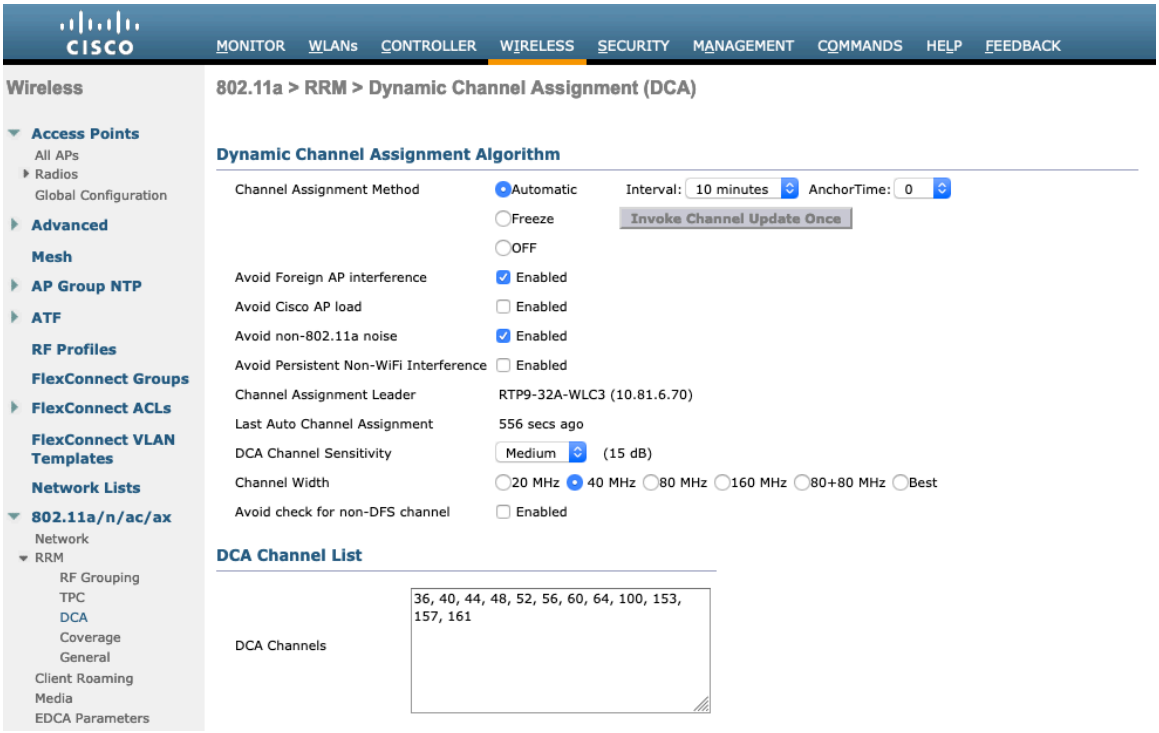
If using automatic power level assignment, a maximum and minimum power level can be specified.



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

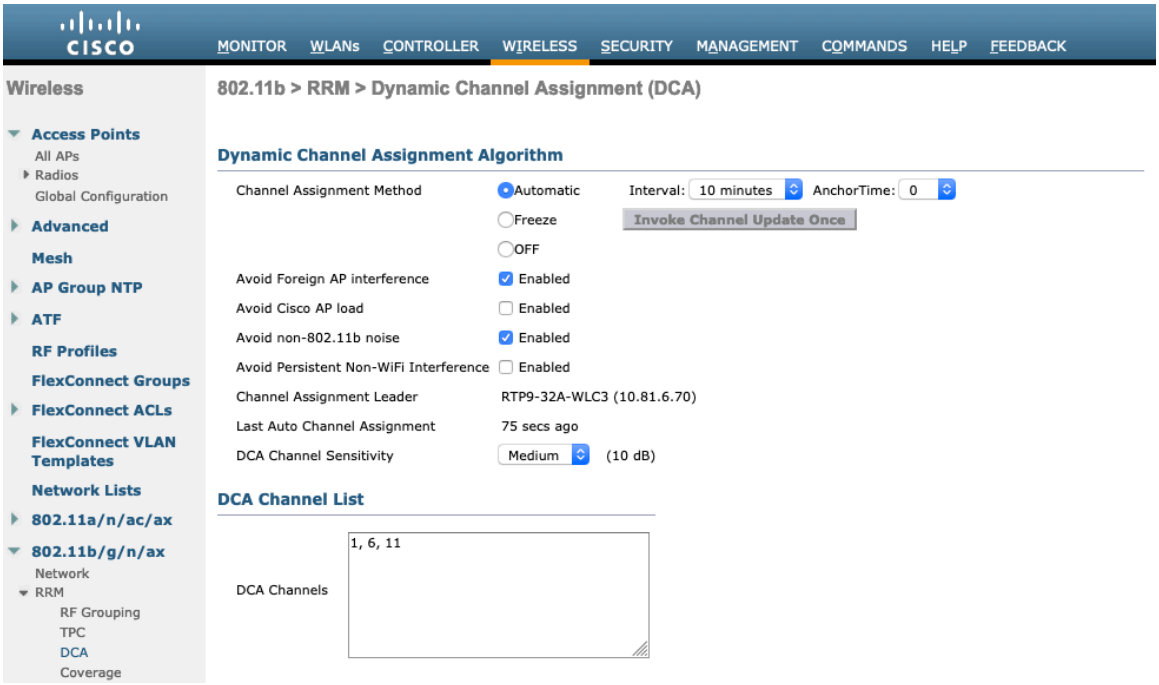
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

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



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

It is recommended to configure the 2.4 GHz channel for 20 MHz even if using Cisco 802.11n Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.



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

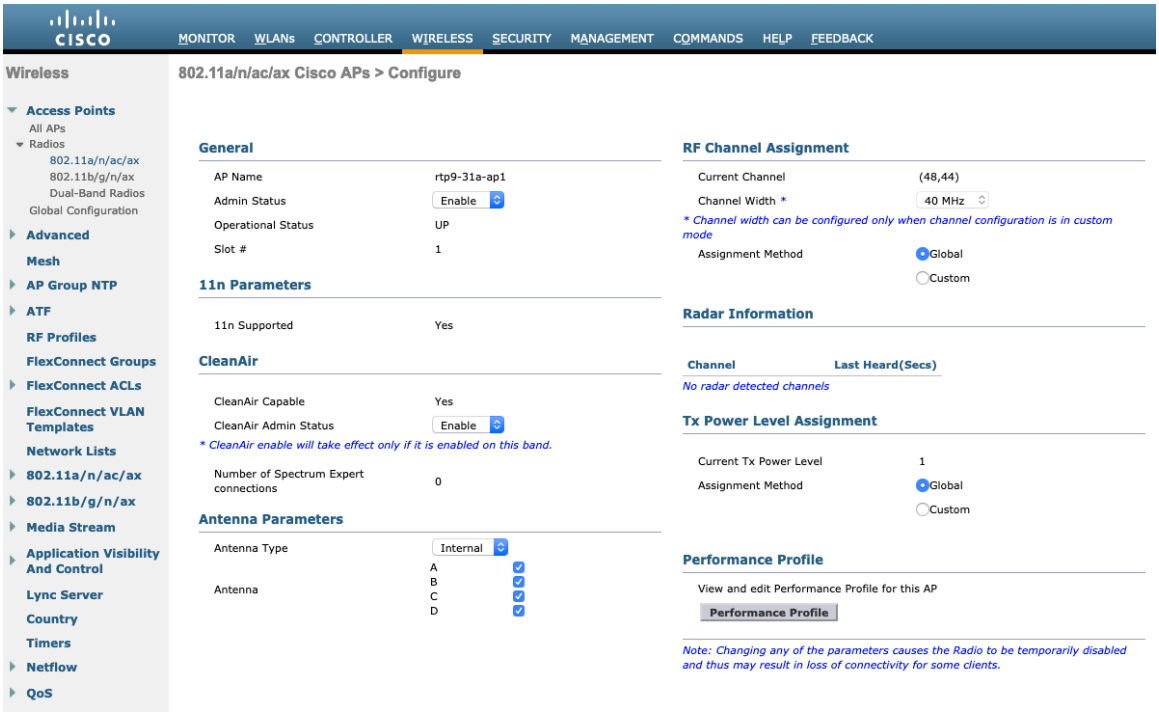
Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

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

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

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

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



Client Roaming

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

EDCA Parameters

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

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

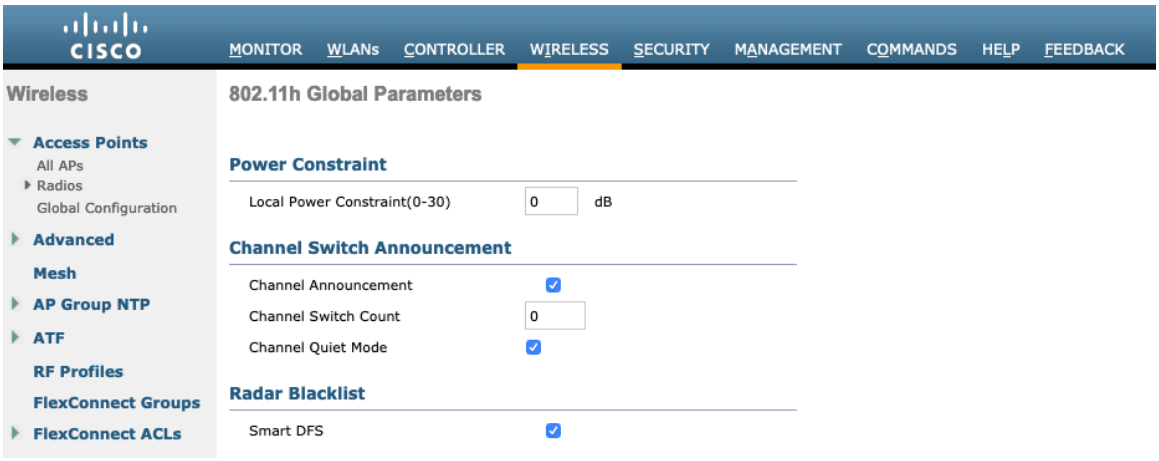
LLM is not supported on the Cisco 802.11n/ac Access Points.

DFS (802.11h)

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

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

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



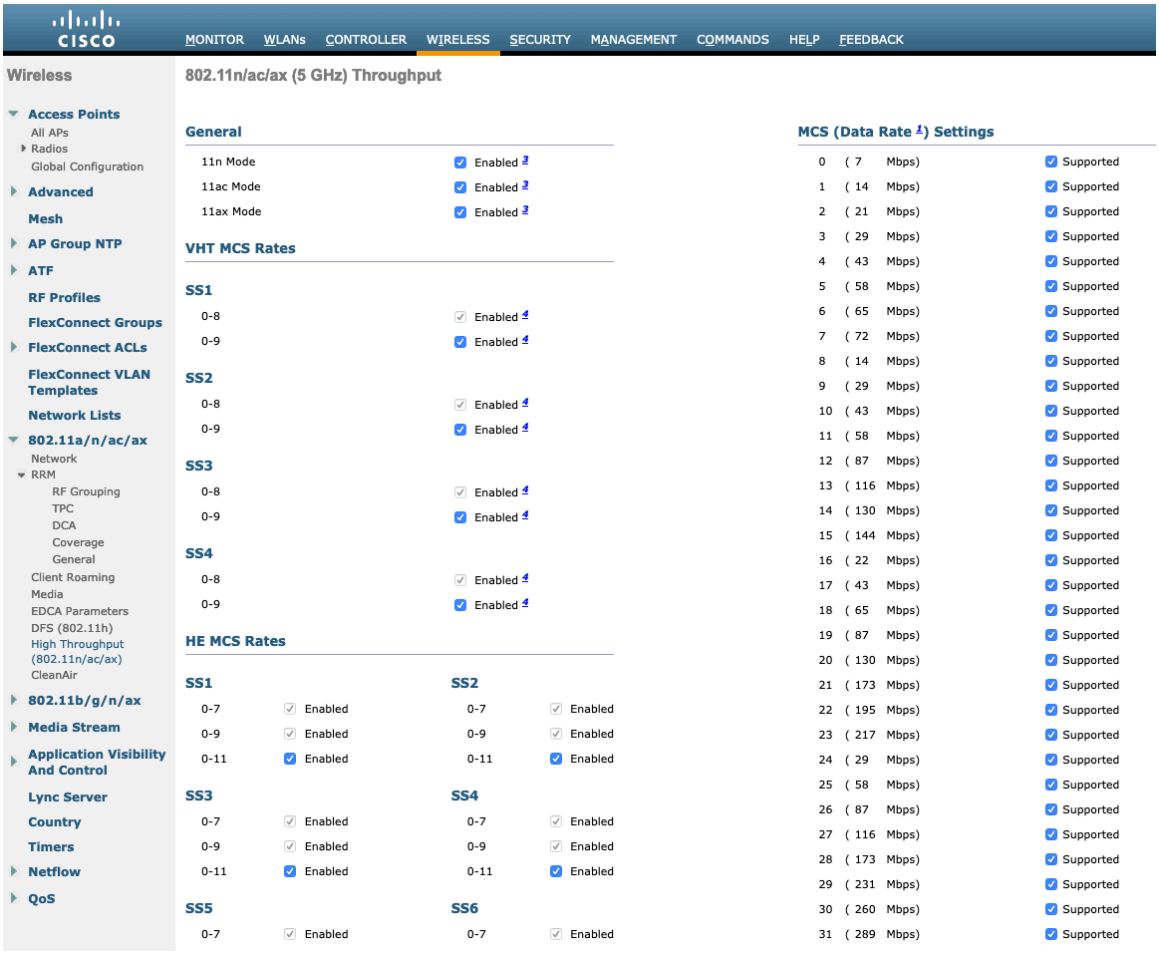
High Throughput (802.11n/ac)

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

802.11ac data rates are applicable to 5 GHz only.

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

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



Frame Aggregation

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

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

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

A-MSDU

User Priority 1, 2 = Enabled

User Priority 0, 3, 4, 5, 6, 7 = Disabled

A-MPDU

User Priority 0, 3, 4, 5 = Enabled

User Priority 1, 2, 6, 7 = Disabled

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

```
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
```

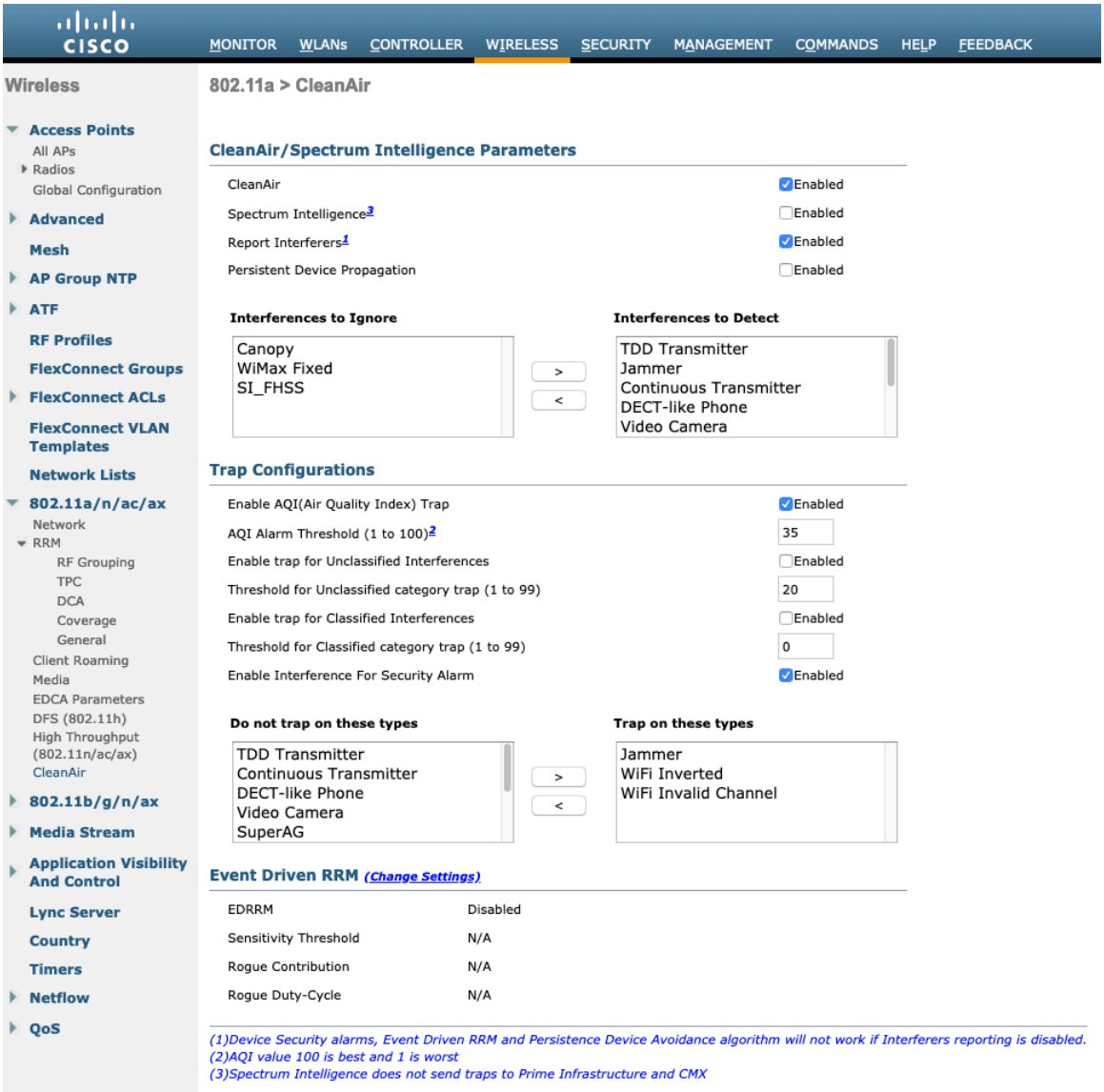
config 802.11b 11nSupport a-mpdu tx priority 7 disable

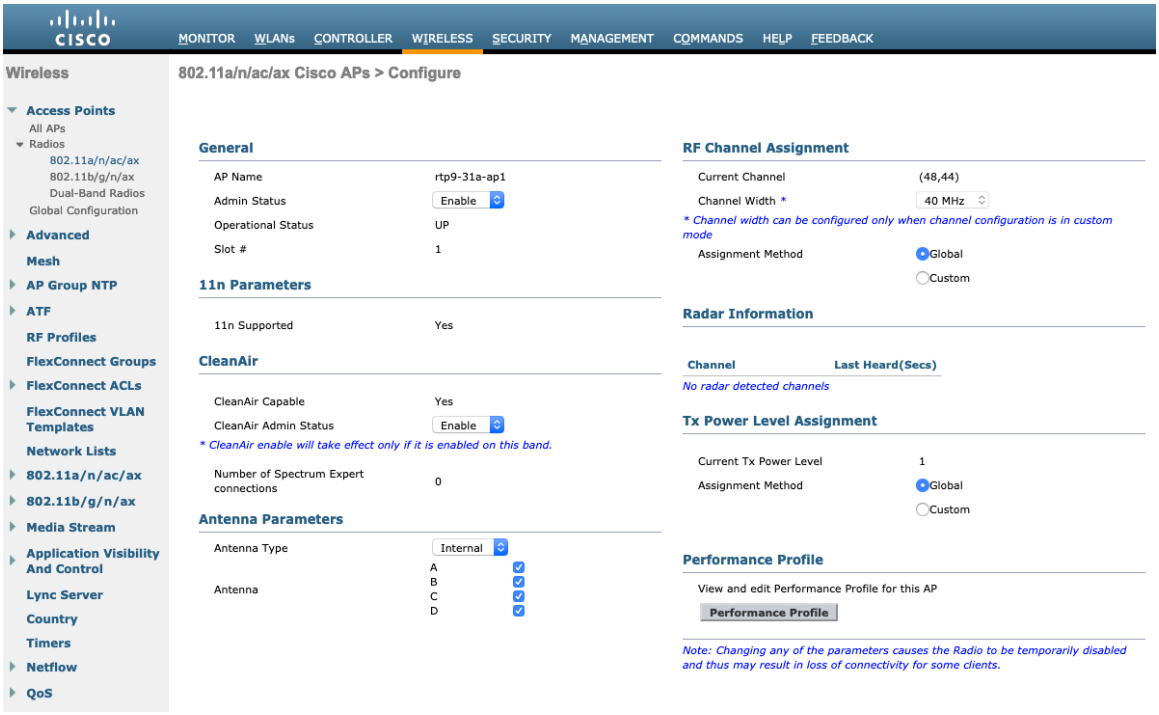
To view the current A-MPDU and A-MSDU configuration, enter either **show 802.11a** for 5 GHz or **show 802.11b** for 2.4 GHz.

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

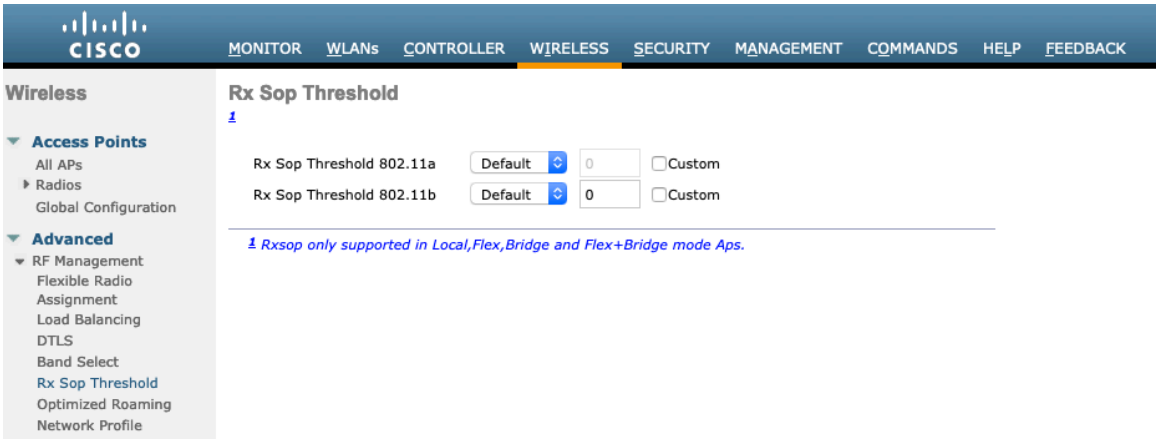
CleanAir should be **Enabled** when utilizing Cisco access points with CleanAir technology in order to detect any existing interferers.


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
Global Configuration
Advanced
Mesh
AP Group NTP
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
Network Lists
802.11a/n/ac/ax
Network
RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
DFS (802.11h)
High Throughput (802.11n/ac/ax)
CleanAir
802.11b/g/n/ax
Media Stream
Application Visibility And Control
Lync Server
Country
Timers
Netflow
QoS
802.11a > CleanAir
CleanAir/Spectrum Intelligence Parameters
CleanAir
Enabled
Spectrum Intelligence
Enabled
Report Interferers
Enabled
Persistent Device Propagation
Enabled
Interferences to Ignore
Canopy
WiMax Fixed
SI_FHSS
Interferences to Detect
TDD Transmitter
Jammer
Continuous Transmitter
DECT-like Phone
Video Camera
Trap Configurations
Enable AQI(Air Quality Index) Trap
Enabled
AQI Alarm Threshold (1 to 100)
35
Enable trap for Unclassified Interferences
Enabled
Threshold for Unclassified category trap (1 to 99)
20
Enable trap for Classified Interferences
Enabled
Threshold for Classified category trap (1 to 99)
0
Enable Interference For Security Alarm
Enabled
Do not trap on these types
TDD Transmitter
Continuous Transmitter
DECT-like Phone
Video Camera
SuperAG
Trap on these types
Jammer
WiFi Inverted
WiFi Invalid Channel
Event Driven RRM (Change Settings)
EDRRM
Disabled
Sensitivity Threshold
N/A
Rogue Contribution
N/A
Rogue Duty-Cycle
N/A
(1)Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled.
(2)AQI value 100 is best and 1 is worst
(3)Spectrum Intelligence does not send traps to Prime Infrastructure and CMX



Rx Sop Threshold

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



WLAN Settings

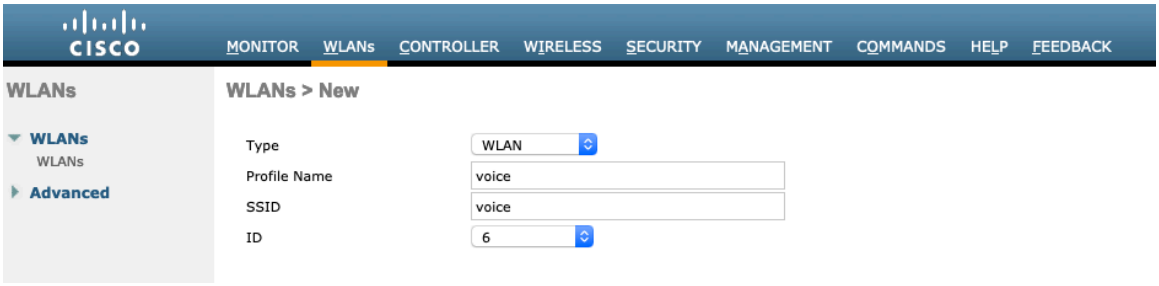
It is recommended to have a separate SSID for the Cisco Wireless Phone 840 and 860.

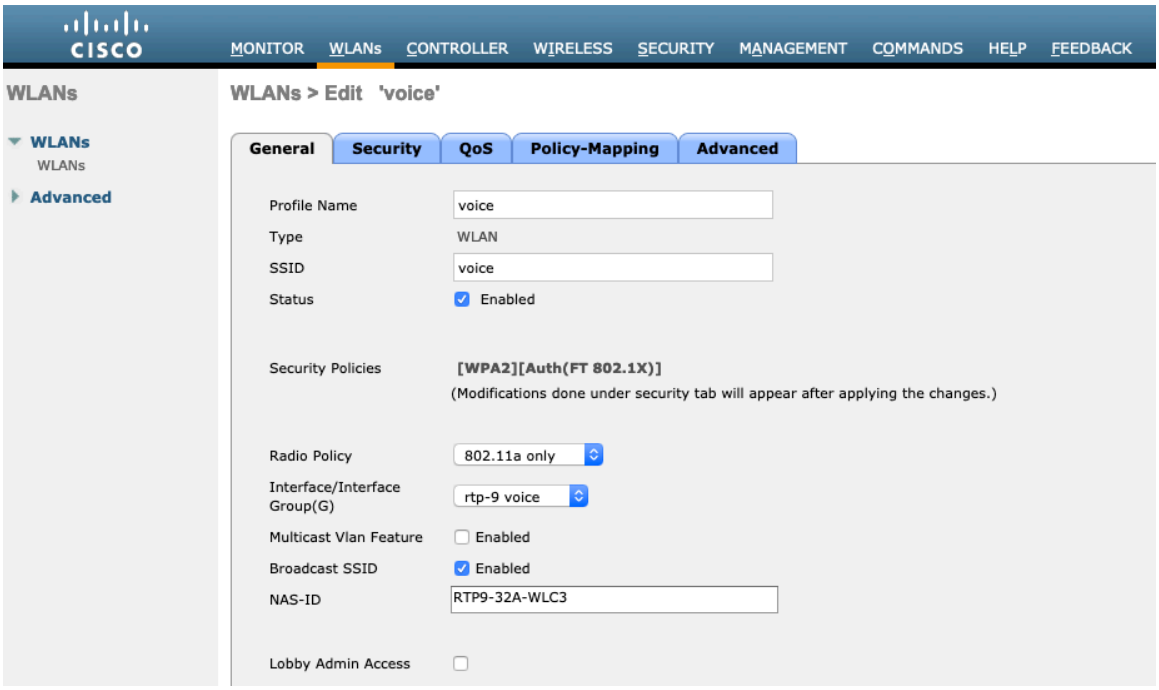
However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

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

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

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



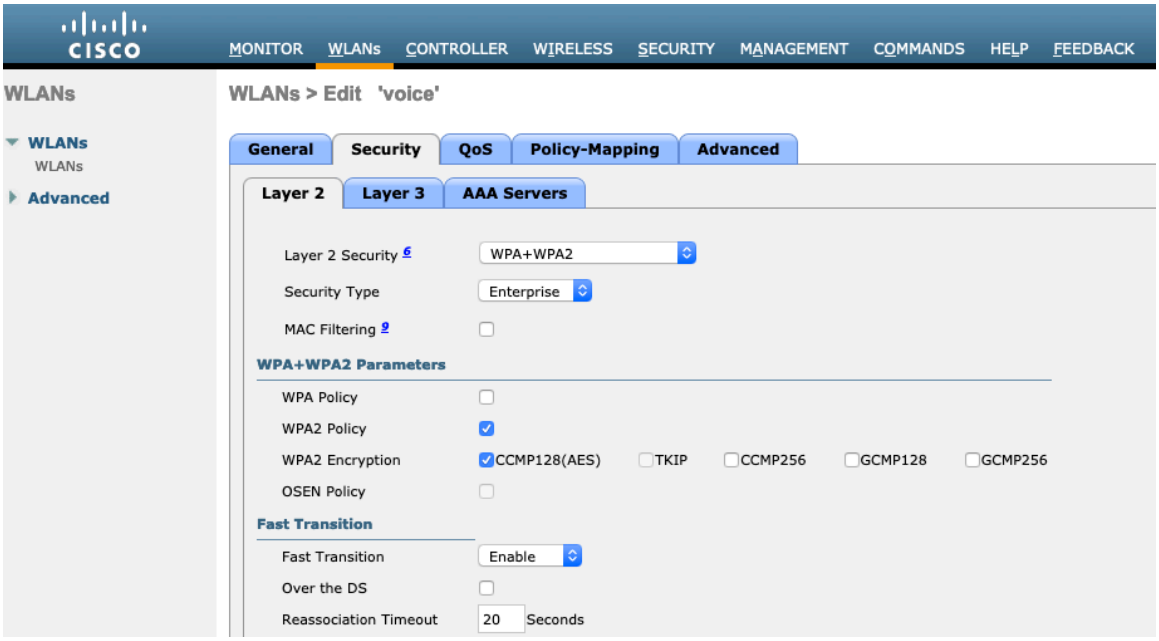


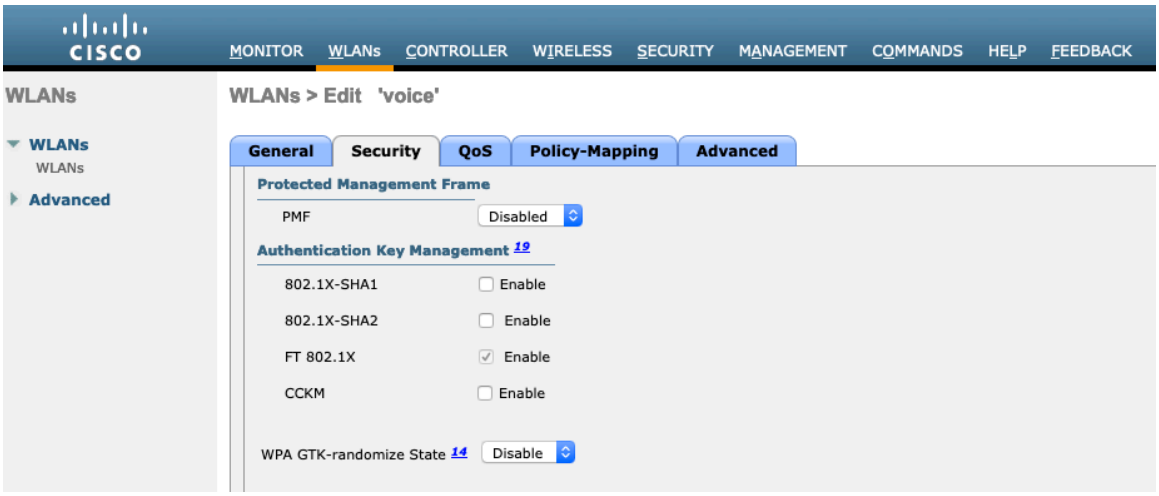
To utilize 802.11r (FT) for fast secure roaming, check the box to enable Fast Transition.

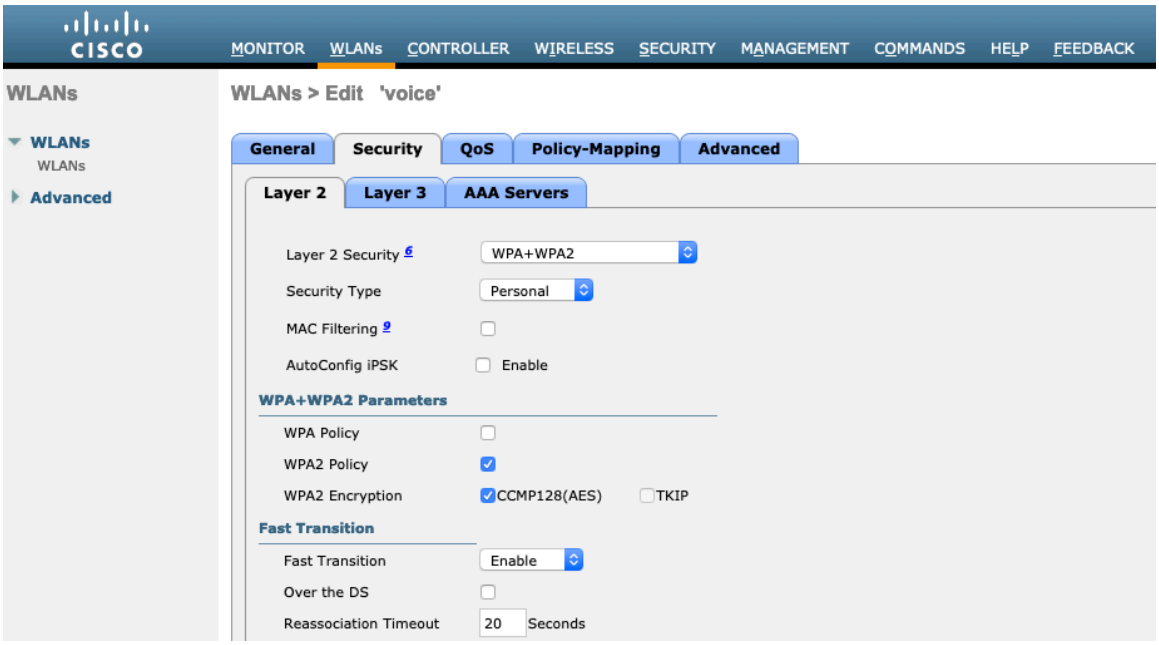
Is recommended to uncheck **Over the DS** to utilize the Over the Air method instead of the Over the Distribution System method.

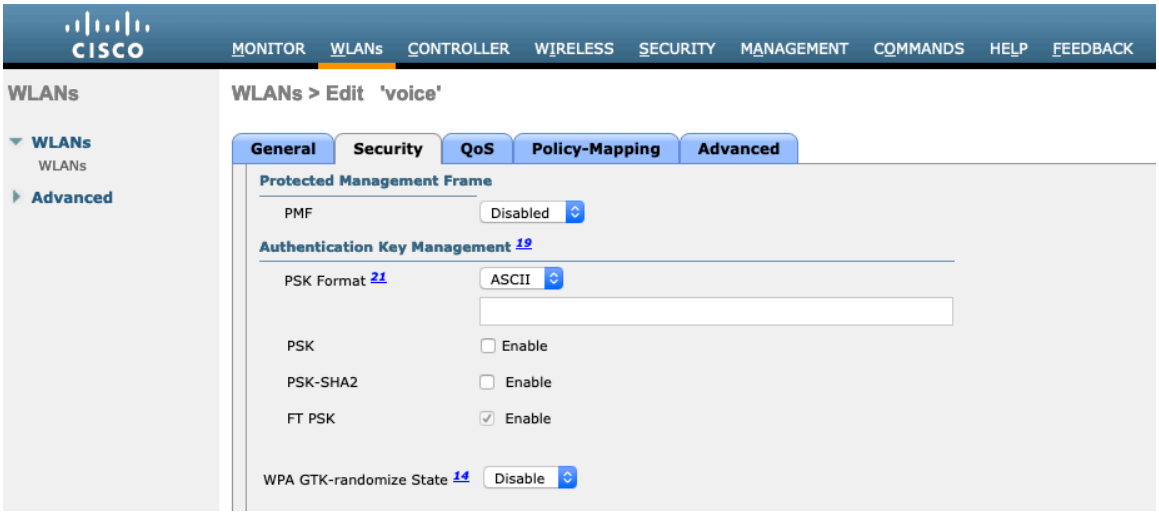
Protected Management Frame should be set to **Optional** or **Disabled.**

Enable WPA2 policy with AES encryption then either FT 802.1x or FT PSK for authenticated key management type depending on whether 802.1x or PSK is to be utilized.

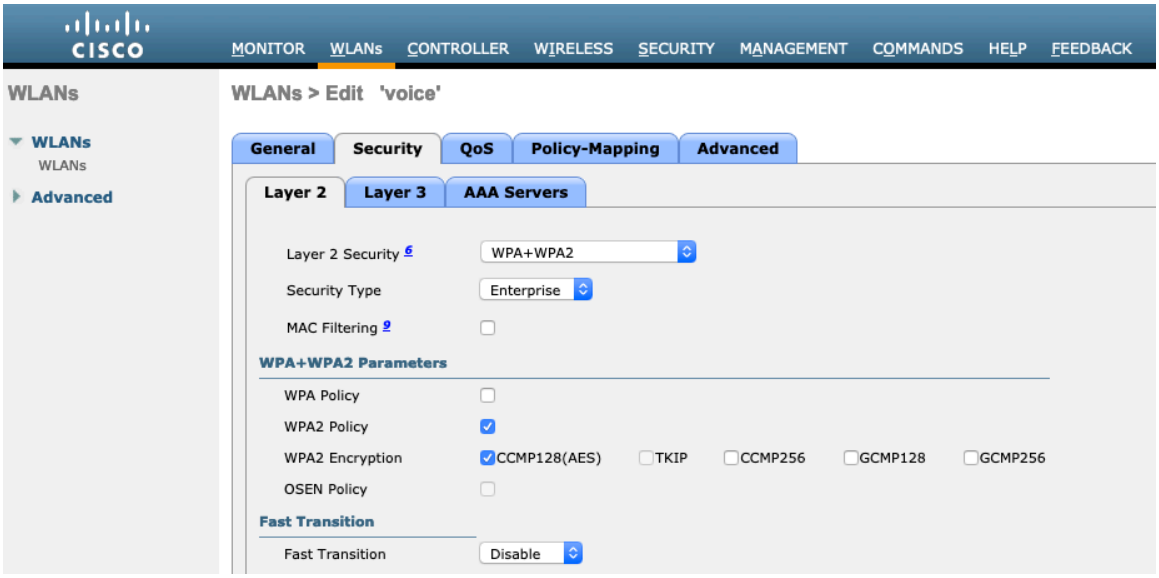

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'voice'
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security 6 WPA+WPA2
Security Type Enterprise
MAC Filtering 9
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption CCMP128(AES) TKIP CCMP256 GCMP128 GCMP256
OSEN Policy
Fast Transition
Fast Transition Enable
Over the DS
Reassociation Timeout 20 Seconds

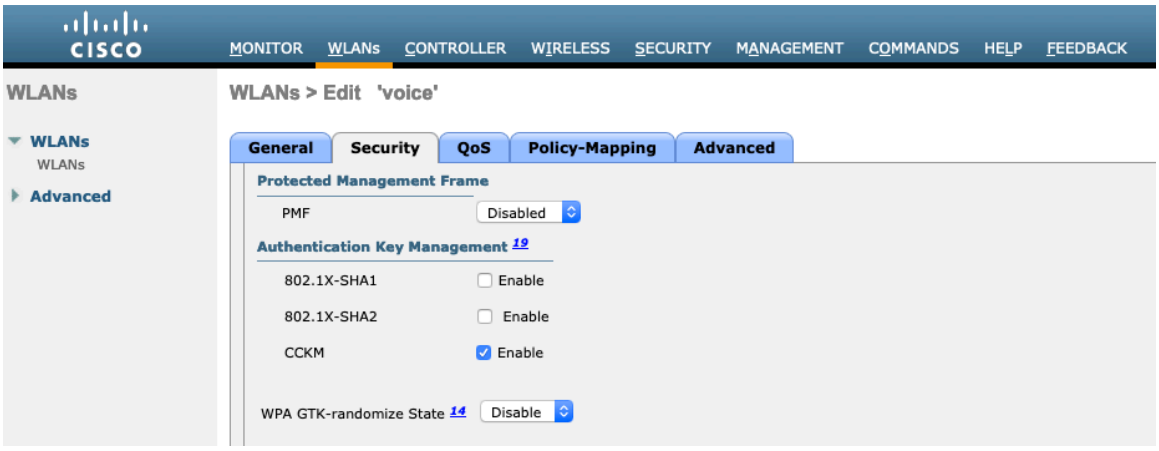

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'voice'
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Protected Management Frame
PMF Disabled
Authentication Key Management 19
802.1X-SHA1 Enable
802.1X-SHA2 Enable
FT 802.1X Enable
CCKM Enable
WPA GTK-randomize State 14 Disable


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'voice'
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security 6 WPA+WPA2
Security Type Personal
MAC Filtering 9
AutoConfig iPSK Enable
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption CCMP128(AES) TKIP
Fast Transition
Fast Transition Enable
Over the DS
Reassociation Timeout 20 Seconds



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





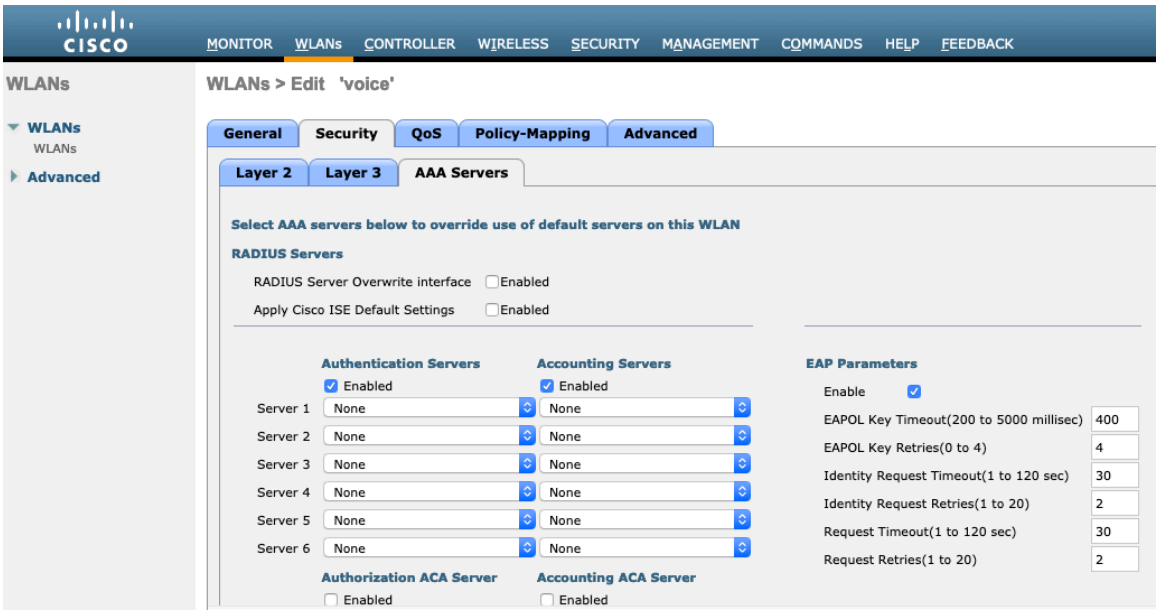
802.1x, CCKM and/or PSK may also be enabled if wanting to utilize the same SSID for various type of voice clients, where some clients do not support 802.11r (FT) depending on whether 802.1x or PSK is being utilized.

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

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

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

If wanting to configure the EAP parameters at the per SSID level, check **Enable** in the EAP Parameters section and enter the desired values.

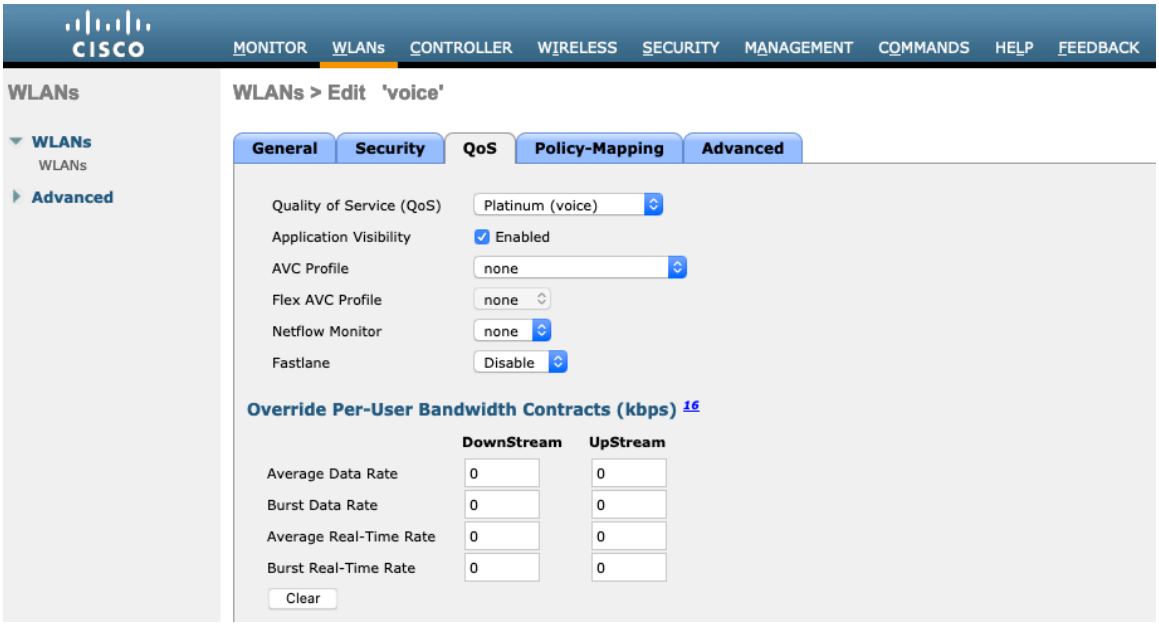


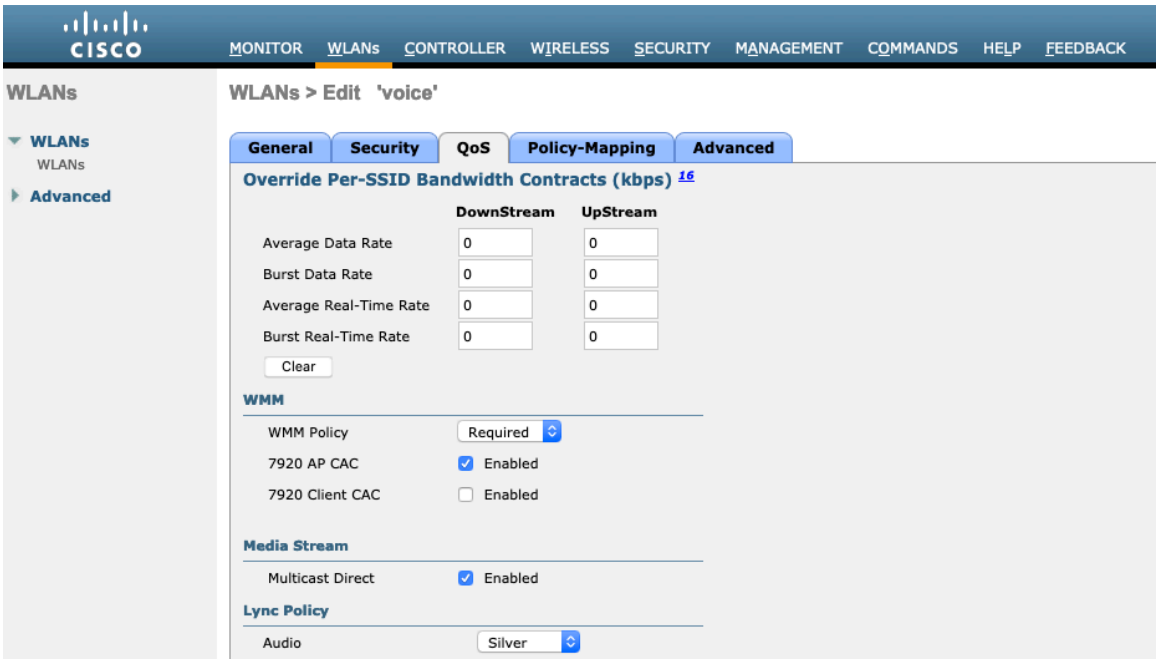
The WMM policy should be set to **Required** only if the Cisco Wireless Phone 840 and 860 or other WMM enabled phones will be using this SSID.

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

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

Enabling WMM will enable the 802.11e version of QBSS.





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

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

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

Configure **Client Exclusion** as necessary.

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

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

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

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

DHCP Address Assignment Required should be disabled.

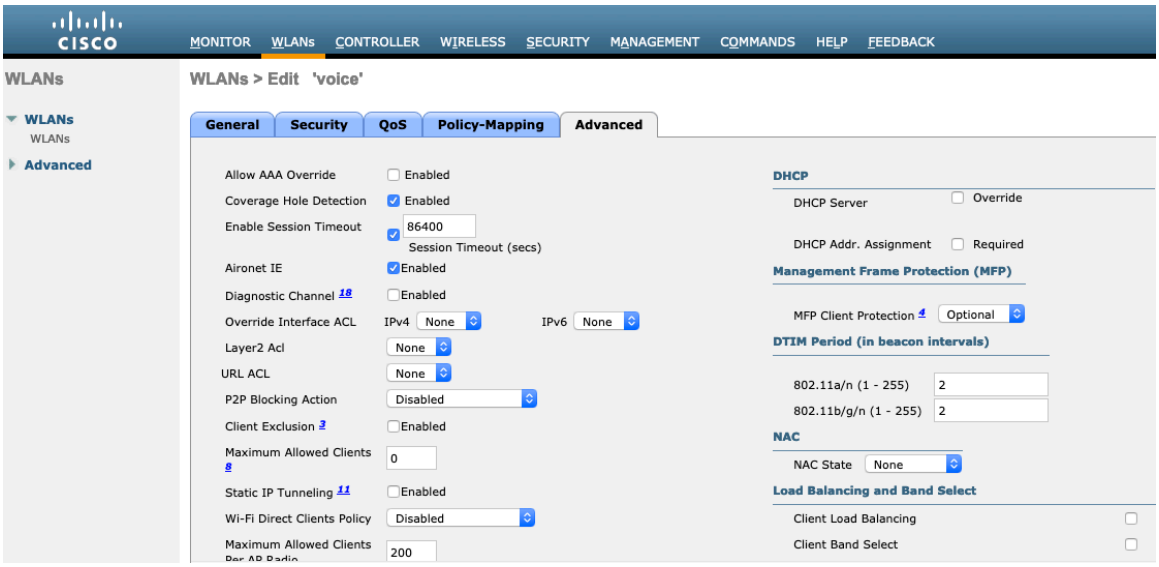
Management Frame Protection should be set to **Optional** or **Disabled.**

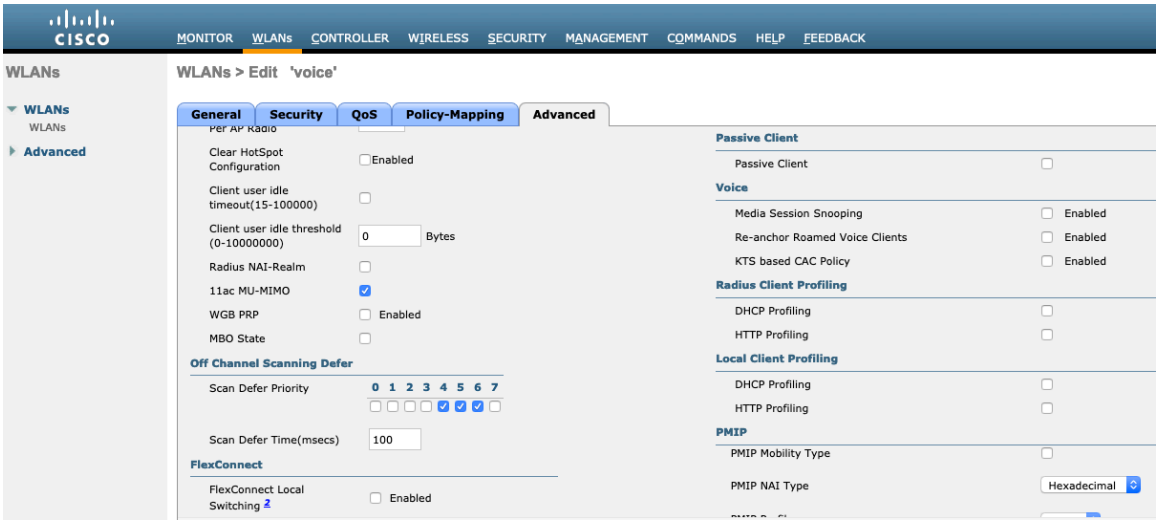
Use a **DTIM Period** of **2** with a beacon period of **100 ms**.

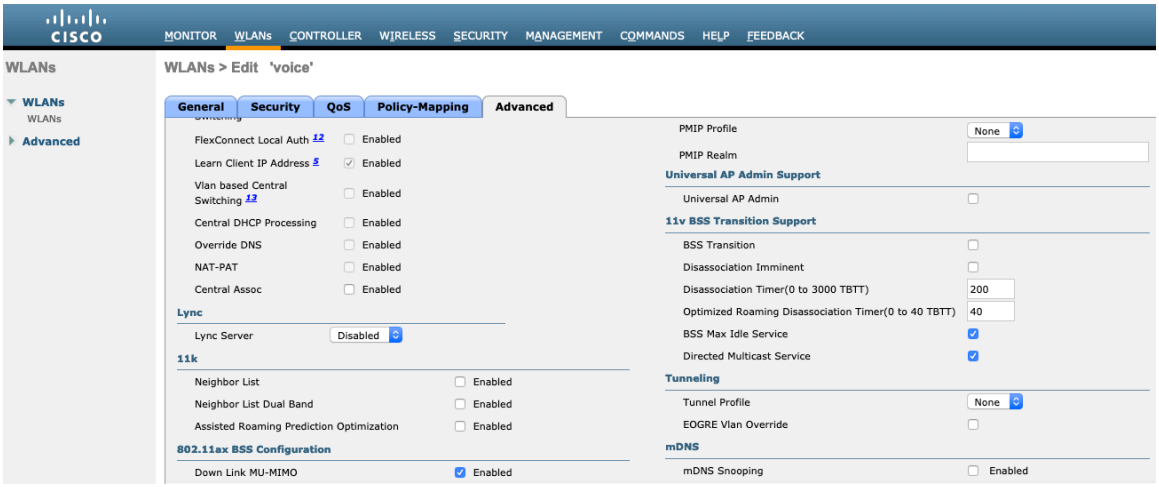
Ensure **Client Load Balancing** and **Client Band Select** are disabled.

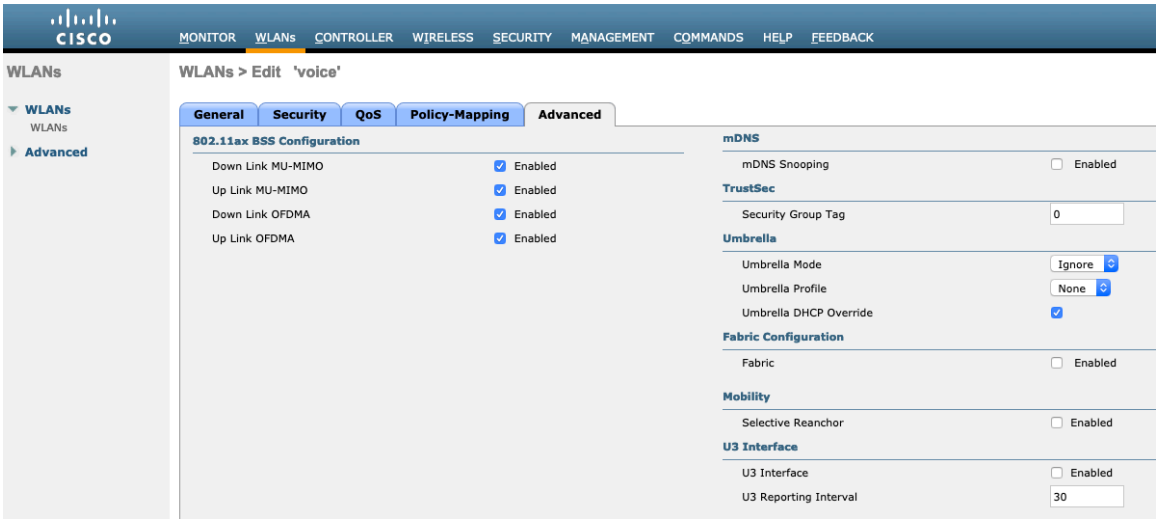
It is recommended to set **Re-anchor Roamed Voice Clients** to disabled as this can cause brief interruptions with wireless LAN connectivity when a call is terminated after performing an inter-controller roaming.

It is recommend to enable 802.11k and 802.11v



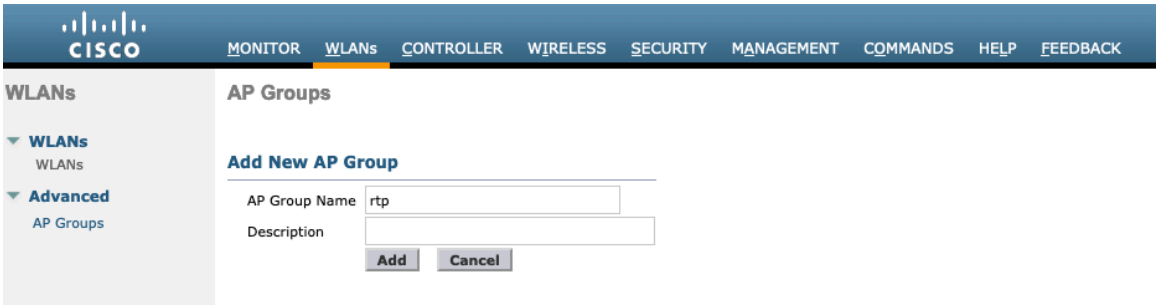


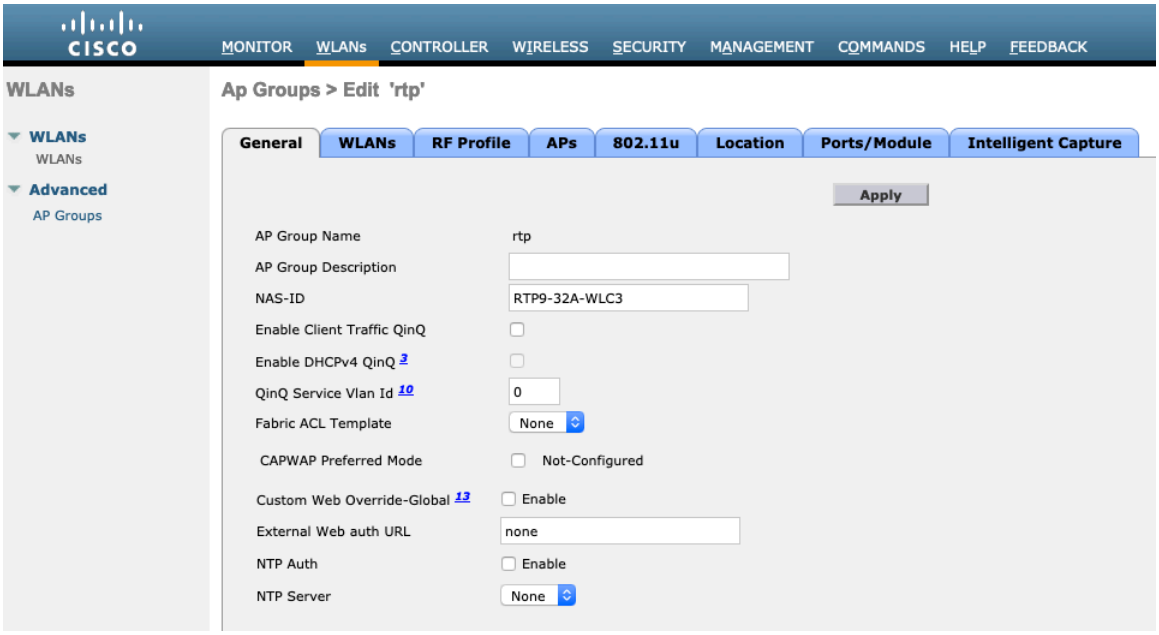




AP Groups

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.

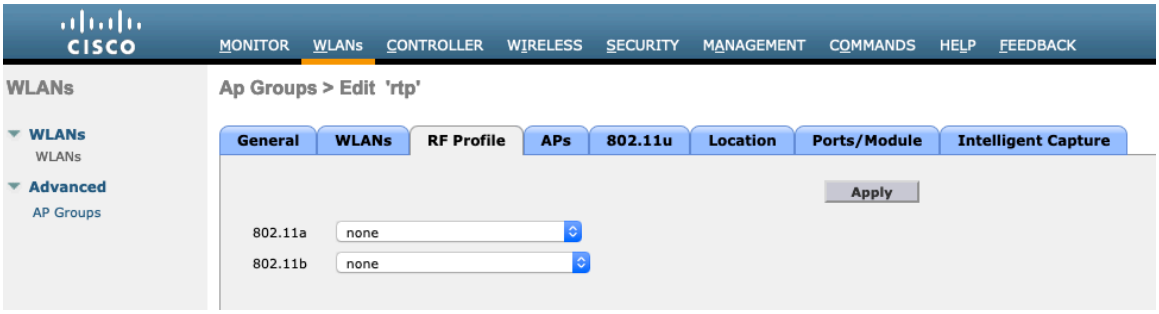




On the **WLANs** tab, select the desired SSIDs and interfaces to map to then select **Add**.

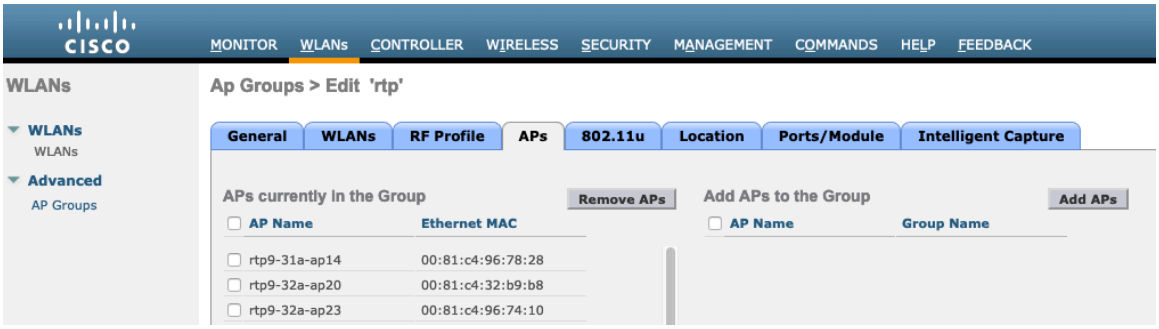
On the **RF Profile** tab, select the desired 802.11a or 802.11b RF Profile, then select **Apply**.

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.

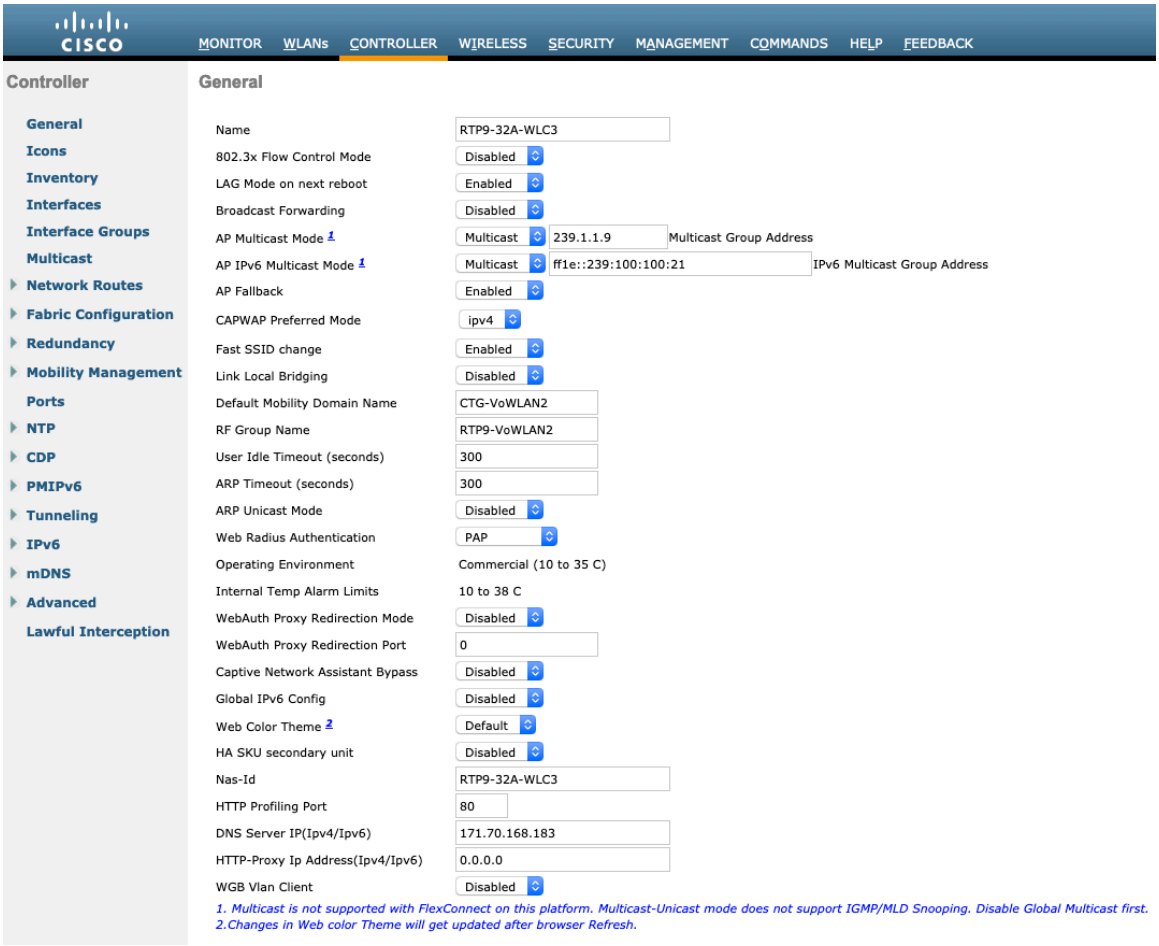


Controller Settings

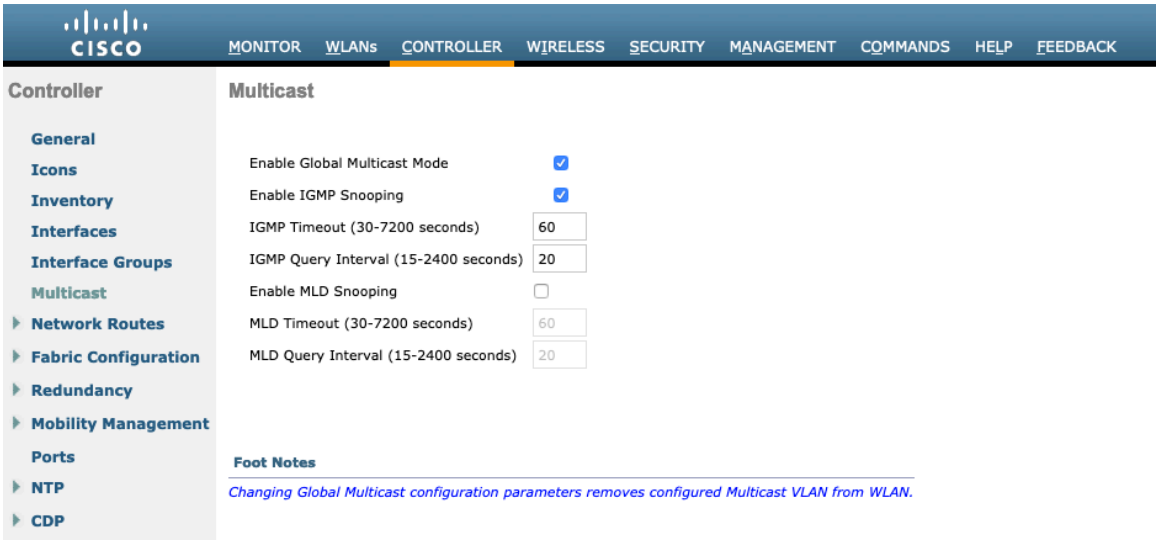
Ensure the Cisco Wireless LAN Controller hostname is configured correctly.

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

Configure the desired AP multicast mode.

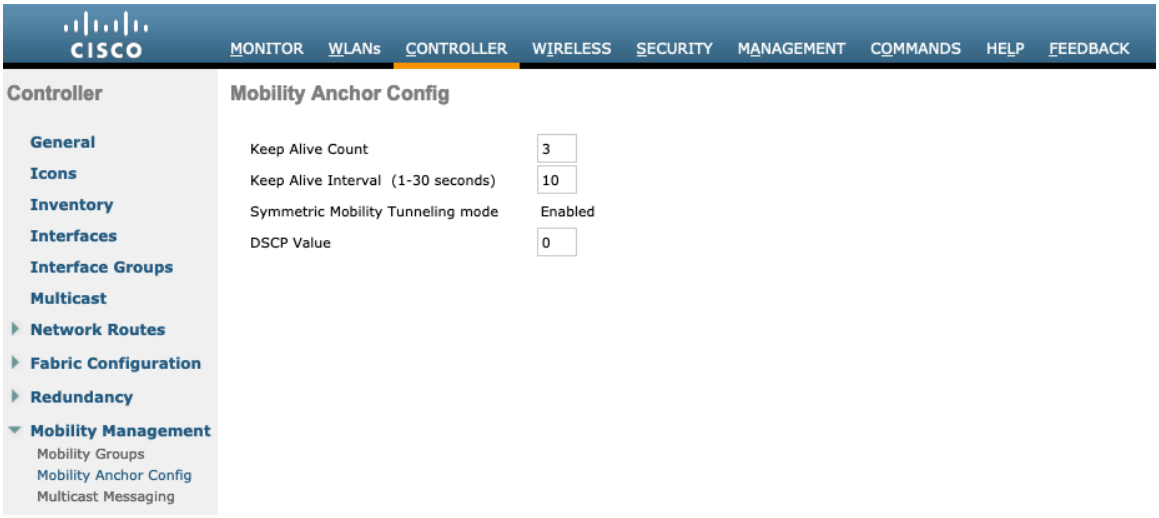


If utilizing multicast, then **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be enabled.

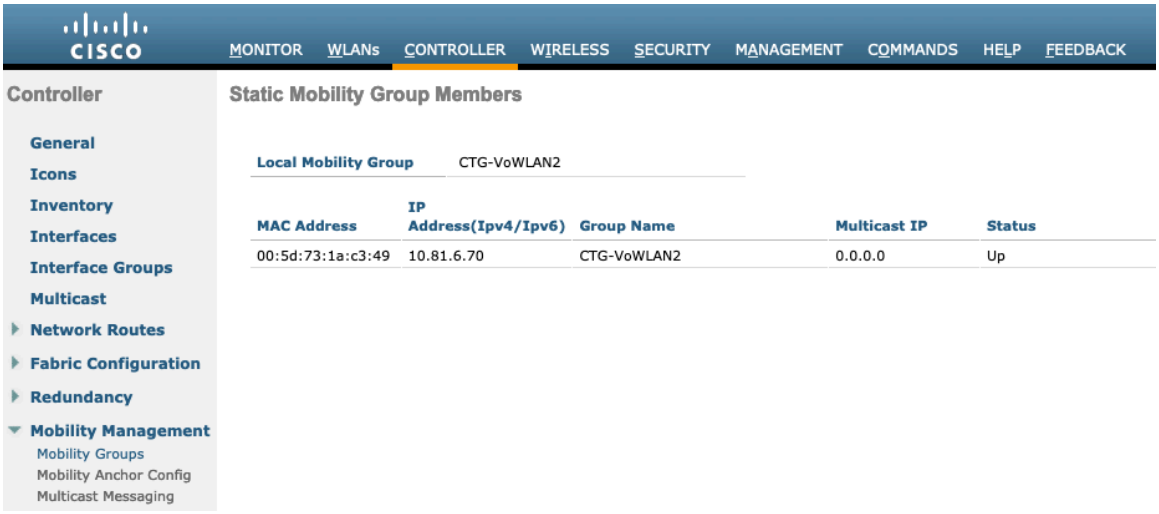


If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling** should be **Enabled**.

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)

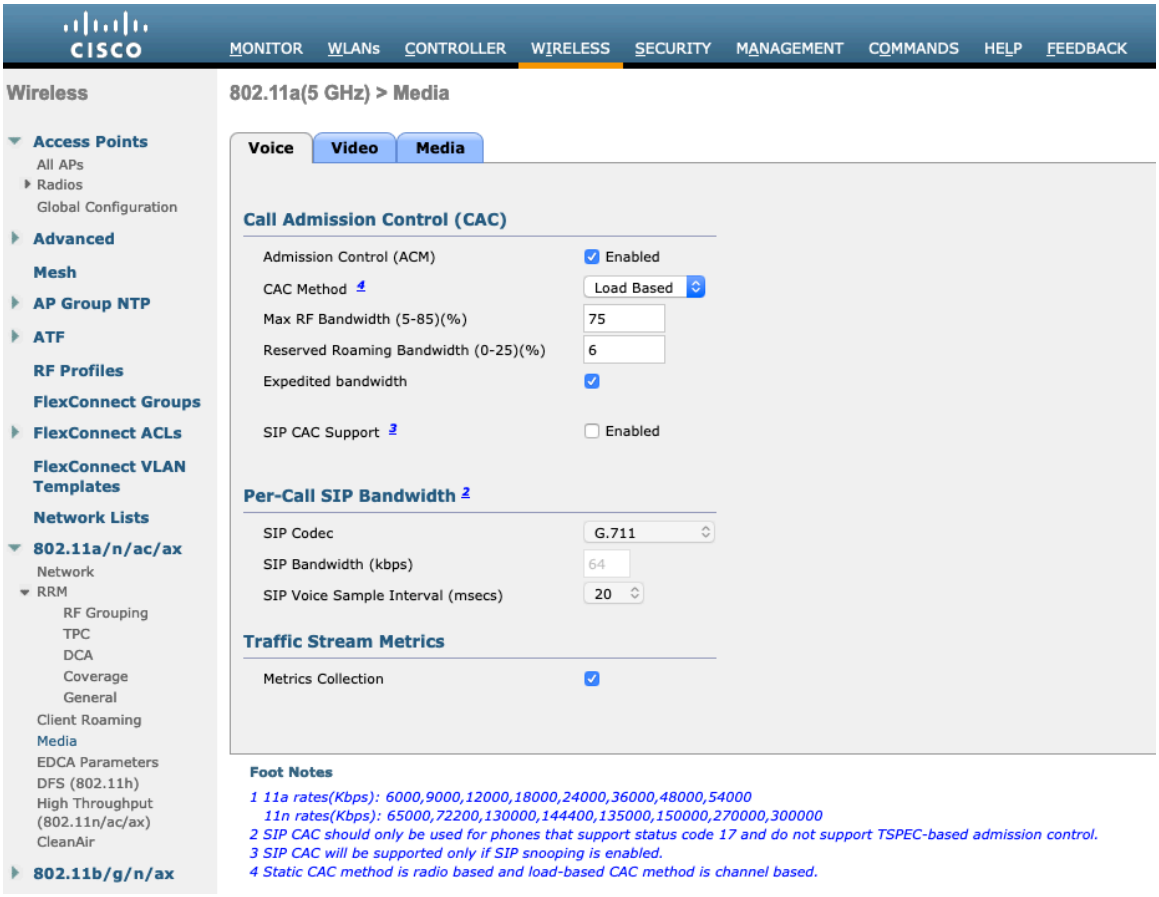
It is recommended to enable **Admission Control Mandatory** for **Voice** and configure the maximum bandwidth and reserved roaming bandwidth percentages for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

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

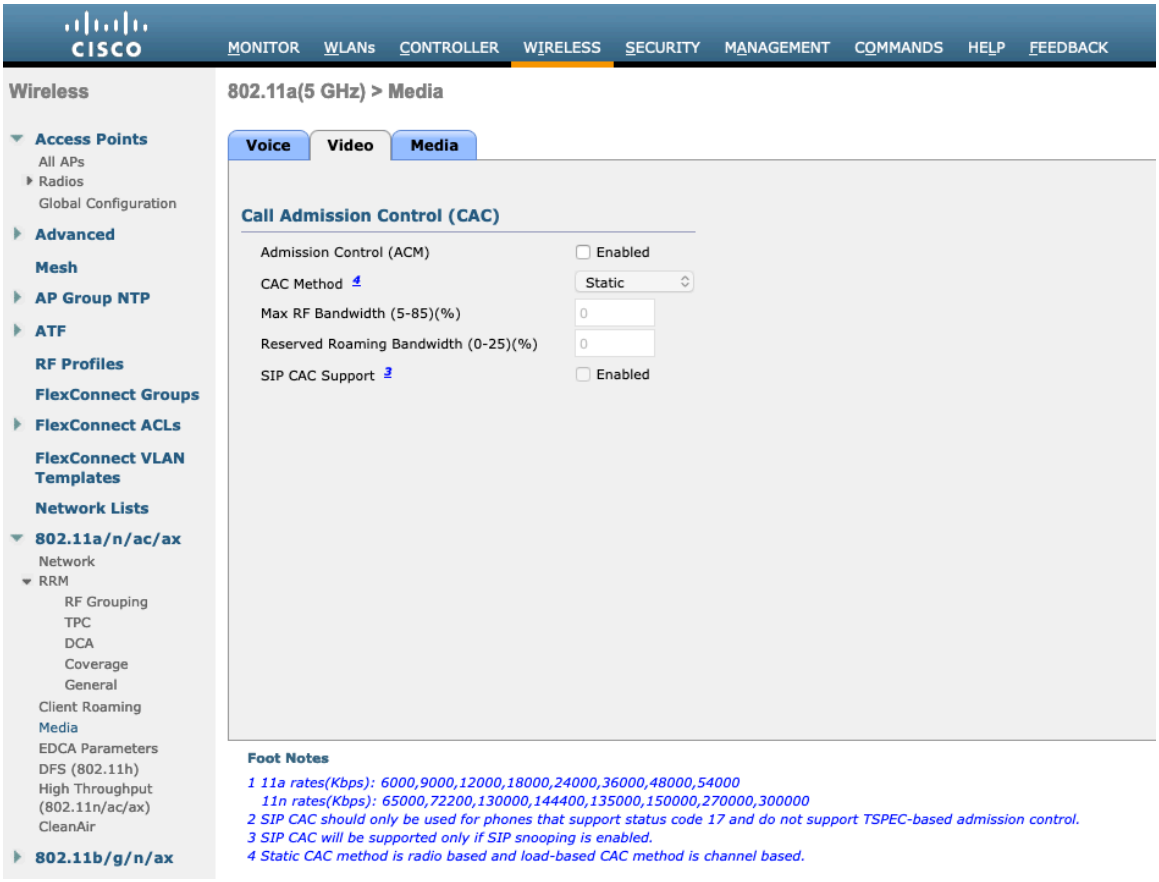
Roaming clients are not limited to using the reserved roaming bandwidth, but roaming bandwidth is to reserve some bandwidth for roaming clients in case all other bandwidth is utilized.

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.



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…..... Required

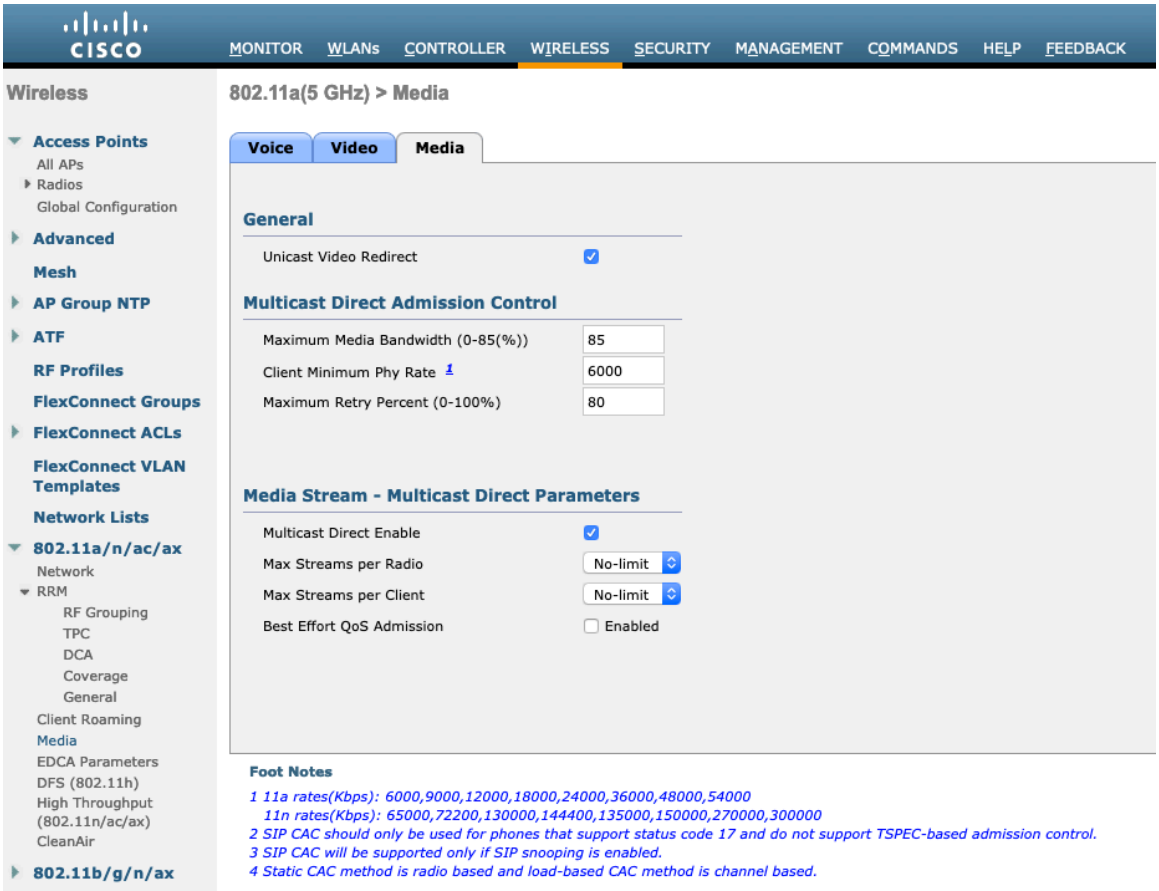
Dot11-Phone Mode (7920)…..... ap-cac-limit
Wired Protocol…..... None

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.

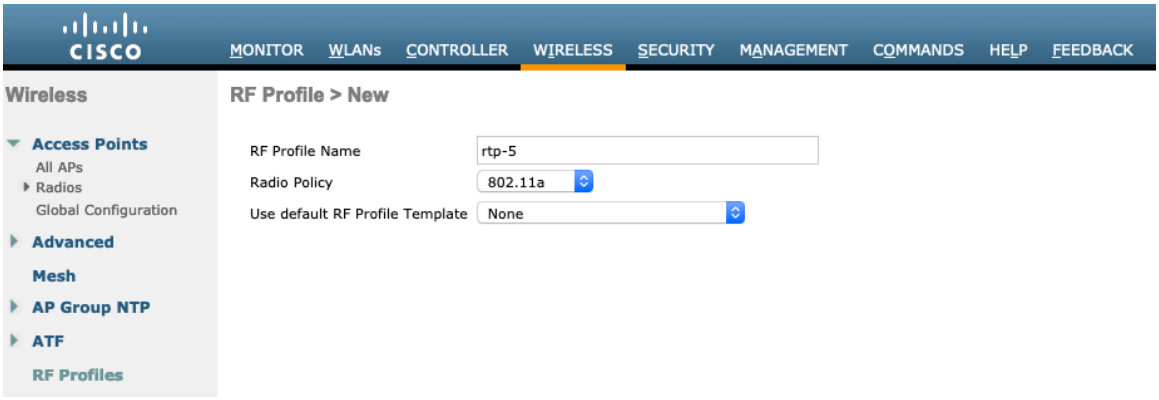


RF Profiles

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 Wireless Phone 840 and 860 to be applied to 5 GHz radios only. RF Profiles are applied to an AP group once created.

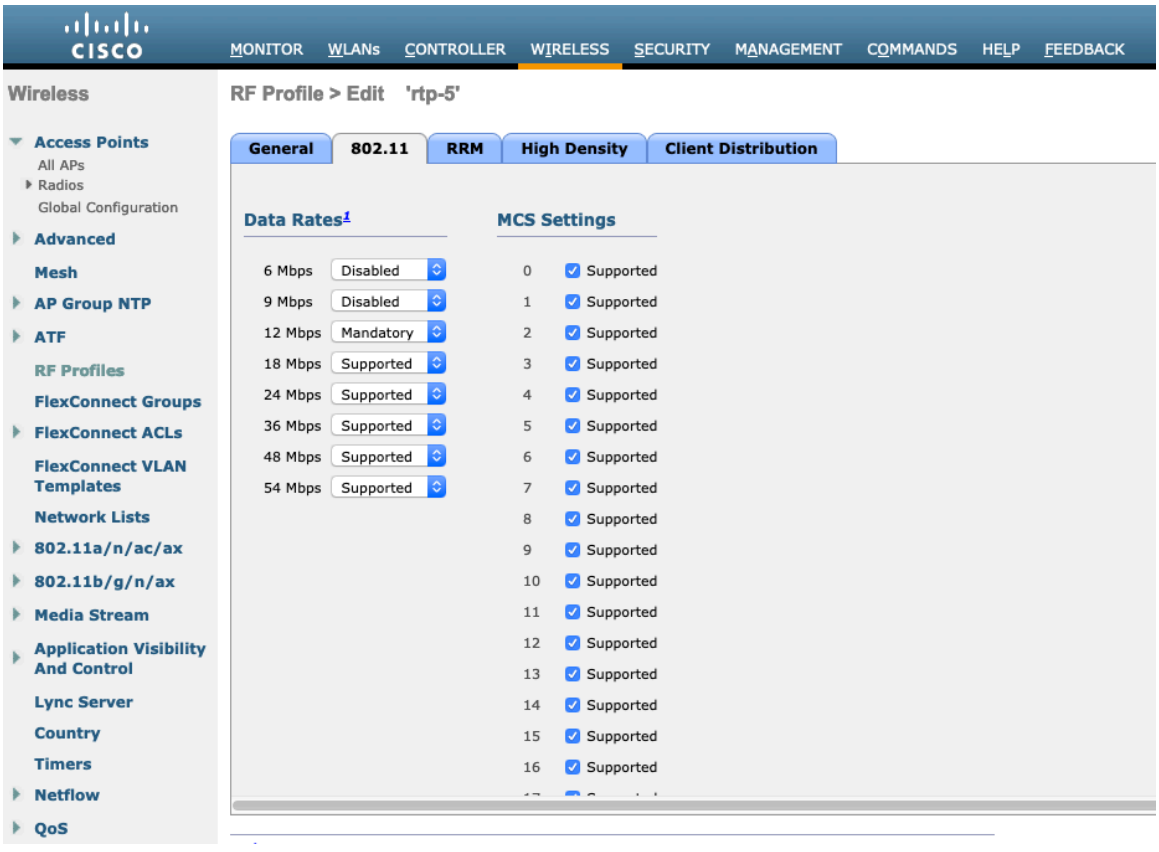
When creating an RF Profile, the **RF Profile Name** and **Radio Policy** must be defined.

Select 802.11a or 802.11b/g for the **Radio Policy**.

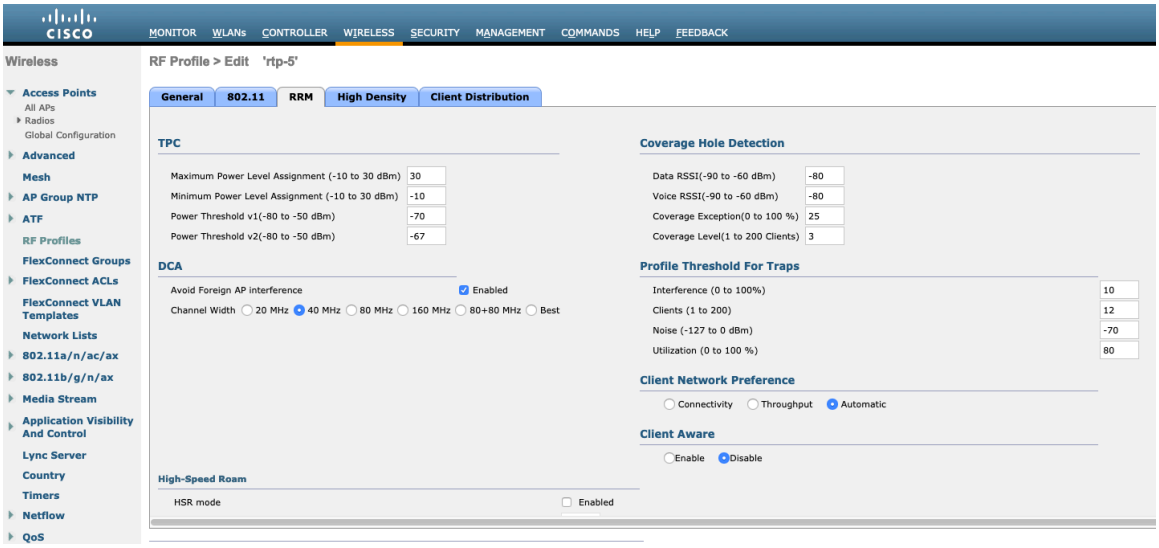


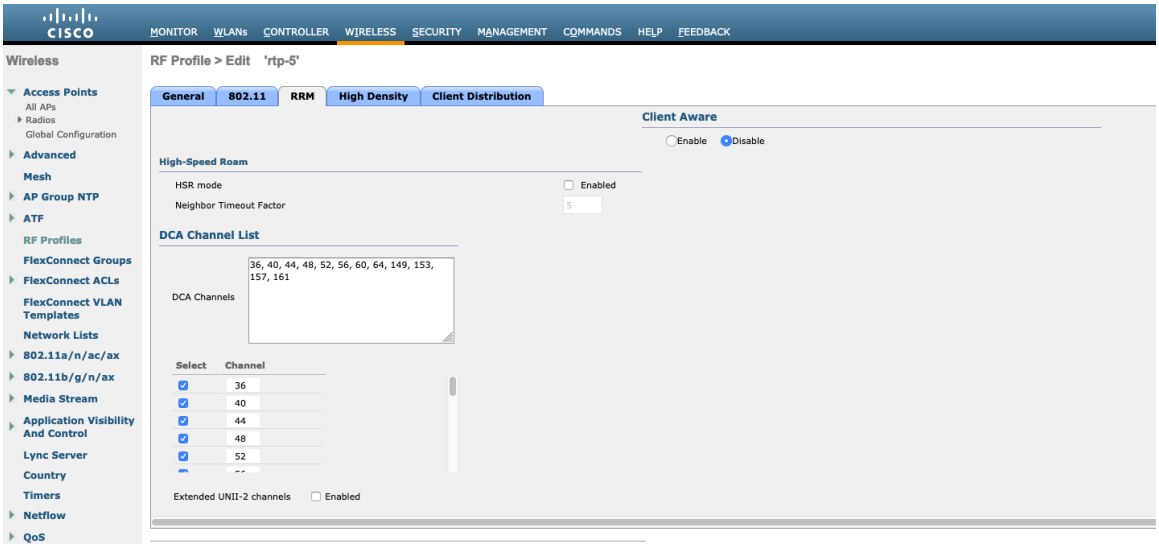
On the **802.11** tab, configure the data rates as desired.

Is recommended to enable 12 Mbps as **Mandatory** and 18 Mbps and higher as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

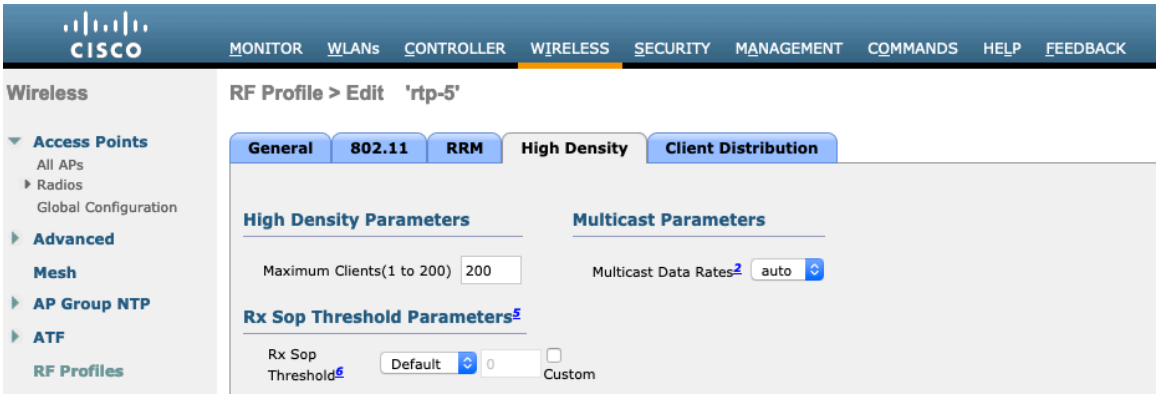


On the **RRM** tab, the **Maximum Power Level Assignment** and **Minimum Power Level Assignment** settings as well as other **DCA**, **TPC**, and **Coverage Hole Detection** settings can be configured.





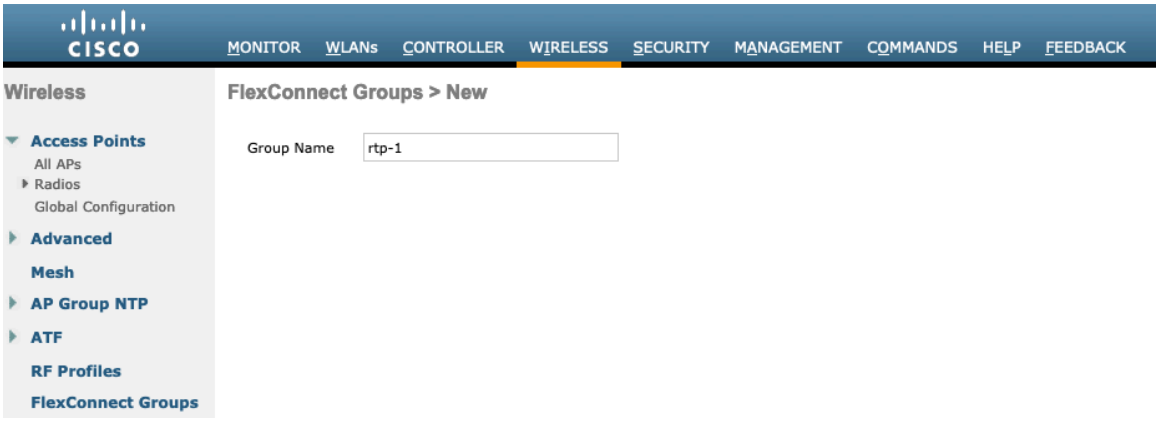
On the **High Density** tab, **Maximum Clients**, **Multicast Data Rates**, and **Rx Sop Threshold** can be configured. It is recommended to use the default value for **Rx Sop Threshold**.

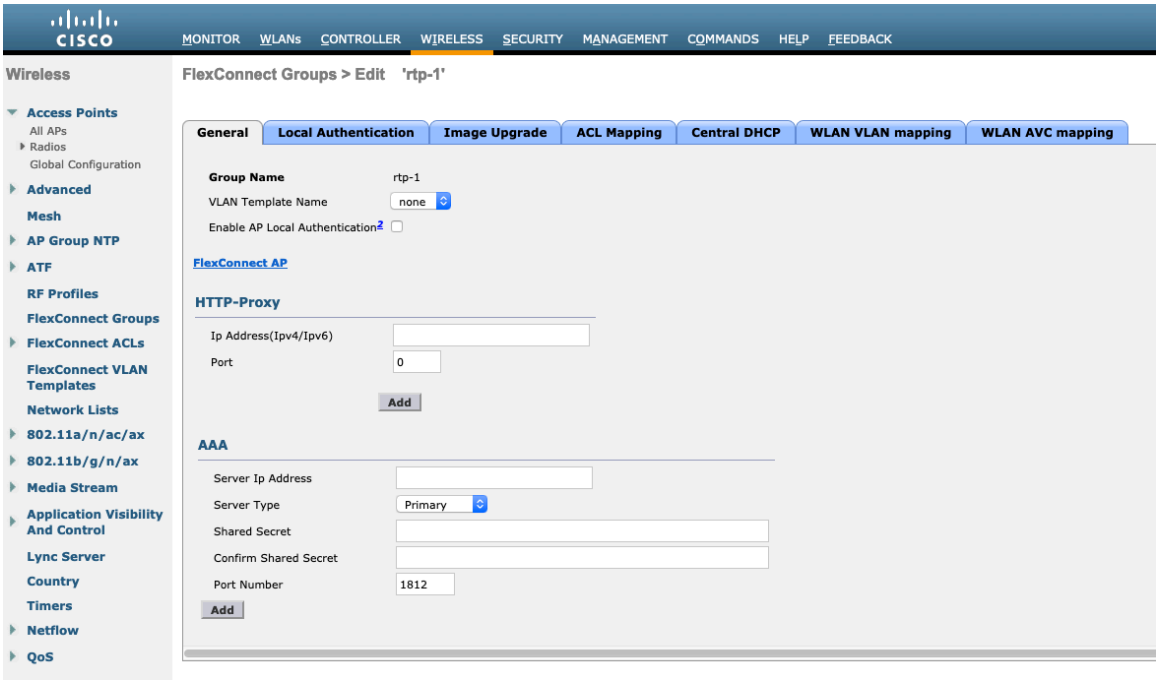


FlexConnect Groups

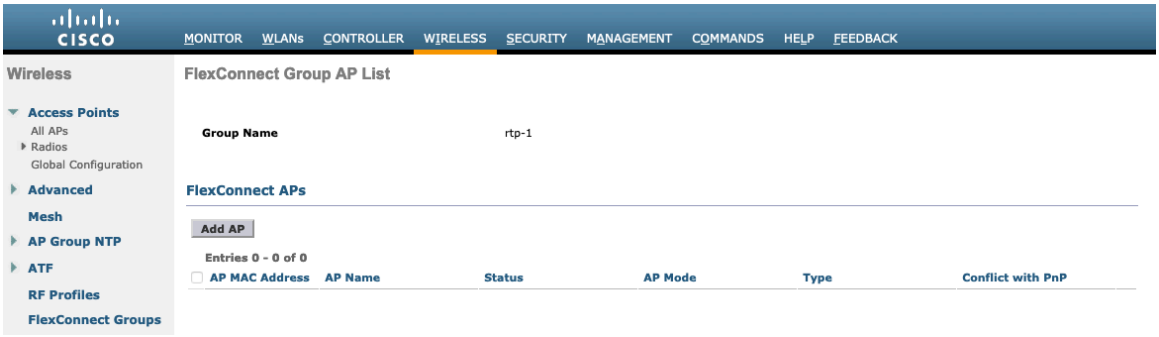
All access points configured for FlexConnect mode need to be added to a FlexConnect Group.

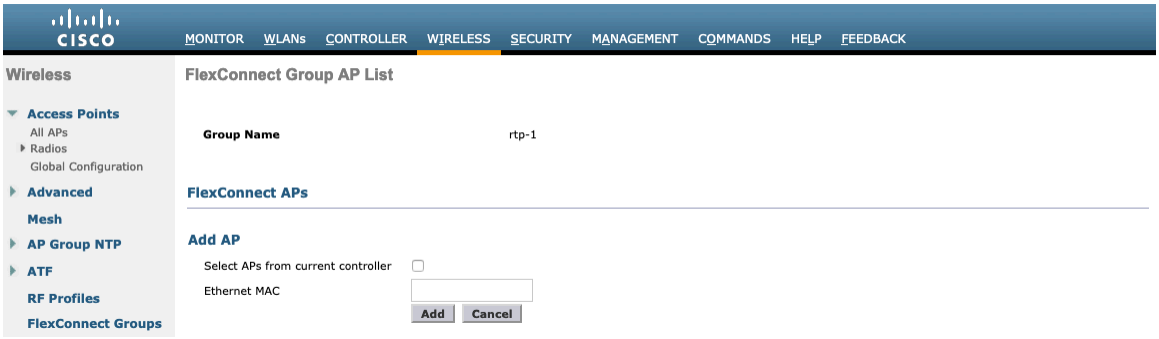
If utilizing 802.11r (FT) or CCKM, then seamless roams can only occur when roaming to access points within the same FlexConnect Group.





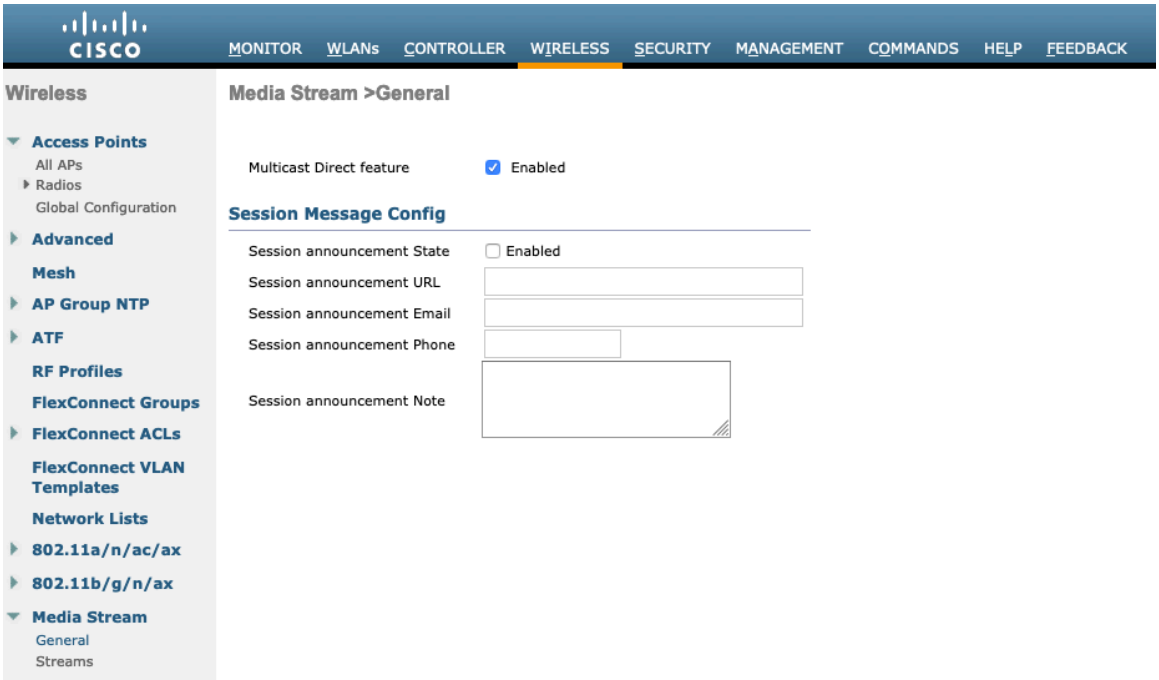
The maximum number of access points allowed per FlexConnect Group is limited, which is WLC model specific.



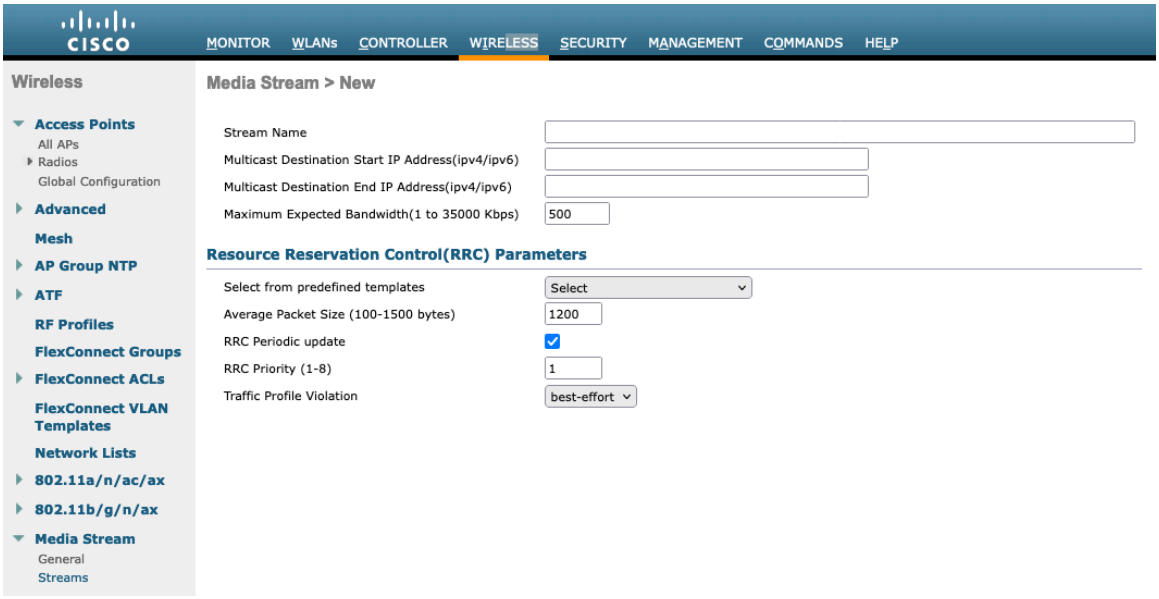


Multicast Direct

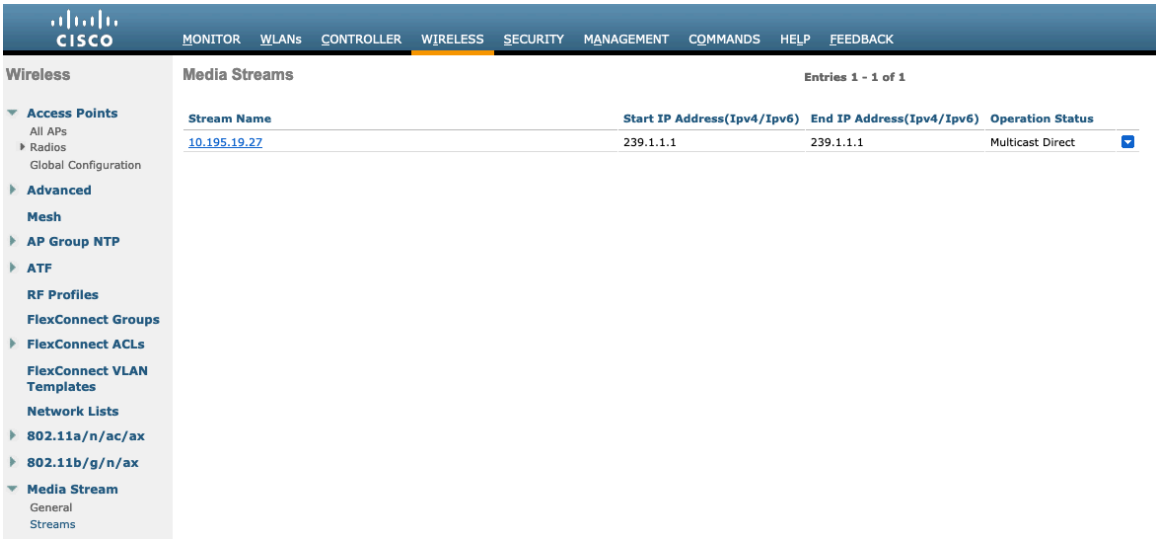
In the Media Stream settings, **Multicast Direct feature** should be enabled.



