Cisco Wireless IP Phone 8821 and 8821-EX Deployment Guide

The Cisco Wireless IP Phone 8821 and 8821-EX are adaptable for all mobile professionals, from users on the move within an office environment to nurses and doctors in a healthcare environment to associates working in the warehouse, on the sales floor, or in a call center. Staff, nurses, doctors, educators, and IT personnel can be easily reached when mobile. The Cisco Wireless IP Phone 8821 is IP54 rated, which is designed to provide protection from dust, liquid splashes, and moisture, where the Cisco Wireless IP Phone 8821-EX is IP67 rated for increased dust and water protection.

This guide provides information and guidance to help the network administrator deploy the Cisco Wireless IP Phone 8821 and 8821-EX in a wireless LAN environment.

Revision History

Date	Comments
08/24/16	11.0(2) Release
10/08/16	11.0(2)SR2 Release
02/07/17	11.0(3) Release
05/04/17	11.0(3)SR2 Release
08/01/17	11.0(3)SR3 Release
10/18/17	11.0(3)SR4 Release
04/02/18	11.0(3)SR6 Release
06/13/18	11.0(4) Release
09/05/18	11.0(4)SR1 Release
12/16/19	11.0(4)SR3 Release
01/24/20	11.0(5)SR1 Release
03/11/20	11.0(5)SR2 Release
09/11/20	11.0(5)SR3 Release
11/09/20	11.0(6) Release
04/07/21	11.0(6)SR1 Release
01/20/22	11.0(6)SR2 Release
02/27/24	11.0(6)SR5 Release

Contents

Cisco Wireless IP Phone 8821 and 8821-EX Overview **6**

Phone Models *6*

Requirements *6*
Site Survey 7
Call Control 8
Wireless LAN 8

Protocols *16*

Wi-Fi *17*
Regulatory 19

Bluetooth *20*

Languages *21*

8821-EX Certifications *22*

Battery Life *22*

Phone Care *24*

Accessories *25*

Wireless LAN Design **27**

802.11 Network *27*
5 GHz (802.11a/n/ac) 27
2.4 GHz (802.11b/g/n) 28
Signal Strength and Coverage 29
Data Rates 32
Rugged Environments 33

Security *35*
Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST) 36
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) 37
Protected Extensible Authentication Protocol (PEAP) 37

Quality of Service (QoS) *37*
Call Admission Control (CAC) 38
Traffic Classification (TCLAS) 38
QoS Basic Service Set (QBSS) 39
Wired QoS 39

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

Power Management *43*

Call Capacity *44*

Multicast *44*

Configuring the Cisco Wireless LAN **45**

Cisco AireOS Wireless LAN Controller and Lightweight Access Points *45*
802.11 Network Settings 46
WLAN Settings 56
Controller Settings 65
Call Admission Control (CAC) 67
RF Profiles 70
FlexConnect Groups 72

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....108
Mobility Settings....108
Call Admission Control (CAC)....109
Multicast....110
Advanced Settings....113
Sample Configuration....115

Cisco Mobility Express and Lightweight Access Points....*122*
Controller Settings....123
802.11 Network Settings....124
WLAN Settings....127
RF Profiles....135
Multicast Direct....137

Cisco Autonomous Access Points....*138*
802.11 Network Settings....138
WLAN Settings....142
Call Admission Control (CAC)....152
QoS Policies....153
Power Management....156
Sample Configuration....157

Cisco Meraki Access Points....*162*
Creating the Wireless Network....162
SSID Configuration....165
Radio Settings....169
Firewall and Traffic Shaping....171

Configuring Cisco Call Control....173

Cisco Unified Communications Manager....*173*
Device Enablement....173
Device Pools....173
Phone Button Templates....174
Security Profiles....175
SIP Profiles....176
Common Settings....179
QoS Parameters....179
G.722 and iSAC Advertisement....180
Audio Bit Rates....180
Wireless LAN Profiles....181

Cisco Unified Communications Manager Express....*189*
Sample Configuration....189

Product Specific Configuration Options....*193*

Configuring the Cisco Wireless IP Phone 8821 and 8821-EX....204

Wi-Fi Profile Configuration....*204*
Automatic Provisioning....204
Local User Interface....205
Admin Webpage....213
Bulk Deployment Utility....216

Certificate Management....*223*
Manual Installation....223

Simple Certificate Enrollment Protocol (SCEP) 226
Certificate Removal 258
Bluetooth Settings *259*
Local Contacts *261*
Battery Status *266*
Upgrading Firmware *266*
IP Phone Services 268
Troubleshooting 269
Problem Report Tool *269*
Phone Webpages *271*
Device Information 271
Network Setup 272
Streaming Statistics 273
Device Logs 274
WLAN Signal Indicator *279*
Neighbor List *279*
WLAN Statistics *280*
Call Statistics *280*
Status Messages *281*
Diagnostics *281*
Restoring Factory Defaults *283*
Capturing a Screenshot of the Phone Display *284*
Additional Documentation 285

Cisco Wireless IP Phone 8821 and 8821-EX Overview

The Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX, 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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-8821-K9=	Cisco Wireless IP Phone 8821	2.4 GHz = 2.4 dBi 5 GHz = 3.0 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-8821-EX-K9=	Cisco Wireless IP Phone 8821-EX				

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

802.11j (channels 34, 38, 42, 46) are not supported.