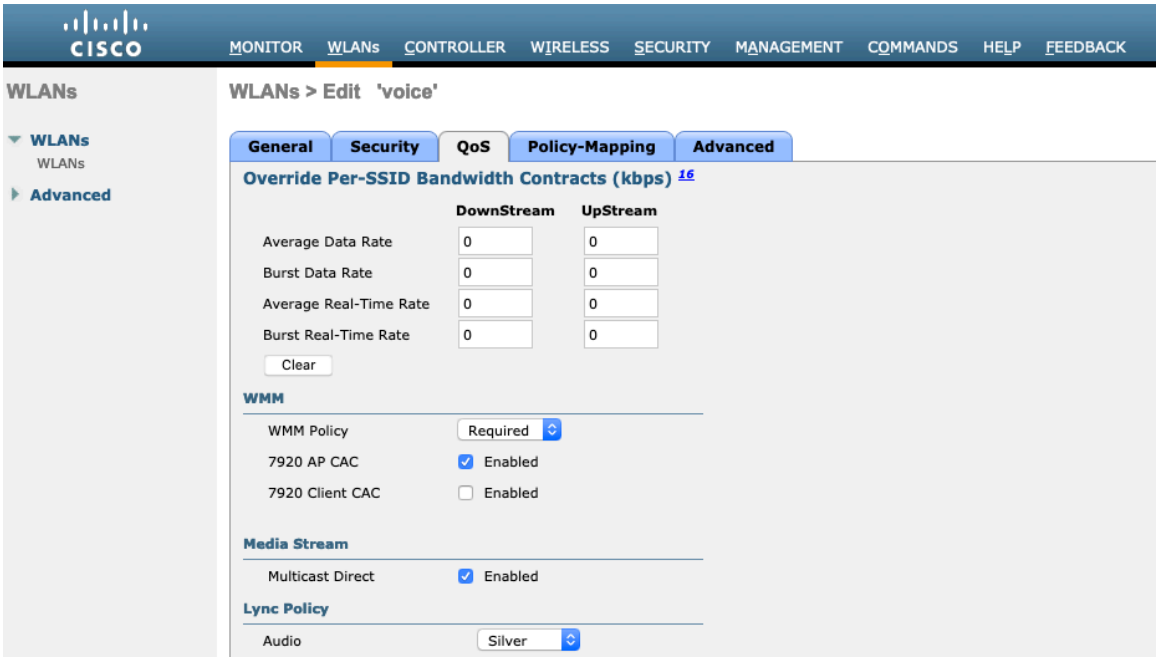
Then configure the media streams as necessary.



Once saved, then the media stream will be displayed.



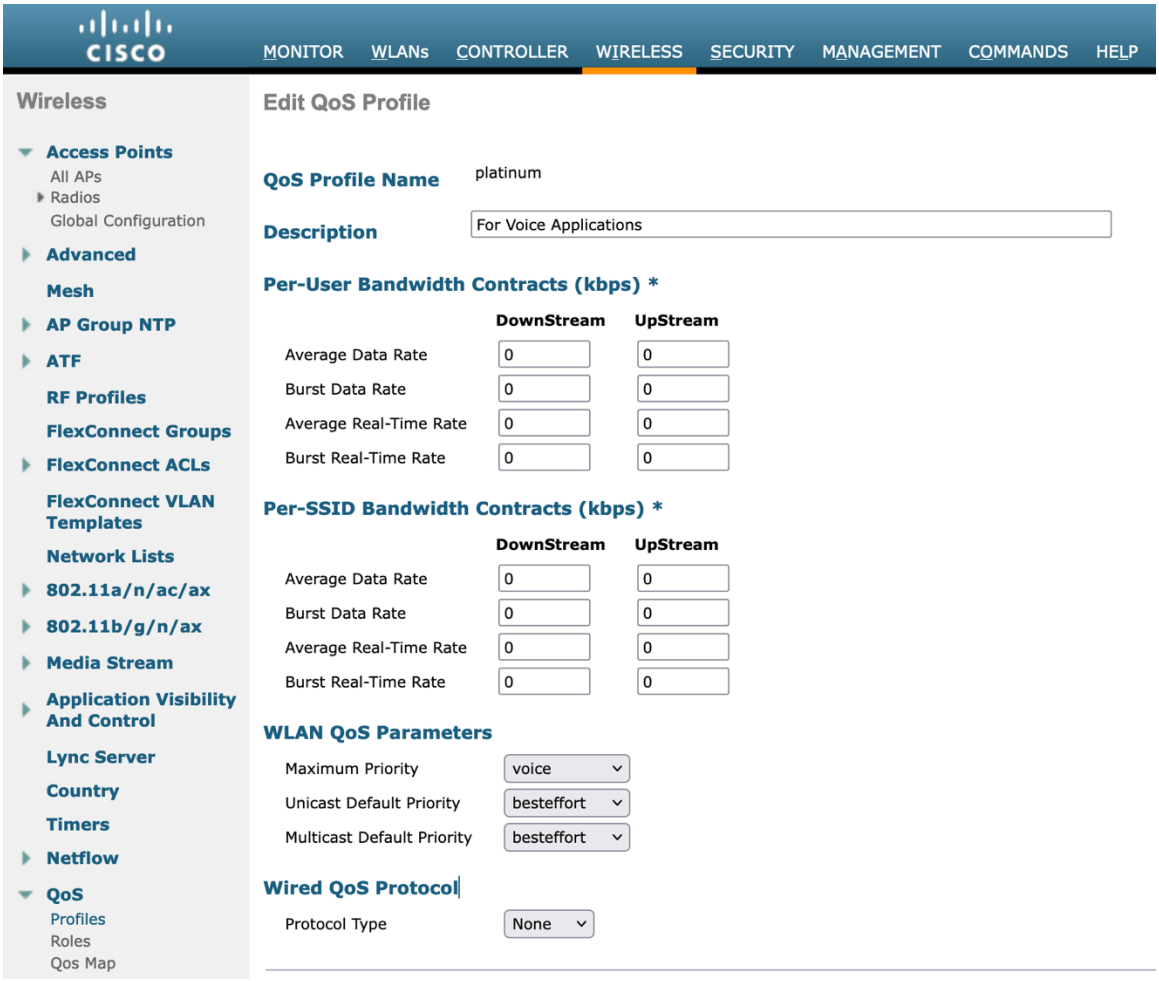
After **Multicast Direct feature** is enabled, then there will be an option to enable **Multicast Direct** in the QoS menu of the WLAN configuration.

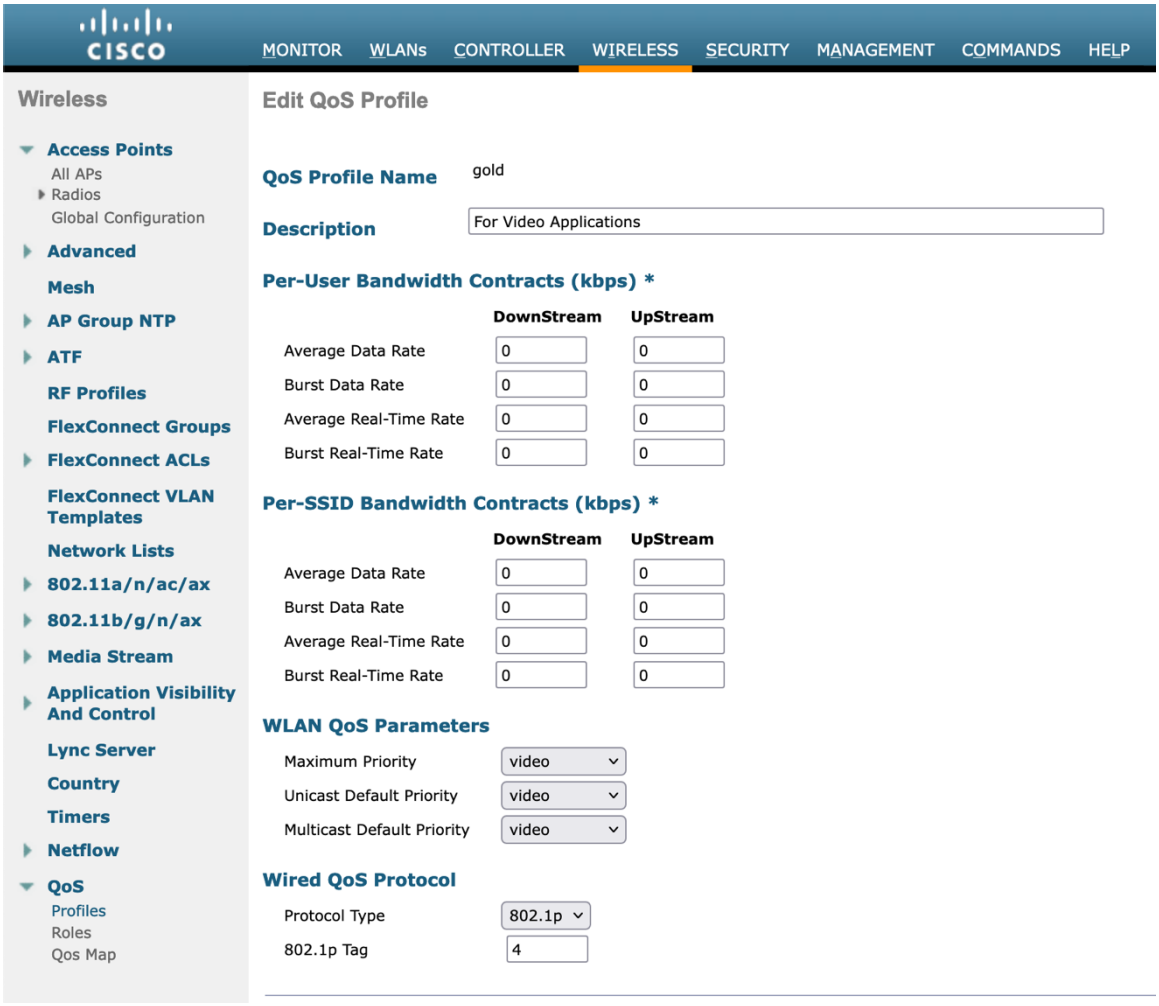


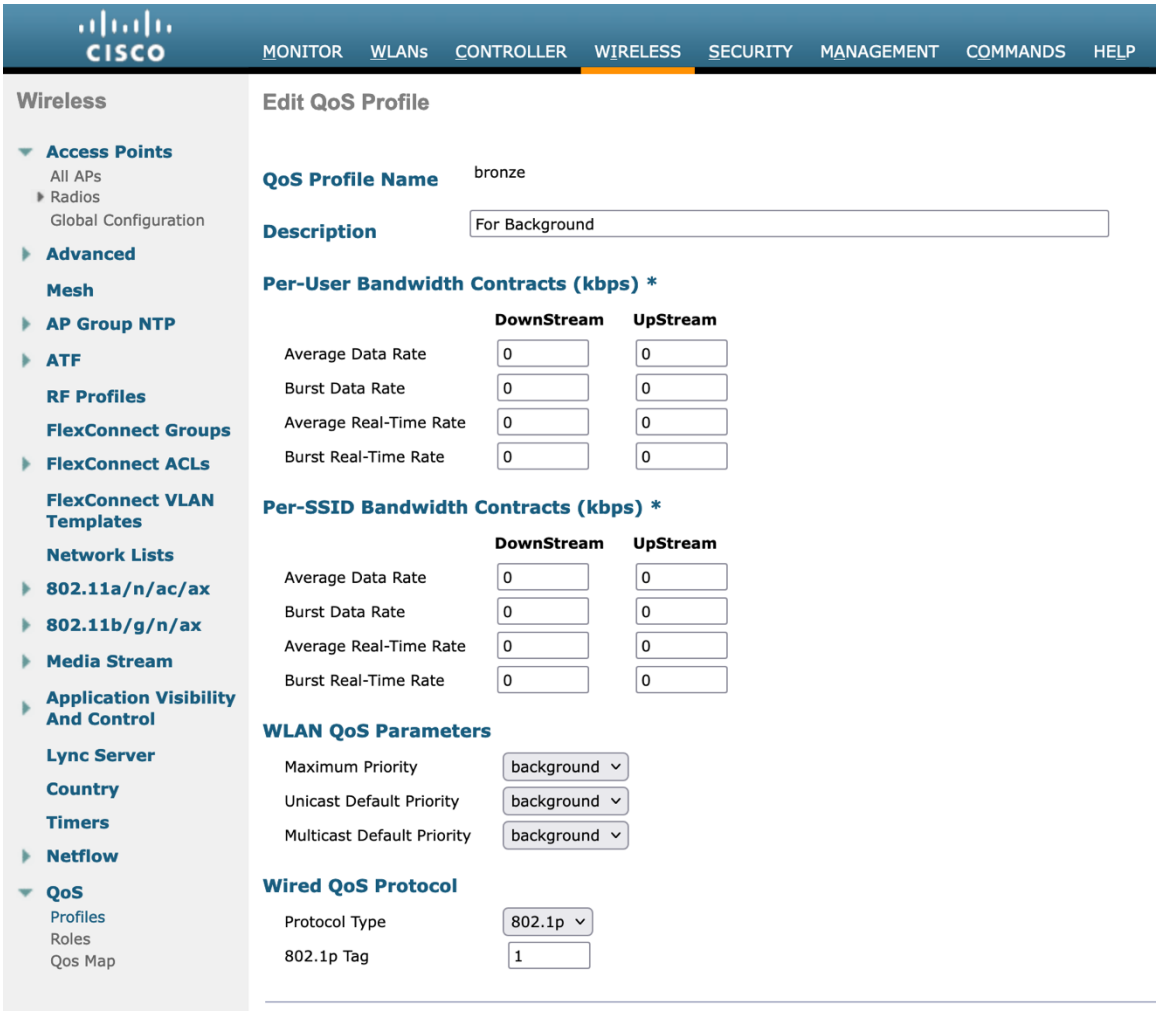
QoS Profiles

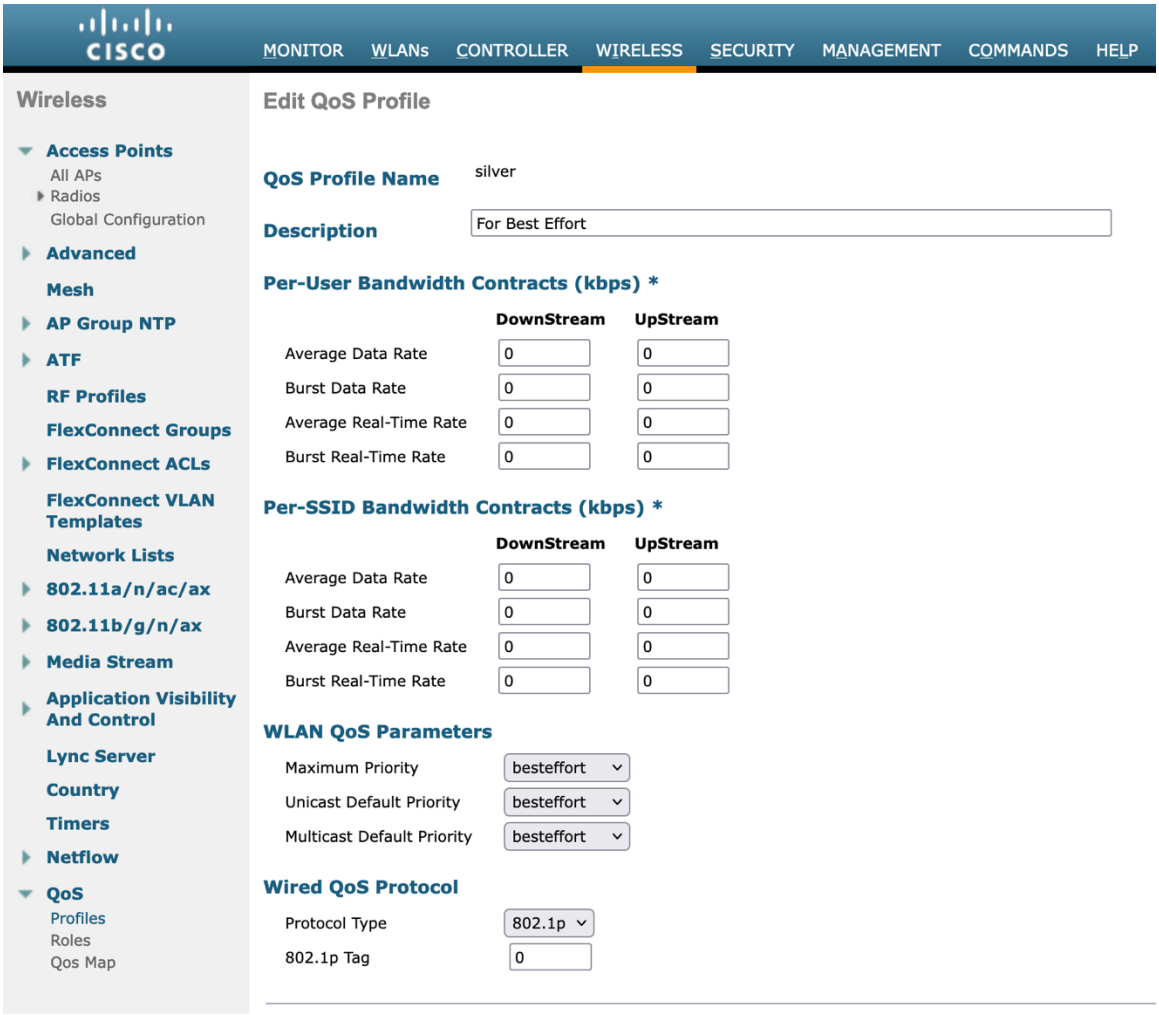
Configure the four QoS profiles per below.

QoS Profile	Protocol Type	802.1p Tag
Platinum	None	N/A
Gold	802.1p	4
Bronze	802.1p	1
Silver	802.1p	0


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless
Access Points
All APs
Radios
Global Configuration
Advanced
Mesh
AP Group NTP
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
Network Lists
802.11a/n/ac/ax
802.11b/g/n/ax
Media Stream
Application Visibility And Control
Lync Server
Country
Timers
Netflow
QoS
Profiles
Roles
Qos Map
Edit QoS Profile
QoS Profile Name
platinum
Description
For Voice Applications
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
voice
Unicast Default Priority
besteffort
Multicast Default Priority
besteffort
Wired QoS Protocol
Protocol Type
None


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless
Access Points
All APs
Radios
Global Configuration
Advanced
Mesh
AP Group NTP
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
Network Lists
802.11a/n/ac/ax
802.11b/g/n/ax
Media Stream
Application Visibility And Control
Lync Server
Country
Timers
Netflow
QoS
Profiles
Roles
Qos Map
Edit QoS Profile
QoS Profile Name
gold
Description
For Video Applications
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
Unicast Default Priority
Multicast Default Priority
video
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
4


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless
Access Points
All APs
Radios
Global Configuration
Advanced
Mesh
AP Group NTP
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
Network Lists
802.11a/n/ac/ax
802.11b/g/n/ax
Media Stream
Application Visibility And Control
Lync Server
Country
Timers
Netflow
QoS
Profiles
Roles
Qos Map
Edit QoS Profile
QoS Profile Name
bronze
Description
For Background
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
Unicast Default Priority
Multicast Default Priority
background
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
1

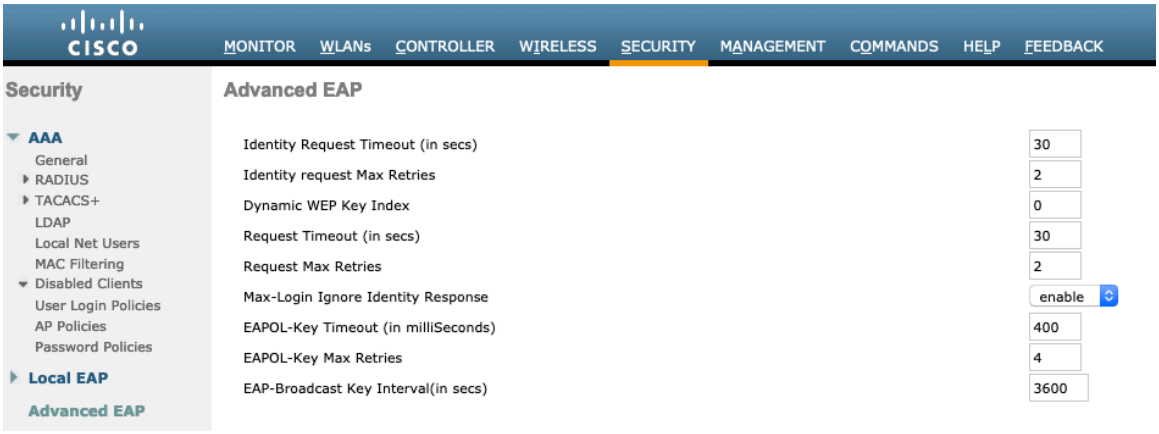


Advanced Settings

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, the **EAP-Request Timeout** on the Cisco Wireless LAN Controller should be set to at least 20 seconds.

In later versions of Cisco Wireless LAN Controller software, the default **EAP-Request Timeout** was changed from 2 to 30 seconds.

For deployments where EAP failures occur frequently, the **EAP-Request Timeout** should be reduced below 30 seconds.

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

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

If using PSK then it is recommended to reduce the **EAPOL-Key Timeout** to 400 milliseconds from the default of 1000 milliseconds with **EAPOL-Key Max Retries** set to 4 from the default of 2.

If using 802.1x, then using the default values where the **EAPOL-Key Timeout** is set to 1000 milliseconds and **EAPOL-Key Max Retries** are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.

The **EAPOL-Key Timeout** should not exceed 1000 milliseconds (1 second).

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

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

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

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

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

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

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

Auto-Immune

The Auto-Immune feature can optionally be enabled for protection against denial of service (DoS) attacks.

Although when this feature is enabled there can be interruptions introduced with voice over wireless LAN, therefore it is recommended to disable the Auto-Immune feature on the Cisco Wireless LAN Controller.

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

```
(Cisco Controller) >show wps summary

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

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

Signature Policy
  Signature Processing…..... Enabled
```

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

```
(Cisco Controller) >config wps auto-immune disable
```

CCKM Timestamp Tolerance

The default CCKM timestamp tolerance is set to 1000 ms.

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

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

Use the following command to configure the CCKM timestamp tolerance per Cisco recommendations.

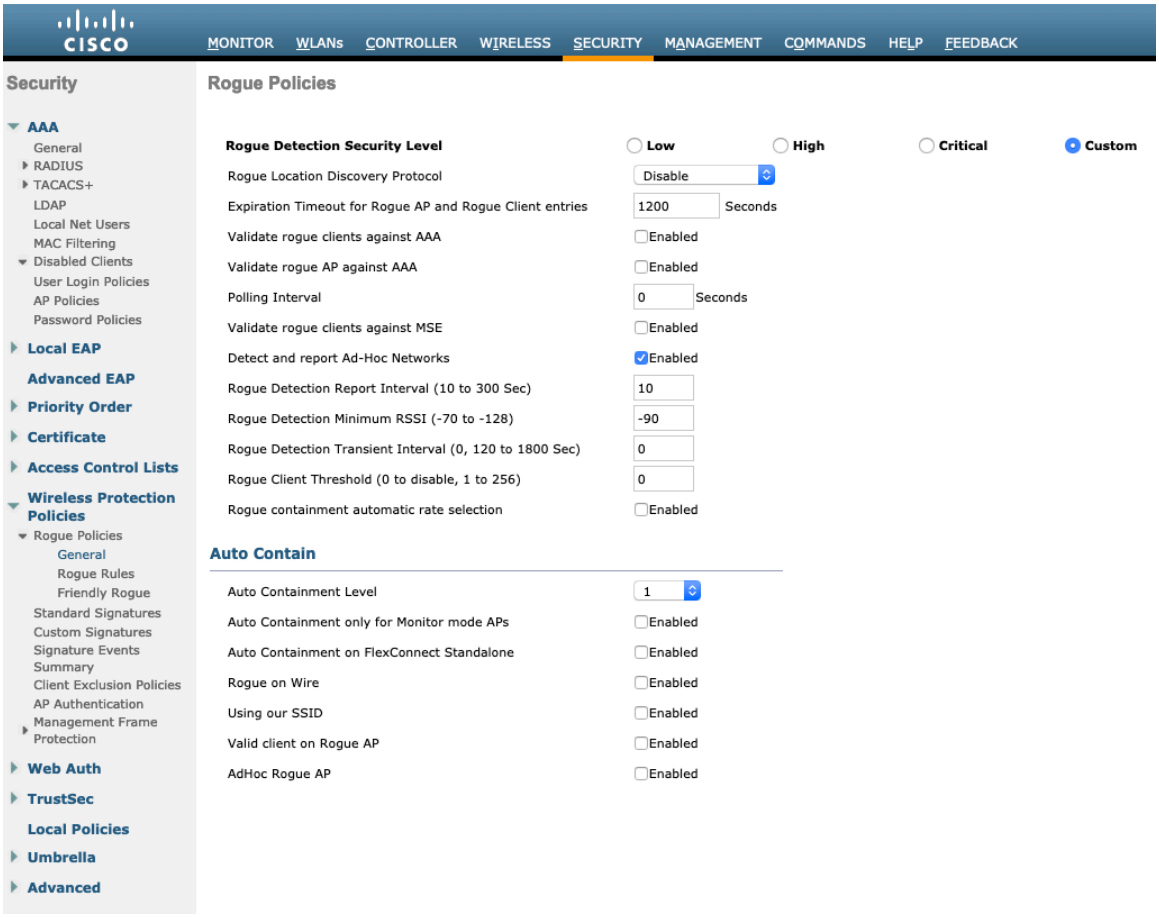
```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id >
```

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

```
CCKM tsf Tolerance…..... 5000
```

Rogue Policies

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



Cisco Catalyst IOS XE Wireless LAN Controller and Lightweight Access Points

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

- Ensure **802.11r (FT)** or **CCKM** is **Enabled**
- Set **Quality of Service (QoS) SSID Policy** to **Platinum**
- Set the **WMM Policy** to **Required**
- Recommended to set **802.11k** to **Enabled**
- Recommended to set **802.11v** to **Enabled**
- 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

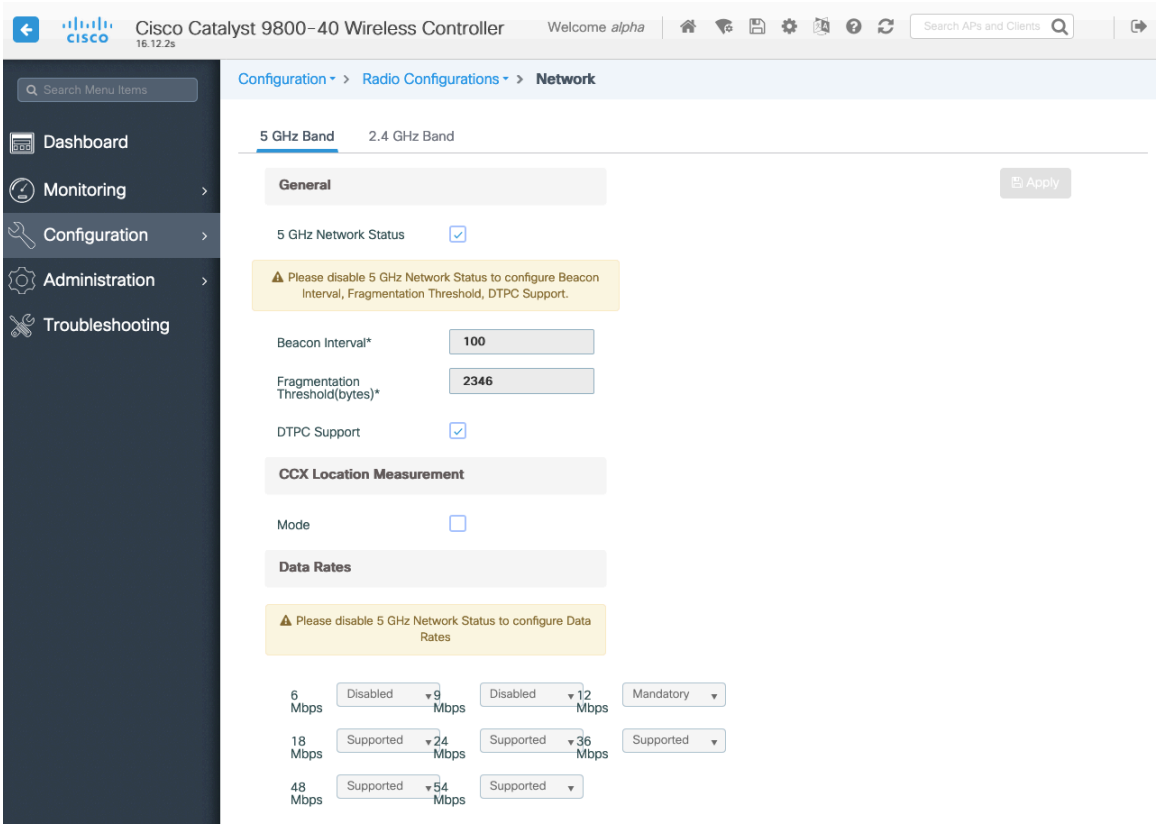
It is recommended to have the Cisco Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

If wanting to use 5 GHz, ensure the 5 GHz network status is **Enabled**.

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

Ensure **DTPC Support** is enabled.

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



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

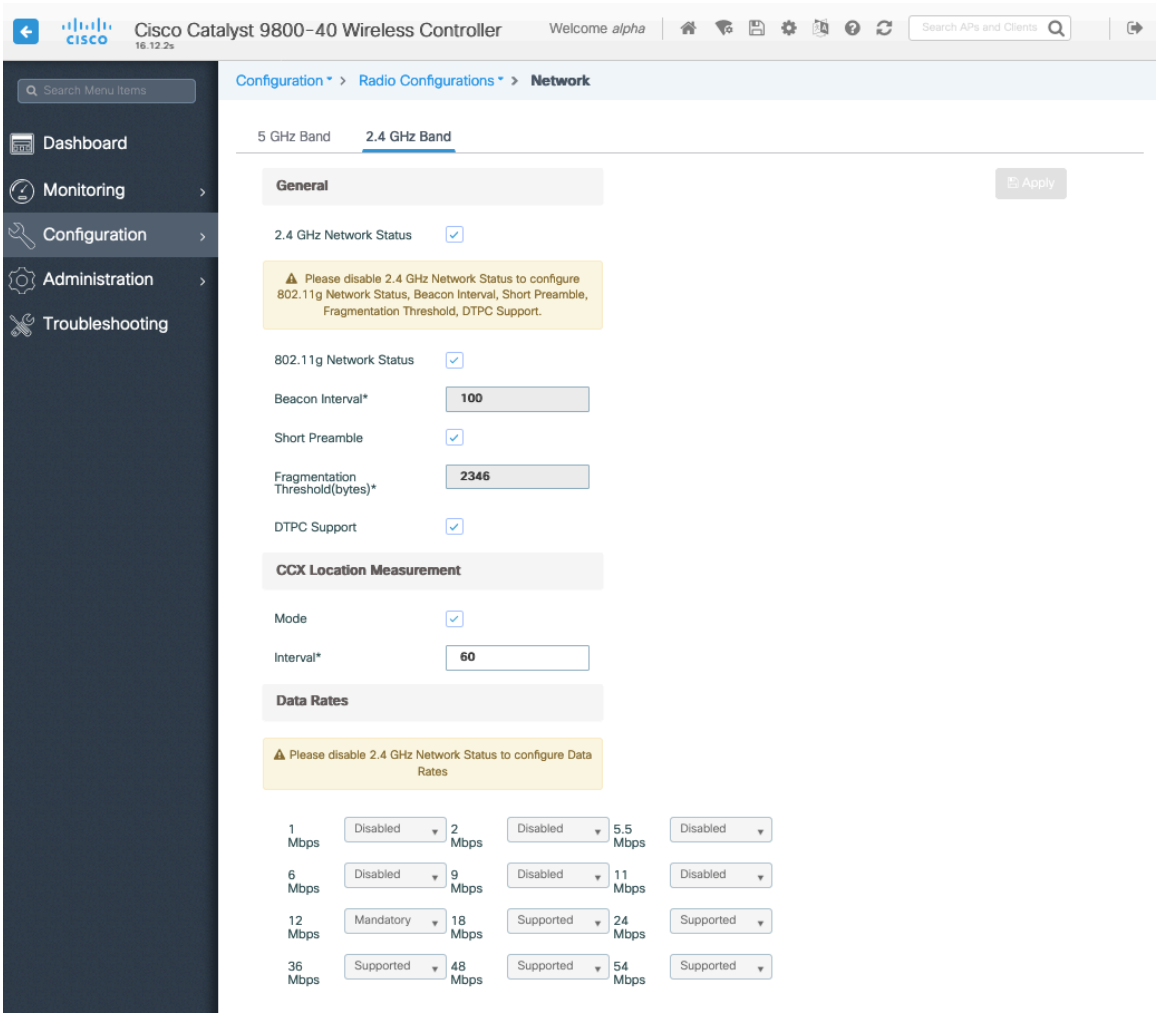
Set the **Beacon Period** to **100 ms**.

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

Ensure **DTPC Support** is enabled.

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

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



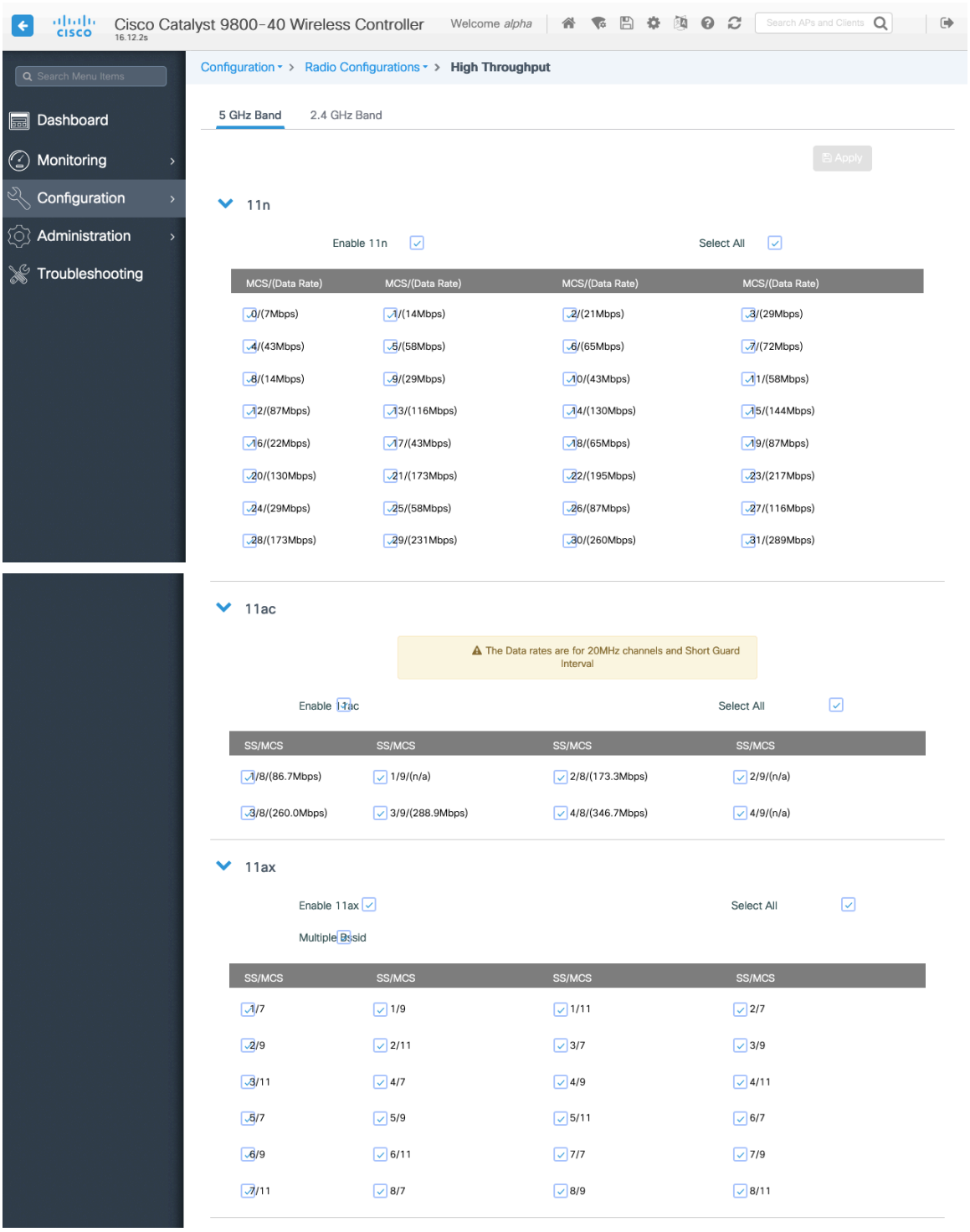
High Throughput (802.11n/ac)

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

802.11ac data rates are applicable to 5 GHz only.

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

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



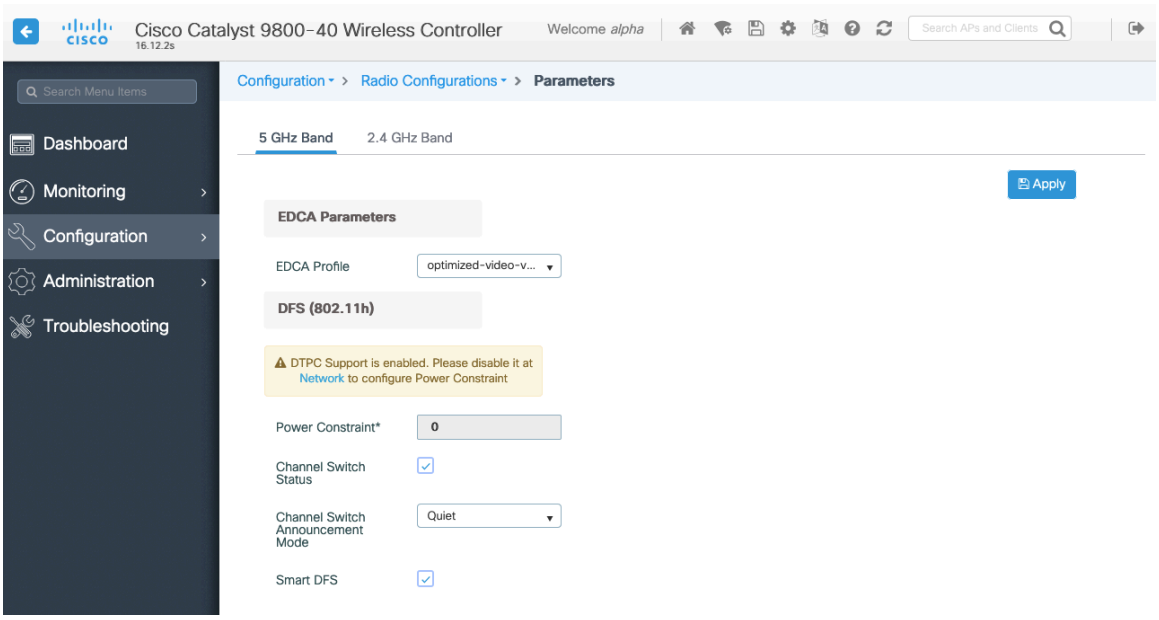
Parameters

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

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

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

Channel Switch Announcement Mode should be set to **Quiet**.

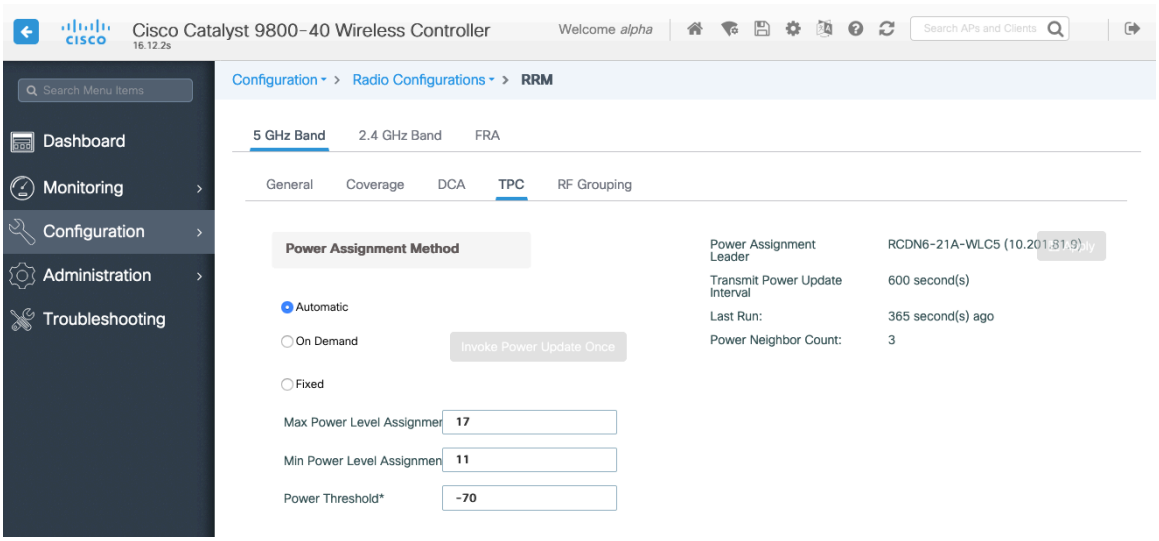


RRM

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

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

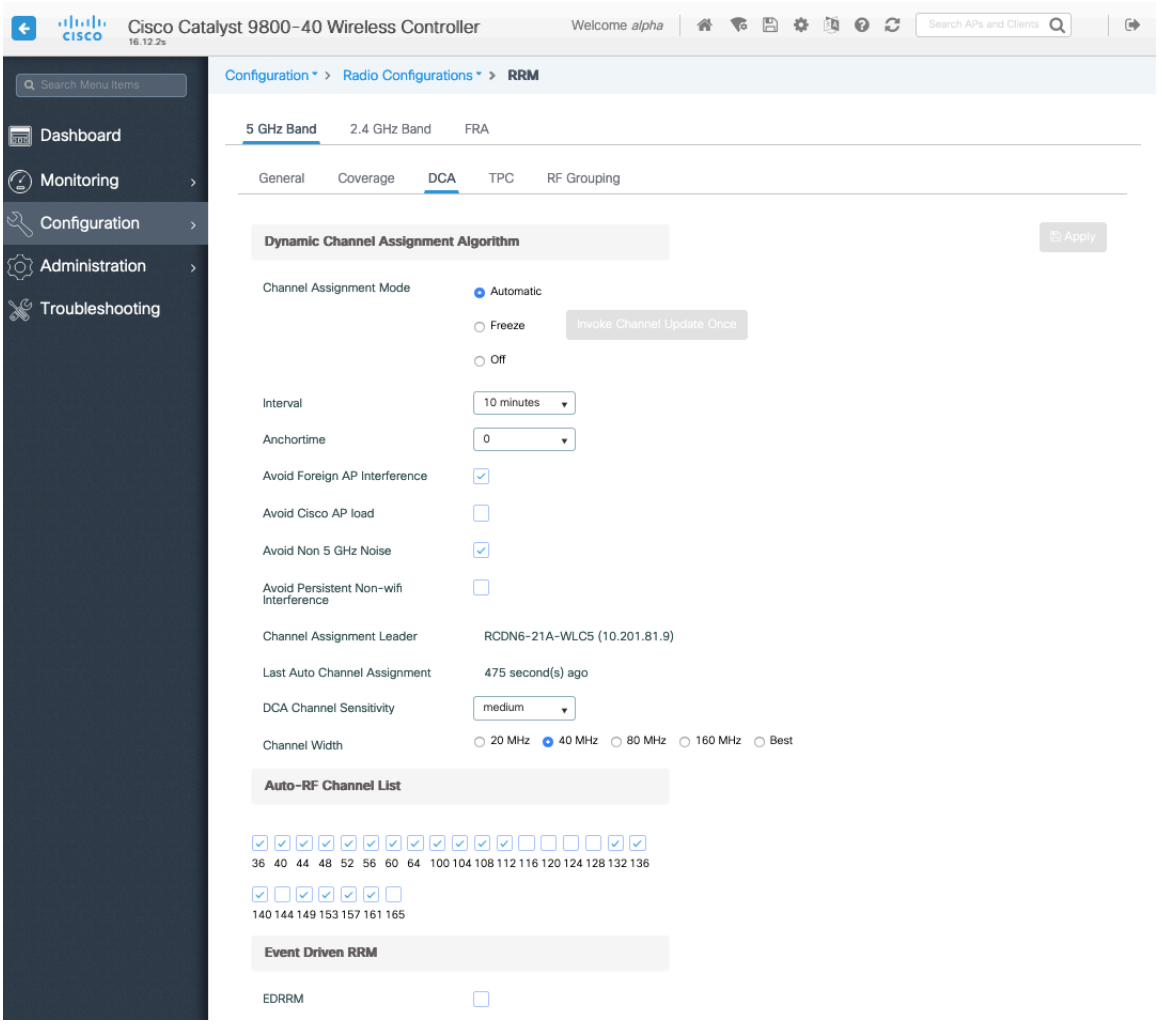
If using automatic power level assignment, a maximum and minimum power level can be specified.



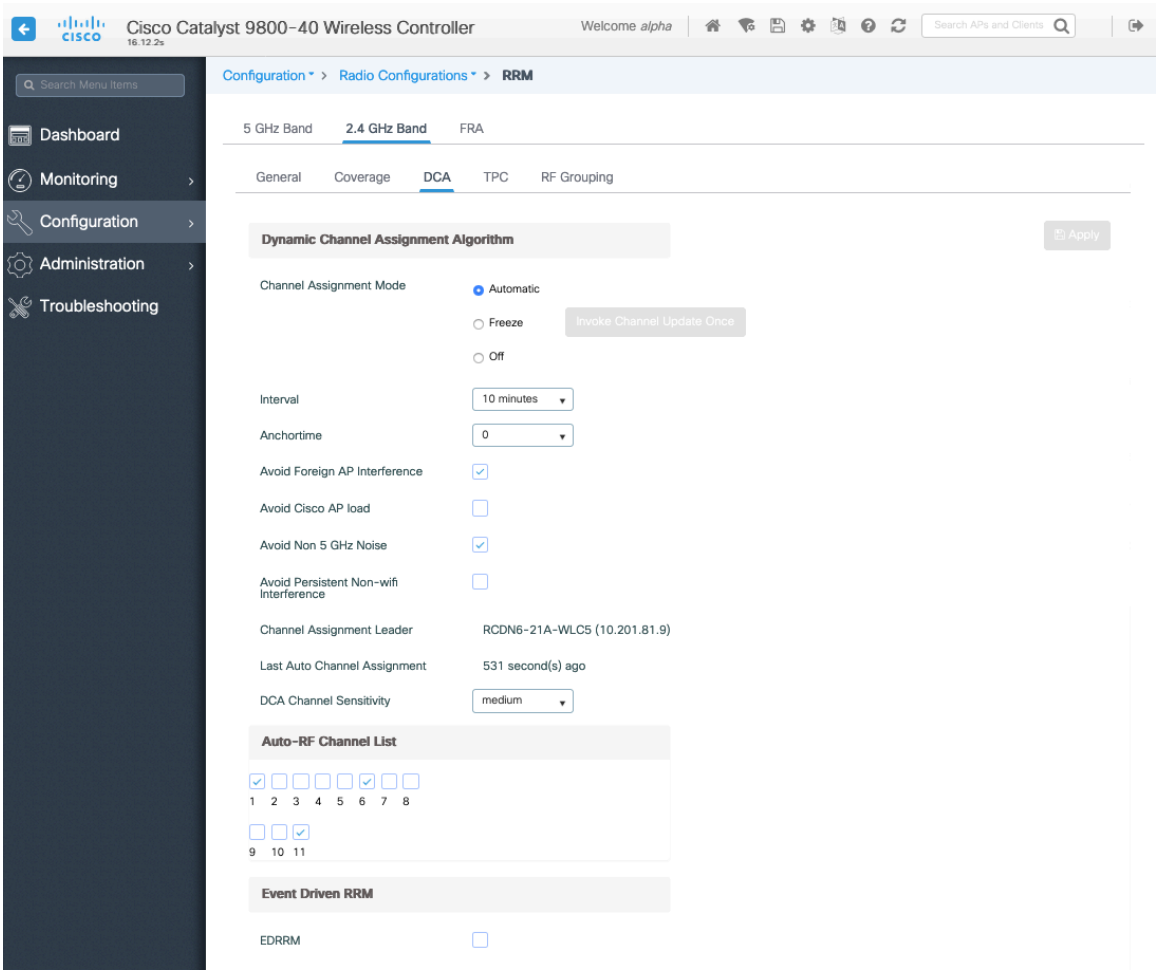
If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.

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

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



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



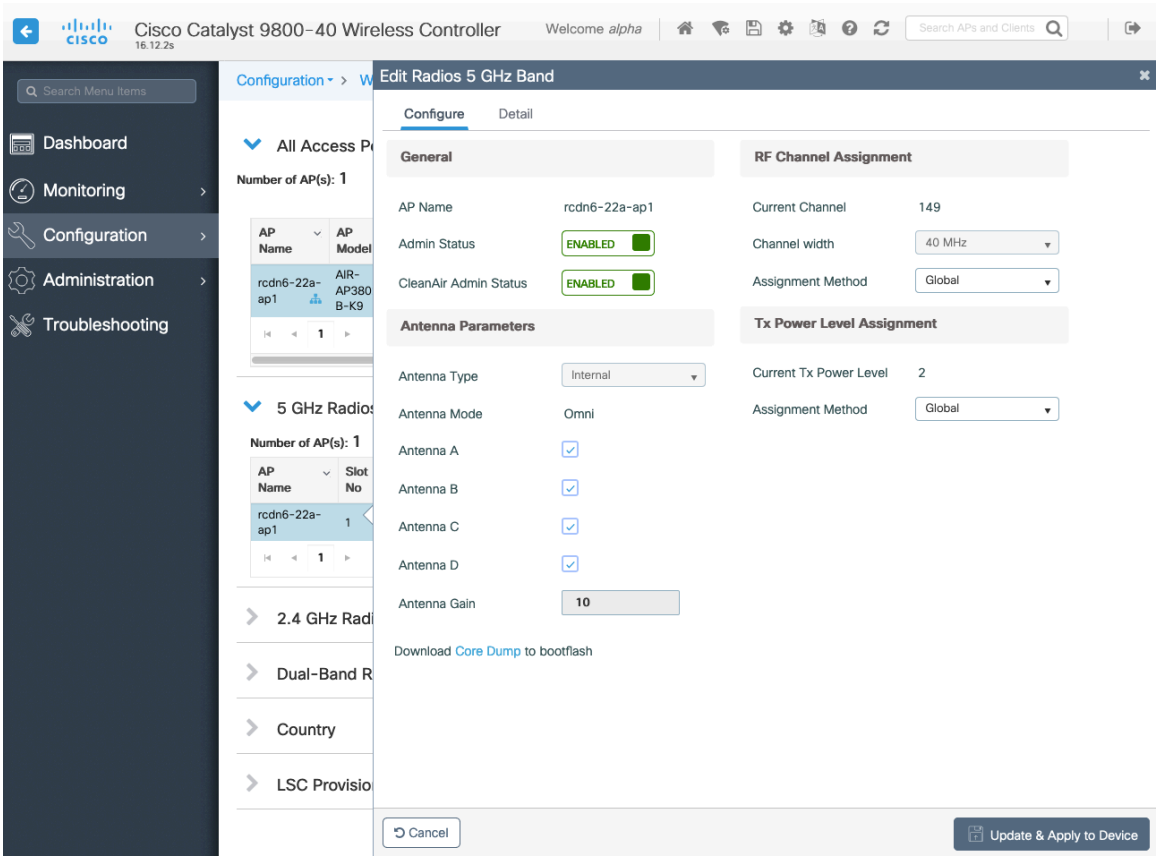
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

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

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

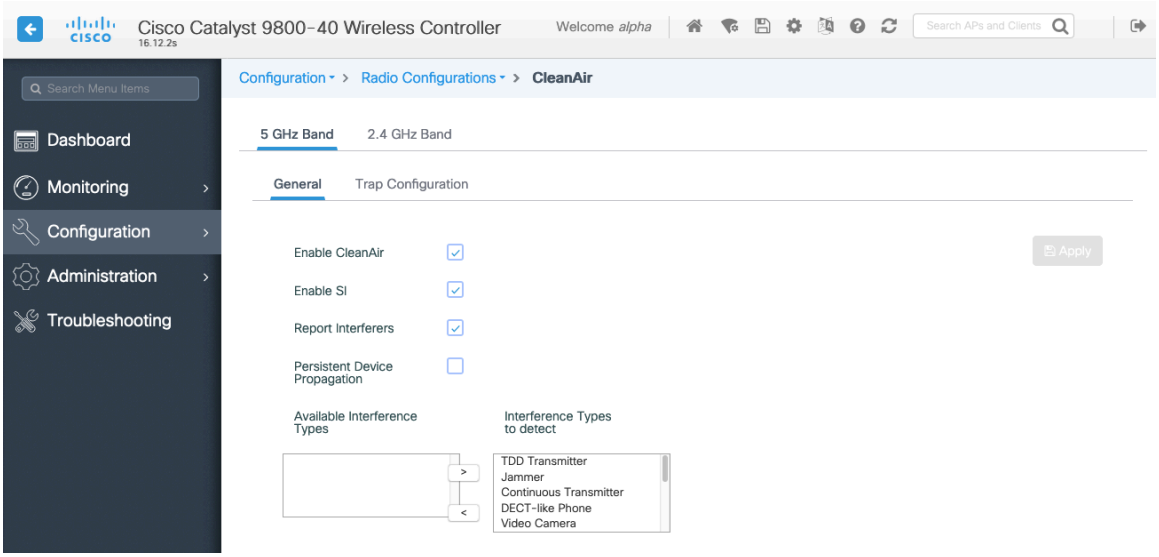
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

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



CleanAir

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



WLAN Settings

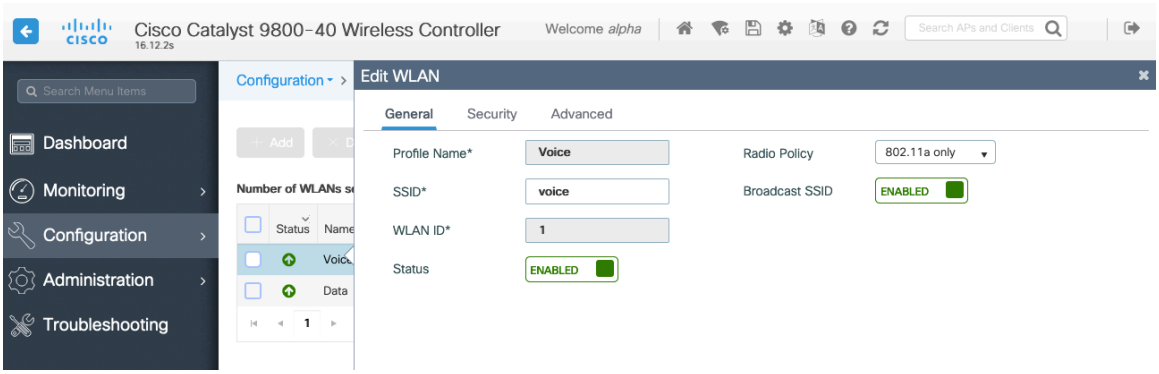
It is recommended to have a separate SSID for the Cisco Wireless Phone 840 and 860.

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

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

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

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

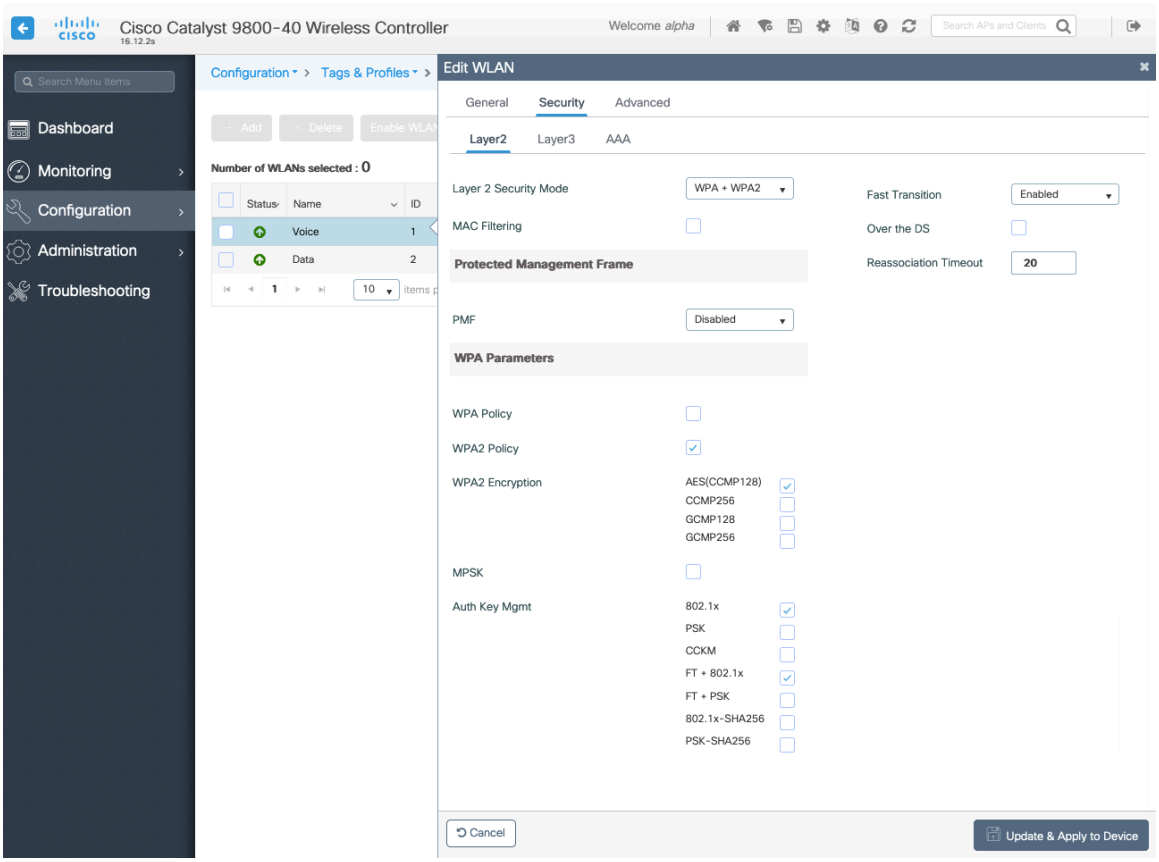


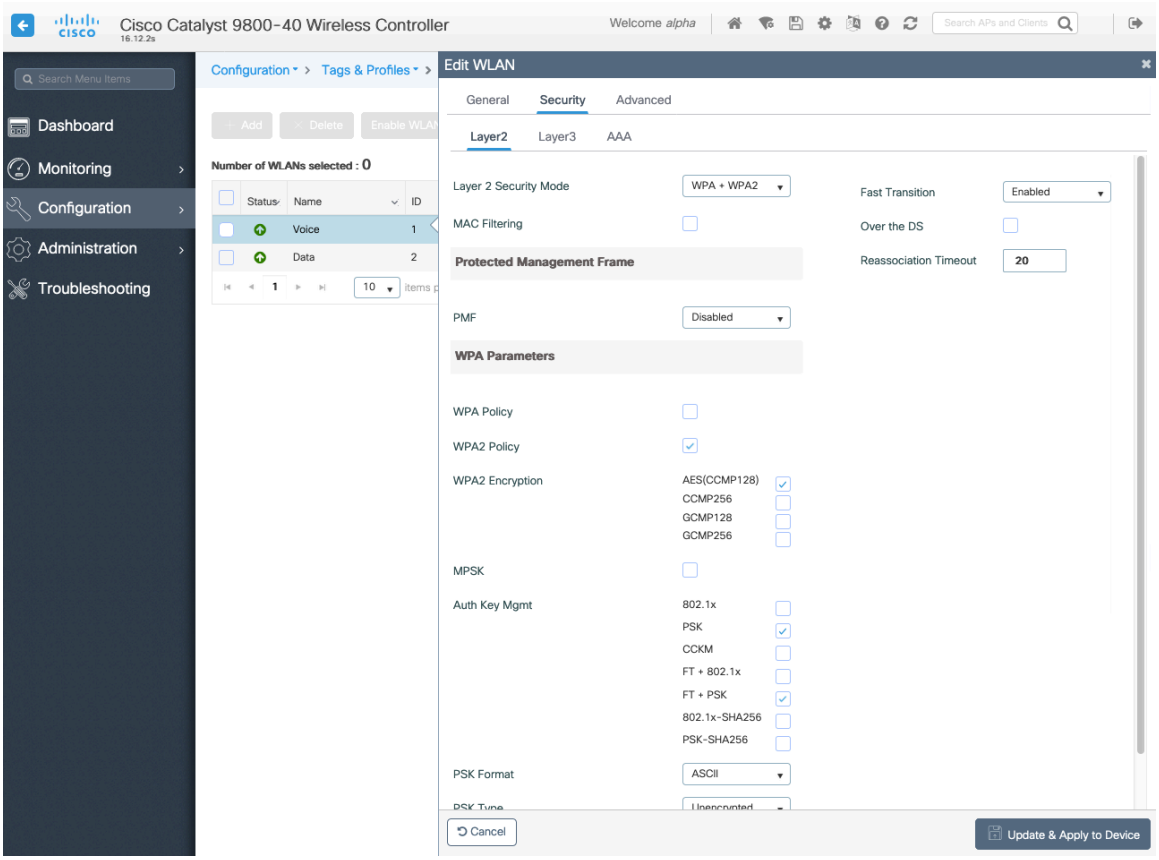
To utilize 802.11r (FT) for fast secure roaming, set **Fast Transition** to **Enabled**.

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

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

Enable WPA2 policy with AES(CCMP128) encryption then either FT 802.1x or FT PSK for authenticated key management type depending on whether 802.1x or PSK is to be utilized.


Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles >
Add
Delete
Enable WLAN
Number of WLANs selected : 0
Status
Name
ID
Voice
1
Data
2
10
items p
Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
MPSK
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
Fast Transition
Enabled
Over the DS
Reassociation Timeout
20
Cancel
Update & Apply to Device

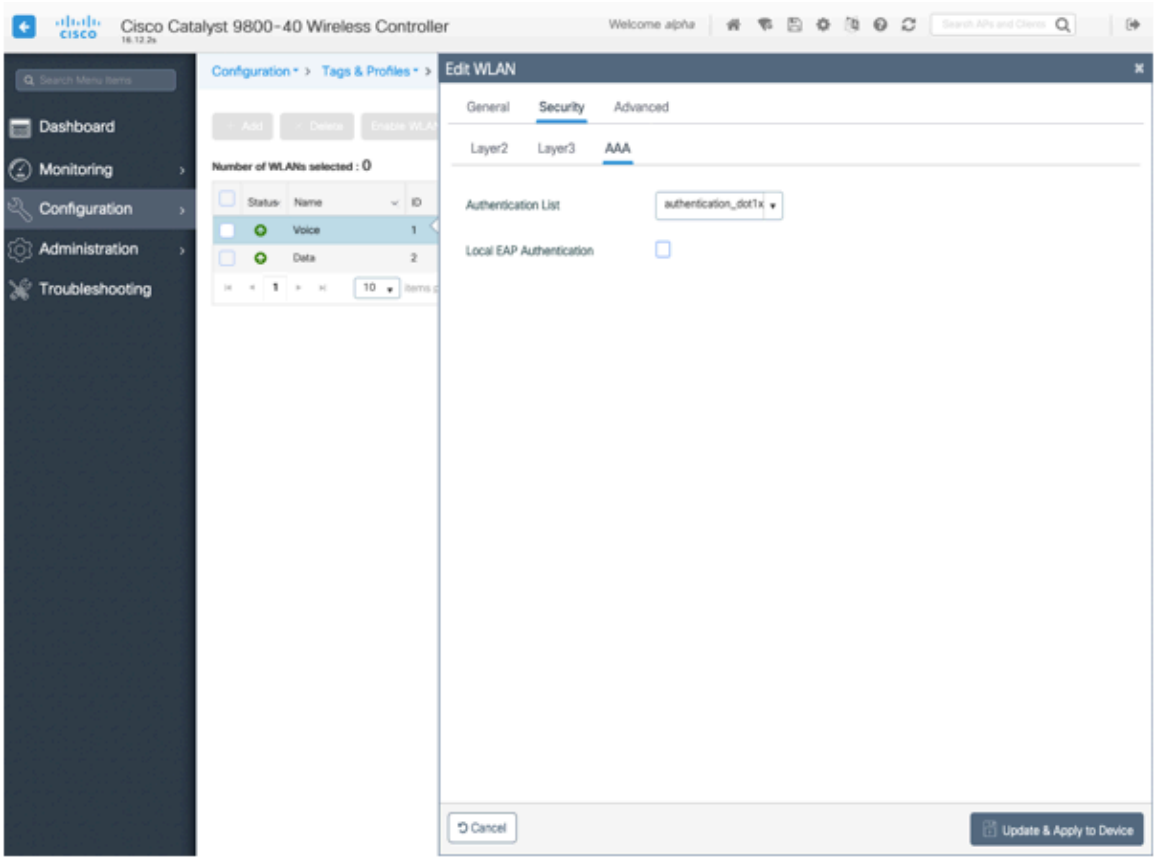

Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles >
Add
Delete
Enable WLAN
Number of WLANs selected : 0
Status
Name
ID
Voice
1
Data
2
10
items p
Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
MPSK
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
PSK Format
ASCII
Fast Transition
Enabled
Over the DS
Reassociation Timeout
20
Cancel
Update & Apply to Device

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 Wireless Phone 840 and 860 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 Wireless Phone 840 and 860 or other WMM enabled phones will be using this SSID.

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

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

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

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

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

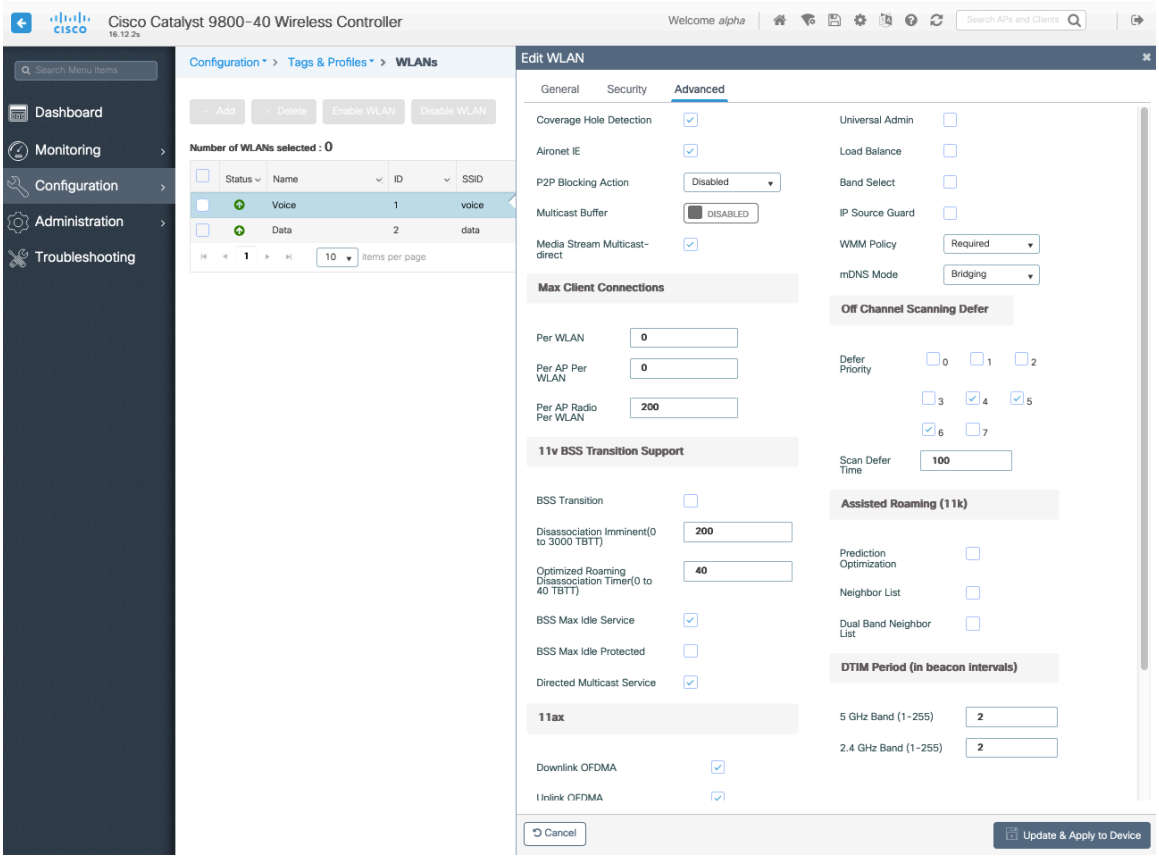
If using best effort applications frequently or if DSCP values for priority applications (e.g. voice and call control) are not preserved to the access point, then is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well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

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**.

It is recommend to enable 802.11k and 802.11v.

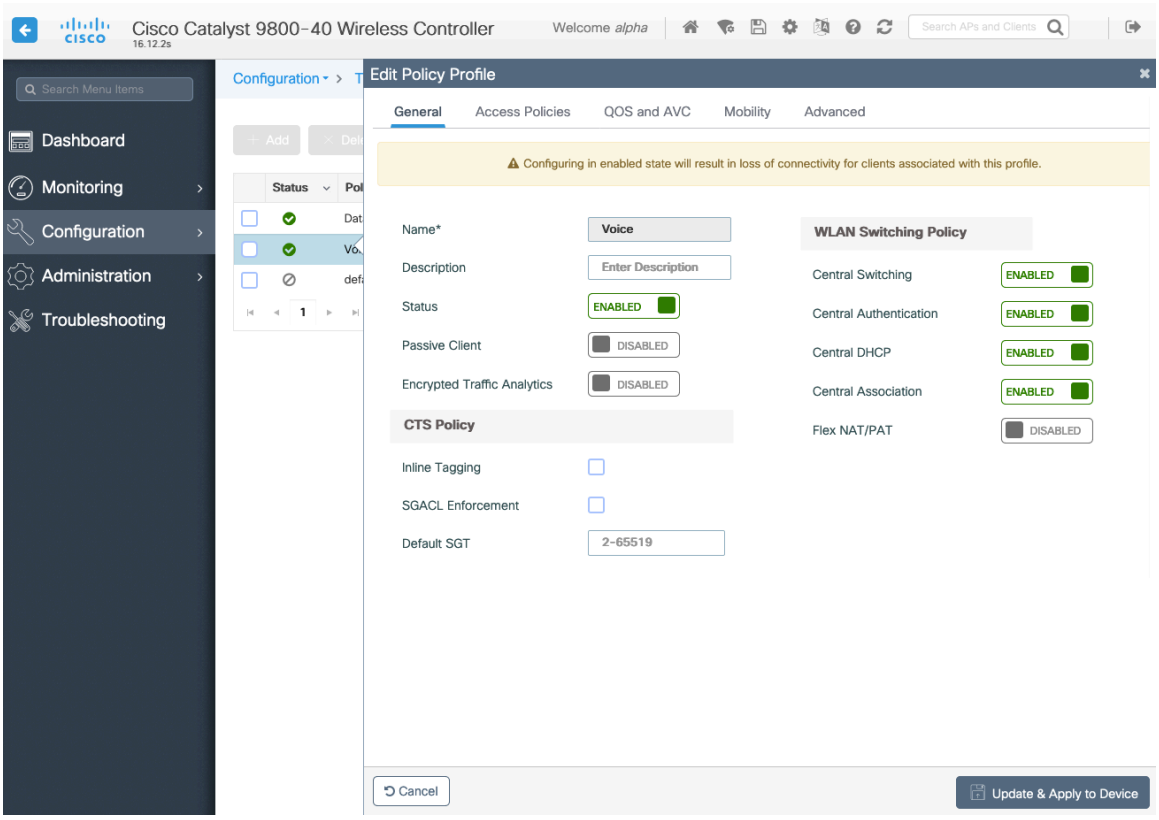


Policy Profiles

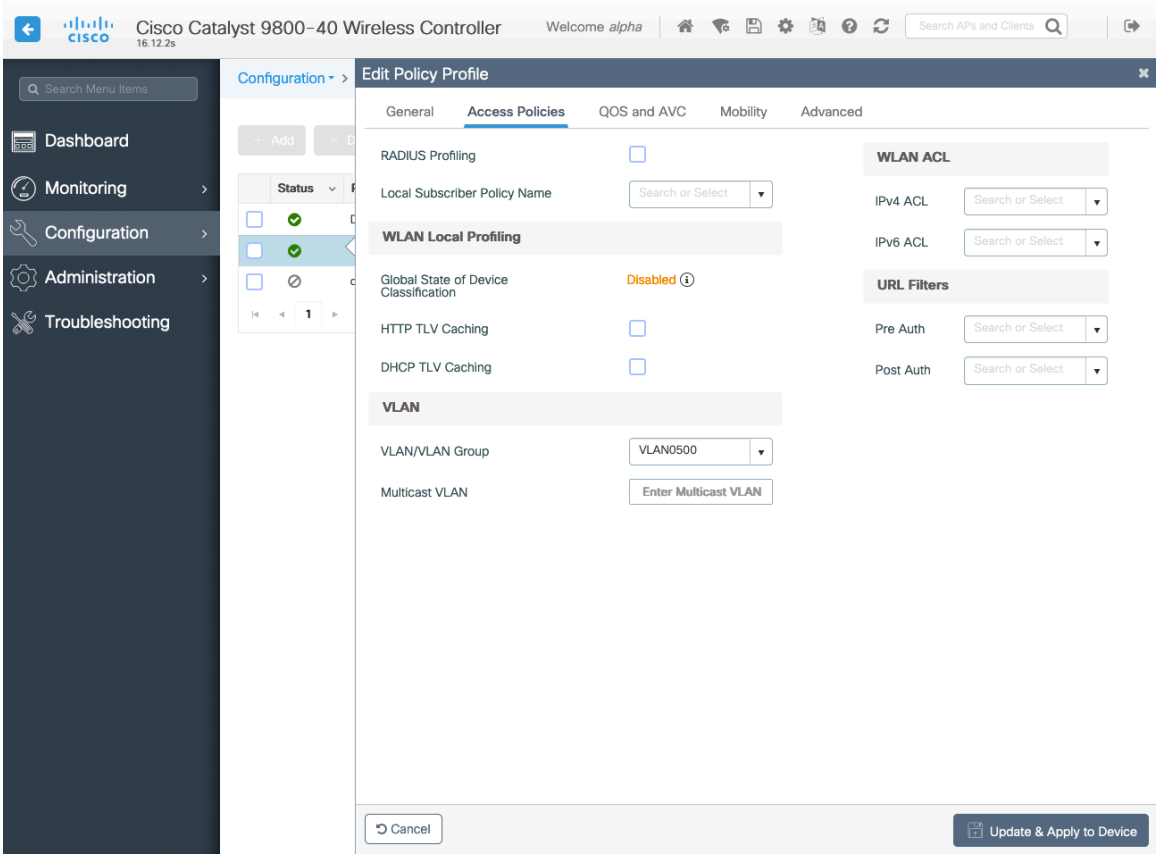
Policy Profiles are used to define additional settings regarding access, QoS, Mobility, and advanced settings.

Policy Profiles are then mapped to a WLAN Profile via a Policy Tag, which then can be applied to an access point.

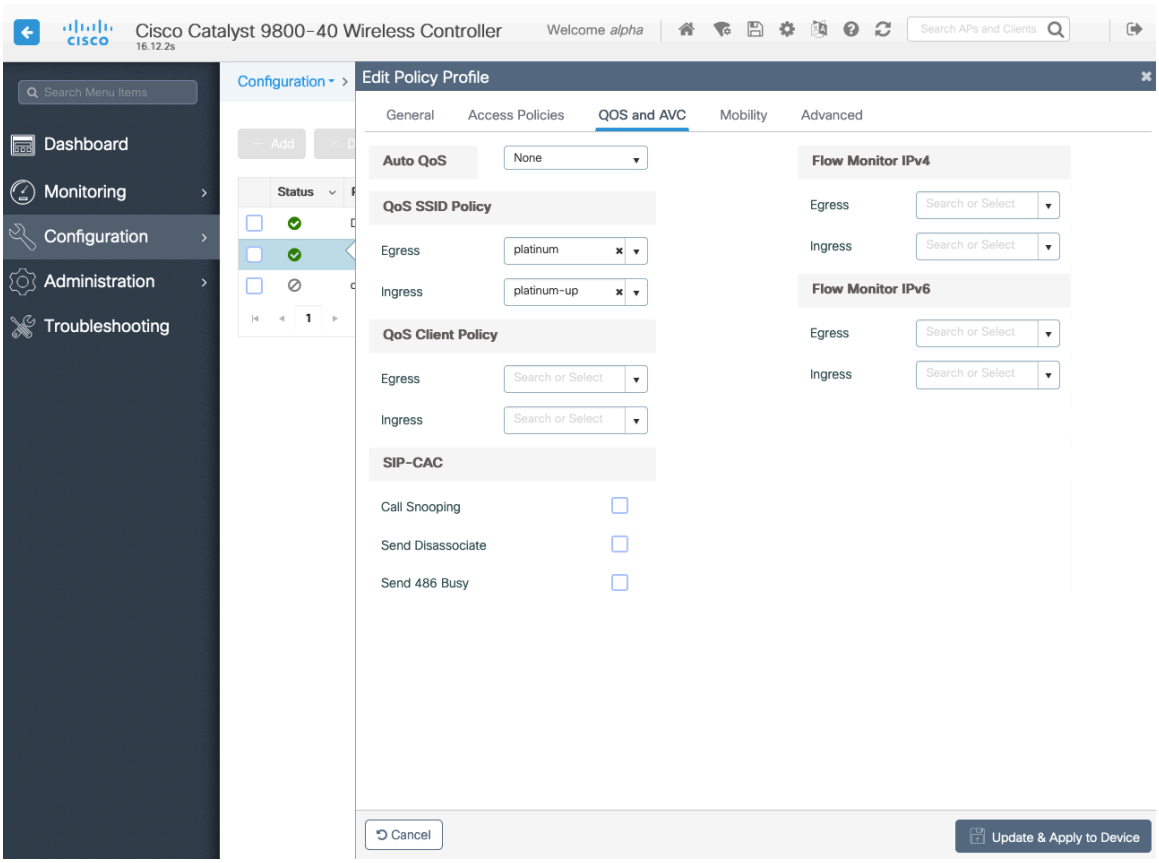
Ensure the **Status** of the policy profile is **Enabled**.



Select the **VLAN** or **VLAN Group** to be utilized with the policy profile.



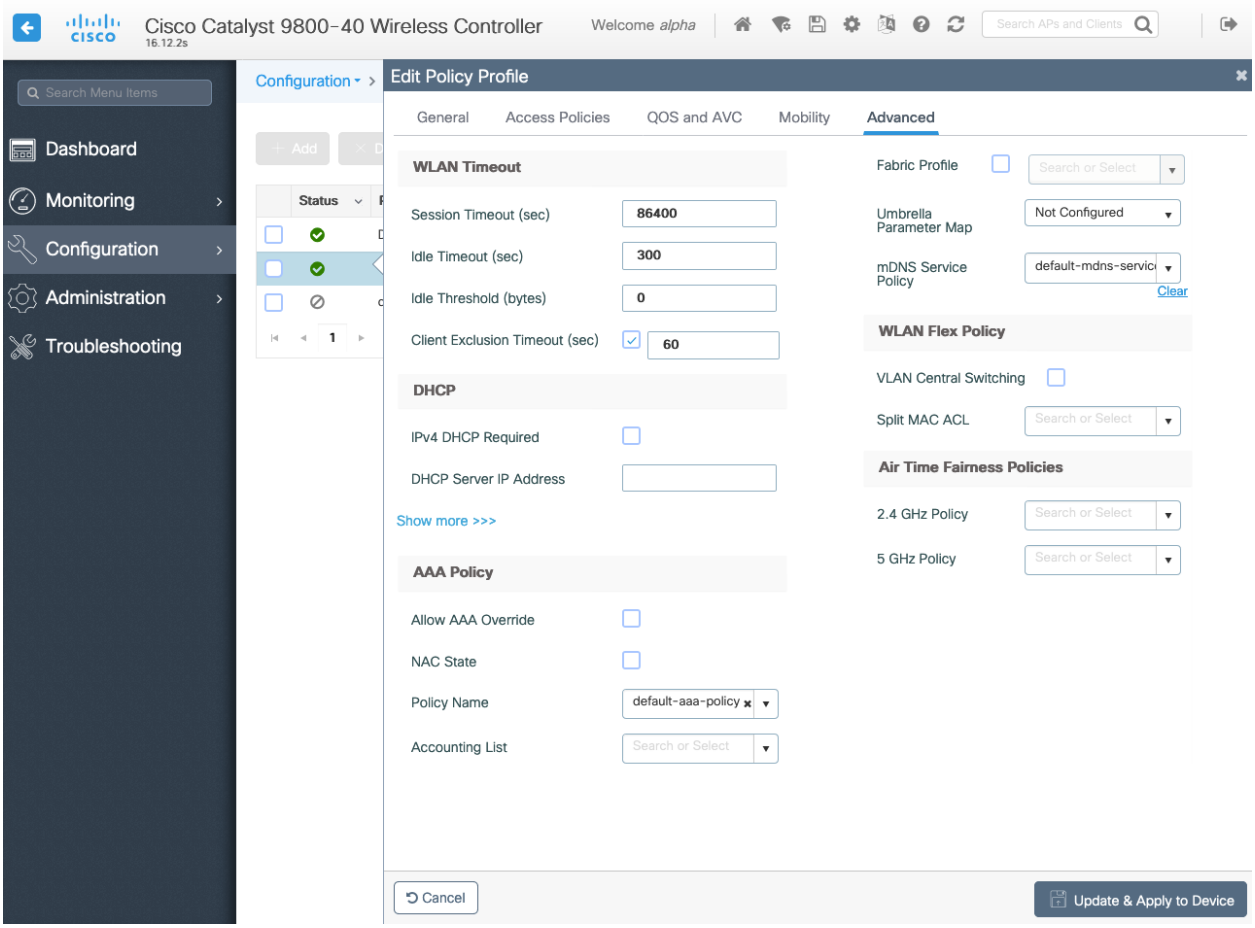
Ensure the QoS SSID Policy is set to **Platinum** for egress and **Platinum-up** for ingress.



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

Configure **Client Exclusion Timeout** as necessary.

IPv4 DHCP Required should be disabled.



RF Profiles

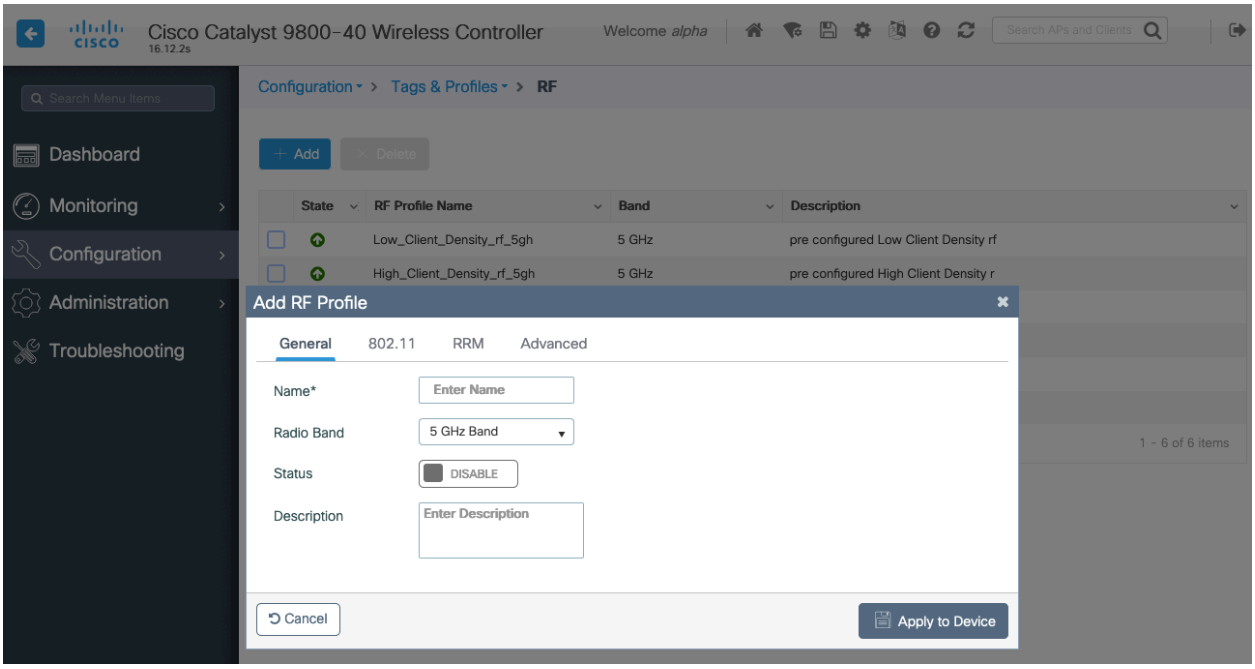
RF Profiles can be created to specify which frequency bands, data rates, RRM settings, and advanced settings a group of access points should use.

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

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

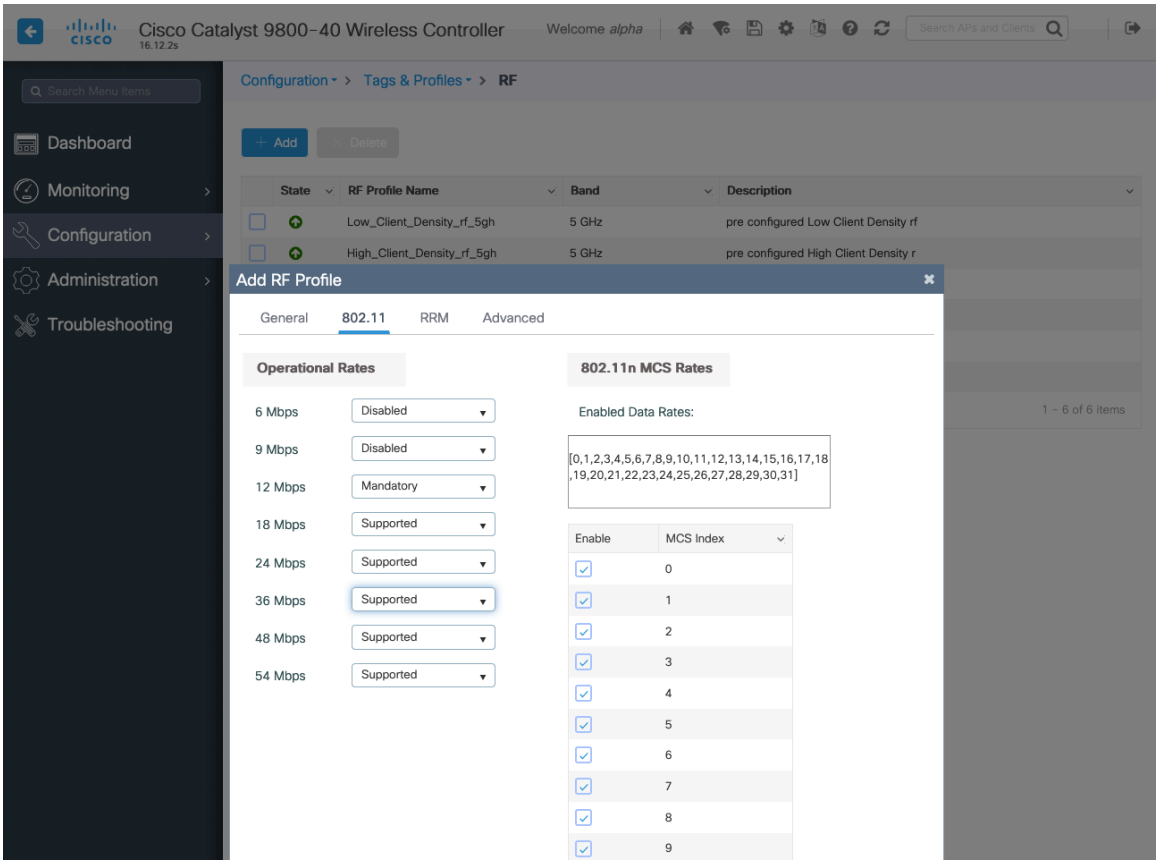
When creating an RF Profile, the **Name** and **Radio Band** must be defined.

Select **5 GHz Band** or **2.4 GHz Band** for the **Radio Band**.

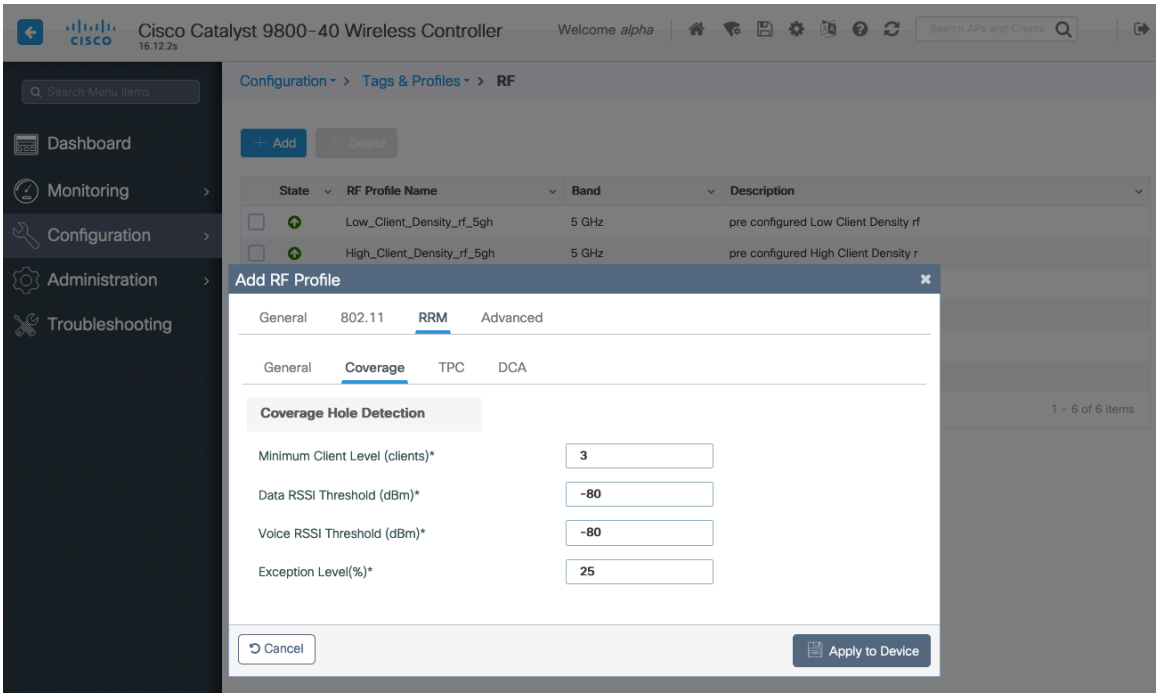


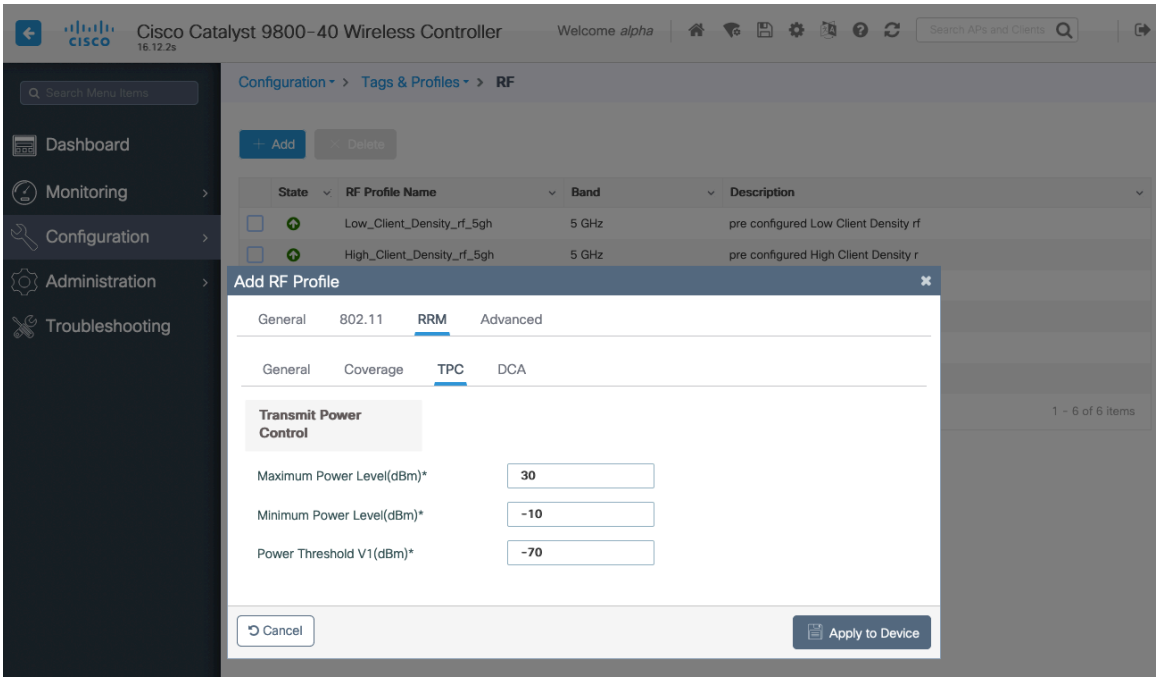
On the **802.11** tab, configure the data rates as necessary.

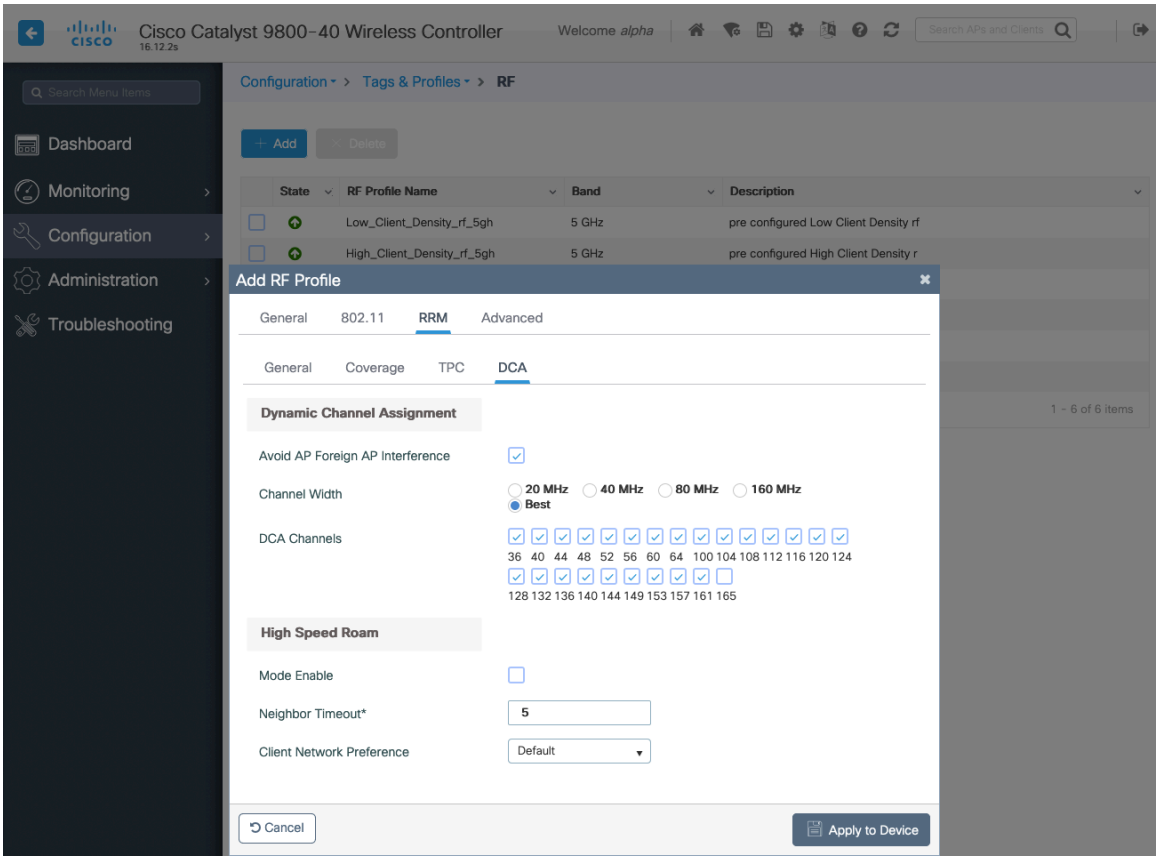
Is recommended to enable 12 Mbps as **Mandatory** and 18 Mbps and higher as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.



On the **RRM** tab, the **Maximum Power Level** and **Minimum Power Level** settings as well as other **DCA**, **TPC**, and **Coverage** settings can be configured.

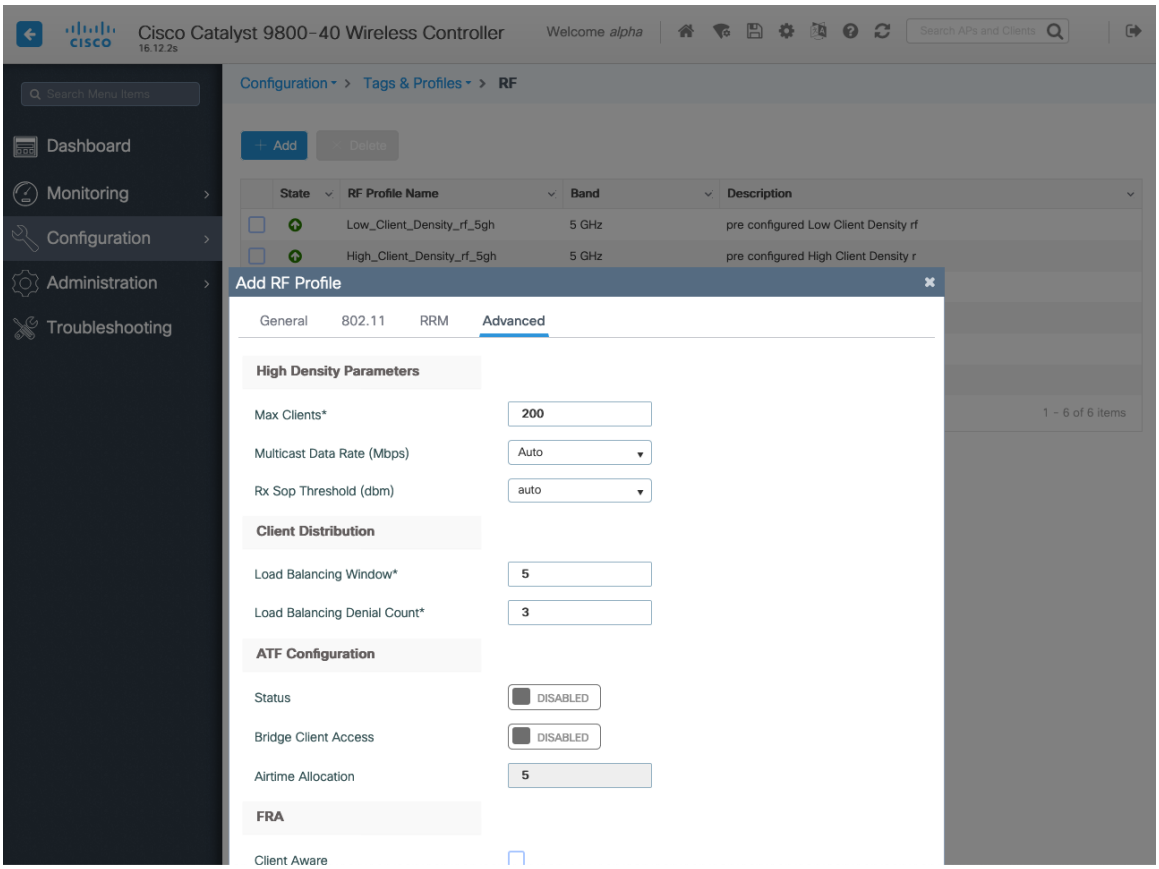

Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles > RF
Add
Delete
State
RF Profile Name
Band
Description
Low_Client_Density_rf_5gh
5 GHz
pre configured Low Client Density rf
High_Client_Density_rf_5gh
5 GHz
pre configured High Client Density r
1 - 6 of 6 items
Add RF Profile
General
802.11
RRM
Advanced
General
Coverage
TPC
DCA
Coverage Hole Detection
Minimum Client Level (clients)*
3
Data RSSI Threshold (dBm)*
-80
Voice RSSI Threshold (dBm)*
-80
Exception Level(%)*
25
Cancel
Apply to Device


Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles > RF
Add
Delete
State
RF Profile Name
Band
Description
Low_Client_Density_rf_5gh
5 GHz
pre configured Low Client Density rf
High_Client_Density_rf_5gh
5 GHz
pre configured High Client Density r
1 - 6 of 6 items
Add RF Profile
General
802.11
RRM
Advanced
General
Coverage
TPC
DCA
Transmit Power Control
Maximum Power Level(dBm)*
30
Minimum Power Level(dBm)*
-10
Power Threshold V1(dBm)*
-70
Cancel
Apply to Device



On the **Advanced** tab, **Maximum Clients**, **Multicast Data Rate**, **Rx Sop Threshold**, and other advanced settings can be configured.

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



Flex Profiles

Flex Profiles are used to define the settings the access point should use when in Flexconnect mode.

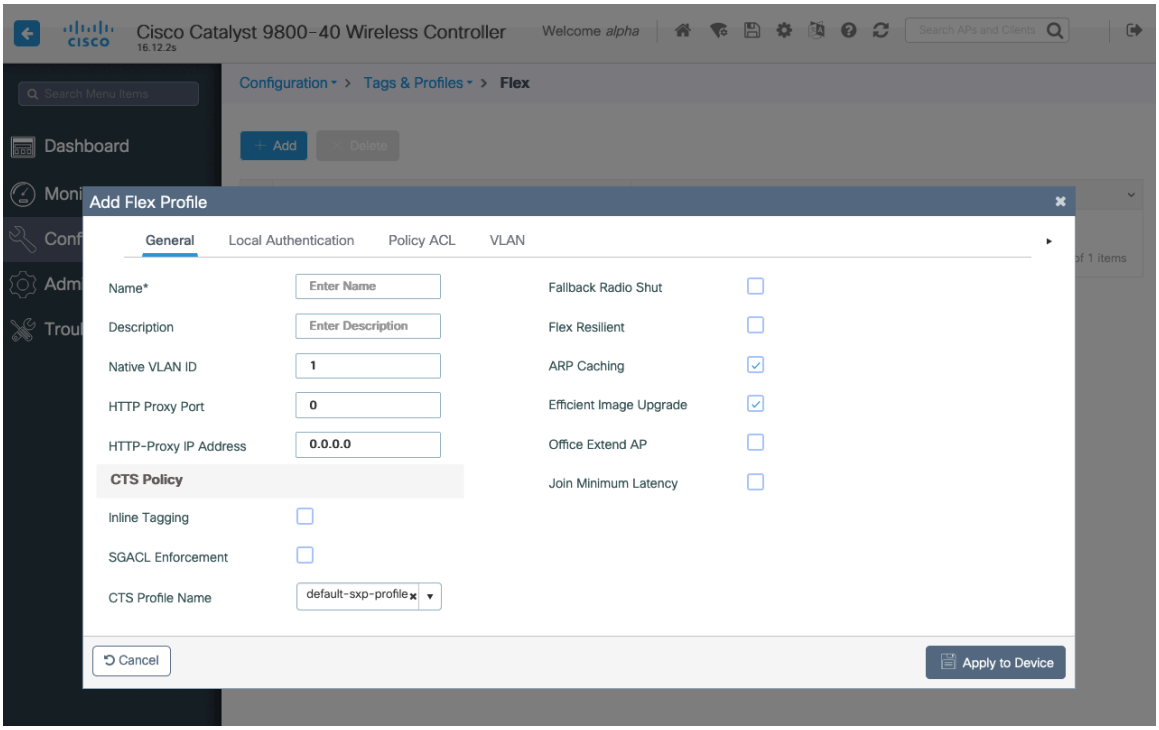
Flex Profiles are then mapped to a Site Tag, which then can be applied to an access point.

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

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

Ensure **ARP Caching** is **Enabled**.

Enable **Local Authentication** as necessary.