Channel 14 for Japan is not supported.

Requirements

The Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX.

Site Survey

Before deploying the Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX.

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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX can hold a signal for at least 5 seconds.

Channel Utilization

Channel Utilization levels should be kept under 40%.

The Cisco Wireless IP Phone 8821 and 8821-EX convert the 0-255 scale value to a percentage, so 105 would equate to around 40% in the Cisco Wireless IP Phone 8821 and 8821-EX.

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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX are supported on the following call control platforms.

- Cisco Unified Communications Manager (CUCM)
  - Minimum = 9.1(2)
  - Recommended = 11.5(1), 12.0(1), 12.5(1), 14.0(1) and later
- Cisco Unified Communications Manager Express (CUCME)
  - Minimum = 10.5
  - Recommended = 11.7 and later
- Cisco Unified Survivable Remote Site Telephony (SRST)
  - Minimum = 10.5
  - Recommended = 11.7 and later

Note: Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable Cisco Wireless IP Phone 8821 and 8821-EX device support.

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

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

With release 10.5 of Cisco Unified Communications Manager Express, the Cisco Wireless IP Phone 8821 and 8821-EX are to utilize the fast track method utilizing the Cisco Unified IP Phone 9971 as the reference model (use 7975 as reference model if needing softkey template support).

With release 11.0 and 11.5 of Cisco Unified Communications Manager Express, the Cisco Wireless IP Phone 8821 and 8821-EX can utilize the Cisco IP Phone 8861 as the reference model.

With release 11.7 and later of Cisco Unified Communications Manager Express, there is native support for the Cisco Wireless IP Phone 8821 and 8821-EX, therefore can use the Cisco IP Phone 8821 as the model type.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/feature/phone_feature/phone_feature_support_guide.html#_Toc436645184

Wireless LAN

The Cisco Wireless IP Phone 8821 and 8821-EX are supported on the following Cisco Wireless LAN solutions.

- Cisco AireOS Wireless LAN Controller and Cisco Lightweight Access Points
  - Minimum = 8.0.121.0
  - Recommended = 8.3.150.0, 8.5.182.0, 8.8.130.0, 8.10.185.0
- Cisco Catalyst IOS XE Wireless LAN Controller and Cisco Lightweight Access Points
  - Minimum = 16.12.1s
  - Recommended = 17.3.8, 17.6.6, 17.9.4, 17.12.1
- 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, 8.10.185.0

- Cisco Autonomous Access Points

  Minimum = 12.4(21a)JY

  Recommended = 15.2(4)JB6, 15.3(3)JF15, 15.3(3)JPP

- Cisco Meraki Access Points

  Minimum = MR 25.9, MX 13.33

  Recommended = MR 29.7.1, MX 18.107.5

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 IP Phone 8821 and 8821-EX are supported on the following Cisco Aironet access point platforms.

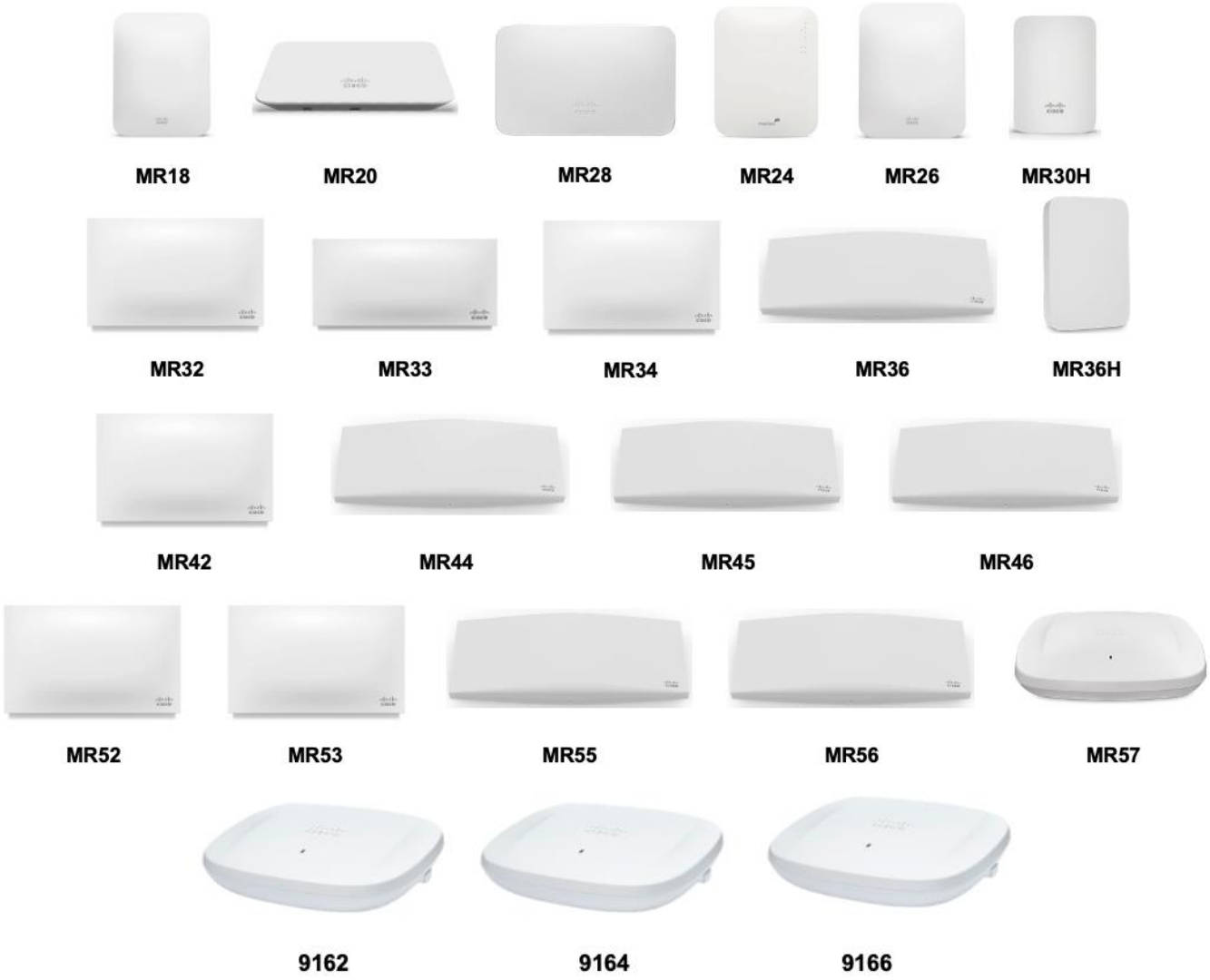
Note: The Cisco Wireless IP Phone 8821 and 8821-EX are supported with the Cisco AP3600 when the internal 802.11a/b/g/n radio is utilized, however is not supported if the 802.11ac module (AIR-RM3000AC) for the Cisco AP3600 is installed.

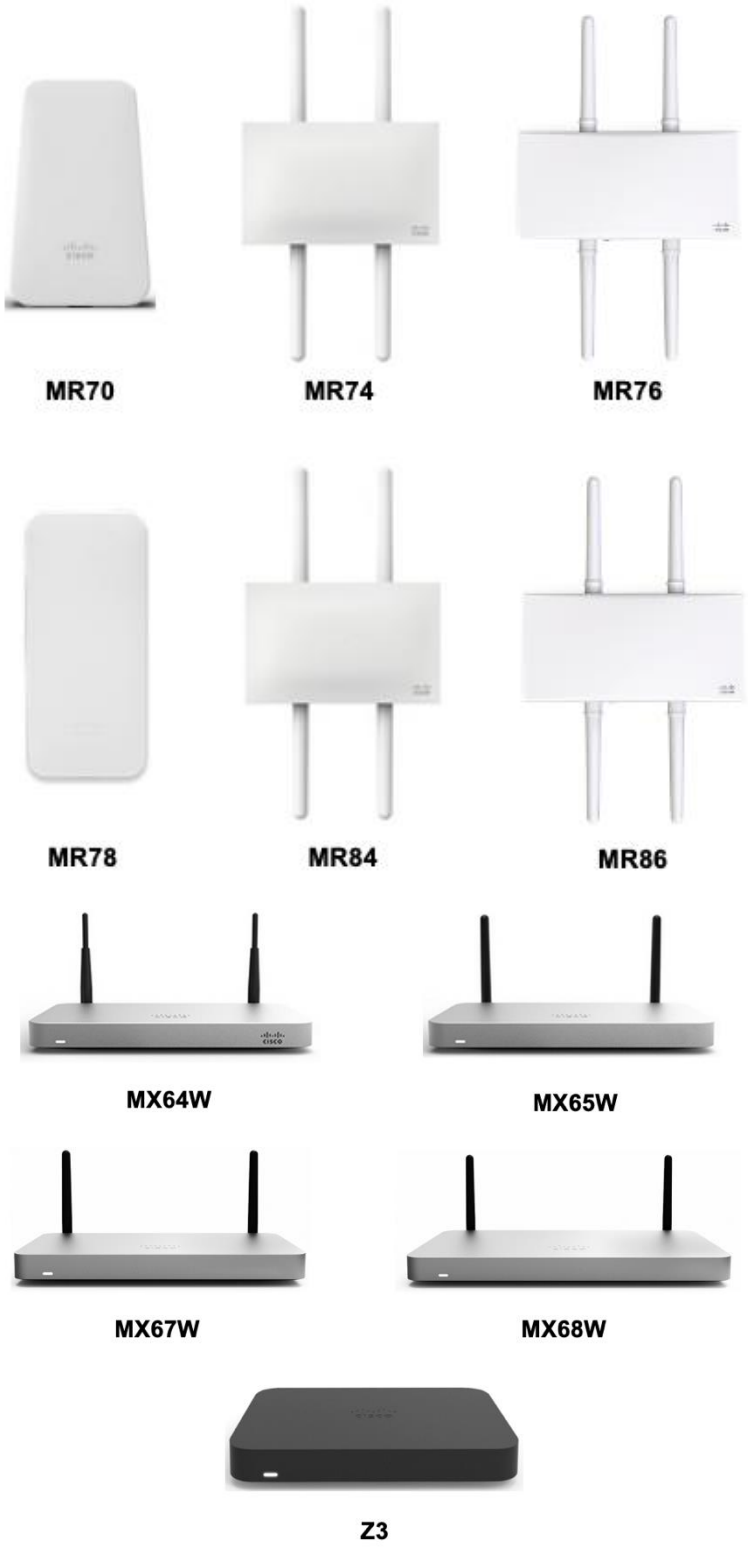
The table below lists the modes that are supported by each Cisco Aironet access point.