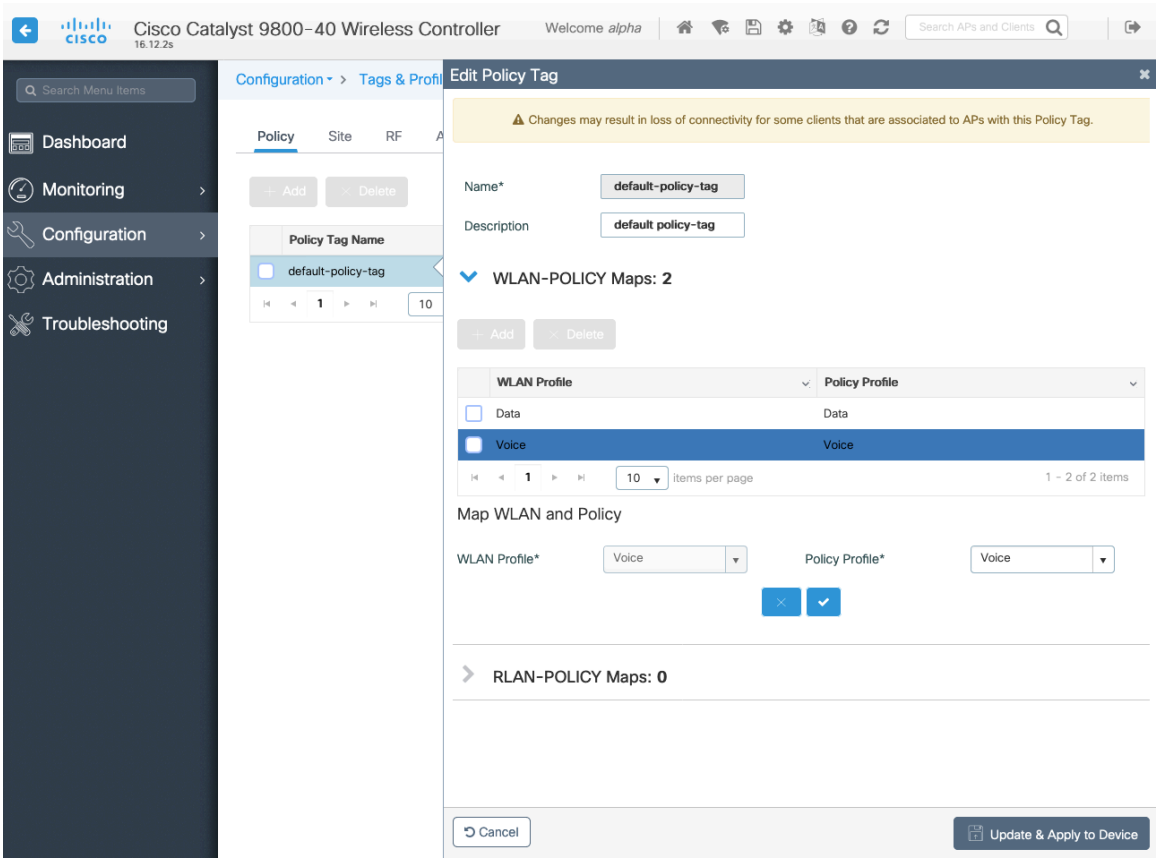
Tags

Policy Tag

Policy Tags define the mapping of WLAN Profiles and Policy Profiles.

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

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



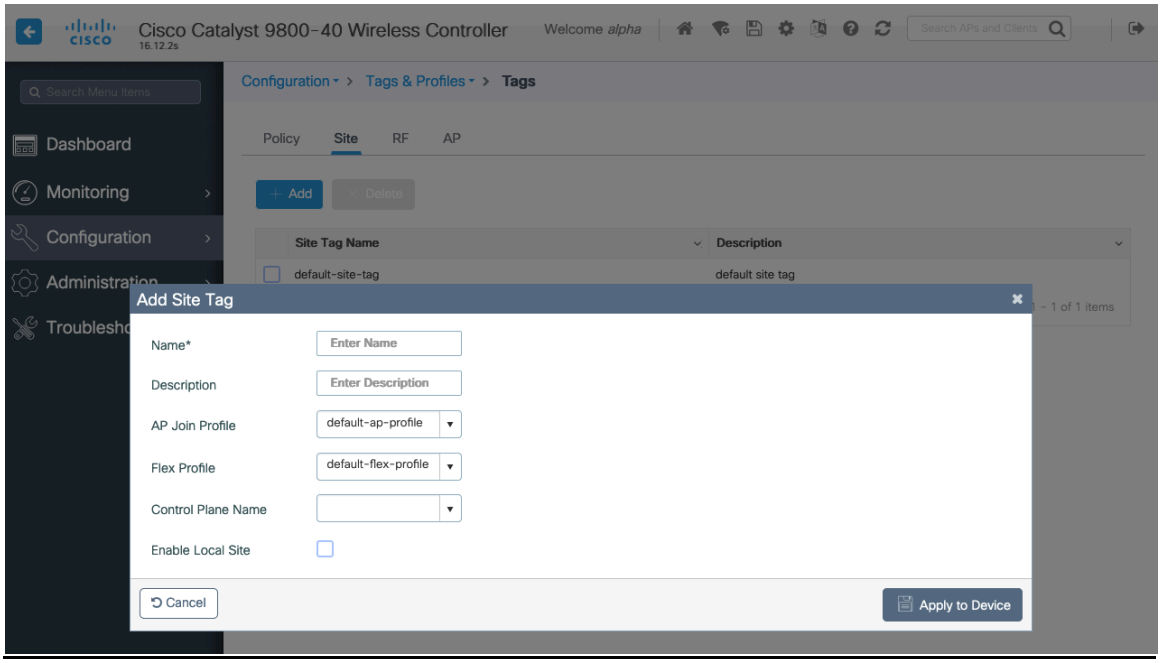
Site Tag

Site Tags define which AP Join Profile and Flex Profile should be used.

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

When creating a Site Tag, click **Add**, select the **AP Join Profile** to be used.

When creating a Site Tag to include a Flex Profile, ensure **Enable Local Site** is not checked, then select the necessary **Flex Profile**.

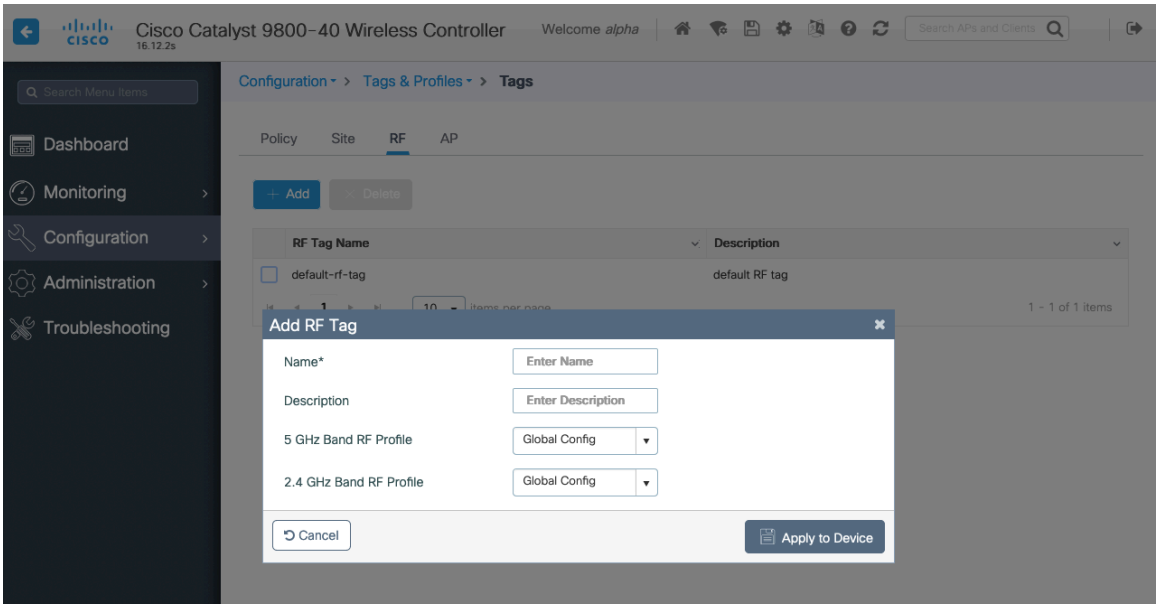


RF Tag

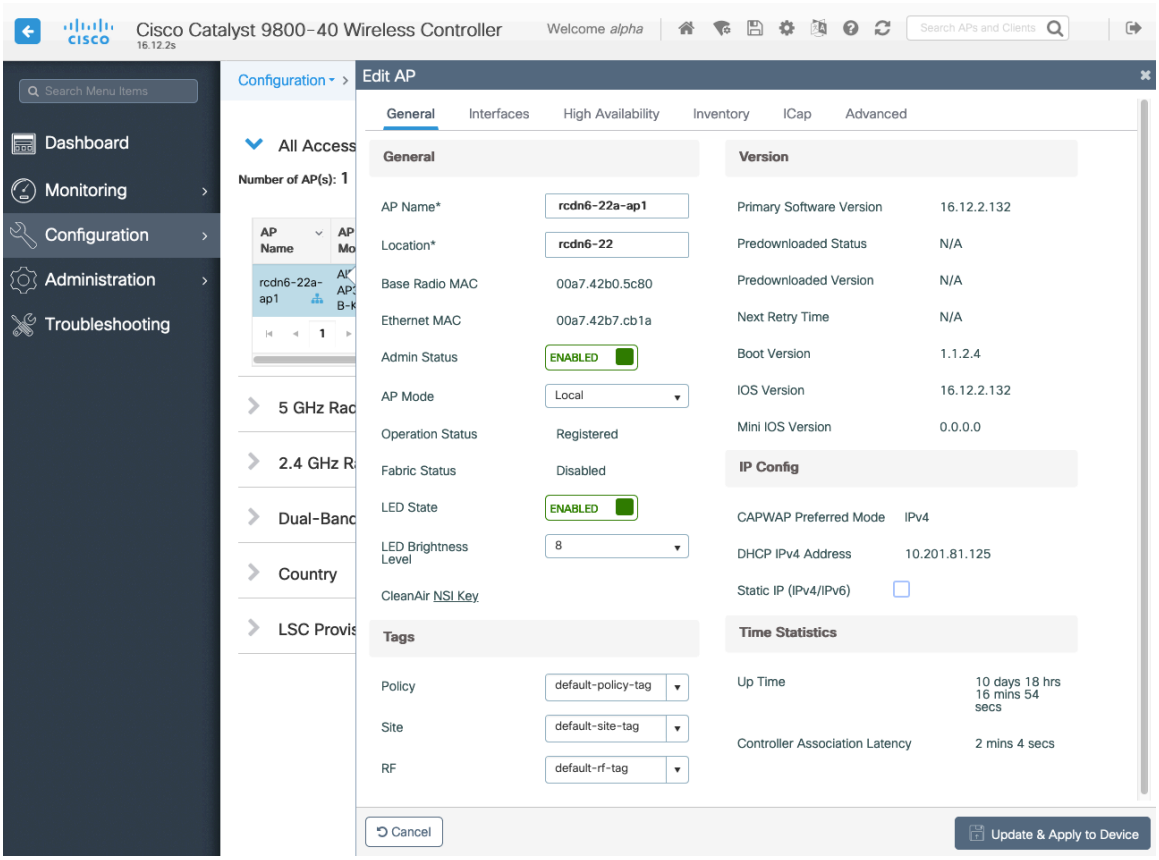
RF Tags define which RF Profiles should be used for 2.4 GHz and 5 GHz.

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

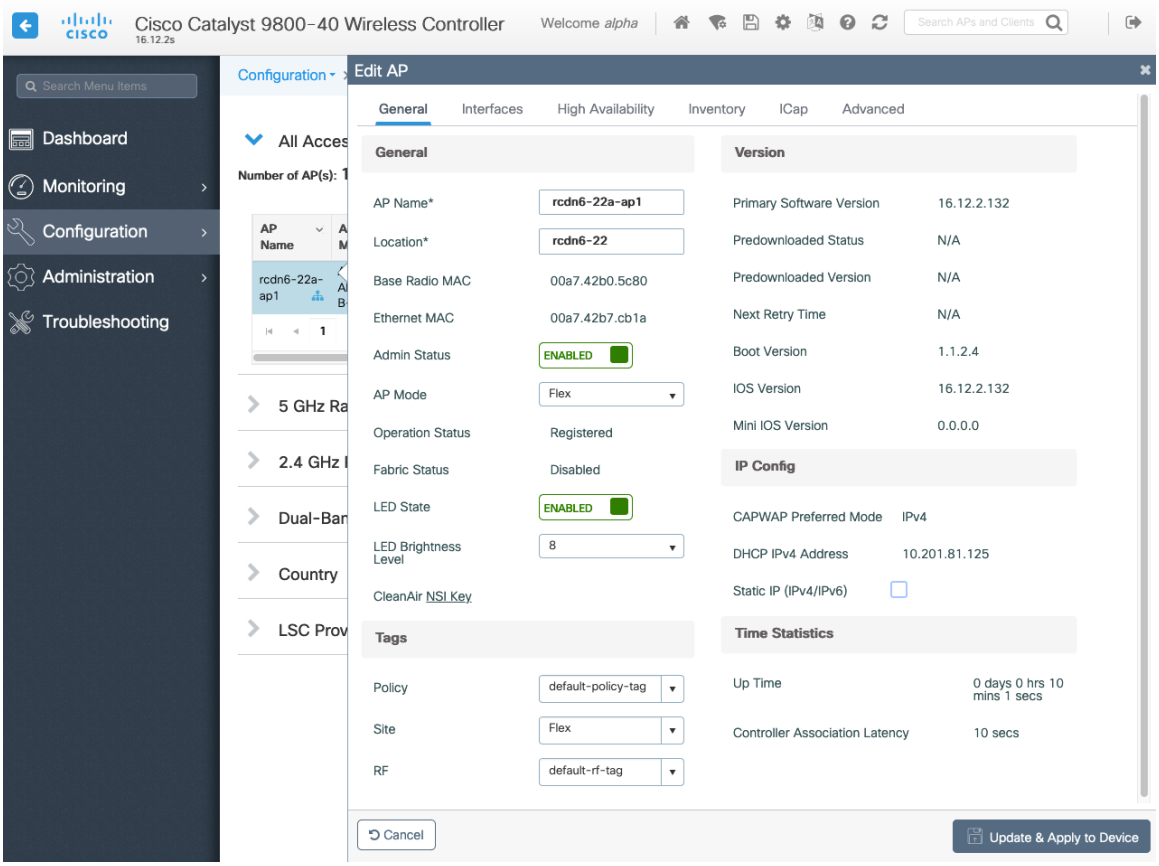
When creating a RF Tag, select the **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be used.



Once tags are defined, they can then be applied to an access point.



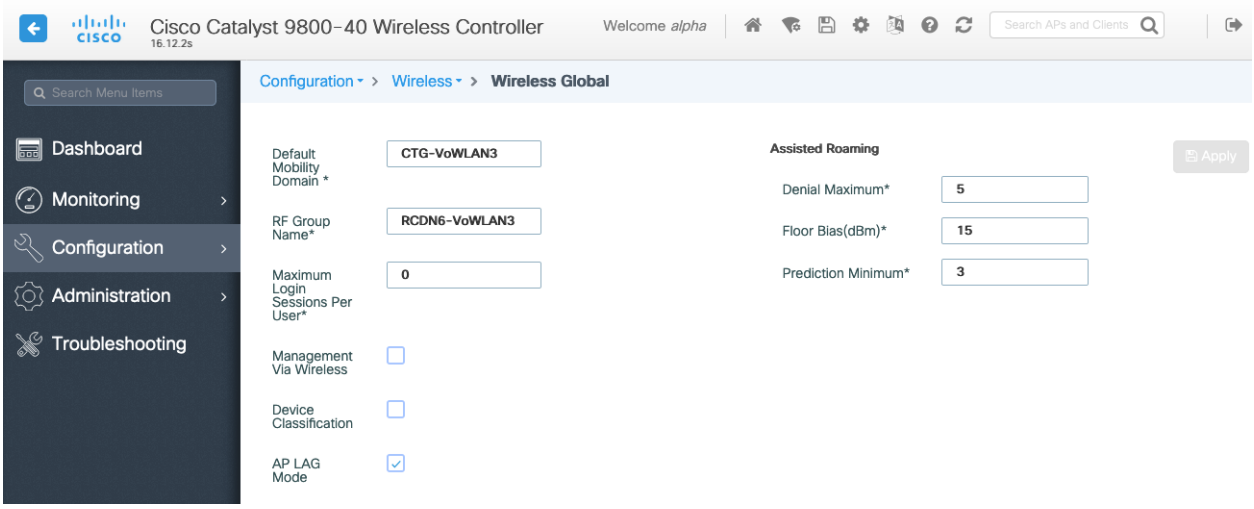
If a Site Tag is applied including a configured Flex Profile, then the **AP Mode** will be changed to **Flex** automatically.



Controller Settings

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

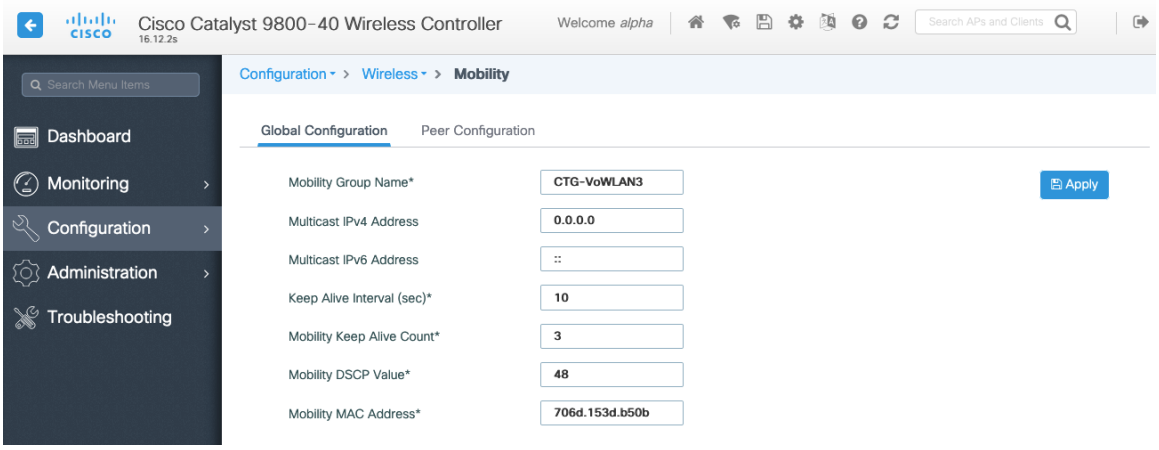
Enable **AP LAG Mode**.

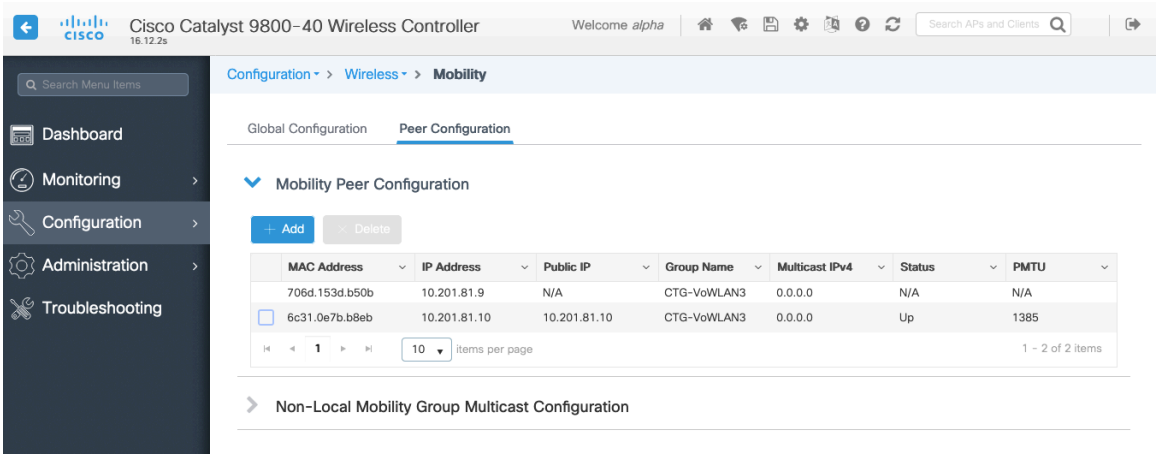


Mobility Settings

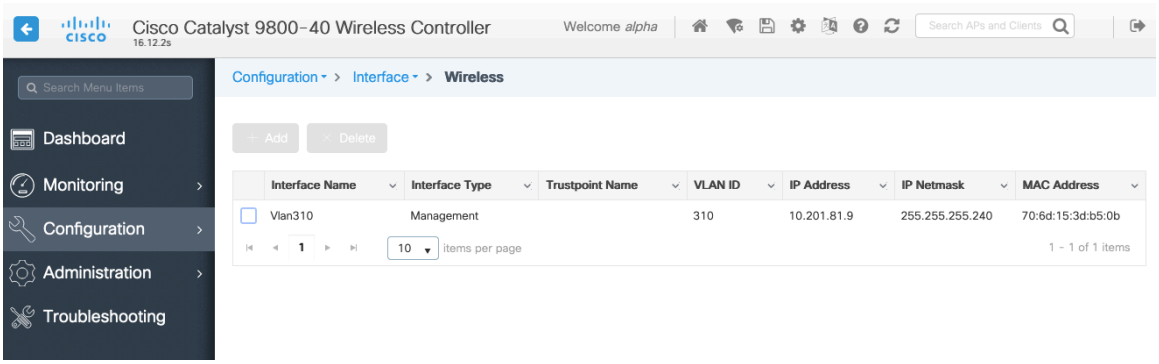
When multiple Cisco Wireless LAN Controllers are to be in the same mobility group, then the IP address and MAC address of each Cisco Wireless LAN Controller should be added to the Mobility Peer configuration.

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





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



Call Admission Control (CAC)

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

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

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

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

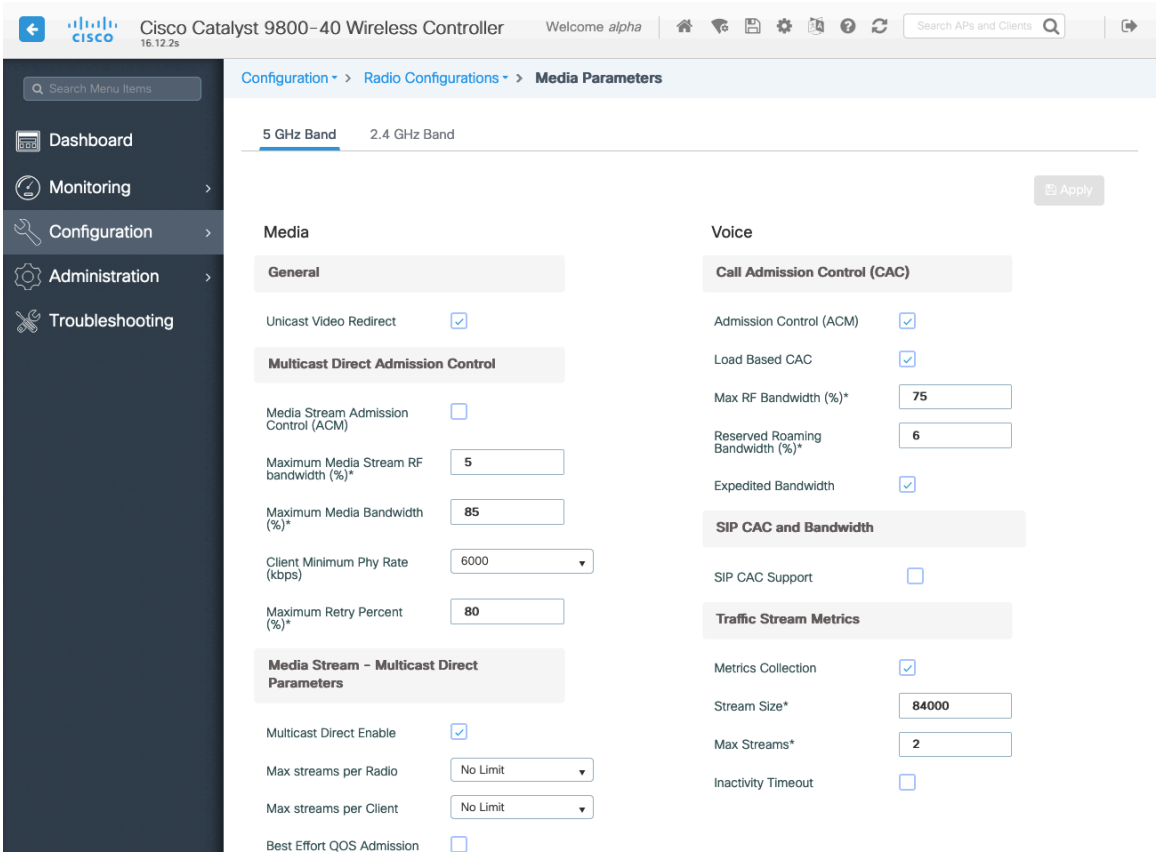
Load Based CAC will account for all energy on the channel.

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

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

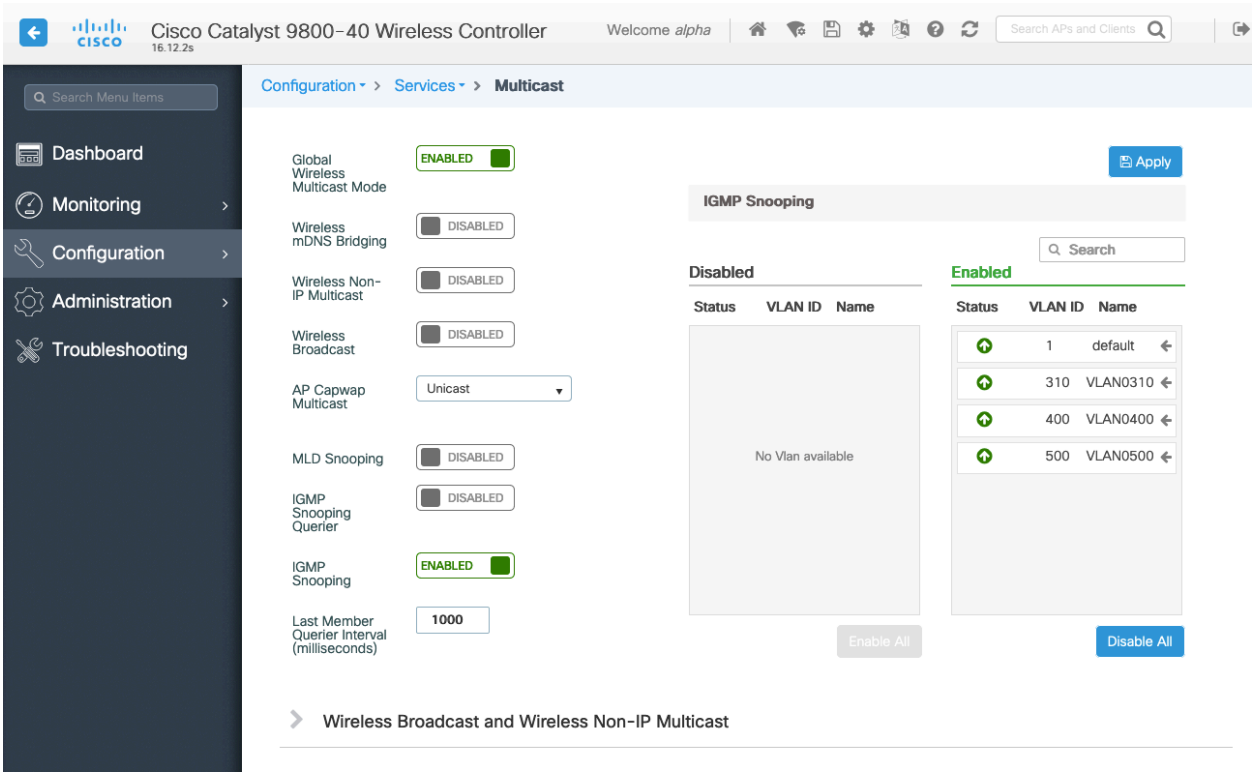
Ensure the **Inactivity Timeout** is Disabled.

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

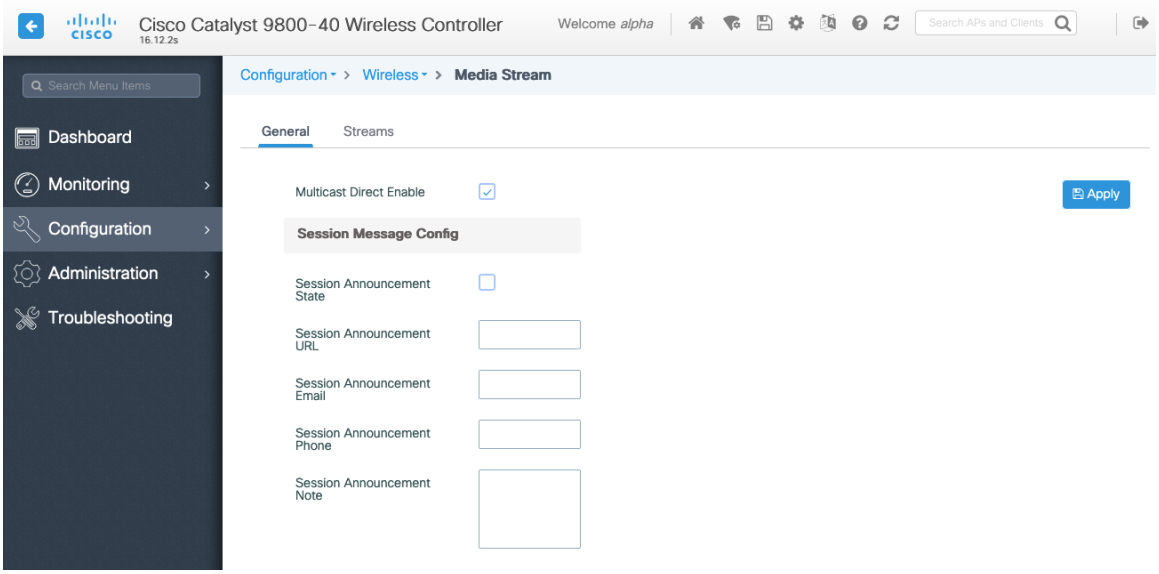


Multicast

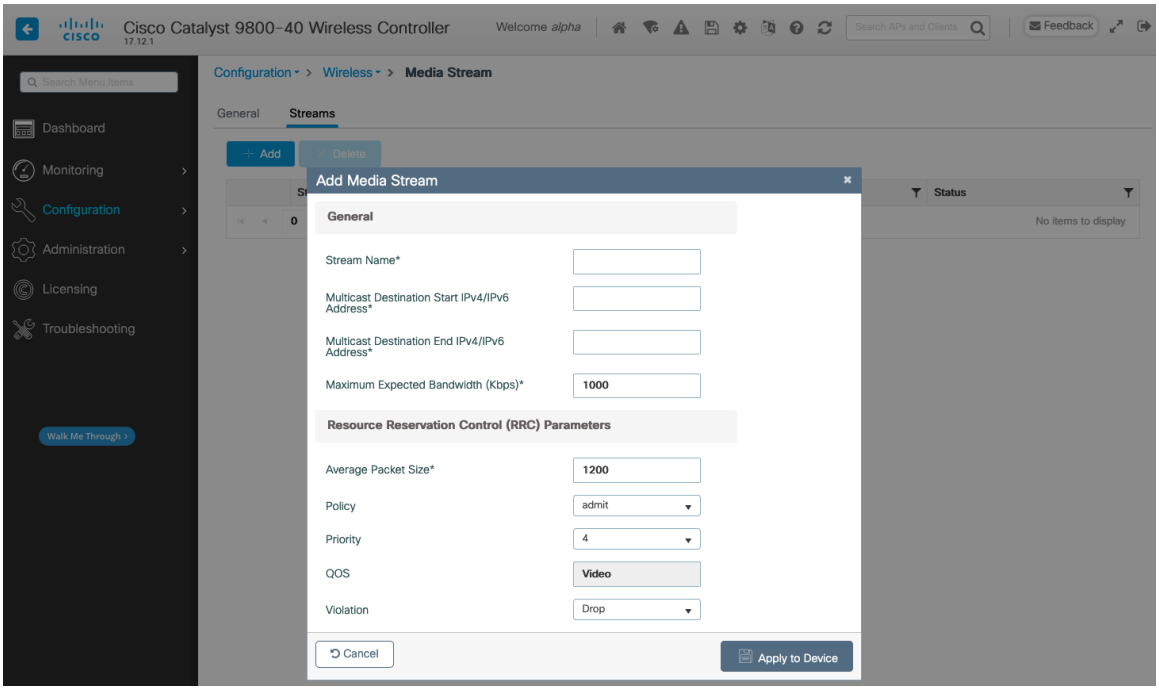
If utilizing multicast, then **Global Wireless Multicast Mode** and **IGMP Snooping** should be **Enabled**.



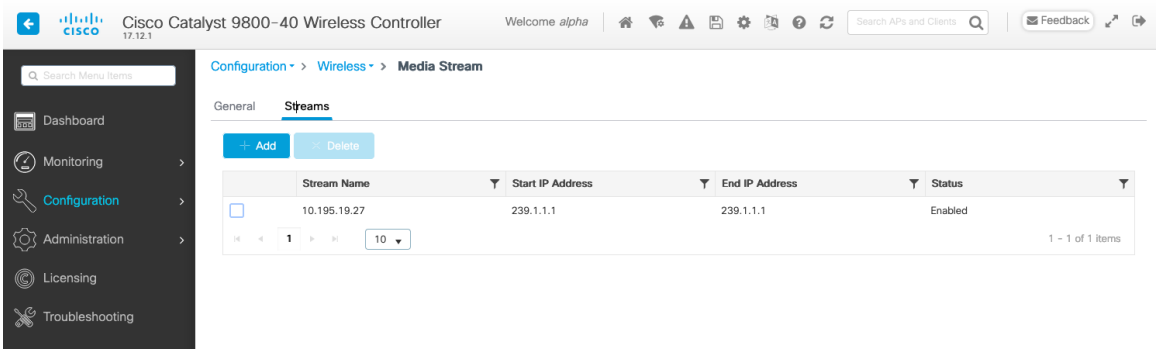
In the Media Stream settings, **Multicast Direct Enable** should be **Enabled**.



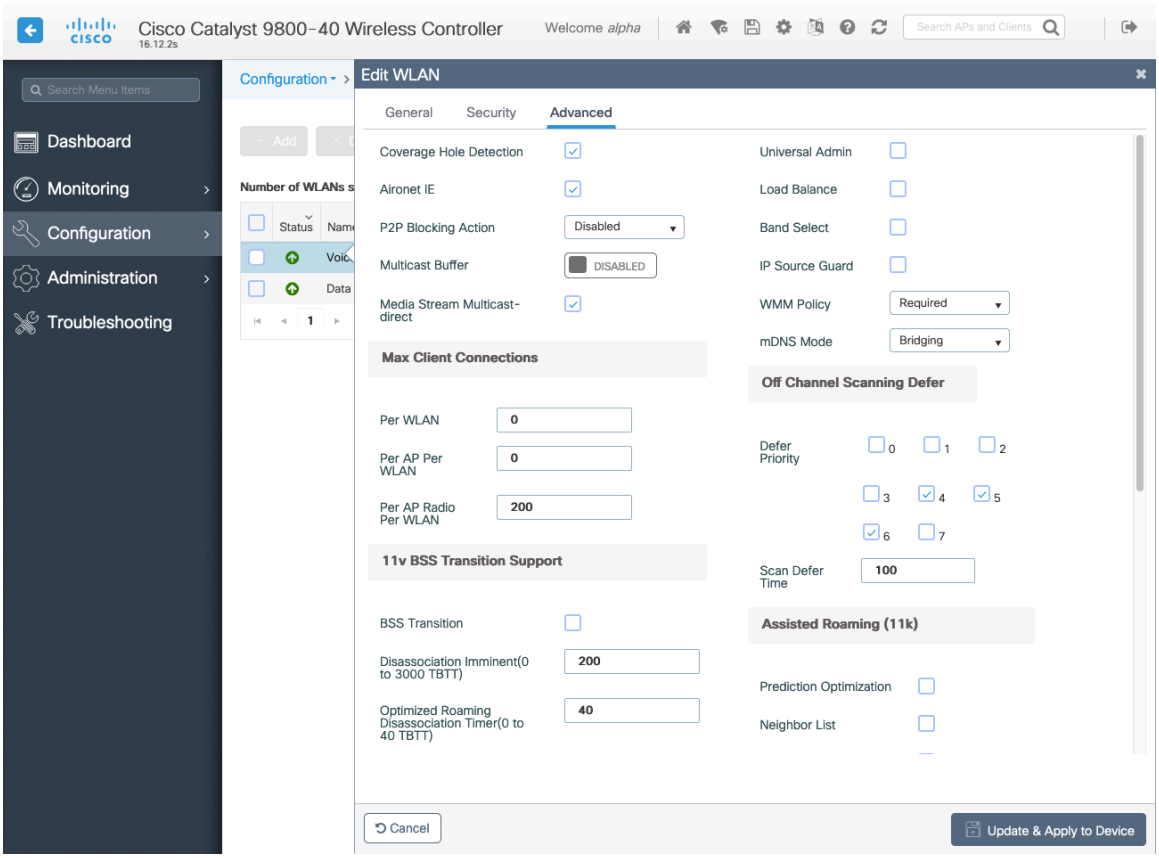
Then configure the media streams as necessary.



Once saved, then the media stream will be displayed.



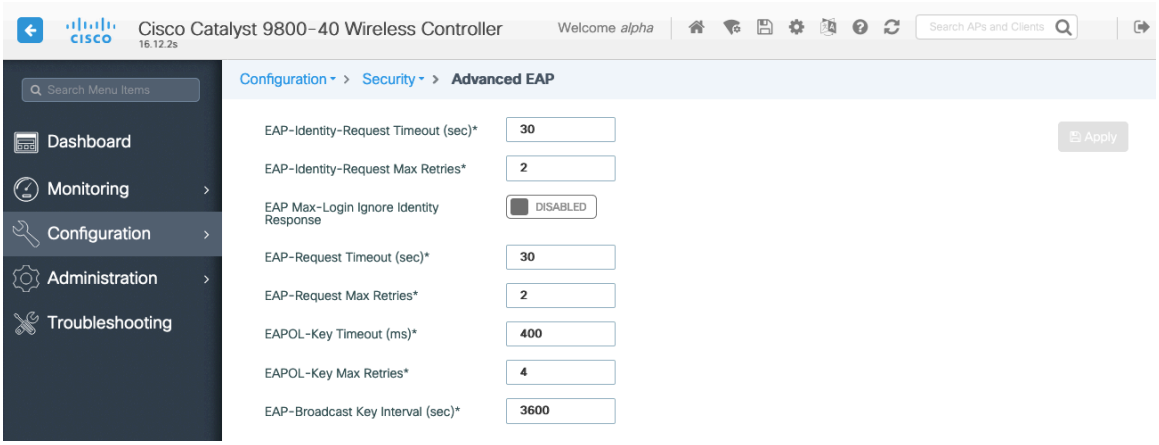
And enable **Multicast Direct** in the WLAN configuration.



Advanced Settings

Advanced EAP Settings

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



If using 802.1x, the **EAP-Request Timeout** on the Cisco Wireless LAN Controller should be set to 30 seconds.

For deployments where EAP failures occur frequently, the **EAP-Request Timeout** should be reduced below 30 seconds.

If using PSK then it is recommended to reduce the **EAPOL-Key Timeout** to 400 milliseconds from the default of 1000 milliseconds with **EAPOL-Key Max Retries** set to 4 from the default of 2.

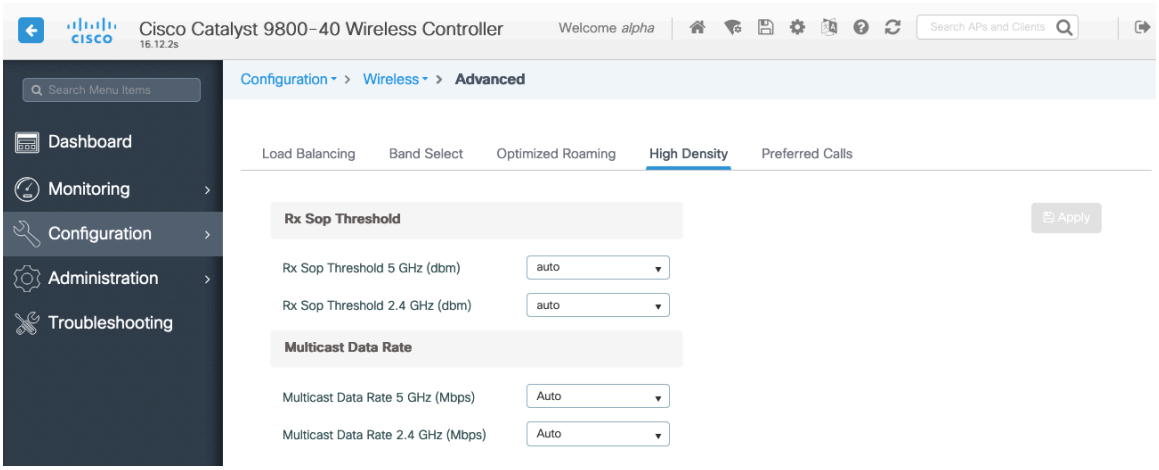
If using 802.1x, then using the default values where the **EAPOL-Key Timeout** is set to 1000 milliseconds and **EAPOL-Key Max Retries** are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.

The **EAPOL-Key Timeout** should not exceed 1000 milliseconds (1 second).

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

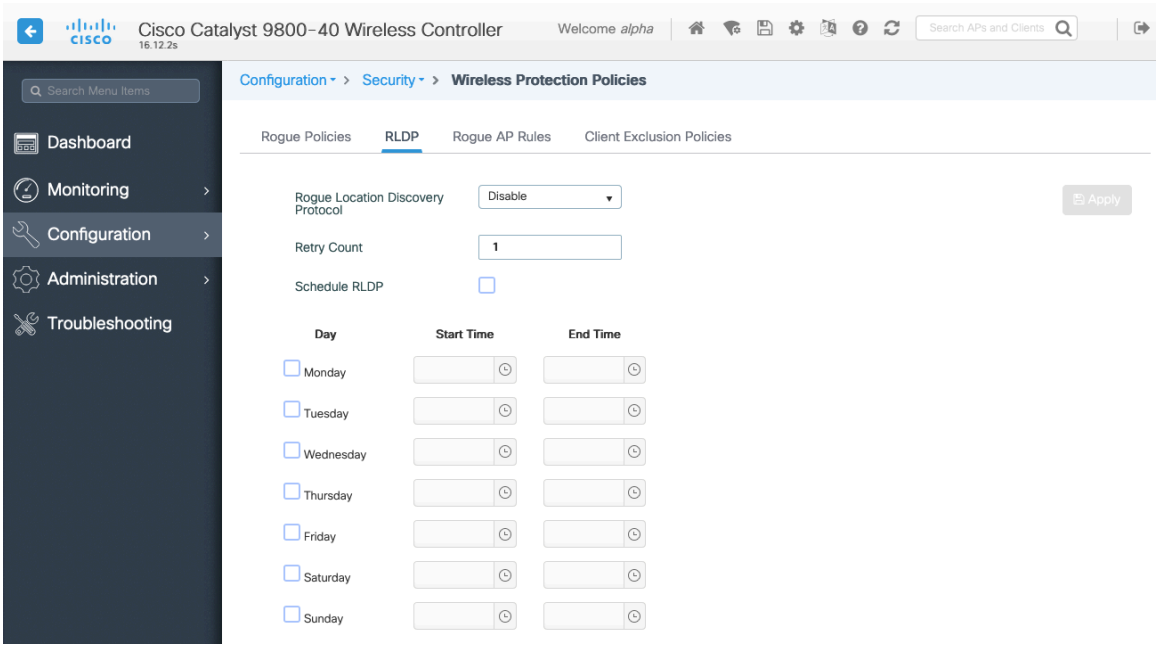
Rx Sop Threshold

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



Rogue Policies

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



Sample Configuration

```
version 16.12
service timestamps debug 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 self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33313130 36383230 3031301E 170D3139 30373130 30343236
  35375A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31313036
  38323030 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100B74F D6A0DE5D DFB2CDD2 5196AAB1 86C8BD48 3AAAF455 C4E7D559
  41A10FE1 87EC742C C5014113 9A0FD83A F490EA64 DF68A513 AA6900C4 810A9FED
  870309EA 781EB999 882F7374 EC79D592 DEC6C126 A5FB5666 905C24D8 B2064CD4
  66823D6E 7E9A07F3 B043D632 EEDF4CAF D306C303 843493AA F44126E3 A07DE905
  6B6C5B8E C8E6C9E6 45D79F62 B813FF8C B44FA7AC AEDB8A9E 55B75096 E4E76BC3
  D5B90900 1A0C7CD0 910B6C63 920E9666 39EC3702 387757F1 C26F0BB5 89D4733D
  FED71CF4 33002C77 0F721B21 5578C850 590BC846 7CB79469 A51CEBA5 96EA8672
  DDB82A44 69EEDA13 DD83B0FA 3221A839 5F985C86 F2C57B78 8E6608B6 18A346D2
  035D3B68 26BF0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 141B4651 019E0AEC 8E64EB65 C0E023ED 60F6062C
  0F301D06 03551D0E 04160414 1B465101 9E0AEC8E 64EB65C0 E023ED60 F6062C0F
  300D0609 2A864886 F70D0101 05050003 82010100 3319F2A7 3E88539F 85C08F28
  67553F93 408DCCC6 EFE2704E C142766C 5FFE0E97 0AFDE0EA 816CB4E2 60FFBC26
  6E411C57 3F1AB3F8 2F1E9959 AED26C86 2C0B059D B692C72C B5859A15 999916F8
  699587DC 94409E7C FF685698 2FB9ACEC 9315F1AA 357E3877 7AE1E37C F5CD7E46
  EB3ADC44 3F22A9E0 EA35E6B8 E5508721 0E8754A1 6A6E3A6A C7FD8E64 6C3C722C
  F90919C9 DE675E5C 301FF83A 0593ACE6 4A469209 CAAEC53F 5102FDD3 AE378090
```

```
  46282E00 BCF65EB7 4C257EFD 57986F82 B6DD8336 CEA82E27 63B4C6C5 F92945E8
  2AFE9A95 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 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 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
```

```
wireless profile airtime-fairness default-atf-policy 0
wireless profile flex default-flex-profile
 description “default flex profile”
wireless profile mesh default-mesh-profile
 description “default mesh profile”
wireless profile policy Data
 ipv4 flow monitor wireless-avc-basic input
 ipv4 flow monitor wireless-avc-basic output
 service-policy input silver-up
 service-policy output silver
 session-timeout 86400
 vlan VLAN0400
 no shutdown
wireless profile policy Voice
 ipv4 flow monitor wireless-avc-basic input
 ipv4 flow monitor wireless-avc-basic output
 service-policy input platinum-up
 service-policy output platinum
 session-timeout 86400
 vlan VLAN0500
 no shutdown
wireless profile policy default-policy-profile
 description “default policy profile”
 vlan default
wireless tag site default-site-tag
 description “default site tag”
wireless tag policy default-policy-tag
 description “default policy-tag”
 wlan Data policy Data
 wlan Voice policy Voice
wireless tag rf default-rf-tag
 description “default RF tag”
wireless rf-network RCDN6-VoWLAN3
wireless security dot1x eapol-key retries 4
wireless security dot1x eapol-key timeout 400
no wireless security dot1x max-login-ignore-identity-response
wireless fabric control-plane default-control-plane
wireless media-stream multicast-direct
wireless multicast
wlan Data 2 data
 band-select
 ccx aironet-iesupport
 load-balance
 security dot1x authentication-list authentication_dot1x_day0
 no shutdown
wlan Voice 1 voice
 no assisted-roaming neighbor-list
 no bss-transition
 ccx aironet-iesupport
 channel-scan defer-priority 4
 dtim dot11 24ghz 2
 dtim dot11 5ghz 2
 media-stream multicast-direct
 radio dot11a
 security ft
 security wpa akm ft dot1x
 security dot1x authentication-list authentication_dot1x_day0
```

```
 wmm require
 no shutdown
ap dot11 24ghz rf-profile Low_Client_Density_rf_24gh
 coverage data rssi threshold -90
 coverage level 2
 coverage voice rssi threshold -90
 description “pre configured Low Client Density rfprofile for 2.4gh radio”
 high-density rx-sop threshold low
 tx-power v1 threshold -65
 no shutdown
ap dot11 24ghz rf-profile High_Client_Density_rf_24gh
 description “pre configured High Client Density rfprofile for 2.4gh radio”
 high-density rx-sop threshold medium
 rate RATE_11M disable
 rate RATE_12M mandatory
 rate RATE_1M disable
 rate RATE_2M disable
 rate RATE_5_5M disable
 rate RATE_6M disable
 tx-power min 7
 no shutdown
ap dot11 24ghz rf-profile Typical_Client_Density_rf_24gh
 description “pre configured Typical Client Density rfprofile for 2.4gh radio”
 rate RATE_11M disable
 rate RATE_12M mandatory
 rate RATE_1M disable
 rate RATE_2M disable
 rate RATE_5_5M disable
 rate RATE_6M disable
 no shutdown
ap dot11 24ghz media-stream multicast-direct
ap dot11 24ghz media-stream video-redirect
no ap dot11 24ghz cac voice tspec-inactivity-timeout
ap dot11 24ghz cac voice tspec-inactivity-timeout ignore
ap dot11 24ghz cac voice acm
ap dot11 24ghz edca-parameters optimized-video-voice
ap dot11 24ghz exp-bwreq
ap dot11 24ghz tsm
ap dot11 24ghz rrm txpower max 14
ap dot11 24ghz rrm txpower min 5
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 5ghz rf-profile Low_Client_Density_rf_5gh
 coverage data rssi threshold -90
 coverage level 2
 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
 tx-power min 7
 tx-power v1 threshold -65
 no shutdown
ap dot11 5ghz rf-profile Typical_Client_Density_rf_5gh
 description “pre configured Typical Density rfprofile for 5gh radio”
 no shutdown
ap dot11 5ghz media-stream multicast-direct
ap dot11 5ghz media-stream video-redirect
no ap dot11 5ghz cac voice tspec-inactivity-timeout
ap dot11 5ghz cac voice tspec-inactivity-timeout ignore
ap dot11 5ghz cac voice acm
ap dot11 5ghz exp-bwreq
ap dot11 5ghz tsm
ap dot11 5ghz edca-parameters optimized-video-voice
ap dot11 5ghz channelswitch quiet
ap dot11 5ghz rrm channel dca chan-width 40
ap dot11 5ghz rrm channel dca remove 116
ap dot11 5ghz rrm channel dca remove 120
ap dot11 5ghz rrm channel dca remove 124
ap dot11 5ghz rrm channel dca remove 128
ap dot11 5ghz rrm channel dca remove 144
ap dot11 5ghz rrm txpower max 17
ap dot11 5ghz rrm txpower min 11
ap dot11 5ghz rate RATE_24M supported
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap country US
ap lag support
ap tag-source-priority 2 source filter
ap tag-source-priority 3 source ap
ap profile default-ap-profile
 capwap backup primary RCDN6-21A-WLC5 10.201.81.9
 capwap backup secondary RCDN6-22A-WLC6 10.201.81.10
 description “default ap profile”
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
 hyperlocation
 lag
 mgmtuser username <REMOVED> password 0 <REMOVED> secret 0 <REMOVED>
 ntp ip 10.115.162.212
 ssh
end
```

Cisco Mobility Express and Lightweight Access Points

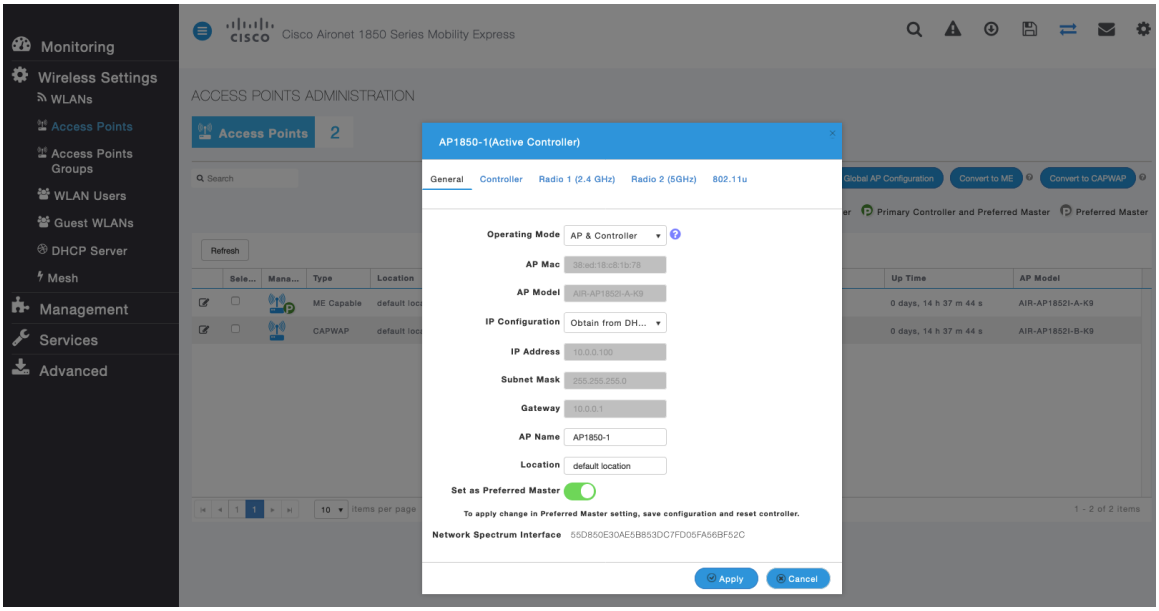
When configuring Cisco Mobility Express and Lightweight Access Points, use the following guidelines:

- Ensure **802.11r (FT)** or **CCKM** is **Enabled**
- Set **Quality of Service (QoS)** to **Platinum**

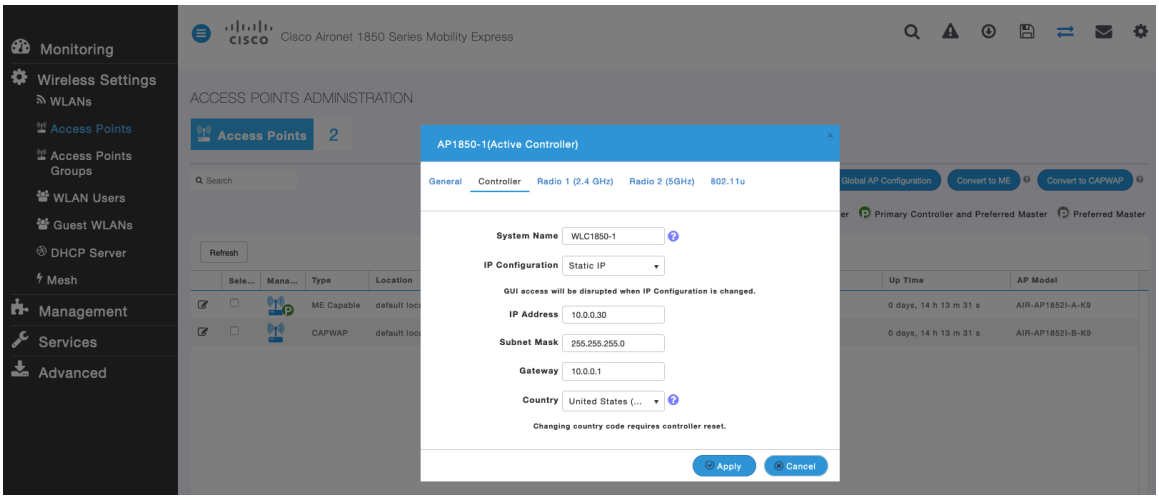
- Recommended to set **802.11k** to **Enabled**
- Recommended to set **802.11v** to **Enabled**
- Disable **P2P (Peer to Peer) Blocking Action**
- Set **Client Band Select** to **Disabled**
- Set **Client Load Balancing** to **Disabled**
- Configure the **Data Rates** as necessary
- Configure **RF Optimization** as necessary
- Set **Traffic Type** to **Voice and Data**
- Enable **CleanAir** if utilizing Cisco access points with CleanAir technology
- Configure **Multicast Direct** as necessary

Controller Settings

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



Configure the Cisco Wireless LAN Controller **System Name** and IP settings as necessary.



802.11 Network Settings

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

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

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

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

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

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

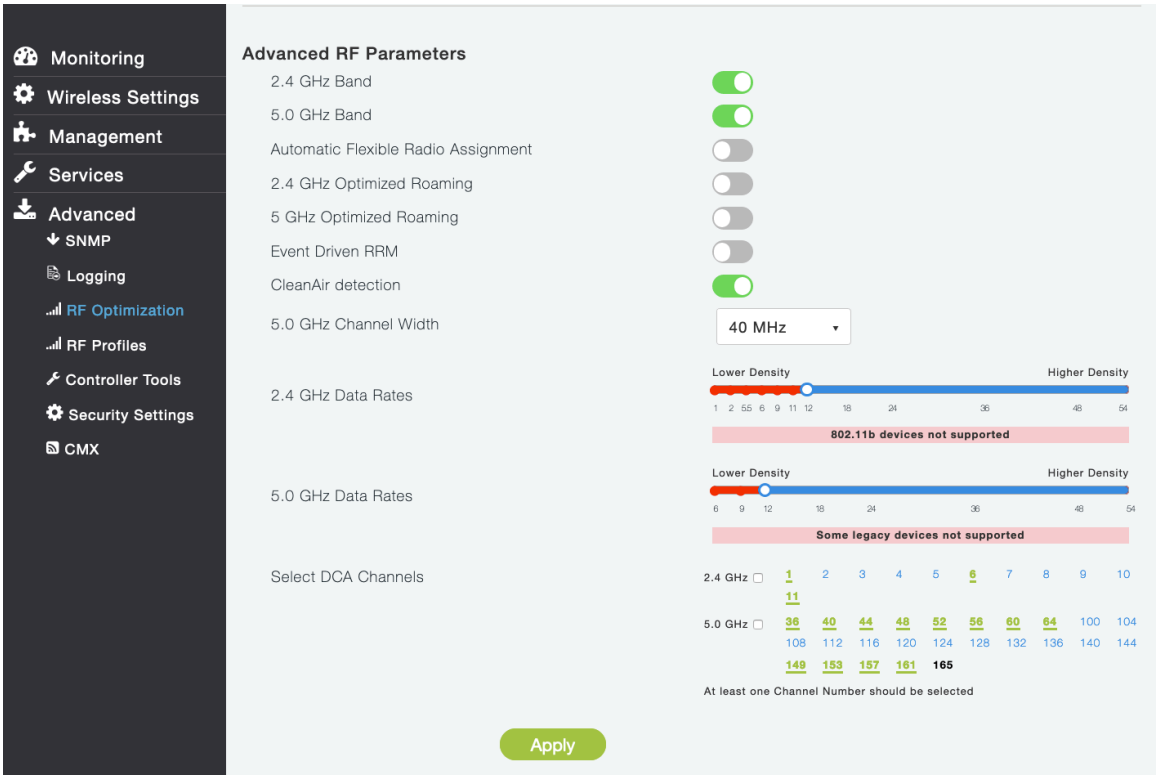
If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.

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

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

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

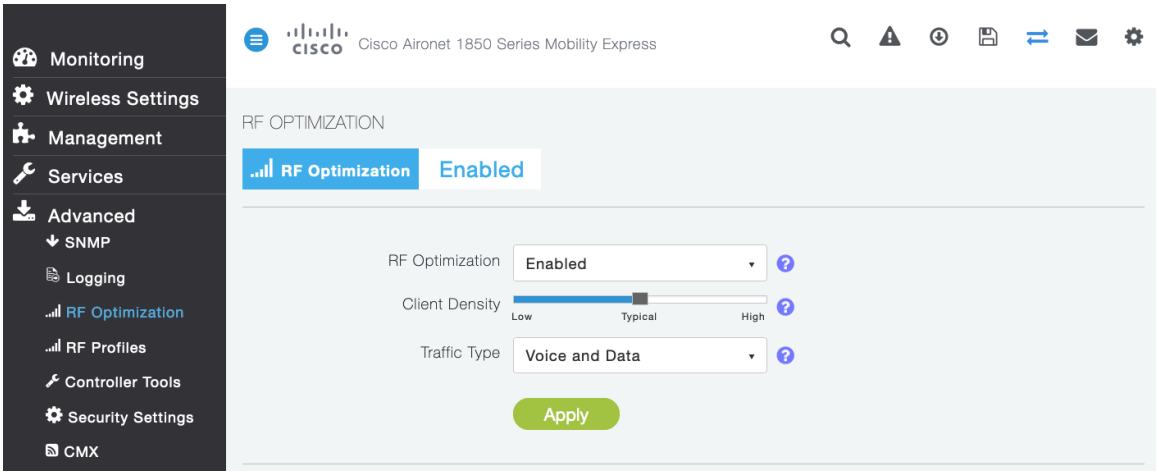
CleanAir detection should be **Enabled** when utilizing Cisco access points with CleanAir technology in order to detect any existing interferers.



RF Optimization

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

Set **Traffic Type** to **Voice and Data**.



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

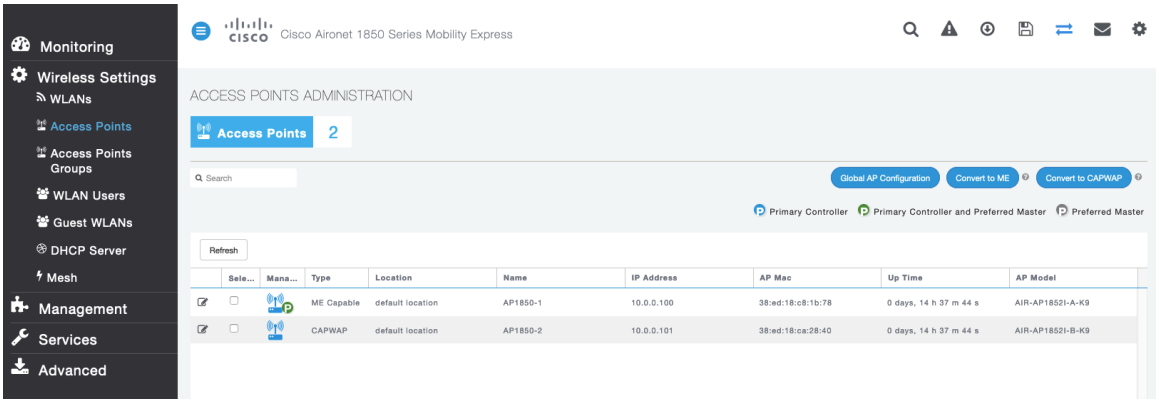
Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

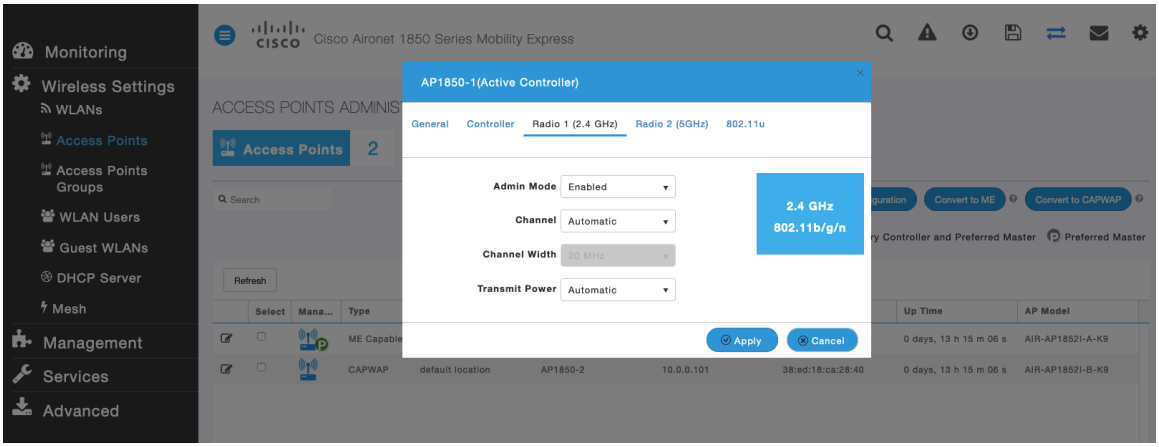
This may be necessary if there is an intermittent interferer present in an area.

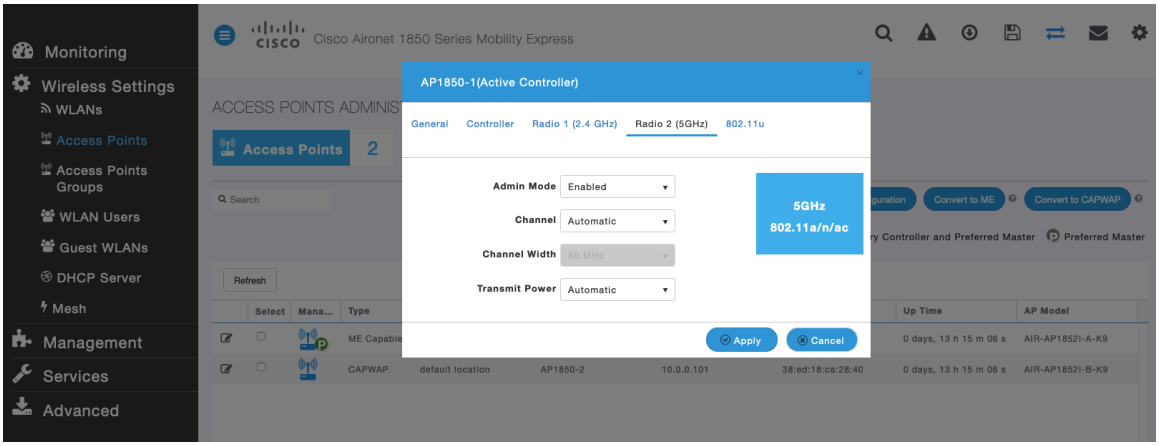
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

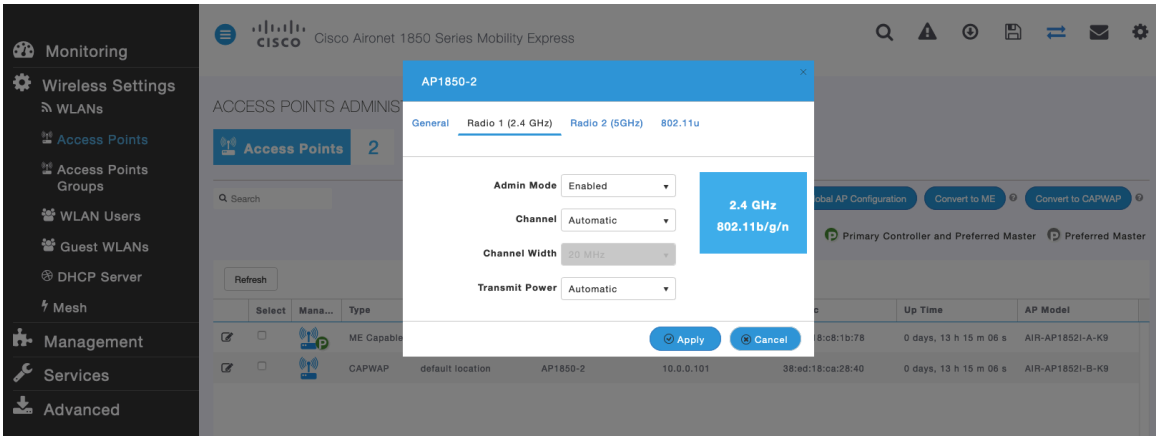
It is recommended to use channel bonding only if using 5 GHz.

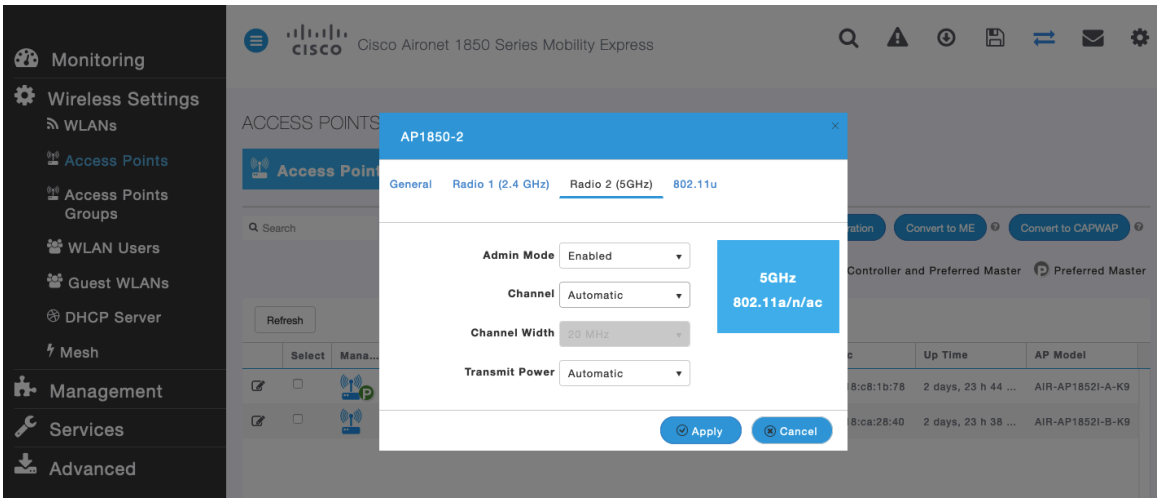
It is recommended to utilize the same channel width for all access points.











WLAN Settings

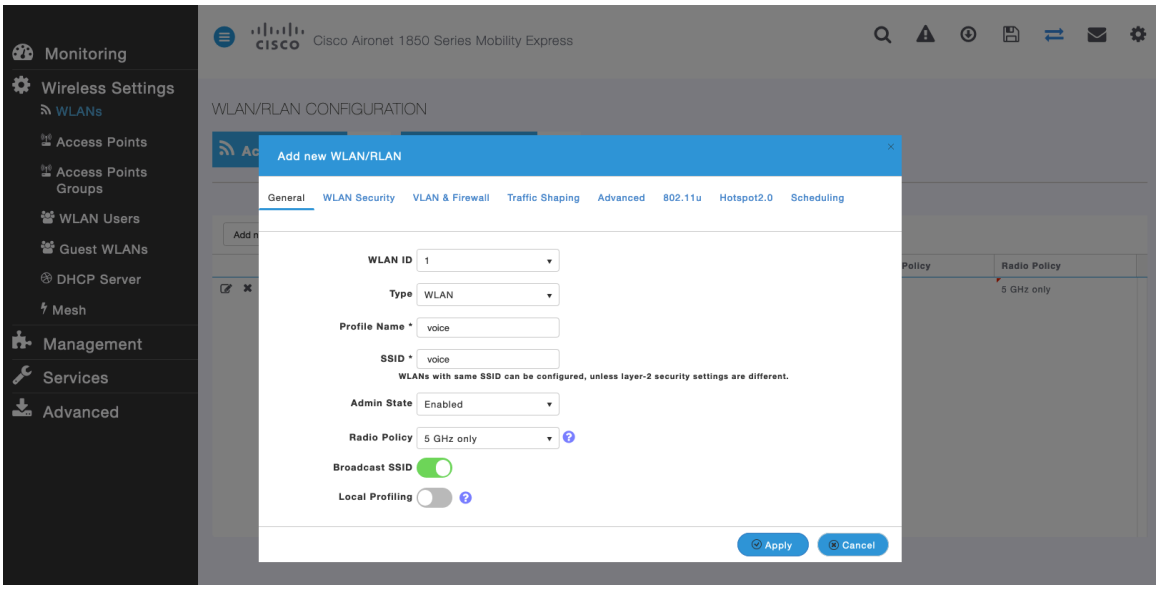
It is recommended to have a separate SSID for the Cisco Wireless Phone 840 and 860.

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

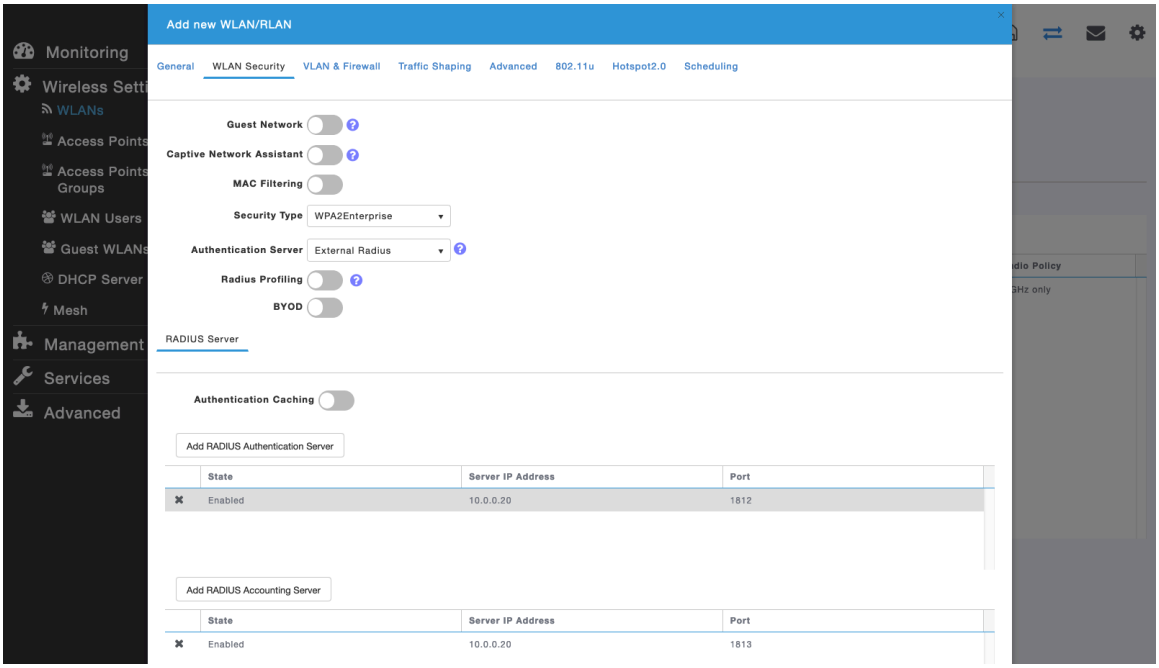
The SSID to be used by the Cisco Wireless Phone 840 and 860 can be configured to only apply to a certain 802.11 radio type (e.g. 5 GHz only).

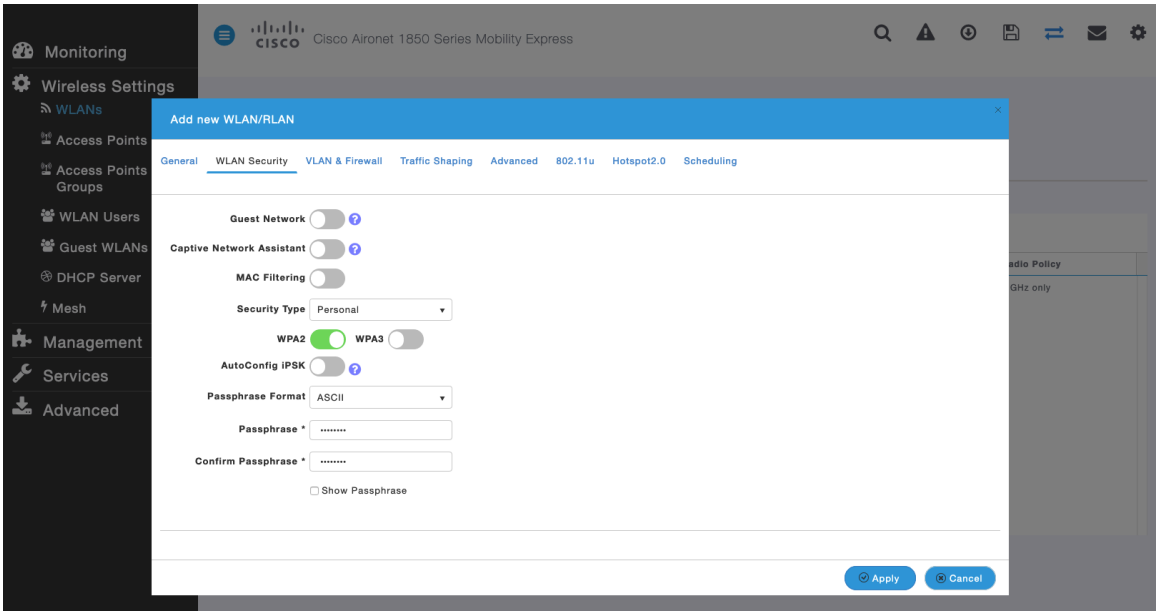
It is recommended to have the Cisco Wireless Phone 840 and 860 operate on the 5 GHz band only due to have many channels available and not as many interferers as the 2.4 GHz band has.

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



To utilize 802.11r (FT) for fast secure roaming, set **Security Type** to either **WPA2Enterprise** or **Personal** depending on whether 802.1x or PSK is to be utilized.

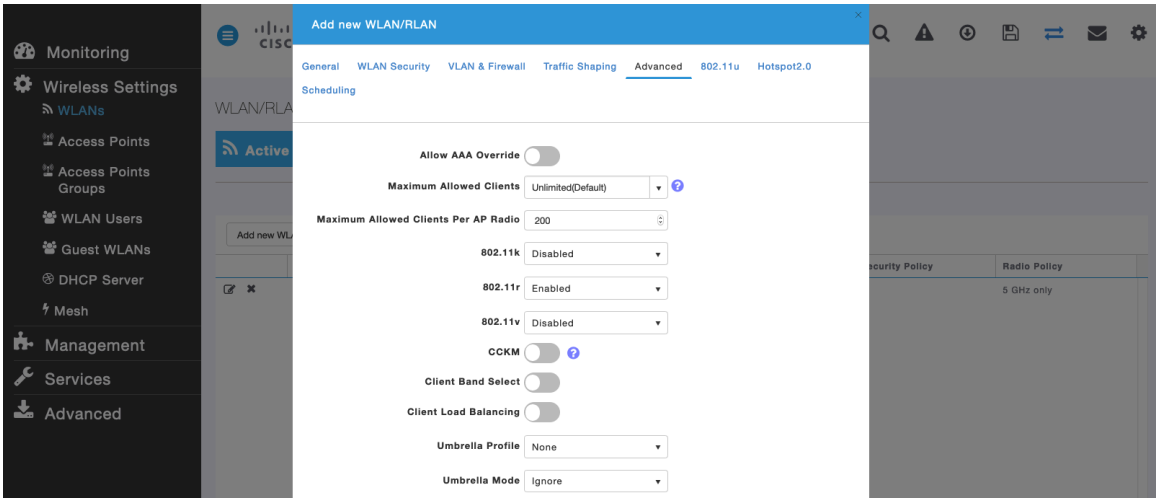




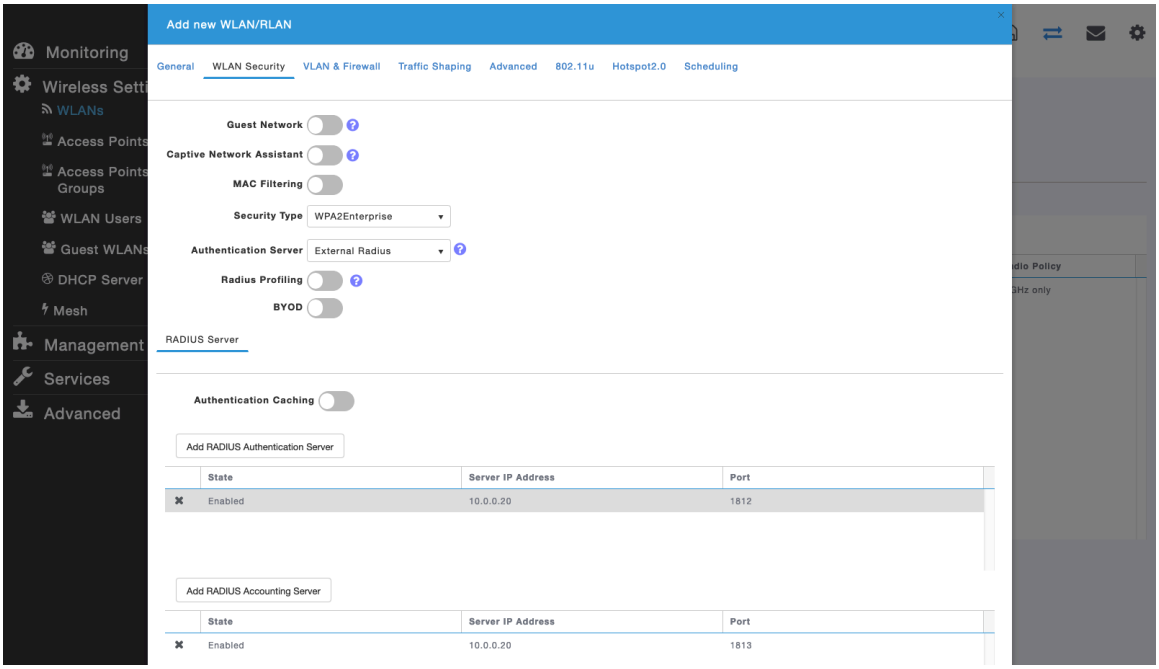
Set **802.11r** to **Enabled** in the **Advanced** tab of the WLAN configuration.

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

It is recommend to enable 802.11k and 802.11v.



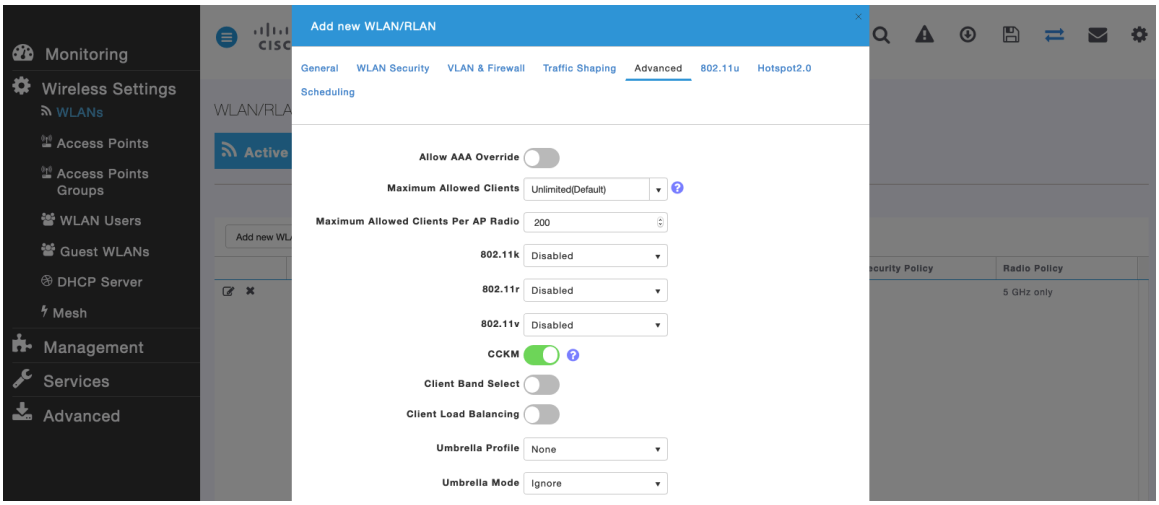
To utilize CCKM for fast secure roaming, set **Security Type** to **WPA2Enterprise**.



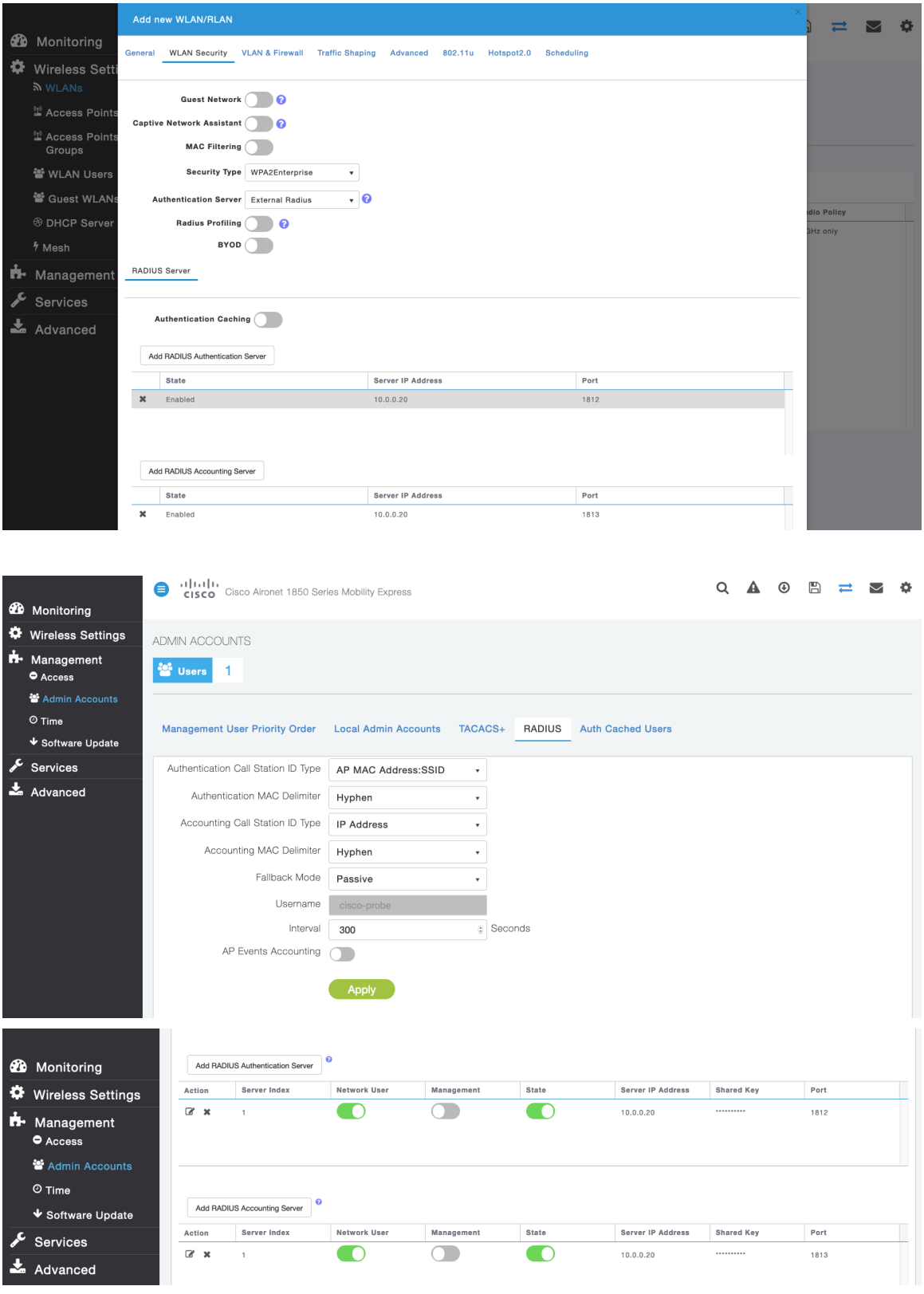
Set **CCKM** to **Enabled** in the **Advanced** tab of the WLAN configuration.

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

It is recommend to enable 802.11k and 802.11v.

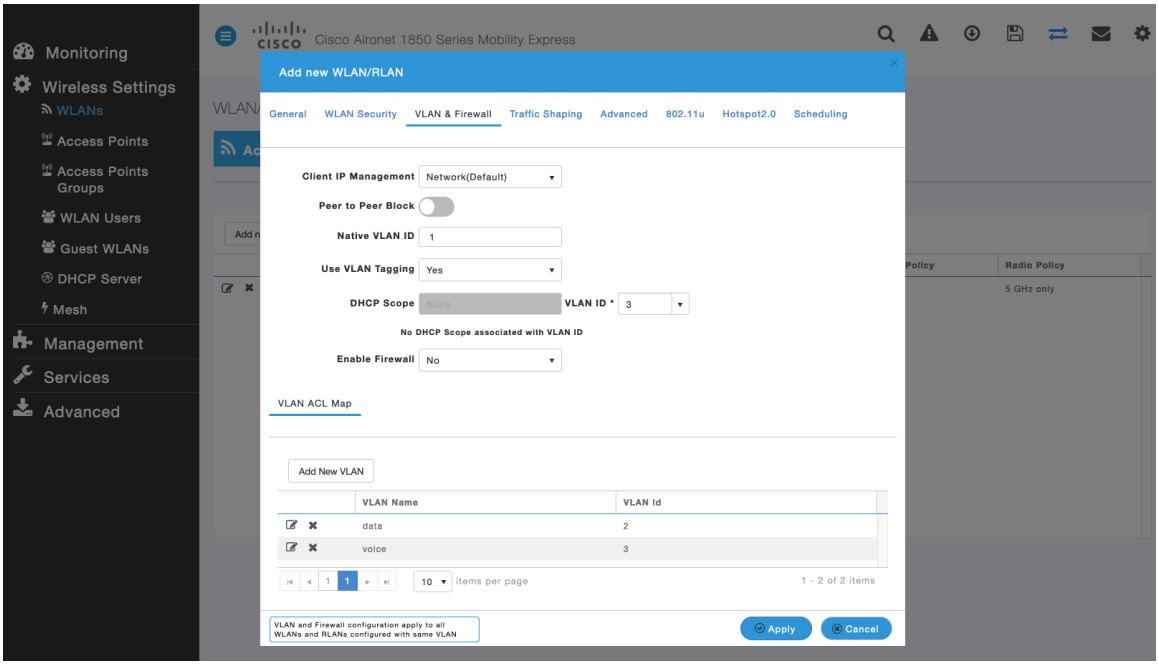


RADIUS Authentication Servers and **Account Servers** can be configured at a per WLAN level to override the global list.

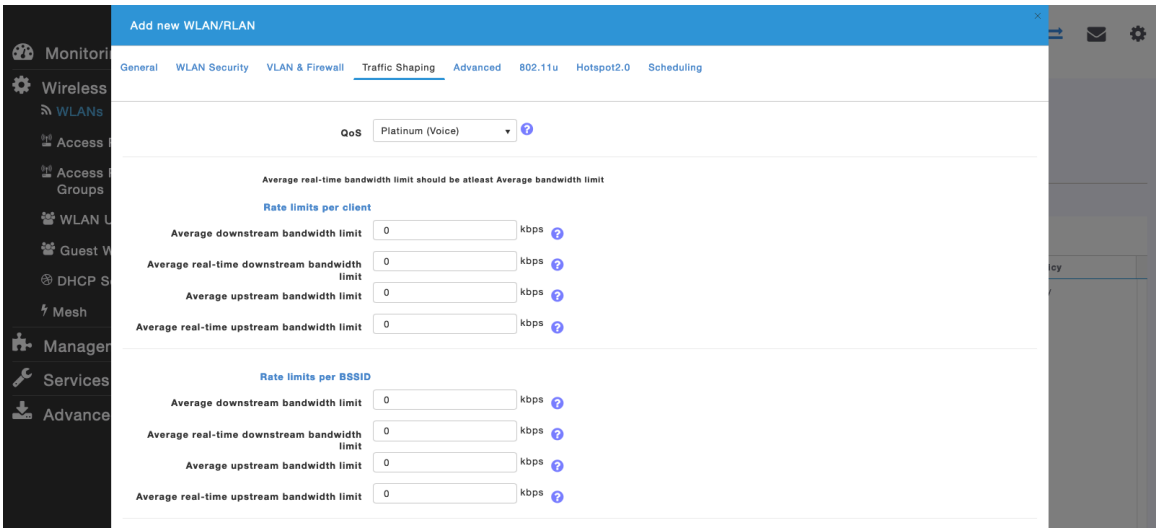


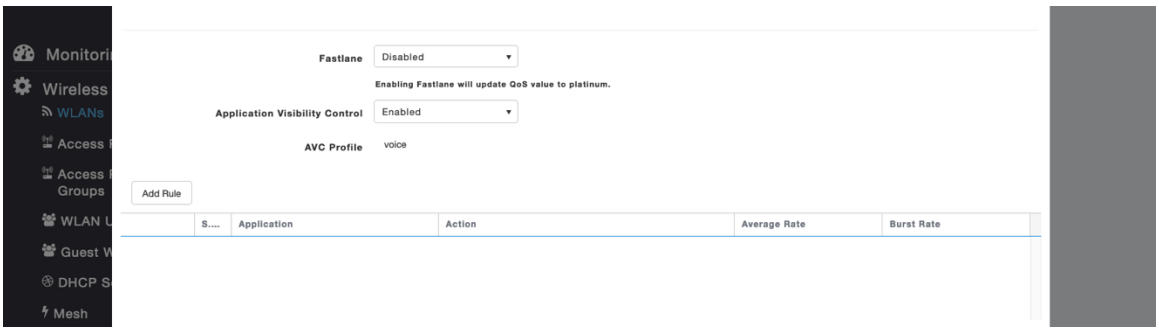
Configure the **Native VLAN ID** and **VLAN ID** for the WLAN as necessary.

Ensure **Peer to Peer Block** is disabled.

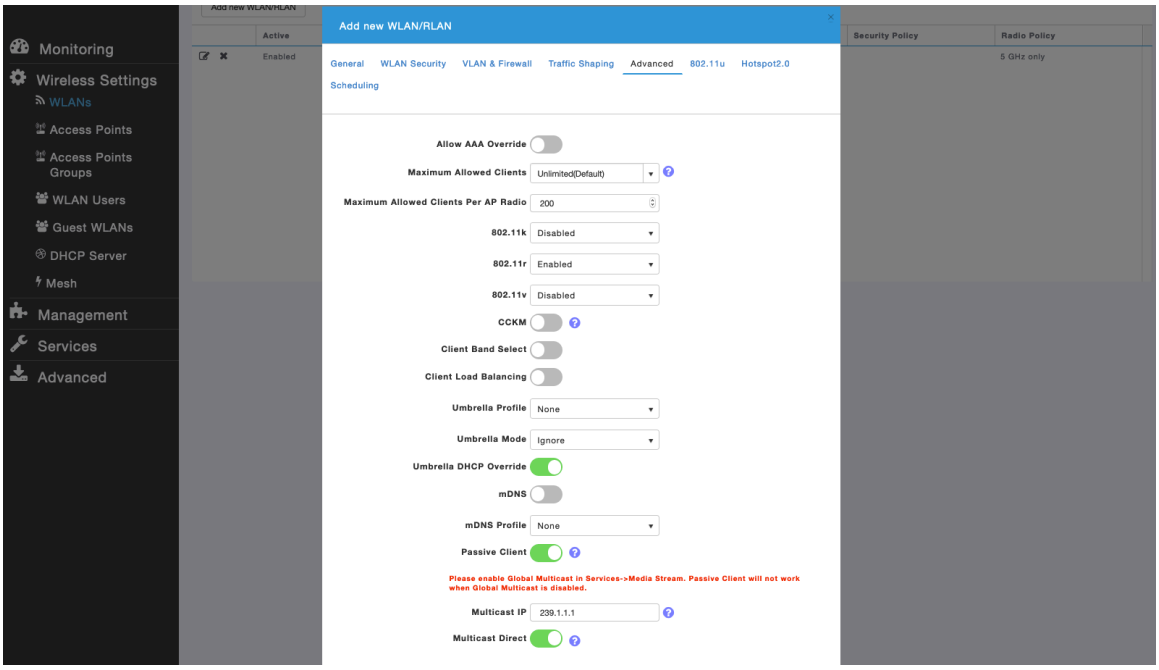


Ensure **Platinum (Voice)** is selected for **QoS**.



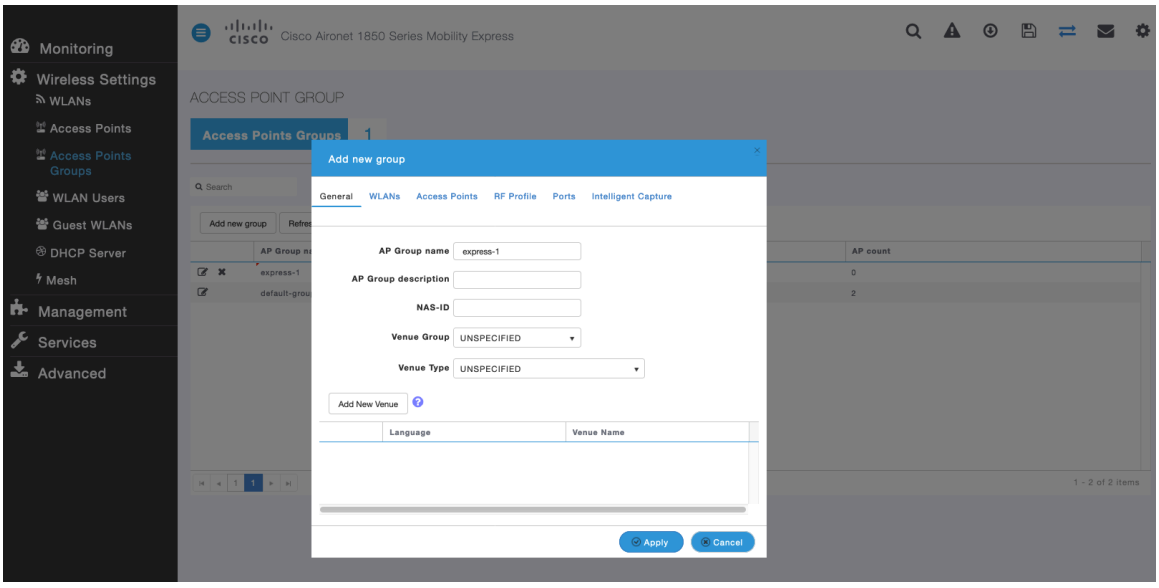


The **Maximum Allowed Clients** and **Maximum Allowed Clients Per AP Radio** can be configured as necessary.

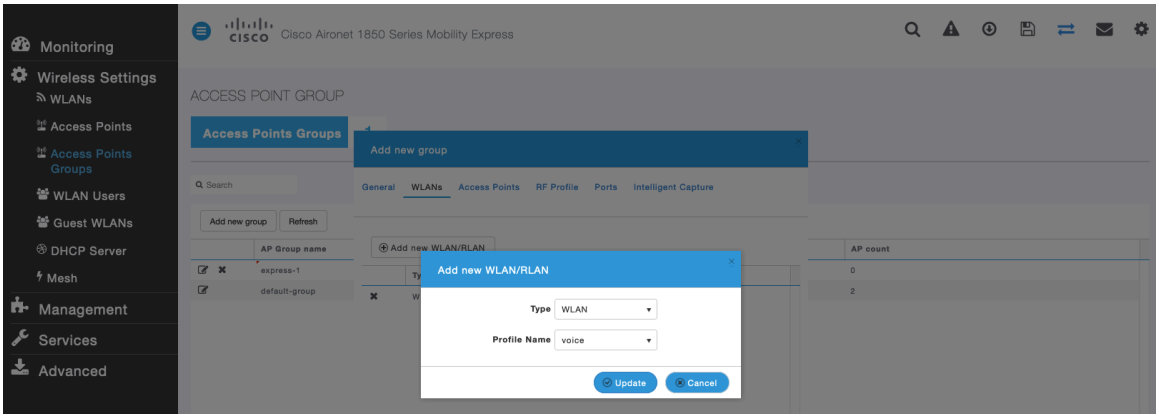


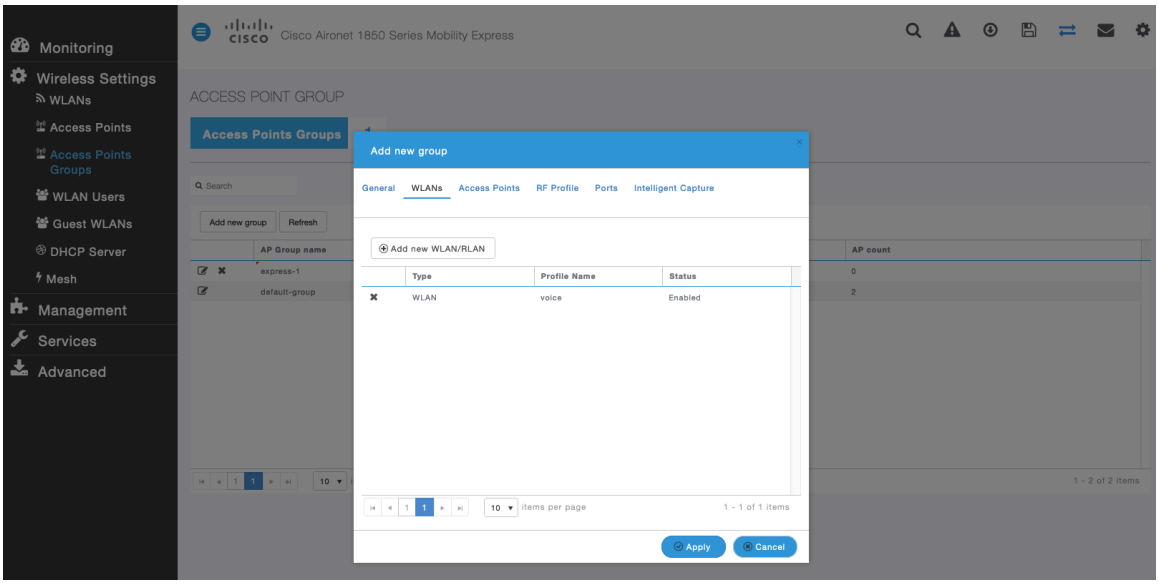
AP Groups

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



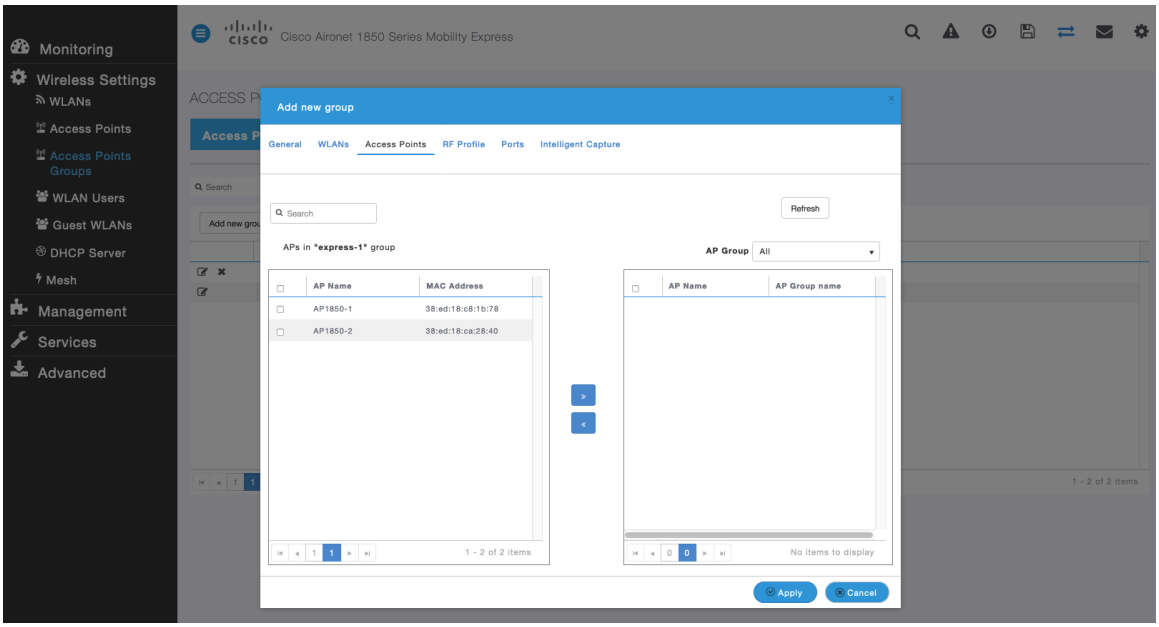
On the **WLANs** tab, select the desired WLANs and interfaces to map to then select **Add**.



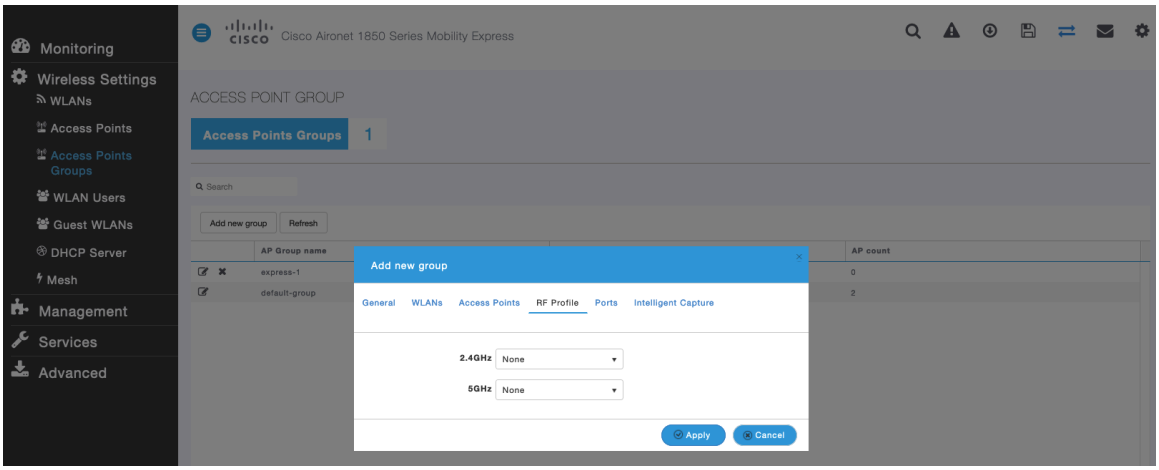


On the **Access Points** tab, select the desired access points then select **Apply**.

Those access points will then reboot.