Cisco AP Series	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	Lightweight	Mobility Express	Autonomous
600	Yes	Yes	Yes	Yes	No	No	Yes	No	No
700	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
700W	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
1040	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
1130	Yes	Yes	Yes	No	No	No	Yes	No	Yes
1140	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
1240	Yes	Yes	Yes	No	No	No	Yes	No	Yes
1250	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
1260	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
1530	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
1540	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1550	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
1560	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
1570	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
1600	Yes	Yes	Yes	Yes	No	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
2600	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
2700	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
2800	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
3500	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
3600	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes

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
890	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes

The Cisco Wireless IP Phone 8821 and 8821-EX are supported on the following Cisco Meraki access point platforms.


MR18
MR20
MR28
MR24
MR26
MR30H
MR32
MR33
MR34
MR36
MR36H
MR42
MR44
MR45
MR46
MR52
MR53
MR55
MR56
MR57
9162
9164
9166



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

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

The Cisco Meraki MR12, MR16, and Z1 access point platforms are not certified for use with Cisco Wireless IP Phone 8821 and 8821-EX deployments.

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
MR18	Yes	Yes	Yes	Yes	No	No
MR20	Yes	Yes	Yes	Yes	Yes	No
MR24	Yes	Yes	Yes	Yes	No	No
MR26	Yes	Yes	Yes	Yes	No	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)
- Traffic Classification (TCLAS)
- Differentiated Services Code Point (DSCP)
- Class of Service (CoS / 802.1p)
- QoS Basic Service Set (QBSS)

Antenna Systems

Some Cisco access points require or allow external antennas.

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

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

Wi-Fi

The following table lists the maximum tx power and receiver sensitivity info for each data rate per 802.11 mode utilized by Cisco Wireless IP Phone 8821 and 8821-EX.

5 GHz Specifications

5 GHz - 802.11a	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 14 dBm (Depends on region)	6 Mbps	OFDM - BPSK	-94 dBm
	9 Mbps	OFDM - BPSK	-93 dBm
	12 Mbps	OFDM - QPSK	-92 dBm
	18 Mbps	OFDM - QPSK	-89 dBm
	24 Mbps	OFDM - 16 QAM	-86 dBm
	36 Mbps	OFDM - 16 QAM	-83 dBm
	48 Mbps	OFDM - 64 QAM	-78 dBm
	54 Mbps	OFDM - 64 QAM	-76 dBm
5 GHz - 802.11n (HT20)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 13 dBm (Depends on region)	7 Mbps (MCS 0)	OFDM - BPSK	-94 dBm
	14 Mbps (MCS 1)	OFDM - QPSK	-91 dBm
	21 Mbps (MCS 2)	OFDM - QPSK	-89 dBm
	29 Mbps (MCS 3)	OFDM - 16 QAM	-86 dBm
	43 Mbps (MCS 4)	OFDM - 16 QAM	-82 dBm
	58 Mbps (MCS 5)	OFDM - 64 QAM	-77 dBm
	65 Mbps (MCS 6)	OFDM - 64 QAM	-76 dBm
	72 Mbps (MCS 7)	OFDM - 64 QAM	-74 dBm
5 GHz - 802.11n (HT40)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 13 dBm	15 Mbps (MCS 0)	OFDM - BPSK	-91 dBm

(Depends on region)	30 Mbps (MCS 1)	OFDM - QPSK	-88 dBm
	45 Mbps (MCS 2)	OFDM - QPSK	-86 dBm
	60 Mbps (MCS 3)	OFDM - 16 QAM	-83 dBm
	90 Mbps (MCS 4)	OFDM - 16 QAM	-79 dBm
	120 Mbps (MCS 5)	OFDM - 64 QAM	-75 dBm
	135 Mbps (MCS 6)	OFDM - 64 QAM	-73 dBm
	150 Mbps (MCS 7)	OFDM - 64 QAM	-72 dBm
5 GHz - 802.11ac (VHT20)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 12 dBm (Depends on region)	7 Mbps (MCS 0)	OFDM - BPSK	-93 dBm
	14 Mbps (MCS 1)	OFDM - QPSK	-90 dBm
	21 Mbps (MCS 2)	OFDM - QPSK	-87 dBm
	29 Mbps (MCS 3)	OFDM - 16 QAM	-84 dBm
	43 Mbps (MCS 4)	OFDM - 16 QAM	-81 dBm
	58 Mbps (MCS 5)	OFDM - 64 QAM	-76 dBm
	65 Mbps (MCS 6)	OFDM - 64 QAM	-75 dBm
	72 Mbps (MCS 7)	OFDM - 64 QAM	-74 dBm
	87 Mbps (MCS 8)	OFDM – 256 QAM	-70 dBm
5 GHz - 802.11ac (VHT40)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 12 dBm (Depends on region)	15 Mbps (MCS 0)	OFDM - BPSK	-90 dBm
	30 Mbps (MCS 1)	OFDM - QPSK	-87 dBm
	45 Mbps (MCS 2)	OFDM - QPSK	-85 dBm
	60 Mbps (MCS 3)	OFDM - 16 QAM	-82 dBm
	90 Mbps (MCS 4)	OFDM - 16 QAM	-79 dBm
	120 Mbps (MCS 5)	OFDM - 64 QAM	-73 dBm
	135 Mbps (MCS 6)	OFDM - 64 QAM	-72 dBm
	150 Mbps (MCS 7)	OFDM - 64 QAM	-72dBm
	180 Mbps (MCS 8)	OFDM – 256 QAM	-67 dBm
	200 Mbps (MCS 9)	OFDM – 256 QAM	-66 dBm
5 GHz - 802.11ac (VHT80)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 12 dBm (Depends on region)	33 Mbps (MCS 0)	OFDM - BPSK	-87 dBm
	65 Mbps (MCS 1)	OFDM - QPSK	-83 dBm
	98 Mbps (MCS 2)	OFDM - QPSK	-81 dBm
	130 Mbps (MCS 3)	OFDM - 16 QAM	-78 dBm
	195 Mbps (MCS 4)	OFDM - 16 QAM	-75 dBm
	260 Mbps (MCS 5)	OFDM - 64 QAM	-73 dBm
	293 Mbps (MCS 6)	OFDM - 64 QAM	-68 dBm
	325 Mbps (MCS 7)	OFDM - 64 QAM	-68 dBm
	390 Mbps (MCS 8)	OFDM – 256 QAM	-64 dBm
	433 Mbps (MCS 9)	OFDM – 256 QAM	-62 dBm

2.4 GHz Specifications

2.4 GHz - 802.11b	Data Rate	Modulation	Receiver Sensitivity
Max Tx Power = 17 dBm (Depends on region)	1 Mbps	DSSS - BPSK	-98 dBm
	2 Mbps	DSSS - QPSK	-96 dBm
	5.5 Mbps	DSSS - CCK	-93 dBm
	11 Mbps	DSSS - CCK	-91 dBm
2.4 GHz - 802.11g	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 14 dBm (Depends on region)	6 Mbps	OFDM - BPSK	-95 dBm
	9 Mbps	OFDM - BPSK	-94 dBm
	12 Mbps	OFDM - QPSK	-93 dBm
	18 Mbps	OFDM - QPSK	-90 dBm
	24 Mbps	OFDM - 16 QAM	-87 dBm
	36 Mbps	OFDM - 16 QAM	-84 dBm
	48 Mbps	OFDM - 64 QAM	-79 dBm
	54 Mbps	OFDM - 64 QAM	-77 dBm
2.4 GHz - 802.11n (HT20)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 13 dBm (Depends on region)	7 Mbps (MCS 0)	OFDM - BPSK	-95 dBm
	14 Mbps (MCS 1)	OFDM - QPSK	-92 dBm
	21 Mbps (MCS 2)	OFDM - QPSK	-90 dBm
	29 Mbps (MCS 3)	OFDM - 16 QAM	-87 dBm
	43 Mbps (MCS 4)	OFDM - 16 QAM	-83 dBm
	58 Mbps (MCS 5)	OFDM - 64 QAM	-78 dBm
	65 Mbps (MCS 6)	OFDM - 64 QAM	-77 dBm
	72 Mbps (MCS 7)	OFDM - 64 QAM	-75 dBm

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

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

To achieve 802.11n/ac connectivity, it is recommended that the Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX will passively scan DFS channels first before engaging in active scans of those channels.

If 802.11d is not enabled, then the Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX.

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

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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX.

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

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

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

Bluetooth Profiles

The Cisco Wireless IP Phone 8821 and 8821-EX support the following Bluetooth profiles.

Hands-Free Profile (HFP)

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

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

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 IP Phone 8821 and 8821-EX currently support the following languages.

Arabic	French	Polish
Bulgarian	German	Portuguese
Catalan	Greek	Romanian
Chinese	Hebrew	Russian

Croatian	Hungarian	Serbian
Czech	Italian	Slovak
Danish	Japanese	Slovenian
Dutch	Korean	Spanish
English	Latvian	Swedish
Estonian	Lithuanian	Thai
Finnish	Norwegian	Turkish

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

Download the locale packages from the Localization page at the following URL:

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

8821-EX Certifications

The Cisco Wireless IP Phone 8821-EX is certified for ANSI/ISA 12.12.01 & CAN/CSA C22.2 No. 213 Class I and II, Division 2 and Class III, Division 1 and 2.

Certification ensures that the equipment is fit for its intended purpose and that adequate information is supplied with it to ensure that it can be used safely.

ANSI/ISA 12.12.01 & CAN/CSA C22.2 No. 213 Class I and II, Division 2 and Class III, Division 1 and 2

Laws and regulations in most municipalities, states, and provinces in North America require certain products to be tested to a specific standard or group of standards when they are to be classified safe when used in an explosive environment.