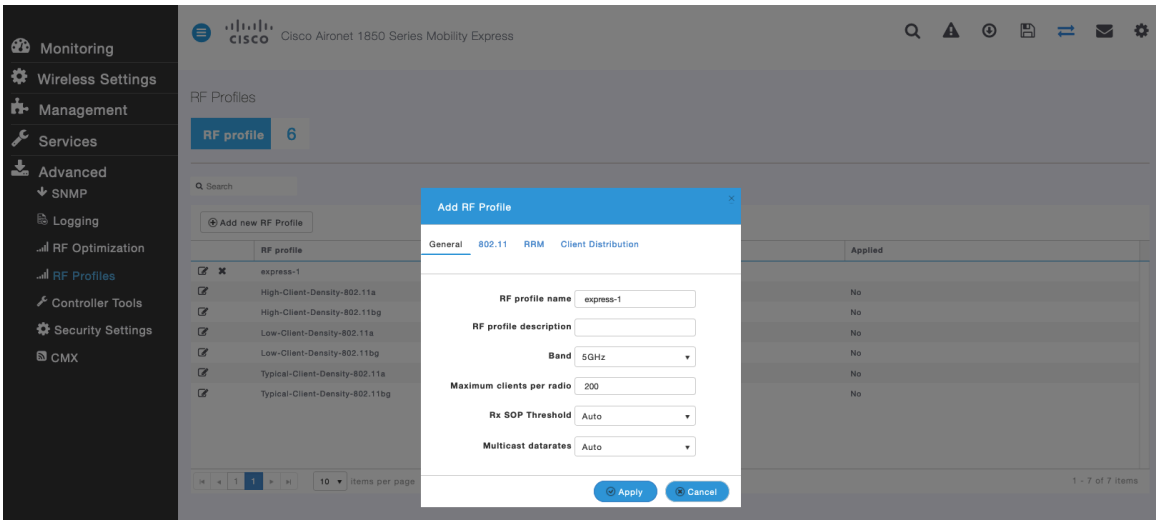
On the **RF Profile** tab, select the desired **2.4GHz** or **5GHz** RF Profile, then select **Apply**.



RF Profiles

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

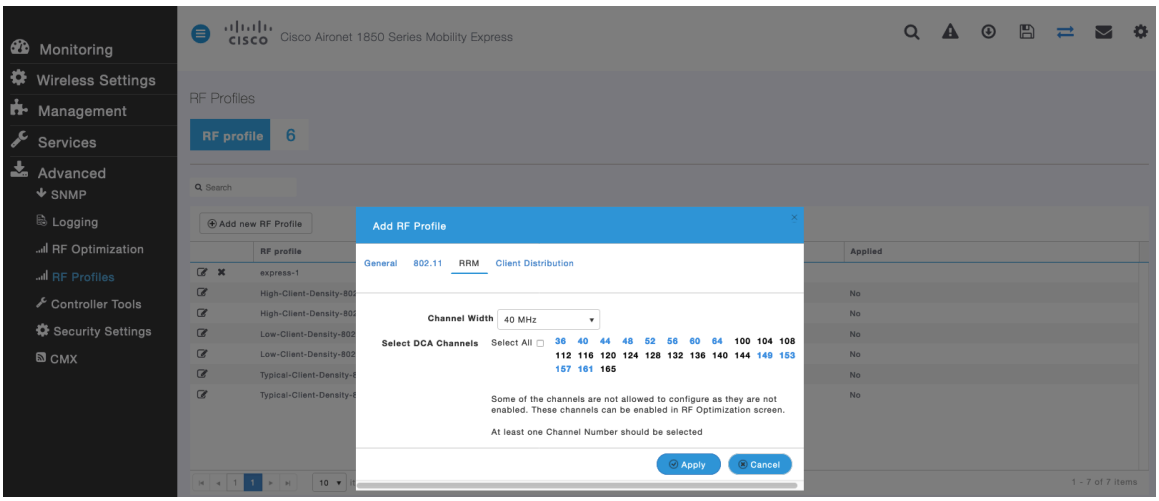
When creating an RF Profile, the **RF Profile Name** and **Radio Policy** must be defined.
Select **5GHZ** or **2.4GHz** for the **Radio Policy**.
Maximum clients per radio, **Multicast data rates**, and **Rx Sop Threshold** can be configured as necessary.
It is recommended to use the default value (**Auto**) for **Rx Sop Threshold**.



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

Is recommended to enable 12 Mbps as **Mandatory** and 18 Mbps and higher as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

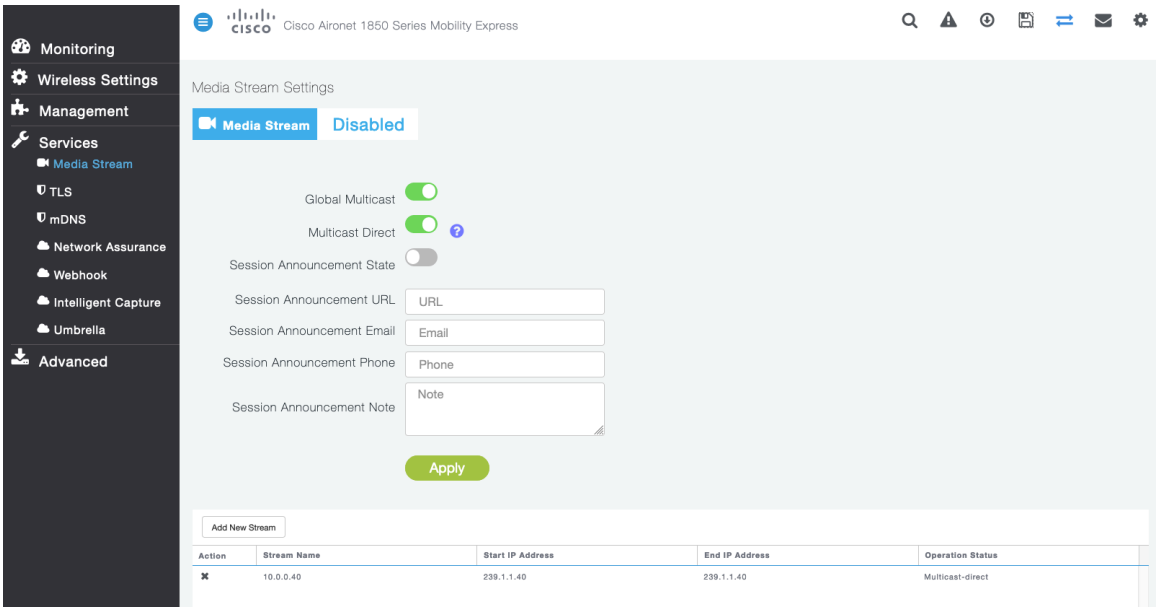
On the **RRM** tab, the **Channel Width** settings and **DCA Channels** can be configured.



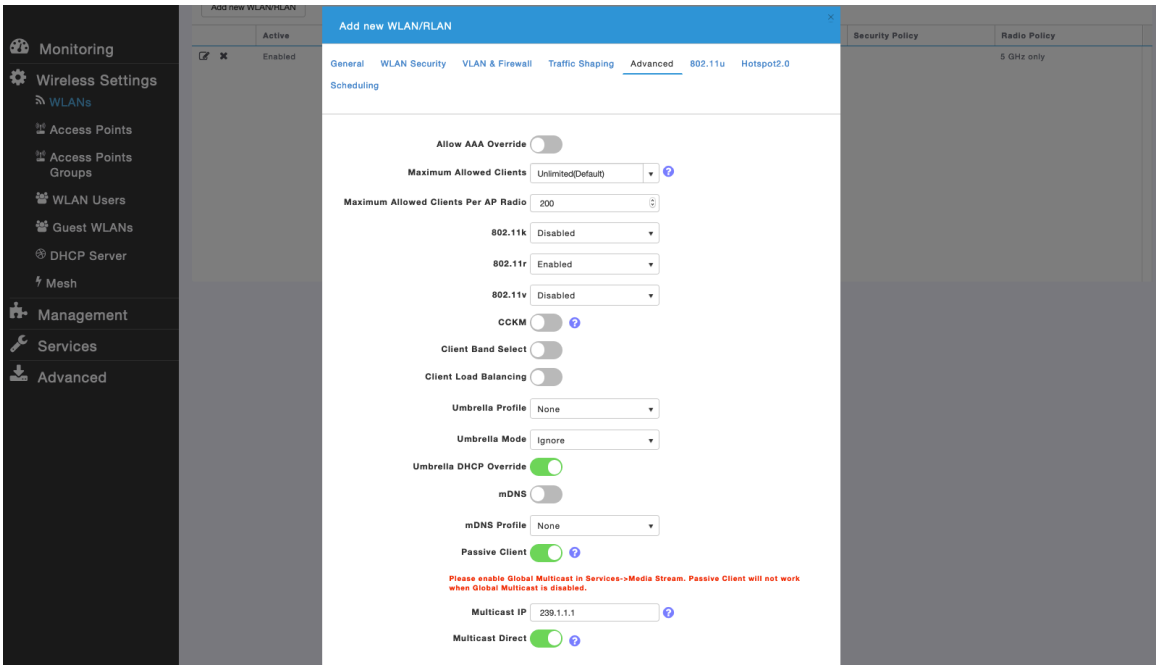
Multicast Direct

In the **Media Stream** settings, enable **Global Multicast** and **Multicast Direct**.

Then configure the streams.



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



Cisco Autonomous Access Points

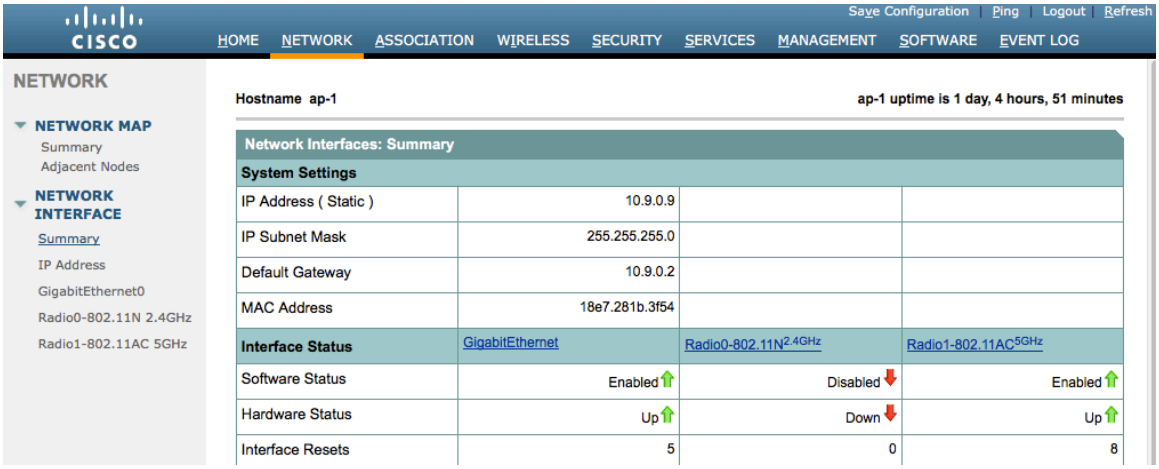
When configuring Cisco Autonomous Access Points, use the following guidelines:

- Ensure **802.11r (FT)** or **CCKM** is **Enabled**
- Recommended to set **802.11k** to **Enabled**
- Recommended to set **802.11v** to **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 Wireless Phone 840 and 860 operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

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



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

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

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

For Cisco Autonomous Access Points, select Dynamic Frequency Selection (DFS) to use auto channel selection.

When DFS is enabled, enable at least one band (bands 1-4).

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

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

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

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

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

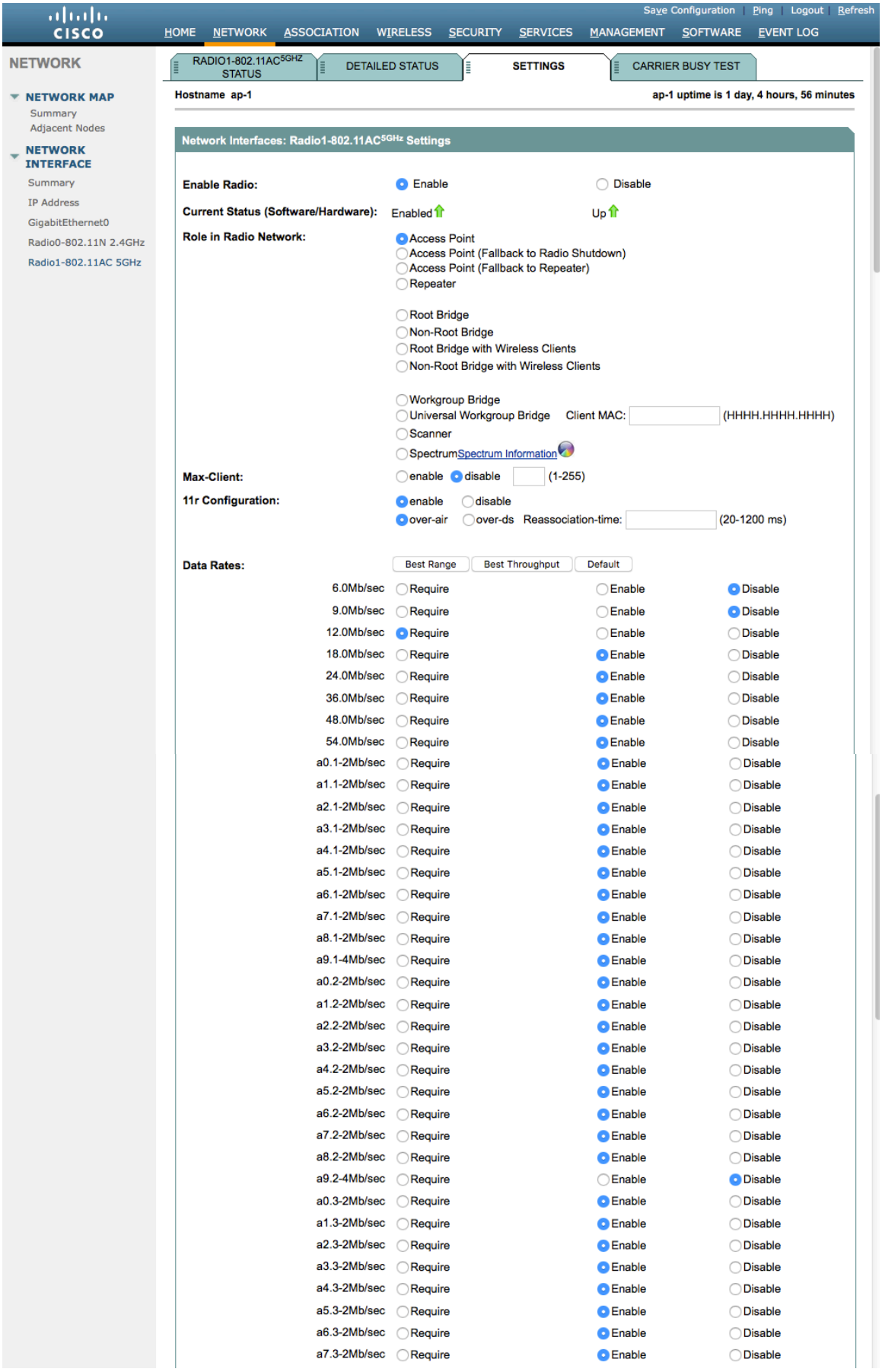
It is recommended to utilize the same channel width for all access points.

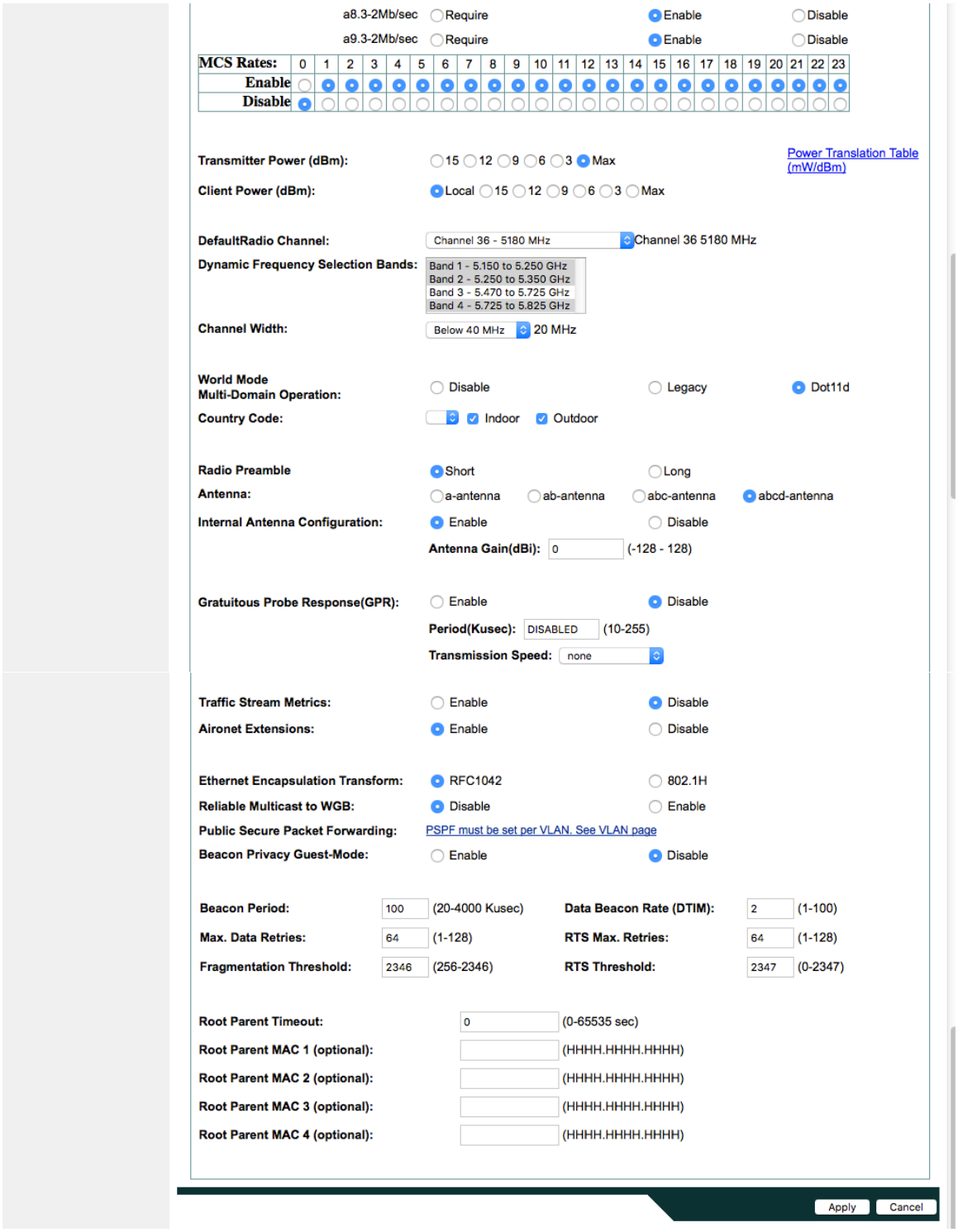
Ensure **Client Power** is configured properly. Do not use default setting of **Max** power for client power on Cisco Autonomous Access Points as that will not advertise DTPC to the client.

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

Ensure **Aironet Extensions** is enabled.

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


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
NETWORK
NETWORK MAP
Summary
Adjacent Nodes
NETWORK INTERFACE
Summary
IP Address
GigabitEthernet0
Radio0-802.11N 2.4GHz
Radio1-802.11AC 5GHz
RADIO1-802.11AC5GHZ STATUS
DETAILED STATUS
SETTINGS
CARRIER BUSY TEST
Hostname ap-1
ap-1 uptime is 1 day, 4 hours, 56 minutes
Network Interfaces: Radio1-802.11AC5GHz Settings
Enable Radio: Enable Disable
Current Status (Software/Hardware): Enabled Up
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
Workgroup Bridge
Universal Workgroup Bridge Client MAC: (HHHH.HHHH.HHHH)
Scanner
SpectrumSpectrum Information
Max-Client: enable disable (1-255)
11r Configuration: enable disable
over-air over-ds Reassociation-time: (20-1200 ms)
Data Rates: Best Range Best Throughput Default
6.0Mb/sec Require Enable Disable
9.0Mb/sec Require Enable Disable
12.0Mb/sec Require Enable Disable
18.0Mb/sec Require Enable Disable
24.0Mb/sec Require Enable Disable
36.0Mb/sec Require Enable Disable
48.0Mb/sec Require Enable Disable
54.0Mb/sec Require Enable Disable
a0.1-2Mb/sec Require Enable Disable
a1.1-2Mb/sec Require Enable Disable
a2.1-2Mb/sec Require Enable Disable
a3.1-2Mb/sec Require Enable Disable
a4.1-2Mb/sec Require Enable Disable
a5.1-2Mb/sec Require Enable Disable
a6.1-2Mb/sec Require Enable Disable
a7.1-2Mb/sec Require Enable Disable
a8.1-2Mb/sec Require Enable Disable
a9.1-4Mb/sec Require Enable Disable
a0.2-2Mb/sec Require Enable Disable
a1.2-2Mb/sec Require Enable Disable
a2.2-2Mb/sec Require Enable Disable
a3.2-2Mb/sec Require Enable Disable
a4.2-2Mb/sec Require Enable Disable
a5.2-2Mb/sec Require Enable Disable
a6.2-2Mb/sec Require Enable Disable
a7.2-2Mb/sec Require Enable Disable
a8.2-2Mb/sec Require Enable Disable
a9.2-4Mb/sec Require Enable Disable
a0.3-2Mb/sec Require Enable Disable
a1.3-2Mb/sec Require Enable Disable
a2.3-2Mb/sec Require Enable Disable
a3.3-2Mb/sec Require Enable Disable
a4.3-2Mb/sec Require Enable Disable
a5.3-2Mb/sec Require Enable Disable
a6.3-2Mb/sec Require Enable Disable
a7.3-2Mb/sec Require Enable Disable



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

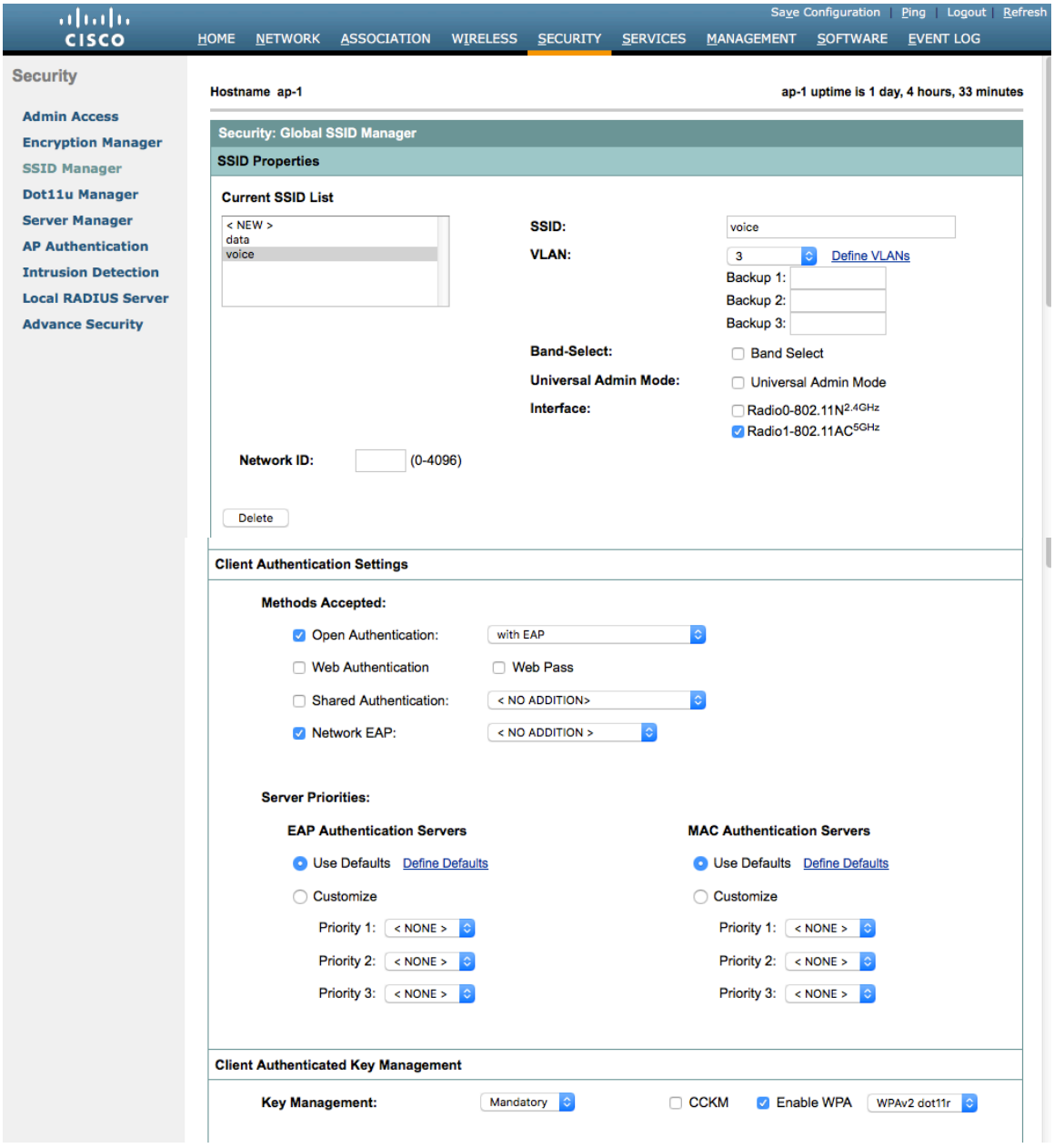
It is recommended to have a separate SSID for the Cisco Wireless Phone 840 and 860.

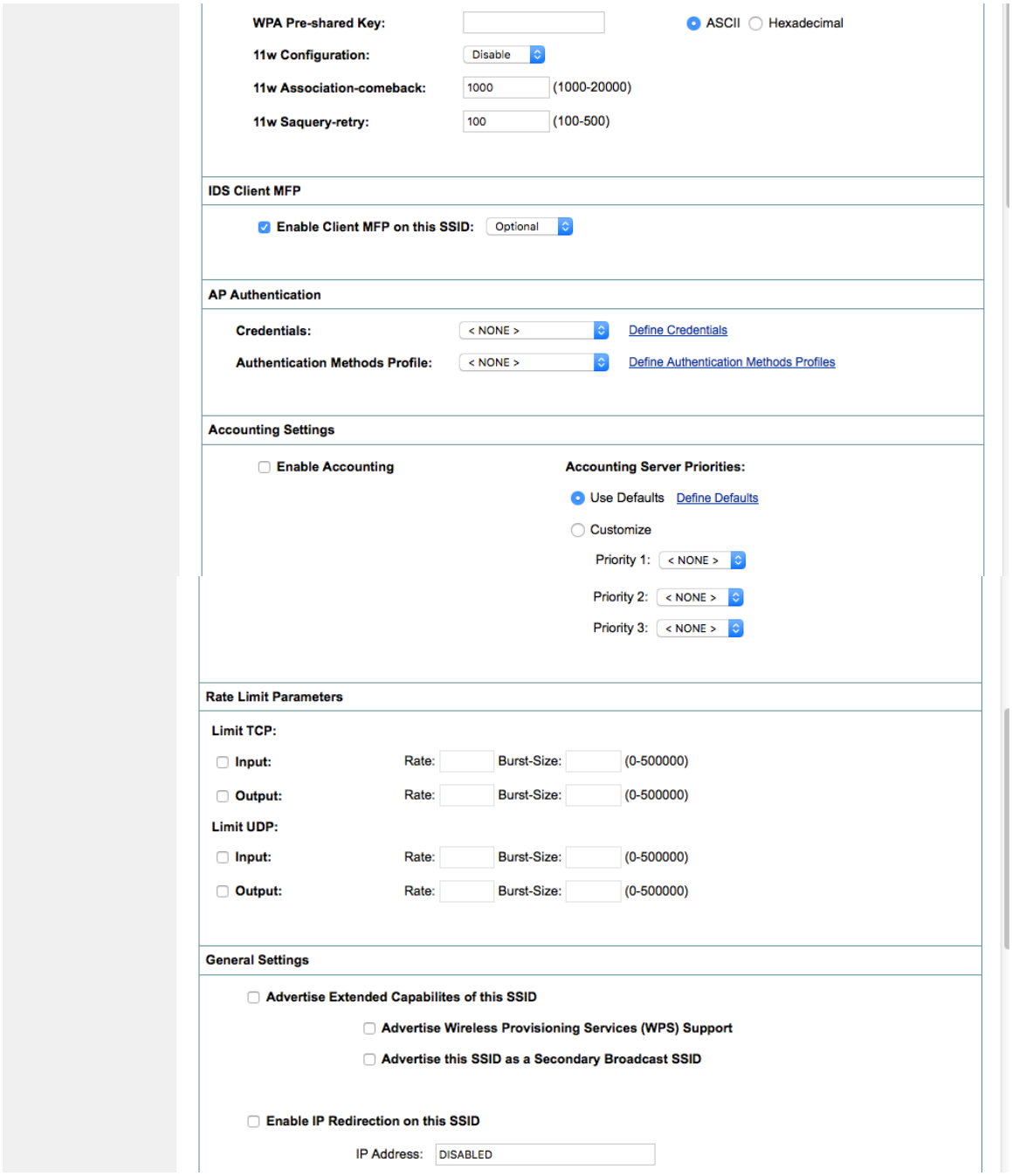
However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

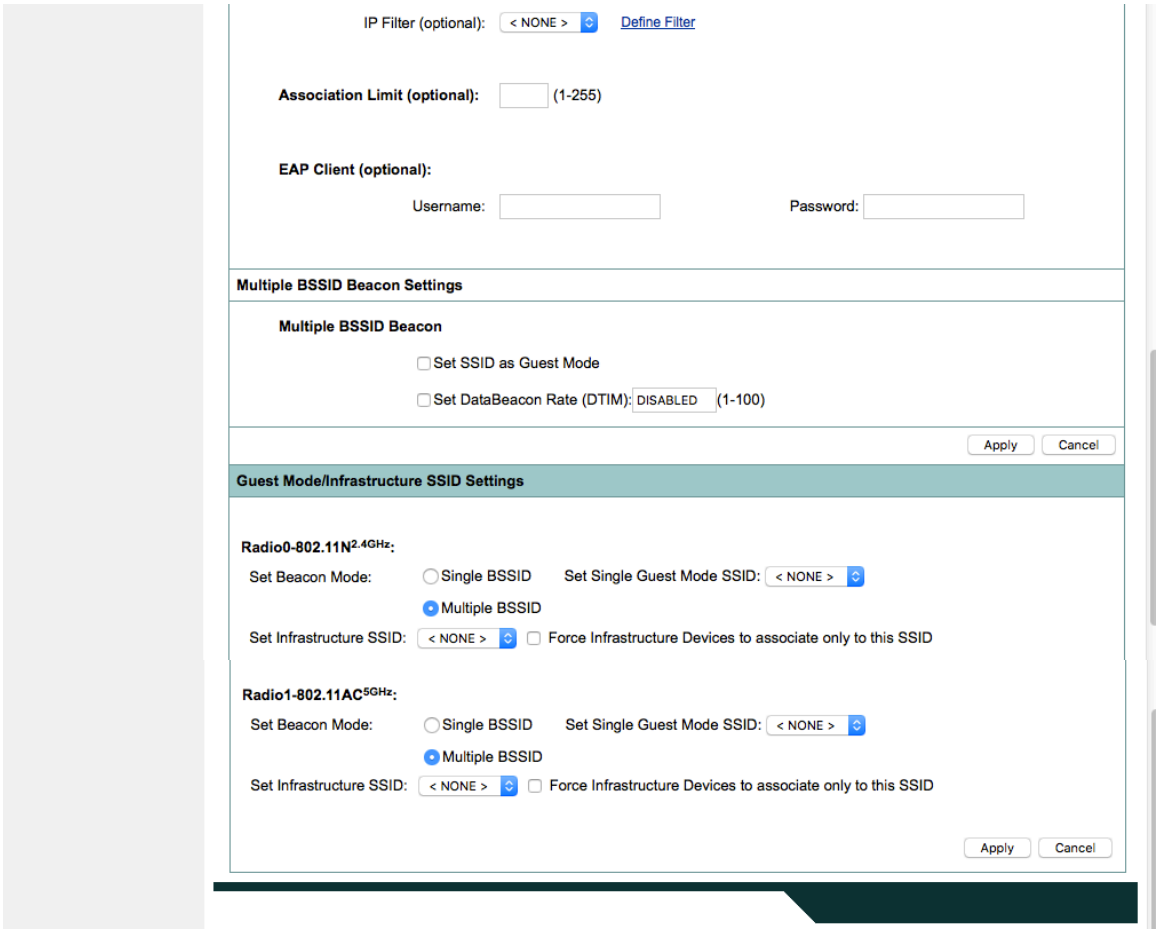
The SSID to be used by the Cisco Wireless Phone 840 and 860 can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

Enable **WPA2** key management.

Ensure either **11r** or **CCKM** is enabled, where 11r is recommended.

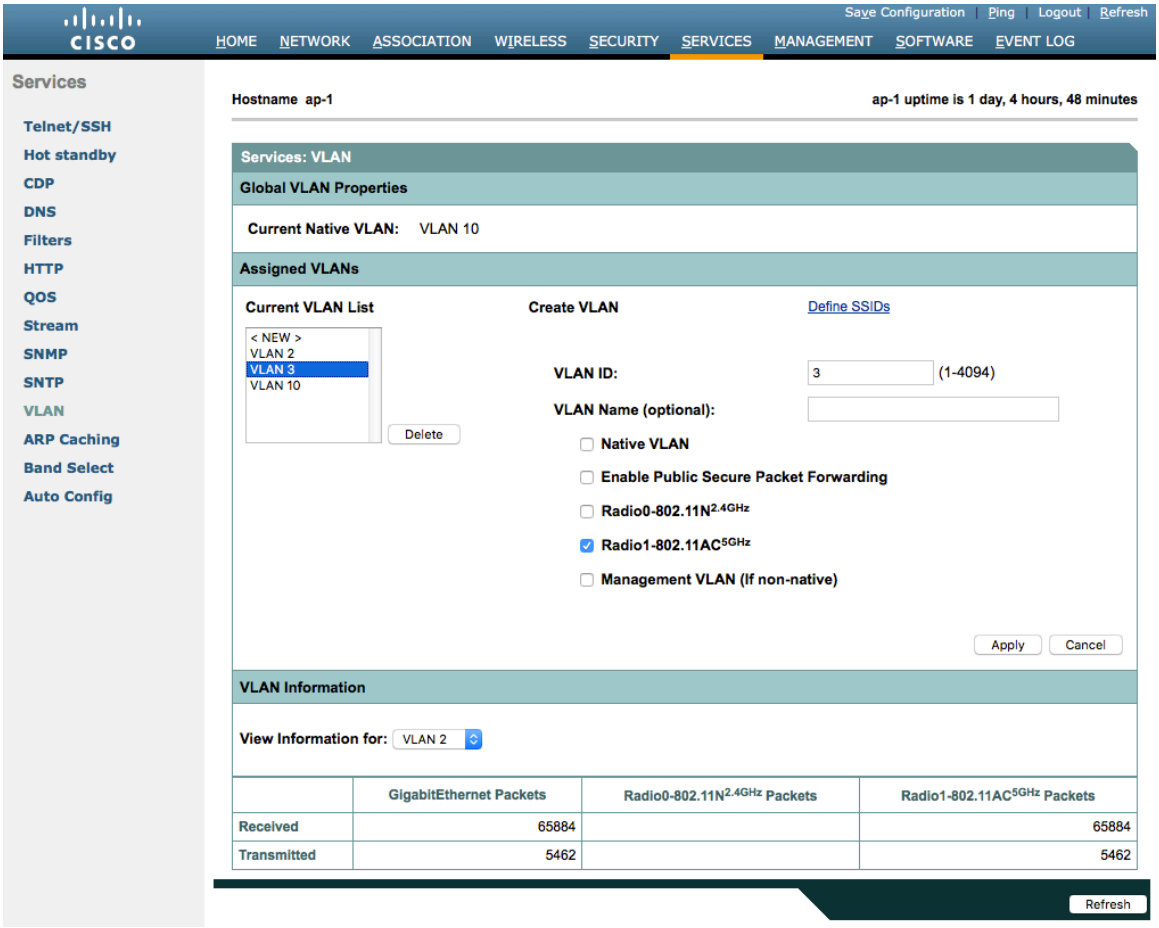



WPA Pre-shared Key:
ASCII
Hexadecimal
11w Configuration:
Disable
11w Association-comeback:
1000
(1000-20000)
11w Saquery-retry:
100
(100-500)
IDS Client MFP
Enable Client MFP on this SSID:
Optional
AP Authentication
Credentials:
< NONE >
Define Credentials
Authentication Methods Profile:
< NONE >
Define Authentication Methods Profiles
Accounting Settings
Enable Accounting
Accounting Server Priorities:
Use Defaults
Define Defaults
Customize
Priority 1:
< NONE >
Priority 2:
< NONE >
Priority 3:
< NONE >
Rate Limit Parameters
Limit TCP:
Input:
Rate:
Burst-Size:
(0-500000)
Output:
Rate:
Burst-Size:
(0-500000)
Limit UDP:
Input:
Rate:
Burst-Size:
(0-500000)
Output:
Rate:
Burst-Size:
(0-500000)
General Settings
Advertise Extended Capabilites 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

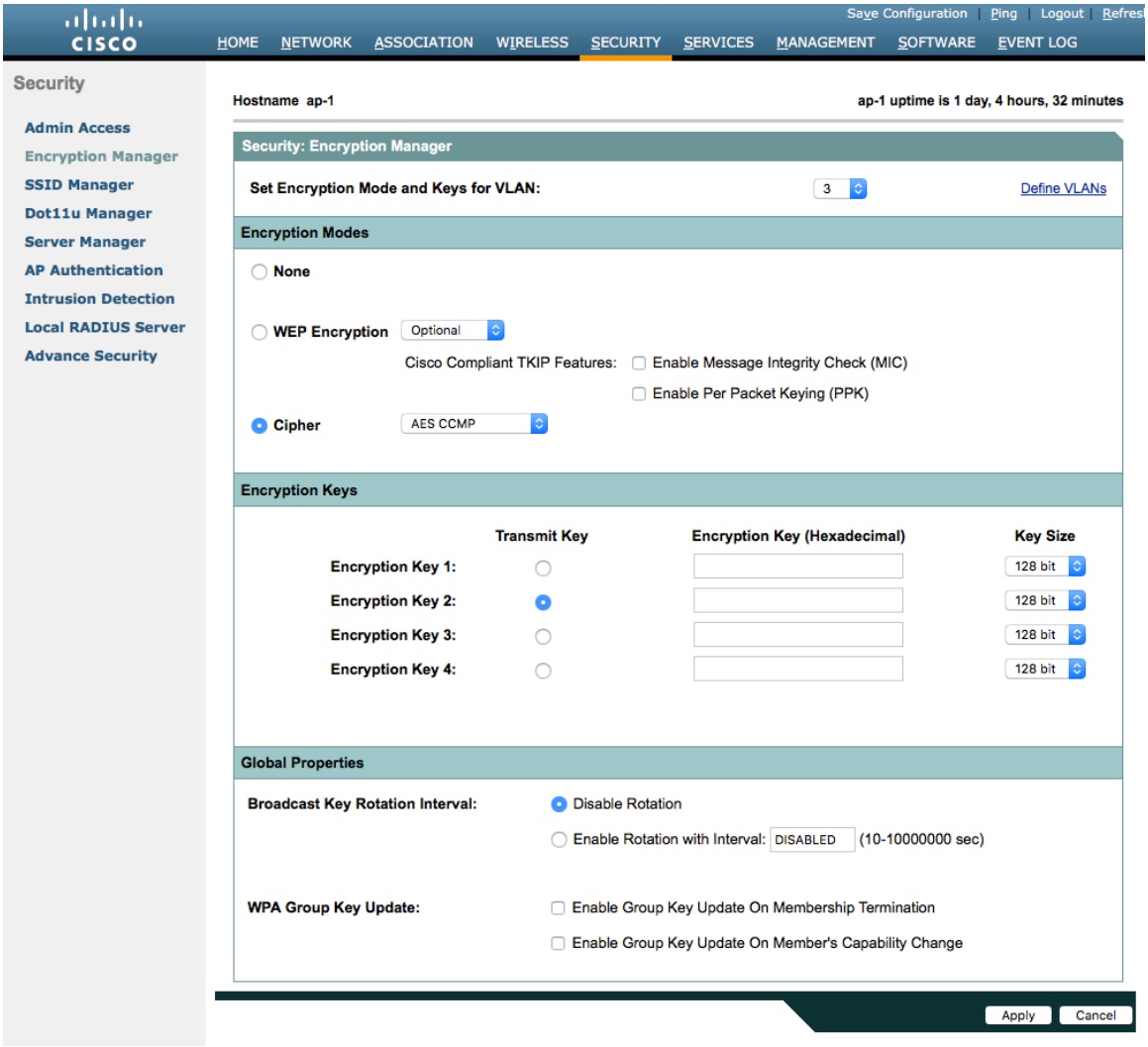


Segment wireless voice and data into separate VLANs.

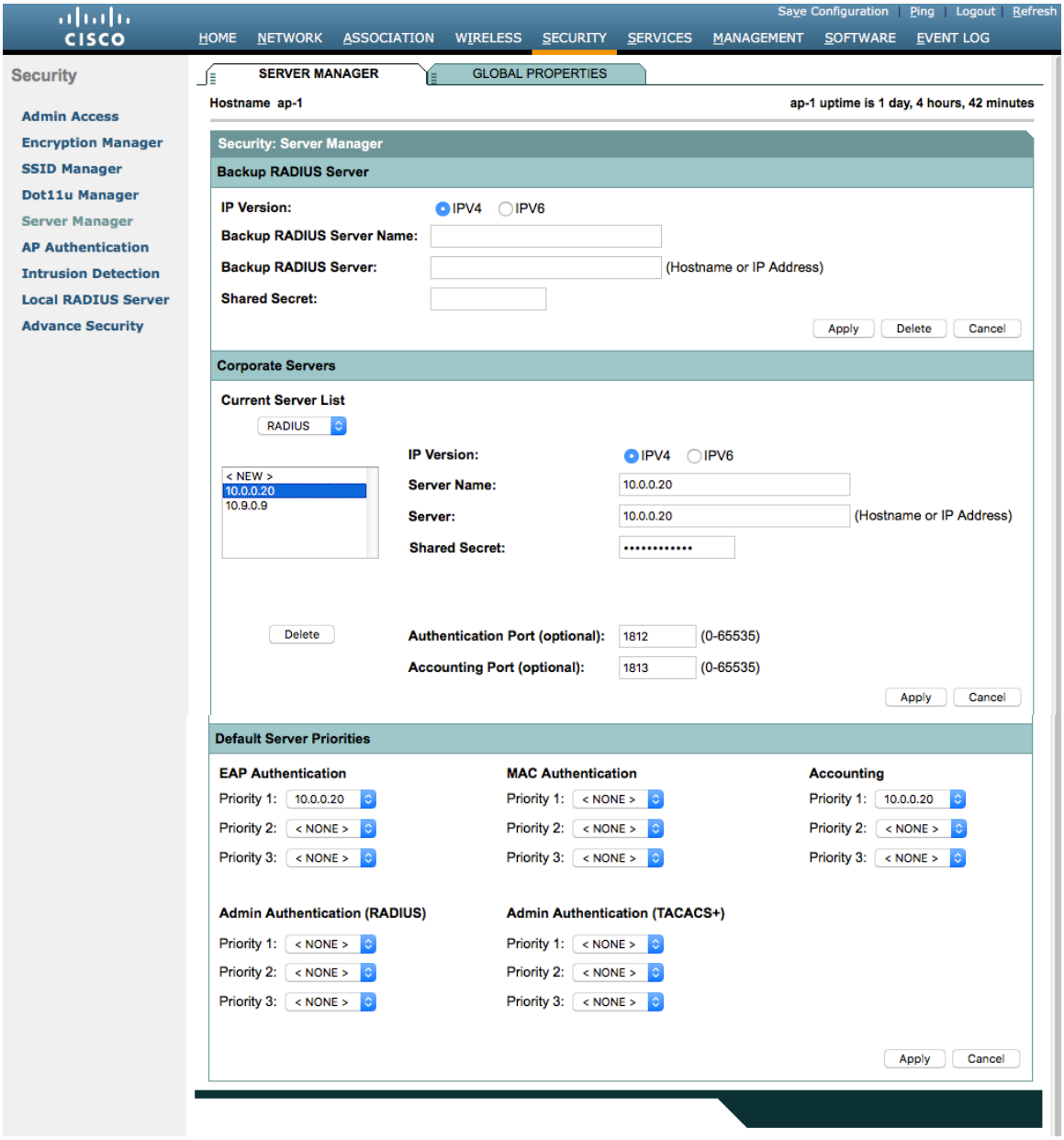
Ensure that Public Secure Packet Forwarding (PSPF) is not enabled for the voice VLAN as this will prevent clients from communicating directly when associated to the same access point. If PSPF is enabled, then the result will be no way audio.



Ensure **AES** is selected for encryption type.



Configure the RADIUS servers to be used for authentication and accounting.

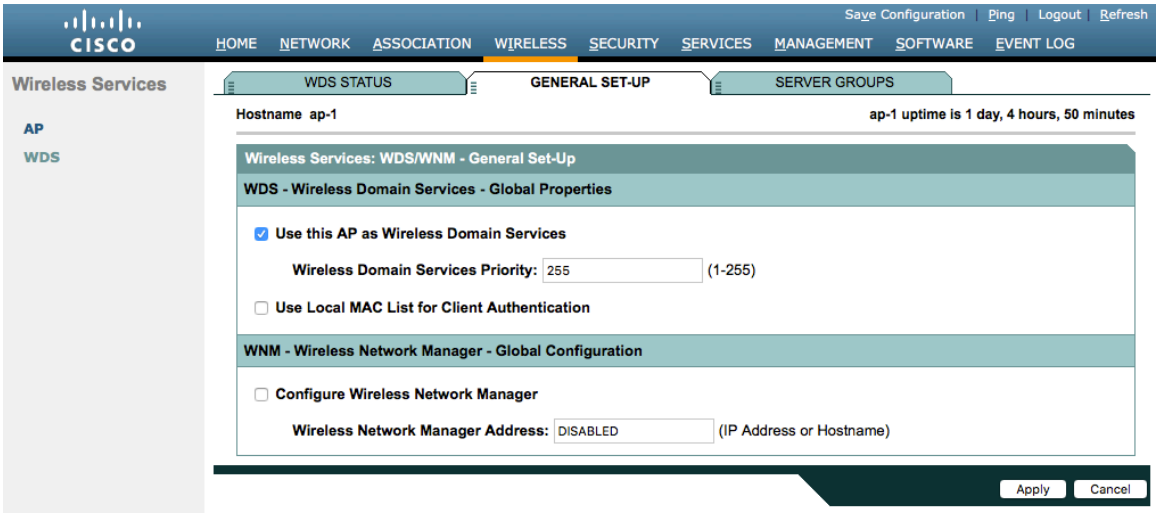


Wireless Domain Services (WDS)

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.

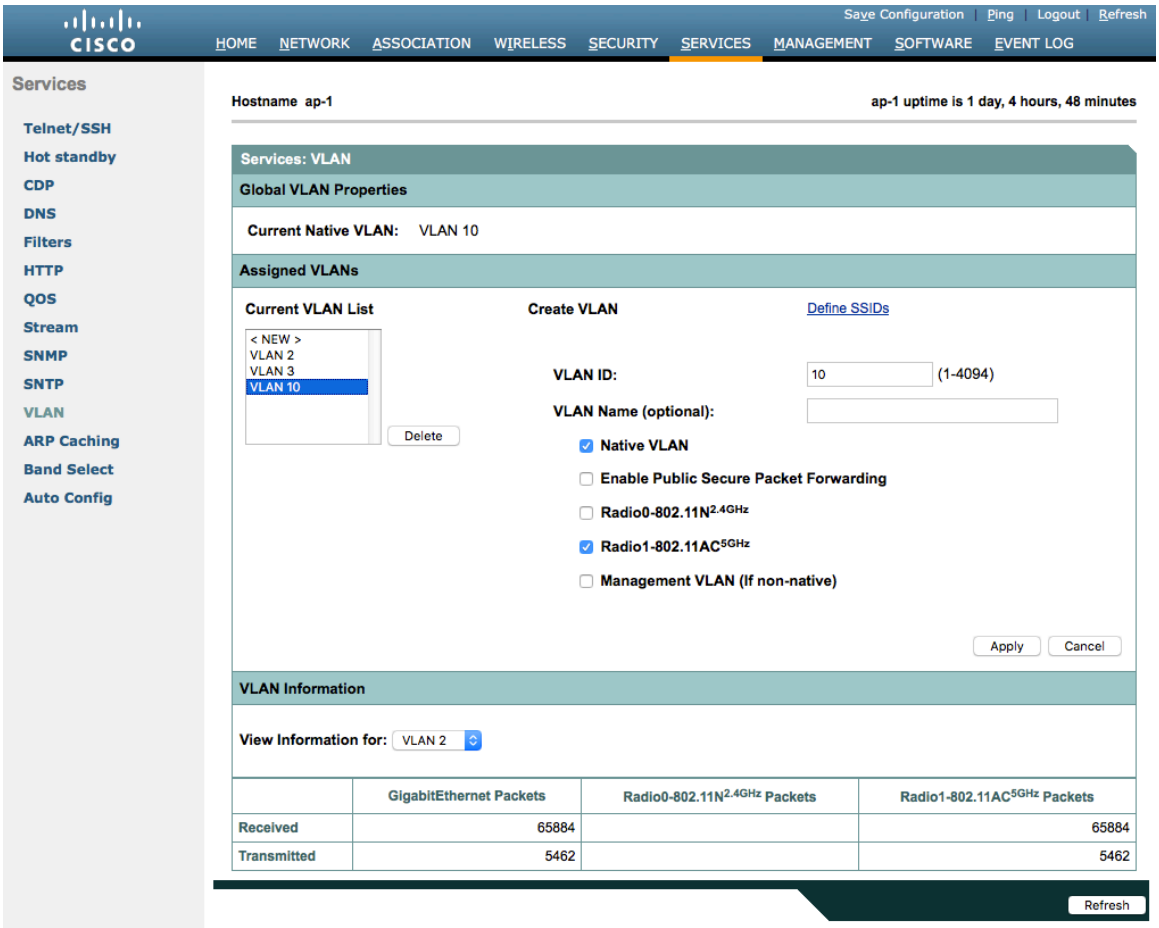
Configure the primary WDS server with the highest priority (e.g. 255) and the backup WDS server with a lower priority (e.g. 254).



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.

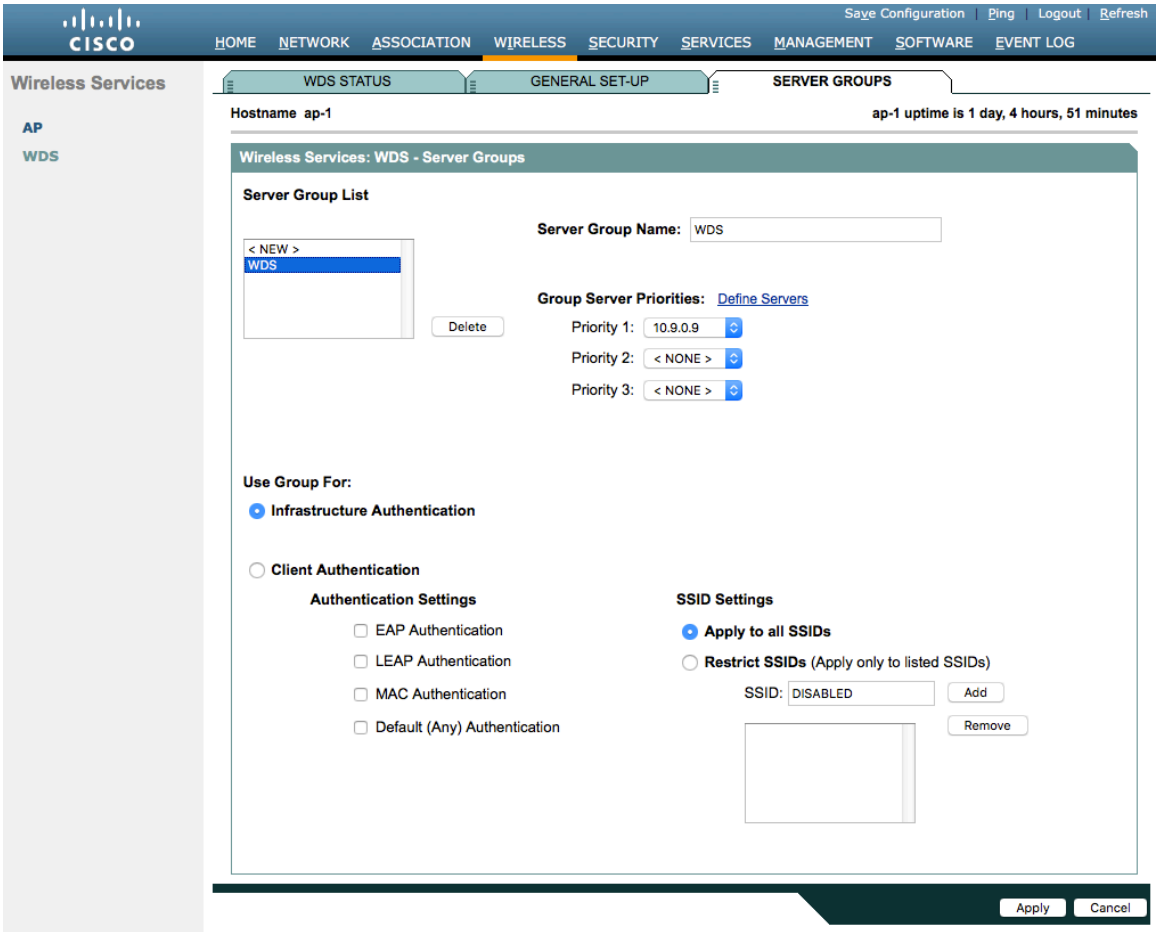


Server groups for Wireless Domain Services must be defined.

First, define the server group to be used for infrastructure authentication.

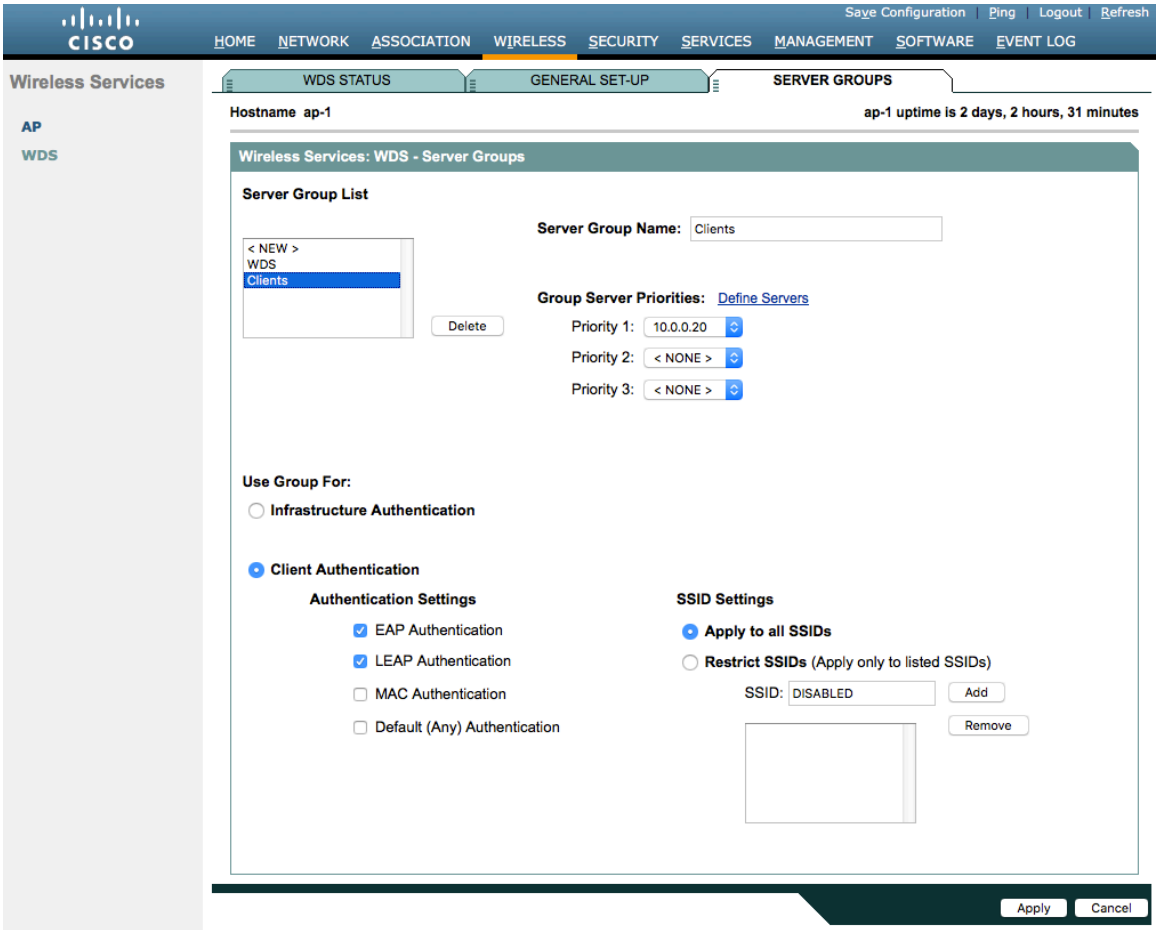
Is recommended to use local RADIUS for infrastructure authentication.

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.

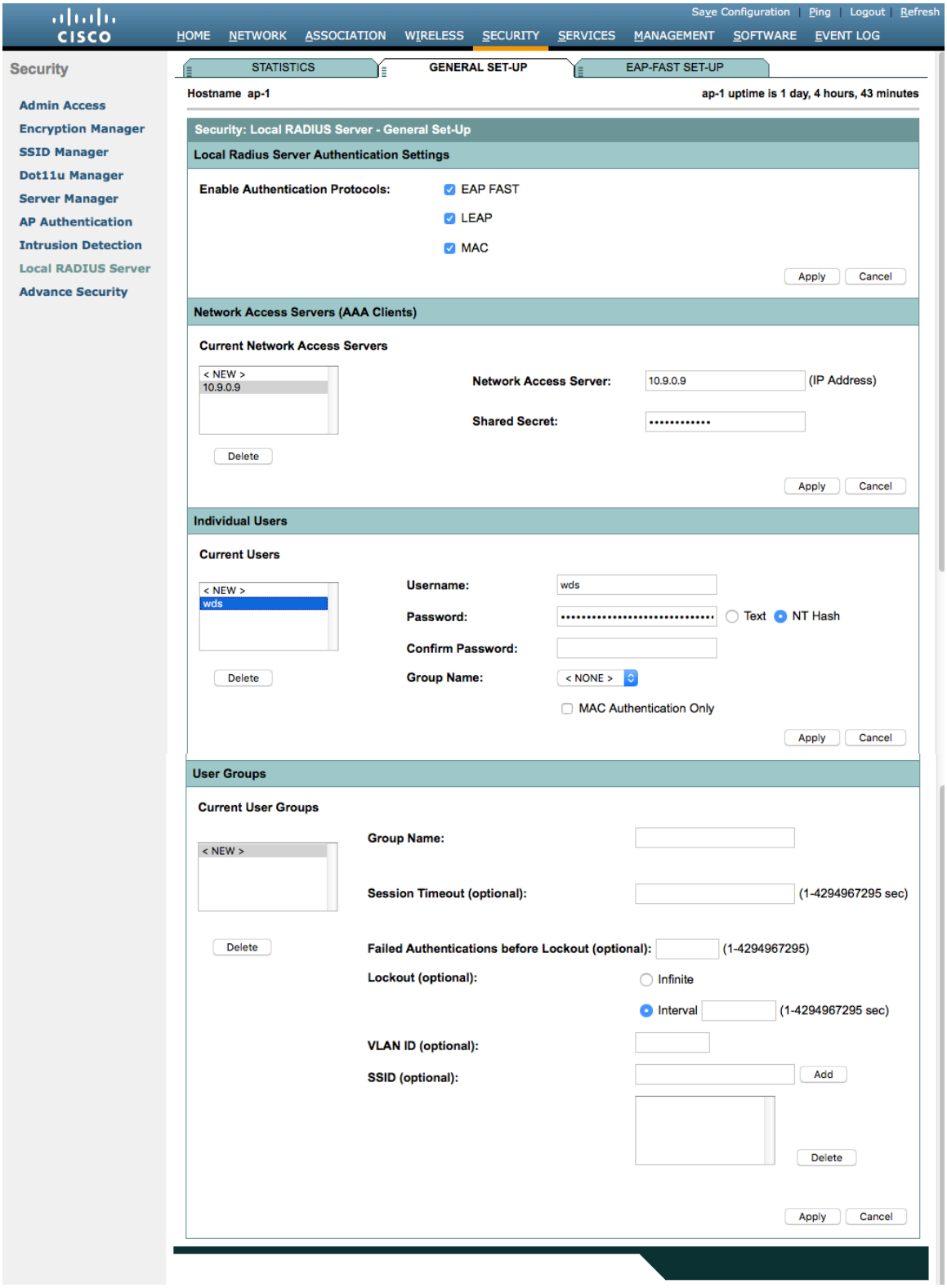


To utilize local RADIUS for infrastructure authentication, enable all authentication protocols.

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.

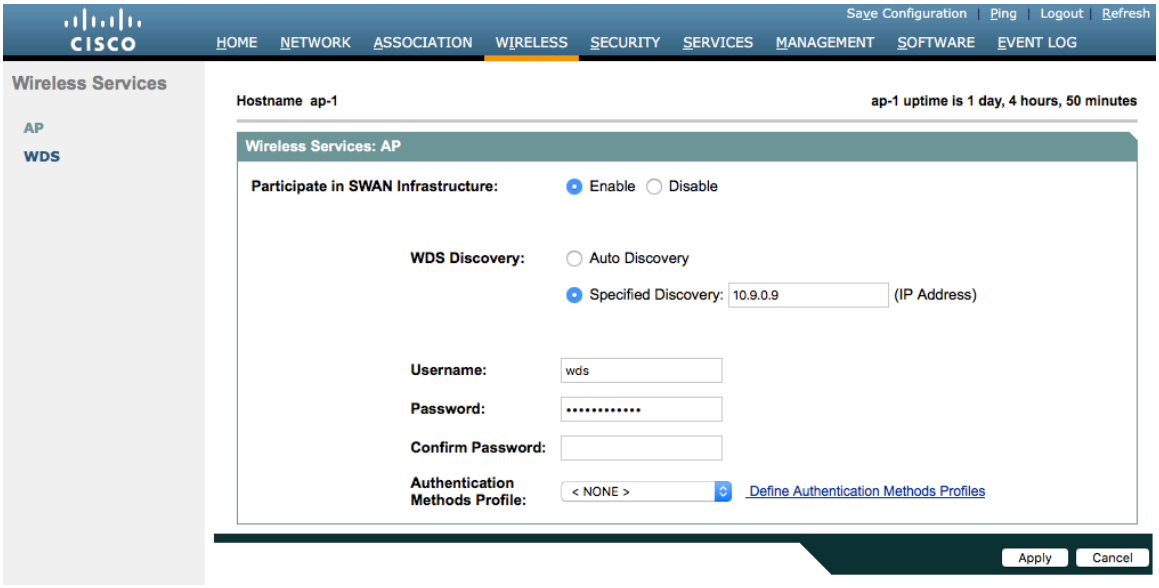


Once the desired access points have been configured successfully to enable Wireless Domain Services, then all access points including those serving as WDS servers need to be configured to be able to authenticate to the WDS servers.

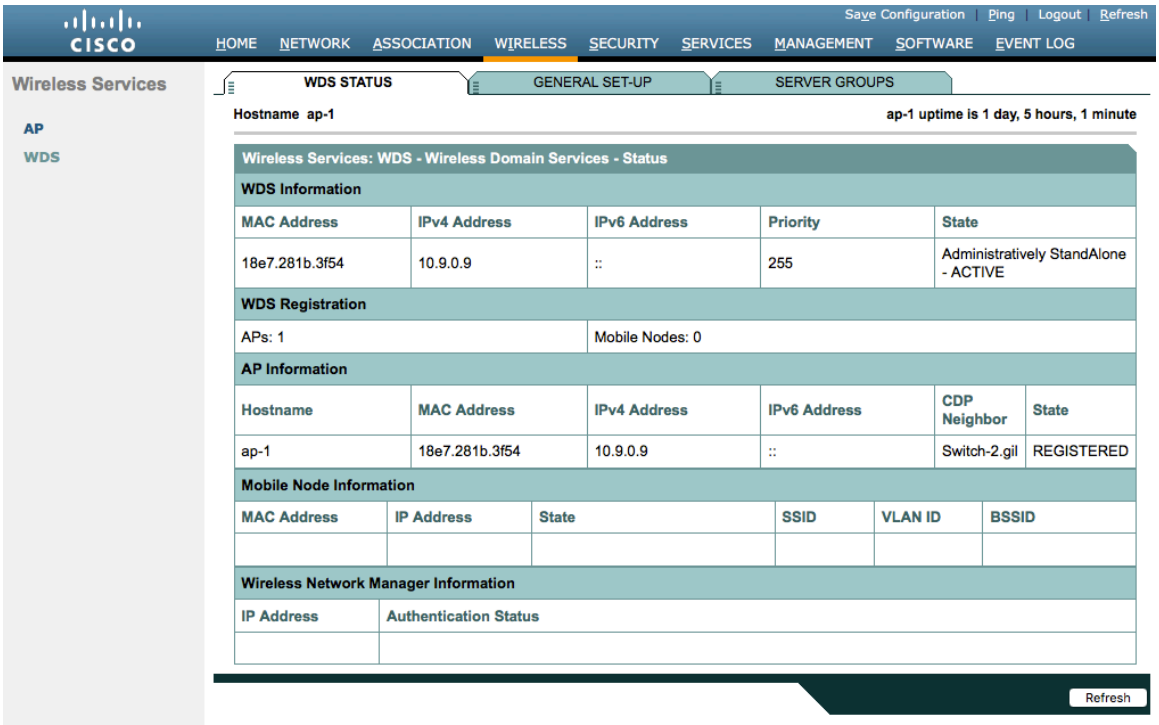
Enable **Participate in SWAN Infrastructure**.

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.



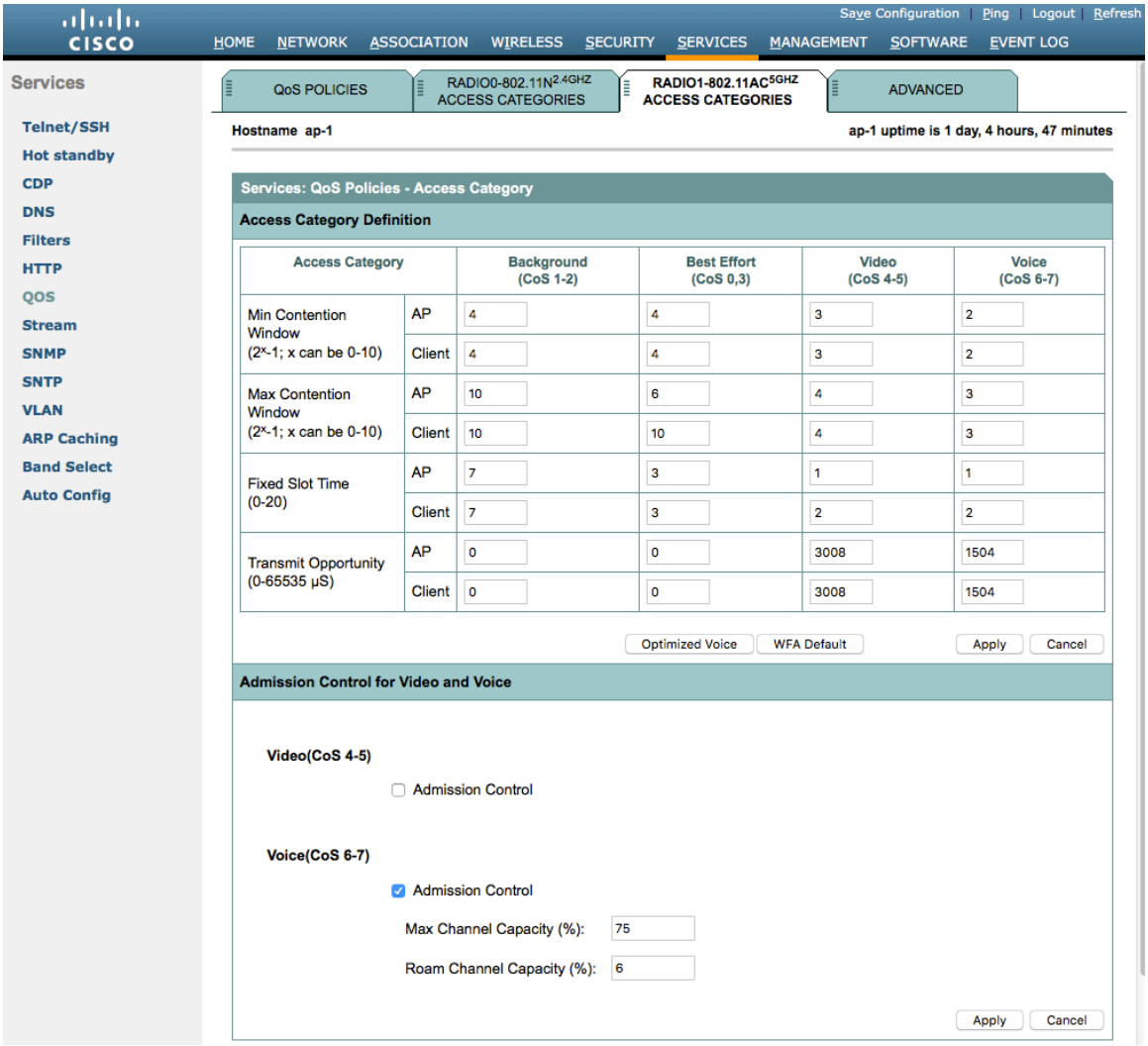
Call Admission Control (CAC)

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.

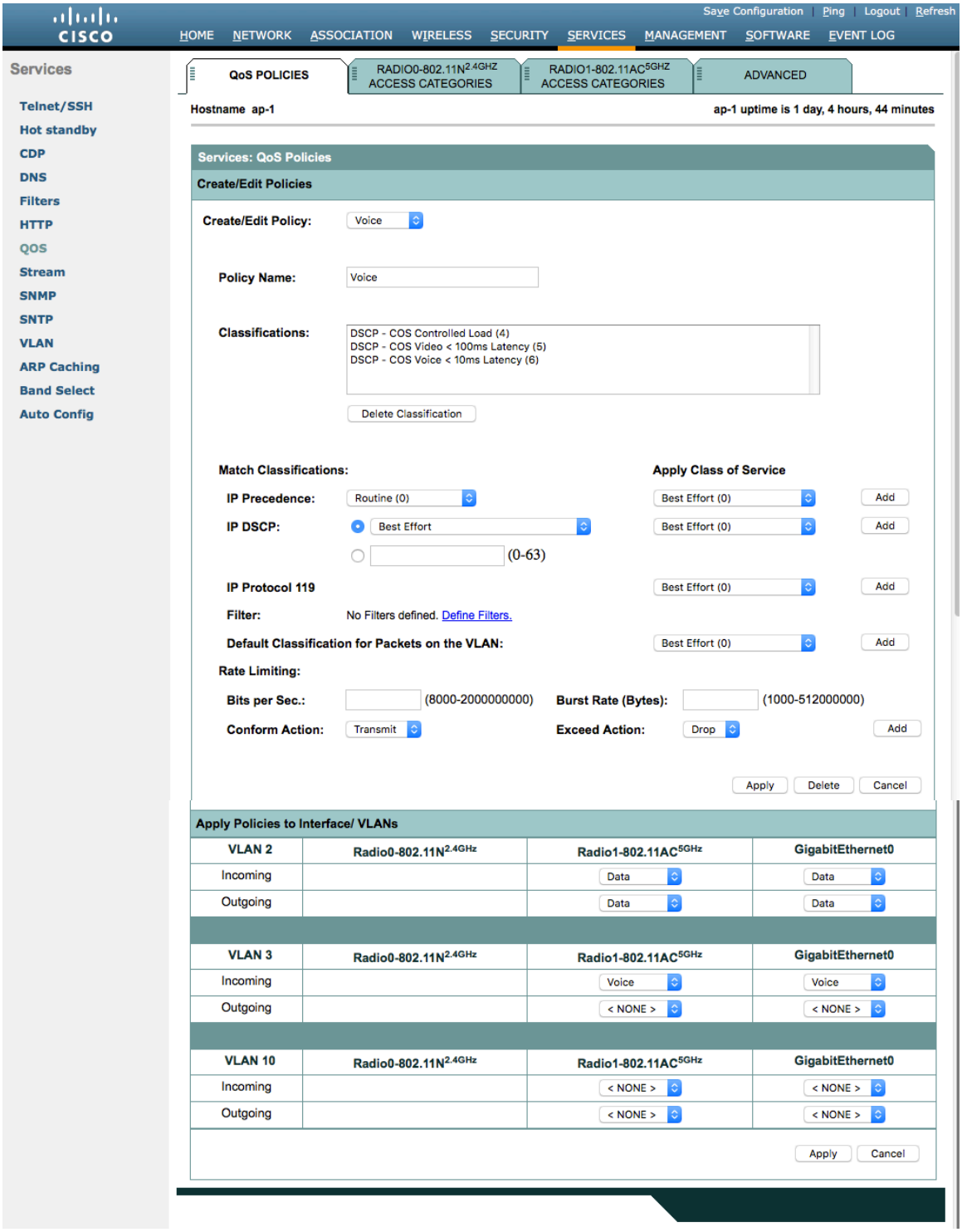
```
Dot11 ssid voice
  vlan 3
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2 dot11r
  admit-traffic
```



QoS Policies

Configure the following QoS policy on the Cisco Autonomous Access Point to enable DSCP to CoS (WMM UP) mapping.

This allows packets to be placed into the proper queue as long as those packets are marked correctly when received at the access point level.

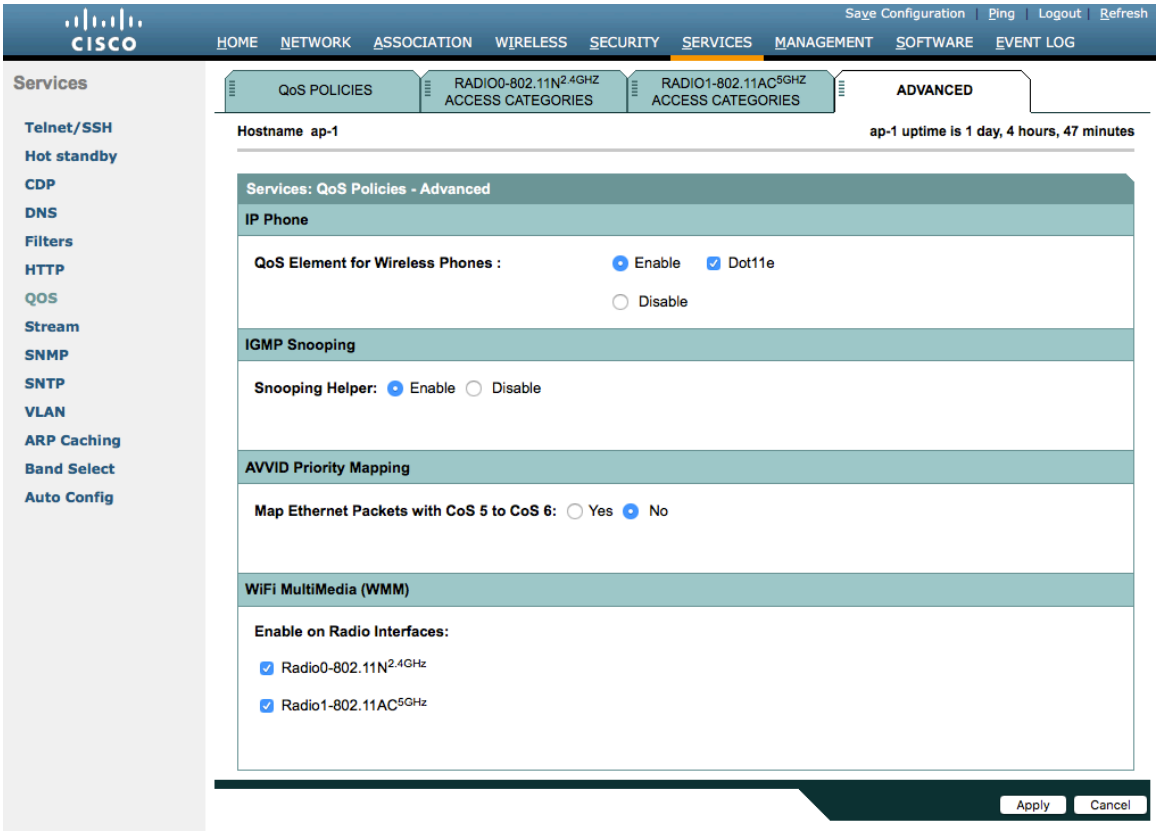


To enable QBSS, select **Enable** and check **Dot11e**.

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

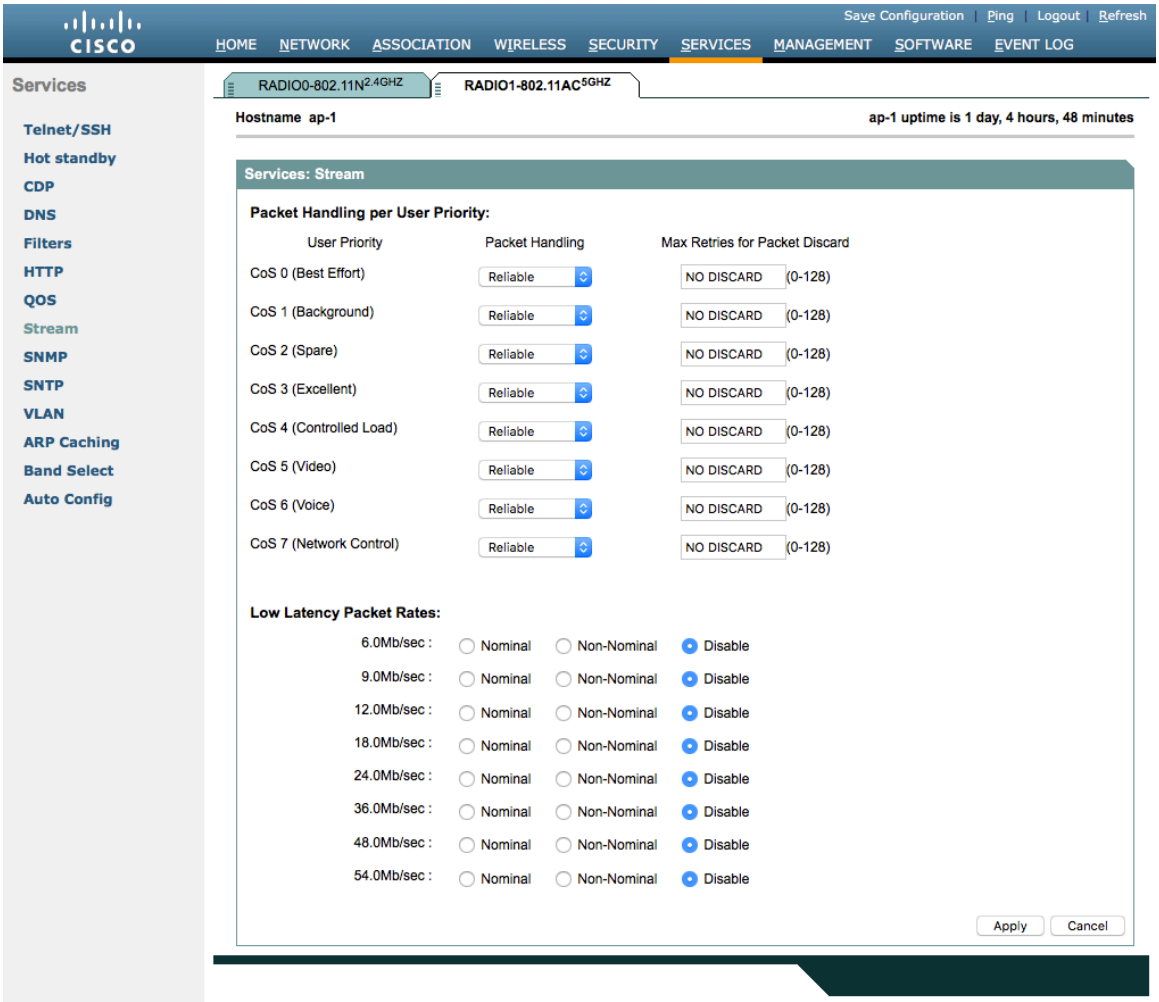
Ensure **IGMP Snooping** is enabled.

Ensure **Wi-Fi MultiMedia (WMM)** is enabled.



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

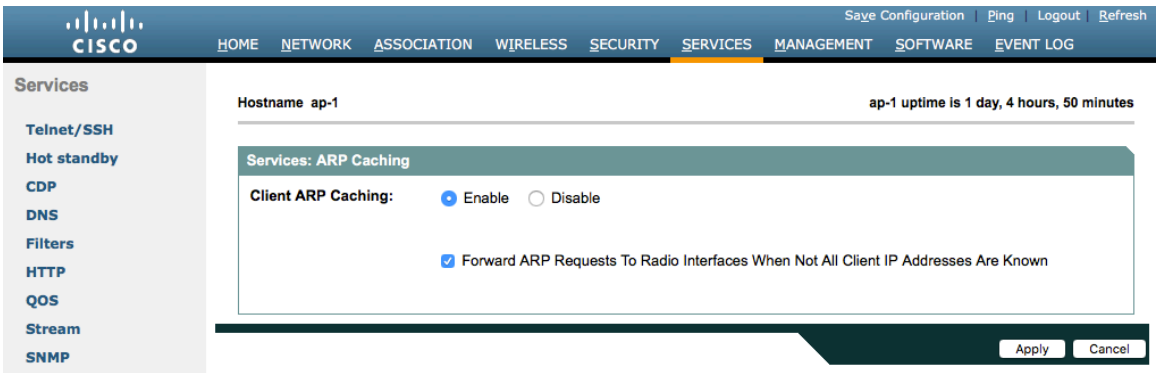
If the **Stream** feature is enabled, ensure that only voice packets are being put into the voice queue. Signaling packets should be put into a separate queue. This can be ensured by setting up a QoS policy mapping the DSCP to the correct queue.



Power Management

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

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



Sample Configuration

```
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap-1
!
logging rate-limit console 9
!
aaa new-model
!
aaa group server radius rad_eap
 server name 10.0.0.20
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
 server name 10.0.0.20
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius WDS
 server name 10.9.0.9
!
aaa group server radius Clients
 server name 10.0.0.20
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login method_WDS group WDS
aaa authentication login method_Clients group Clients
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
clock timezone -0500 -5 0
clock summer-time -0400 recurring
no ip source-route
no ip cef
ip domain name cisco.com
ip name-server 10.0.0.30
ip name-server 10.0.0.31
!
dot11 pause-time 100
dot11 syslog
!
dot11 ssid data
```

```
  vlan 2
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2
!
dot11 ssid voice
  vlan 3
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2 dot11r
!
dot11 arp-cache optional
dot11 phone dot11e
!
no ipv6 cef
!
crypto pki trustpoint TP-self-signed-672874324
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-672874324
 revocation-check none
 rsakeypair TP-self-signed-672874324
!
crypto pki certificate chain TP-self-signed-672874324
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 36373238 37343332 34301E17 0D313630 38303332 33303533
  385A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3637 32383734
  33323430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  CB155DD1 3421B13F CD121F42 7A62D9F5 38EBC966 4420F38A 38DFAFF2 D43CD3B9
  5F5A1B75 7910F9F5 6E9EDEF4 730942C7 17DC4CBC E5AE3E49 0AF79419 0BEF34BC
  5DCEB4E2 FF2978CB C34D5AEE ED1DFB58 C7BF6592 61C1AD25 3EF87205 15EA58C2
  0A5E2B15 7F08FAEA 5DA2BFA7 95E56C60 22C229C7 024A91D7 A4FEB50B 5425357F
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
  23041830 168014FC 2FE6CF0E E0380A40 11381459 5D596E3E A684DA30 1D060355
  1D0E0416 0414FC2F E6CF0EE0 380A4011 3814595D 596E3EA6 84DA300D 06092A86
  4886F70D 01010505 00038181 0053F55B 5EBB1FE2 C849BC45 47D0E710 0200404E
  A8B174BC A46EB56A 857166C3 B9FD71DF 7264F5AF DC804A67 16BD35A2 4F39AFD7
  0BD24F71 BAF916AC E984343C A54B7395 E5D15237 8897D436 A150BFB2 DC23E8D3
  AFF0A51C B6253153 C4E2C022 66F1E361 B2EE49E2 763FCBC7 6381E7F7 61B6E14D
  60CDF947 2C044617 37211E5F CE
        quit
username <REMOVED> privilege 15 password 7 <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 cs4
class-map match-all _class_Voice3
 match ip dscp ef
!
policy-map Voice
 class _class_Voice0
  set cos 4
```

```
 class _class_Voice1
  set cos 5
class _class_Voice2
  set cos 5
class _class_Voice3
  set cos 6
policy-map Data
 class class-default
  set cos 0
!
bridge irb
!
interface Dot11Radio0
 no ip address
 shutdown
 antenna gain 0
 traffic-metrics aggregate-report
 stbc
 mbssid
 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 http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
  nas 10.9.0.9 key 7 <REMOVED>
  user wds nthash 7 <REMOVED>
!
radius-server attribute 32 include-in-access-req format %h
!
radius server 10.0.0.20
 address ipv4 10.0.0.20 auth-port 1812 acct-port 1813
 key 7 <REMOVED>
!
radius server 10.9.0.9
 address ipv4 10.9.0.9 auth-port 1812 acct-port 1813
 key 7 <REMOVED>
!
access-list 111 permit tcp any any neq telnet
bridge 1 route ip
!
wlccp ap username wds password 7 <REMOVED>
wlccp ap wds ip address 10.9.0.9
wlccp authentication-server infrastructure method_WDS
wlccp authentication-server client eap method_Clients
wlccp authentication-server client leap method_Clients
wlccp wds priority 255 interface BVI1
!
line con 0
 access-class 111 in
line vty 0 4
 access-class 111 in
 transport input all
!
sntp server 10.0.0.2
sntp broadcast client
end
```

Cisco Meraki Access Points

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

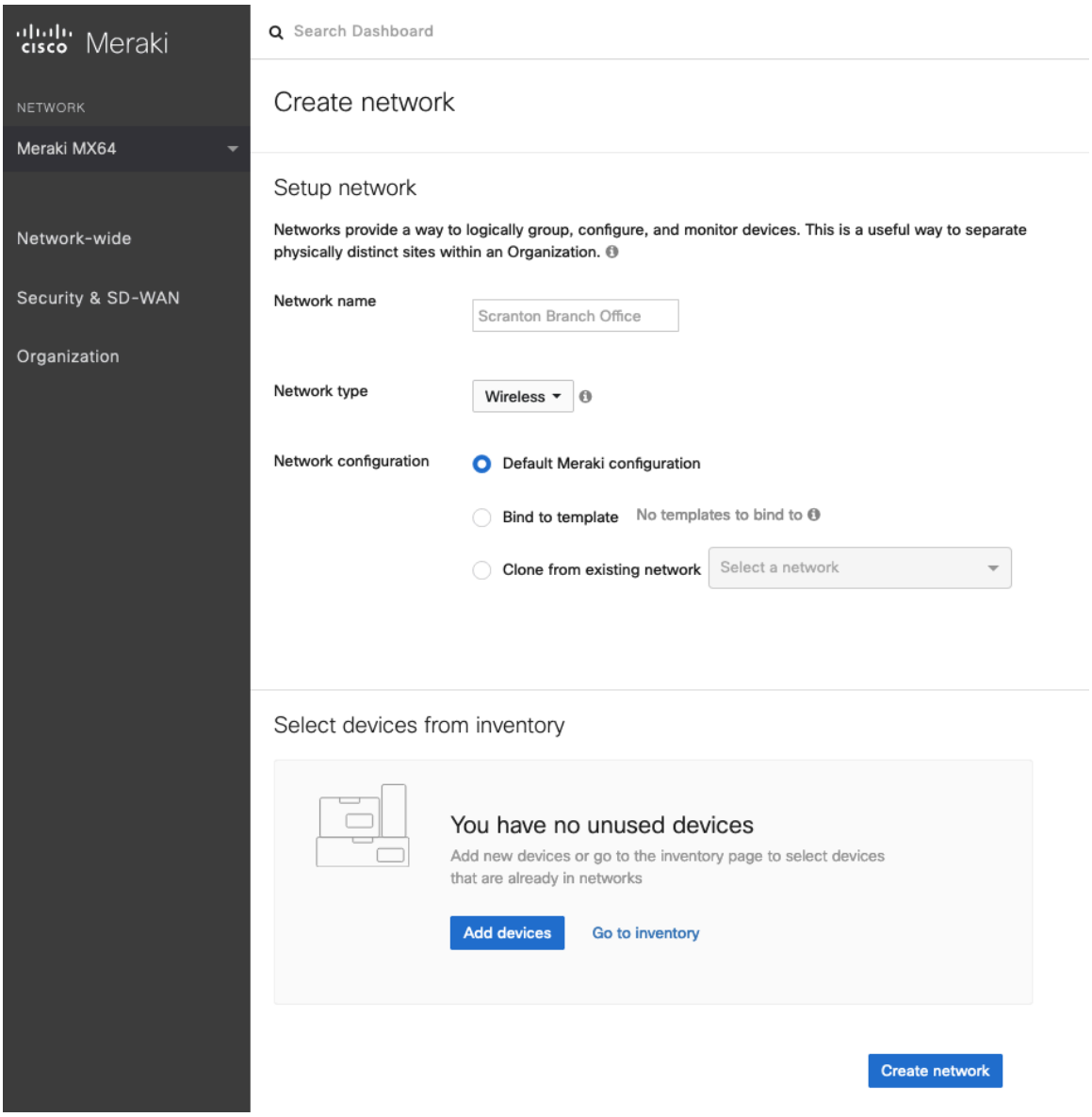
- Enable **802.11r** for **WPA2-Enterprise** or **Pre-shared key**
- Set **Splash page** to **None**
- Enable **Bridge mode**
- Enable **VLAN tagging**
- Set **Band selection** to **5 GHz band only**
- Configure the **Data Rates** as necessary
- Configure **Quality of Service (QoS)**

Creating the Wireless Network

A wireless network must be created prior to adding any Cisco Meraki access points to provide WLAN service.

Select **Create a new network** from the drop-down menu.

Select **Wireless** for Network type then click **Create**.

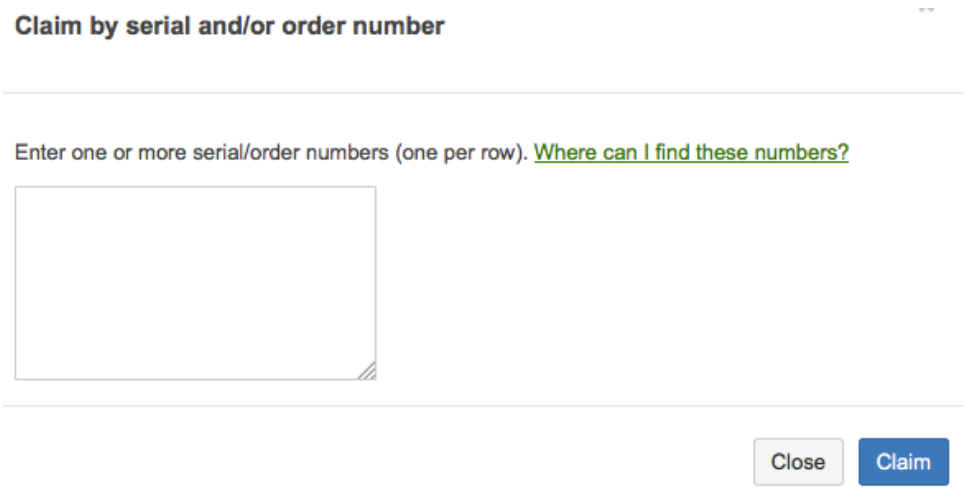


Cisco Meraki access points can be claimed either by specifying the serial number or order number.

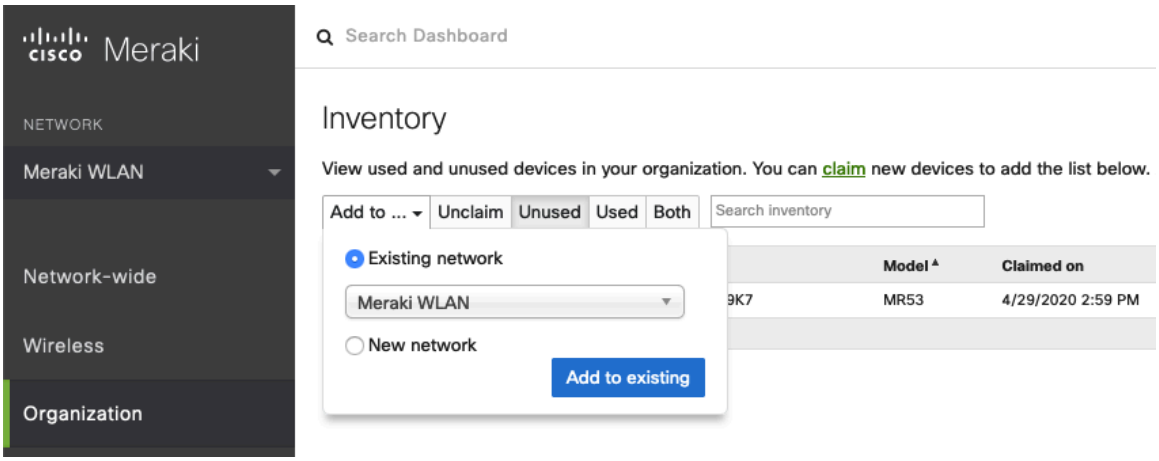
Once claimed, those Cisco Meraki access points will then be listed in the available inventory.

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

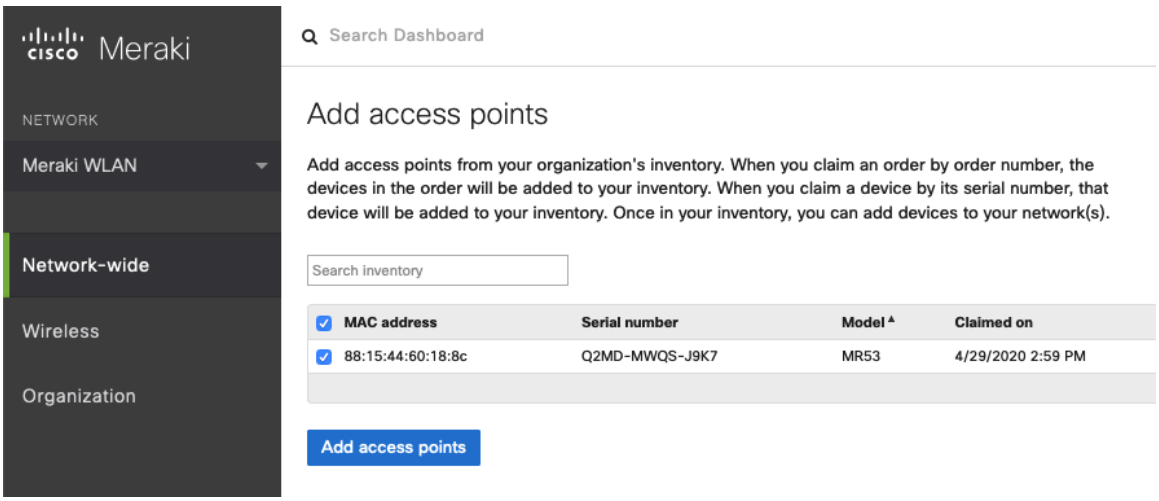
Access points can also be claimed by selecting **Add APs** on the **Wireless > Monitor > Access points** page, then selecting **Claim**.



Once claimed, Cisco Meraki access points can be added to the desired wireless network via the **Organization > Configure > Inventory** page.



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



SSID Configuration

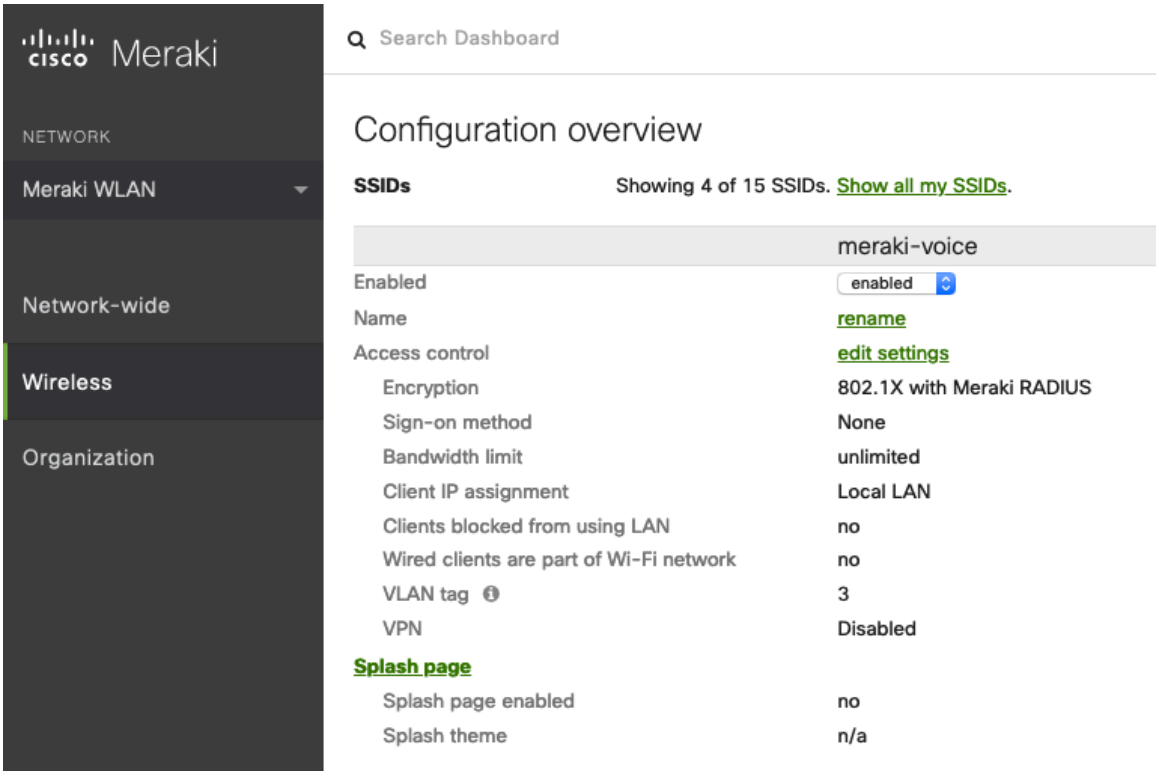
To create a SSID, select the desired network from the drop-down menu then select **Wireless > Configure > SSIDs**.

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

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

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

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



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

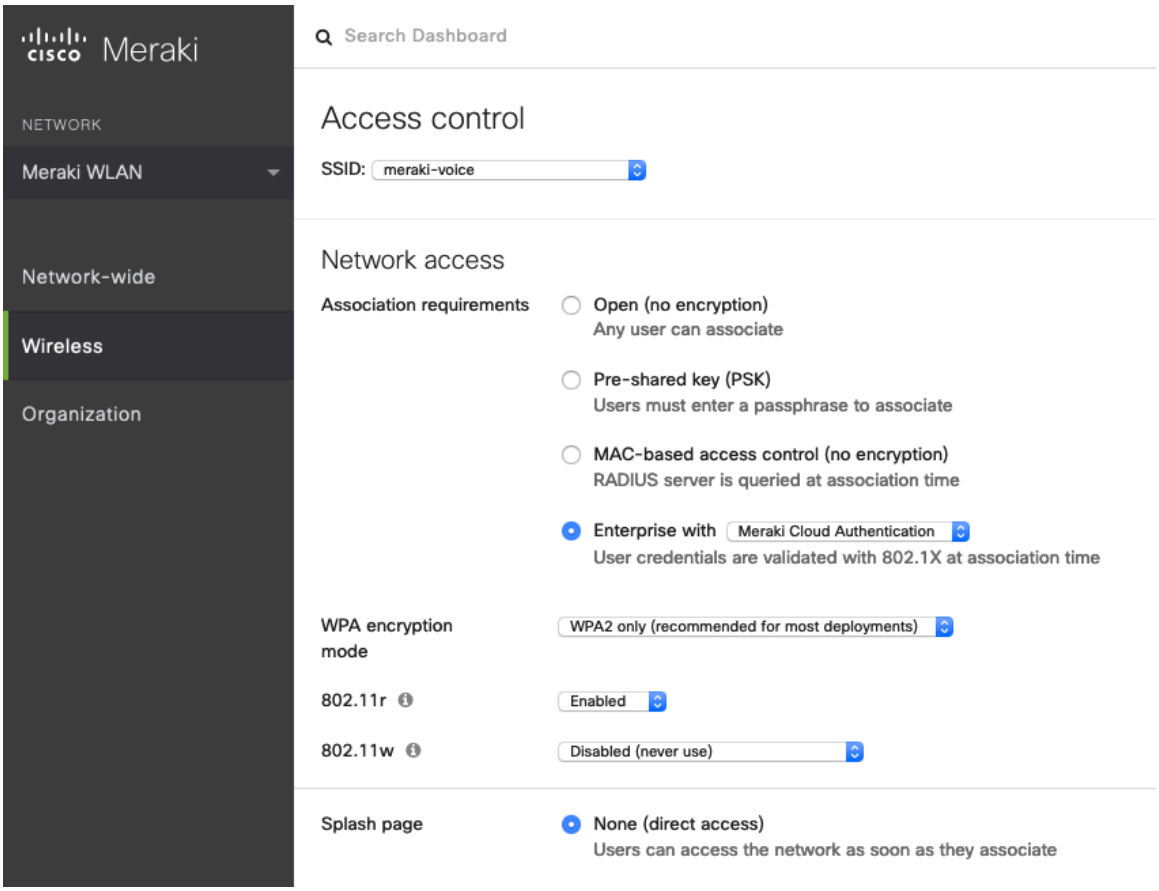
The Cisco Meraki authentication server or an external RADIUS server can be utilized when selecting **WPA2-Enterprise**.

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

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

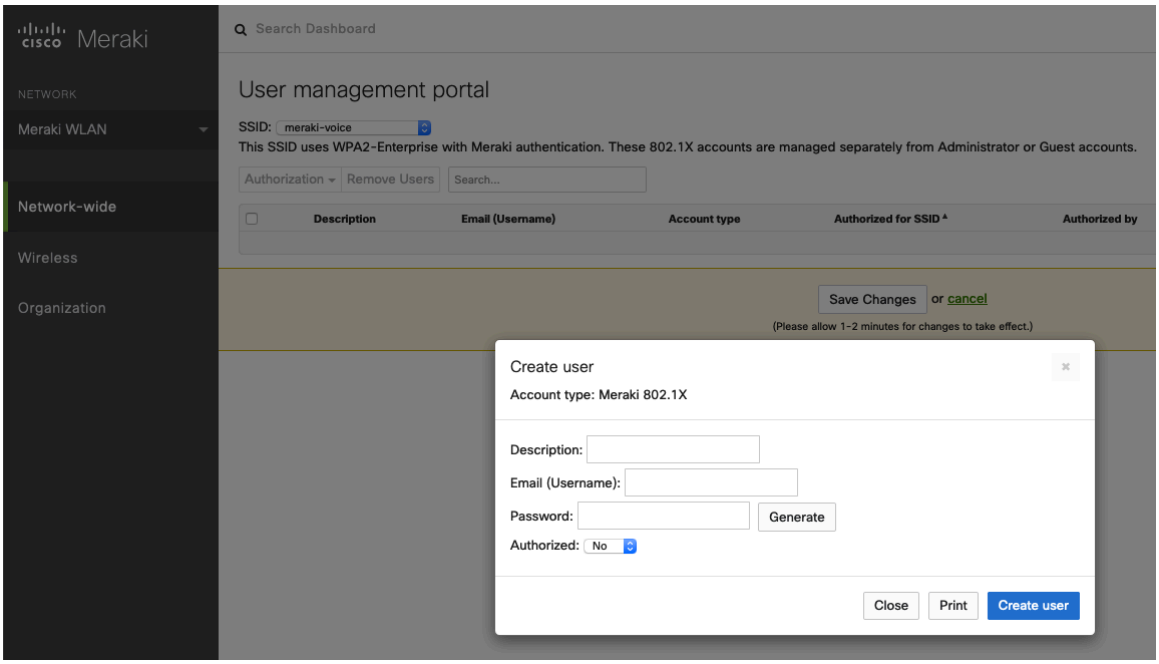
Ensure **802.11r** is enabled.

Ensure Splash page is set to **None** to enable direct access.



Note: Cisco Meraki access points support 802.11r (FT) for fast secure roaming, but do not support Cisco Centralized Key Management (CCKM).

If **WPA2-Enterprise** is enabled where the Cisco Meraki authentication server will be utilized as the RADIUS server, then a user account must be created on the **Network-wide > Configure > Users** page, which the Cisco Wireless Phone 840 and 860 will be configured to use for 802.1x authentication.



On the **Wireless > Configure > Access control** page, recommend to enable **Bridge mode**, where the Cisco Wireless Phone 840 and 860 will obtain DHCP from the local LAN instead of the Cisco Meraki network; unless call control, other endpoints, etc. are cloud-based.

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

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

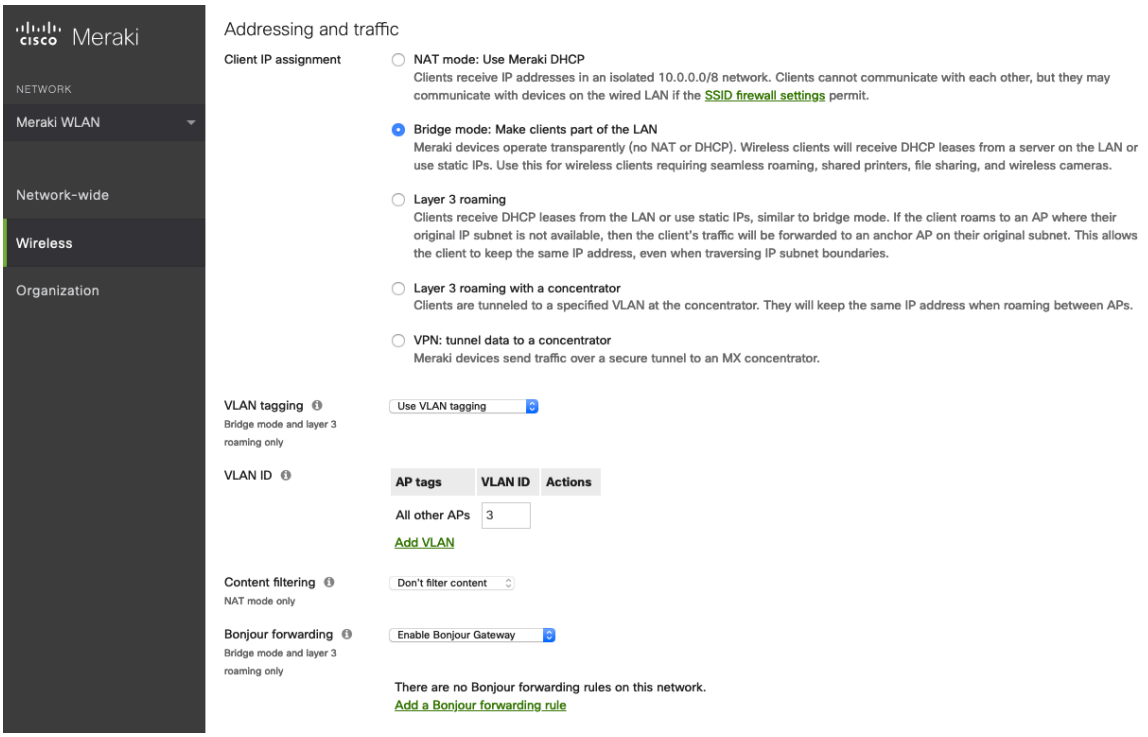
If VLAN tagging is utilized, ensure that the Cisco Meraki access point is connected to a switch port configured for trunk mode allowing that VLAN.

If utilizing Cisco Meraki MS Switches, reference the **Cisco Meraki MS Switch VoIP Deployment Guide**.