In North America, hazardous locations have traditionally been defined by the following combination of Class and Division:

- **Class I** - A location where a quantity of flammable gas or vapor, sufficient to produce an explosive or ignitable mixture, may be present in the air.
- **Class II** - A location made hazardous by the presence of combustible elements.
- **Class III** - A location made hazardous by the presence of easily ignitable fibers in the air.

- **Division 1** - A location where a classified hazard is likely to exist.
- **Division 2** - A location where a classified hazard does not normally exist but is possible under abnormal conditions.

More recently in North America, for Class I hazards, locations can be classified under the zone system.

Note: If the Cisco Wireless IP Phone 8821-EX is to be used in a hazardous environment, then the environment should be regulated by the CSA standards.

The Cisco Wireless IP Phone 8821-EX is not ATEX certified, therefore should not be used in an ATEX environment.

Battery Life

The Cisco Wireless IP Phone 8821 and 8821-EX have a 2060 mAh smart battery.

The Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX battery approximately every 2 years.

The battery's manufacture date is printed on the back of the battery, which can help determine the age of the battery.

With the 11.0(5) release, the Cisco Wireless IP Phone 8821 can get up to 11.5 hours of talk time when charging the battery inside the phone or when charging spare batteries using the newer Desktop Charger or Multicharger for the Cisco Wireless IP Phone 8821. Previous releases provided up to 9.5 hours of talk time.

The Cisco Wireless IP Phone 8821-EX can offer up to 9.5 hours of talk time when charging the battery inside the phone or when charging spare batteries using the Desktop Charger or Multicharger for the Cisco Wireless IP Phone 8821-EX.

The table below lists the maximum on call and idle times per scan mode.

Phone Model	Call State	Scan Mode	Battery Time
8821	On Call	Continuous	Up to 11.5 hours
		Auto	Up to 11.5 hours
	Idle	Continuous	Up to 45 hours
		Auto	Up to 145 hours
8821-EX	On Call	Continuous	Up to 9.5 hours
		Auto	Up to 9.5 hours
	Idle	Continuous	Up to 45 hours
		Auto	Up to 145 hours

Note: The newer Desktop Charger and Multicharger for the Cisco Wireless IP Phone 8821 must be used when charging spare batteries for the Cisco Wireless IP Phone 8821 running 11.0(5) or later software in order to get up to 11.5 hours of talk time.

The Cisco Wireless IP Phone 8821-EX utilizes a different Desktop Charger and Multicharger than what is to be used with the Cisco Wireless IP Phone 8821.

The Cisco Wireless IP Phone 8821-EX has a coin screw on the battery door to secure it to the phone.

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

Usage

Battery life will be reduced when the Cisco Wireless IP Phone 8821 or 8821-EX user is on call, roaming, turning the display on, using Bluetooth, using applications, receiving XSI messages, or navigating the menus on the phone.

If using XSI applications or waking up the display frequently, it is recommended to set the display sleep timer under **Settings > Phone settings > Display > Sleep** to **10 seconds** and set the brightness level under **Settings > Phone settings > Display > Brightness** to level 5.

Coverage

Ensure the Cisco Wireless IP Phone 8821 and 8821-EX remain in a good RF coverage area and is able to maintain a constant connection to the Cisco Unified Communications Manager.

If the Cisco Wireless IP Phone 8821 or 8821-EX user travels out of range and remains out of range for a significant duration, battery life can be reduced.

Scan Mode

The Cisco Wireless IP Phone 8821 and 8821-EX supports 3 different scan modes (**Continuous**, **Auto**, **Single AP**), where Continuous is the default configuration.

The configured scan mode will determine the battery life baseline.

- **Continuous** scan mode is designed for Cisco Wireless IP Phone 8821 and 8821-EX users that are constantly on the move where frequent roaming events occur and to maximize performance and connectivity, but power consumption is higher.
- **Auto** scan mode is designed for Cisco Wireless IP Phone 8821 and 8821-EX users that roam occasionally and require more idle battery life than **Continuous** scan mode can offer, but roaming performance may be decreased.
- **Single AP** scan mode is designed for Cisco Wireless IP Phone 8821 and 8821-EX users that do not roam and require maximum idle battery life.

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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 or 8821-EX subscribes to a multicast stream, then the Cisco Wireless IP Phone 8821 or 8821-EX 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.

On Call Power Save in the Wi-Fi Profile should remain **Enabled** so the Cisco Wireless IP Phone 8821 and 8821-EX can utilize U-APSD.

If **On Call Power Save** is Disabled, then the Cisco Wireless IP Phone 8821 and 8821-EX will utilize active mode when on call, but still use U-APSD when in idle.

Only disable **On Call Power Save** for troubleshooting purposes.

Phone Care

The Cisco Wireless IP Phone 8821 is IP54 rated, which is designed to provide protection from dust, liquid splashes, and moisture, where the Cisco Wireless IP Phone 8821-EX is IP67 rated for increased dust and water protection.

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

For thorough cleaning, we recommend using Caviwipes™ or Saniwipes™.