https://meraki.cisco.com/lib/pdf/meraki_whitepaper_msvoip.pdf

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
```



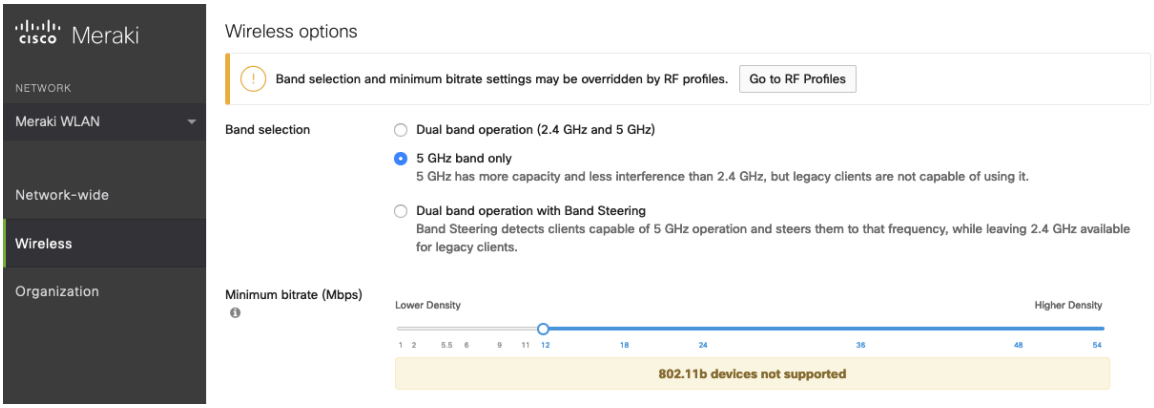
On the **Wireless > Configure > Access control** page, the frequency band for the SSID to be used by the Cisco Wireless Phone 840 and 860 can be configured as necessary.

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

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

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

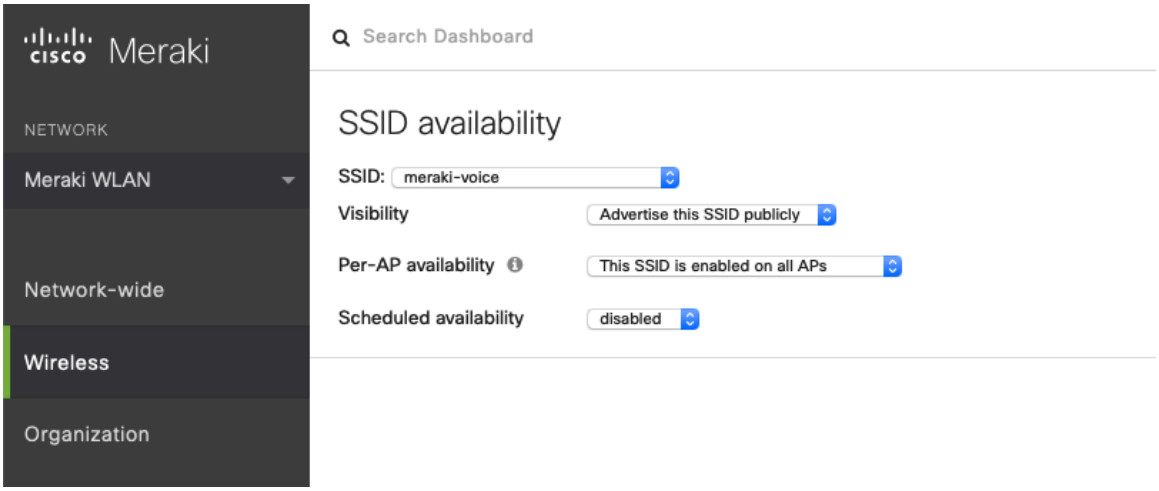
Cisco Meraki access points currently utilize a DTIM period of **1** with a beacon period of **100 ms**; which both are non-configurable.



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

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

A schedule for SSID availability can be configured as necessary, however it is recommended to set **Scheduled Availability** to **Disabled**.

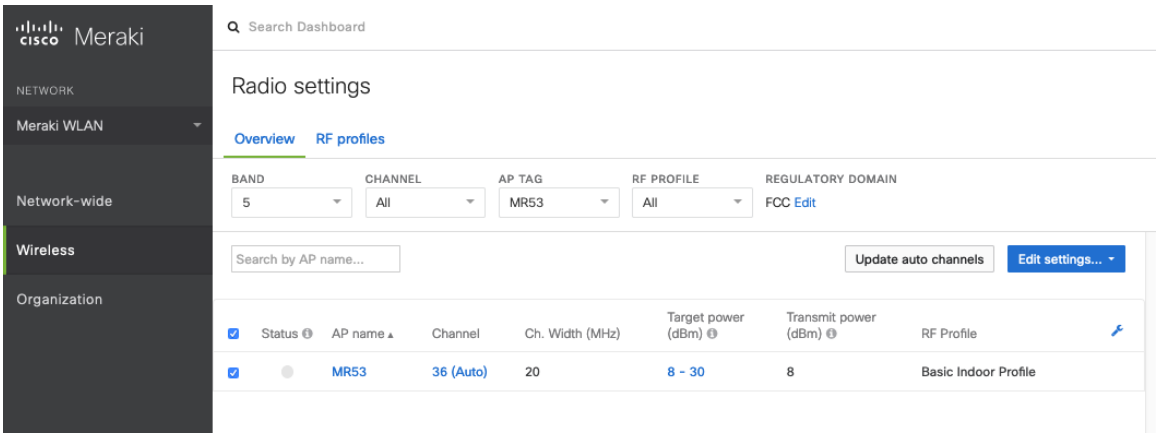


Radio Settings

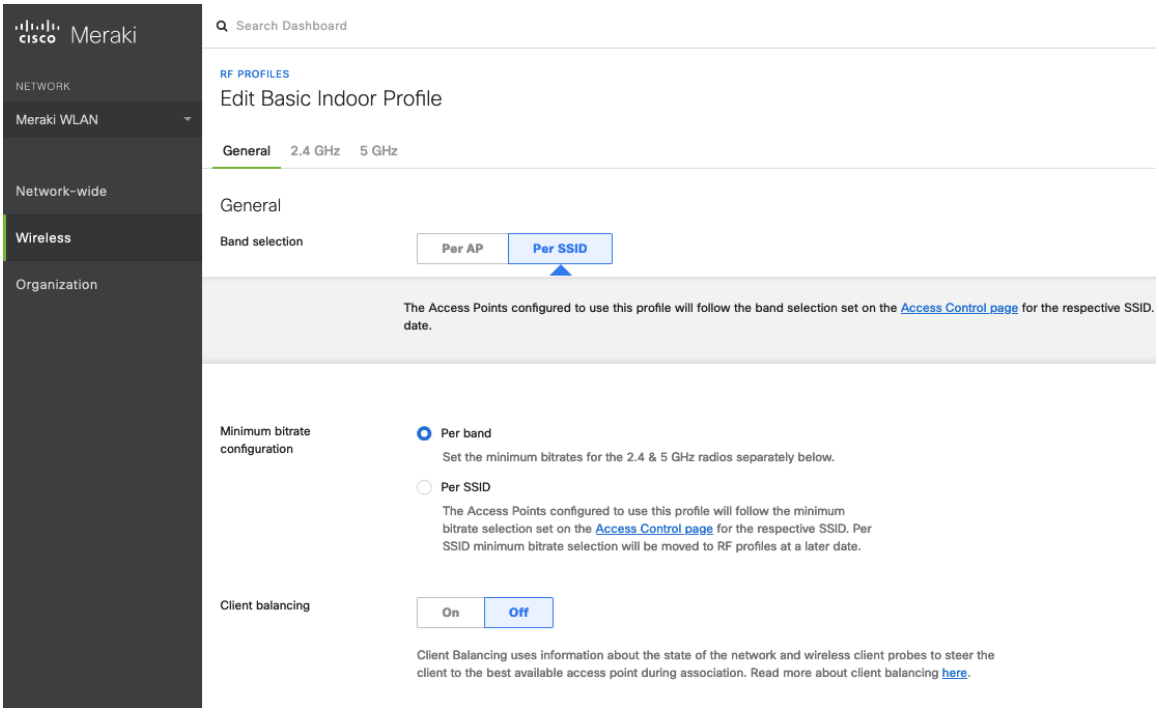
On the **Wireless > Configure > Radio settings** page, access points can be configured in bulk or by individual access point to define the automatic or manual channel and transmit power settings.

When using Cisco Meraki access points it is recommended to select **Auto** for the channel and transmit power to utilize what is defined in the RF Profile.

However, individual access points can be configured with static channel and transmit power for either 5 or 2.4 GHz radios, which may be necessary if there is an intermittent interferer present in an area. While other access points can be enabled for **Auto** and work around the access points that are have static channel assignments.



It is recommended to either modify the standard **Basic Indoor Profile** or create a new RF Profile with **Band selection** set to **Per SSID** and **Client balancing** set to **Off**.



In the RF Profile, the **Channel width** for 5 GHz radios can be set to use 20 MHz, 40 MHz, or 80 MHz channels.

2.4 GHz radios utilize 20 MHz channel width and can not be configured for any other channel width.

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

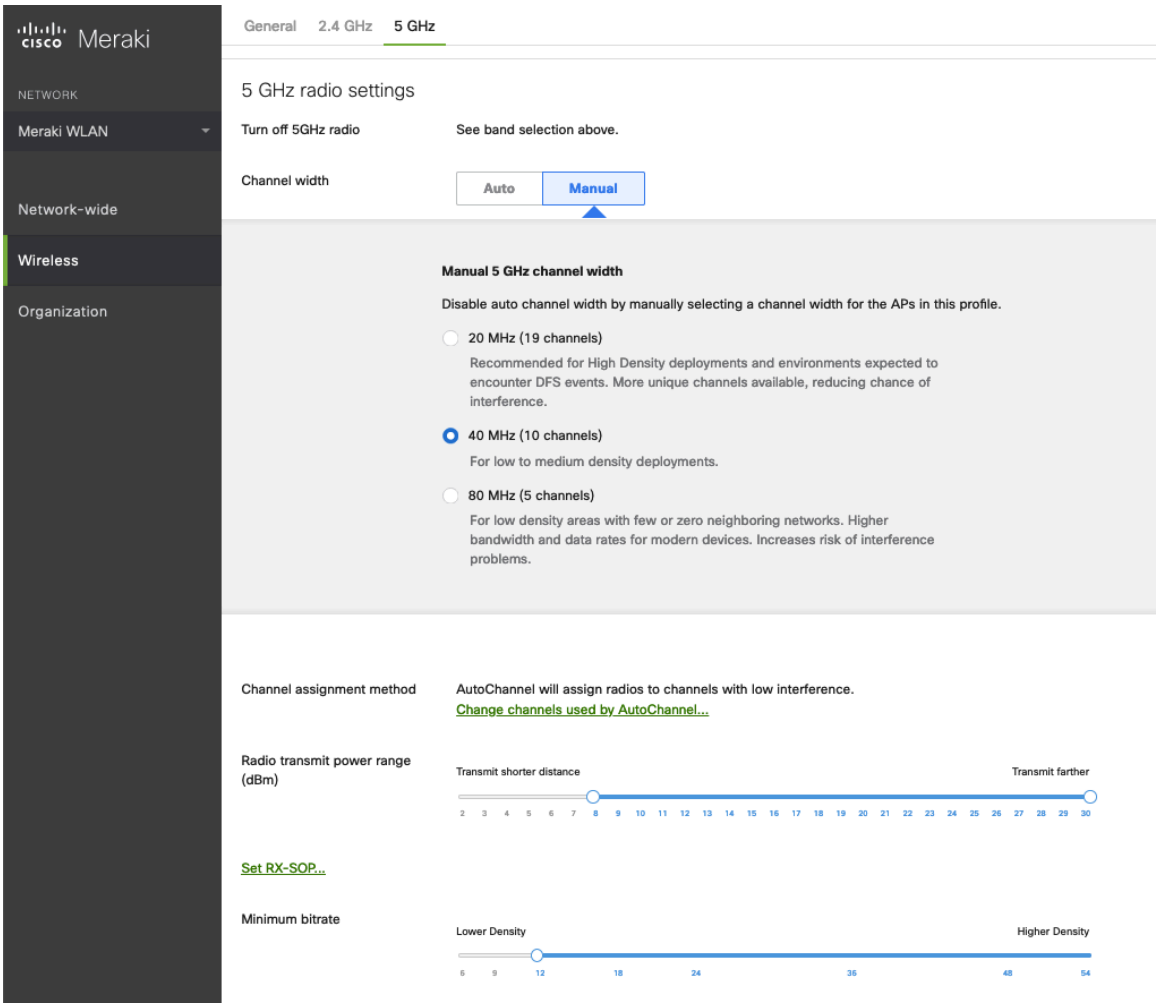
5 GHz channels to be used by **AutoChannel** can also be configured in the RF Profile.

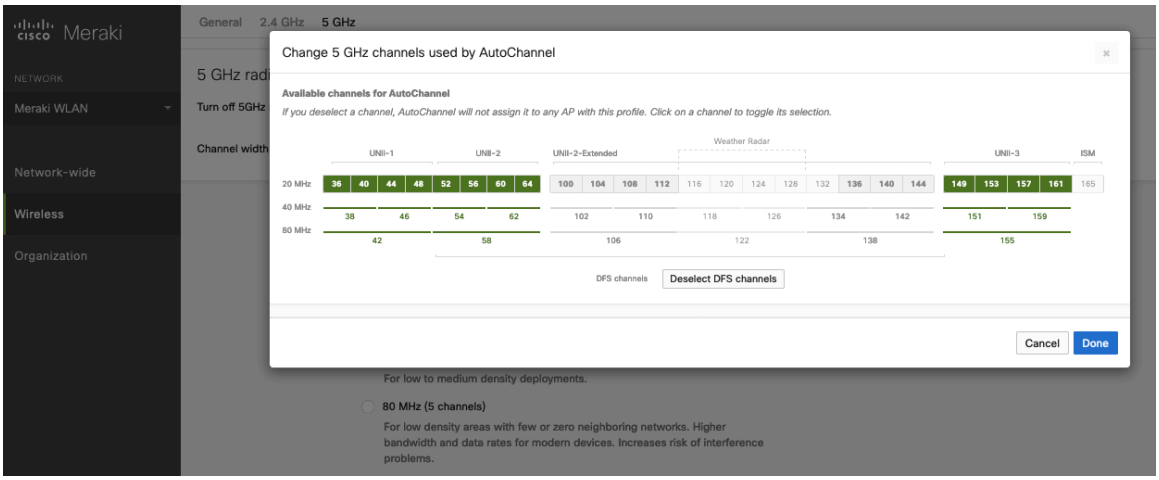
2.4 GHz channels used by **AutoChannel** are limited to channels 1, 6, and 11 only.

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

If the **Minimum bitrate configuration** is set to Per band, then it will override what is defined in the SSID configuration.

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





Note: Cisco Meraki access points do not support Dynamic Transmit Power Control (DTPC), therefore the Cisco Wireless Phone 840 and 860 will utilize the maximum transmit power supported for the current channel and data rate.

Firewall and Traffic Shaping

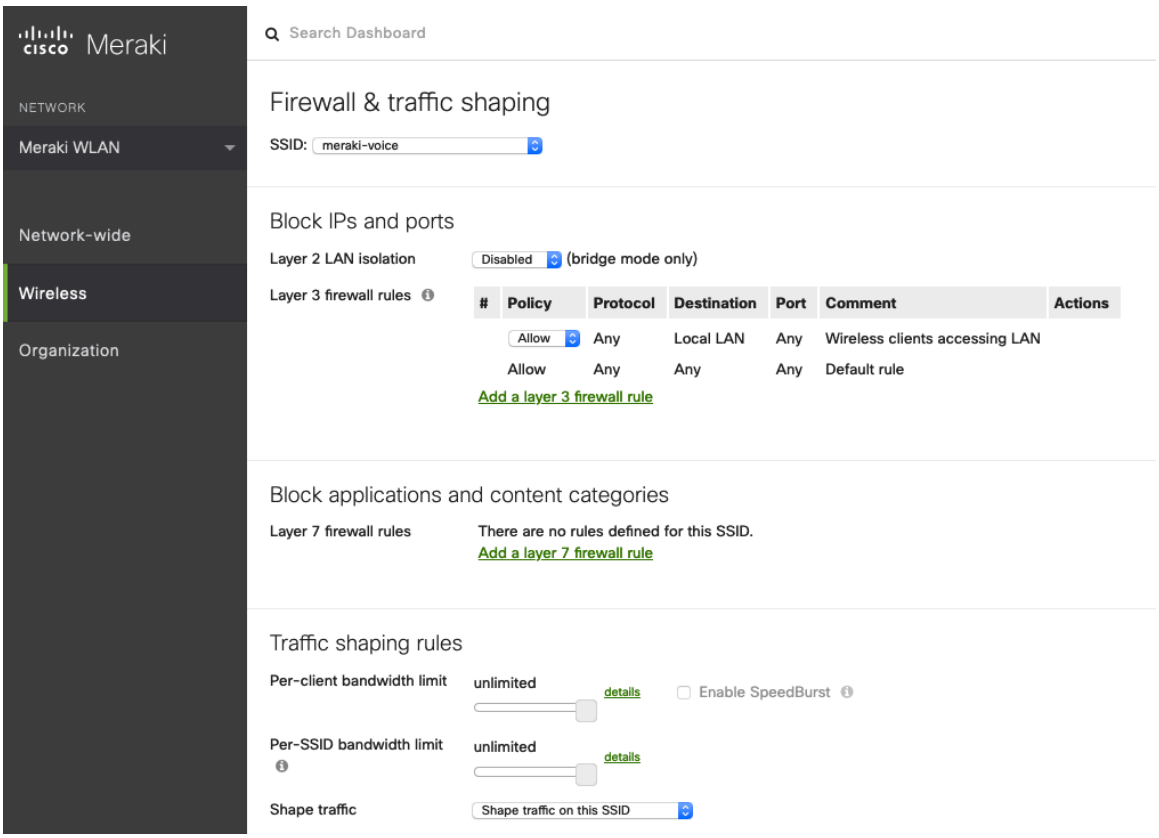
On the **Wireless > Configure > Firewall & traffic shaping** page, firewall and traffic shaping rules can be defined.

Ensure a **Layer 3 firewall rule** is configured to allow local LAN access for wireless clients.

To allow traffic shaping rules to be defined select **Shape traffic on this SSID** in the drop-down menu for **Shape traffic**.

Once **Shape traffic on this SSID** has been applied, then select **Create a new rule** to define **Traffic shaping rules**.

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



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

Configuring Cisco Call Control

Cisco Unified Communications Manager

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

Device Enablement

To enable the Cisco Wireless Phone 840 or 860 device type in the Cisco Unified Communications Manager, the corresponding device enabler (QED) COP file for each phone model must be installed via the Cisco Unified Operating System Administration webpage for each Cisco Unified Communications Manager server.

Each Cisco Unified Communication Manager node may not have to be restarted after the device enabler (QED) COP file has been installed.

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

11.5(1)SU4 and lower

- Reboot all Cisco Unified Communications Manager nodes.

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

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

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

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

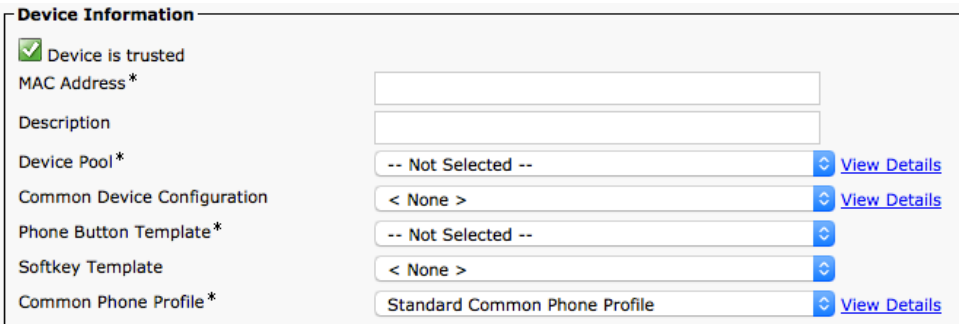
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

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

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

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

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



Note: The Cisco Wireless Phone 840 and 860 utilize the **Calling Search Space** for direct calls and the **Rerouting Calling Search Space** for transfers, therefore ensure both options are configured properly.

The hostname for the Cisco Unified Communications Manager server and the associated certificates need to match by either using the fully qualified domain name (FQDN) or IP address.

Manufacturing Certificate Authority (CA) Certificates

A new manufacturing certificate authority (CA) is being utilized for the Cisco Wireless Phone 840 and 860.

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

1. To install the new Cisco Manufacturing CA certificates, first download the missing root and intermediate certificates from the externally available Cisco PKI website.
   https://www.cisco.com/security/pki

   The missing certificates to complete the chain of trust up to and including the root for the new MICs are below:

   - Cisco Manufacturing CA III (cmca3) - Intermediate
     http://www.cisco.com/security/pki/certs/cmca3.pem

   - Cisco Basic Assurance Root CA 2099 (cbarc2099) - Root for Cisco Manufacturing CA III
     http://www.cisco.com/security/pki/certs/cbarc2099.pem

2. Using your web browser, login to the **Cisco Unified Operating System Administration** web page.
3. Under the **Security** menu, select **Certificate Management**.
4. Select **Upload Certificate/Certificate Chain**.
5. Select **CallManager-trust** for the **Certificate Purpose**, browse to the certificate, then select **Upload**.

   Note: Repeat this step for all certificates on the Cisco Unified Communication Manager publisher only as the certificate will replicate to all other Cisco Unified Communication Manager nodes.
6. Select **CAPF-trust** for the **Certificate Purpose**, browse to the certificate, then select **Upload**.

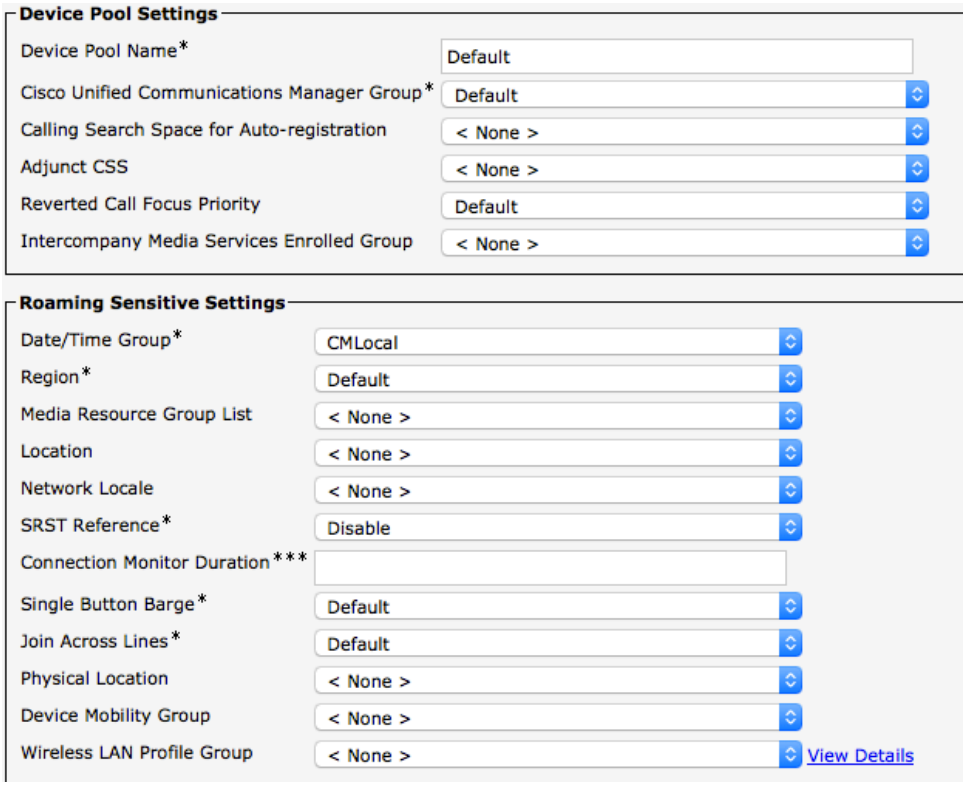
   Note: Repeat this step for all certificates on the Cisco Unified Communication Manager publisher only.

Device Pools

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

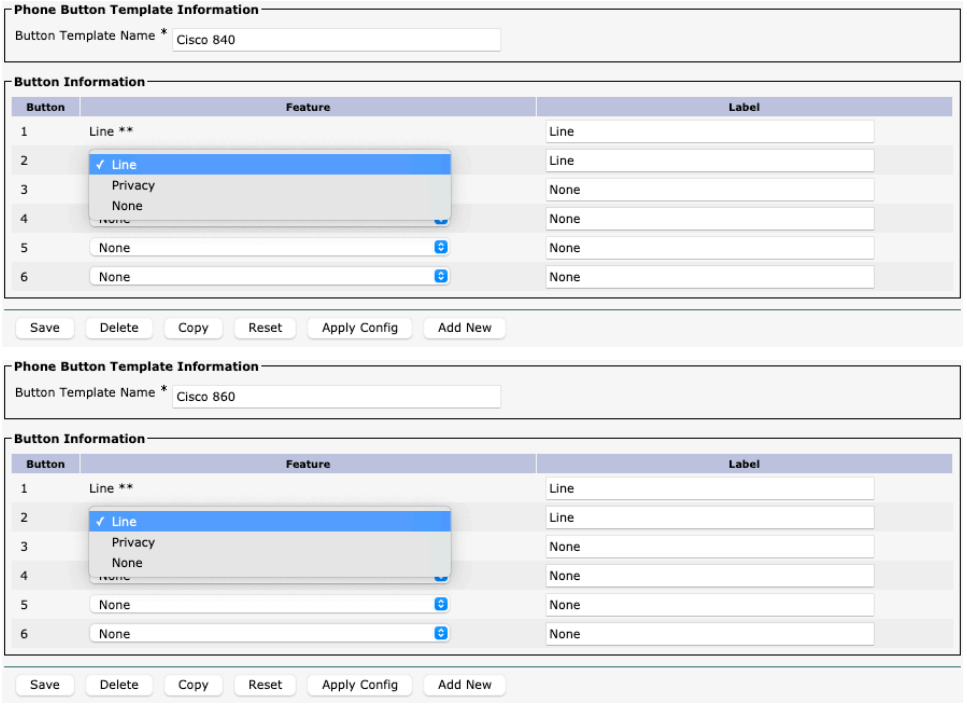
The device pool defines common settings (e.g. Cisco Unified Communications Manager Group, etc.), roaming sensitive settings (e.g. Date/Time Group, Region, etc.), local route group settings, device mobility related information settings, and other group settings.

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



Phone Button Templates

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



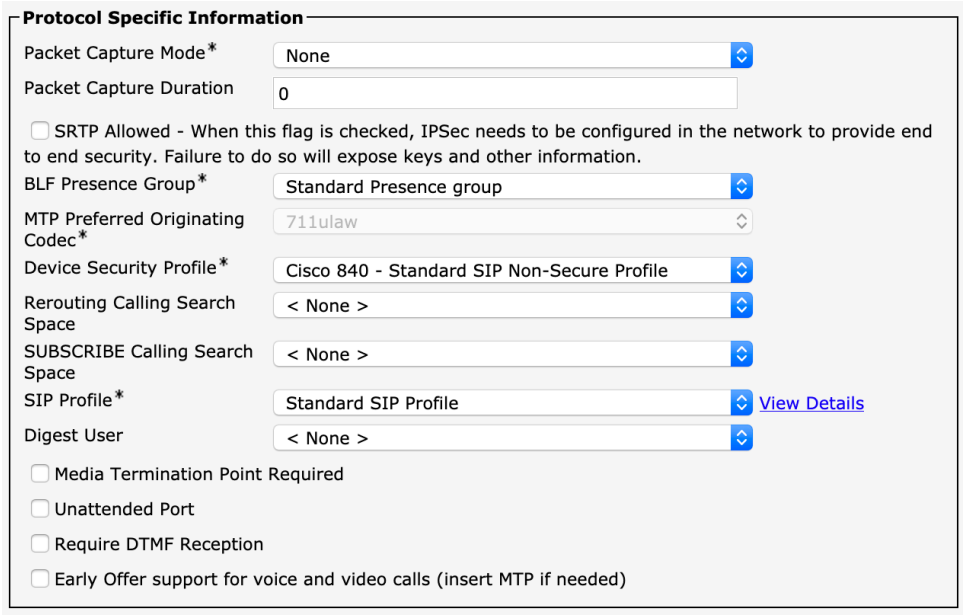
Security Profiles

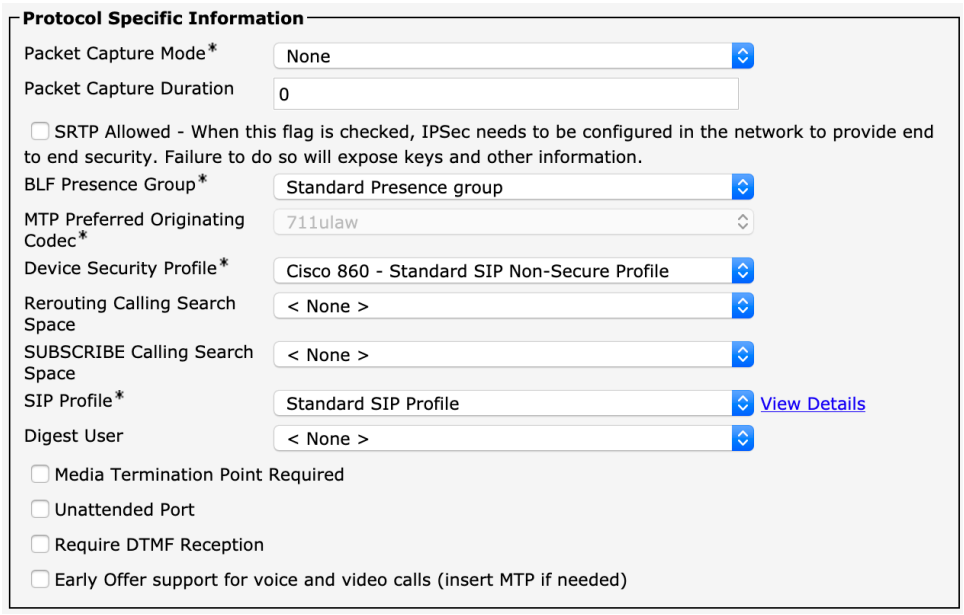
When creating a new Cisco Wireless Phone 840 or 860, a **Device Security Profile** must be configured.

Security profiles can be utilized to enable authenticated mode or encrypted mode, where signaling, media and configuration file encryption is then enabled.

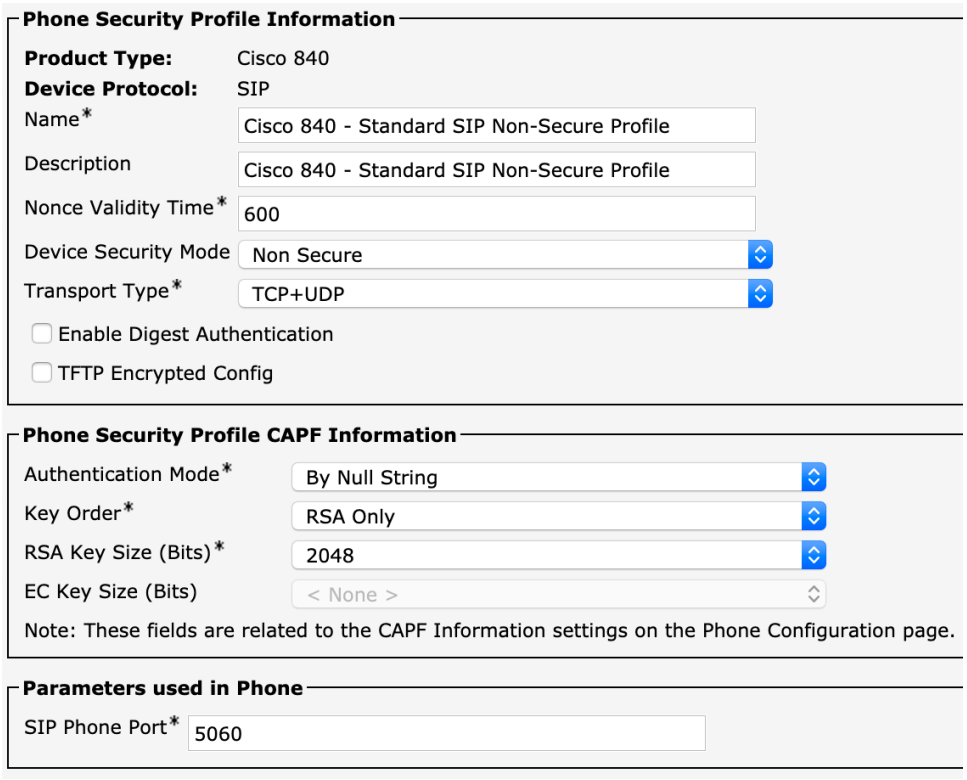
The Certificate Authority Proxy Function (CAPF) must be operational in order to utilize a Locally Significant Certificate (LSC) with a security profile.

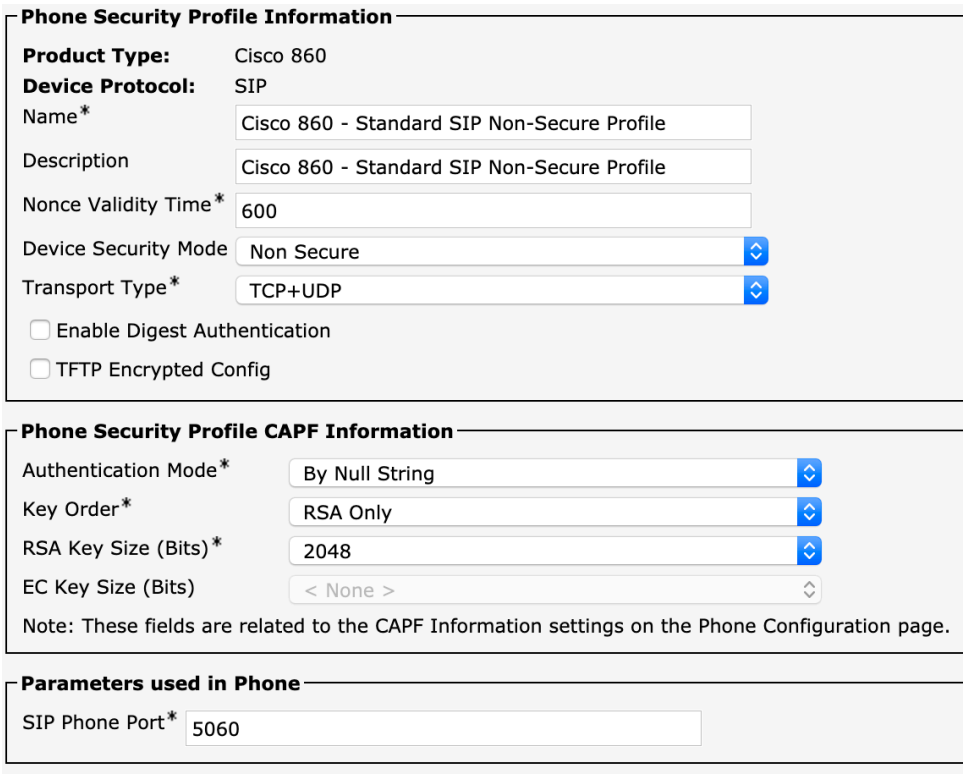
The Cisco Wireless Phone 840 and 860 have a Manufacturing Installed Certificate (MIC), which can be utilized with a security profile as well.





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



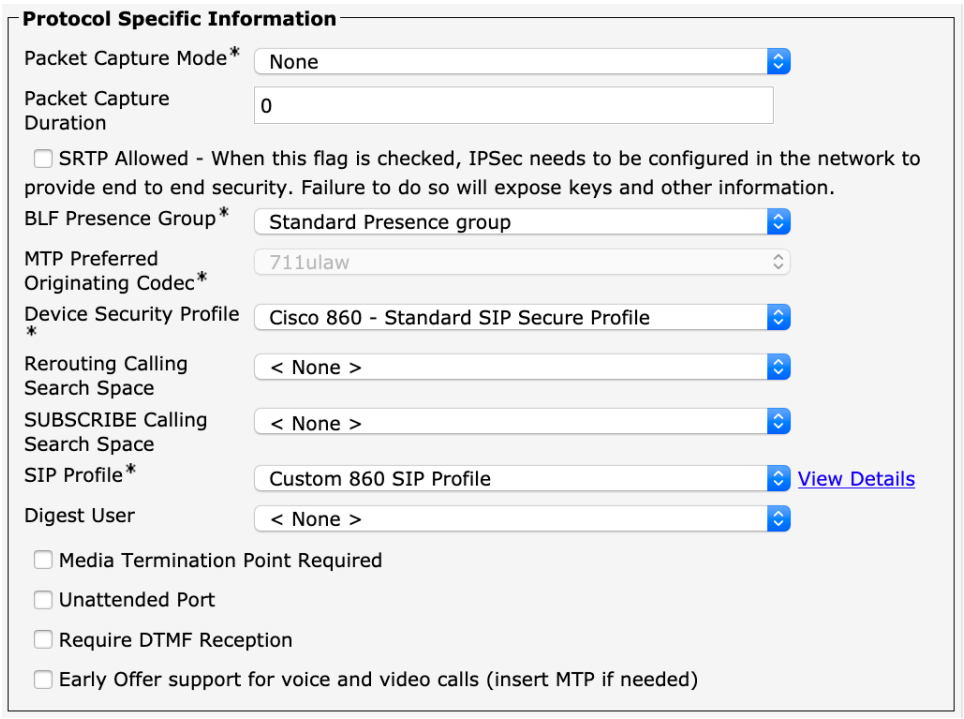


Note: Transport type must be set as TCP+UDP or TCP as UDP is not supported.

SIP Profiles

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

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



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

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

Timer Register Delta (seconds) = 30 (default = 5)

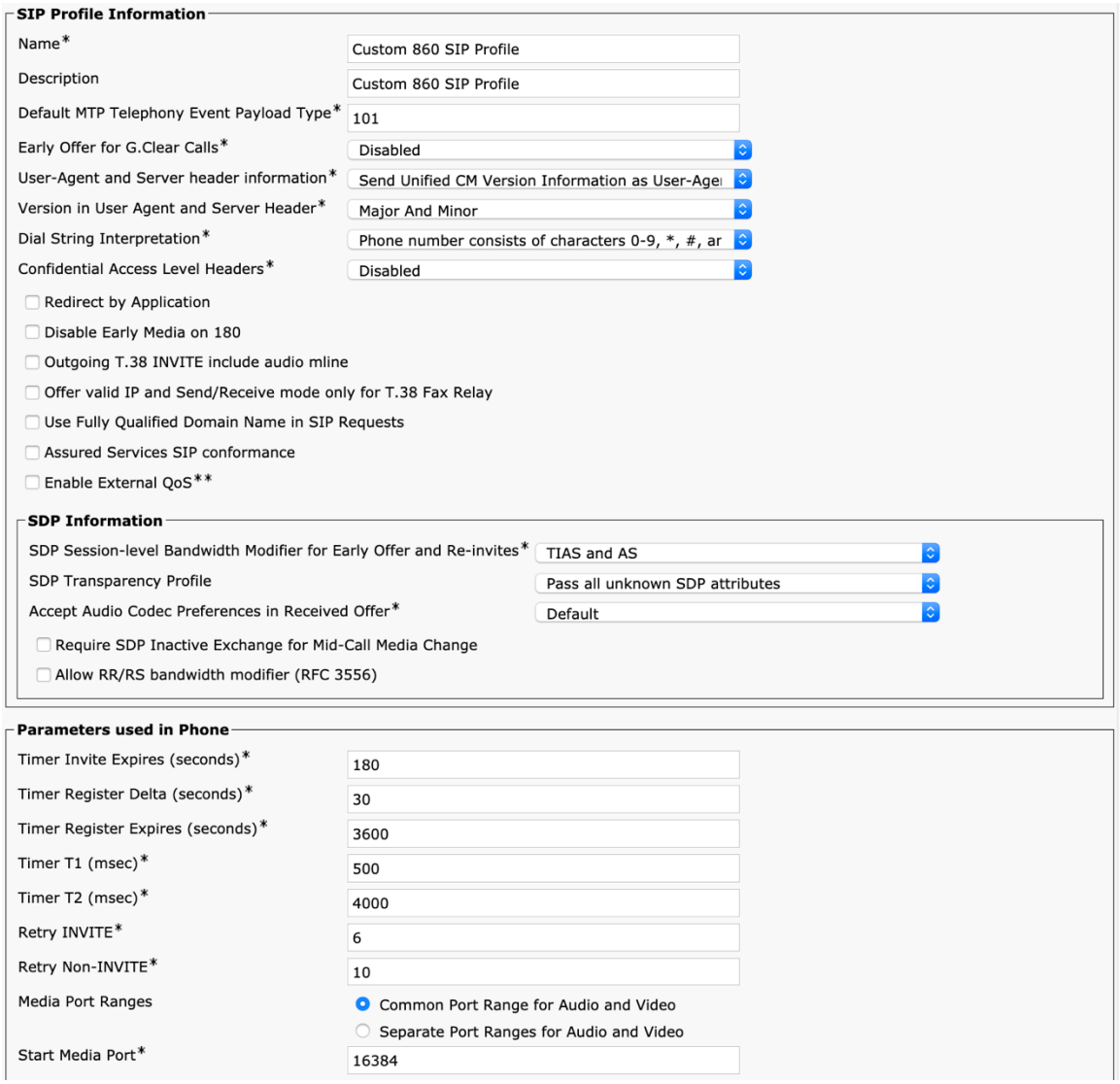
Timer Keep Alive Expires (seconds) = 300 (default = 120)

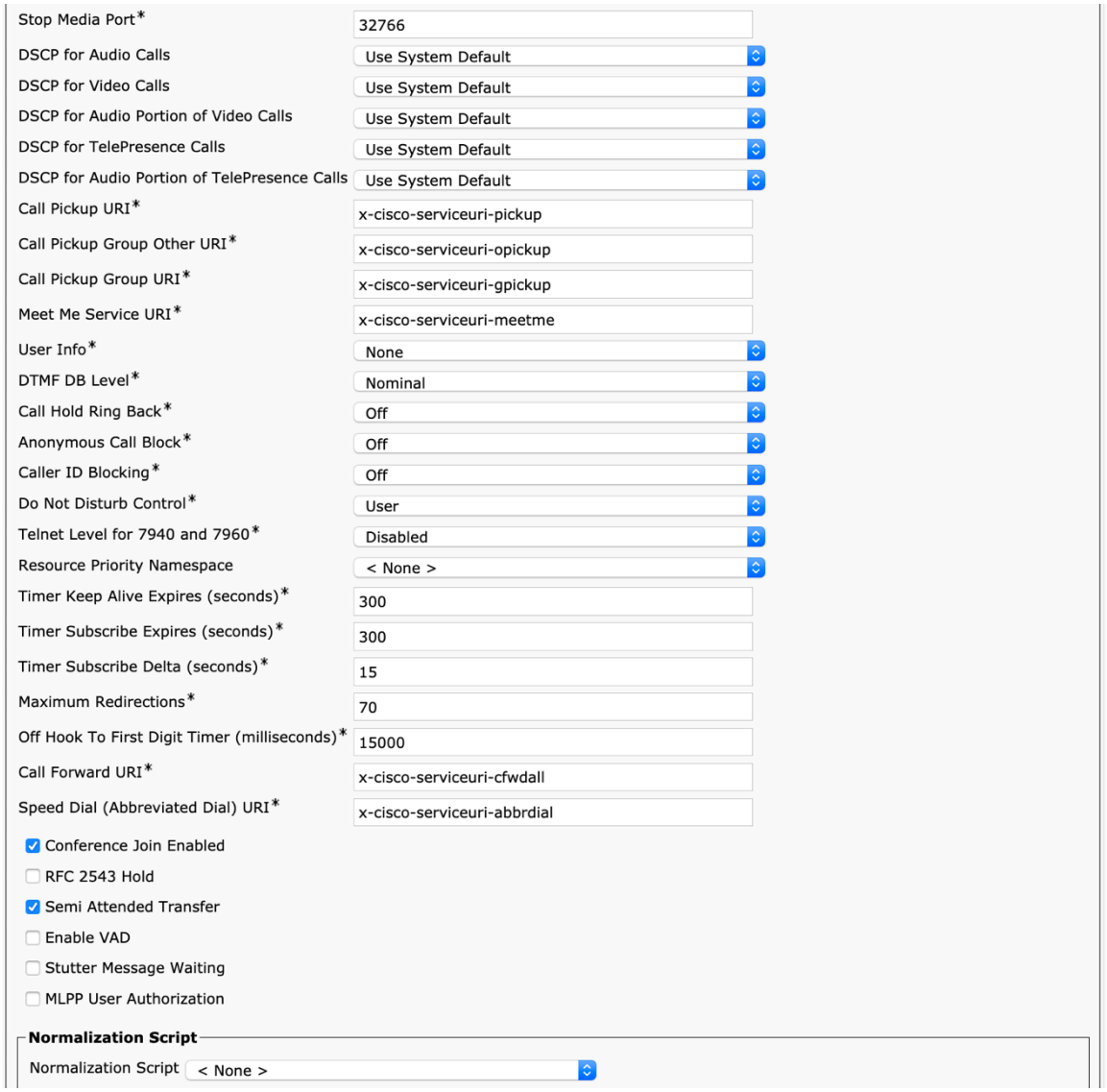
Timer Subscribe Expires (seconds) = 300 (default = 120)

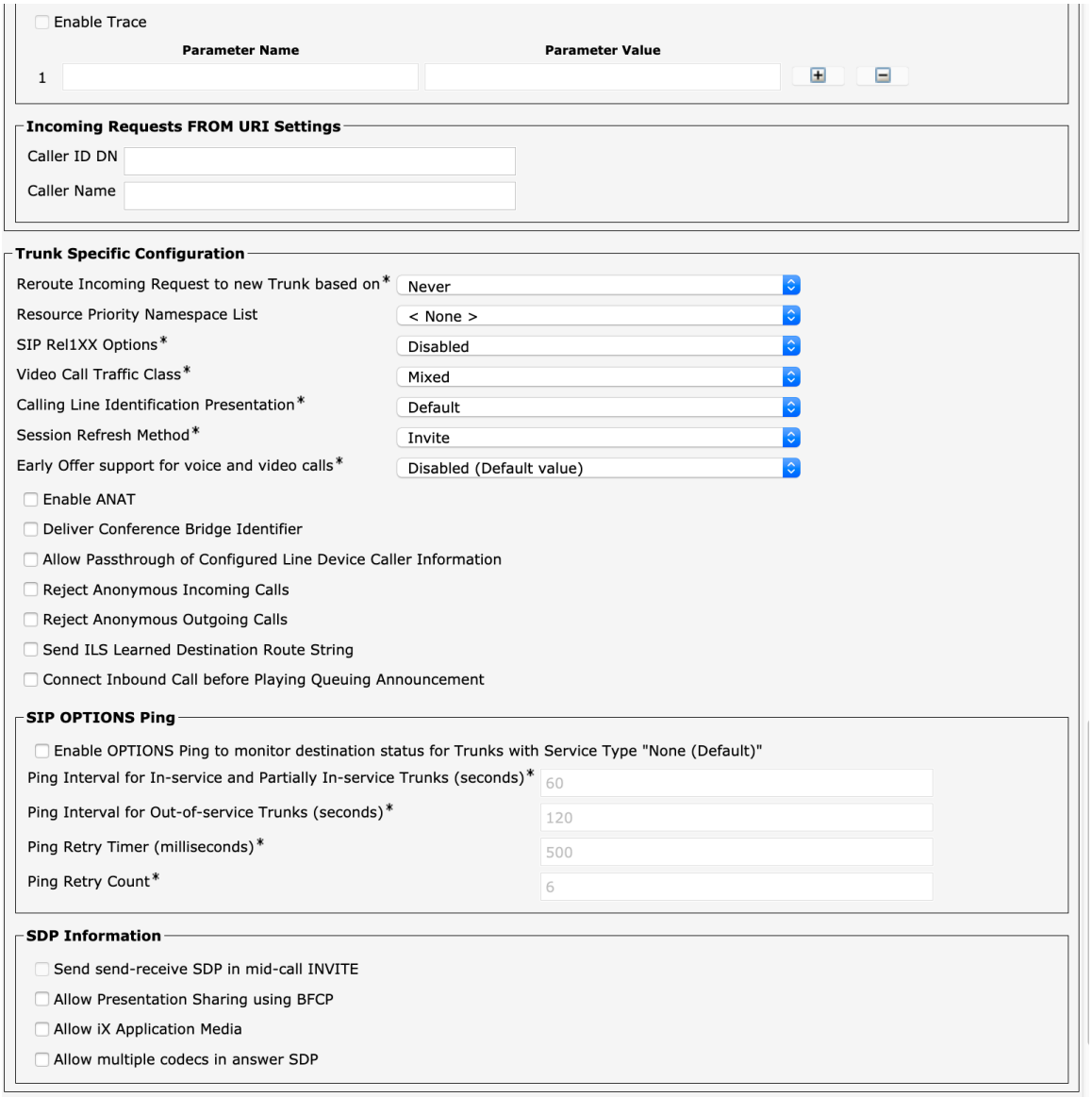
Timer Subscribe Delta (seconds) = 15 (default = 5)

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

Custom SIP Profile Example


SIP Profile Information
Name*
Custom 860 SIP Profile
Description
Custom 860 SIP Profile
Default MTP Telephony Event Payload Type*
101
Early Offer for G.Clear Calls*
Disabled
User-Agent and Server header information*
Send Unified CM Version Information as User-Age
Version in User Agent and Server Header*
Major And Minor
Dial String Interpretation*
Phone number consists of characters 0-9, *, #, ar
Confidential Access Level Headers*
Disabled
Redirect by Application
Disable Early Media on 180
Outgoing T.38 INVITE include audio mline
Offer valid IP and Send/Receive mode only for T.38 Fax Relay
Use Fully Qualified Domain Name in SIP Requests
Assured Services SIP conformance
Enable External QoS**
SDP Information
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*
TIAS and AS
SDP Transparency Profile
Pass all unknown SDP attributes
Accept Audio Codec Preferences in Received Offer*
Default
Require SDP Inactive Exchange for Mid-Call Media Change
Allow RR/RS bandwidth modifier (RFC 3556)
Parameters used in Phone
Timer Invite Expires (seconds)*
180
Timer Register Delta (seconds)*
30
Timer Register Expires (seconds)*
3600
Timer T1 (msec)*
500
Timer T2 (msec)*
4000
Retry INVITE*
6
Retry Non-INVITE*
10
Media Port Ranges
Common Port Range for Audio and Video
Separate Port Ranges for Audio and Video
Start Media Port*
16384


Stop Media Port*
32766
DSCP for Audio Calls
Use System Default
DSCP for Video Calls
Use System Default
DSCP for Audio Portion of Video Calls
Use System Default
DSCP for TelePresence Calls
Use System Default
DSCP for Audio Portion of TelePresence Calls
Use System Default
Call Pickup URI*
x-cisco-serviceuri-pickup
Call Pickup Group Other URI*
x-cisco-serviceuri-opickup
Call Pickup Group URI*
x-cisco-serviceuri-gpickup
Meet Me Service URI*
x-cisco-serviceuri-meetme
User Info*
None
DTMF DB Level*
Nominal
Call Hold Ring Back*
Off
Anonymous Call Block*
Off
Caller ID Blocking*
Off
Do Not Disturb Control*
User
Telnet Level for 7940 and 7960*
Disabled
Resource Priority Namespace
< None >
Timer Keep Alive Expires (seconds)*
300
Timer Subscribe Expires (seconds)*
300
Timer Subscribe Delta (seconds)*
15
Maximum Redirections*
70
Off Hook To First Digit Timer (milliseconds)*
15000
Call Forward URI*
x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*
x-cisco-serviceuri-abbrdial
Conference Join Enabled
RFC 2543 Hold
Semi Attended Transfer
Enable VAD
Stutter Message Waiting
MLPP User Authorization
Normalization Script
Normalization Script
< None >

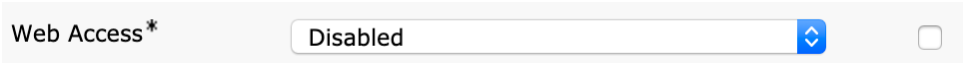


Common Settings

Some settings such as **Web Access** can be configured on an enterprise phone, common phone profile or individual phone level.

Web Access is disabled by default for the Cisco Wireless Phone 840 and 860.

Override common settings can be enabled at either configuration level.

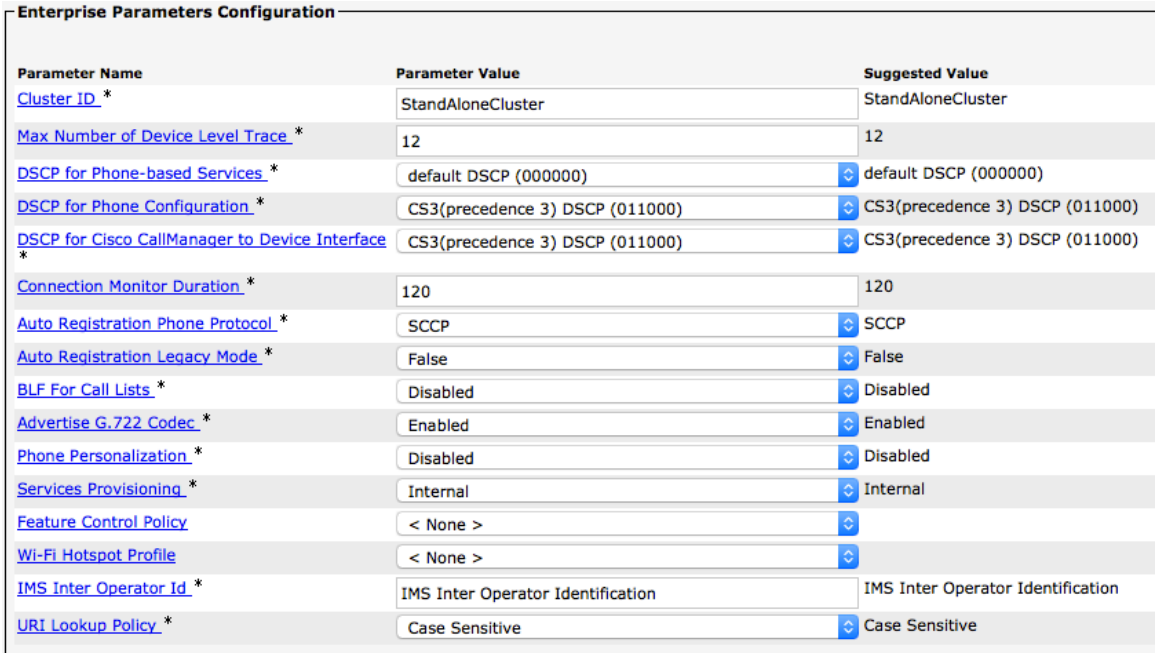


QoS Parameters

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

The default DSCP value for SIP communications and phone configuration is set to CS3.

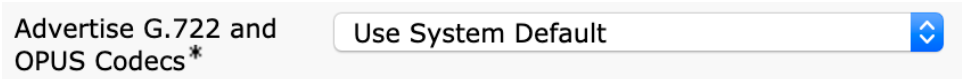
Phone based services are configured to be best effort traffic by default.



G.722 and Opus Advertisement

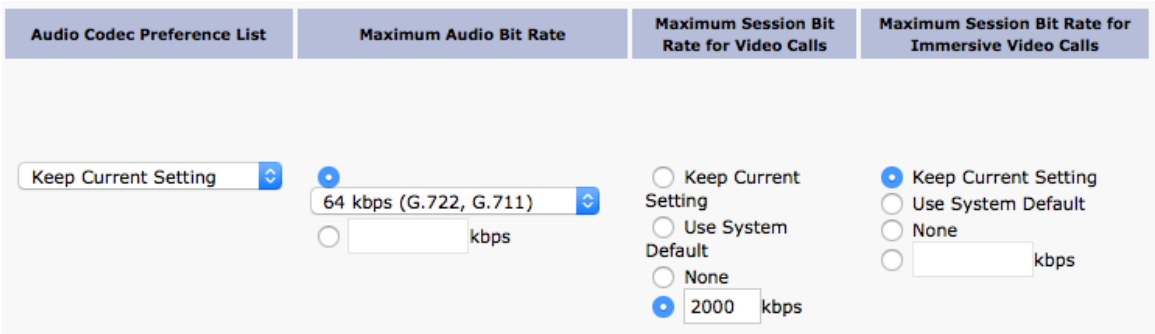
Cisco Unified Communications Manager supports the ability to configure whether G.722 and Opus are to be a supported codec system wide or not.

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



Audio Bit Rates

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



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

Audio Codec	Audio Bit Rate
Opus	6-510 Kbps
G.722 / G.711	64 Kbps
G.729	8 Kbps

Product Specific Configuration Options

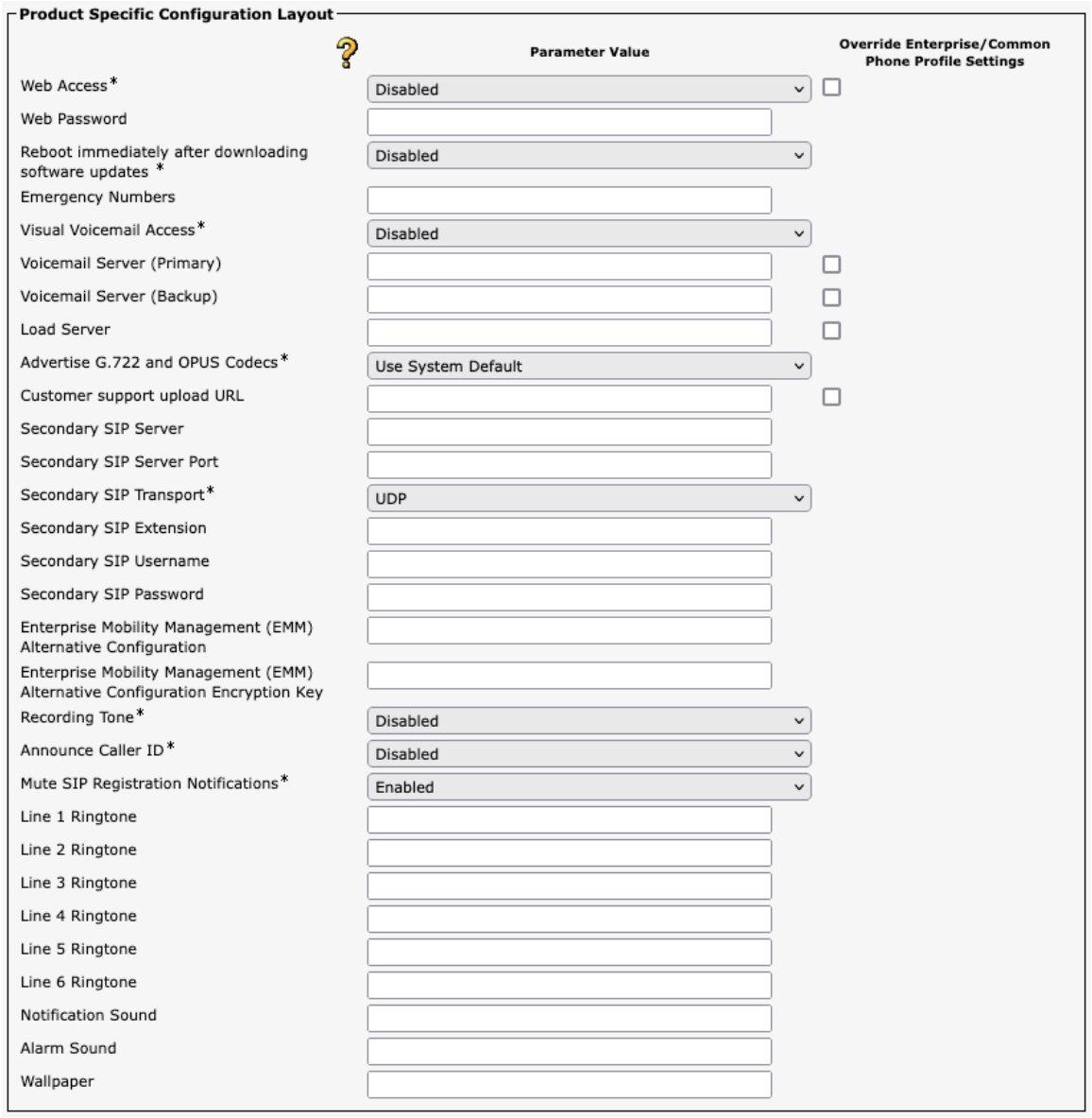
In Cisco Unified Communications Manager Administration, the following configuration options are available for the Cisco Wireless Phone 840 and 860.

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

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

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

Cisco Wireless Phone 840 and 860 Configuration Options



Field Name	**Description**
Web Access	This parameter specifies whether the phone will accept connections from a web browser or other HTTP client. Disabling the web server functionality of the phone will block access to the phones internal web pages. These pages provide statistics and configuration information.
Web Password	This parameter specifies the password to access the phone's Web interface. Enter a 8-127 character password.
Reboot immediately after downloading software updates	This parameter specifies whether the phone will reboot immediately after downloading a software update or if it will notify the user to manually reboot. The phone must be rebooted to apply software updates.
Emergency Numbers	This parameter specifies the emergency numbers that can be dialed without unlocking the phone keypad. For example, in the United States, the 911 emergency number is a good candidate so that it can be dialed without unlocking

	the phone. To specify more than one number, use a comma as separator. For example, if you want to enter 411, 511, and 911 as emergency numbers, then enter 411,511,911 in the field without spaces.
Visual Voicemail Access	This parameter enables or disables access to Visual Voicemail.
Voicemail Server (Primary)	This parameter contains the address of the primary voicemail server for Visual Voicemail.
Voicemail Server (Backup)	This parameter contains the address of the backup voicemail server for Visual Voicemail.
Load Server	This parameter specifies that the phone will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IP address (using standard IP addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades.
Advertise G.722 and Opus Codecs	This parameter specifies whether the phone will advertise the G.722 and Opus codecs or not. Codec negotiation involves two steps: first, the phone must advertise the supported codec(s) to the Cisco Unified CallManager (not all endpoints support the same set of codecs). Second, when the Cisco Unified CallManager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. The options are Use System Default (this phone will defer to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (this phone will not advertise G.722 or Opus support), and Enabled (this phone will advertise G.722 and Opus support).
Customer support upload URL	This URL is used to upload problem report files when the user has run the “Problem Reporting Tool” on the endpoint.
Secondary SIP Server	This parameter contains the address of the server for the optional second registration.
Secondary SIP Server Port	This parameter contains the far-end port number for the optional second registration.
Secondary SIP Transport	This parameter contains the transport type for the optional second registration.
Secondary SIP Extension	This parameter contains the SIP extension for the optional second registration.
Secondary SIP Username	This parameter contains the SIP username for the optional second registration.
Secondary SIP Password	This parameter contains the SIP password for the optional second registration.
Enterprise Mobility Management (EMM) Alternative Configuration	This parameter specifies the file to configure the native Cisco applications, when the phone is not managed by an Enterprise Mobility Management (EMM) solution.
Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key	This parameter specifies the encryption key used to generate the Enterprise Mobility Management (EMM) Alternative Configuration file.

Recording Tone	This parameter 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.
Announce Caller ID	This parameter specifies whether the phone will announce caller identification information for incoming calls or not.
Mute SIP Registration Notifications	This parameter specifies whether the notifications for SIP registration events will be muted or not.
Line 1 Ringtone	This parameter specifies the ringtone for line 1. Can specify a pre-existing ringtone or a ringtone file to download and use for line 1.
Line 2 Ringtone	This parameter specifies the ringtone for line 2. Can specify a pre-existing ringtone or a ringtone file to download and use for line 2.
Line 3 Ringtone	This parameter specifies the ringtone for line 3. Can specify a pre-existing ringtone or a ringtone file to download and use for line 3.
Line 4 Ringtone	This parameter specifies the ringtone for line 4. Can specify a pre-existing ringtone or a ringtone file to download and use for line 4.
Line 5 Ringtone	This parameter specifies the ringtone for line 5. Can specify a pre-existing ringtone or a ringtone file to download and use for line 5.
Line 6 Ringtone	This parameter specifies the ringtone for line 6. Can specify a pre-existing ringtone or a ringtone file to download and use for line 6.
Notification Sound	This parameter specifies the notification sound files to download. Multiple files can be specified using the comma separated format. Once the files have been downloaded, the notification sound will need to be configured via the Custom Settings application, Android Settings, or in other application settings.
Alarm Sound	This parameter specifies the alarm sound files to download. Multiple files can be specified using the comma separated format. Once the files have been downloaded, the alarm sound will need to be configured via the Custom Settings application, Android Settings, or in other application settings.
Wallpaper	This parameter specifies the wallpaper files to download. Multiple files can be specified using the comma separated format. Once the files have been downloaded, the lock screen wallpaper and home screen wallpaper will need to be configured via the Custom Settings application or Android Settings.

Note: If wanting to keep the web password or secondary SIP password enabled long-term, or if utilizing the Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key option, then should utilize a secure profile with TFTP encryption enabled.

Wallpaper files are downloaded to the **/sdcard/pictures** folder of the Cisco Wireless Phone 840 and 860, which will need to be part of the file path when configuring the wallpaper in the Custom Settings application.

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

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

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

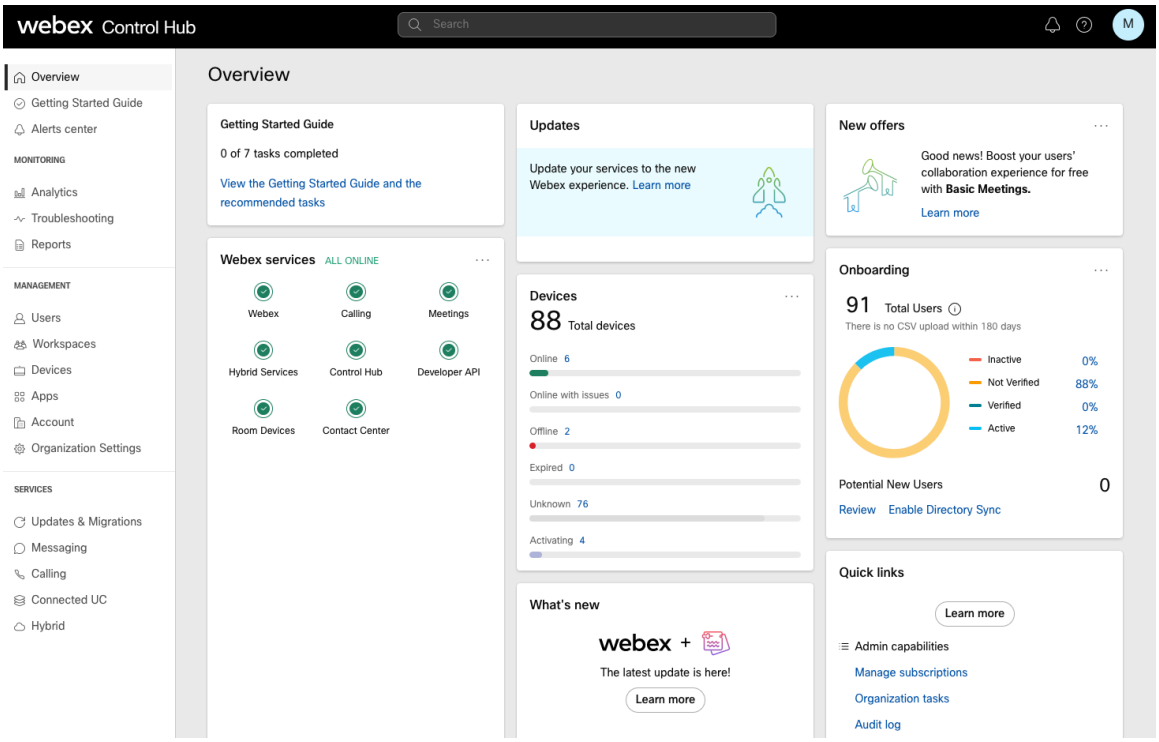
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

https://www.cisco.com/c/en/us/support/collaboration-endpoints/webex-wireless-phone/products-release-notes-list.html

Webex Calling

Webex Calling enables cloud registration, therefore a VPN connection is not required as long as the Cisco Wireless Phone 840 or 860 has direct internet connectivity.

The Cisco Wireless Phone 840 and 860 must be running firmware version 1.6(0) or later to be able to register to Webex Calling.



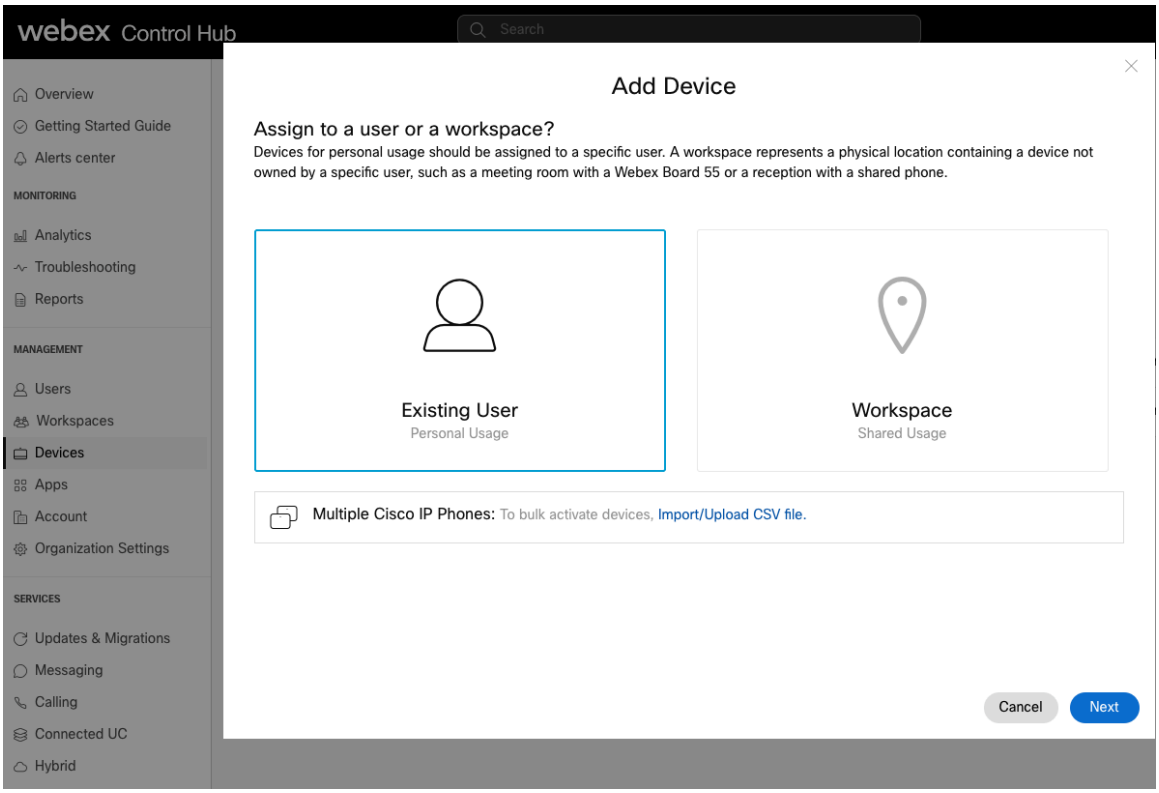
A Cisco Wireless Phone 840 or 860 can be added to Webex Calling and assigned to a user for personal usage or as a workspace for shared usage.

Personal Usage

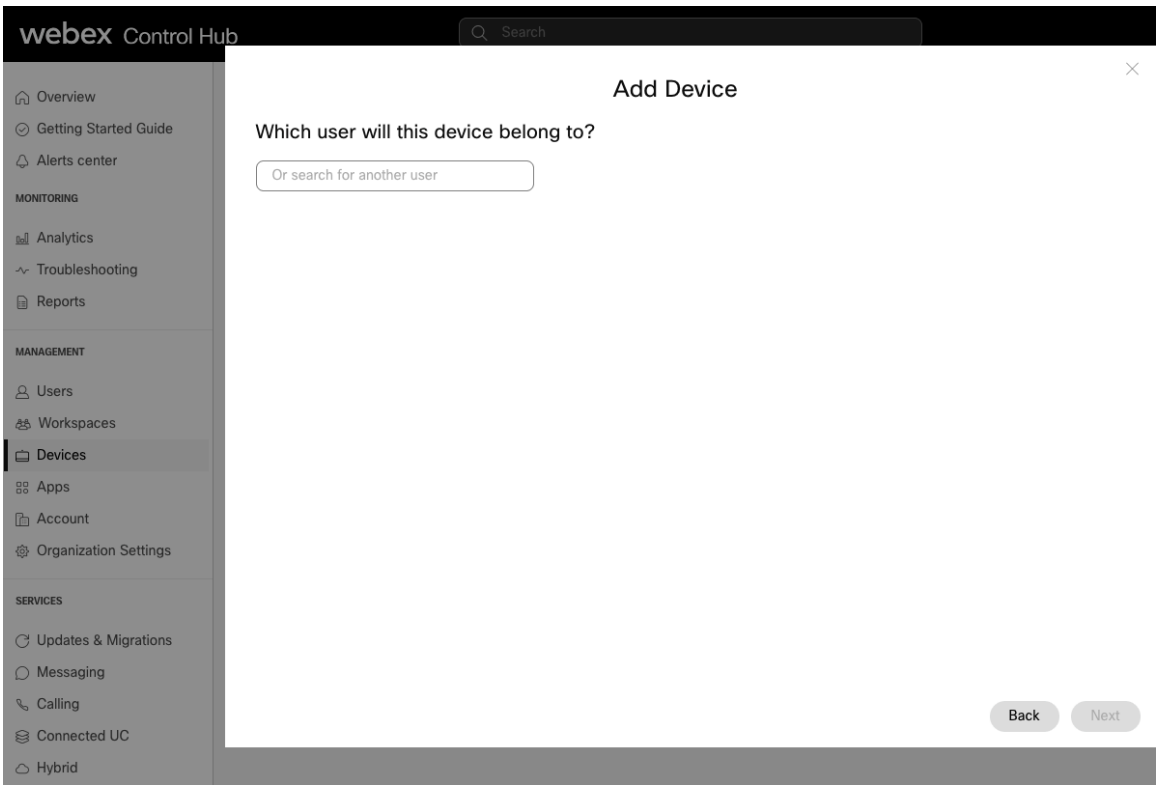
A Cisco Wireless Phone 840 or 860 can be configured for a user for personal usage via **Devices**.

To add a device for a user, navigate to **Devices**, then select **Add Device**.

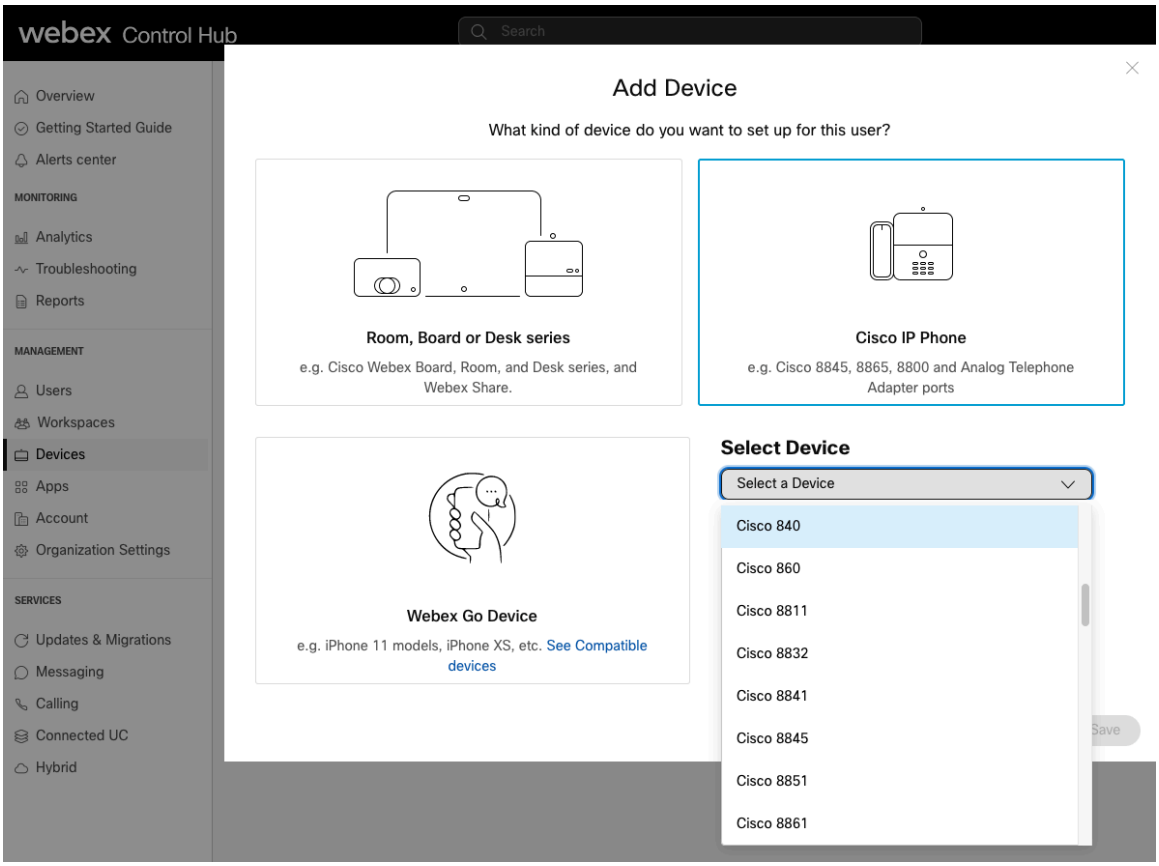
On the next screen, select **Existing User**, then click **Next**.



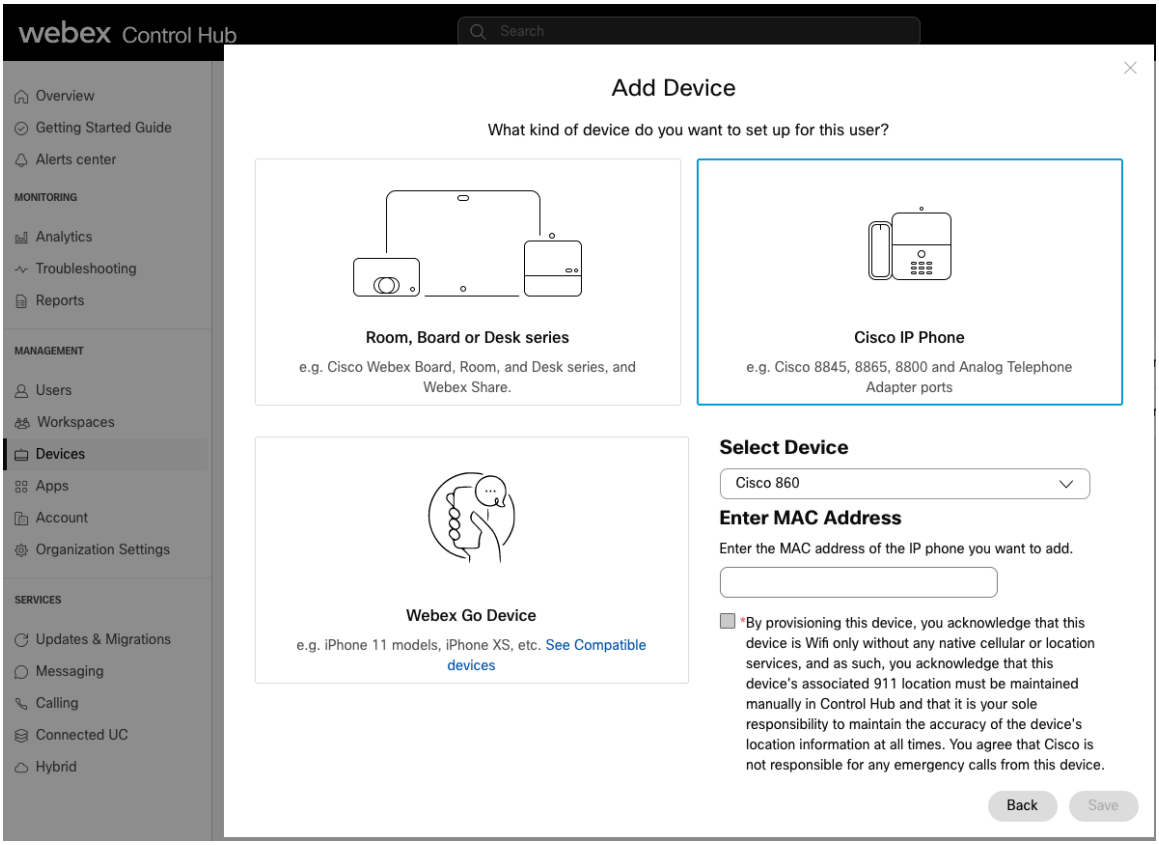
Search for the user to assign the Cisco Wireless Phone 840 or 860 to, then click **Next**.



Select **Cisco IP Phone**, then either **Cisco 840** or **Cisco 860** from the drop-down list.



Enter the **MAC Address** of the Cisco Wireless Phone 840 or 860, check the box below, then select **Save**.

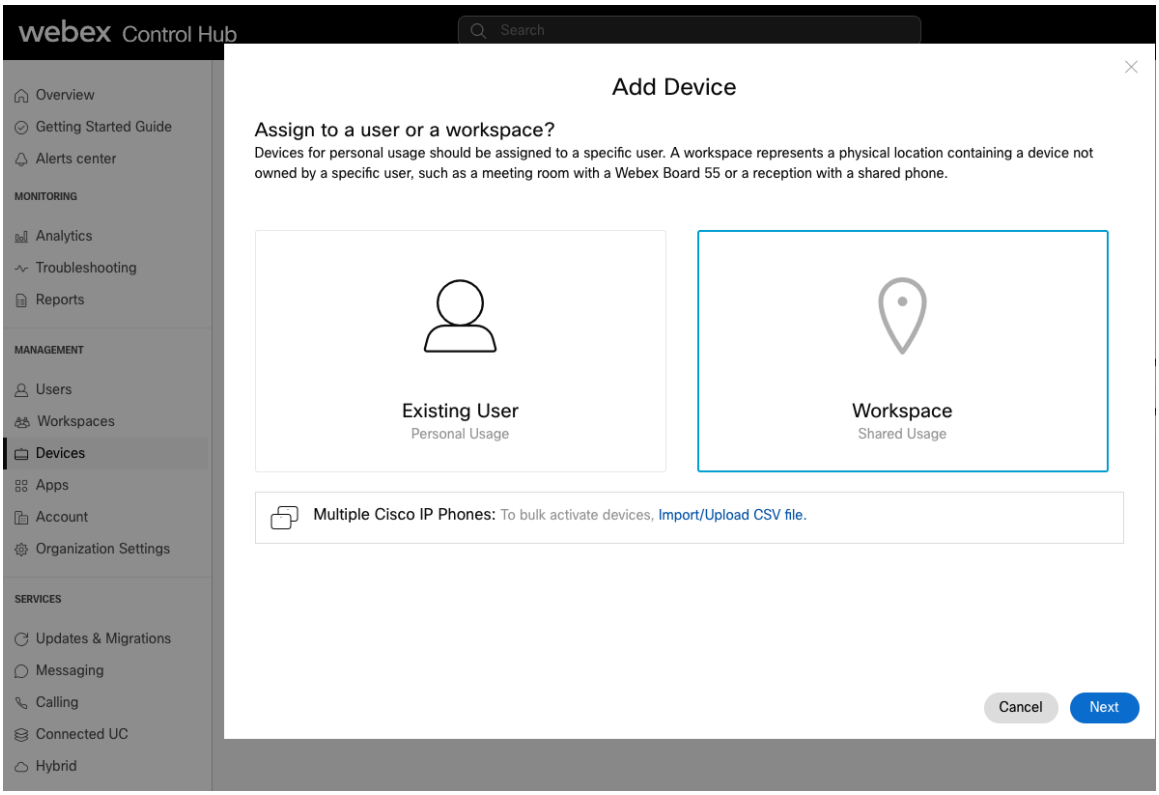


Select the user via **Users** to configure or modify services.

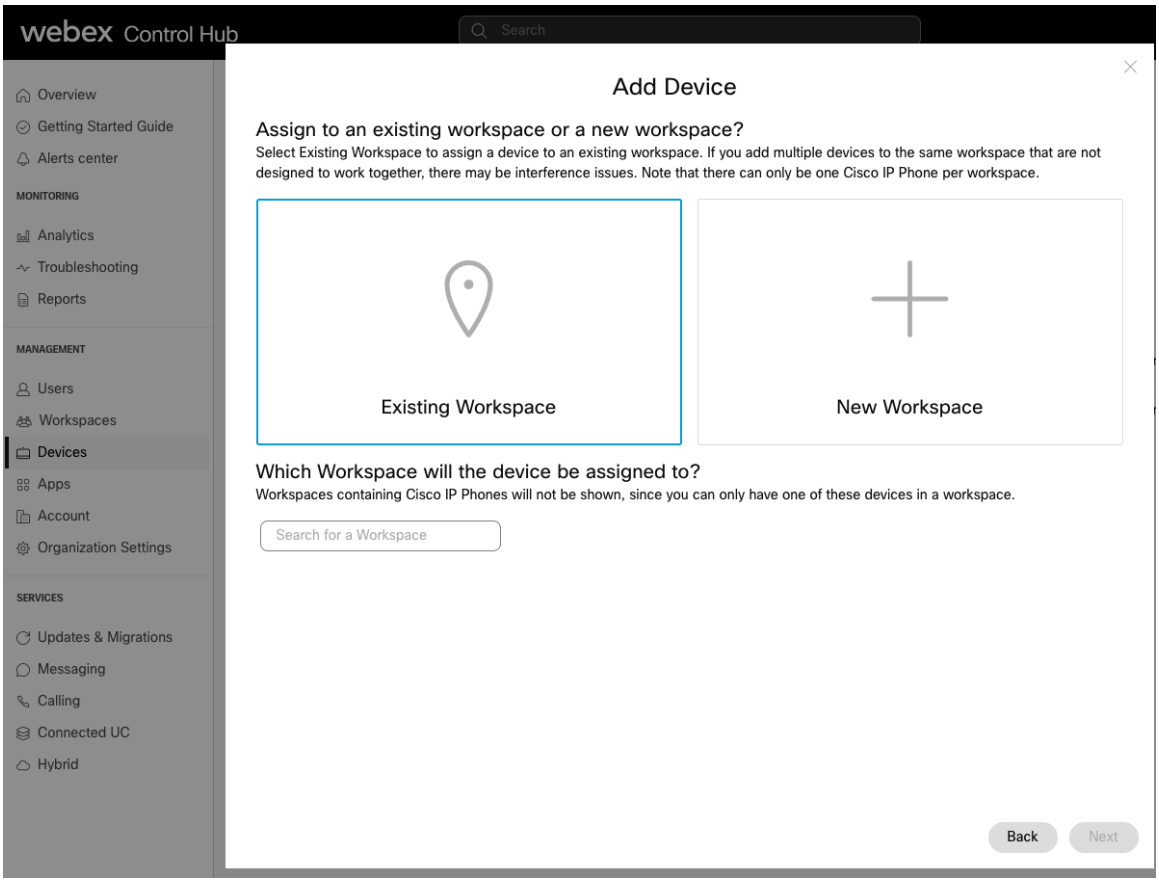
Shared Usage

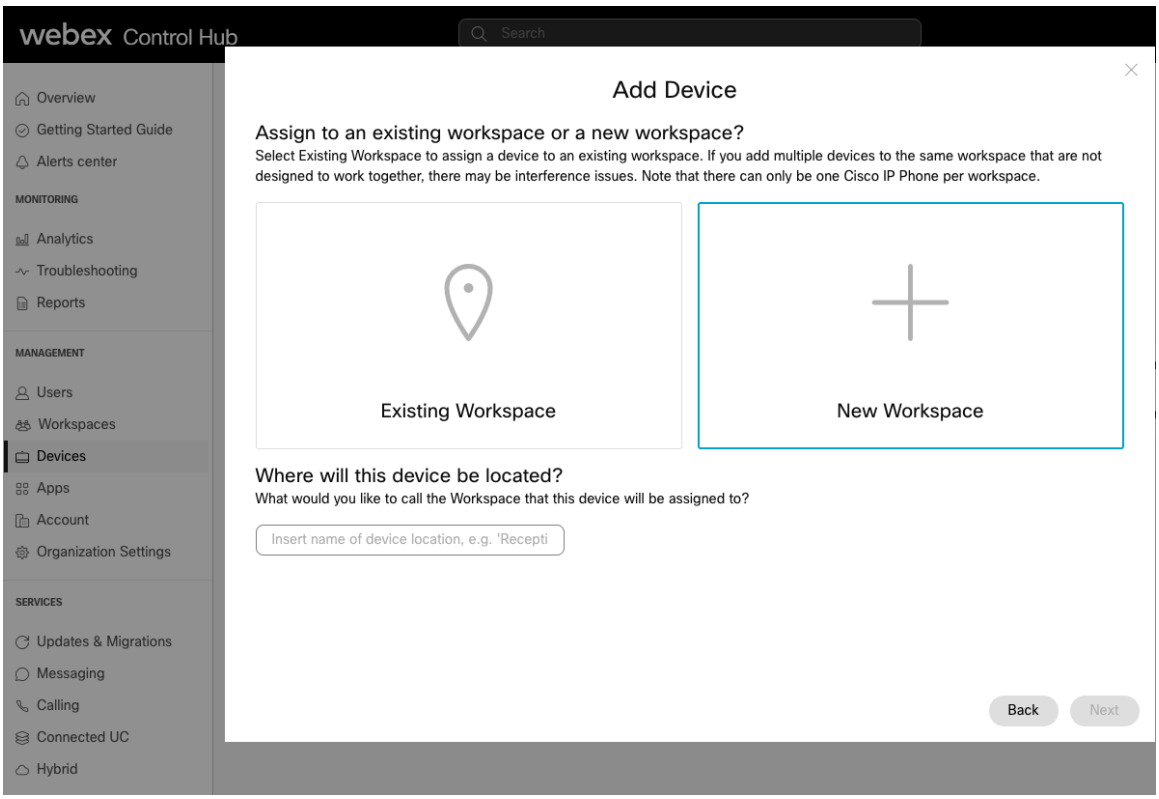
A Cisco Wireless Phone 840 or 860 can be configured as a workspace either via **Devices** or **Workspaces**.

To add a workspace via **Devices**, navigate to **Devices**, then select **Add Device**.
On the next screen, select **Workspace**, then click **Next**.

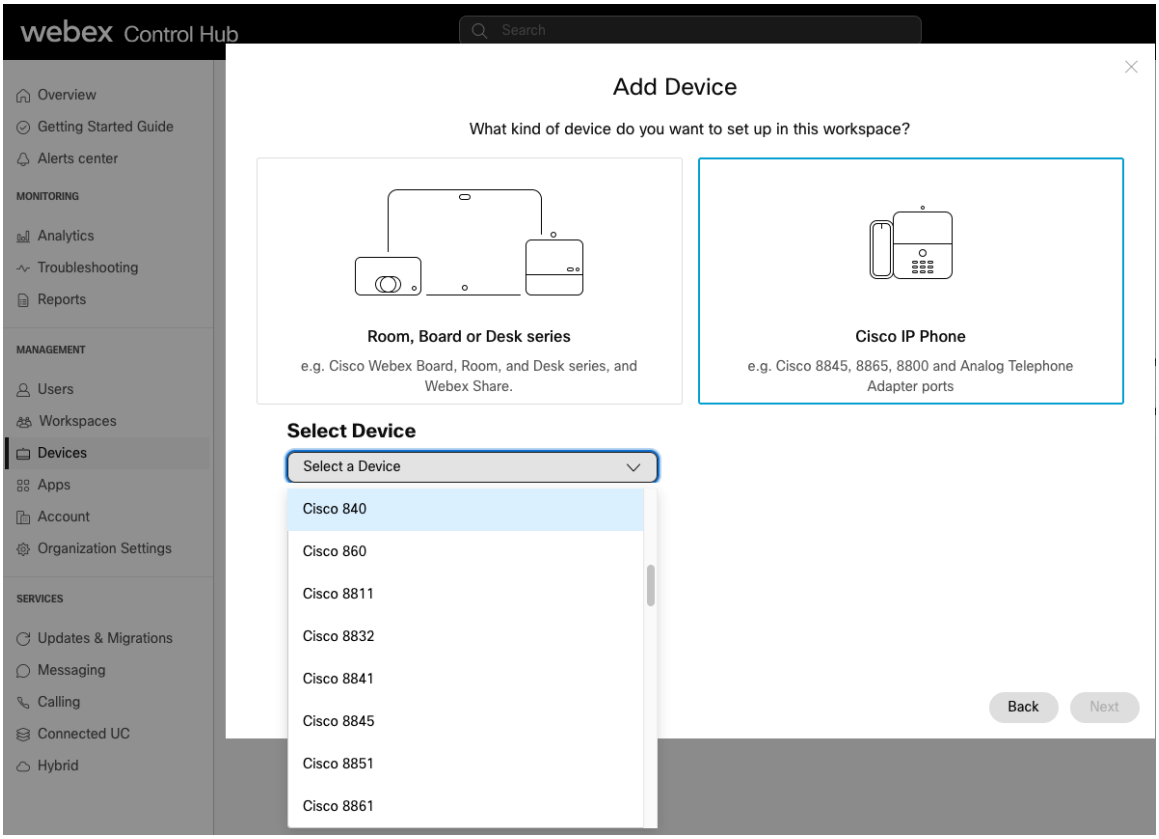


Select either **Existing Workspace** or **New Workspace**.
Depending on which option is selected, either search for or enter the workspace name, then click **Next**.

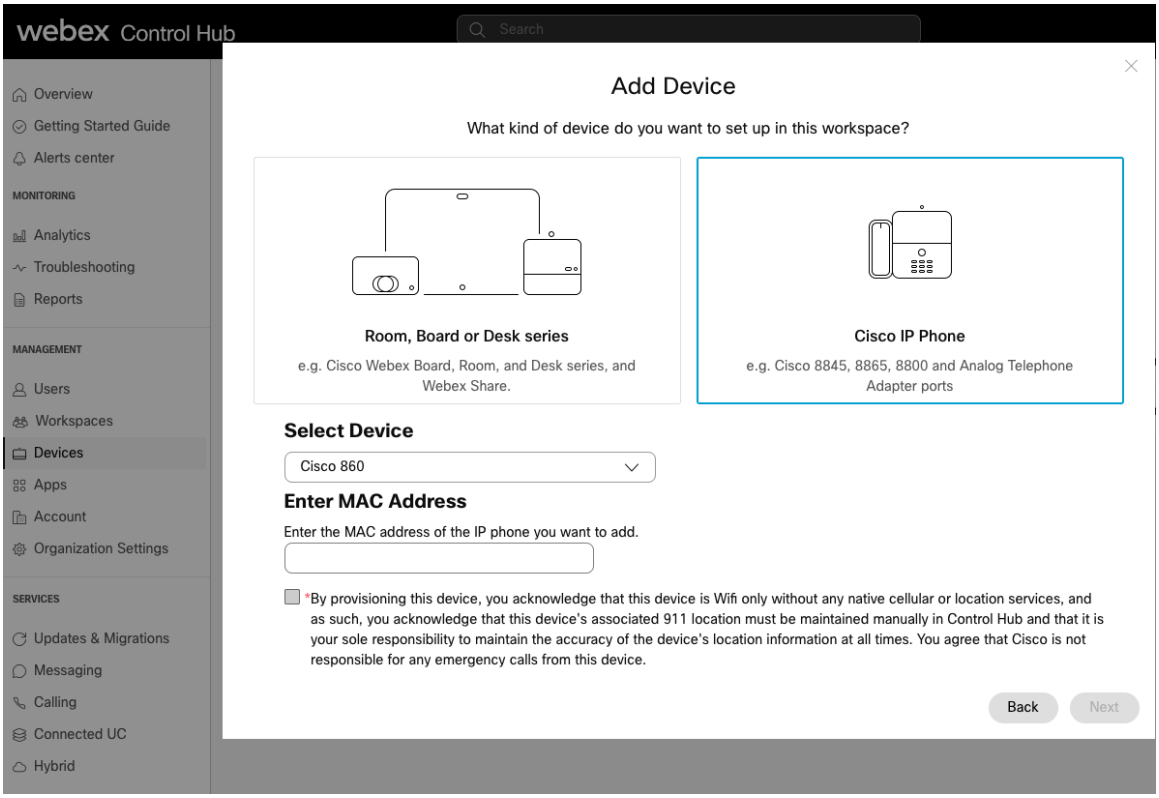




Select **Cisco IP Phone**, then either **Cisco 840** or **Cisco 860** from the drop-down list.



Enter the **MAC Address** of the Cisco Wireless Phone 840 or 860, check the box below, then select **Next**.

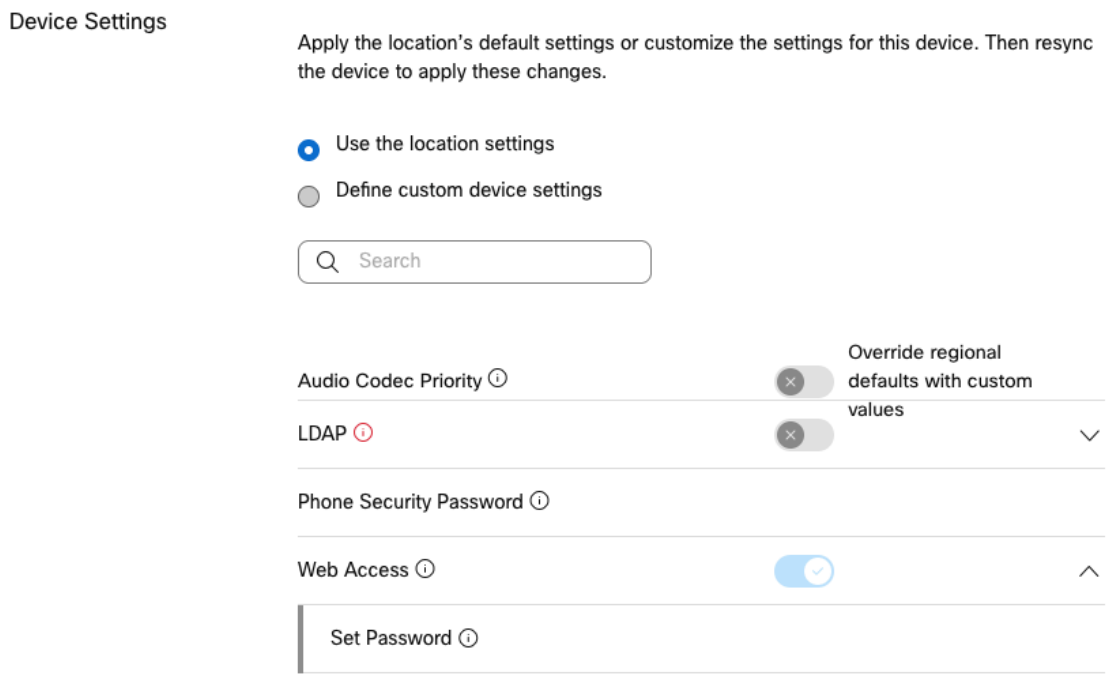


Configure the **Location**, **Phone Number**, **Extension**, and **Calling Plan** on the next screen, then select **Save**.

Select the existing workspace via **Workspaces** to configure or modify services.

Device Settings

The following configuration options are available for the Cisco Wireless Phone 840 and 860.



For information on network requirements for Webex Calling, refer to the **Port Reference Information for Webex Calling** document at this URL:

https://help.webex.com/en-us/article/b2exve/Port-Reference-Information-for-Webex-Calling

For more information, see the **Cisco Wireless Phone 840 and 860 Administration Guide** at this URL:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Configuring the Cisco Wireless Phone 840 and 860

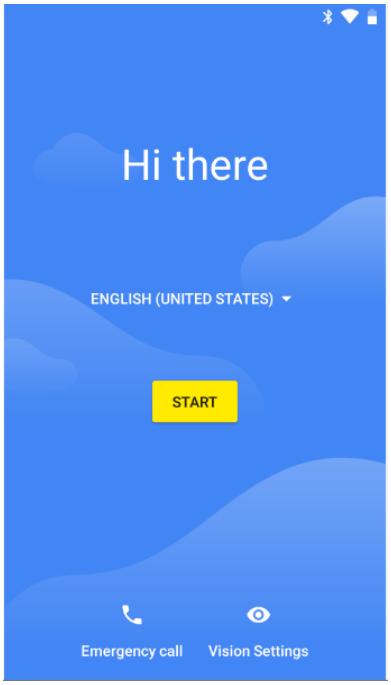
To configure the Cisco Wireless Phone 840 and 860, either use an Enterprise Mobility Management (EMM) application or the Cisco Wireless Phone Configuration Management utility for central provisioning, or use the local user interface for manual configuration.

Enterprise Mobility Management (EMM)

If wanting to utilize a management tool to manage the Cisco Wireless Phone 840 and 860 configuration plus the ability to allow third-party applications, then an Enterprise Mobility Management (EMM) application should be leveraged.

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

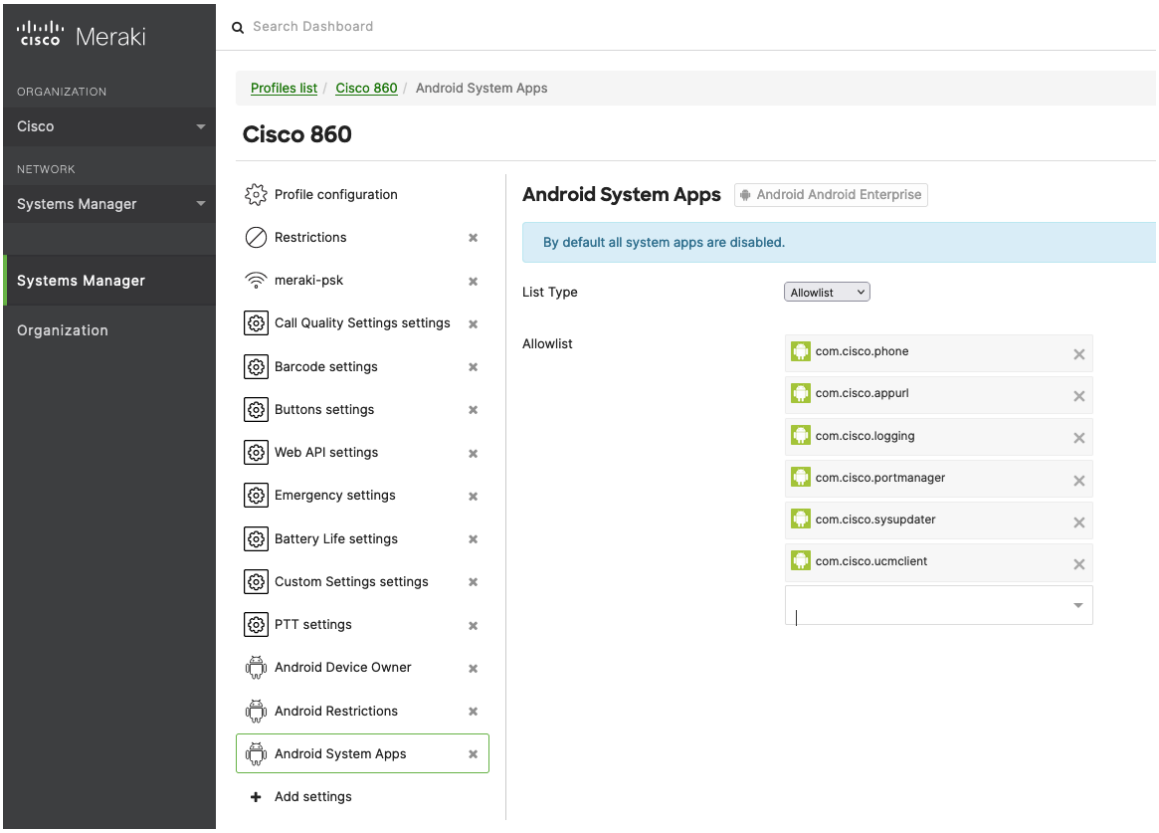
On the startup screen, quickly tap the display 6 times and then can scan a QR code to enroll the Cisco Wireless Phone 840 or 860 to the EMM via the device owner method.



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

- **Cisco Phone** = com.cisco.phone
- **Application URLs** = com.cisco.appurl
- **Diagnostics** = com.cisco.diagnostics
- **Logging** = com.cisco.logging
- **Port Manager** = com.cisco.portmanager

- **System Updater** = com.cisco.sysupdater
- **UCM Client** = com.cisco.ucmclient

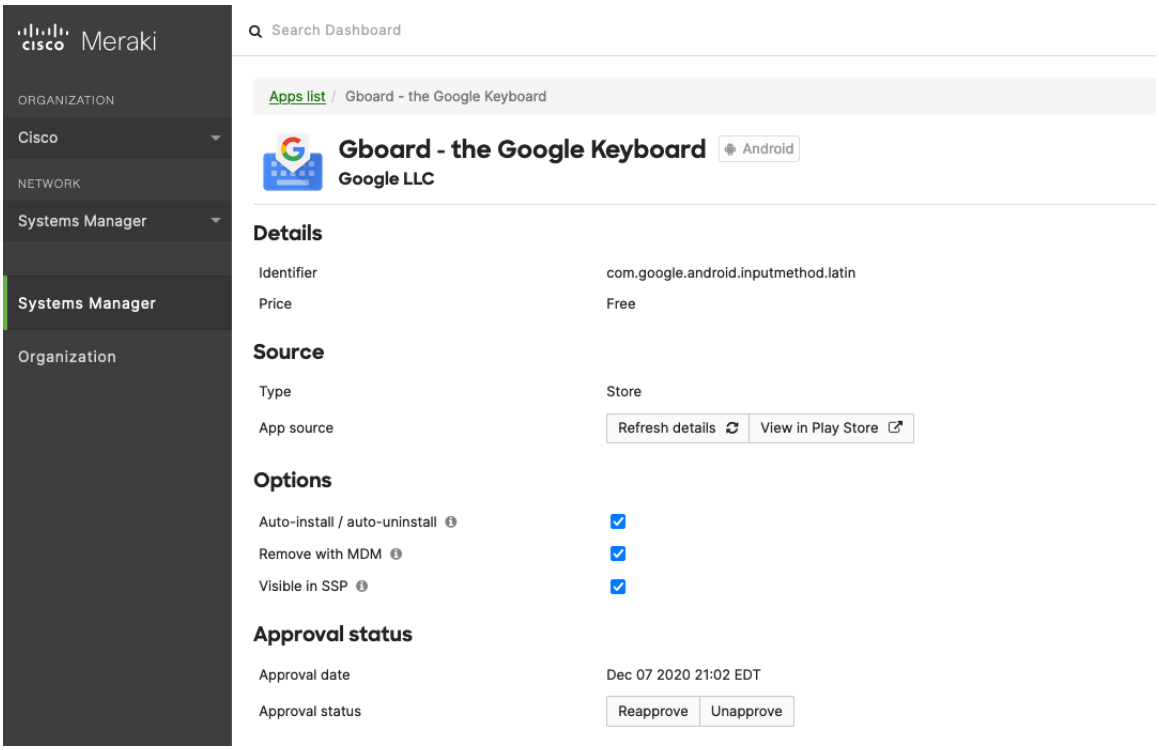


Below is the list of Cisco applications specific to the Cisco Wireless Phone 840 and 860 that will be available in the Google Play Store and can optionally be added when enrolling the phone using the device owner method.

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

Other applications can be allowed as necessary.

Depending on the EMM platform utilized, the **Gboard - the Google Keyboard** application may also need to be added when enrolling the phone using the device owner method



Please see the EMM application documentation for additional information.

Note: If wanting to automatically issue certificates to the Cisco Wireless Phone 840 and 860 in bulk, then need to utilize an EMM applicaton.

Cisco Wireless Phone Configuration Management Utility

If wanting to utilize a management tool to manage the Cisco Wireless Phone 840 and 860 configuration and use of third-party applications is not allowed, then it is recommended to utilize the an Cisco Wireless Phone Configuration Management utility.

With the 1.5(0) release, the Cisco Wireless Phone Configuration Management utility (https://configure.cisco.com) is now an additional option for Cisco Wireless Phone 840 and 860 phone management.

A Cisco.com account is required to access the Cisco Wireless Phone Configuration Management utility.

To enable the Cisco Wireless Phone 840 and 860 to utilize the configuration file generated by the utility, the phone must be factory reset then scan the QR code generated by the utility at the startup screen. Failure to scan the code to allow the utility to manage the phone will not enable the phone to download the configuration file.

Note: The Cisco Wireless Phone Configuration Management Utility is currently not supported for Cisco Wireless Phone 840 or 860 registered to Webex Calling.

Creating Configuration Files

To create a downloadable configuration file using the Cisco Wireless Phone Configuration Management utility, navigate to the **Deployment Configuration** tab and configure the necessary application parameters.

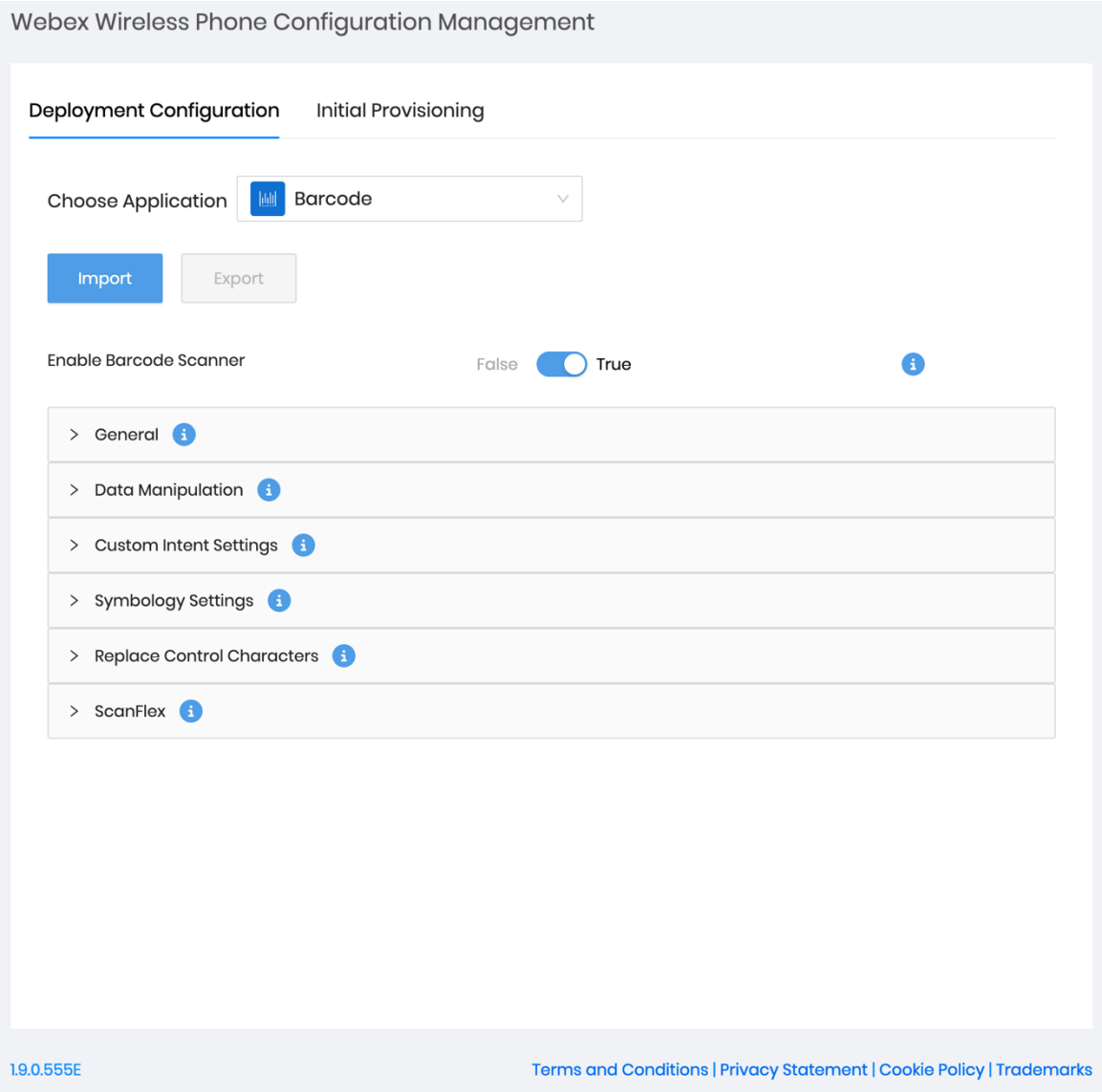
Select **Export** to save the configuration file, which is exported in ZIP format.

Configure Application Settings

Select the necessary application from the drop-down list then configure the necessary parameters.

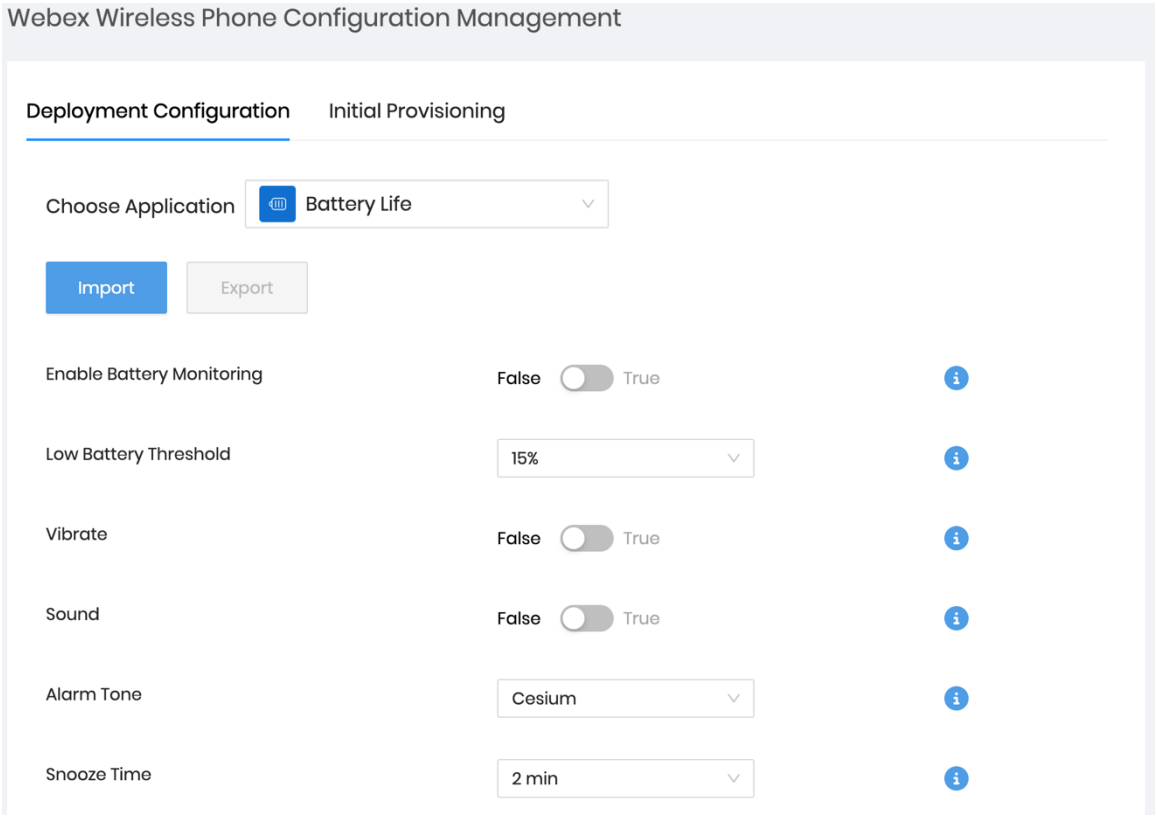
Barcode

To configure the Barcode settings select **Barcode** from the drop-down list.



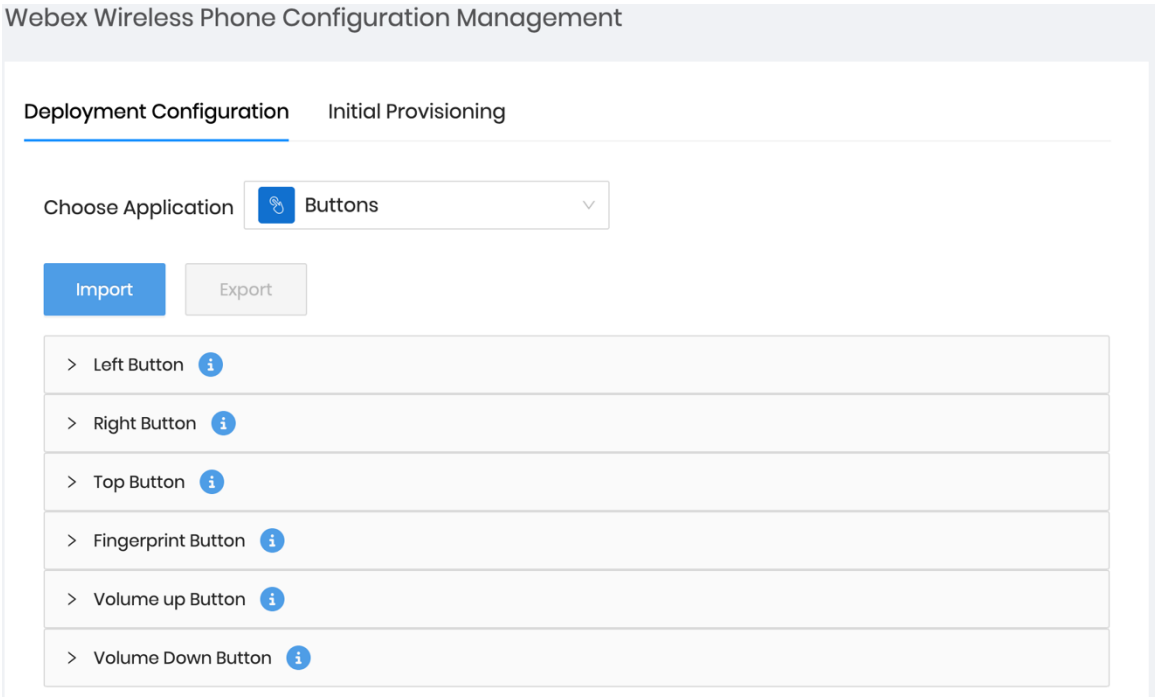
Battery Life

To configure the Battery Life settings select **Battery Life** from the drop-down list.



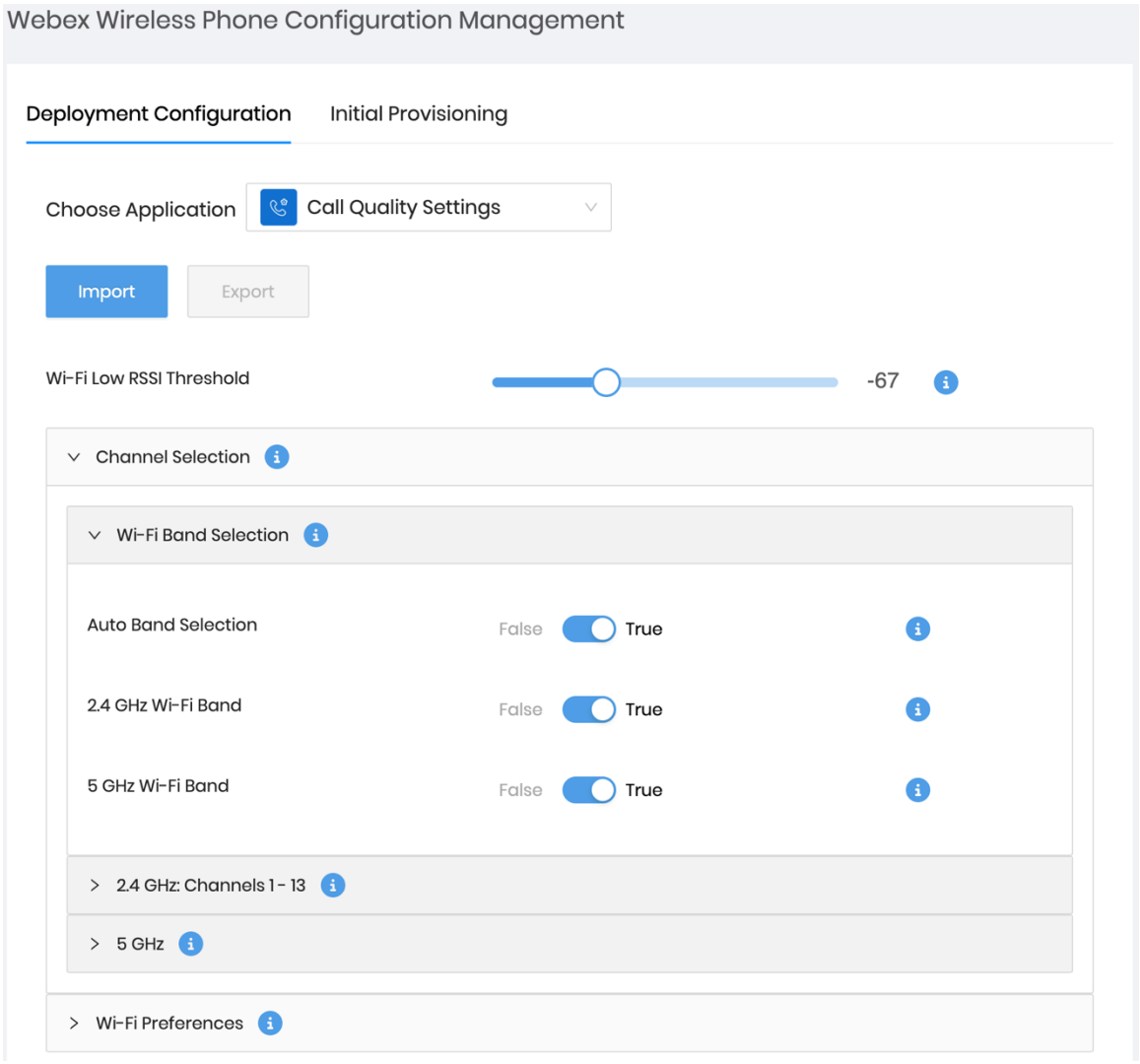
Buttons

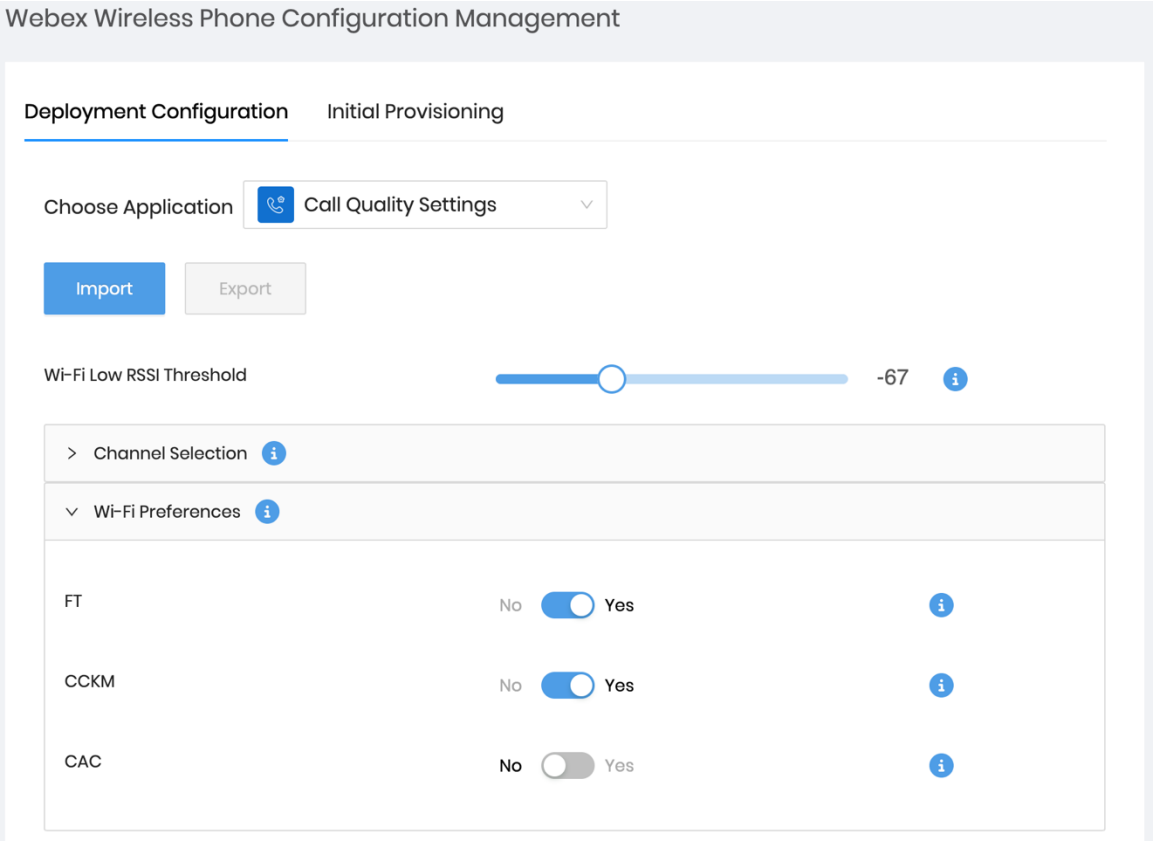
To configure the Buttons settings select **Buttons** from the drop-down list.



Call Quality Settings

To configure the Call Quality Settings select **Call Quality Settings** from the drop-down list.


Webex Wireless Phone Configuration Management
Deployment Configuration
Initial Provisioning
Choose Application
Call Quality Settings
Import
Export
Wi-Fi Low RSSI Threshold
-67
Channel Selection
Wi-Fi Band Selection
Auto Band Selection
False
True
2.4 GHz Wi-Fi Band
False
True
5 GHz Wi-Fi Band
False
True
2.4 GHz: Channels 1 - 13
5 GHz
Wi-Fi Preferences

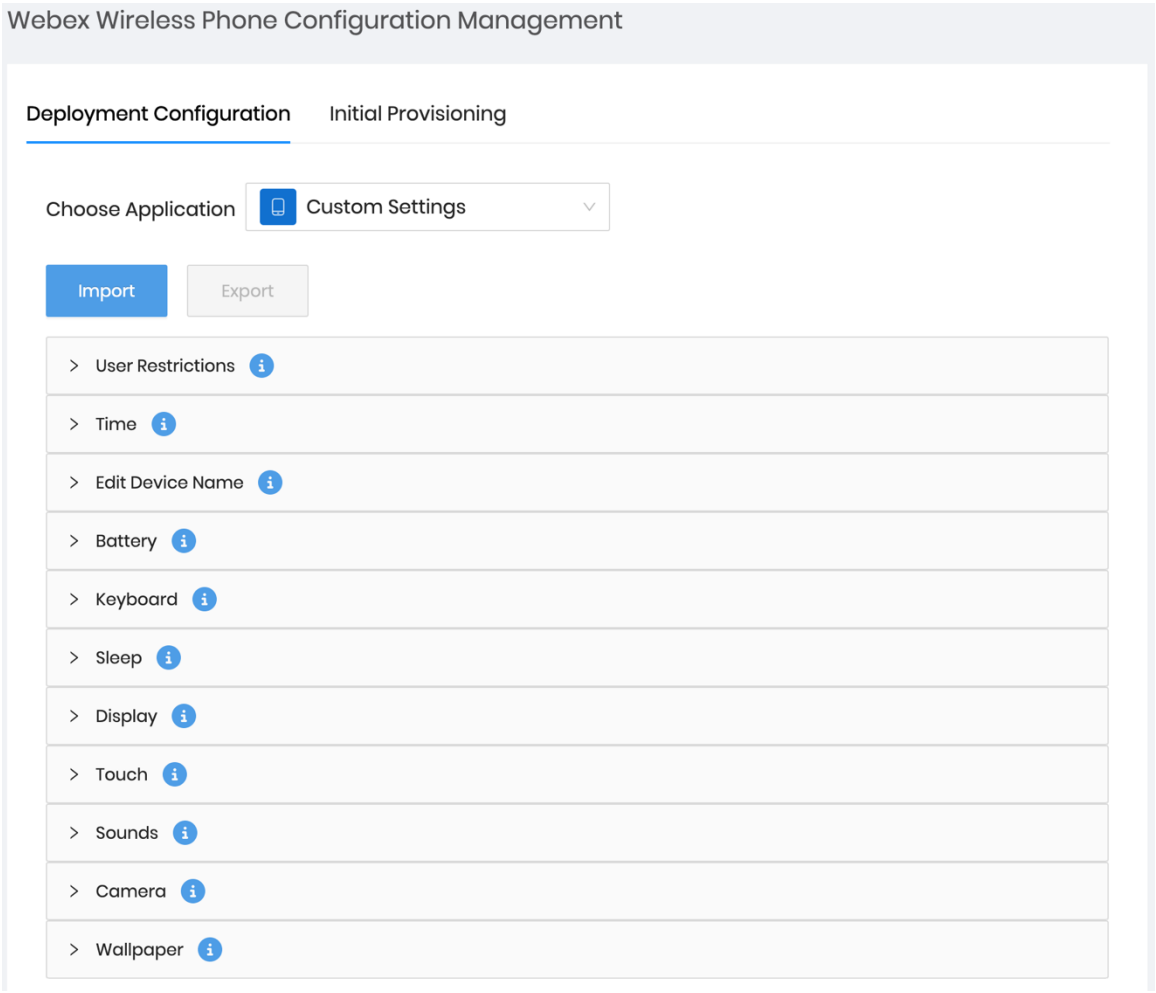


Note: The 1.8(0) release enables the option to disable **CAC** (Call Admission Control).

With the 1.9(0) release, **CAC** (Call Admission Control) is disabled by default and is now an opt-in feature.

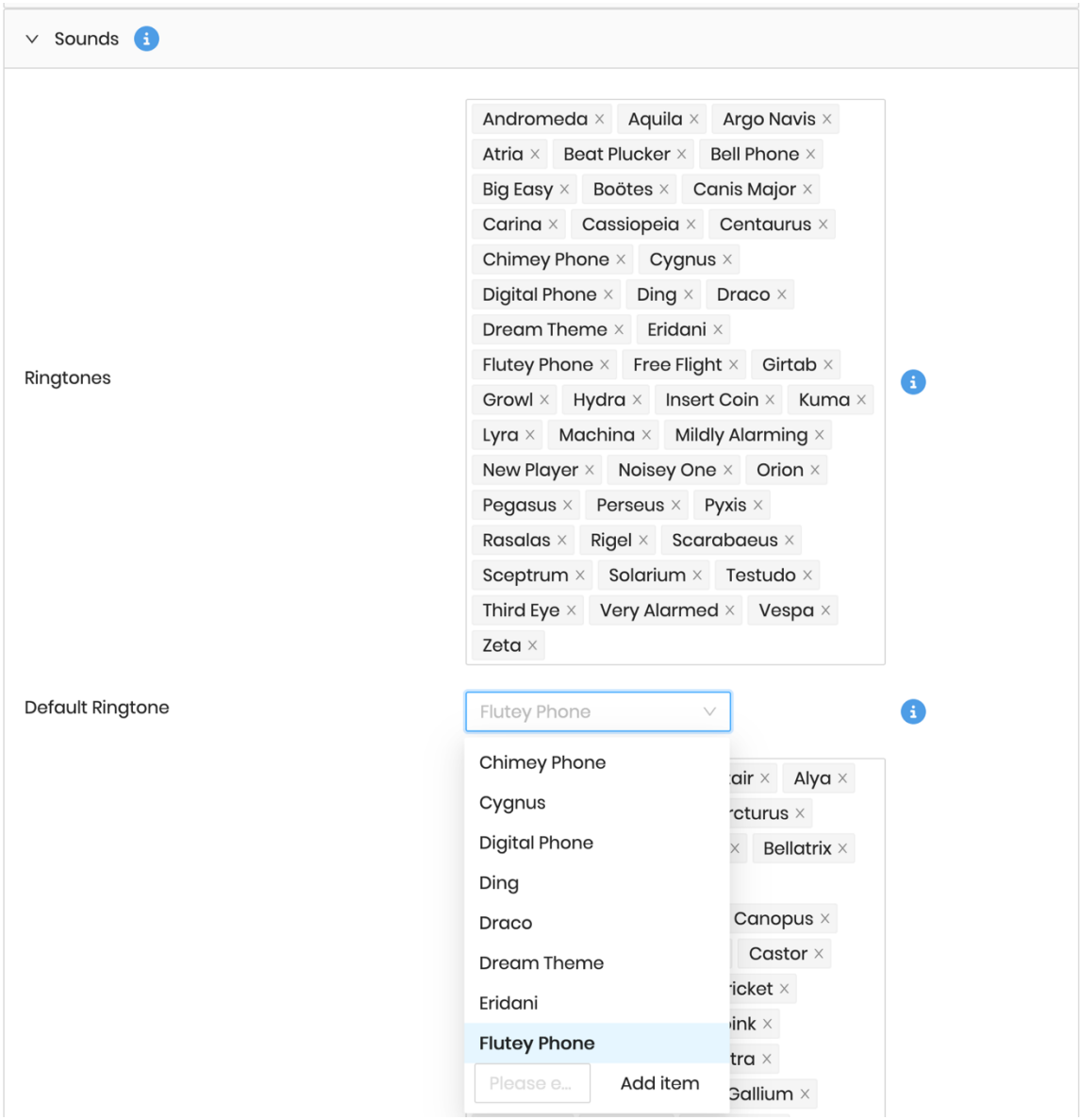
Custom Settings

To configure the Custom Settings select **Custom Settings** from the drop-down list.



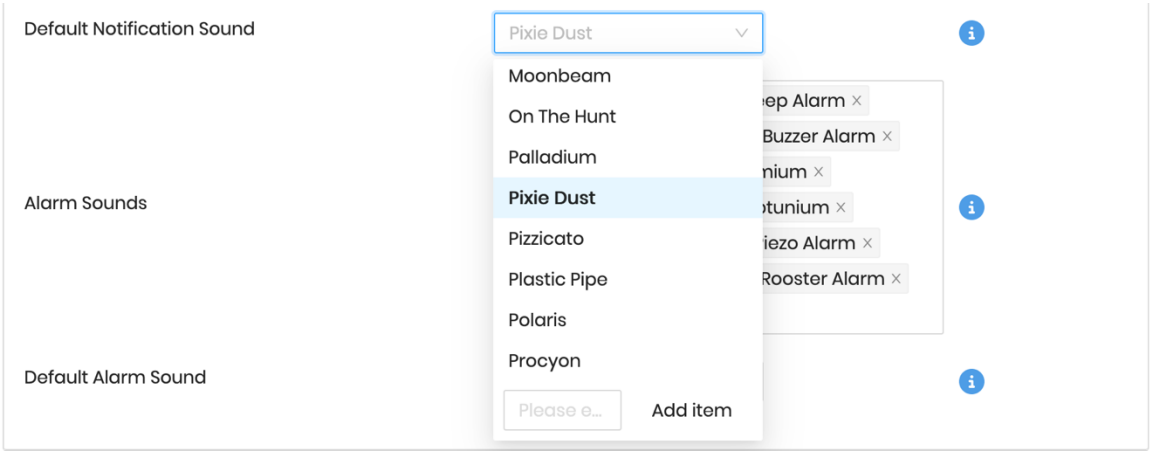
The **Default Ringtone** can be managed within the **Sounds** menu.

If wanting to configure a custom ringtone as the **Default Ringtone**, enter the name of the notification sound, then select **Add item**.



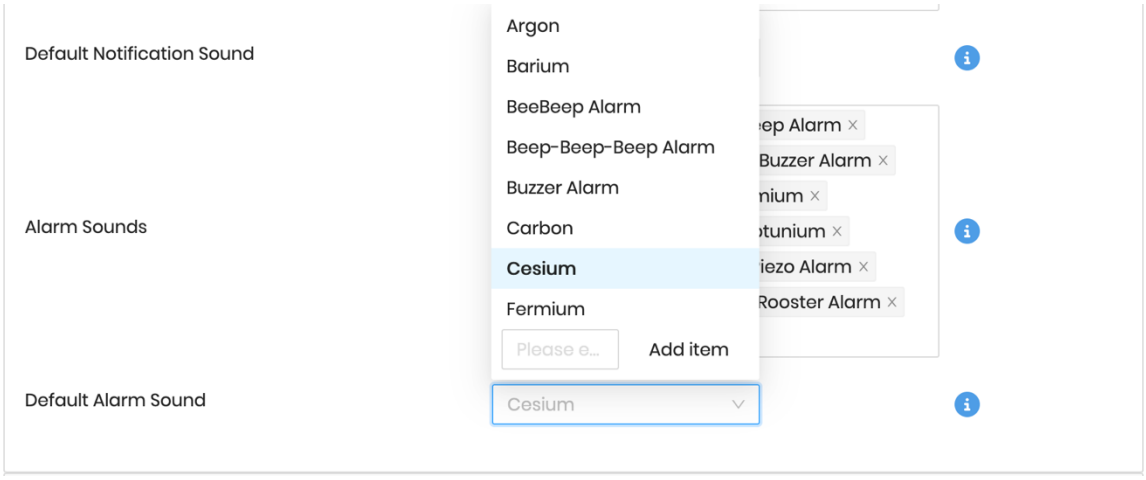
The **Default Notification Sound** can be managed within the **Sounds** menu.

If wanting to configure a custom notification sound as the **Default Notification Sound**, enter the name of the notification sound, then select **Add item**.

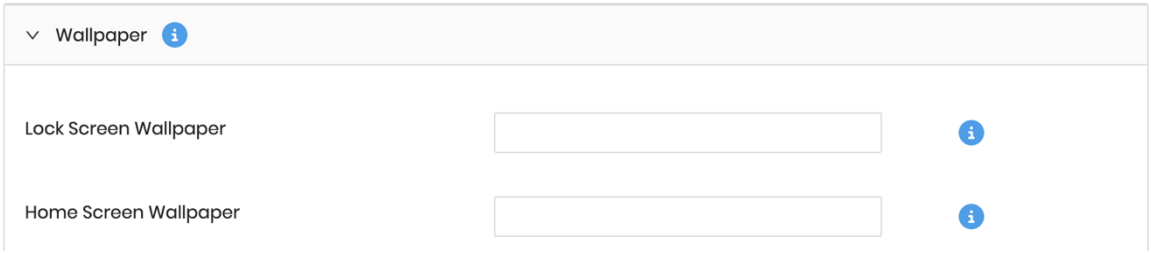


The **Default Alarm Sound** can be managed within the **Sounds** menu.

If wanting to configure a custom alarm sound as the **Default Alarm Sound**, enter the name of the alarm sound, then select **Add item**.

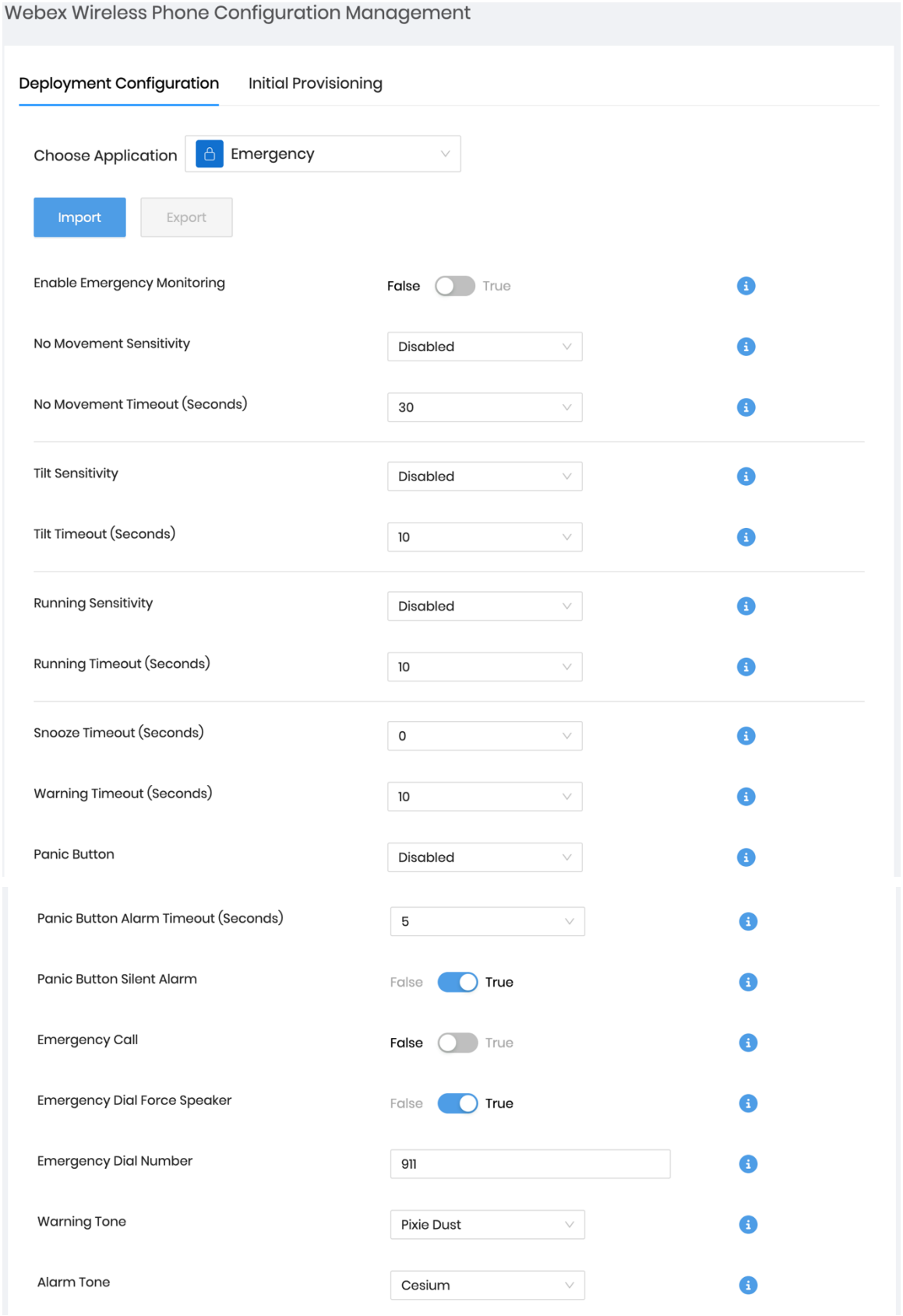


The **Lock Screen Wallpaper** and **Home Screen Wallpaper** can be managed within the **Wallpaper** menu.



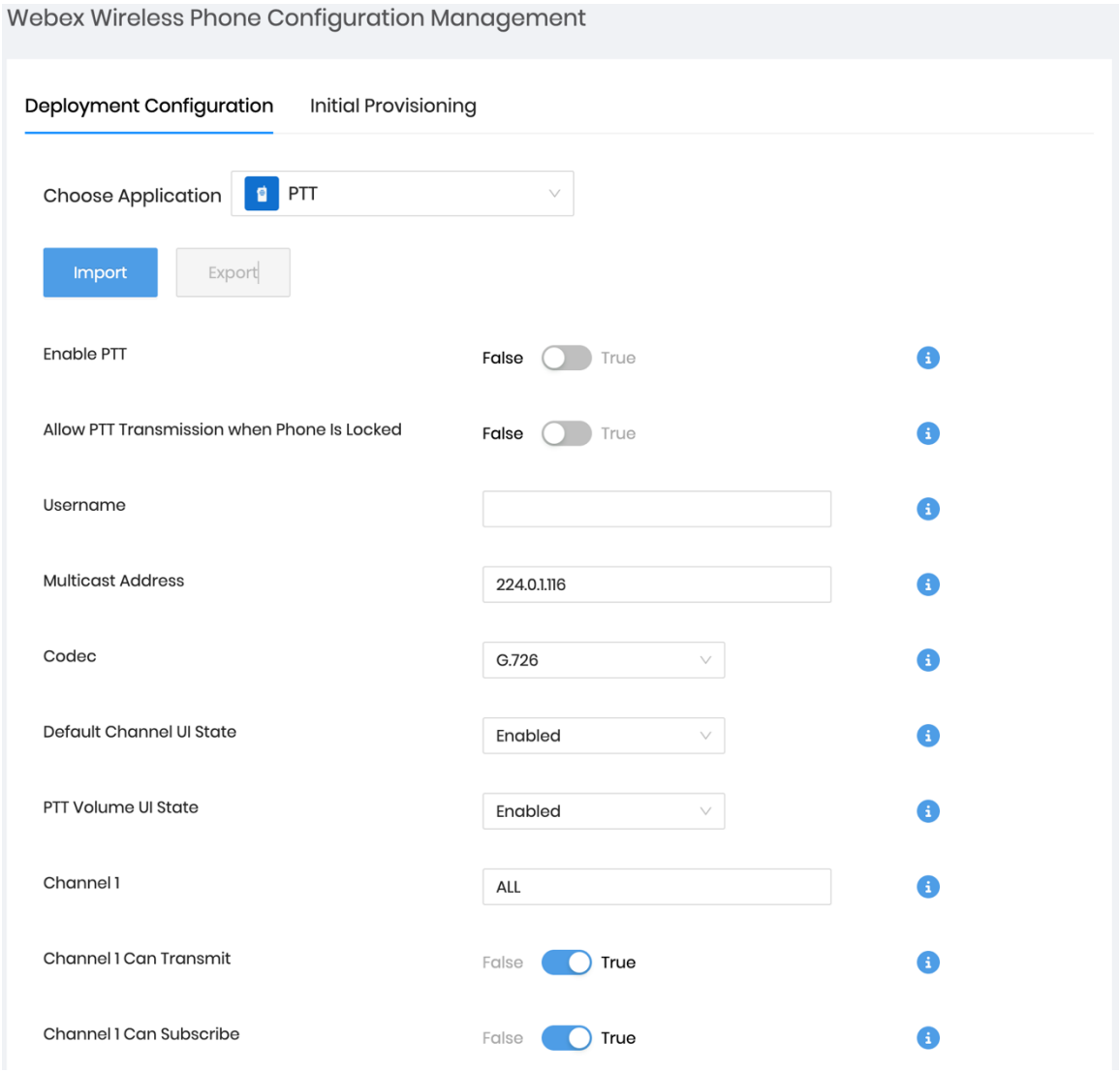
Emergency

To configure the Emergency settings select **Emergency** from the drop-down list.



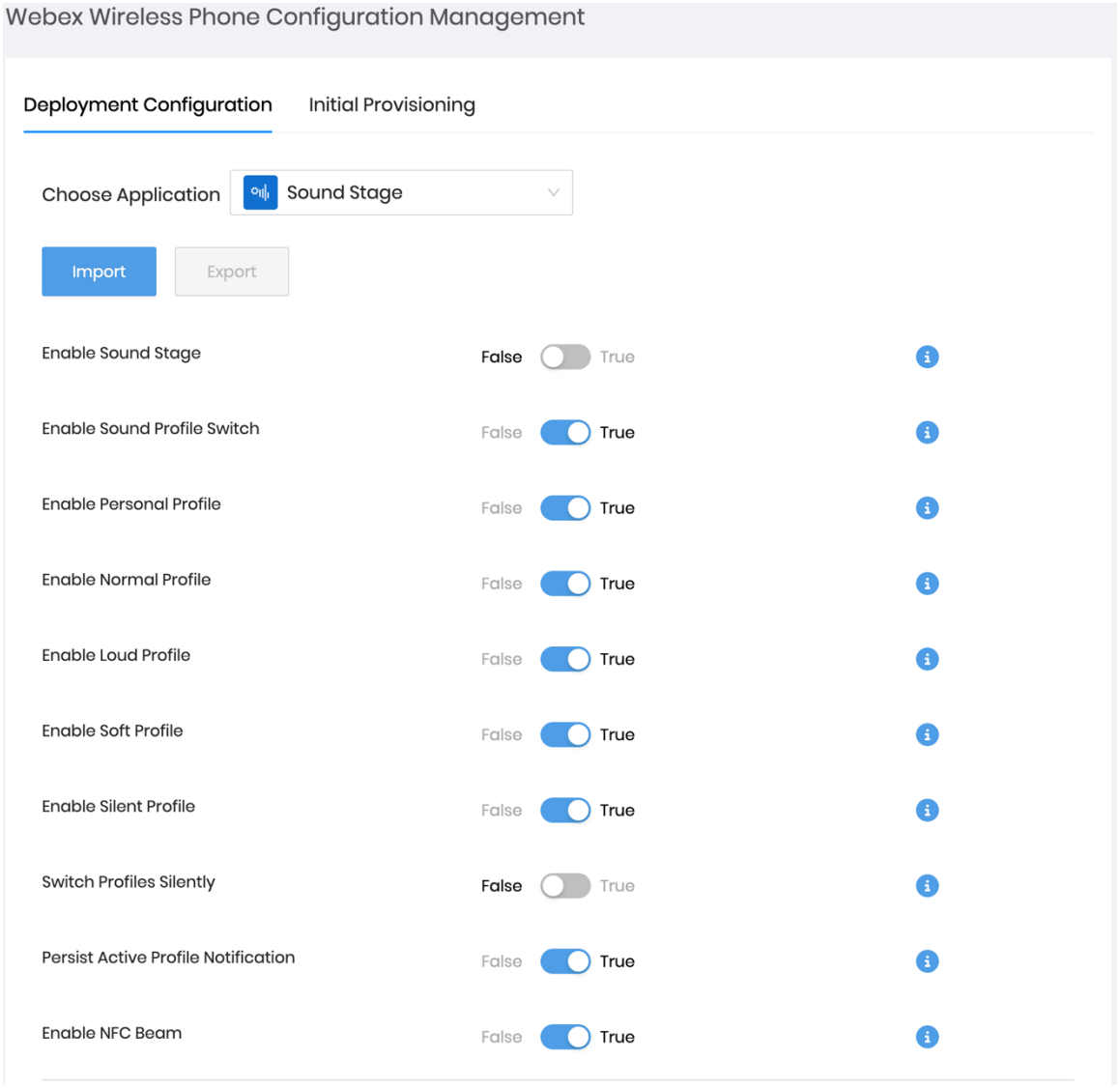
PTT

To configure the PTT settings select **PTT** from the drop-down list.



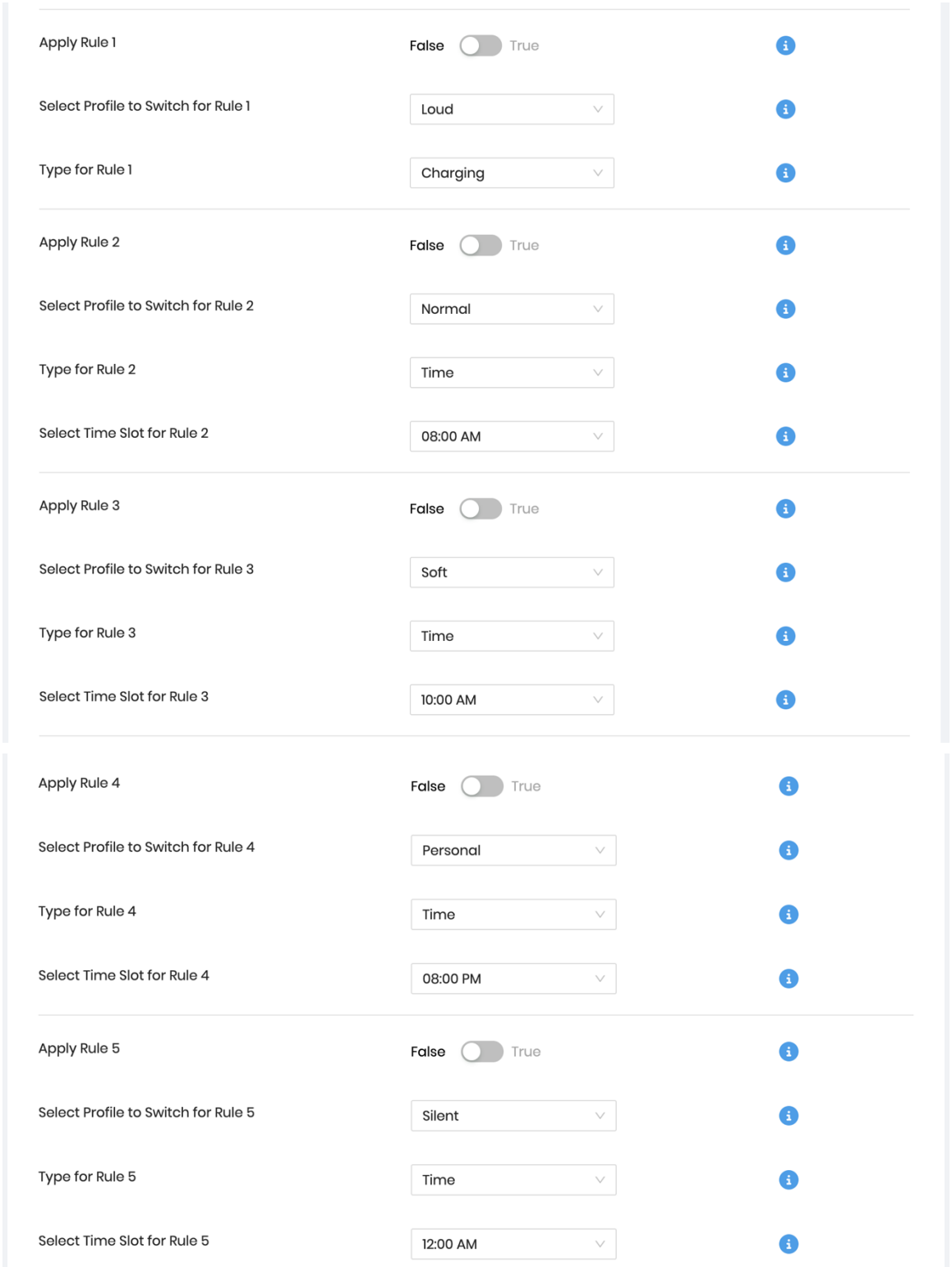
Sound Stage

To configure the Sound Stage settings select **Sound Stage** from the drop-down list.



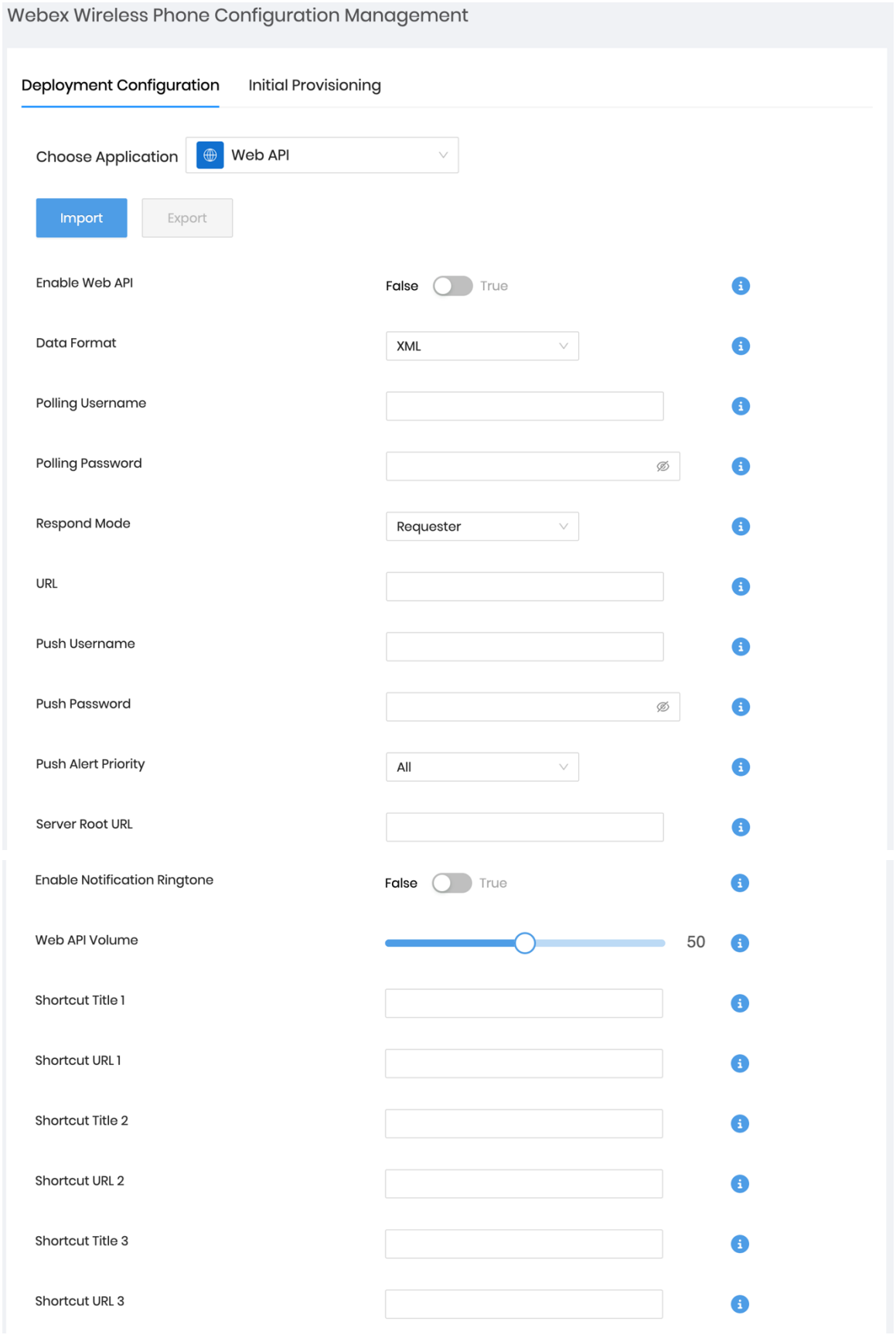
Pre-configured profiles (**Normal**, **Loud**, **Soft**, **Silent**) and a custom personal profile can be configured and adjusted as necessary.

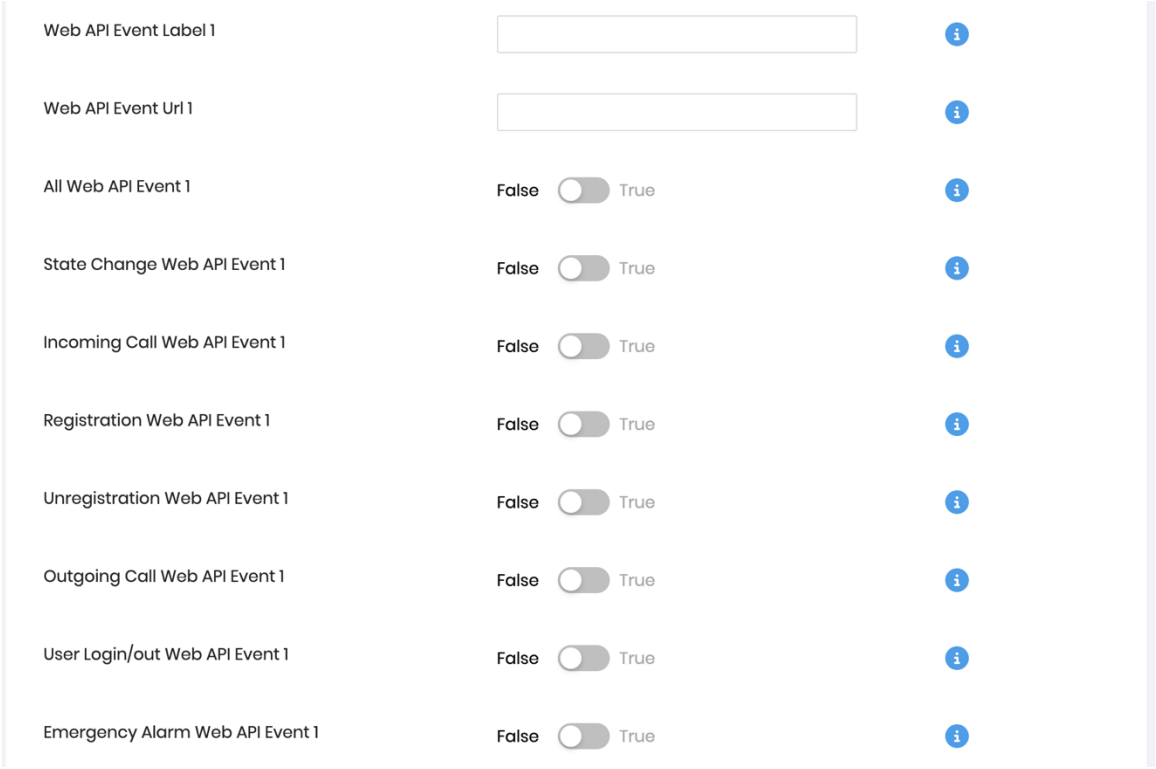
Rules can then be configured to switch to a profile when a specific condition is met.



Web API

To configure the Web API settings select **Web API** from the drop-down list.


Webex Wireless Phone Configuration Management
Deployment Configuration
Initial Provisioning
Choose Application
Web API
Import
Export
Enable Web API
False
True
Data Format
XML
Polling Username
Polling Password
Respond Mode
Requester
URL
Push Username
Push Password
Push Alert Priority
All
Server Root URL
Enable Notification Ringtone
False
True
Web API Volume
50
Shortcut Title 1
Shortcut URL 1
Shortcut Title 2
Shortcut URL 2
Shortcut Title 3
Shortcut URL 3



Configure the Device Policy Controller Application

The Device Policy Controller is a new application that allows an administrator to disable applications in entirety as well as to define the Wi-Fi profile parameters and optional Phone Unlock Pin/Password when the Cisco Wireless Phone 840 and 860 is managed by the Cisco Wireless Phone Configuration Management Utility.

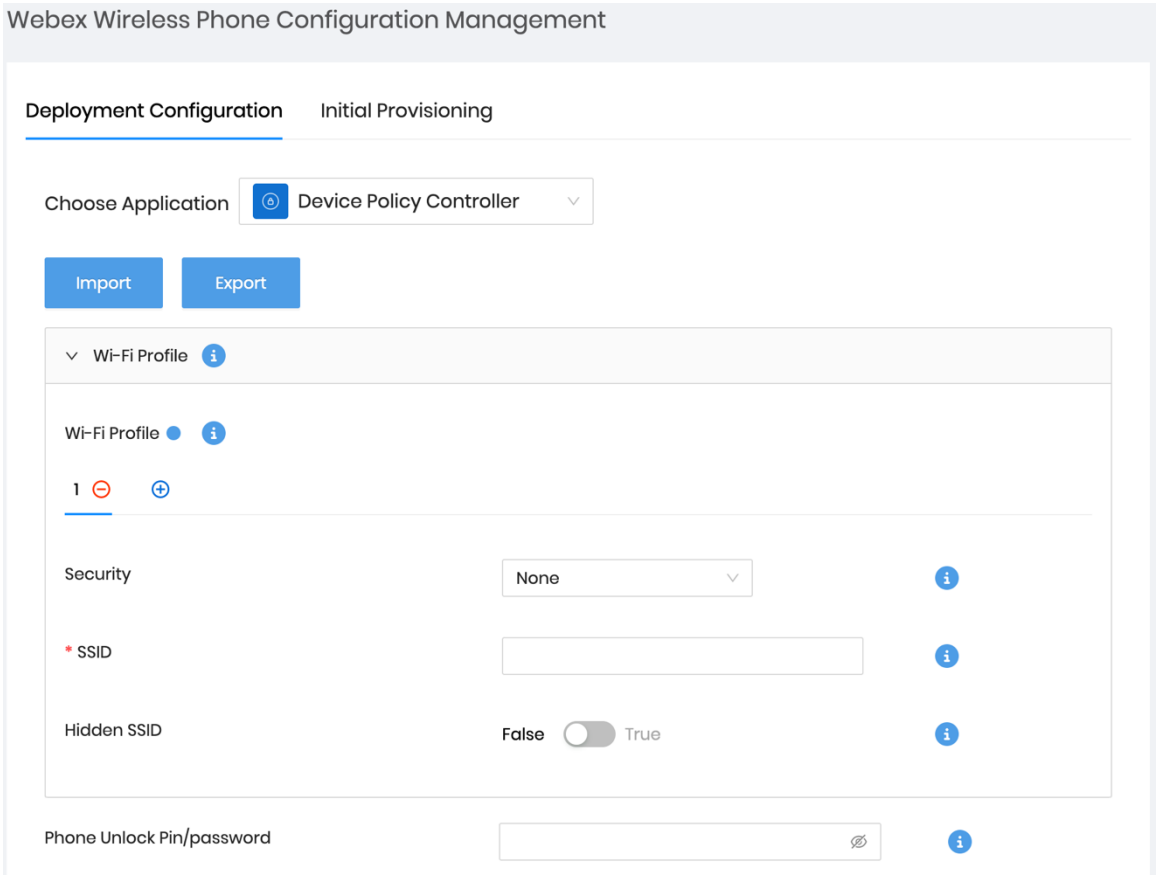
Up to 5 Wi-Fi profiles can be configured.

The following security configurations are supported.

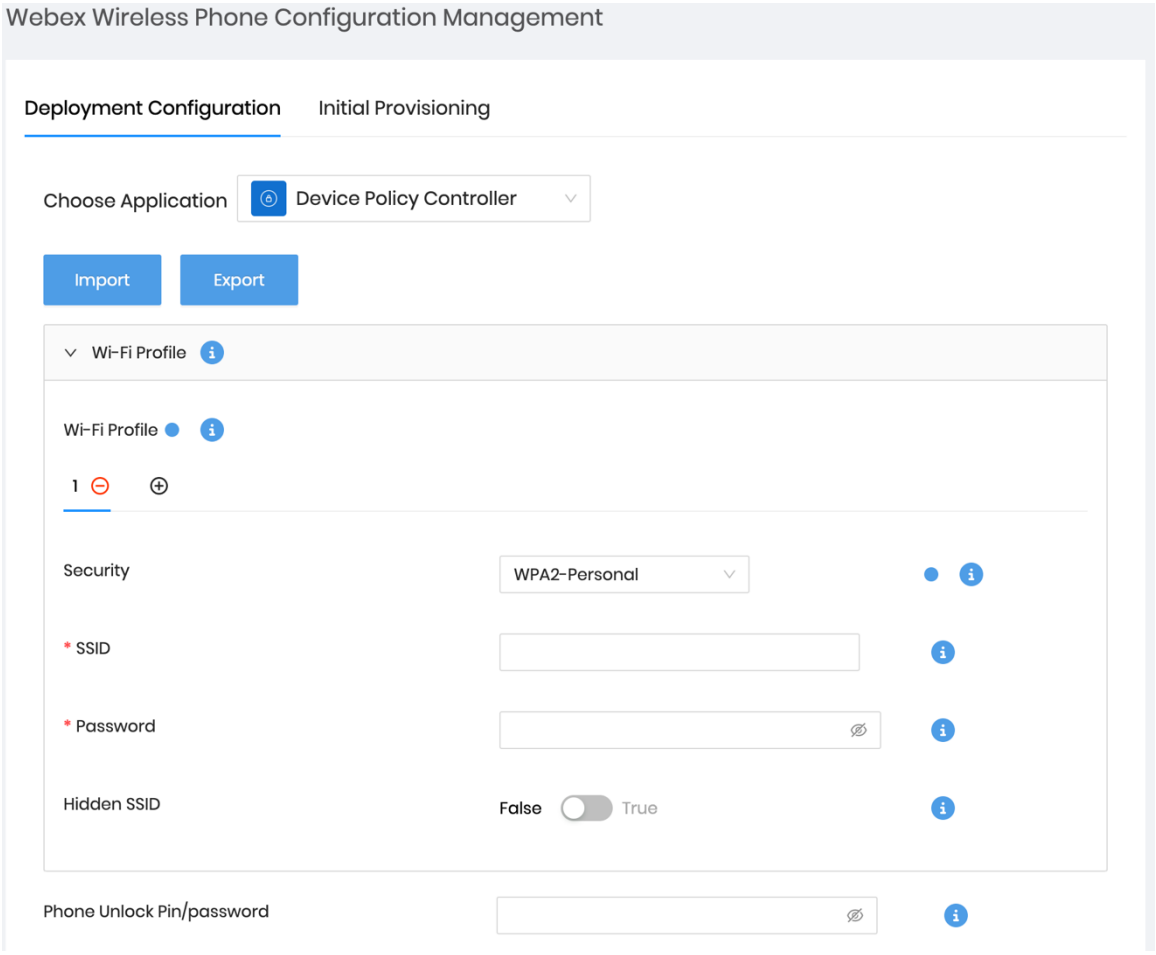
Security Mode	EAP Method	Phase 2 Authentication
None	N/A	None
WPA2-Personal	N/A	None
WPA2-Enterprise	PEAP	GTC, MSCHAPV2
WPA2-Enterprise	TTLS	GTC, MSCHAP, MSCHAPV2, PAP

Note: The Cisco Wireless Phone Configuration Management Utility does not support EAP-TLS (TLS).

To connect to an open Wi-Fi network, enter the **SSID**, then set **Security** to **None**.