Caviwipes™ and Saniwipes™ contain up to 17% isopropanol. Any cleaning solution containing a higher amount of isopropanol, including pure isopropanol, or an alternative alcohol-based liquid could potentially damage the phone.

Excessive use of Caviwipes™ or Saniwipes™ (more than 3 times / day) could potentially damage the phone.

Do not use bleach or other caustic products to clean the phone.

Do not use compressed air to clean the phone as it can damage the phone and voids the phone warranty.

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

For more information, refer to the **Cisco Wireless IP Phone 8821 and 8821-EX User Guide** at this URL:
https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html

Accessories

The following accessories are available for the Cisco Wireless IP Phone 8821 and 8821-EX.

- Batteries
- Phone Power Supply
- Holster Case
- Leather Case
- Lanyard
- Desktop Chargers
- Multichargers
- Headsets (Cisco 521 and Cisco 522)

For more information, refer to the **Cisco Wireless IP Phone 8821 Series Accessory Guide** at this URL:
https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html

Note: The Desktop Charger and Multicharger are different for the Cisco Wireless IP Phone 8821 and the Cisco Wireless IP Phone 8821-EX. The chargers look the same except that the chargers for the Cisco Wireless IP Phone 8821-EX show a graphic of the Cisco Wireless IP Phone 8821-EX and they do not have the voltage label as the chargers for the Cisco Wireless IP Phone 8821 have.

Other Accessories

Only the third-party accessories listed below are certified for use with the Cisco Wireless IP Phone 8821 and 8821-EX.

- USB to Ethernet Dongles
  - Apple USB 2.0 Ethernet Adapter (www.apple.com)
  - Belkin B2B048 USB 3.0 Gigabit Ethernet Adapter (www.belkin.com)
  - D-Link DUB-E100 USB 2.0 Fast Ethernet Adapter (www.dlink.com)
  - Linksys USB3GIG USB 3.0 Gigabit Ethernet Adapter (www.linksys.com)
  - Linksys USB300M USB 2.0 Ethernet Adapter (www.linksys.com)

Note: Cisco does not endorse, support, or test third-party cases or covers for the Cisco Wireless IP Phone 8821. Using the Cisco Wireless IP Phone 8821 or 8821-EX with third-party cases or covers may void the warranty.

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/8821/english/technical_bulletin/Cisco_Technical_Bulletin_for_Wireless_IP_Phone_8821_RC3.pdf

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 IP Phone 8821 and 8821-EX.

802.11 Network

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

5 GHz (802.11a/n/ac)

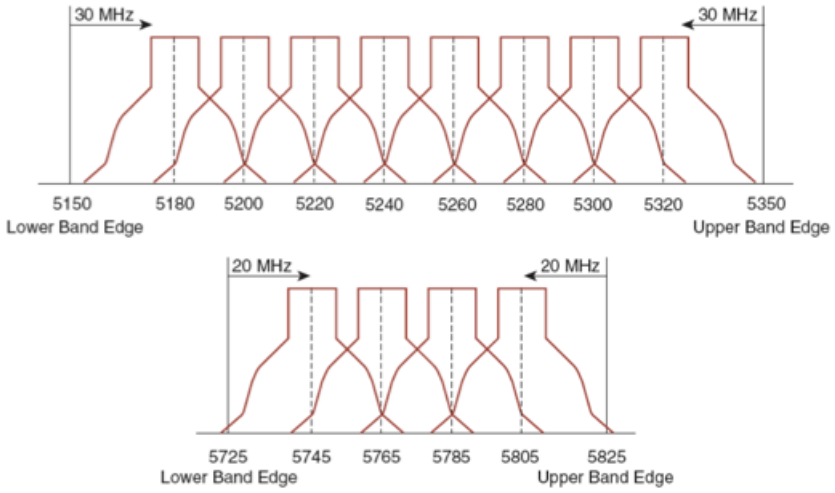
5 GHz is the recommended frequency band to utilize for operation of the Cisco Wireless IP Phone 8821 and 8821-EX.

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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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.

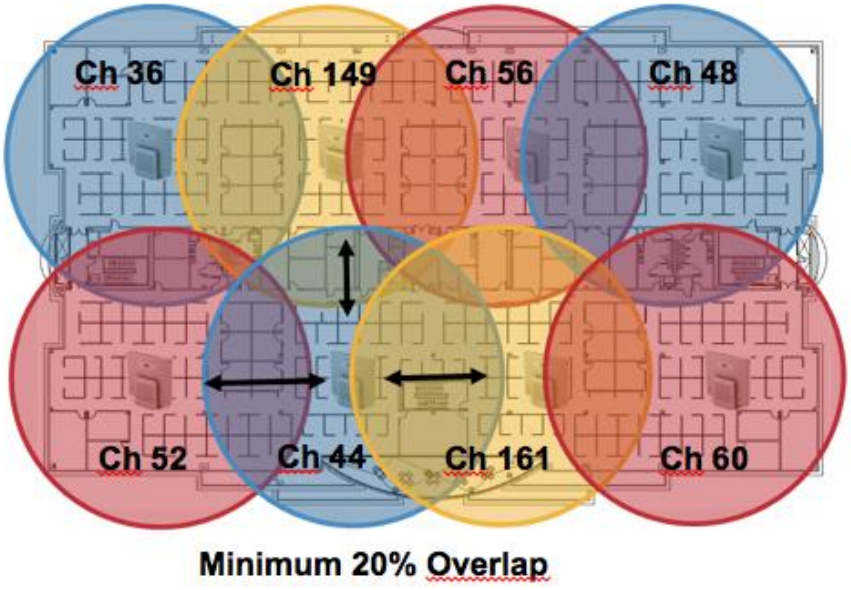
If there are repeated radar events detected by the access point (just or falsely), determine if the radar signals are impacting a single channel (narrowband) or multiple channels (wideband), then potentially disable use of that channel or channels in the wireless LAN.