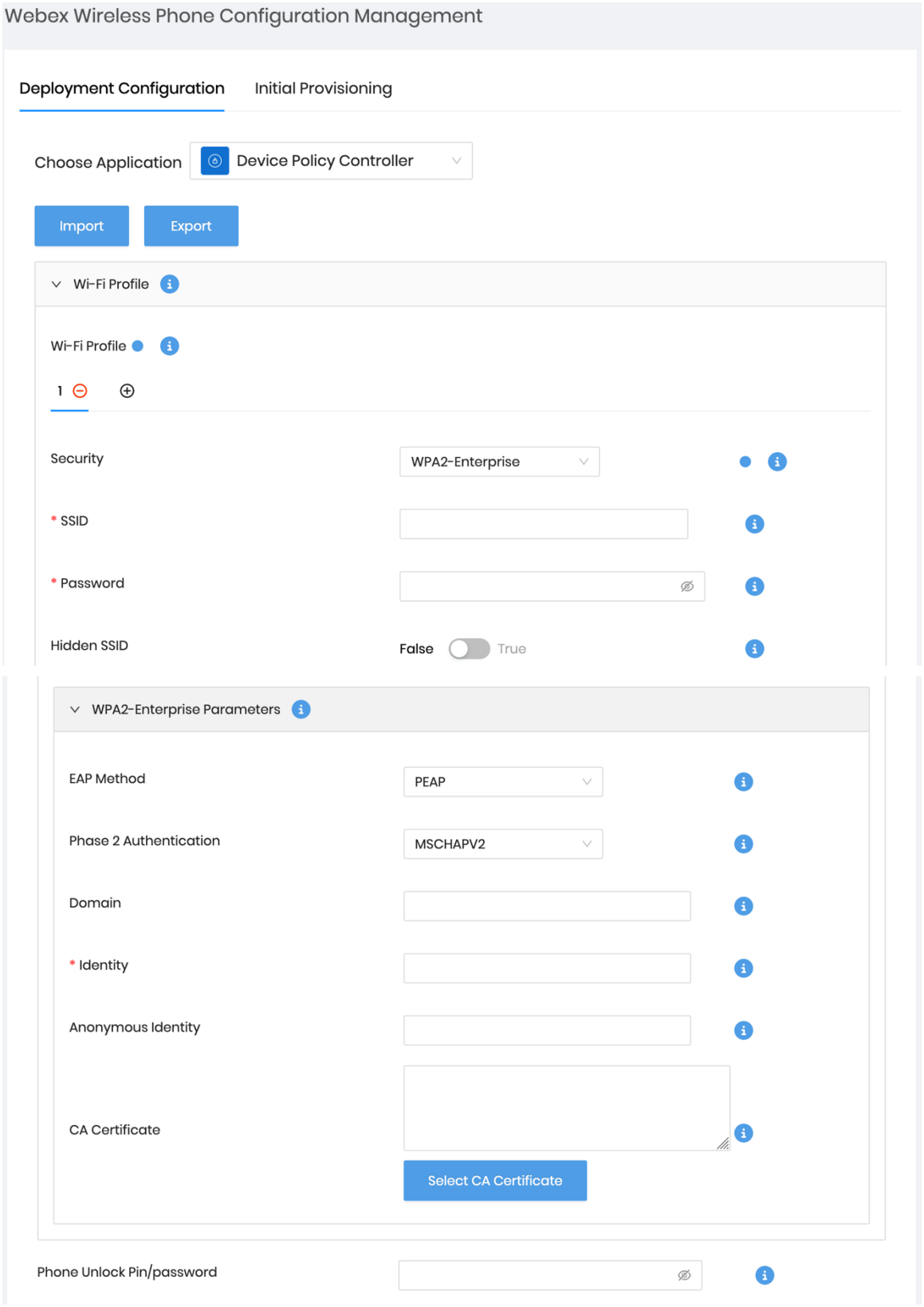


To connect to a PSK enabled Wi-Fi network, enter the **SSID**, set **Security** to **WPA2-Personal**, then enter the 8-63 ASCII or 64 HEX **Password**.



To connect to an EAP enabled Wi-Fi network, enter the **SSID**, set **Security** to **WPA2-Enterprise**, then select the **EAP method**.

If configuring a PEAP or EAP-TTLS (TTLS) Wi-Fi network, select the **Phase 2 authentication** method and configure **CA certificate** as necessary in Base-64 (PEM) encoding format minus the header and footer, then enter the **Identity** and **Password**.



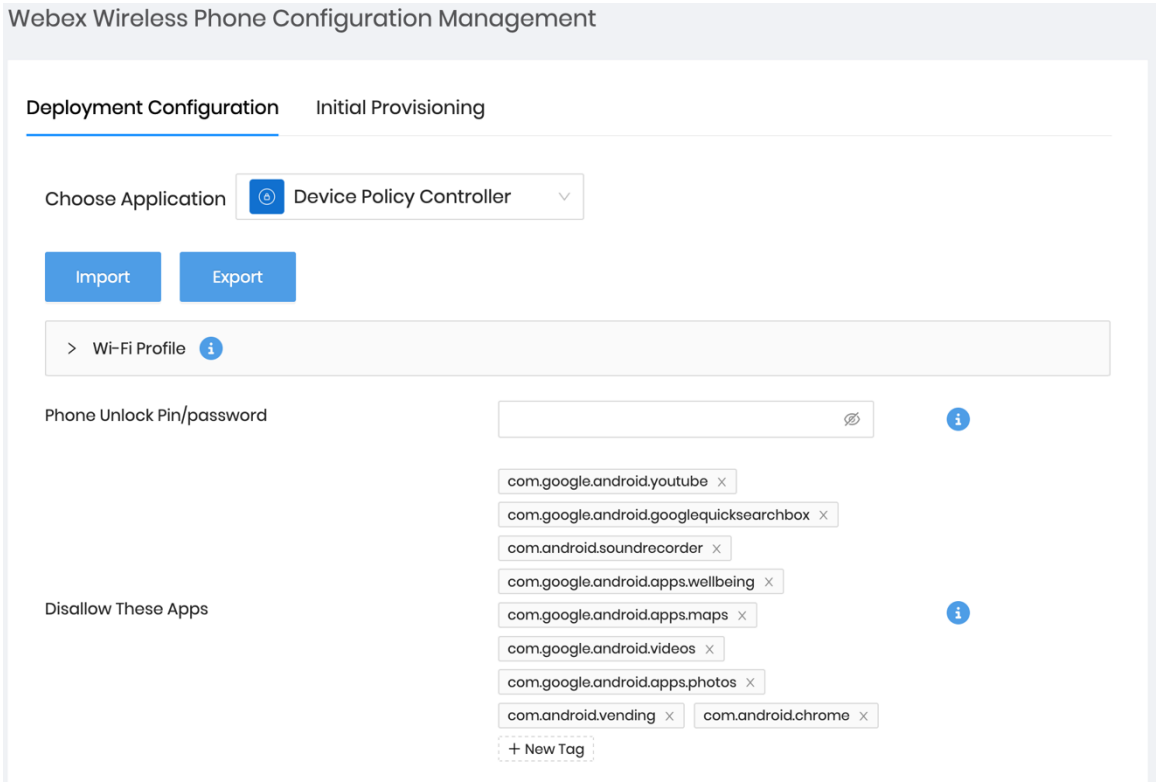
Note: A non-broadcasted Wi-Fi network must be configured as a **Hidden SSID**; otherwise the Wi-Fi network will show as not in range. Set **Hidden SSID** to **True** to connect to a non-broadcasted Wi-Fi network.

Ensure the configured Wi-Fi network points to the Cisco Unified Communications Manager; otherwise you will need to manually configure the TFTP server in the Cisco Wireless Phone 840 and 860's phone application.

Ensure the CA certificate format is correct, where the header and footer are removed and there are no spaces or carriage returns included.

The following applications are disallowed by default; however the list of disabled applications can be configured further as necessary.

- **Chrome** = com.android.chrome
- **Digital Wellbeing** = com.google.android.apps.wellbeing
- **Google** = com.google.android.googlequicksearchbox
- **Google TV** = com.google.android.videos
- **Maps** = com.google.android.apps.maps
- **Photos** = com.google.android.apps.photos
- **Play Store** = com.android.vending
- **Sound Recorder** = com.android.soundrecorder
- **YouTube** = com.google.android.youtube



Note: Ensure critical applications are not disallowed in the Device Policy Controller configuration.

- **Smart Launcher** = com.cisco.smartlauncher
- **Device Policy Controller** = com.cisco.devicepolicycontroller
- **Cisco Phone** = com.cisco.phone
- **Application URLs** = com.cisco.appurl

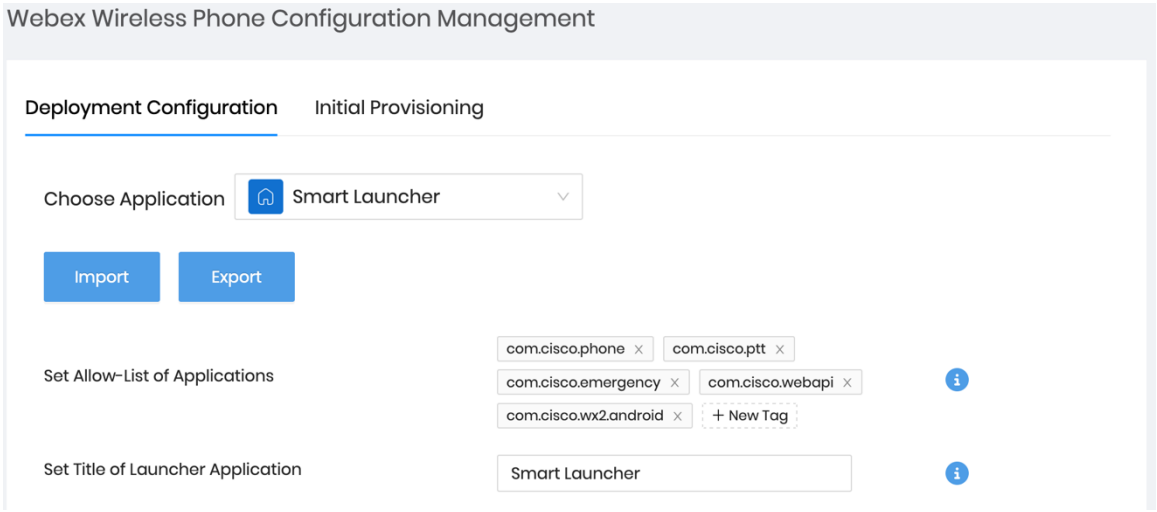
- **Logging** = com.cisco.logging
- **Port Manager** = com.cisco.portmanager
- **System Updater** = com.cisco.sysupdater
- **UCM Client** = com.cisco.ucmclient
- **Web API** = com.cisco.webapi
- **Settings** = com.android.settings

Configure the Smart Launcher Application

The Smart Launcher is a new application that limits which applications are accessible to the end user when the Cisco Wireless Phone 840 and 860 is managed by the Cisco Wireless Phone Configuration Management Utility.

The following applications are enabled by default to be displayed in the Smart Launcher view; however the list of allowed applications can be configured further as necessary.

- **Cisco Phone** = com.cisco.phone
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- **Web API** = com.cisco.webapi
- **Webex** = com.cisco.wx2.android



Below is the list of applications that are pre-installed in the Cisco Wireless Phone 840 and 860, which can either be added to the Device Policy Controller configuration to disallow those applications (minus the **Settings** application) or added to the Smart Launcher configuration to allow those applications and be accessible via the Smart Launcher view.

Cisco Pre-installed Applications

- **Barcode** = com.cisco.barcode.service
- **Battery Life** = com.cisco.batterylife
- **Buttons** = com.cisco.buttons
- **Call Quality Settings** = com.cisco.callquality

- **Custom Settings** = com.cisco.customsettings
- **Diagnostics** = com.cisco.diagnostics
- **Emergency** = com.cisco.emergency
- **PTT** = com.cisco.ptt
- **Sound Stage** = com.cisco.soundstage
- **Web API** = com.cisco.webapi
- **Webex** = com.cisco.wx2.android

Other Pre-installed Applications

- **Calculator** = com.google.android.calculator
- **Calendar** = com.google.android.calendar
- **Camera** = com.android.camera2
- **Chrome** = com.android.chrome
- **Clock** = com.android.deskclock
- **Contacts** = com.google.android.contacts
- **Digital Wellbeing** = com.google.android.apps.wellbeing
- **Drive** = com.google.android.apps.docs
- **Duo** = com.google.android.apps.tachyon
- **Files** = com.google.android.documentsui
- **Gmail** = com.google.android.gm
- **Google** = com.google.android.googlequicksearchbox
- **Google TV** = com.google.android.videos
- **Keep Notes** = com.google.android.keep
- **Maps** = com.google.android.apps.maps
- **Photos** = com.google.android.apps.photos
- **Play Store** = com.android.vending
- **Settings** = com.android.settings
- **Sound Recorder** = com.android.soundrecorder
- **YouTube** = com.google.android.youtube
- **YT Music** = com.google.android.apps.youtube.music

Note: The Smart Launcher can be configured for the phone only mode, by allowing the Cisco Phone application only. Ensure the **Settings** application and other critical applications are not disallowed in the Device Policy Controller configuration.

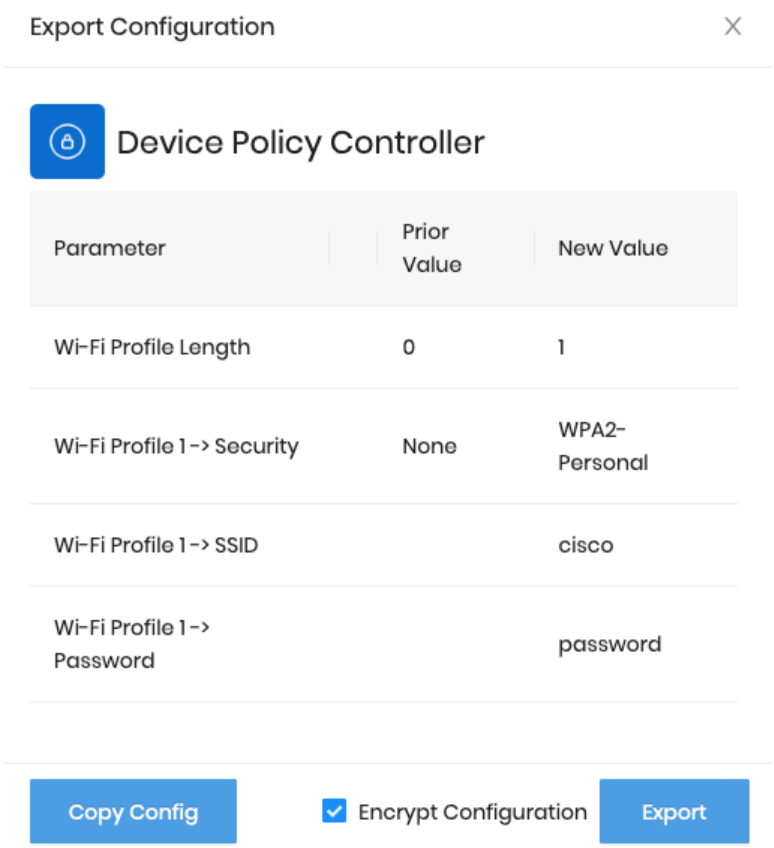
Export Configuration Files

When all necessary application configuration changes are complete and ready to save the configuration, select **Export**.

A confirmation screen will then be displayed to confirm the changes that were made.

To protect the file, ensure **Encrypt Configuration** is checked (default settings) before selecting **Export**.

Once the changes have been verified, select **Export**.



The configuration file will be exported in a ZIP format (e.g. CP8x0_config_6-8-2023.zip), which contains the following files:

- **CP8x0_config_<MM-DD-YYYY>.json.enc**= Encrypted config file to be uploaded to Cisco Unified Communications Manager
- **CP8x0_key_<MM-DD-YYYY.txt**= Encryption key used to encrypt the config file

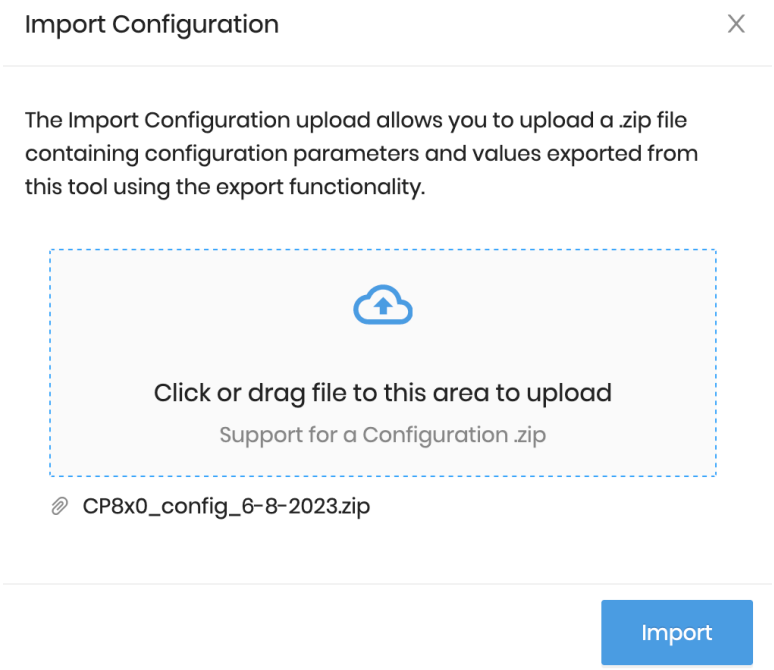
The **CP8x0_config_<MM-DD-YYYY>.json.enc** file can be renamed as necessary in case multiple files will be uploaded to the Cisco Unified Communications Manager.

Note: The non-encrypted configuration option is for troubleshooting purposes only.

Import Configuration Files

If wanting to utilize a previously exported ZIP file to made additional configurations changes, select **Import**.

Drag the saved ZIP file to the **Import Configuration** window, then select **Import**.



Note: Ensure the previously saved ZIP file has not been altered.

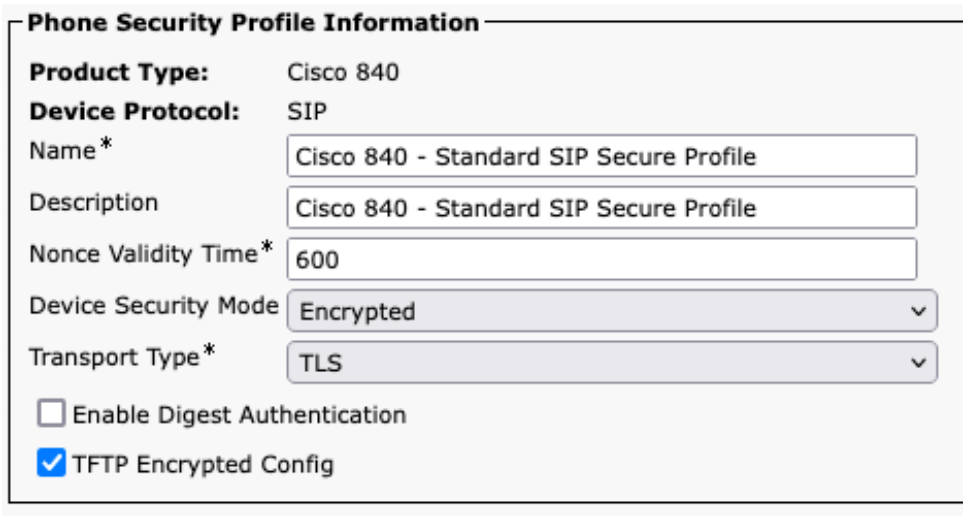
The ZIP file can be renamed, but the inner files can not be altered as that will cause an import to fail.

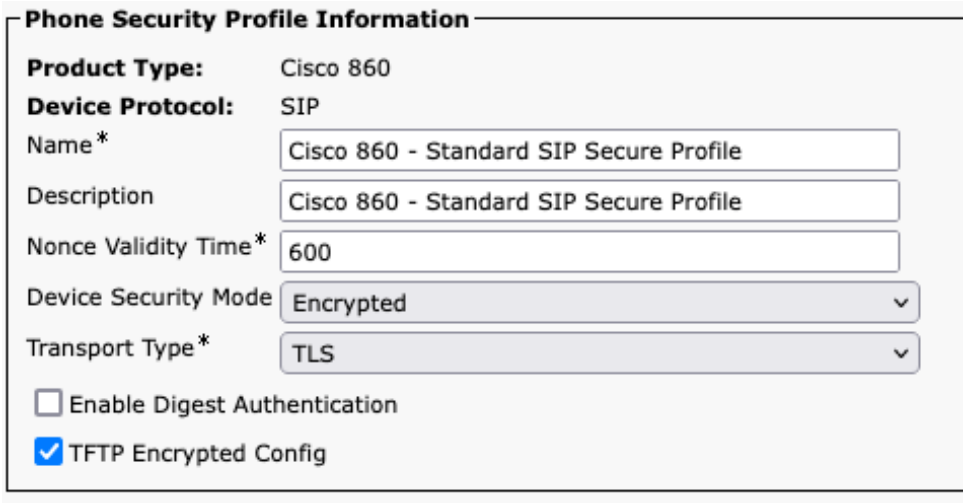
Configuring Cisco Unified Communications Manager

Use the following guidelines to configure the Cisco Unified Communications Manager to utilize the Cisco Wireless Phone Configuration Management utility.

Create a Secure Profile with TFTP Encryption

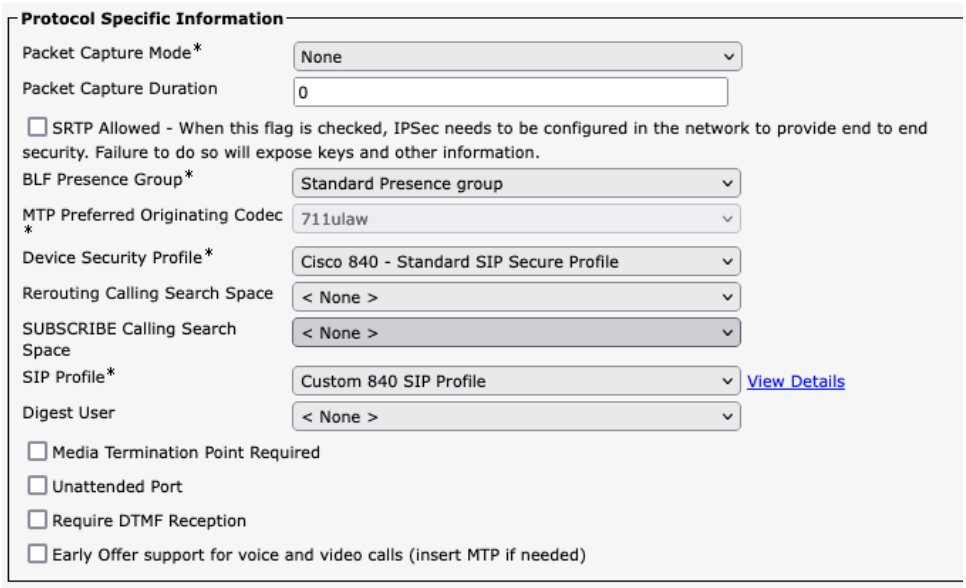
Prior to configuring the Cisco Unified Communications Manager to host an exported file from the Cisco Wireless Phone Configuration Management utility, the Cisco Wireless Phone 840 and 860 should be configured to utilize a security profile in which TFTP encryption is enabled so data is not passed down to the Cisco Wireless Phone 840 and 860 in clear text.

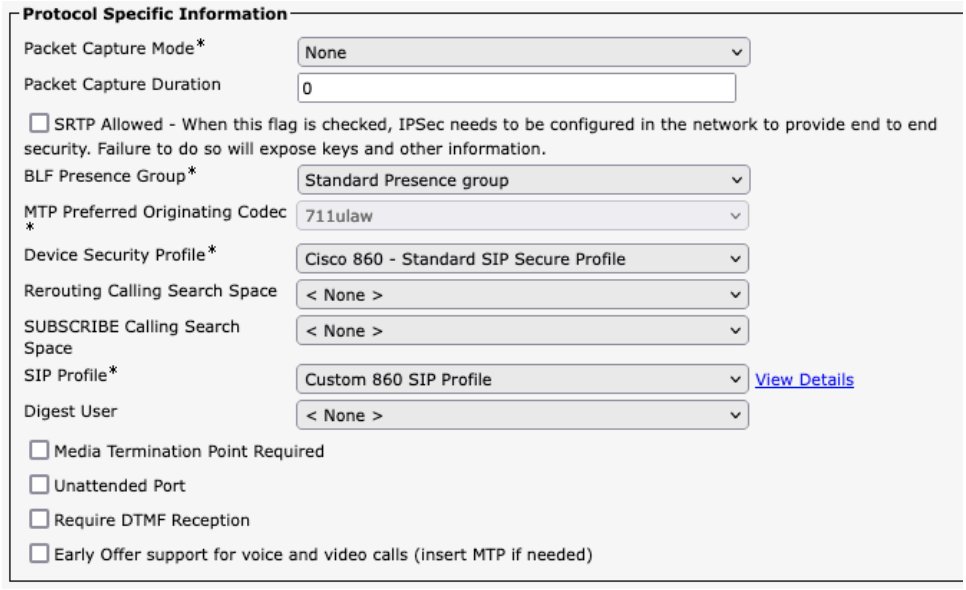




Once the security profile has been created, it then needs to be applied to the Cisco Wireless Phone 840 and 860 to enable TFTP encryption for the Cisco Wireless Phone 840 and 860 configuration files.

Select the configured security profile from the **Device Security Profile** drop-down menu.





Upload Configuration Files

Extract the **CP8x0_config_<MM-DD-YYYY>.json.enc** file from the downloaded encrypted ZIP file and upload the file to all Cisco Unified Communications Manager nodes running the TFTP service via Cisco Unified OS Administration page. Then restart the TFTP service for all nodes.

Can optionally utilize the **Load Server** option in Cisco Unified Communications Manager to host the config files.

Note: The **CP8x0_config_<MM-DD-YYYY>.json.enc** file can be renamed as necessary in case multiple files will be uploaded to the Cisco Unified Communications Manager.

Configure the Cisco Wireless Phone 840 and 860 Product Specific Configuration Options

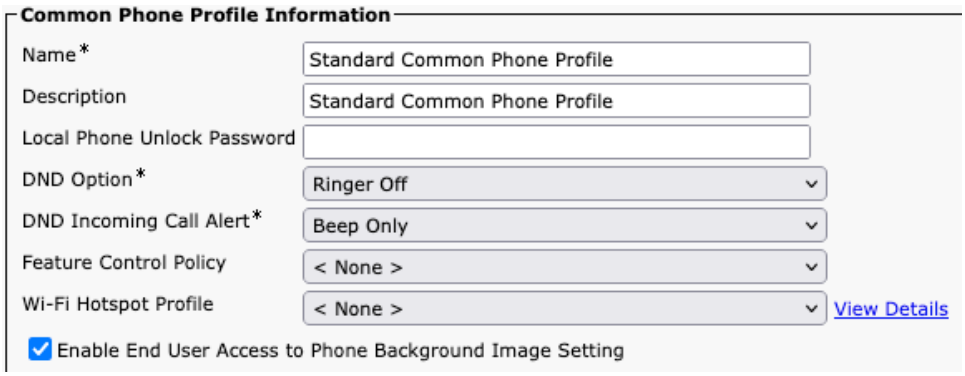
The Cisco Wireless Phone 840 and 860 must be configured to inform which file to download and encryption key to use to decrypt the file.

Configure the **Enterprise Mobility Management (EMM) Alternative Configuration** product specific configuration option with the name of the extracted file (e.g. **CP8x0_config_<MM-DD-YYYY>.json.enc** or the name the name of the file was renamed to).

Configure the **Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key** product specific configuration option with the key of the extracted **CP8x0_key_<MM-DD-YYYY.txt** file.

Configure a Local phone Unlock Password

The **Local Phone Unlock Password** (default = **#) can be used to exit the Smart Launcher and gain access to the standard Android interface, therefore it is recommended to configure a **Local Phone Unlock Password** via a **Common Phone Profile** at **Device > Device Settings > Common Phone Profile** and apply it to the Cisco Wireless Phone 840 and 860.



Enrolling the Cisco Wireless Phone 840 and 860

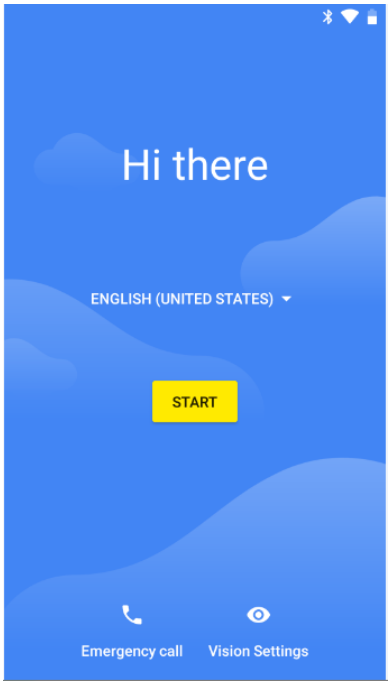
To utilize the Cisco Wireless Phone Configuration Management utility, the Cisco Wireless Phone 840 and 860 must be upgraded to firmware 1.5(0) or later first.

Once the Cisco Wireless Phone 840 and 860 have been upgraded to 1.5(0) or later, then they must be factory reset by navigating to **Settings > System > Advanced > Reset options** > **Erase all data (factory reset)**.

To enable the Cisco Wireless Phone 840 and 860 to utilize the configuration file generated by the utility, the phone must be factory reset then scan the QR code generated by the utility at the startup screen. Failure to scan the code to allow the utility to manage the phone will not enable the phone to download the configuration file.

Note: Once the Cisco Wireless Phone 840 and 860 are enrolled to the Cisco Wireless Phone Configuration Management utility, then can push subsequent updates without having to factory reset the phones.

On the startup screen, quickly tap the display 6 times to be prompted to scan a QR code to enroll the Cisco Wireless Phone 840 or 860 to the Cisco Wireless Phone Configuration Management utility.



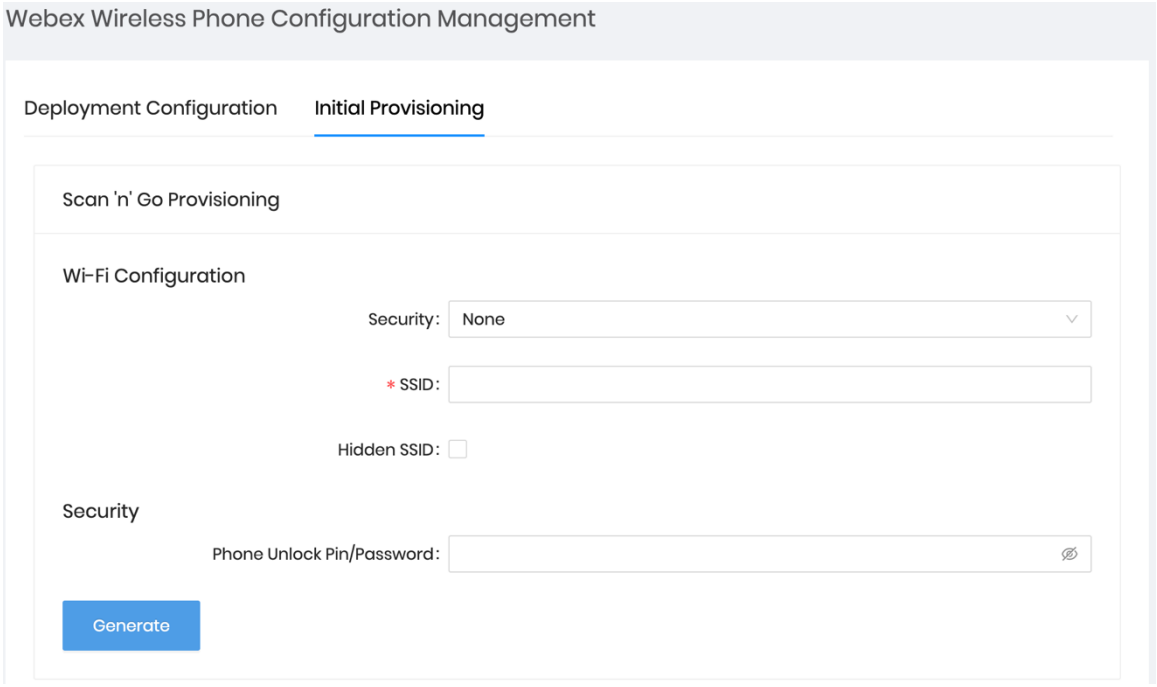
On the **Initial Provisioning** tab of the Cisco Wireless Phone Configuration Management utility, configure the Wi-Fi network parameters and optional Phone Unlock Pin/Password to utilize for initial provisioning.

The following security configurations are supported.

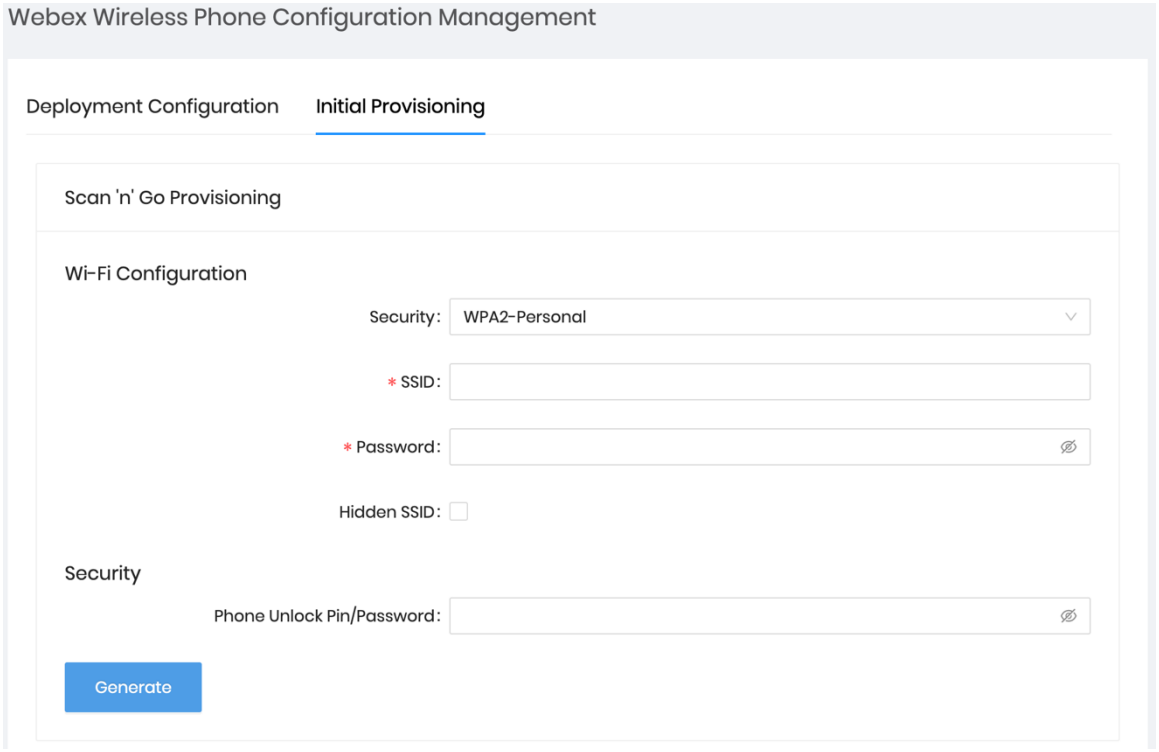
Security Mode	EAP Method	Phase 2 Authentication
None	N/A	None
WPA2-Personal	N/A	None
WPA2-Enterprise	PEAP	GTC, MSCHAPV2
WPA2-Enterprise	TTLS	GTC, MSCHAP, MSCHAPV2, PAP

Note: The Cisco Wireless Phone Configuration Management Utility does not support EAP-TLS (TLS).

To connect to an open Wi-Fi network, enter the **SSID**, then set **Security** to **None**.

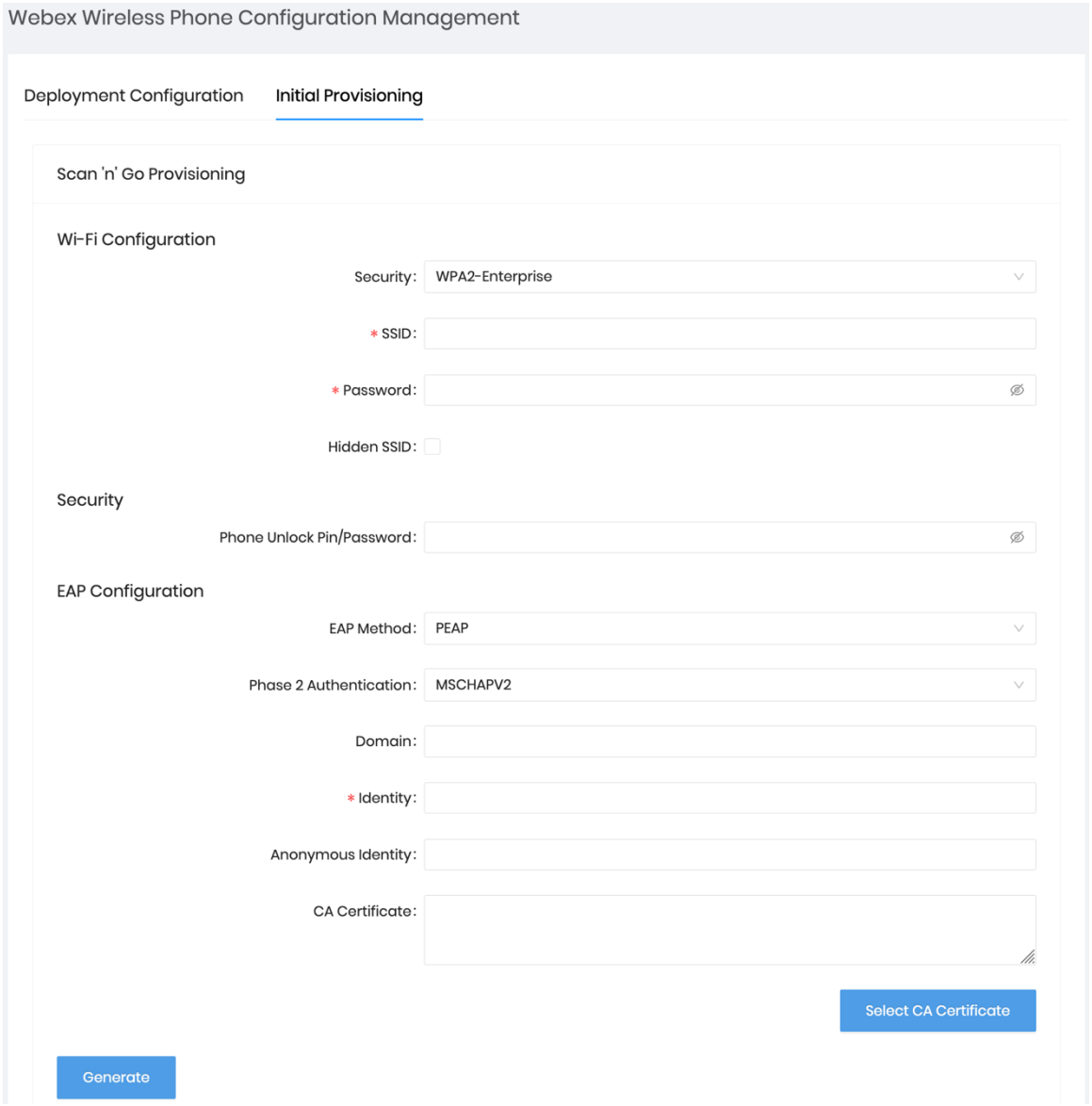


To connect to a PSK enabled Wi-Fi network, enter the **SSID**, set **Security** to **WPA2-Personal**, then enter the 8-63 ASCII or 64 HEX **Password**.



To connect to an EAP enabled Wi-Fi network, enter the **SSID**, set **Security** to **WPA2-Enterprise**, then select the **EAP method**.

If configuring a PEAP or EAP-TTLS (TTLS) Wi-Fi network, select the **Phase 2 authentication** method and configure **CA certificate** as necessary in Base-64 (PEM) encoding format minus the header and footer, then enter the **Identity** and **Password**.



Note: A non-broadcasted Wi-Fi network must be configured as a **Hidden SSID**; otherwise the Wi-Fi network will show as not in range. Set **Hidden SSID** to **True** to connect to a non-broadcasted Wi-Fi network.

Ensure the configured Wi-Fi network points to the Cisco Unified Communications Manager via DHCP option 150 or DHCP option 66; otherwise you will need to manually configure the TFTP server in the Cisco Wireless Phone 840 and 860's phone application.

Ensure the CA certificate format is correct, where the header and footer are removed and there are no spaces or carriage returns included.

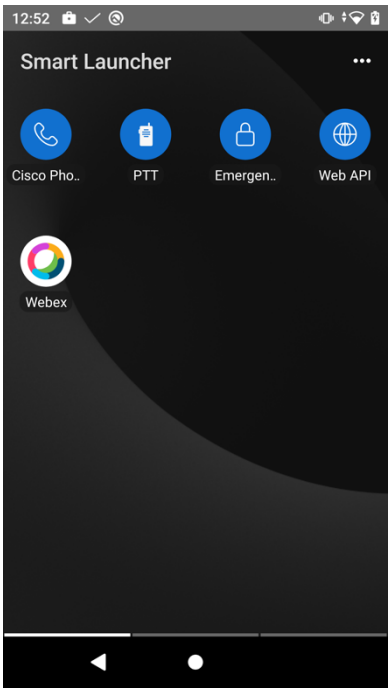
Select **Generate** to create the QR code, then the QR code will be displayed.

Note: In order for the QR code to be generated successfully, the total number of characters including CA certificate characters must not exceed 2041 characters.

Scan the QR code with the Cisco Wireless Phone 840 or 860.

The QR code can be saved in case the Cisco Wireless Phone 840 or 860 is not nearby. If so, suggest to save the QR code as a PDF file or as a screenshot as saving the file as a PNG file will alter the file and cause the QR code scan to fail.

The Cisco Wireless Phone 840 and 860 will then attempt to download the specified file from the Cisco Unified Communications Manager and update the applications and other settings accordingly.



Note: The Cisco Wireless Phone 840 and 860 must be in range of the configured Wi-Fi network, otherwise setup will fail.

Manual Configuration

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

Wi-Fi Profile Configuration

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

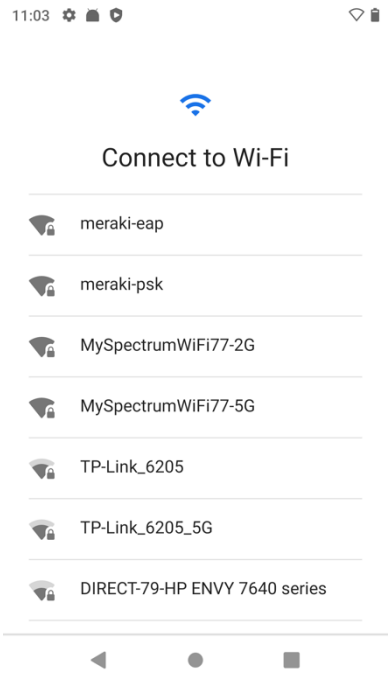
- For an out of box (factory reset) phone, configure the Wi-Fi network via the startup wizard or select **Set up offline**.
- Configuration options will be determined by whether a broadcasted Wi-Fi network is being configured or a Wi-Fi network is being manually configured.

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

Security Mode	EAP Method	Key Management	Encryption
None	N/A	None	None
WPA2-Personal	N/A	WPA2	AES
WPA2-Enterprise	PEAP	WPA2	AES
WPA2-Enterprise	TLS	WPA2	AES
WPA2-Enterprise	TTLS	WPA2	AES

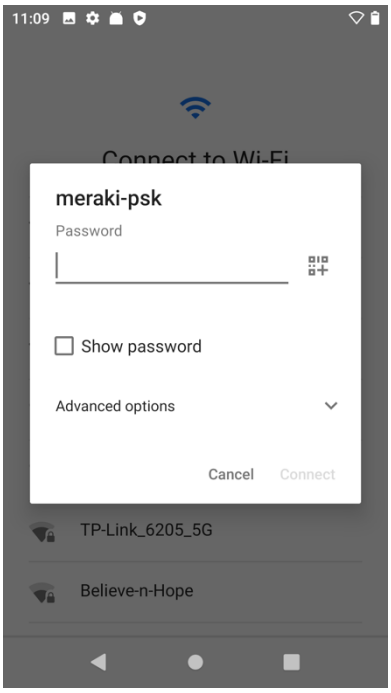
Configuring a Broadcasted Wi-Fi Network

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

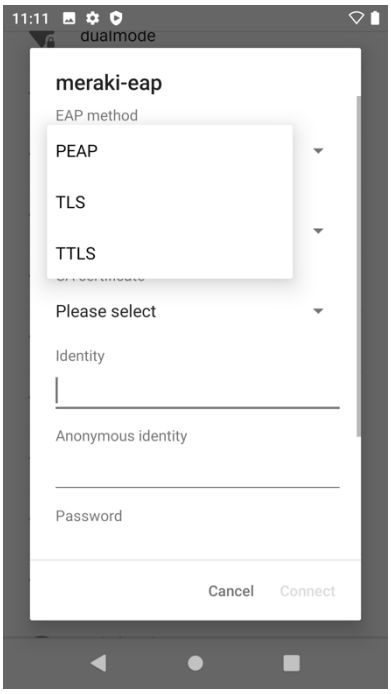


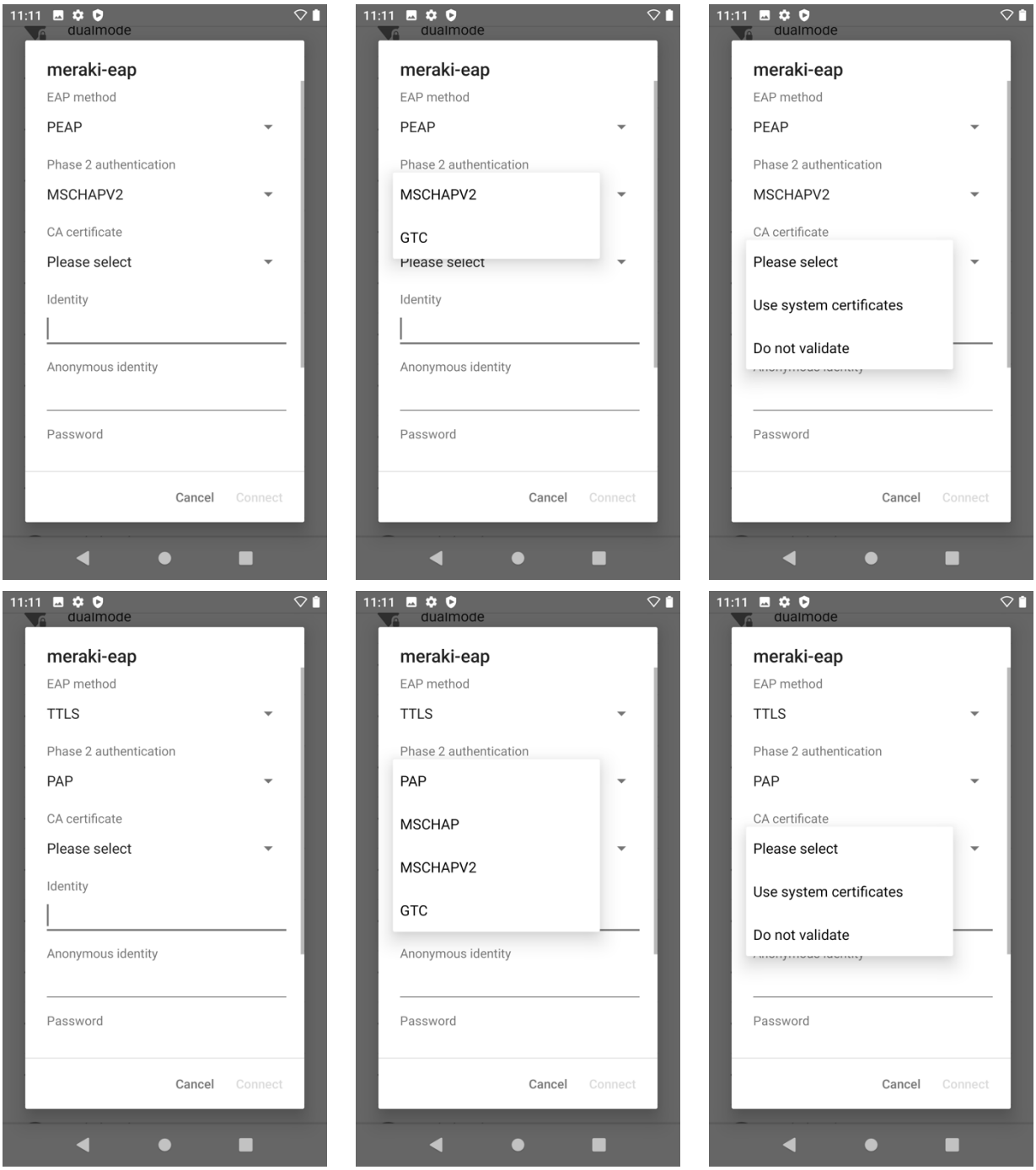
- To connect to an open Wi-Fi network, simply click on the Wi-Fi network name.

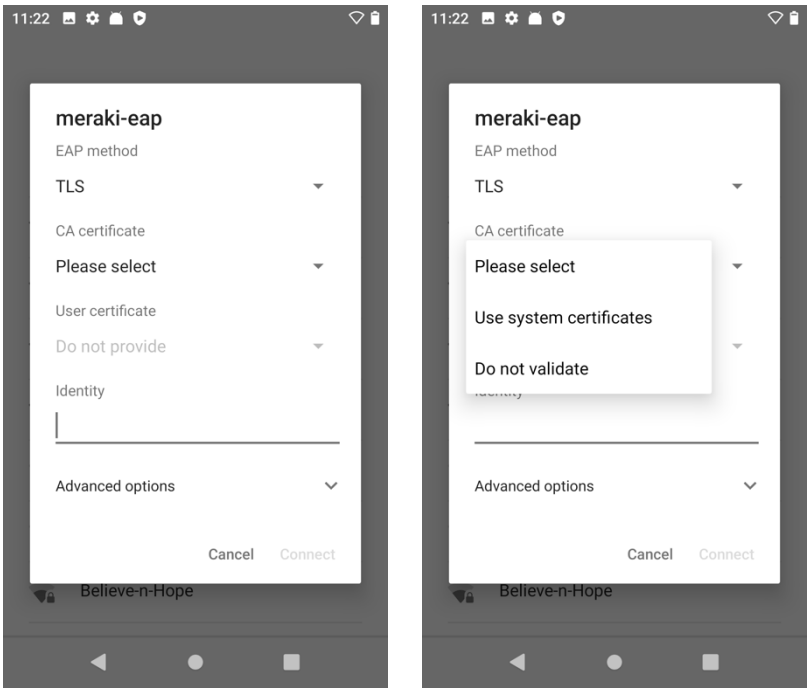
- To connect to a PSK enabled Wi-Fi network, click on the Wi-Fi network name, then enter the 8-63 ASCII or 64 HEX **Password**.



- To connect to an EAP enabled Wi-Fi network, click on the Wi-Fi network name, then select the **EAP method**.
- If configuring a PEAP or EAP-TTLS (TTLS) Wi-Fi network, select the **Phase 2 authentication** method and **CA certificate** option to utilize, then enter the **Identity** and **Password**.
- If configuring an EAP-TLS (TLS) Wi-Fi network, select the **User certificate** and **CA certificate** options to utilize.

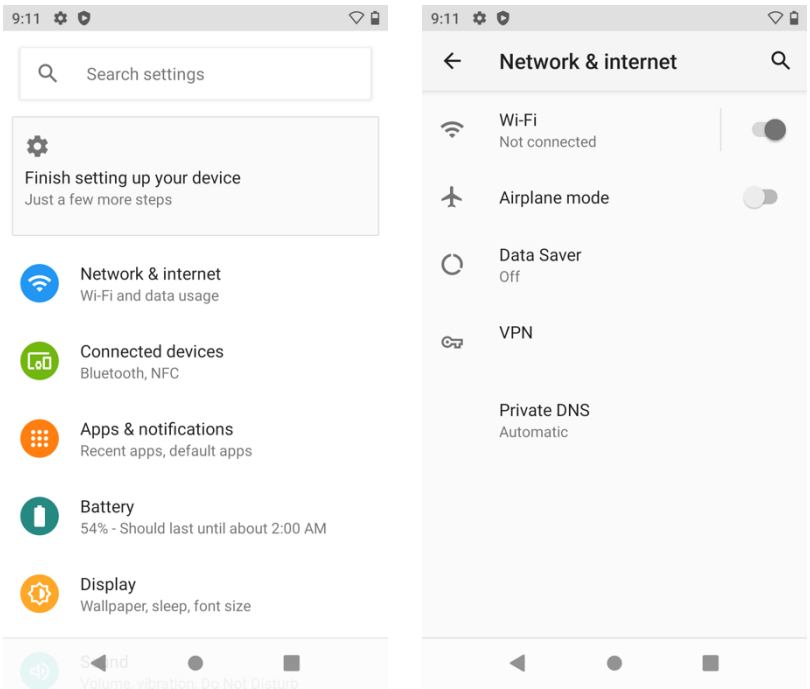



11:11
dualmode
meraki-eap
EAP method
PEAP
Phase 2 authentication
MSCHAPV2
CA certificate
Please select
Identity
Anonymous identity
Password
Cancel
Connect
GTC
Use system certificates
Do not validate
TTLS
PAP
MSCHAP

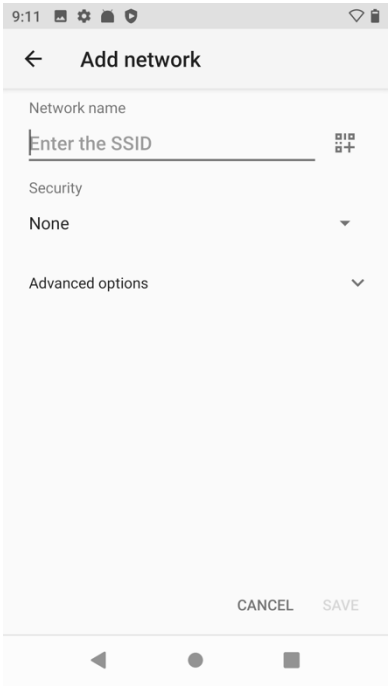


Configuring a Non-Broadcasted Wi-Fi Network

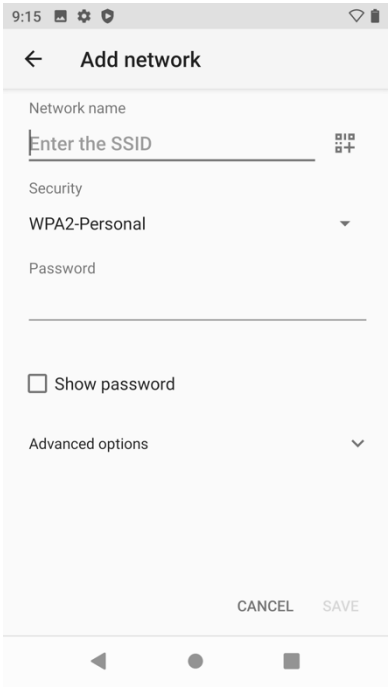
- If manually configuring a non-broadcasted (hidden) Wi-Fi network, swipe up from the bottom of the phone's display to show the installed applications, select **Settings > Network & internet > Wi-Fi**.
- At the bottom of Wi-Fi settings, select **Add Network**, then configure the network name (SSID), security type, and enter the required credentials depending on the Wi-Fi network's security settings.
- A non-broadcasted Wi-Fi network must also be marked as a **Hidden network** in the **Advanced options** section of the Wi-Fi network settings; otherwise the Wi-Fi network will show as not in range.



- To connect to an open Wi-Fi network, enter the **Network name**, then set **Security** to **None**.

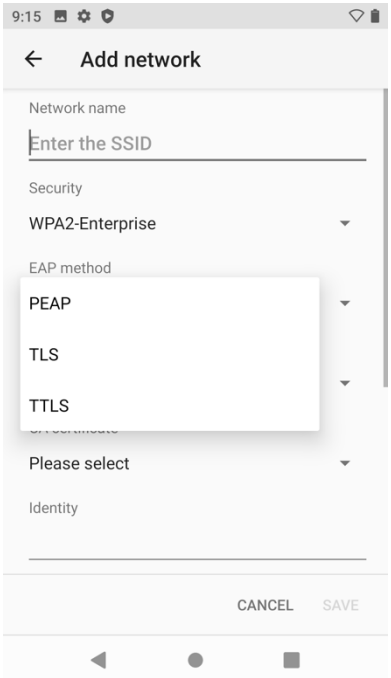


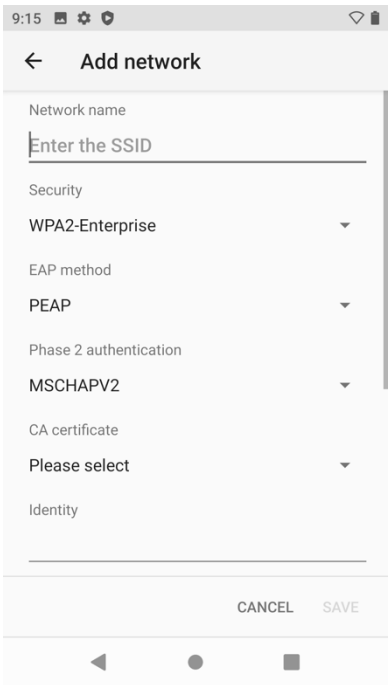
- To connect to a PSK enabled Wi-Fi network, enter the **Network name**, set **Security** to **WPA2-Personal**, then enter the 8-63 ASCII or 64 HEX **Password**.

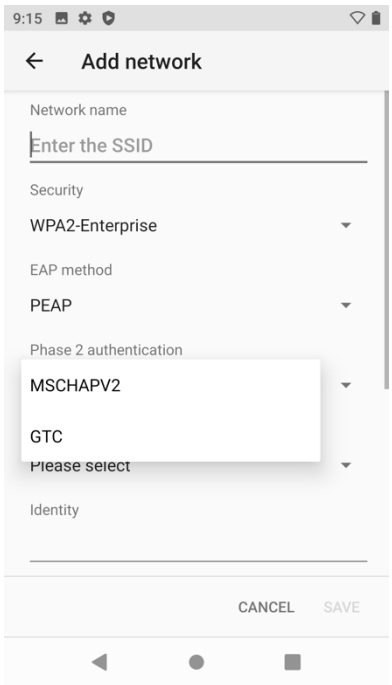


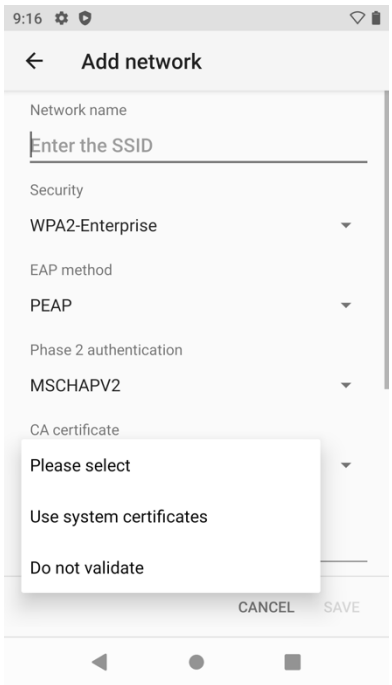
- To connect to an EAP enabled Wi-Fi network, enter the **Network name**, set **Security** to **WPA2-Enterprise**, then select the **EAP method**.

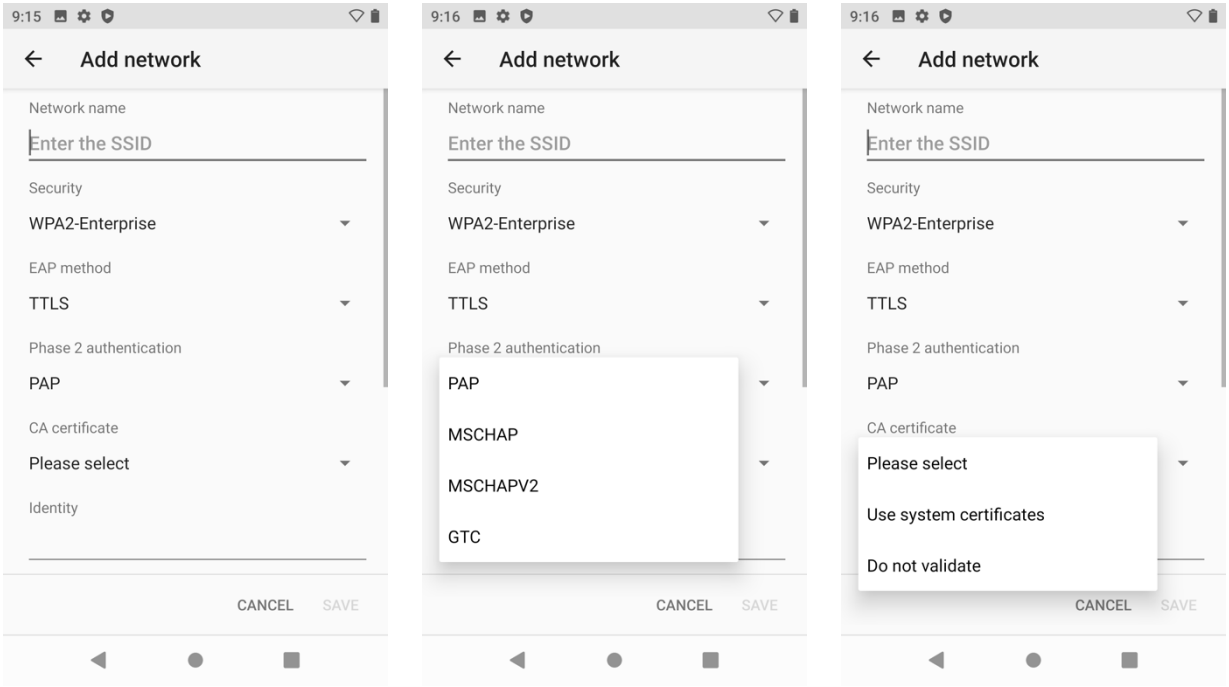
- If configuring a PEAP or EAP-TTLS (TTLS) Wi-Fi network, select the **Phase 2 authentication** method and **CA certificate** option to utilize, then enter the **Identity** and **Password**.
- If configuring an EAP-TLS (TLS) Wi-Fi network, select the **User certificate** and **CA certificate** options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

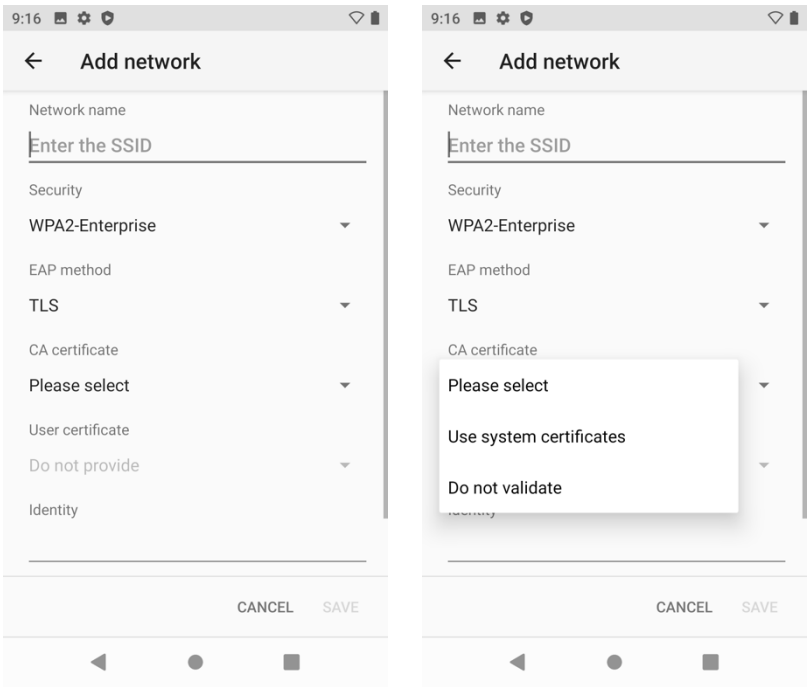






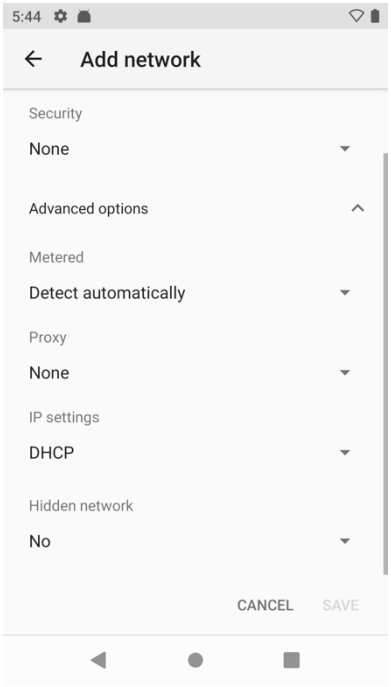


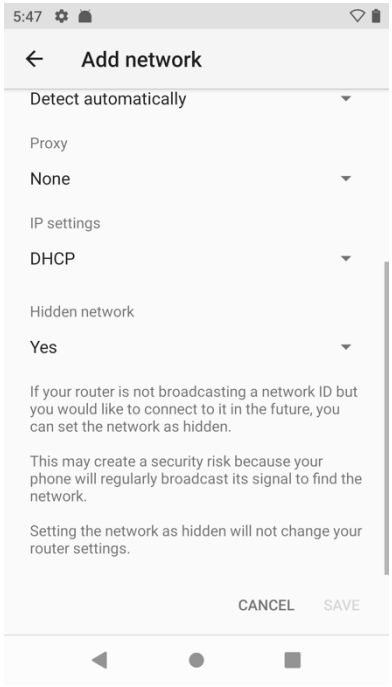




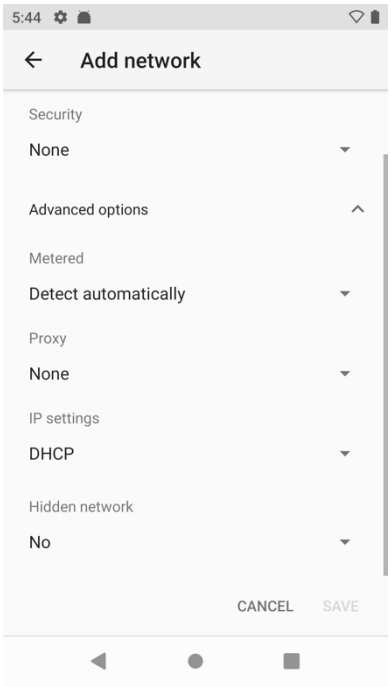
Configuring Advanced Options for the Wi-Fi Network

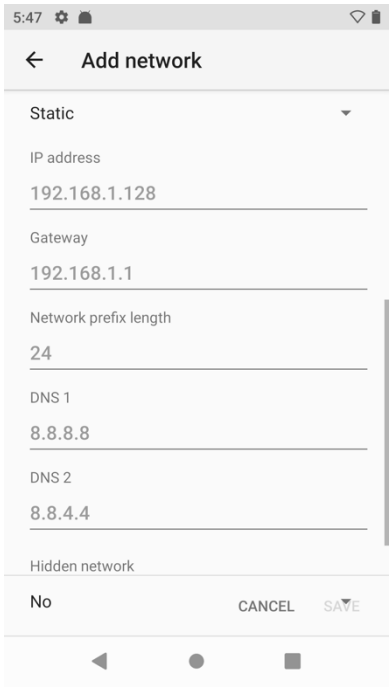
- A non-broadcasted Wi-Fi network must be configured as a **Hidden network** in the **Advanced options** section of the Wi-Fi network settings; otherwise the Wi-Fi network will show as not in range.
- Set **Hidden network** to **Yes** to connect to a non-broadcasted Wi-Fi network.



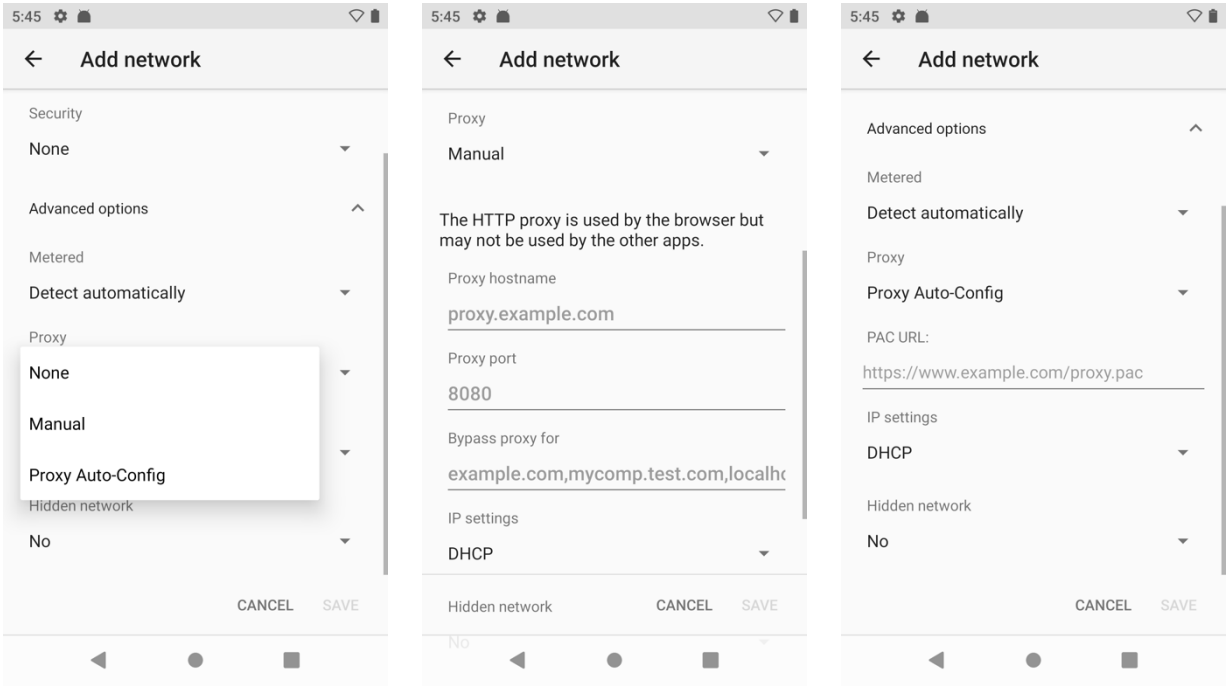


- IP settings (Static or DHCP config) can be configured in the **Advanced options** section of the Wi-Fi network settings.



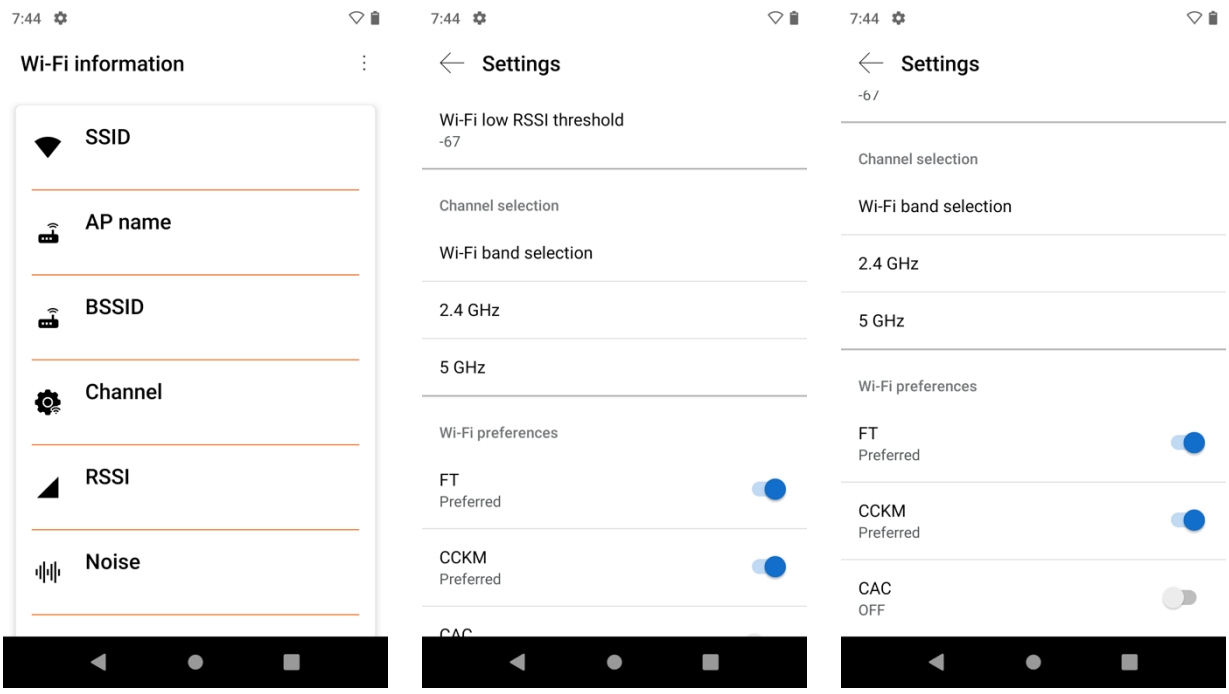


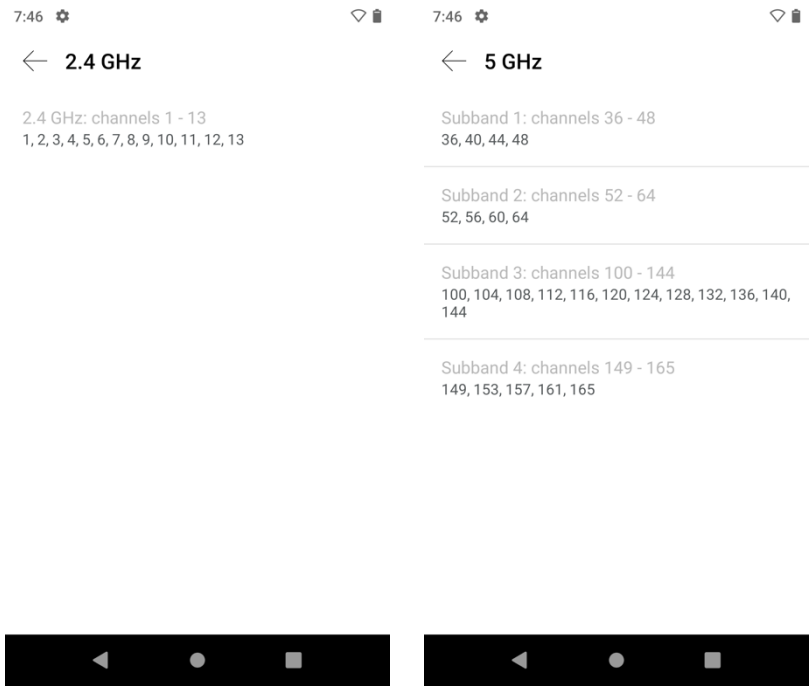
- Proxy settings can also be configured in the **Advanced options** section of the Wi-Fi network settings.



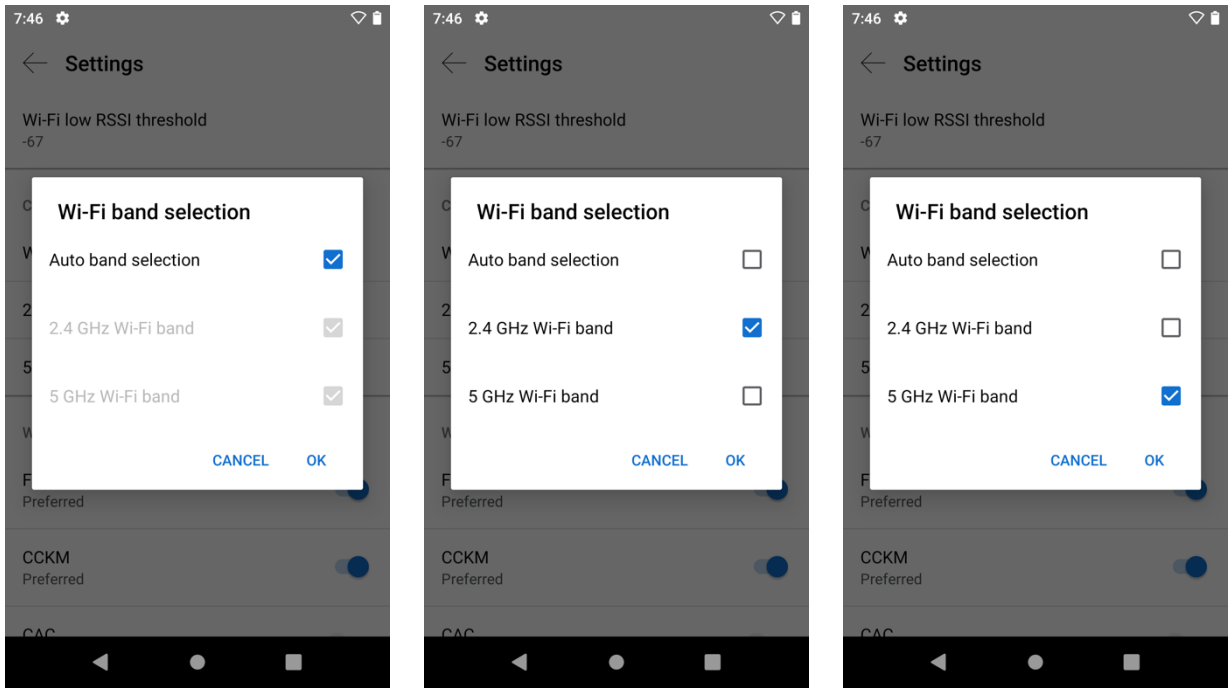
Configuring the Call Quality Settings

- The **Wi-Fi band selection** (Auto, 2.4 GHz, 5 GHz) including enabled channels, fast secure roaming preferences (**FT** and **CCKM**), and the **Wi-Fi low RSSI threshold** can be configured by selecting the three dots in the upper right hand corner while in the **Call Quality Settings** application, then selecting **Settings**.

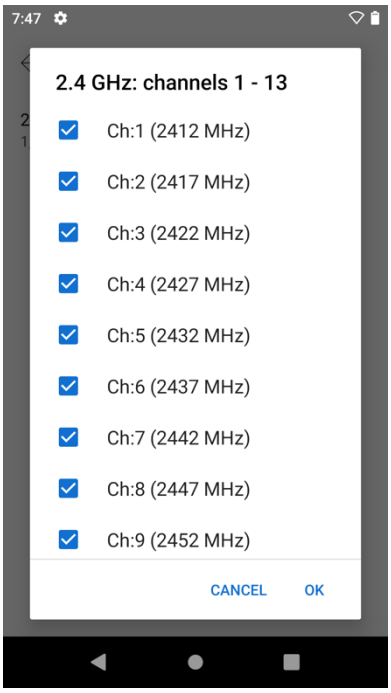


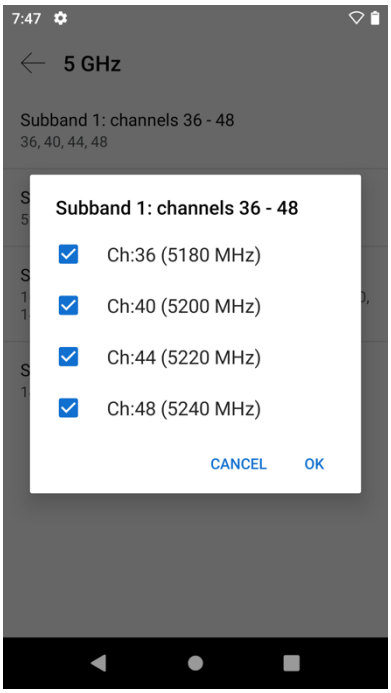


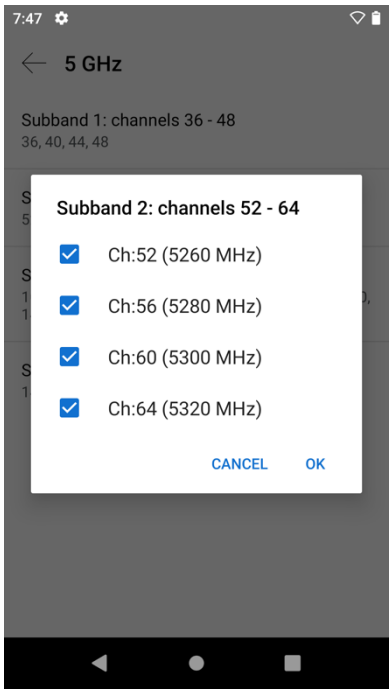
- If wanting to utilize a single Wi-Fi frequency band or to limit the channels to be enabled per Wi-Fi frequency band, select **Wi-Fi band selection**, then uncheck **Auto** and either select **2.4 GHz Wi-Fi band** only, **5 GHz Wi-Fi band** only, or both if wanting to utilize both 2.4 GHz and 5 GHz.

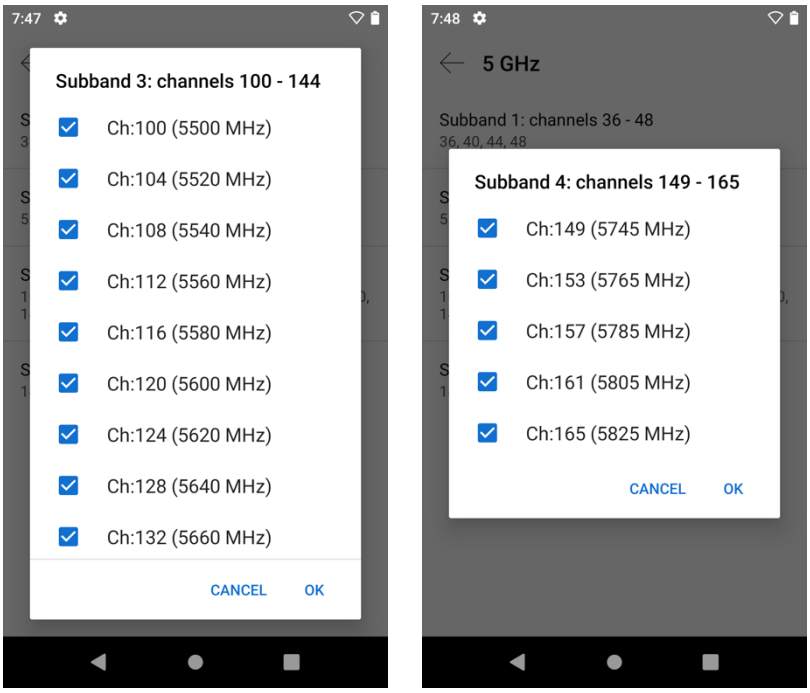


- If **Auto** is unchecked, then the channels to enable per Wi-Fi frequency band can be configured by simply clicking on the desired channel set.

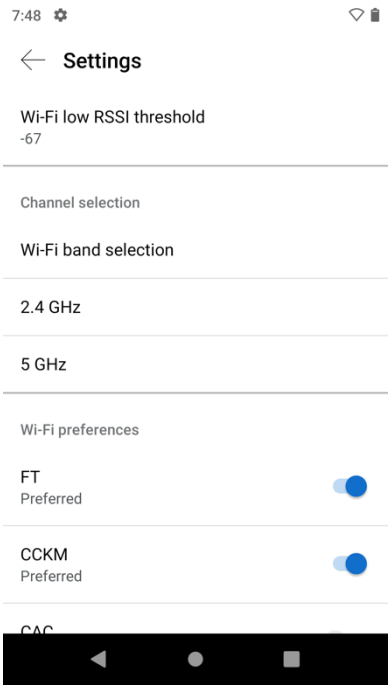

7:47
2.4 GHz: channels 1 - 13
Ch:1 (2412 MHz)
Ch:2 (2417 MHz)
Ch:3 (2422 MHz)
Ch:4 (2427 MHz)
Ch:5 (2432 MHz)
Ch:6 (2437 MHz)
Ch:7 (2442 MHz)
Ch:8 (2447 MHz)
Ch:9 (2452 MHz)
CANCEL
OK


7:47
5 GHz
Subband 1: channels 36 - 48
36, 40, 44, 48
Subband 1: channels 36 - 48
Ch:36 (5180 MHz)
Ch:40 (5200 MHz)
Ch:44 (5220 MHz)
Ch:48 (5240 MHz)
CANCEL
OK


7:47
5 GHz
Subband 1: channels 36 - 48
36, 40, 44, 48
Subband 2: channels 52 - 64
Ch:52 (5260 MHz)
Ch:56 (5280 MHz)
Ch:60 (5300 MHz)
Ch:64 (5320 MHz)
CANCEL
OK



- If wanting to utilize 802.11r (FT) for fast secure roaming, ensure the slider for **FT** is to the right to be set as **Preferred**.
- If wanting to utilize CCKM for fast secure roaming, ensure the slider for **CCKM** is to the right to be set as **Preferred**.
- If both **FT** and **CCKM** are set as **Preferred**, then 802.11r (FT) will be given preference over CCKM.



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

The 1.8(0) release enables the option to disable **CAC** (Call Admission Control).

With the 1.9(0) release, **CAC** (Call Admission Control) is disabled by default and is now an opt-in feature.

WPA3 is not supported.

802.1x-SHA2 key management is not supported.

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

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

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Certificate Management

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

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

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

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

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

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

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

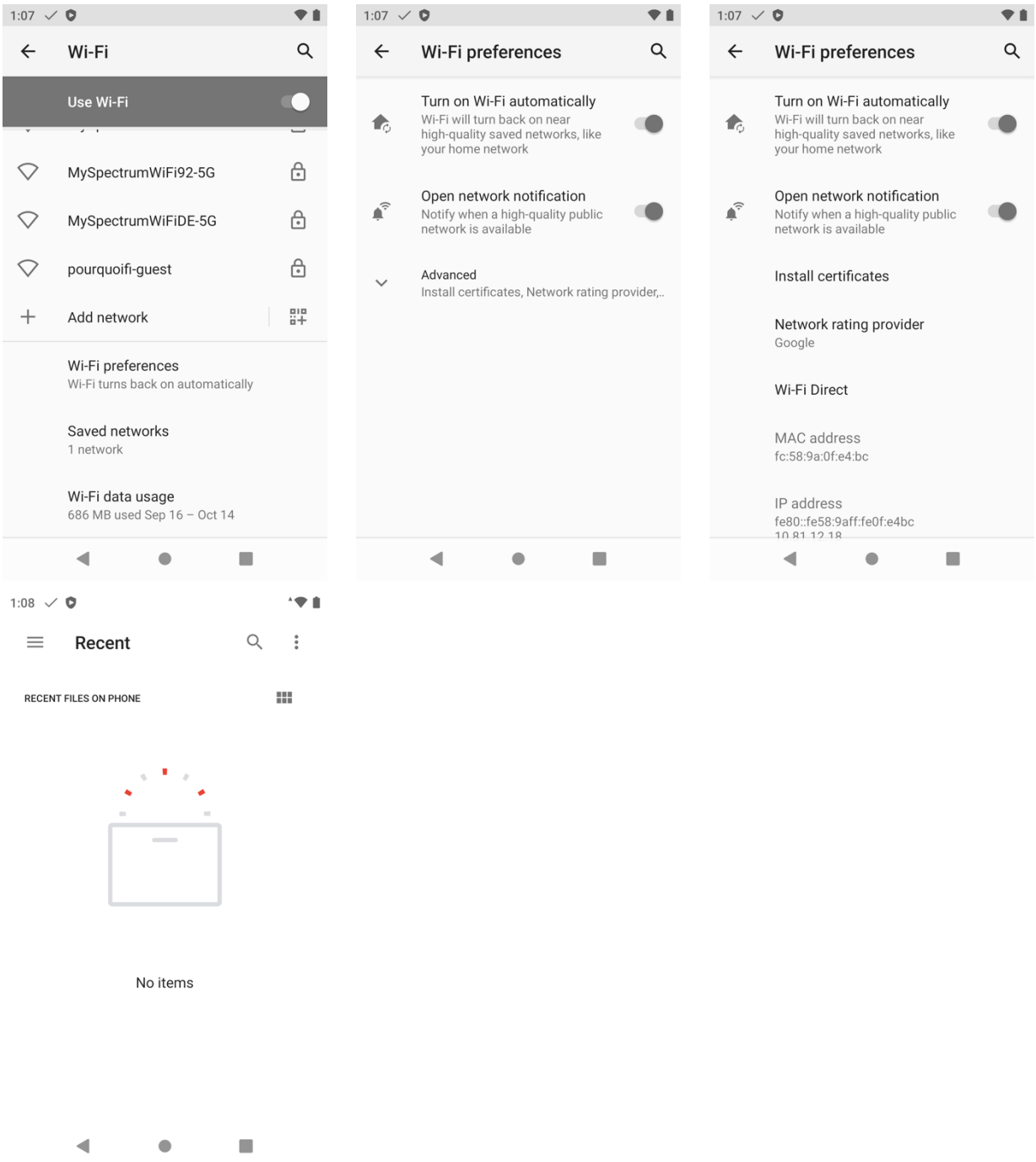
Installing Certificates

Certificates can be automatically installed via an Enterprise Mobility Management (EMM) application if supported by the EMM. Refer to the EMM documentation for more information.

Certificates can also be manually installed within Wi-Fi settings or Security settings.

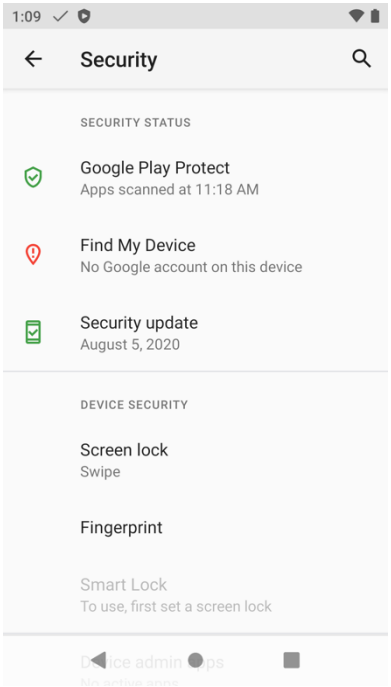
To manually install certificates via Wi-Fi settings, select **Settings > Network & internet > Wi-Fi > Wi-Fi Preferences > Advanced**, then select **Install certificates**.

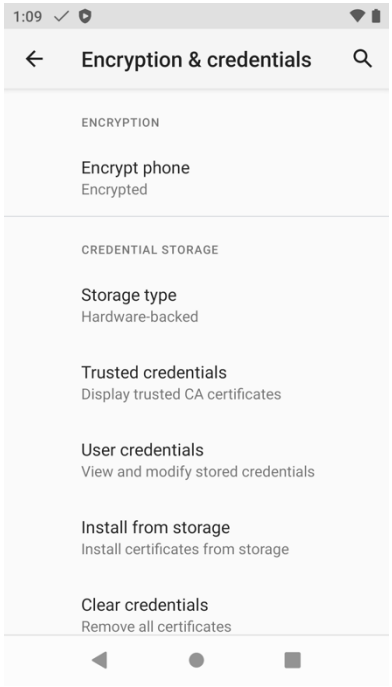
The certificate downloaded or copied to the phone's storage prior can then be selected to be installed.

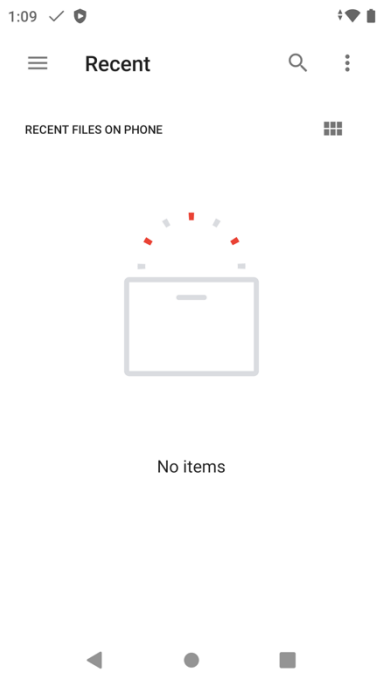


To install certificates via Security settings, select **Settings > Security > Encryption & credentials**, then select **Install from storage**.

The certificate downloaded or copied to the phone's storage prior can then be selected to be installed.





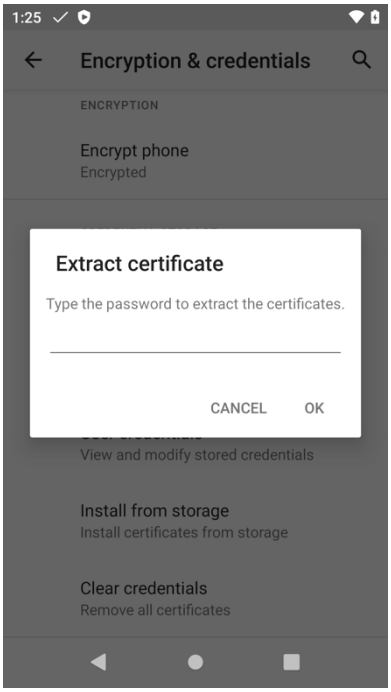


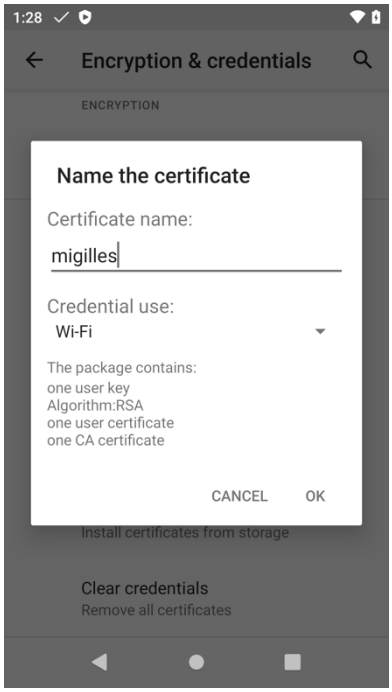
A user certificate must be installed to utilize **EAP-TLS**.

A password may need to be entered to extract the certificates and keys.

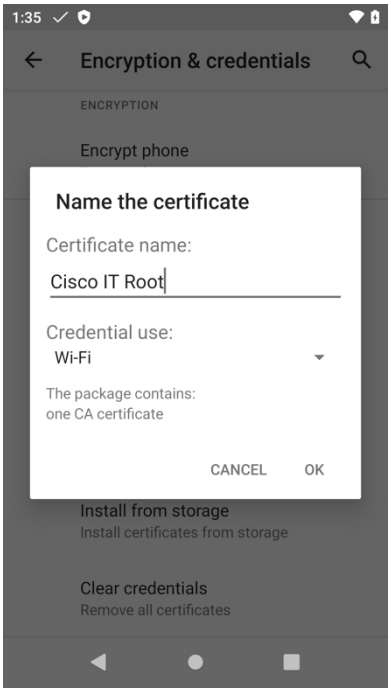
A certificate name can then be entered.

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





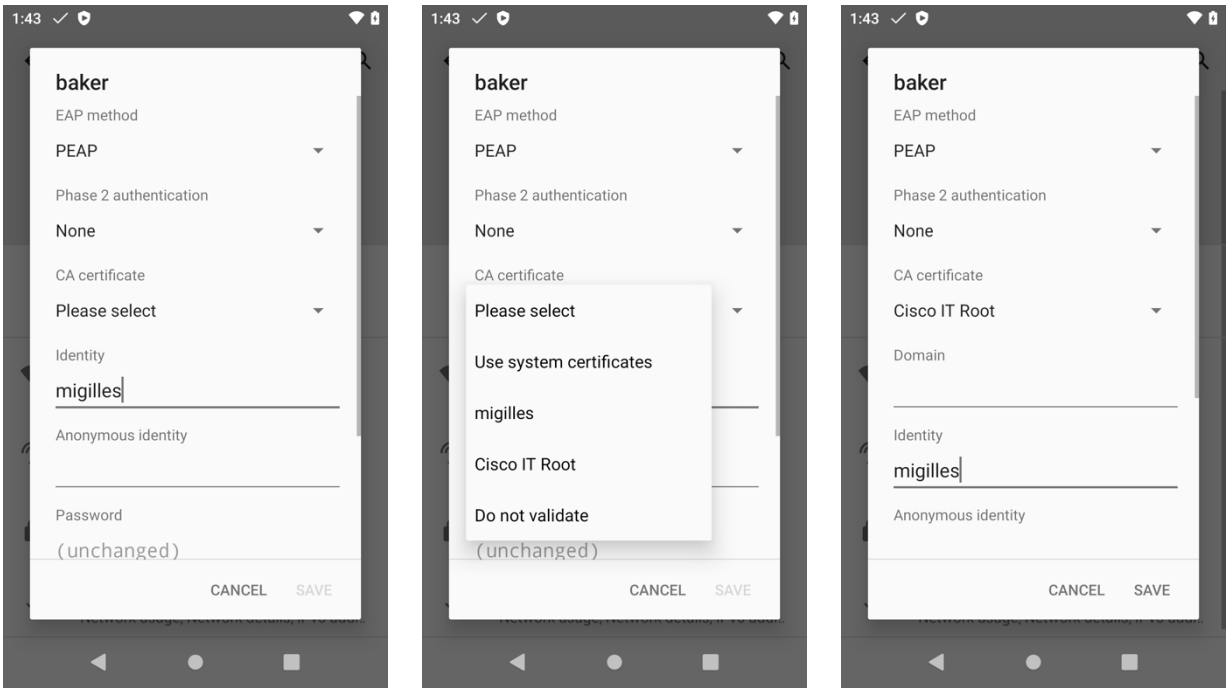
The root CA certificate that issued the RADIUS server's certificate must be installed to enable server validation for **EAP-TLS**, **EAP-TTLS**, or **PEAP**.



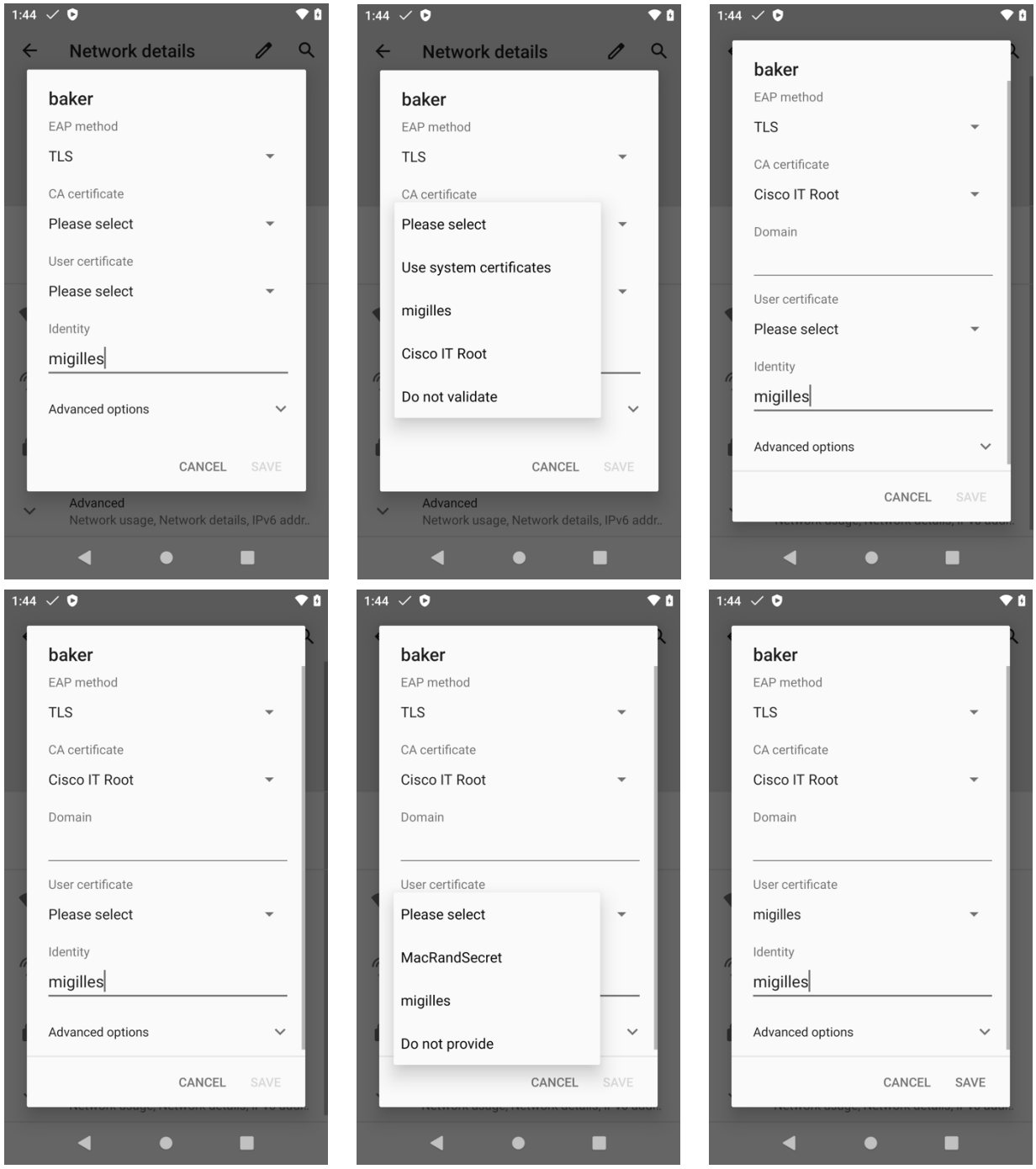
Configuring Certificates

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

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



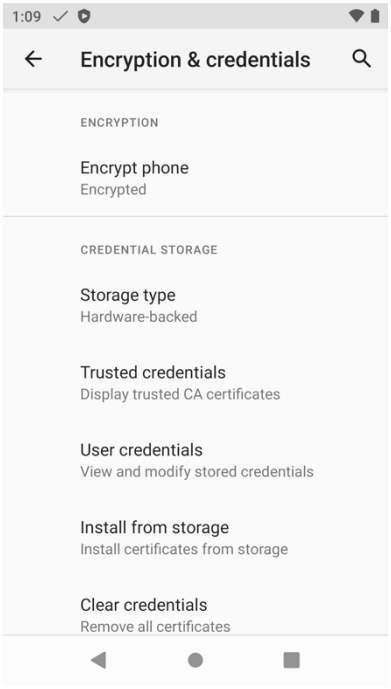
For **EAP-TLS**, the **User certificate** must be configured and the **CA certificate** can optionally be configured to enable server validation.

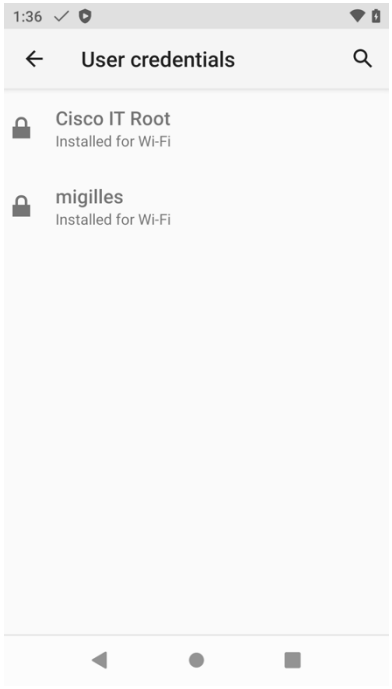


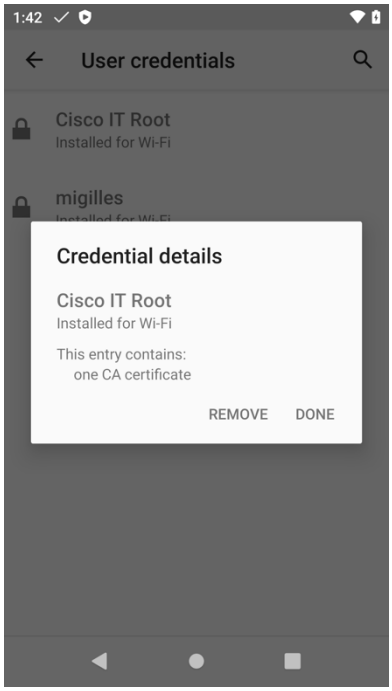
Removing Certificates

Certificates can be removed individually or in bulk.

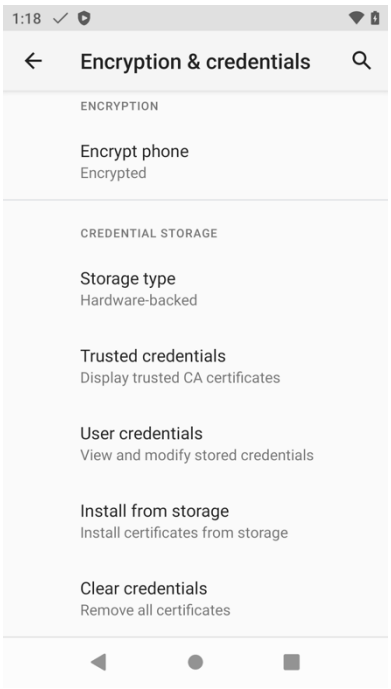
To remove an individual certificate, select the certificate under **Settings** > **Security > Encryption & credentials** > **User credentials**, then select **Remove**.

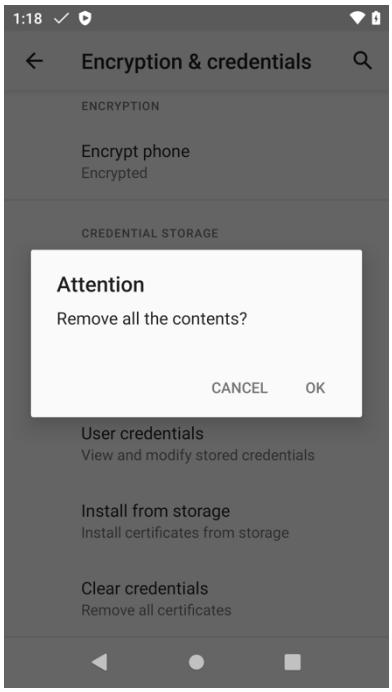






To remove all certificates, select **Clear credentials** under **Settings > Security > Encryption & credentials**, then select **OK** to confirm the removal.

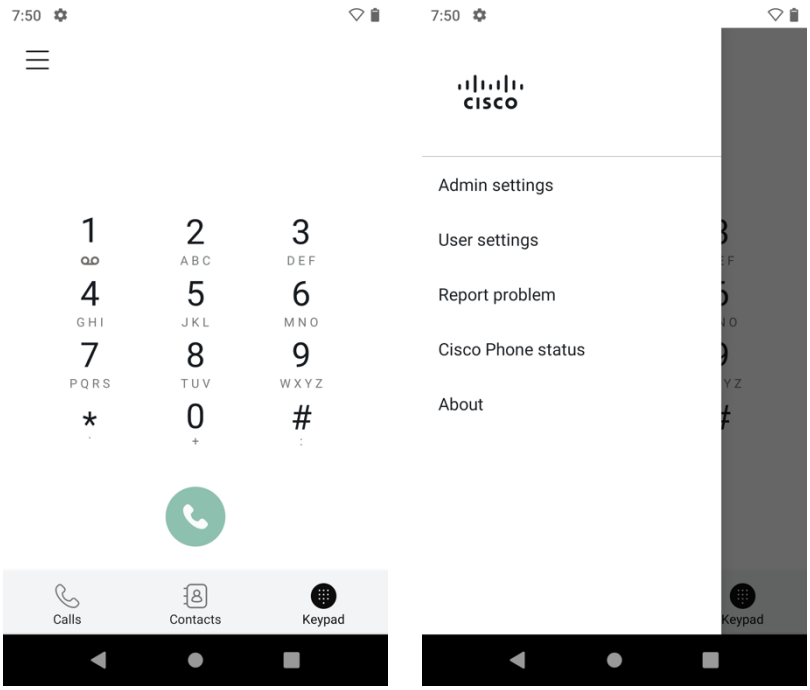




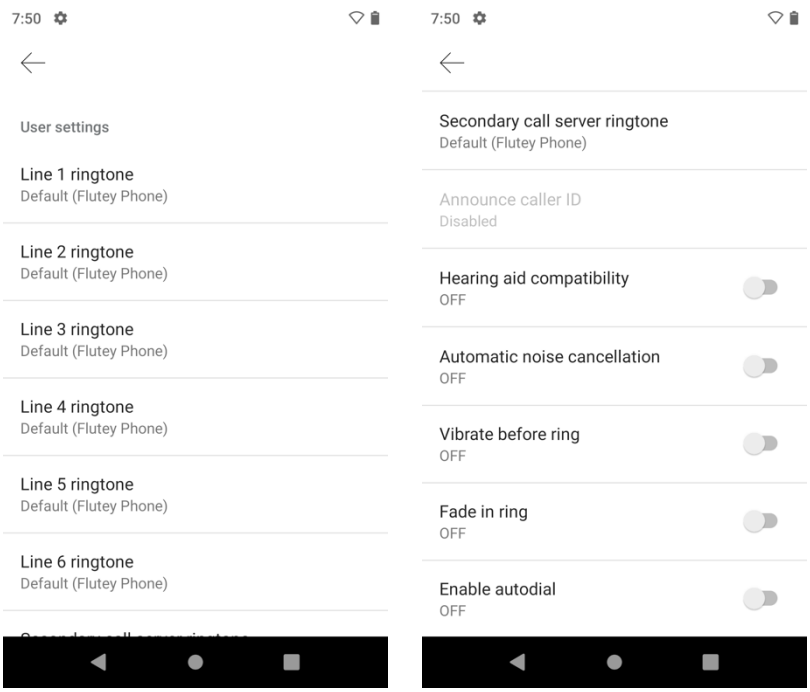
Cisco Phone Application Configuration

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

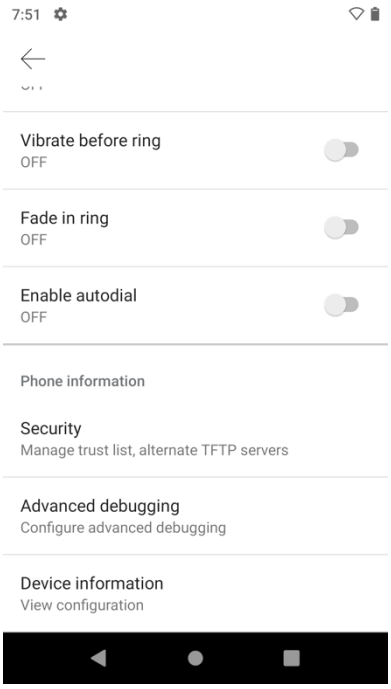
- **Cisco Phone** settings can be configured by selecting the three lines in the upper left hand corner while in the **Cisco Phone** application.



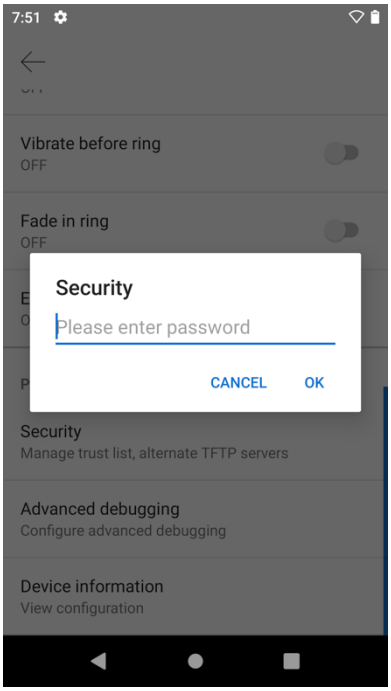
- **User settings** such as ringtones can be configured as necessary.



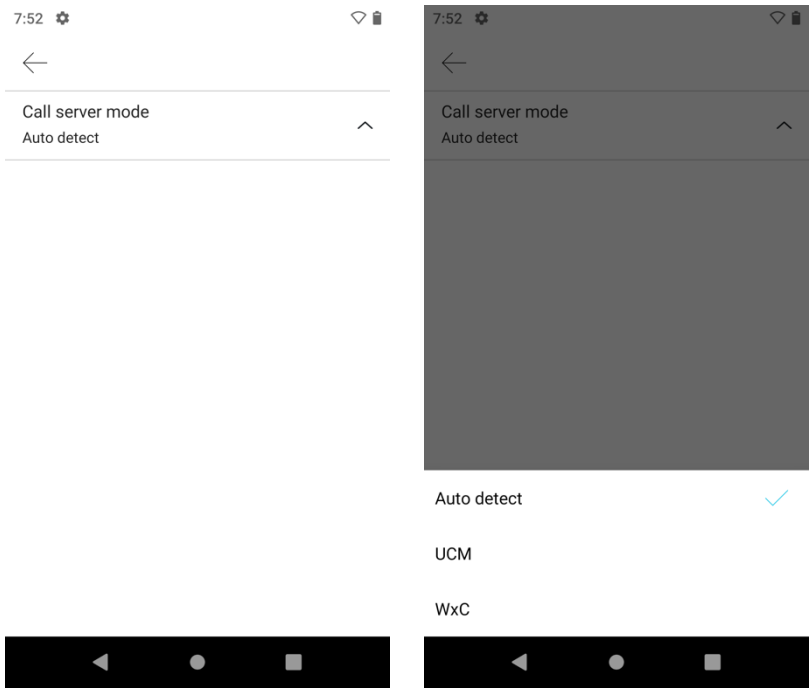
- Trust lists and TFTP servers can be managed by selecting **Phone information > Security**.



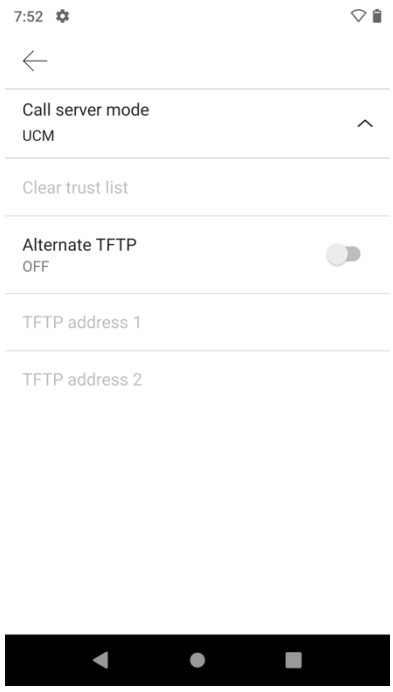
- Once **Phone information > Security** is selected, the **Local Phone Unlock Password** must be entered (default = **#).



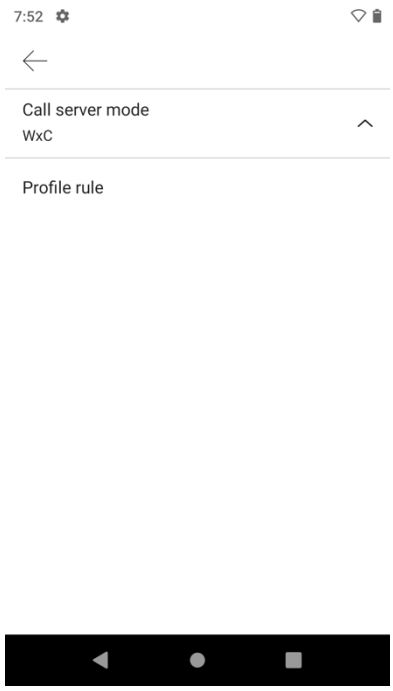
- With the 1.6(0) release, the Call server mode is set to Auto detect, where the Cisco Wireless Phone 840 and 860 will attempt to register to a Cisco Unified Communications Manager if the network is offering DHCP option 150 or DHCP option 66 and the Cisco Wireless Phone 840 or 860 is configured in the Cisco Unified Communications Manager; otherwise it will attempt to register to Webex Calling.



- If wanting to register to Cisco Unified Communications Manager and need to manually configure a TFTP server as the network is not providing DHCP option 150 or DHCP option 66 for the Cisco Unified Communications Manager you want to register to, set the **Call server mode** to **UCM**, enable **Alternate TFTP**, then enter the TFTP server addresses.
- If the Cisco Wireless Phone 840 or 860 was registered to a Cisco Unified Communications Manager previously and want to register to a different Cisco Unified Communications Manager cluster, select **Clear trust list**.



- If wanting to register to Webex Calling and need to manually configure the settings, set the **Call server mode** to **WxC**, select **Profile rule**, then enter the the profile rule information.



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

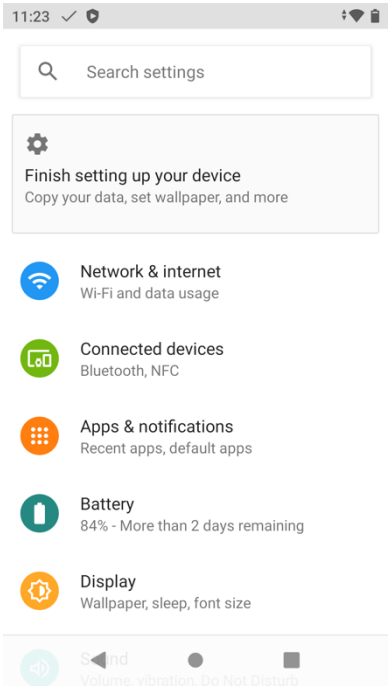
For more information, refer to the **Cisco Wireless Phone 840 and 860 Administration Guide** at this URL:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

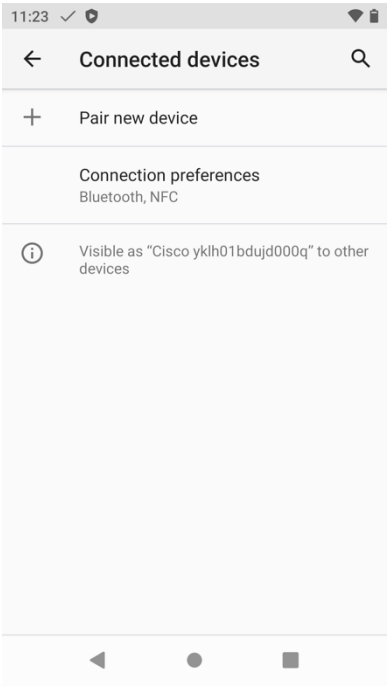
Note: DHCP option 66 is supported as of the 1.2(0) release.

Bluetooth Settings

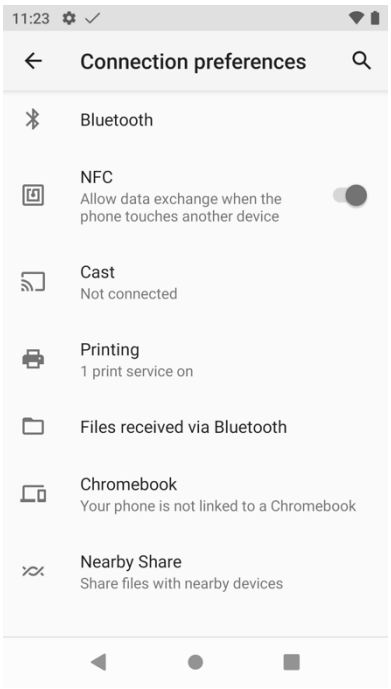
The Cisco Wireless Phone 840 and 860 include Bluetooth support, which enables hands-free communications.
To pair a Bluetooth headset to the Cisco Wireless Phone 840 and 860, follow the instructions below.

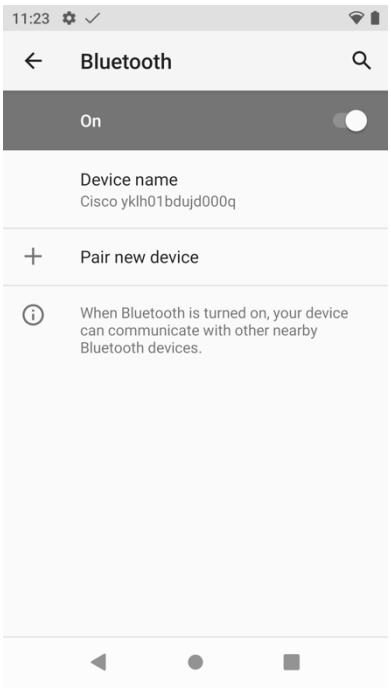
- Navigate to **Settings > Connected devices**.



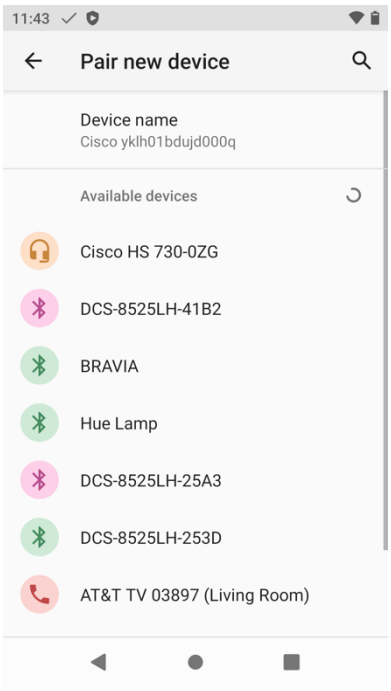


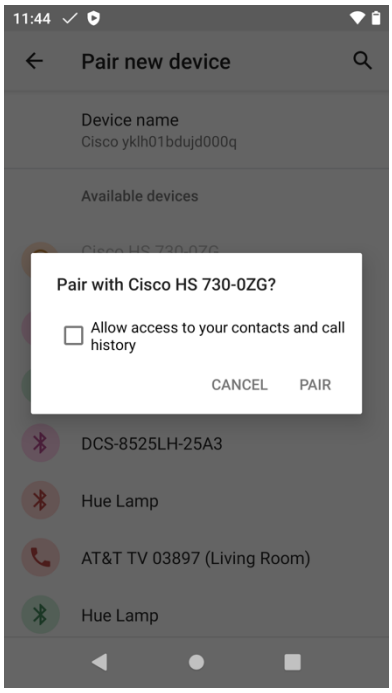
- Ensure that **Bluetooth** is set to **On** in **Settings > Connected devices > Connection Preferences > Bluetooth**.
- The Bluetooth device name can also be changed as necessary.



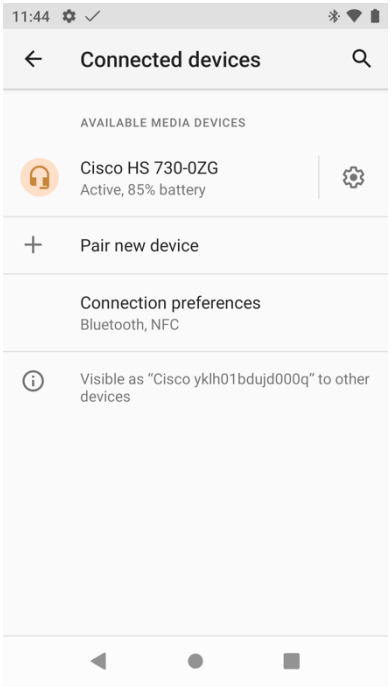


- Ensure the Bluetooth device is in pairing mode, then select **Pair new device.**
- Select the Bluetooth device after it is displayed in the list.
- The Cisco Wireless Phone 840 and 860 will then attempt to pair automatically with the Bluetooth device. If unsuccessful, enter the PIN code when prompted.

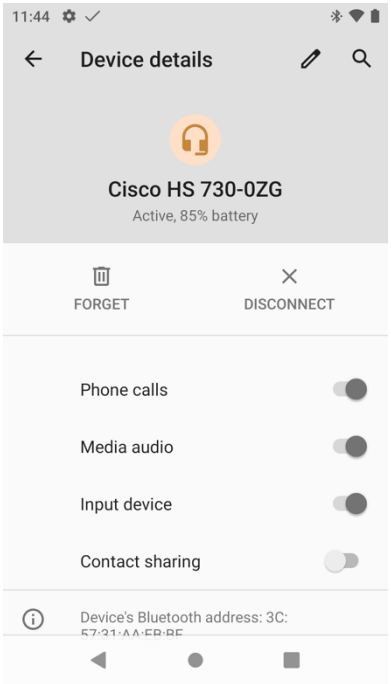




- Once paired, the Cisco Wireless Phone 840 and 860 will attempt to connect to the Bluetooth device.

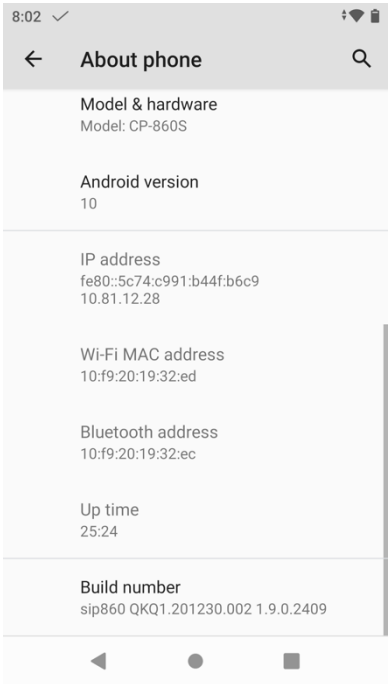


- The Bluetooth device name can be changed in the device details.
- Selecting the Bluetooth device then selecting **Disconnect** will disconnect that currently connected Bluetooth device.
- Select **Forget** to unpair the selected Bluetooth device.



Upgrading Firmware

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



Note: With the 1.10.x releases, the OS version will show as 1.9.1.2908 for the Cisco Wireless Phone 840 and as 1.9.0.2409 for the Cisco Wireless Phone 860; however the Apps bundle version will show as 1.10.1.2284 for the Cisco Wireless Phone 840 and as 1.10.1.2697 for the Wireless Phone 860.

Cisco Unified Communications Manager

To upgrade the firmware, install the signed COP file for Cisco Unified Communications Manager then restart the Cisco TFTP service for all nodes running the Cisco TFTP service.

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

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

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

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

The user will be prompted to confirm to reboot and apply the new firmware unless the **Reboot immediately after downloading software updates** option is enabled in the call server.

Note: The individual firmware COP files for the Cisco Wireless Phone 840 and 860 must be downloaded from Cisco.com and installed manually, as the firmware files are not included in updates for Cisco Unified Communications Manager due to the size of the files.

If the Cisco Unified Communications Manager version is prior to 14 SU1, then is recommended to deploy and utilize an external HTTP load server operating on TCP port 6970. Versions prior to 14 SU1 do not include HTTP range header support, therefore if there is a network interruption during the firmware download, then the download will have to restart instead of picking up where it left off.

Webex Calling

The firmware version to be installed on the Cisco Wireless Phone 840 and 860 is determined by the configured software upgrade channel in Webex Control Hub (Stable, Beta, Latest) and is pushed down automatically as new firmware becomes available for that software upgrade channel.

Cisco Wireless Phone Upgrade Tool

The Cisco Wireless Phone Upgrade Tool (https://webexphoneupgrade.cisco.com) is a cloud based tool that can upgrade a Cisco Wireless Phone 840 or 860 to the 1.6(0) release.

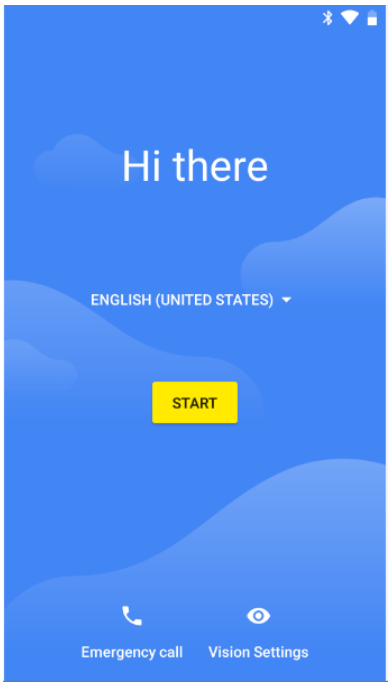
With the new cloud based tool, the Cisco Wireless Phone 840 and 860 firmware can easily be upgraded to the 1.6(0) release by scanning a generated QR code containing the Wi-Fi profile configuration and load server information.

The 1.6(0) release contains Webex Calling support, so this upgrade method will be most beneficial to those that have the Cisco Wireless Phone 840 or 860 and want to register to Webex Calling, but do not have a Cisco Unified Communications manager to upgrade the Cisco Wireless Phone 840 or 860 firmware.

A Cisco.com account is required to access the Cisco Wireless Phone Configuration Management utility.

If the Cisco Wireless Phone 840 or 860 are not new out of box, then they must be factory reset by navigating to **Settings > System > Advanced > Reset options** > **Erase all data (factory reset)**.

On the startup screen, quickly tap the display 6 times to be prompted to scan a QR code to upgrade the Cisco Wireless Phone 840 or 860 firmware.



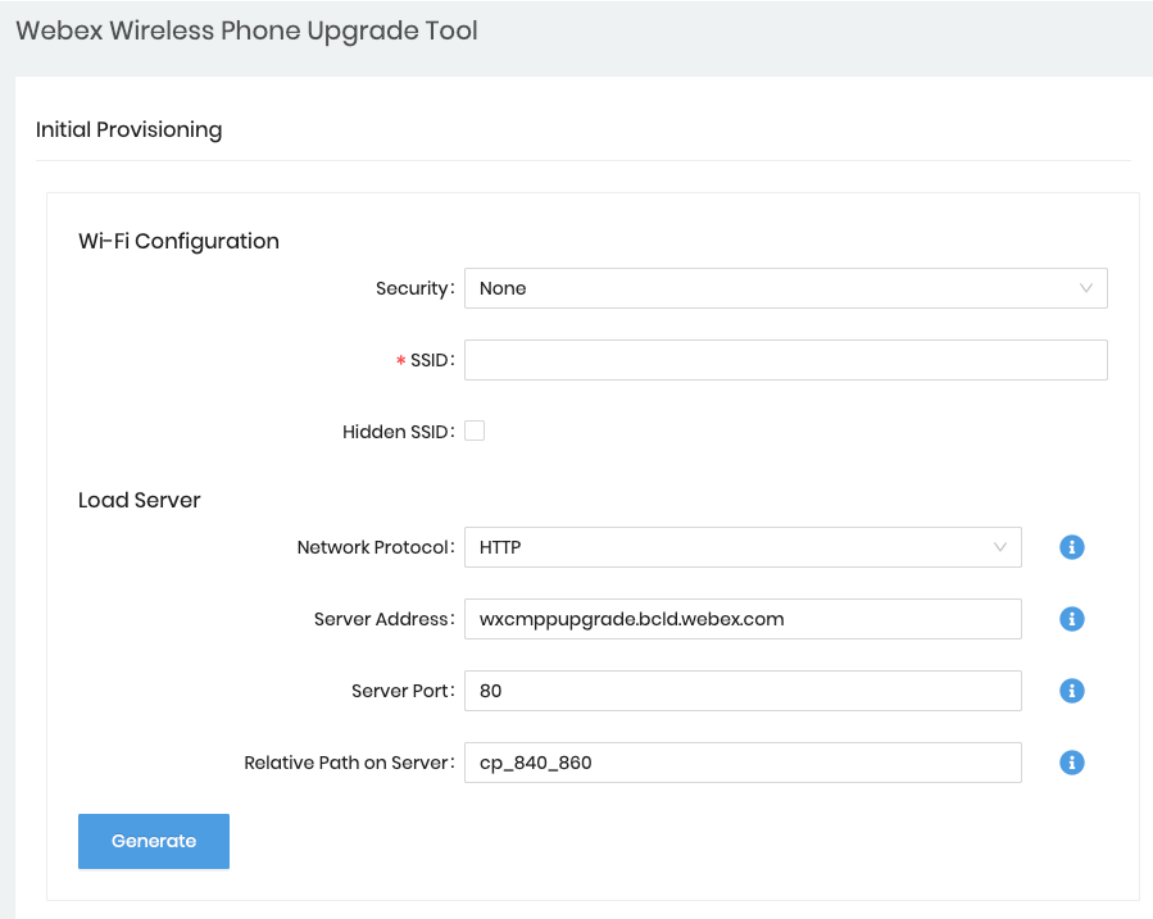
Configure the Wi-Fi configuration and Load Server parameters.

The following security configurations are supported.

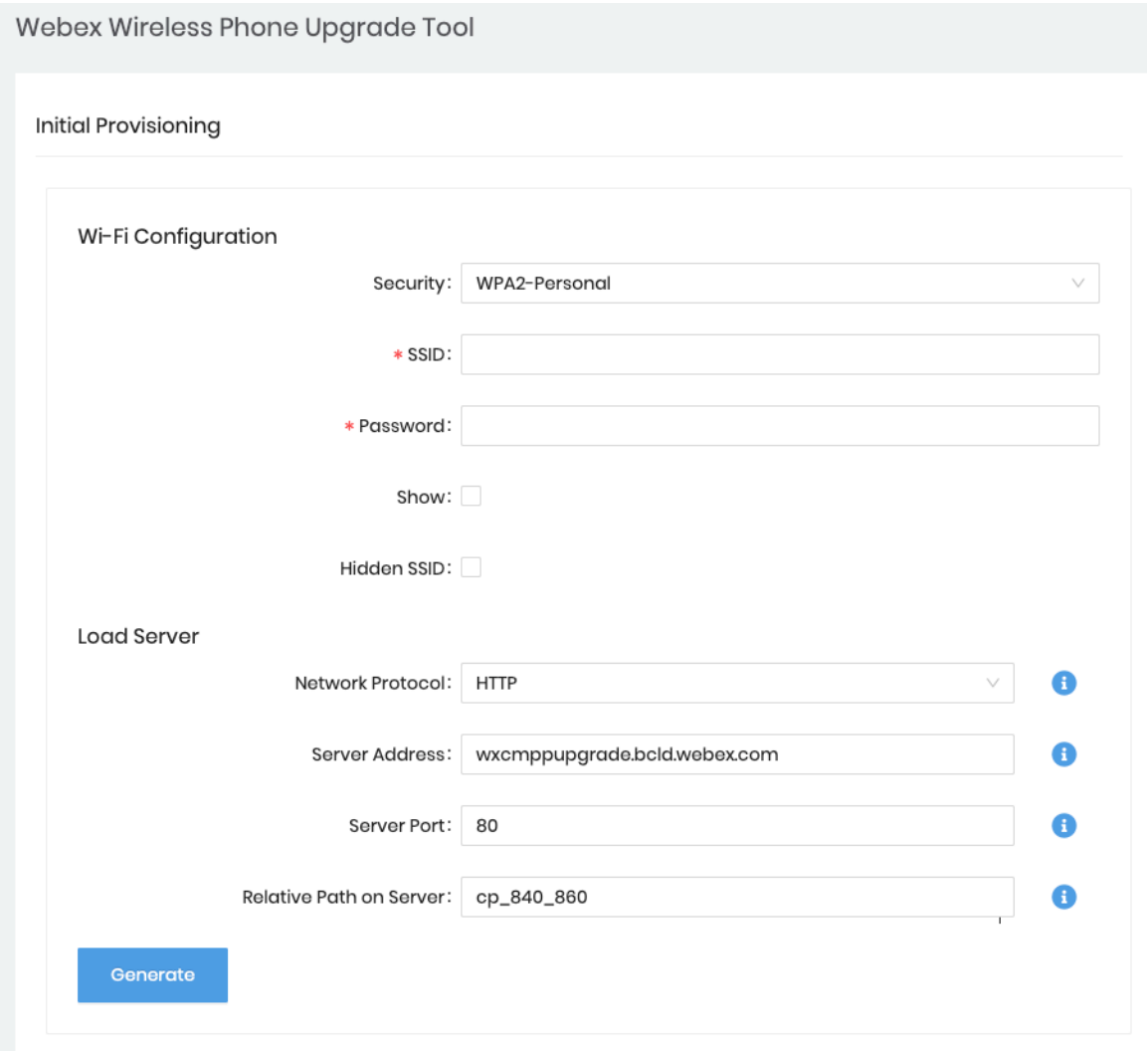
Security Mode	EAP Method	Phase 2 Authentication
None	N/A	None
WPA2-Personal	N/A	None
WPA2-Enterprise	PEAP	GTC, MSCHAPV2
WPA2-Enterprise	TTLS	GTC, MSCHAP, MSCHAPV2, PAP

Note: The Cisco Wireless Phone Upgrade Tool does not support EAP-TLS (TLS).

To connect to an open Wi-Fi network, enter the **SSID**, then set **Security** to **None**.

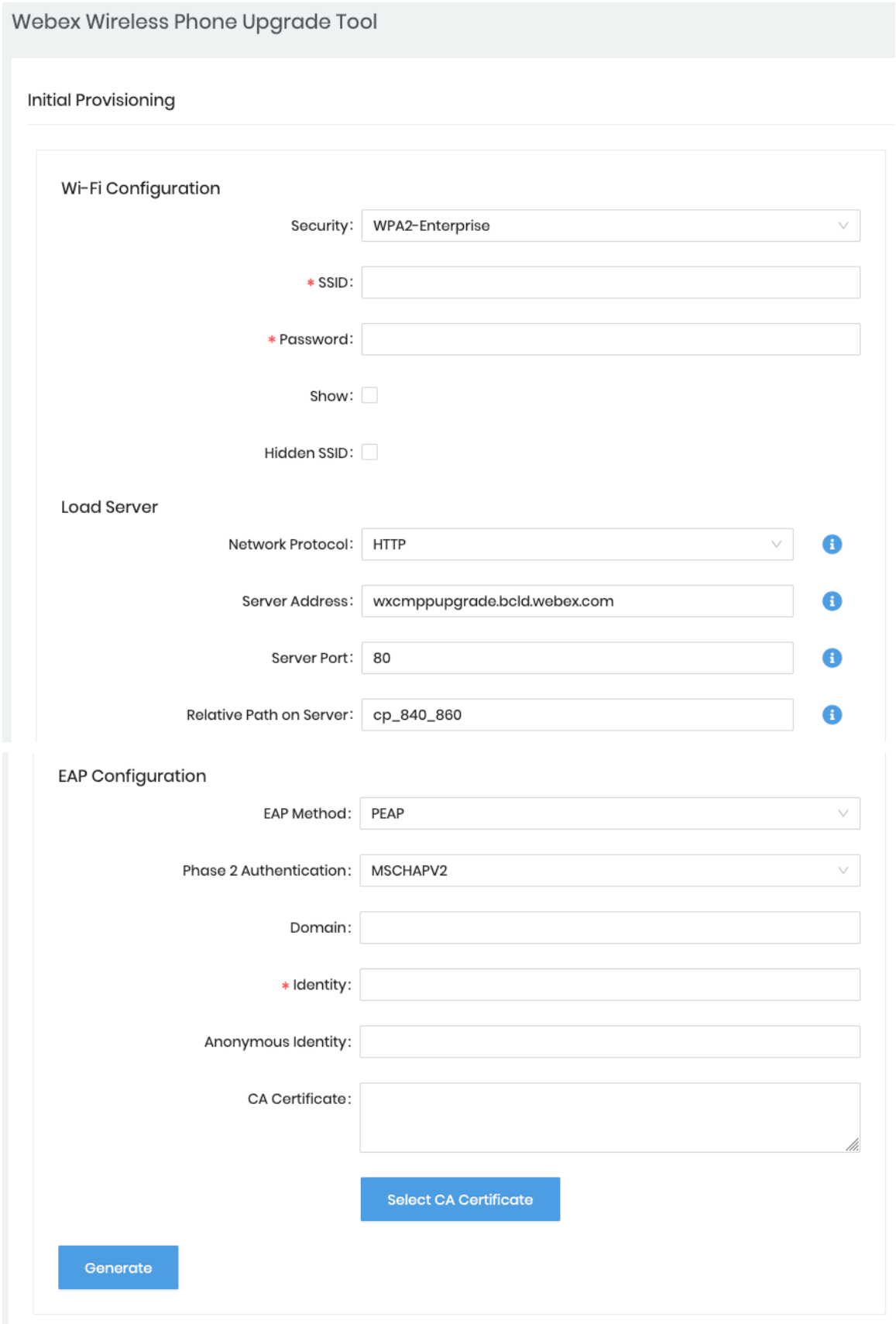


To connect to a PSK enabled Wi-Fi network, enter the **SSID**, set **Security** to **WPA2-Personal**, then enter the 8-63 ASCII or 64 HEX **Password**.



To connect to an EAP enabled Wi-Fi network, enter the **SSID**, set **Security** to **WPA2-Enterprise**, then select the **EAP method**.

If configuring a PEAP or EAP-TTLS (TTLS) Wi-Fi network, select the **Phase 2 authentication** method and configure **CA certificate** as necessary in Base-64 (PEM) encoding format minus the header and footer, then enter the **Identity** and **Password**.



Note: A non-broadcasted Wi-Fi network must be configured as a **Hidden SSID**; otherwise the Wi-Fi network will show as not in range. Set **Hidden SSID** to **True** to connect to a non-broadcasted Wi-Fi network.

Ensure the CA certificate format is correct, where the header and footer are removed and there are no spaces or carriage returns included.

The Cisco Wireless Phone 840 and 860 firmware files can also be downloaded and hosted on an alternative load server instead of using the Cisco managed load server for the firmware upgrade.

The following files will need to be downloaded and uploaded to the alternative HTTP or HTTPS load server.

- http://wxcmppupgrade.bcld.webex.com/cp_840_860/UpgradeDPC.apk
- http://wxcmppupgrade.bcld.webex.com/cp_840_860/sip840-ota_update-signed-1.6.0.1409.zip
- http://wxcmppupgrade.bcld.webex.com/cp_840_860/sip860-ota_update-signed-1.6.0.1852.zip

Note: In order to use the HTTPS method, need to ensure the HTTPS server is issued a certificate from a trusted CA that is included in Android's certificate trust store.

The certificate for the default load server (**wxcmppupgrade.bcld.webex.com**) is not issued from a trusted CA included in Android's certificate trust store; therefore HTTPS should not be used and the default HTTP TCP port 80 configuration should be used.

When configuration is complete, select **Generate** to create the QR code, then the QR code will be displayed.

Scan the QR code with the Cisco Wireless Phone 840 or 860.

The QR code can be saved in case the Cisco Wireless Phone 840 or 860 is not nearby. If so, suggest to save the QR code as a PDF file or as a screenshot as saving the file as a PNG file will alter the file and cause the QR code scan to fail.

The Cisco Wireless Phone 840 and 860 will then attempt to connect to the configured Wi-Fi network and download the firmware files from the load server.

The Cisco Wireless Phone 840 and 860 will then be factory reset automatically.

Note: The Cisco Wireless Phone 840 and 860 must be in range of the configured Wi-Fi network, otherwise the firmware upgrade will fail.

Using the Cisco Wireless Phone 840 and 860

Applications

The Cisco Wireless Phone 840 and 860 have the following pre-installed custom applications.

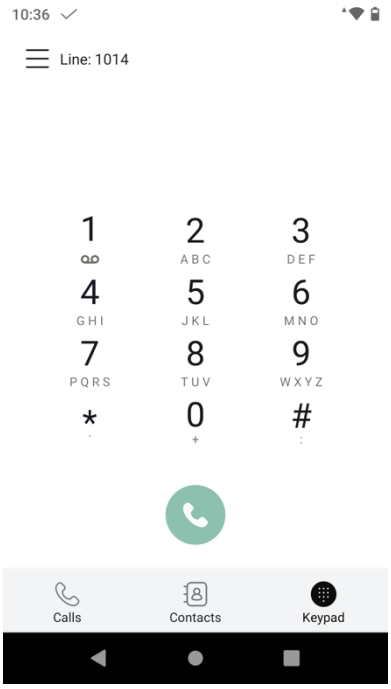
- **Cisco Phone** - Voice and video calling
- **Battery Life** - Battery monitoring
- **Buttons** - Button customizations
- **Call Quality Settings** - Wi-Fi customizations
- **Custom Settings** - User restrictions and device settings
- **Diagnostics** - Hardware troubleshooting
- **Emergency** - Panic button feature
- **Logging** - Advanced debugging
- **PTT** - Push to talk feature
- **System Updater** - Firmware update notifications
- **Web API** – Web API settings
- **Barcode** - Barcode scanning feature (840s and 860s models only)

Cisco Phone

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

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

The Cisco Wireless Phone 840 and 860 is registered to a Cisco Unified Communications Manager or Webex Calling when there is a check mark icon in the notification status bar and the extension is displayed in the Cisco Phone application.

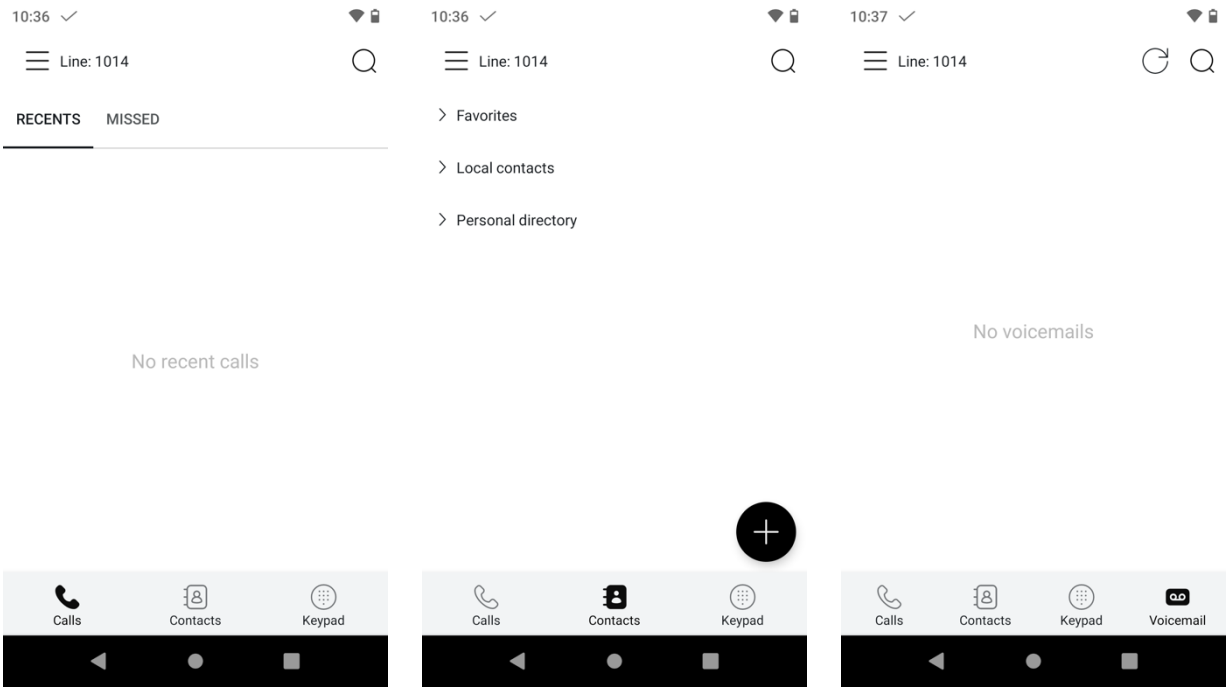


Call history is accessible via the **Calls** tab.

Contacts and favorites are accessible via the **Contacts** tab. To add a **Contact**, select the + icon then select which directory to add the contact to. **Personal directory** requires login in order to view or manage that contact list.

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

Voicemail is accessible via the **Voicemail** tab if **Visual Voicemail Access** is **Enabled** in the call server.



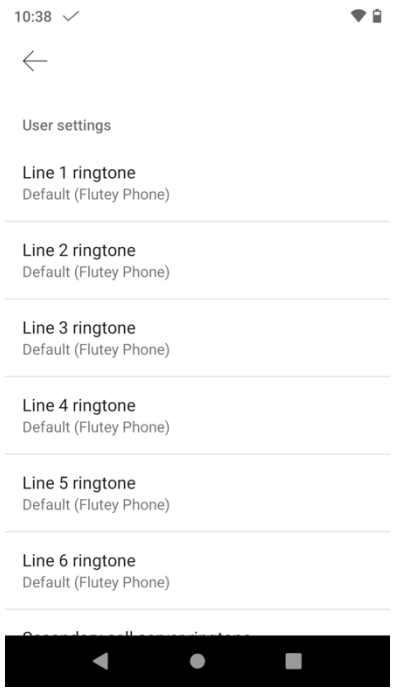
Ringtones can be configured by selecting the three lines in the upper left hand corner then **User settings**.

As of the 1.7(0) release, ringtones can be configured per line, where previous releases only allowed for a single ringtone to be configured.

The 1.8(0) release allows pre-installed ringtones to be configured and managed per line within Cisco Unified Communications Manager.

With the 1.9(0) release, custom ringtones can be configured and managed per line within Cisco Unified Communications Manager, then downloaded to the phone.

With the 1.10(0) release, **None** has been can be added the list of ringtone options, in which the line will not ring if configured as such.

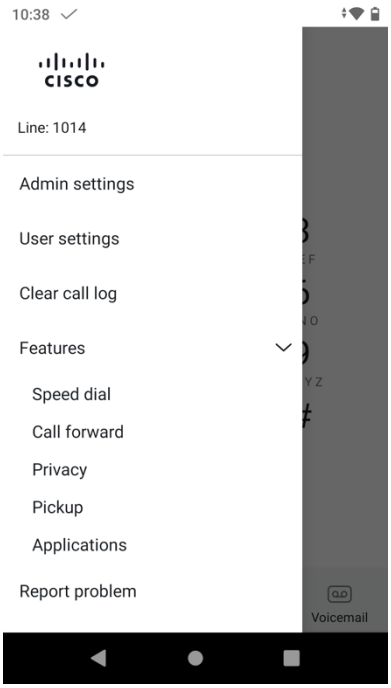


Below are the pre-installed ringtones that can be configured for the **Line 1-6 Ringtone** options within Cisco Unified Communications Manager.

- None
- Andromeda
- Aquila
- Argo Navis
- Atria
- Beat Plucker
- Bell Phone
- Big Easy
- Bootes
- Canis Major
- Carina
- Cassiopeia
- Centaurus
- Chimey Phone
- Cygnus

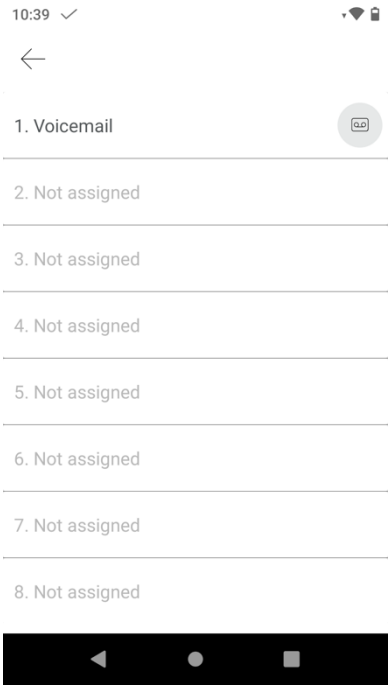
- Digital Phone
- Ding
- Draco
- Dream Theme
- Eridani
- Flutey Phone
- Free Flight
- Girtab
- Growl
- Hydra
- Insert Coin
- Kuma
- Lyra
- Machina
- Mildly Alarming
- New Player
- Noisey One
- Orion
- Pegasus
- Perseus
- Pyxis
- Rasalas
- Rigel
- Scarabaeus
- Sceptrum
- Solarium
- Testudo
- Third Eye
- Very Alarmed
- Vespa
- Zeta

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



To configure speed dials, select **Features** > **Speed dial**.

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

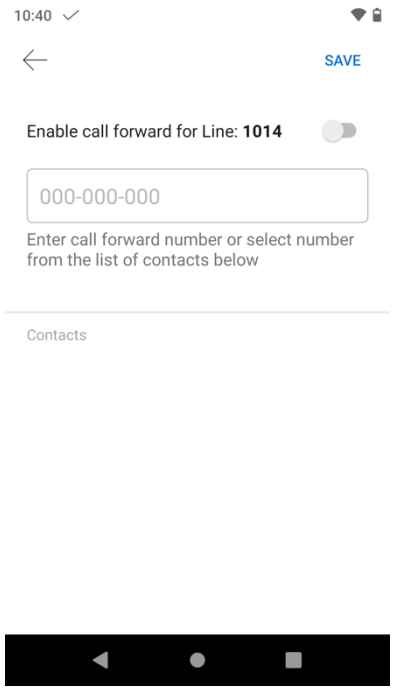


To enable call forward when Cisco Wireless Phone 840 and 860 is registered to Cisco Unified Communications Manager, select **Features** > **Call forward**, tap the slider so it moves to the right, then enter the destination number to forward all calls to.

To enable call forward when Cisco Wireless Phone 840 and 860 is registered to Webex Calling, select **Features** > **Call forward always** or **Features > Call forward when busy**, tap the slider so it moves to the right, then enter the destination number to forward all calls to.

To disable call forward, simply tap the slider so it moves to the left.

Select **SAVE** in the upper right hand corner to save the settings.

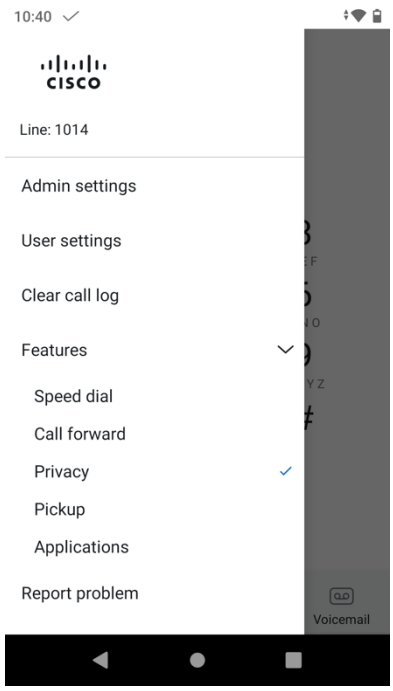


With the 1.3(0) release, the **Privacy** feature is now supported.

To utilize the **Privacy** feature, one of the lines must be a shared line and a custom phone button template with privacy configured for one of the buttons must be created then applied to the phone.

Then to enable privacy, select **Features** > **Privacy**.

A check mark will be displayed to the right of **Privacy** to indicate if the feature is enabled.

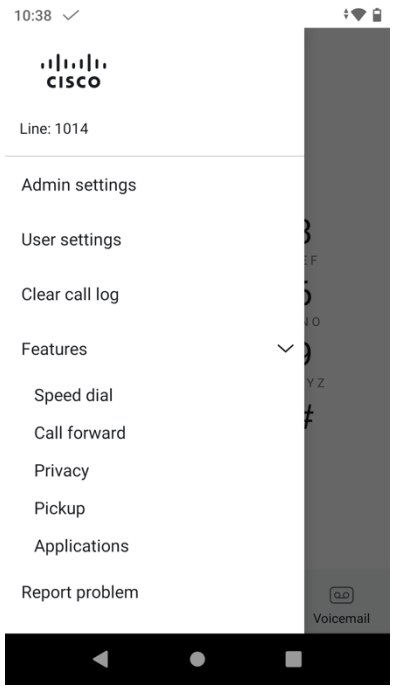


Note: Privacy is not supported for Cisco Wireless Phone 840 and 860 when registered to Webex Calling.

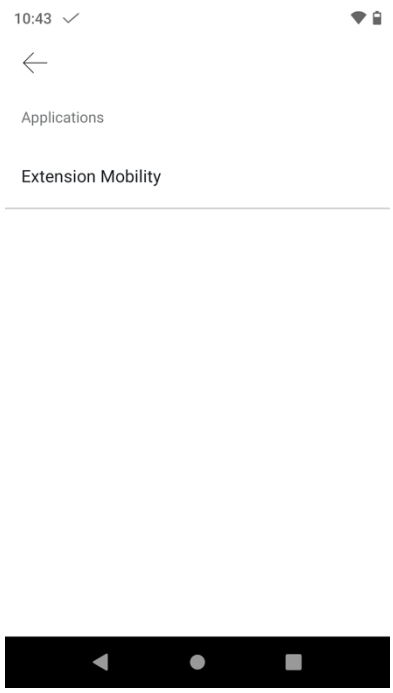
With the 1.9(0) release, the **Call Pickup** feature is now supported.

Ensure a **Call Pickup Group** is configured for a line on the Cisco Wireless Phone 840 and 860 within Cisco Unified Communications Manager.

To utilize the **Call Pickup** feature, select **Features** > **Pickup**.



To access configured applications, select **Features** > **Applications**.

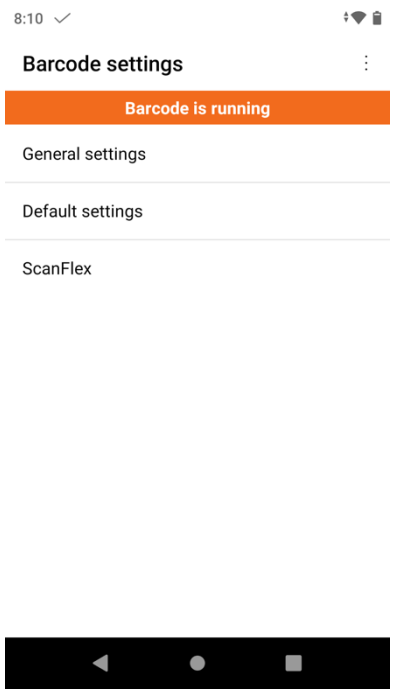


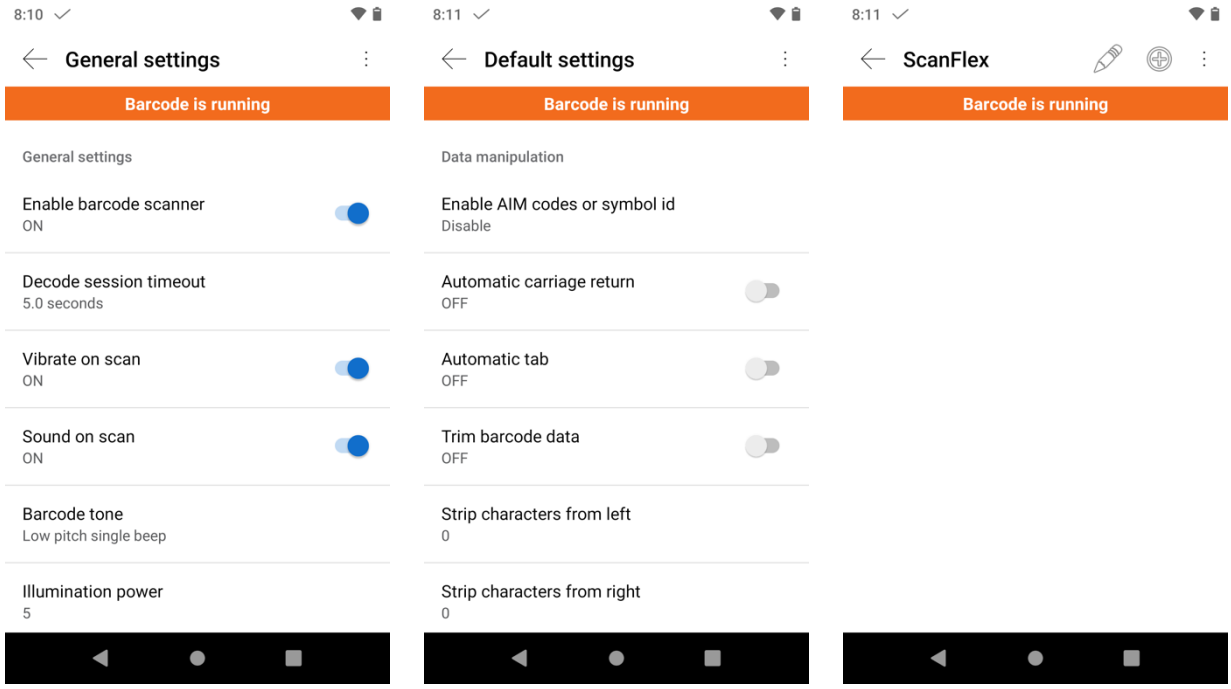
Note: Applications is not supported for Cisco Wireless Phone 840 and 860 when registered to Webex Calling.

Barcode

The barcode scanner is available on the Cisco Wireless Phone 840S and 860S models only.

Barcode scanner settings can be custom configured in the **Barcode** application.

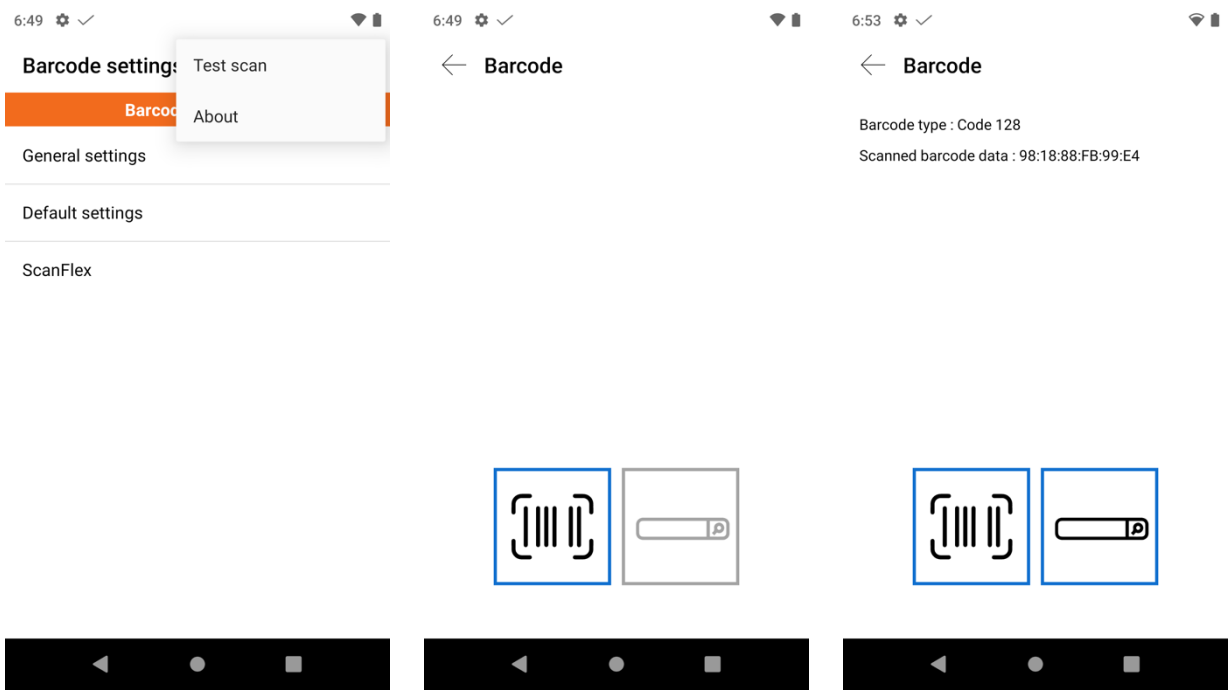


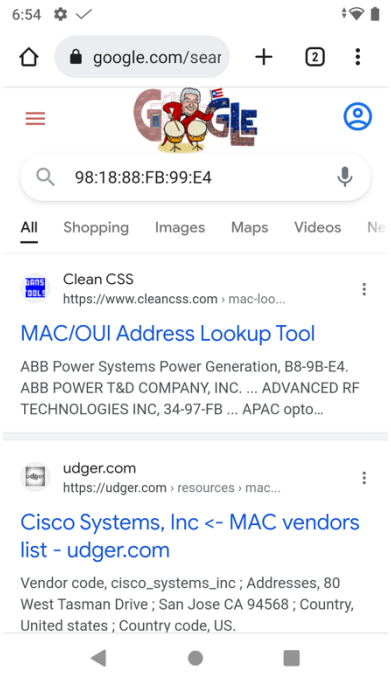


The barcode scanner can be tested by selecting the three dots in the upper right hand corner while in the **Barcode** application, then selecting **Test scan**.

Press the barcode icon below to initiate a barcode scan.

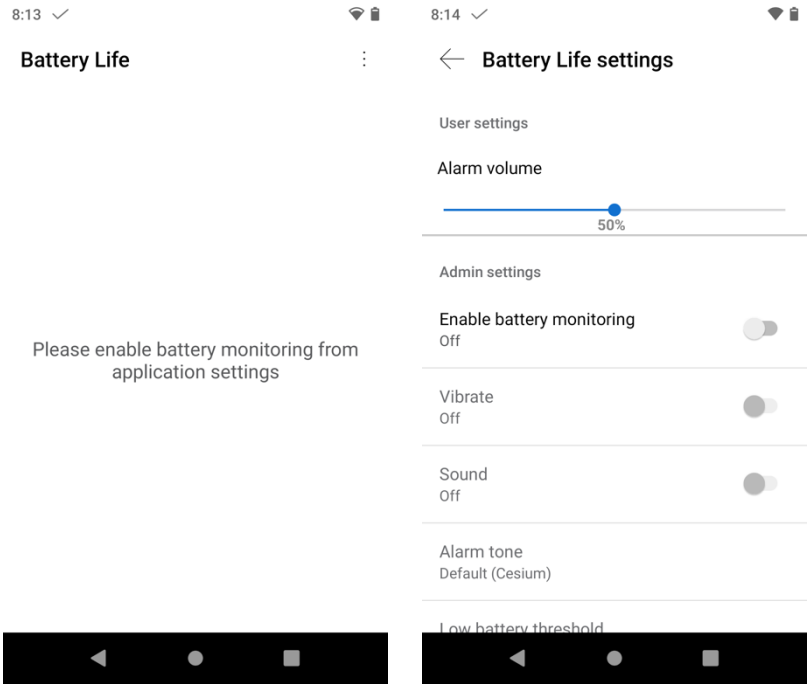
Once the barcode is scanned, can select the lookup icon to perform a search.





Battery Life

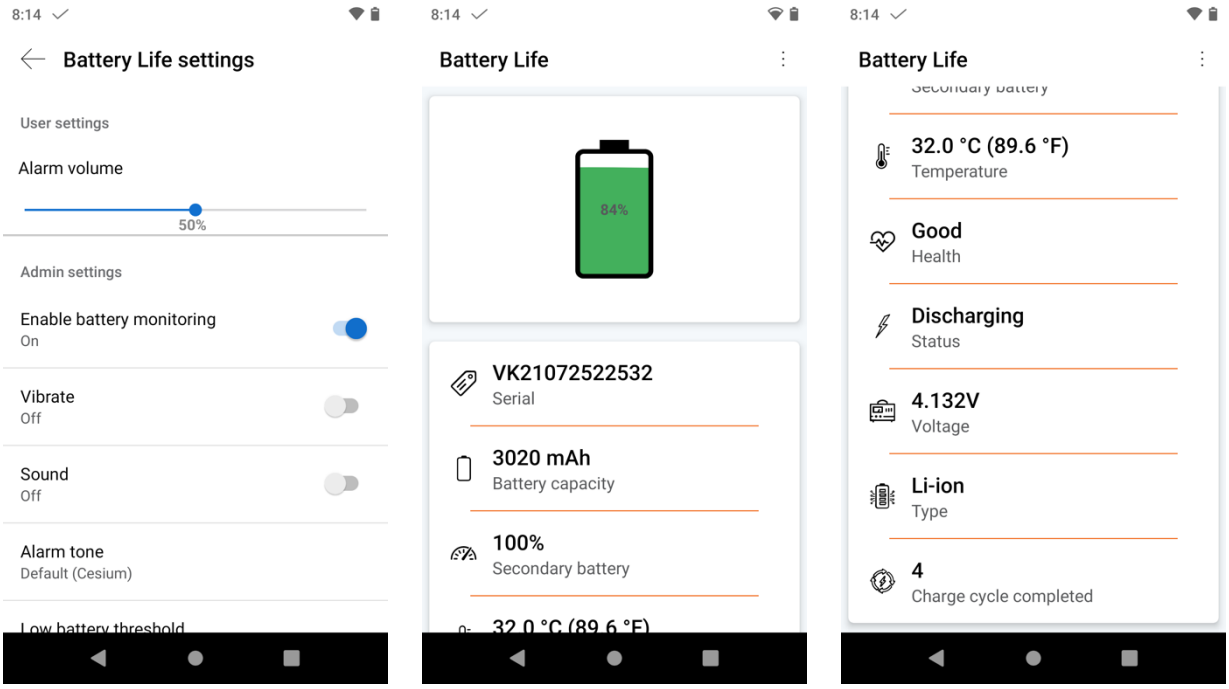
Battery life monitoring can be enabled by selecting the three dots in the upper right hand corner while in the **Battery Life** application, then selecting **Settings**.



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

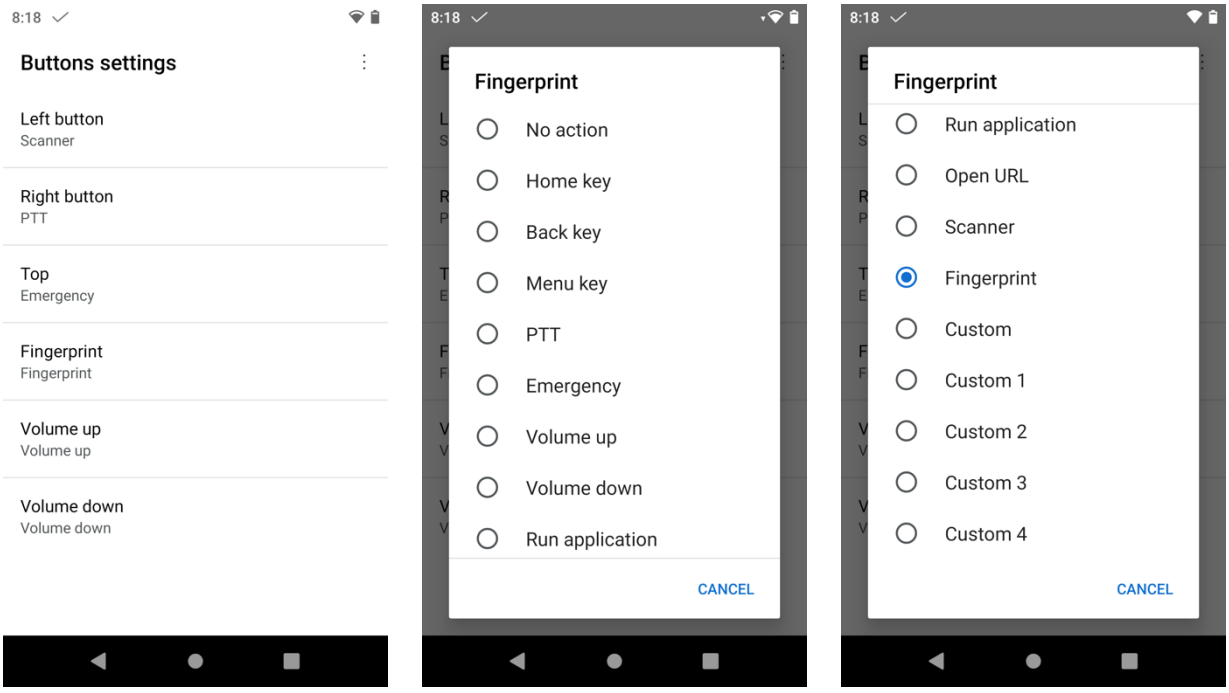
The number of full charge cycles can also be viewed.

Once the number of charge cycles reaches **500**, a notification will be displayed and the battery should be replaced.



Buttons

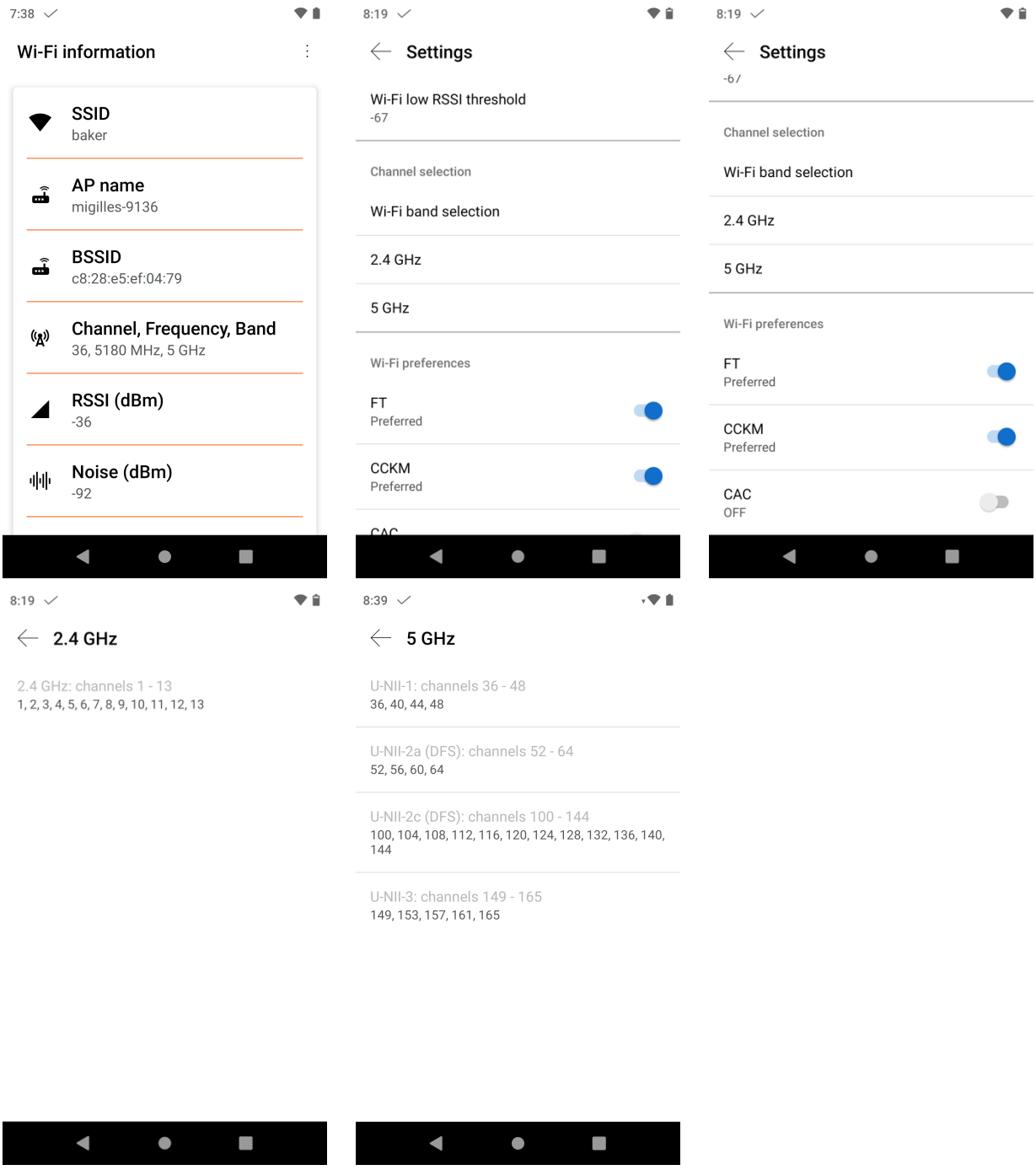
The hard buttons on the Cisco Wireless Phone 840 and 860 can be custom configured in the **Buttons** application.



Note: The Fingerprint button is only available on the Cisco Wireless Phone 860.

Call Quality Settings

The **Wi-Fi band selection** (Auto, 2.4 GHz, 5 GHz) including enabled channels, fast secure roaming preferences (**FT** and **CCKM**), and the **Wi-Fi low RSSI threshold** can be configured by selecting the three dots in the upper right hand corner while in the **Call Quality Settings** application, then selecting **Settings**.

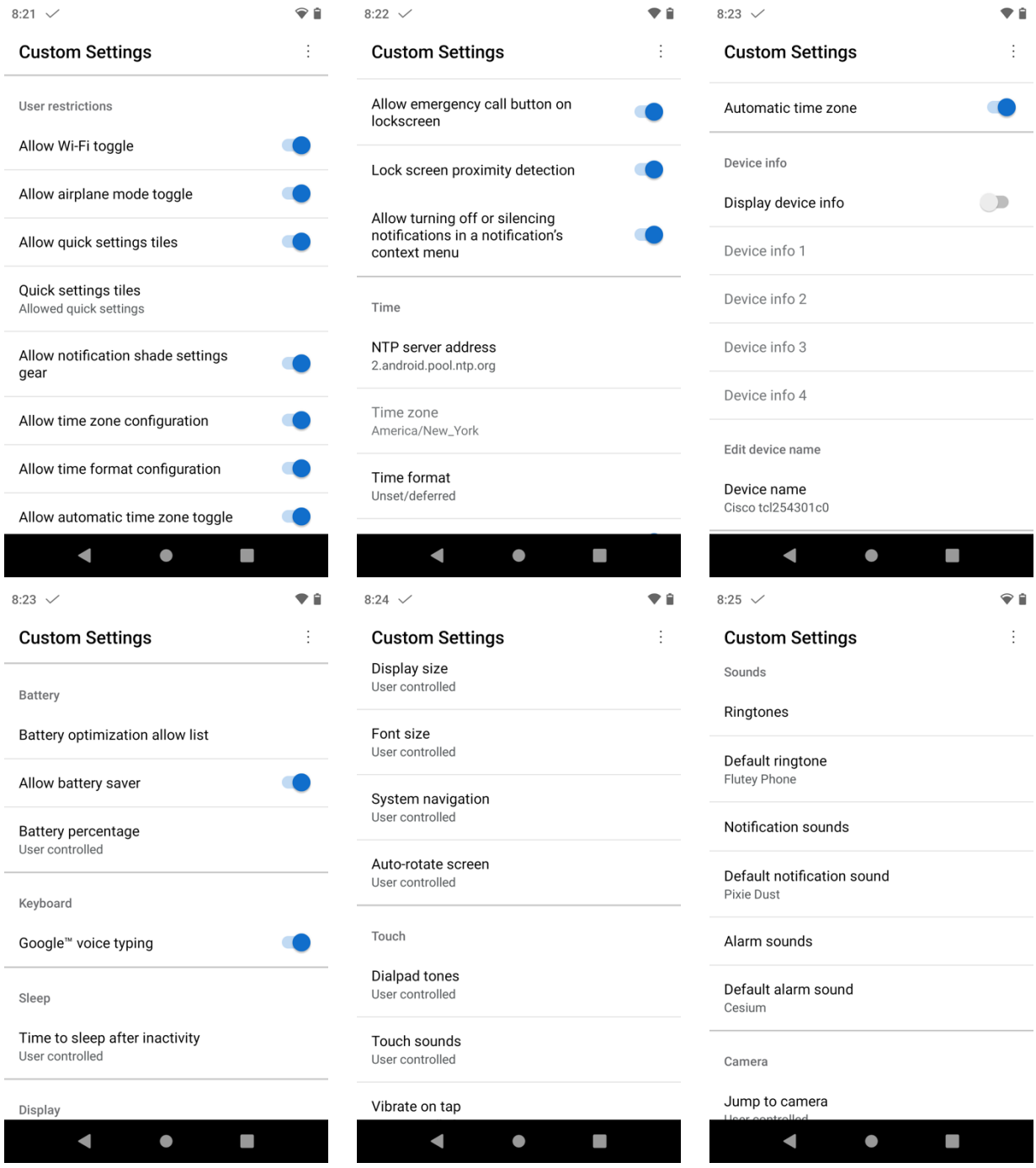


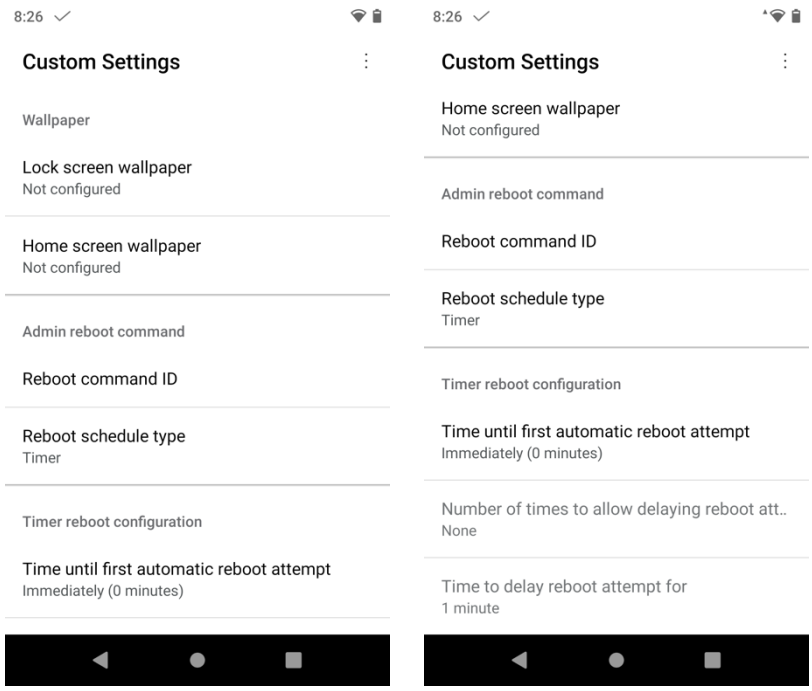
Note: The 1.8(0) release enables the option to disable **CAC** (Call Admission Control).

With the 1.9(0) release, **CAC** (Call Admission Control) is disabled by default and is now an opt-in feature.

Custom Settings

Various settings including user restrictions, time configuration, etc. can be custom configured in the **Custom Settings** application.





Notification sounds can be viewed and managed by selecting **Sounds** > **Notification sounds**.

Alarm sounds can be viewed and managed by selecting **Sounds** > **Alarm sounds**.

The **Default notification sound** and **Default alarm sound** can be managed within the Sounds menu as well.

With the 1.9(0) release, custom notification sounds and alarm sounds can be configured and managed within Cisco Unified Communications Manager, then downloaded to the phone.

Below are the pre-installed notification sounds that can be configured as the **Default notification sound**.

- Adara
- Aldebaran
- Altair
- Alya
- Antares
- Antimony
- Arcturus
- Argon
- Beat Box Android
- Bellatrix
- Beryllium
- Betelgeuse
- Caffeinated Rattlesnake
- Canopus
- Capella
- Captain's Log
- Castor
- Ceti Alpha
- Cobalt
- Cricket
- Dear Deer
- Deneb

- Doink
- Don't Panic
- Drip
- Electra
- Fluorine
- Fomalhaut
- Gallium
- Heaven
- Helium
- Highwire
- Hojus
- Iridium
- Krypton
- Kzurb Sonar
- Lalande
- Look At Me
- Merope
- Mira
- Missed It
- Moonbeam
- On The Hunt
- Palladium
- Pixie Dust
- Pizzicato
- Plastic Pipe
- Polaris
- Procyon
- Proxima
- Radon
- Regulus
- Selenium
- Shaula
- Sirius
- Sirrah
- Space Seed
- Spica
- Strontium
- Syrma
- Ta Da
- Talitha
- Tejat
- Thallium
- Tinkerbell
- Tweeters
- Upsilon
- Vega
- Voila
- Xenon
- Zirconium

Below are the pre-installed alarm sounds that can be configured as the **Default alarm sound**.

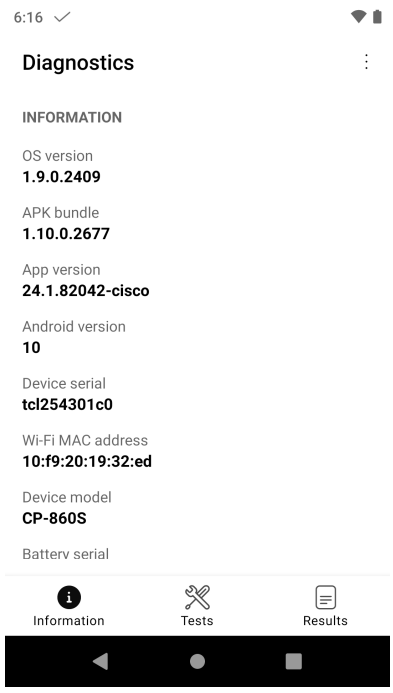
- Argon
- Barium

- BeeBeep Alarm
- Beep-Beep-Beep Alarm
- Buzzer Alarm
- Carbon
- Cesium
- Fermium
- Hassium
- Helium
- Neptunium
- Nobelium
- Osmium
- Piezo Alarm
- Platinum
- Plutonium
- Rooster Alarm
- Scandium

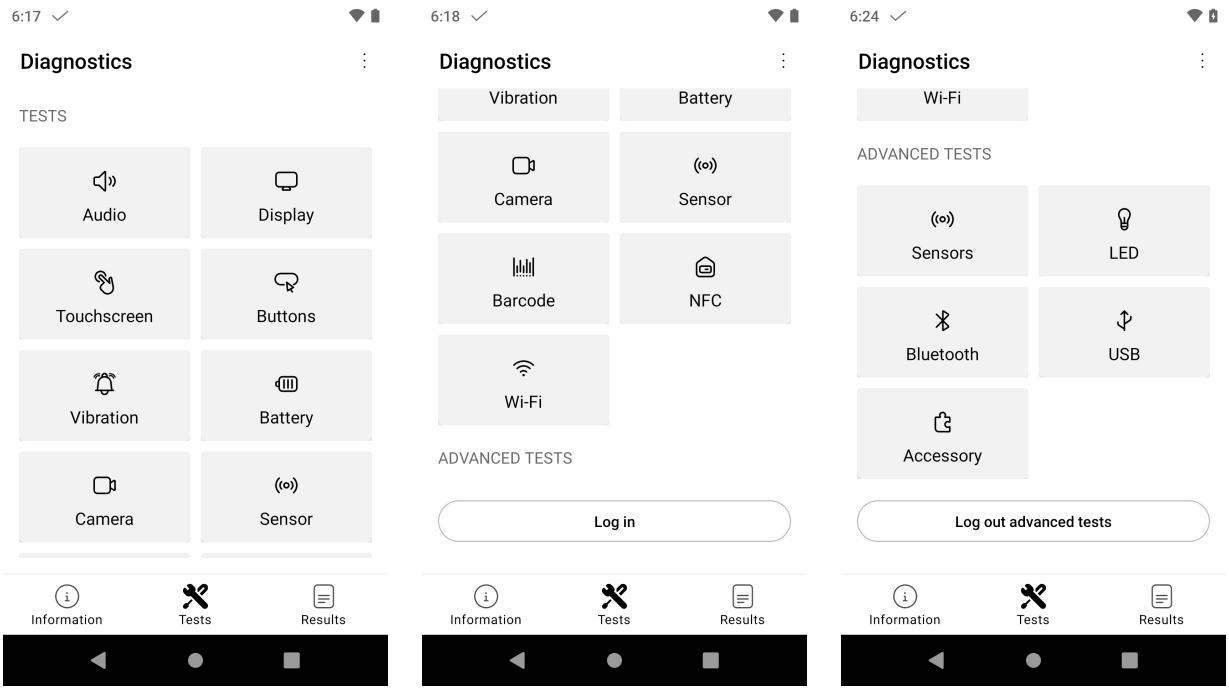
Note: With the 1.5(0) release, DHCP option 42 can now be utilized for NTP server configuration in case the default NTP server (2.android.pool.ntp.org) on the Internet is not accessible.

Diagnostics

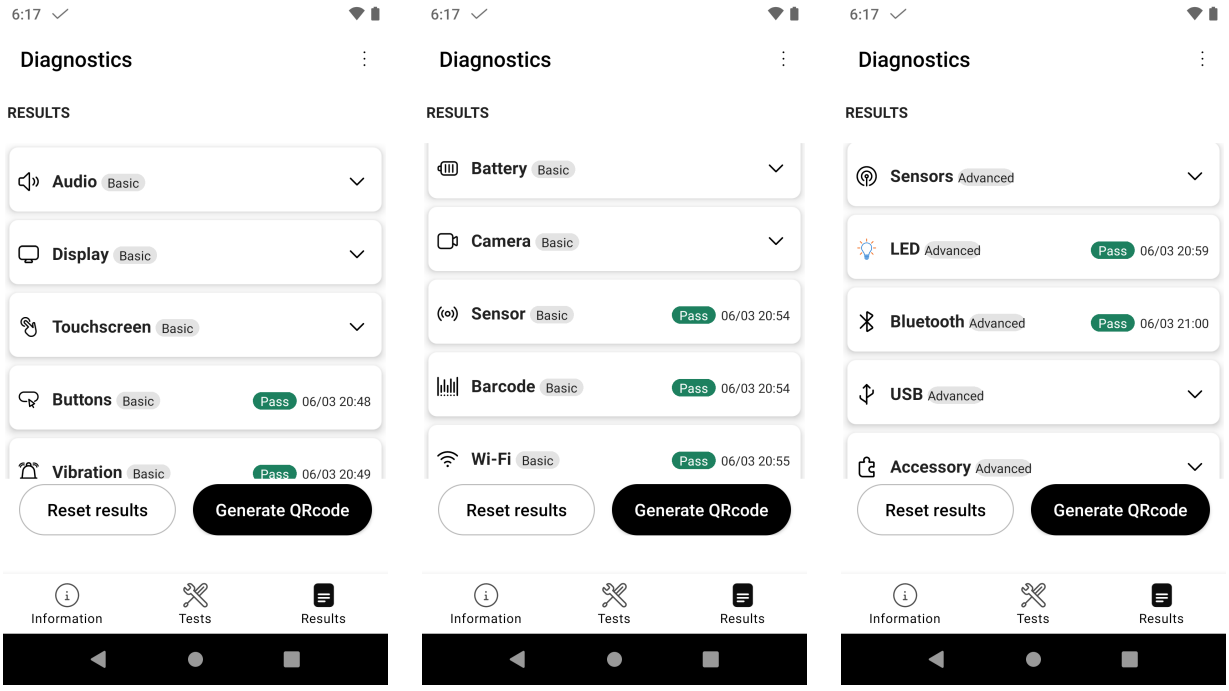
Hardware troubleshooting can be performed using the **Diagnostics** application.



To run select hardware troubleshooting, select the **Tests** tab, then select the desired hardware component.

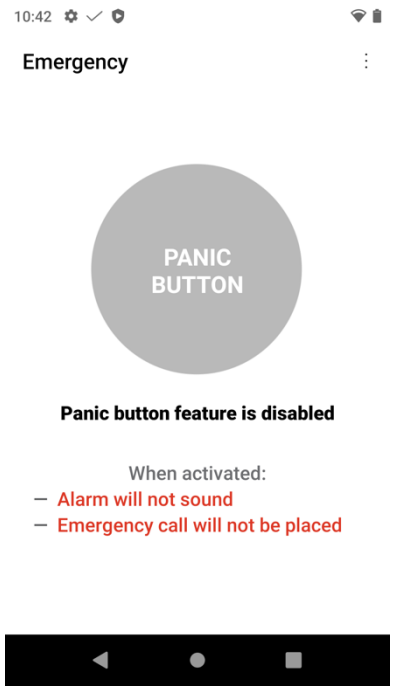


Once the test has completed, the results can be viewed by selecting the **Results** tab, then select the corresponding test item.

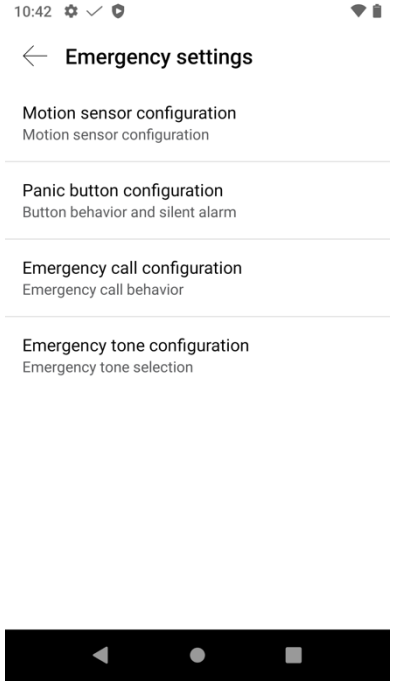


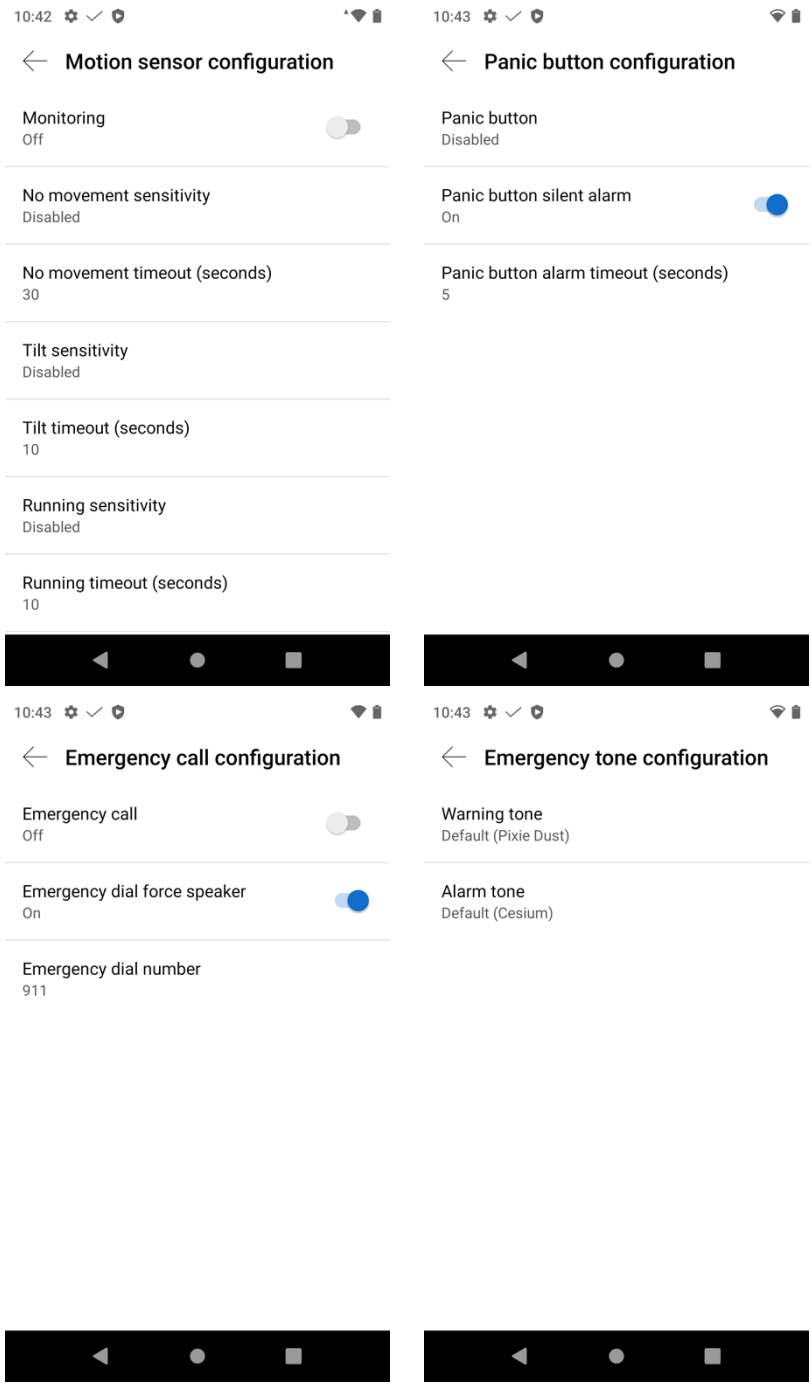
Emergency

Emergency settings including motion sensor, panic button, emergency call and tone configuration can be configured by selecting the three dots in the upper right hand corner while in the **Emergency** application, then selecting **Settings**.


10:42
Emergency
PANIC BUTTON
Panic button feature is disabled
When activated:
– Alarm will not sound
– Emergency call will not be placed

10:43
Emergency
PANIC BUTTON
Long press to trigger panic alarm
When activated:
– Alarm will not sound
– Emergency call will not be placed


10:42
Emergency settings
Motion sensor configuration
Motion sensor configuration
Panic button configuration
Button behavior and silent alarm
Emergency call configuration
Emergency call behavior
Emergency tone configuration
Emergency tone selection

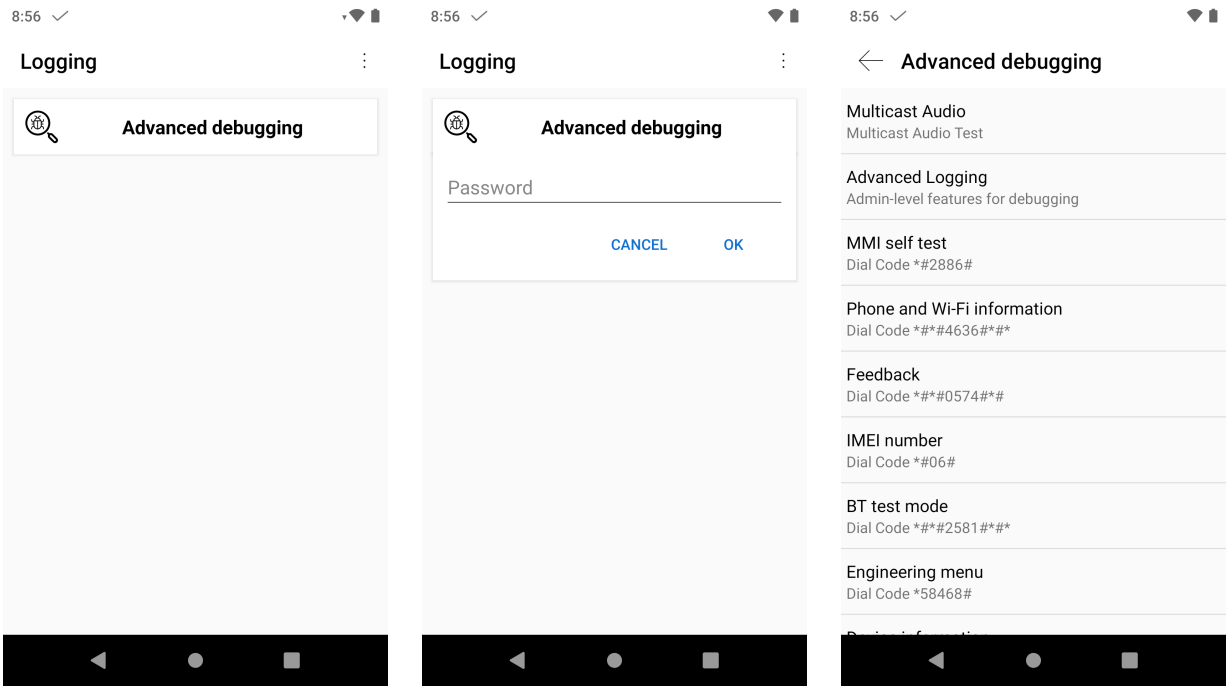


Note: The Emergency button (red button) is located on the top right of the Cisco Wireless Phone 840 and the Cisco Wireless Phone 860.

Logging

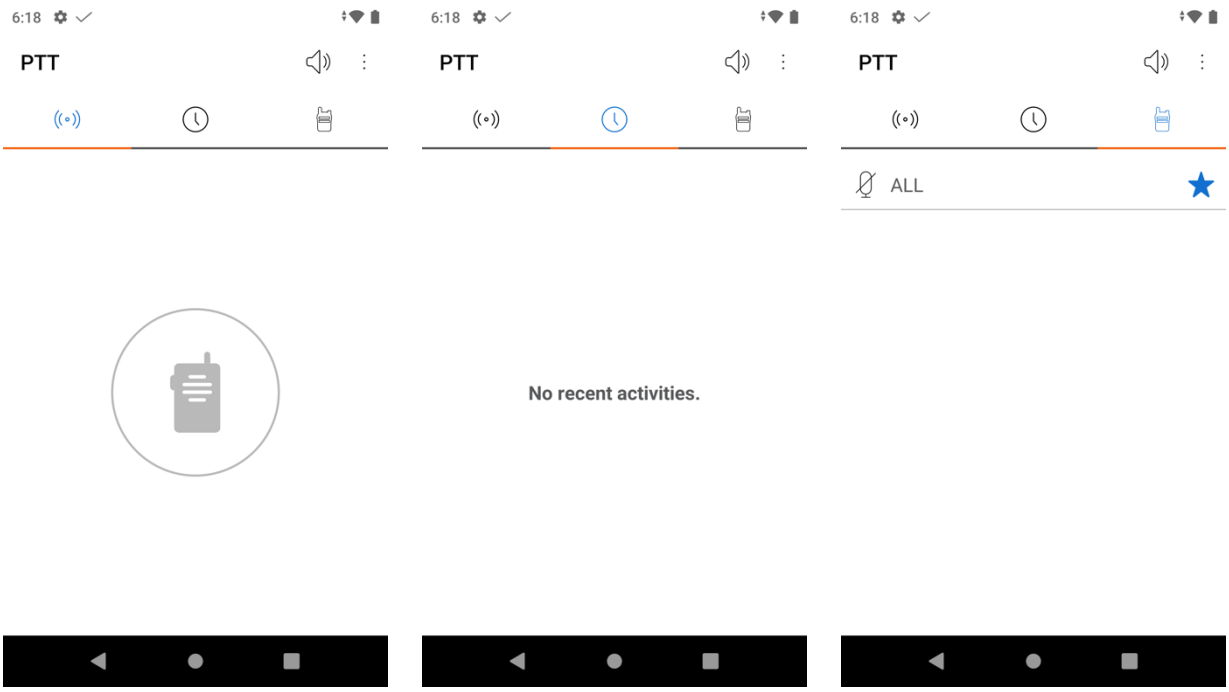
Various debug options are available in the **Logging** application.

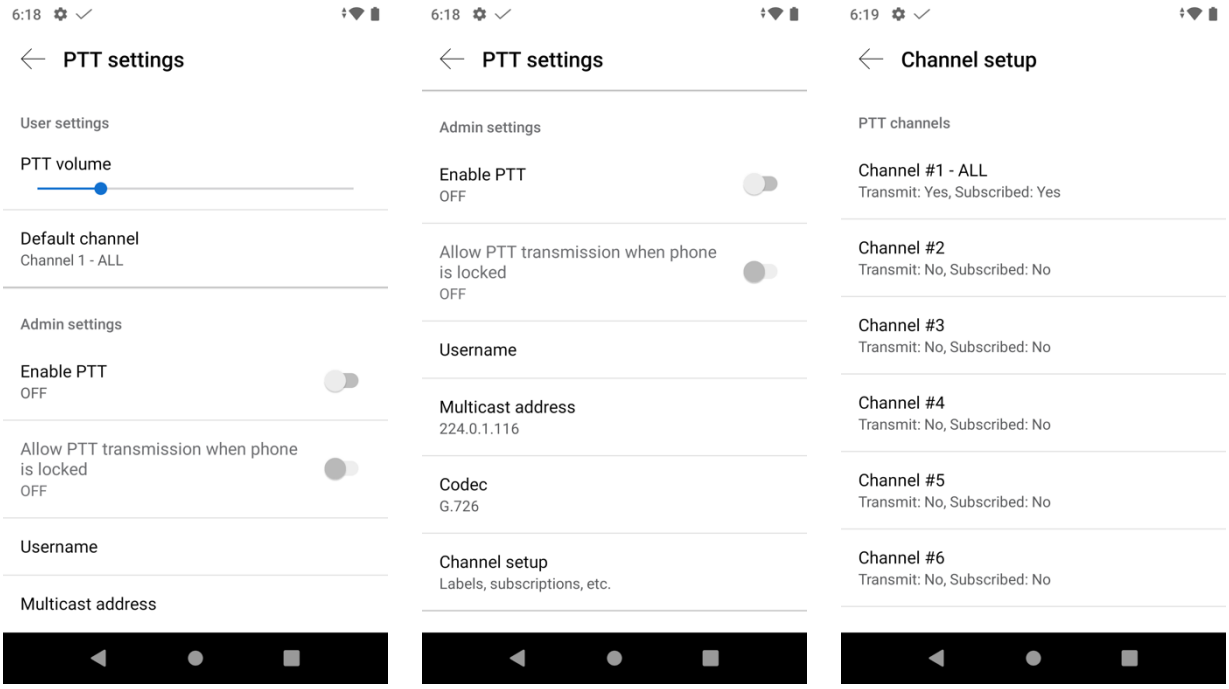
Enter the **Local Phone Unlock Password** when prompted (default = **#).



PTT

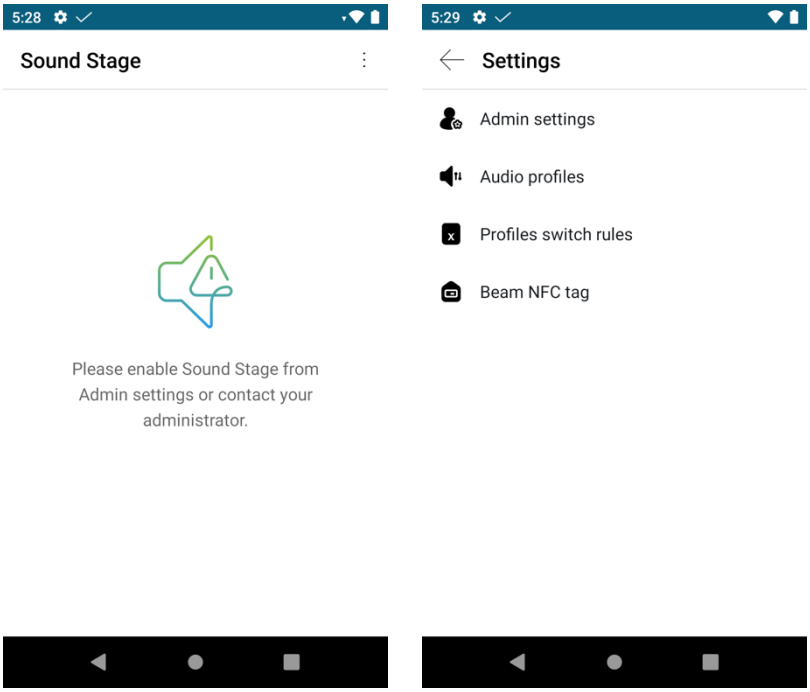
Push to Talk (PTT) settings can be configured by selecting the three dots in the upper right hand corner while in the **PTT** application, then selecting **Settings**.



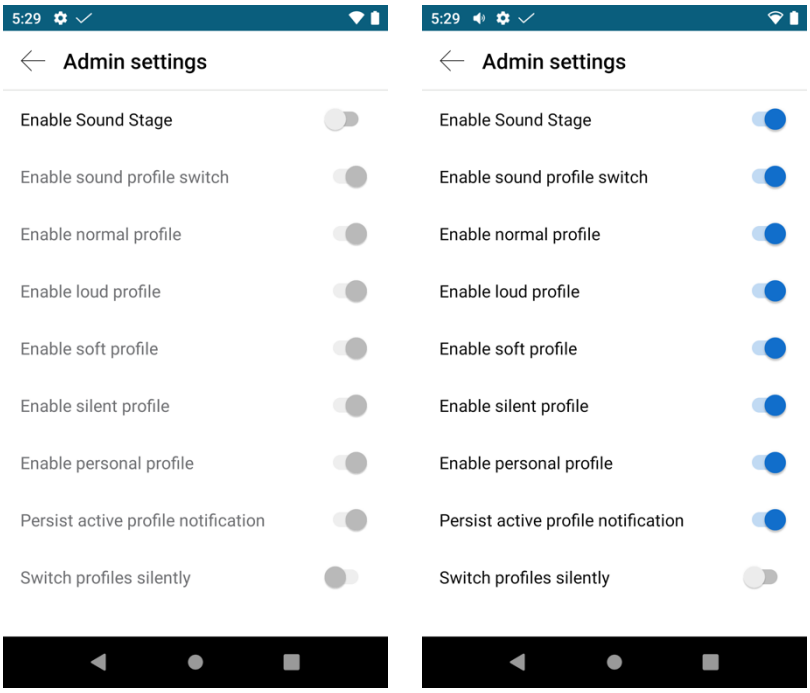


Sound Stage

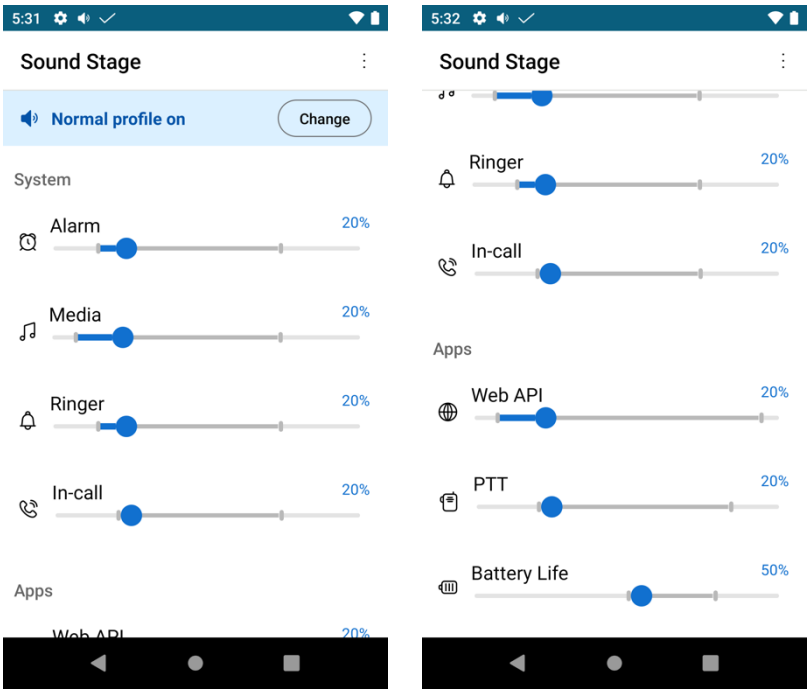
Sound Stage settings can be configured by selecting the three dots in the upper right hand corner while in the **Sound Stage** application, then selecting **Settings**.



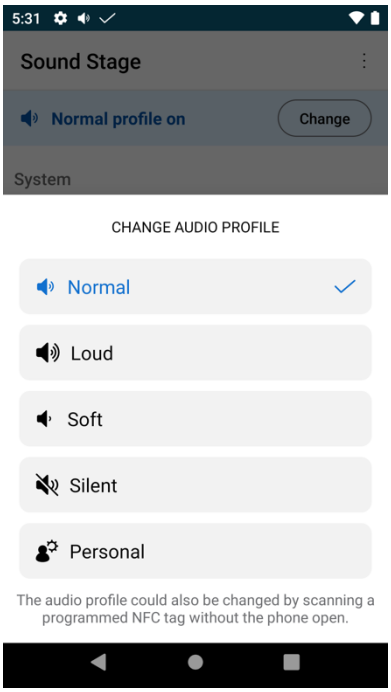
To enable Sound Stage, select **Admin settings** and ensure the slider for **Enable Sound Stage** is to the right.

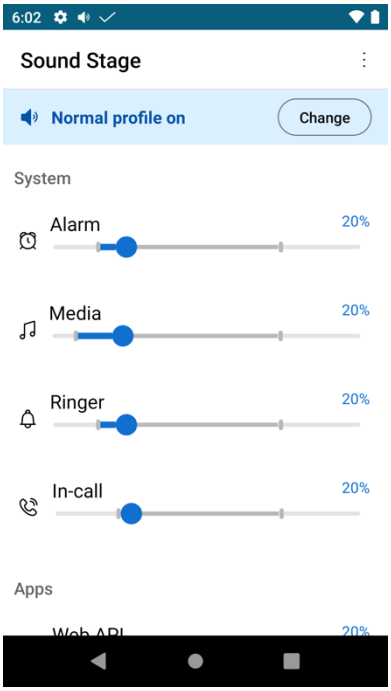


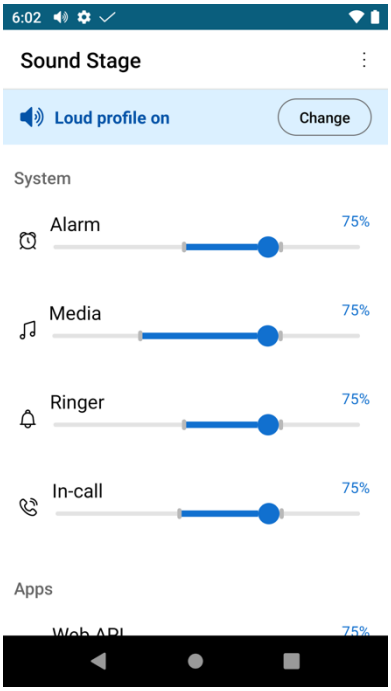
Once **Enable Sound Stage** is enabled, the **Normal profile** will be selected by default.

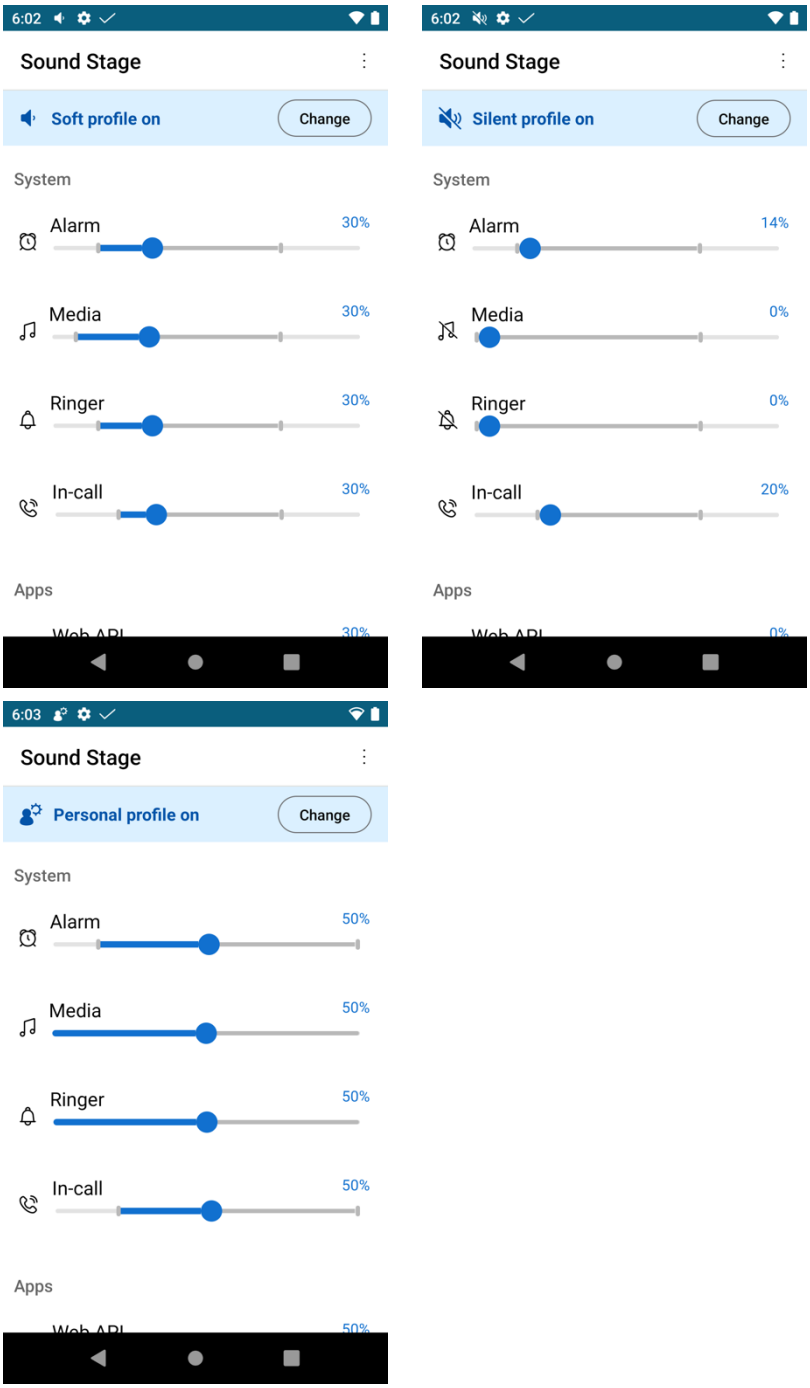


The current audio profile can be changed by selecting **Change** on the main **Sound Stage** screen.


5:31
Sound Stage
Normal profile on
Change
System
CHANGE AUDIO PROFILE
Normal
Loud
Soft
Silent
Personal
The audio profile could also be changed by scanning a programmed NFC tag without the phone open.

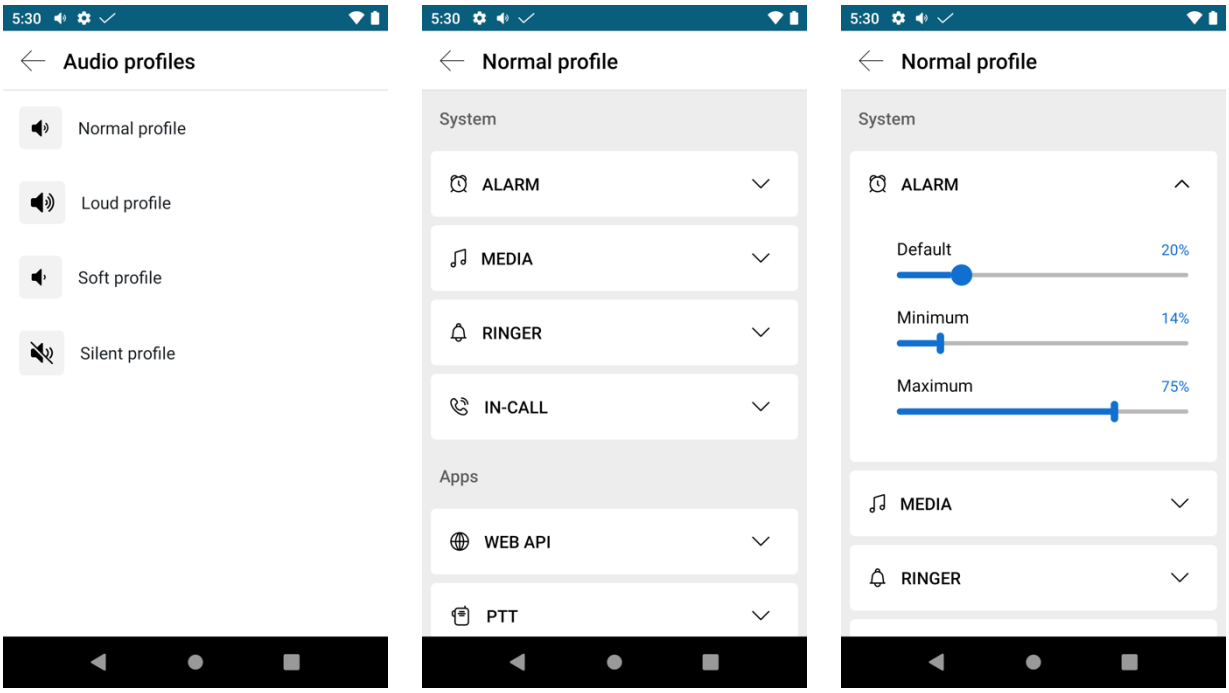

6:02
Sound Stage
Normal profile on
Change
System
Alarm
20%
Media
20%
Ringer
20%
In-call
20%
Apps
20%


6:02
Sound Stage
Loud profile on
Change
System
Alarm
75%
Media
75%
Ringer
75%
In-call
75%
Apps
75%

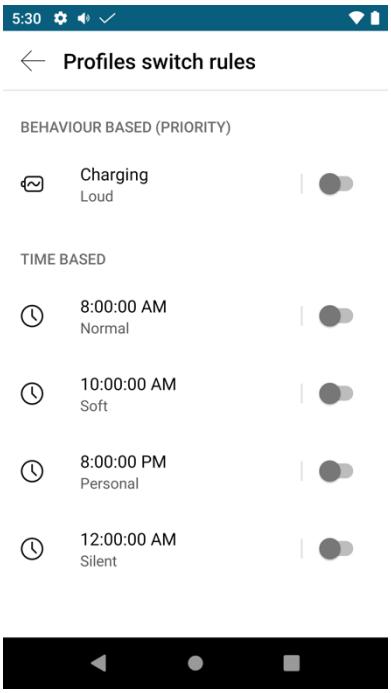


Audio profiles can be configured by selecting **Audio profiles**.

System and application default, minimum, and maximum volumes can be configured per audio profile.

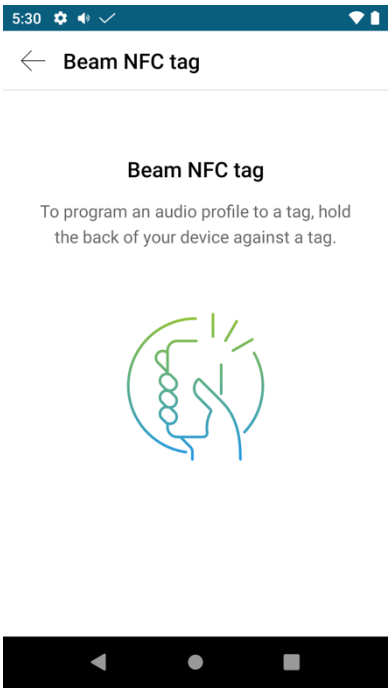


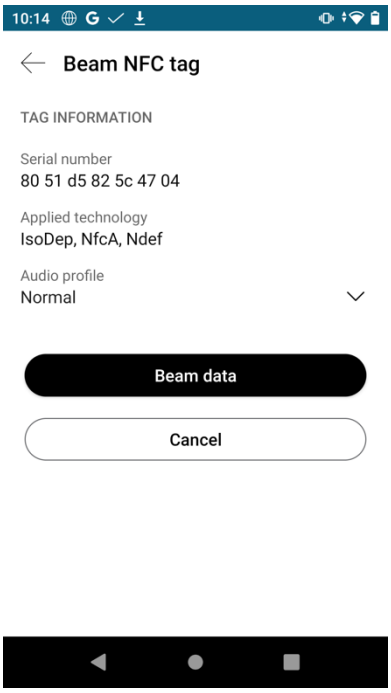
Profiles switch rules can be configured by selecting **Profiles switch rules**.

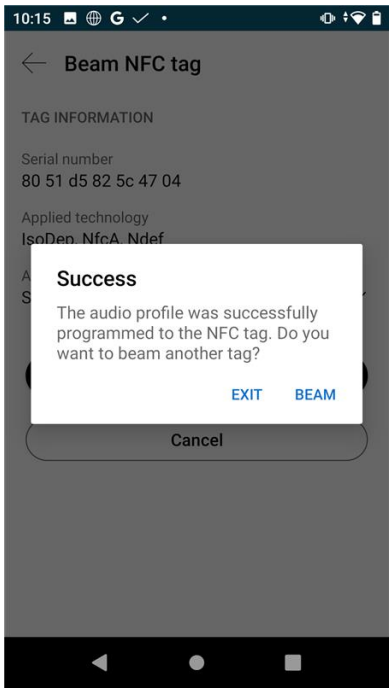


NFC tags can be programmed for a specific audio profile by selecting **Beam NFC tag**.

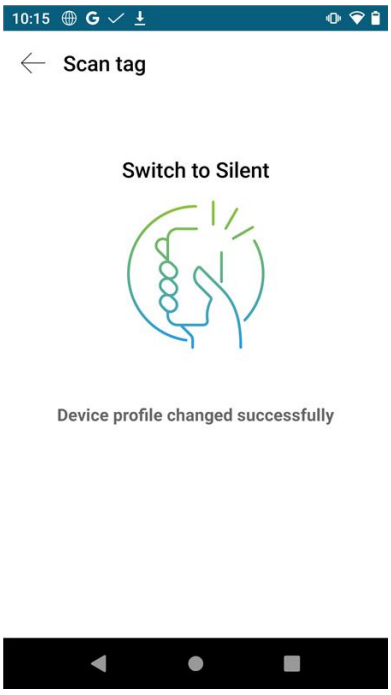
This can be helpful when a user moves from one environment to another either requiring lower or higher volumes.





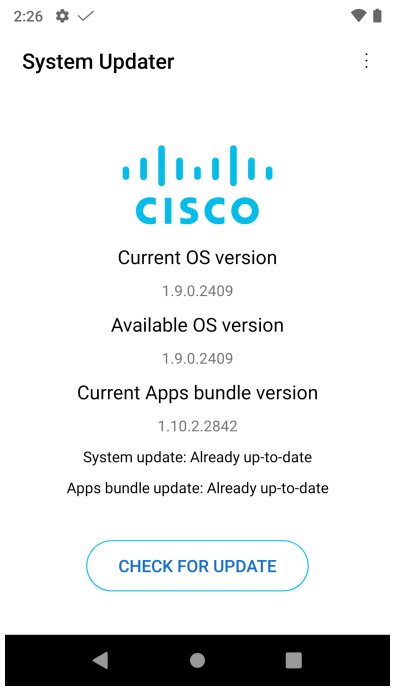


A confirmation screen will be displayed when an NFC tag has been scanned and the audio profile has been configured.



System Updater

The administrator will manage and push down firmware updates to the Cisco Wireless Phone 840 and 860. The user will then be prompted to confirm to reboot and apply the new firmware unless the **Reboot immediately after downloading software updates** option is enabled in the call server.

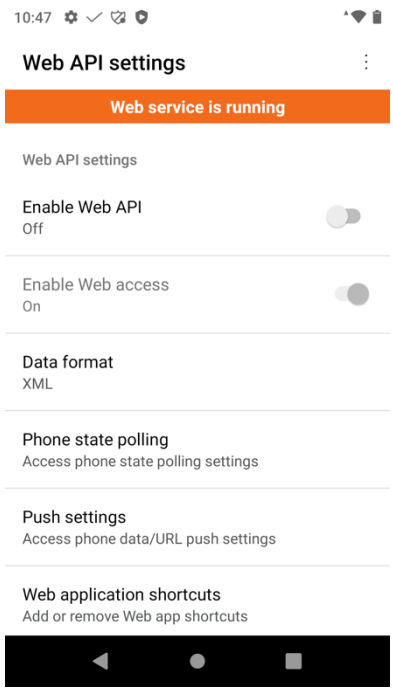


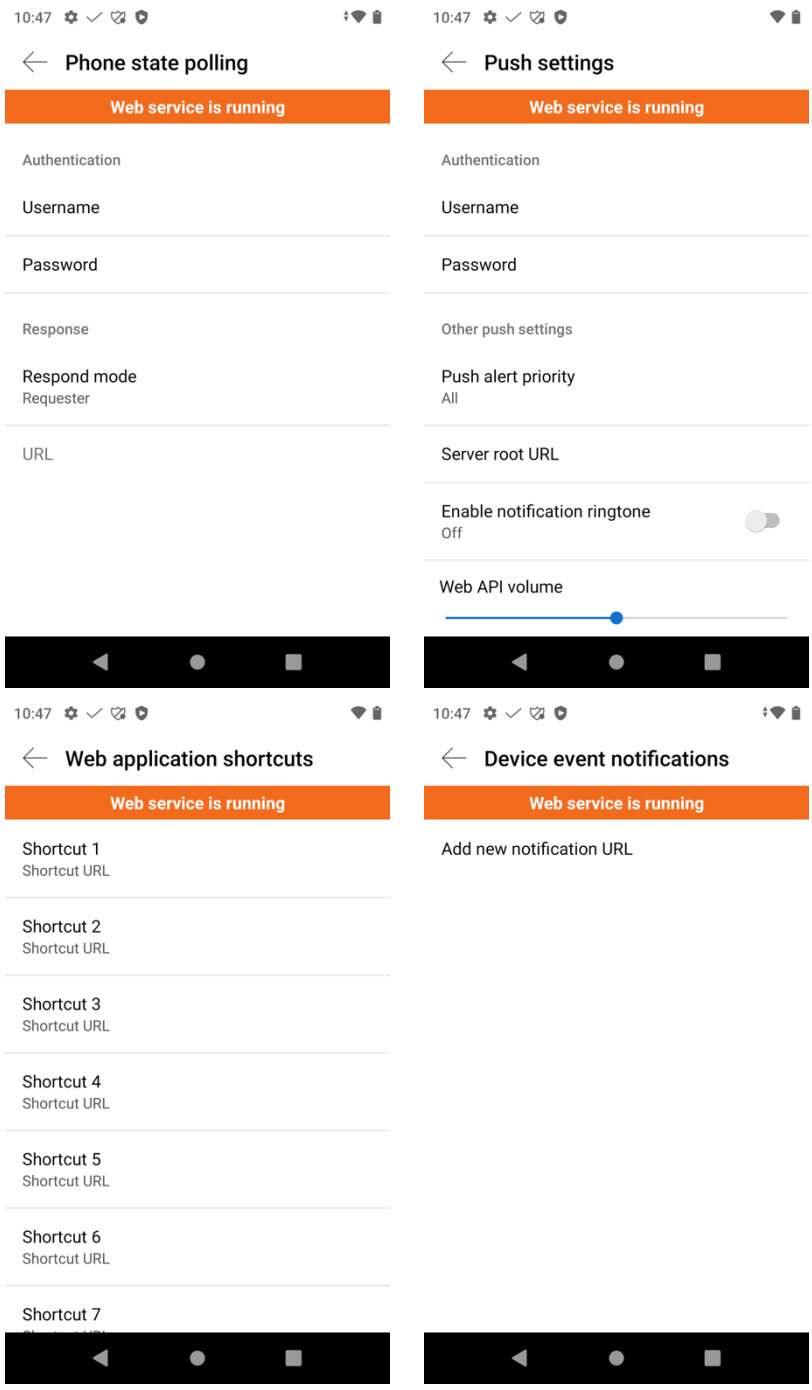
Note: With the 1.10.x releases, the OS version will show as 1.9.1.2908 for the Cisco Wireless Phone 840 and as 1.9.0.2409 for the Cisco Wireless Phone 860; however the Apps bundle version will show as 1.10.1.2284 for the Cisco Wireless Phone 840 and as 1.10.1.2697 for the Wireless Phone 860.

The System Updater application should not be used directly for firmware updates.

Web API

Web API settings can be custom configured in the **Web API** application.





Note: For more information, see the **Cisco Wireless Phone 800 Series Developer's Guide**.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

Application Store

Various types of applications are available for download from Google Play.

Google Play is an application market developed by Google™ for Android OS. The **Play Store** application allows users to browse and download applications published by third-party developers.

A Google account is necessary to download applications.

When first launching Google Play, you will be prompted to sign in with your credentials or register if you do not have an account already.

Google Play can also be accessed at this URL.

https://play.google.com/store

Note: Cisco does not endorse, support, or test third-party applications for the Cisco Wireless Phone 840 or 860.

IP Phone Services

The following document provides the information needed for application developers to create and deploy IP phone services for the Cisco Wireless Phone 840 and 860.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

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.

https://cisco.com/go/phonexsiguide

Application Server Ringtone Override

The Cisco Wireless Phone 840 or 860 can play a pre-installed or custom ringtone per external application server instruction to override the configured ringtone of an associated line.

If wanting to play a custom ringtone, ensure the ringtone is downloaded to the phone.

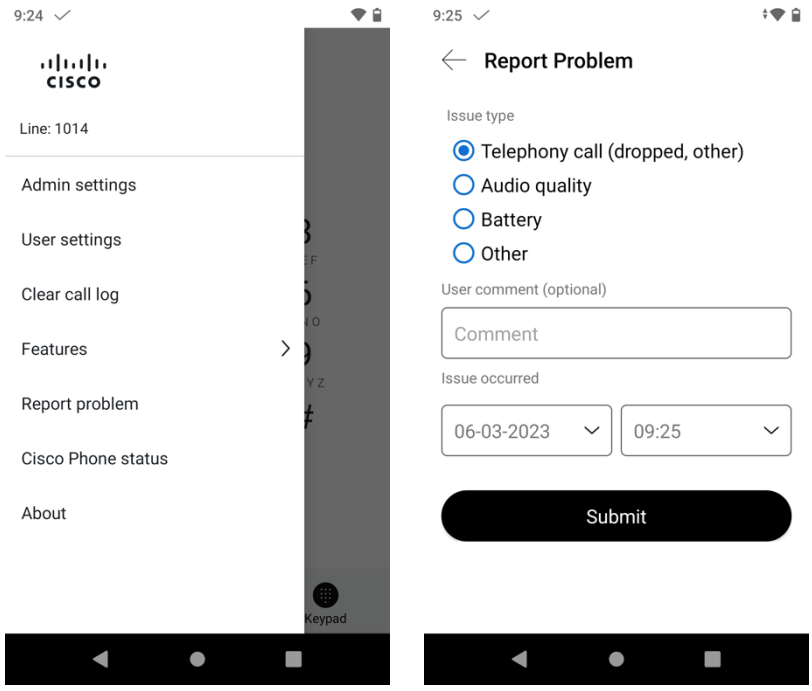
Once the ringtone has been downloaded to the Cisco Wireless Phone 840 or 860, configure the ringtone for the **Alert-Info** field of the **SIP Message Header** within the application server, which is case sensitive (e.g. **file://AlertTone.wav**).

Troubleshooting

Problem Report Tool

A problem report can be created by selecting the three lines in the upper left hand corner while in the **Cisco Phone** application, then selecting **Report problem**.

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



Configure a Customer Support Upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: "SEP001122334455")
- serialno (example: "FCH12345ABC")
- username (the username configured in Cisco Unified Communications Manager, the device owner)
- prt_file (example: "probrep-20141021-162840.tar.gz")

Sample Script

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
```

```
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Phone Webpages

Cisco Wireless Phone 840 and 860 information can be gathered remotely by accessing the phone's webpage interfaces.

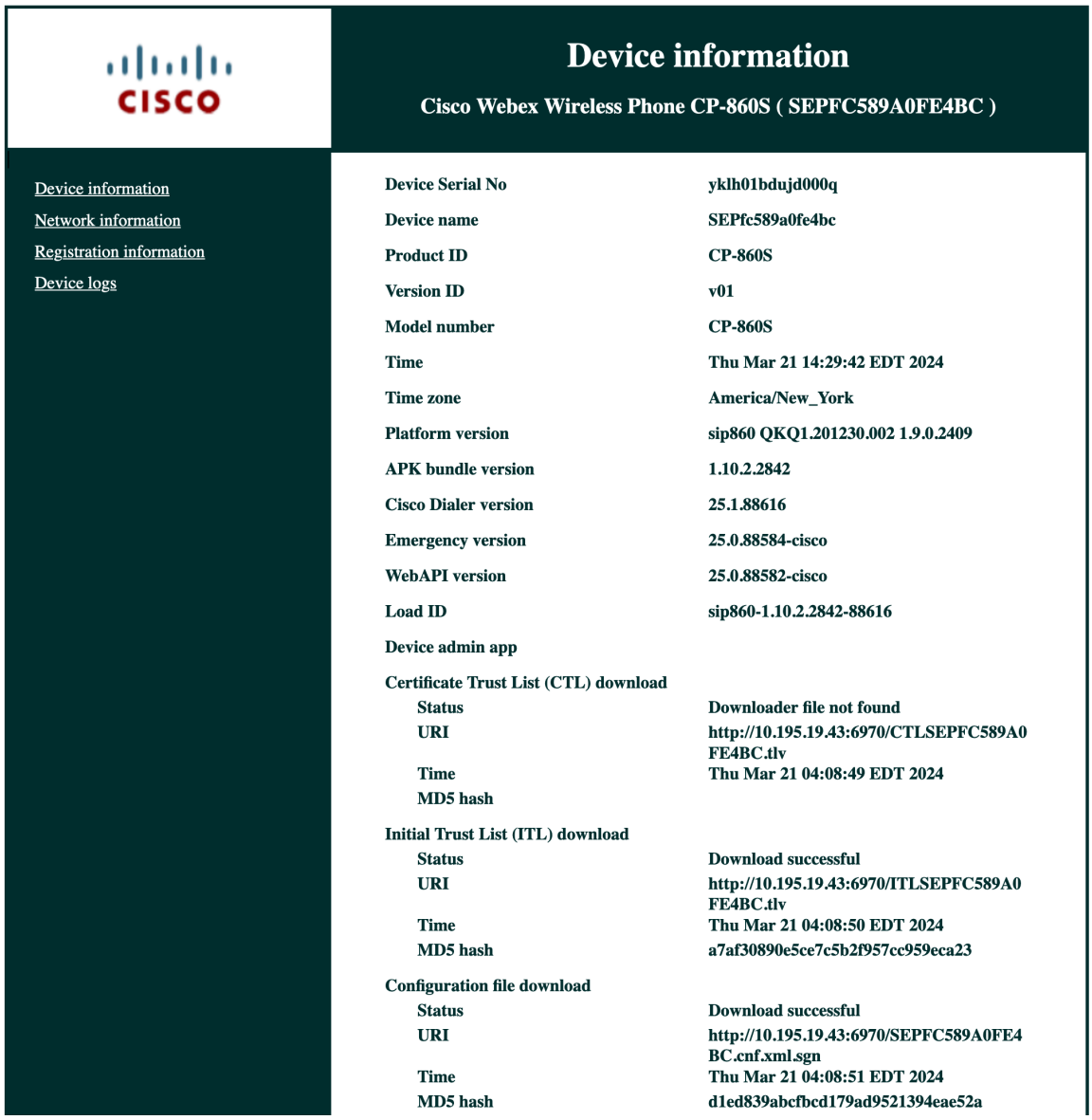
The webpage interface (https://x.x.x.x) contains read-only information regarding device information, network information, registration information, and device logs. To access the webpage interface, **Web Access** must be enabled in the call server.

Device Information

The Cisco Wireless Phone 840 and 860 provide device information, where MAC address and version information is displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco Wireless Phone 840 or 860 then select **Device information** to view this information.

Cisco Unified Communications Manager



Device information

Cisco Webex Wireless Phone CP-860S (SEPFC589A0FE4BC)

Device information
Network information
Registration information
Device logs

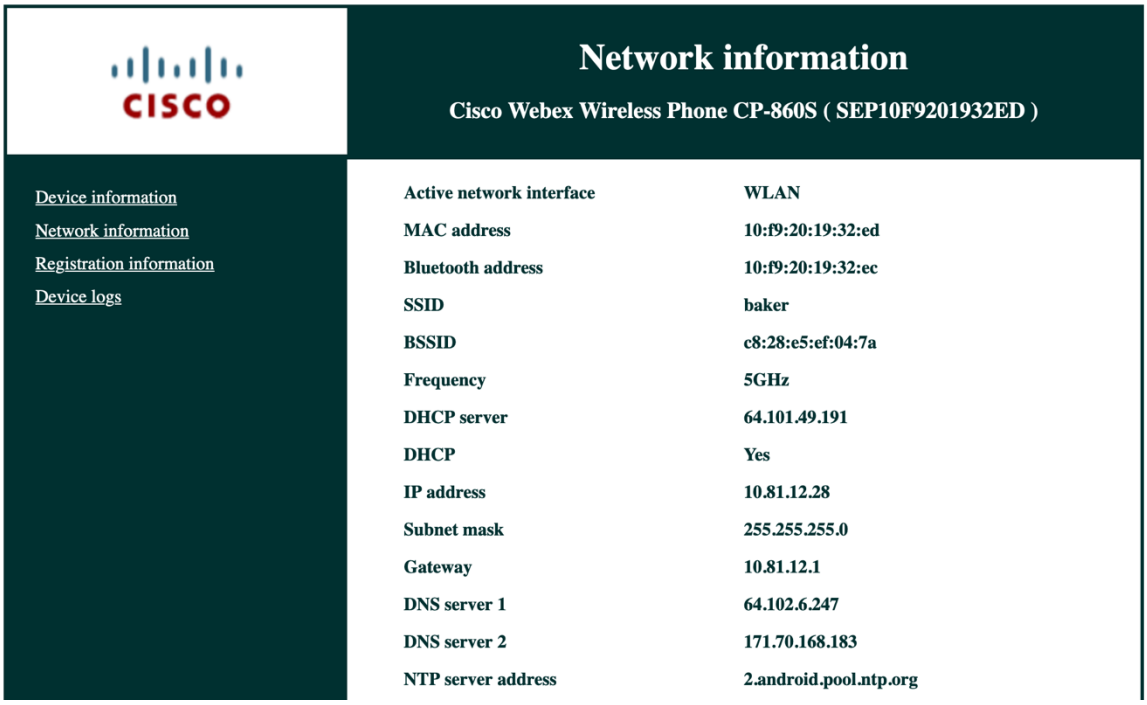
Device Serial No	yklh01bdujd000q
Device name	SEPfc589a0fe4bc
Product ID	CP-860S
Version ID	v01
Model number	CP-860S
Time	Thu Mar 21 14:29:42 EDT 2024
Time zone	America/New_York
Platform version	sip860 QKQ1.201230.002 1.9.0.2409
APK bundle version	1.10.2.2842
Cisco Dialer version	25.1.88616
Emergency version	25.0.88584-cisco
WebAPI version	25.0.88582-cisco
Load ID	sip860-1.10.2.2842-88616
Device admin app	
Certificate Trust List (CTL) download	
Status	Downloader file not found
URI	http://10.195.19.43:6970/CTLSEPFC589A0FE4BC.tlv
Time	Thu Mar 21 04:08:49 EDT 2024
MD5 hash	
Initial Trust List (ITL) download	
Status	Download successful
URI	http://10.195.19.43:6970/ITLSEPFC589A0FE4BC.tlv
Time	Thu Mar 21 04:08:50 EDT 2024
MD5 hash	a7af30890e5ce7c5b2f957cc959eca23
Configuration file download	
Status	Download successful
URI	http://10.195.19.43:6970/SEPFC589A0FE4BC.cnf.xml.sgn
Time	Thu Mar 21 04:08:51 EDT 2024
MD5 hash	d1ed839abcfbcd179ad9521394eae52a

Webex Calling

Network Information

The Cisco Wireless Phone 840 and 860 provide network information, where wireless LAN and network information is displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco Wireless Phone 840 or 860 then select **Network information** to view this information.



Registration Information

The Cisco Wireless Phone 840 and 860 provide registration information, where phone DN and registration status information is displayed.

Browse to the web interface (https://x.x.x.x) of the Cisco Wireless Phone 840 or 860 then select **Registration information** to view this information.

Cisco Unified Communications Manager

Device information
Network information
Registration information
Device logs

Registration information

Cisco Webex Wireless Phone CP-860S (SEP10F9201932ED)

UCM

Phone DN	Shared Line	Auto Answer	Call Forward	Forwarded Address	Status
1014	True	Disabled	Disabled		Not Registered

CANDIDATE SERVERS

Priority	IP Address	Status	Detail
P1:1	10.195.19.43	up	Current server

SECONDARY REGISTRATION

Phone DN	
SIP Server	
Server Port	
Protocol	
SIP Code	
Status	

SECONDARY CANDIDATE SERVERS

Priority	IP Address	Status	Detail

CALL SERVER FEATURES

Hunt Group	Enabled
Hunt Group Status	Logged out
Visual Voicemail	Enabled
Privacy	Enabled

DEVICE SETTINGS

DND	Disabled

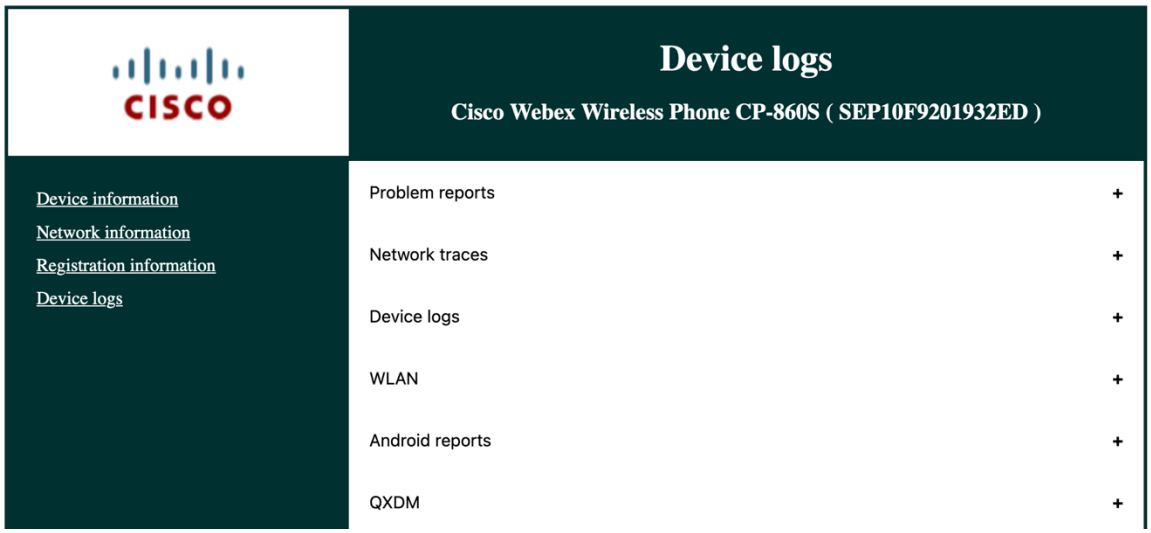
Restart Phone Application

Webex Calling

Device Logs

Device logs can be obtained from the web interface of Cisco Wireless Phone 840 or 860 for troubleshooting purposes.

Browse to the web interface (https://x.x.x.x) of the Cisco Wireless Phone 840 or 860 then select **Device logs** to view this information.



Click the + sign to the right of the log file type (**Problem reports**, **Network Traces**, **Device logs**, **WLAN**, **Android reports**, **QXDM**) to list those log files, which can then be downloaded.

With the 1.6(0) release, a problem report and a network trace can be captured via the Cisco Wireless Phone 840 and 860.

To generate a problem report, select **Generate PRT** under **Problem reports**.

To capture a network trace, select **Start Packet Capture** under **Network traces**. Select **Stop Packet Capture** to stop the packet capture.

WLAN Signal Indicator

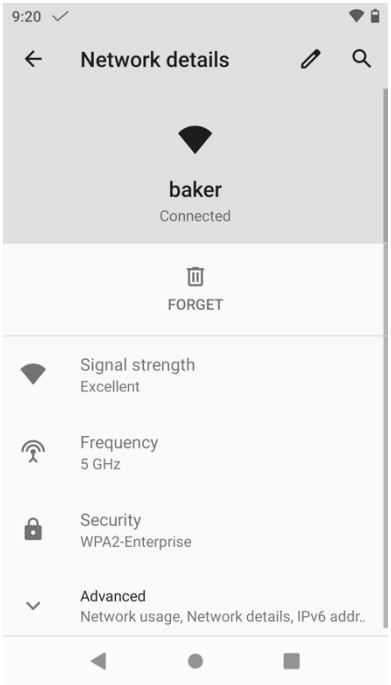
The WLAN signal indicator for the Cisco Wireless Phone 840 and 860 is displayed in the upper right hand corner of the display.

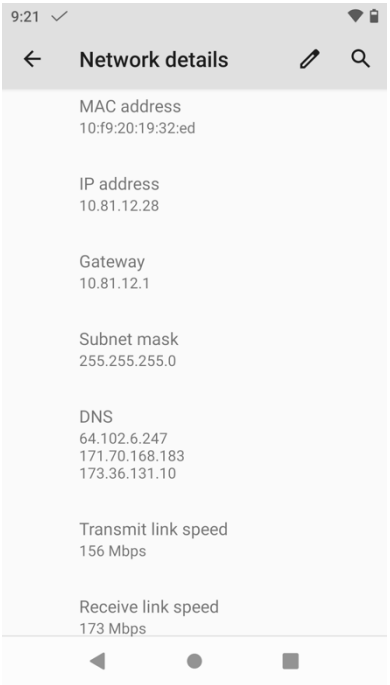
When the Cisco Wireless Phone 840 and 860 is connected to an access point, the icon will be grey in color as shown below.

WLAN Network Information

The current WLAN network information for the Cisco Wireless Phone 840 and 860 can be viewed by selecting **Settings > Network & internet > Wi-Fi**, then selecting the connected Wi-Fi network.

A configured Wi-Fi network can be removed by selecting **Forget**.





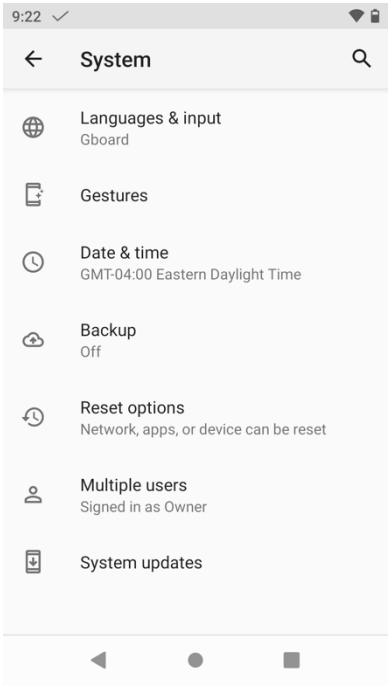
Restoring Factory Defaults

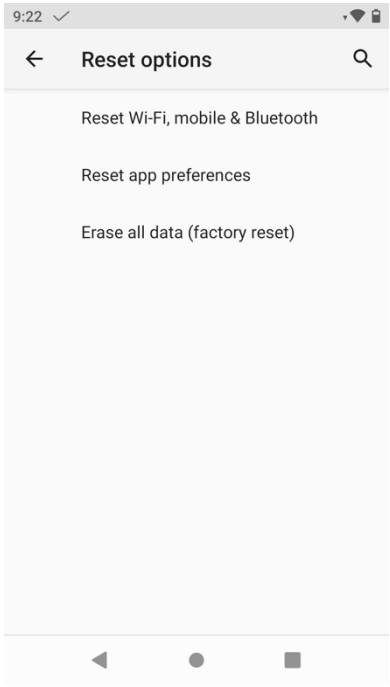
The configuration of the Cisco Wireless Phone 840 and 860 can be reset to factory defaults by selecting **Settings > System > Advanced > Reset options** > **Erase all data (factory reset)**.

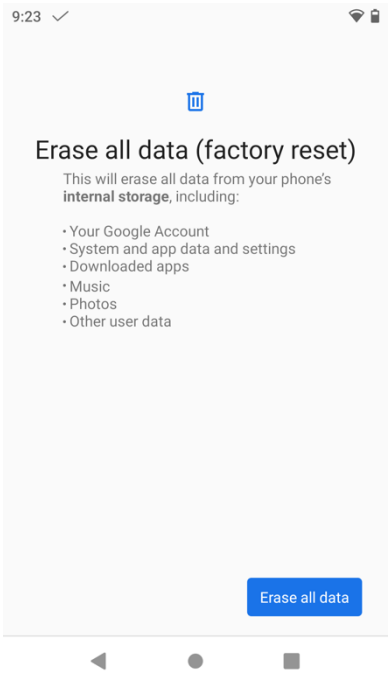
An informational screen will be displayed indicating all of the data that will be erased, where **Erase all data** must be selected to continue with the factory reset.

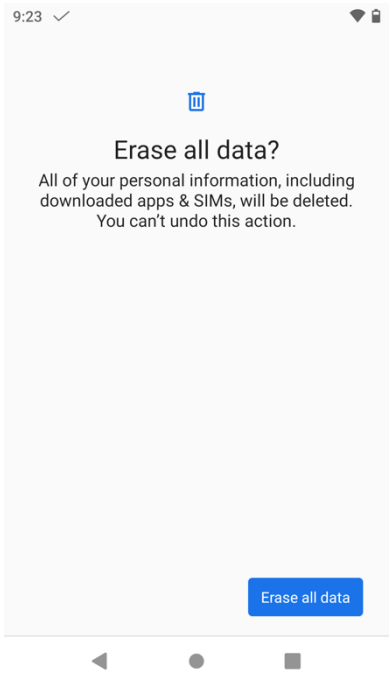
Then a confirmation screen will be displayed, where **Erase all data** must be selected to proceed with the factory data reset.

The phone will then restart and boot with factory settings restored.









If the Cisco Wireless Phone 840 or 860 is not able to boot properly, a factory reset can also be initiated via the following procedure:

- Power the phone off by pressing the **Power** button (button on the top left for the Cisco Wireless Phone 840 and second button from the top on the right side for the Cisco Wireless Phone 860), then select **Power off**.
- Press and hold the **Emergency** button (red button located on the top right of the Cisco Wireless Phone 840 and the Cisco Wireless Phone 860), then power the phone on.
- Keep the **Power** button pressed until the phone vibrates, then release the **Power** button, while continuing to keep the **Emergency** button pressed.
- Once the bootloader screen is displayed, release the **Emergency** button.
- Press the **Volume Down** button until **Recovery mode** is displayed, then press the **Power** button to select that option.
- The phone will restart and return to a new screen that displays the Android icon.
- From this screen, press and hold the **Power** button, then quickly press and release the **Volume Up** button to enter the **Recovery Menu** screen.
- Release the **Power** button once the **Recovery Menu** is displayed.
- Press the **Volume Down** button to highlight **Wipe data/factory reset**, then press the **Power** button to select that option.
- Press the **Volume Down** button to highlight **Factory data reset**, then press the **Power** button to select that option.
- Press the **Power** button again when **Reboot system now** is highlighted.
- The Cisco Wireless Phone 840 or 860 will then restart and have the factory settings restored.

Note: If a Cisco Wireless Phone 840 or 860 is signed into a Google account, then the phone will have factory wipe protection enabled, which remains enabled until the configured Google account is removed.

Factory wipe protection can not be bypassed ever after restoring the default configuration when using the boot factory reset method, as the Google account credentials must be entered as part of the boot factory reset process to fully restore the phone to factory defaults.

Therefore, the Cisco Wireless Phone 840 or 860 should be factory reset via the phone's Android user interface to successfully remove any configured Google accounts.

If then there is a Google account configured in which the credentials are not known and unable to access the phone's Android user interface to factory reset the phone, then the phone is not recoverable and can not be replaced under warranty.

Capturing a Screenshot of the Phone Display

The current display of the Cisco Wireless Phone 840 or 860 can be captured by pressing the power button, then selecting **Screenshot**.

Additional Documentation

Cisco Wireless Phone 840 and 860 Data Sheet

https://www.cisco.com/c/en/us/products/se/2020/11/Collateral/datasheet-c78-744461.html

Cisco Wireless Phone 840 and 860 Administration Guide

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/adminguide/w800_b_wireless-800-administration-guide.html

Cisco Wireless Phone 840 and 860 User Guide

https://www.cisco.com/content/en/us/td/docs/voice_ip_comm/cuipph/800-series/userguide/w800_b_wireless-800-user-guide.html

Cisco Wireless Phone 840 and 860 Quick Reference Guides

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/800-series/qrg/webex_wireless_phone_840_qrg.pdf

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/800-series/qrg/webex_wireless_phone_860_qrg.pdf

Cisco Wireless Phone 840 and 860 Release Notes

https://www.cisco.com/c/en/us/support/collaboration-endpoints/webex-wireless-phone/products-release-notes-list.html

Cisco Wireless Phone 840 and 860 Software

https://software.cisco.com/download/home/286327931

Cisco Unified Communications Manager

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/series.html

Webex Calling

https://help.webex.com

Cisco Voice Software

https://software.cisco.com/download/home/278875240

Cisco Wireless Phone 800 Series Developer's Guide

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/800-series/developersguide/w800_b_wireless-800-developers-guide.html

Cisco IP Phone Services Application Development Notes

https://cisco.com/go/phonexsiguide

Real-Time Traffic over Wireless LAN Design Guide

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

Cisco Wireless Phone 840 and 860 Deployment Guide

Cisco Unified Communications Design Guides

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html

Cisco AireOS Wireless LAN Controller Documentation

https://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html

Cisco Catalyst IOS XE Wireless LAN Controller Documentation

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html

Cisco Mobility Express Documentation

https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-installation-and-configuration-guides-list.html

Cisco Autonomous Access Point Documentation

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/atnms-ap-8x/configuration/guide/cg-book.html

Cisco Meraki Wireless LAN Documentation

https://documentation.meraki.com

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Webex, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, Webex, and the Webex logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

The Bluetooth word mark and logo are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Cisco Systems, Inc., is under license.

© 2024 Cisco Systems, All rights reserved.