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.

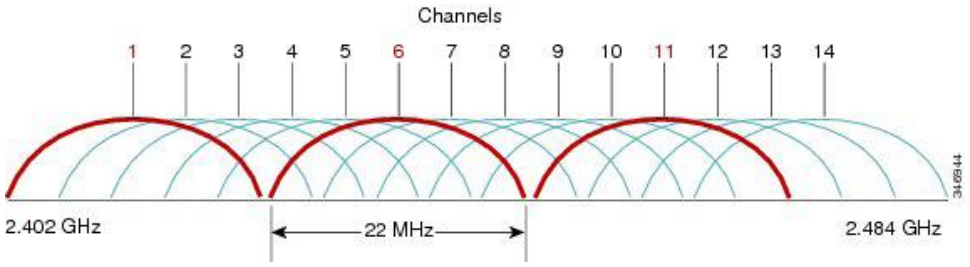
If there is an intermittent interferer, then the access point or access points serving that area may need to have a channel statically assigned.

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.

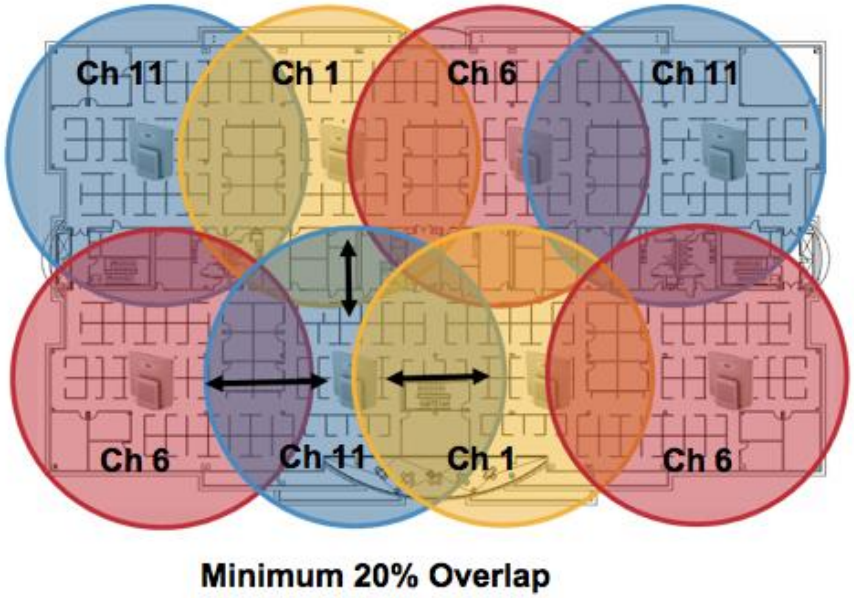
There are only 3 non-overlapping channels in the 2.4 GHz frequency range (channels 1, 6, 11).

Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying the Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX should always have a signal of -67 dBm or higher when using 5 GHz or 2.4 GHz, while the Cisco Wireless IP Phone 8821 and 8821-EX 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%.

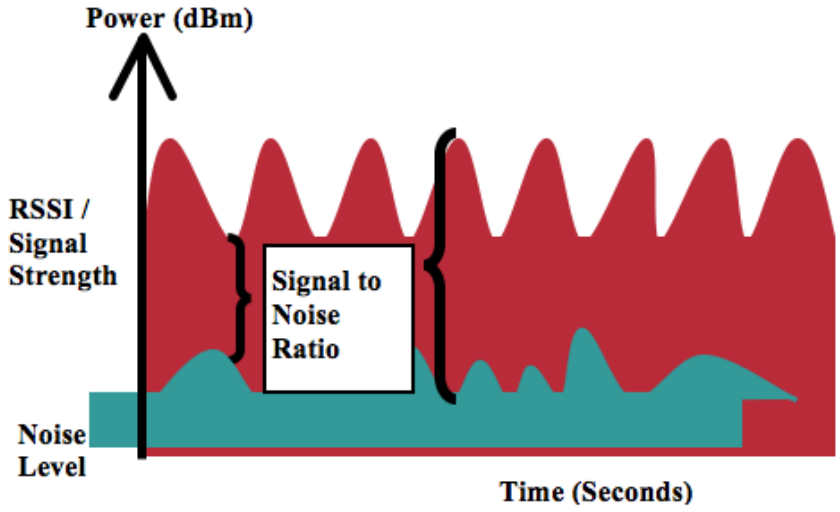
A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal should be maintained.

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).

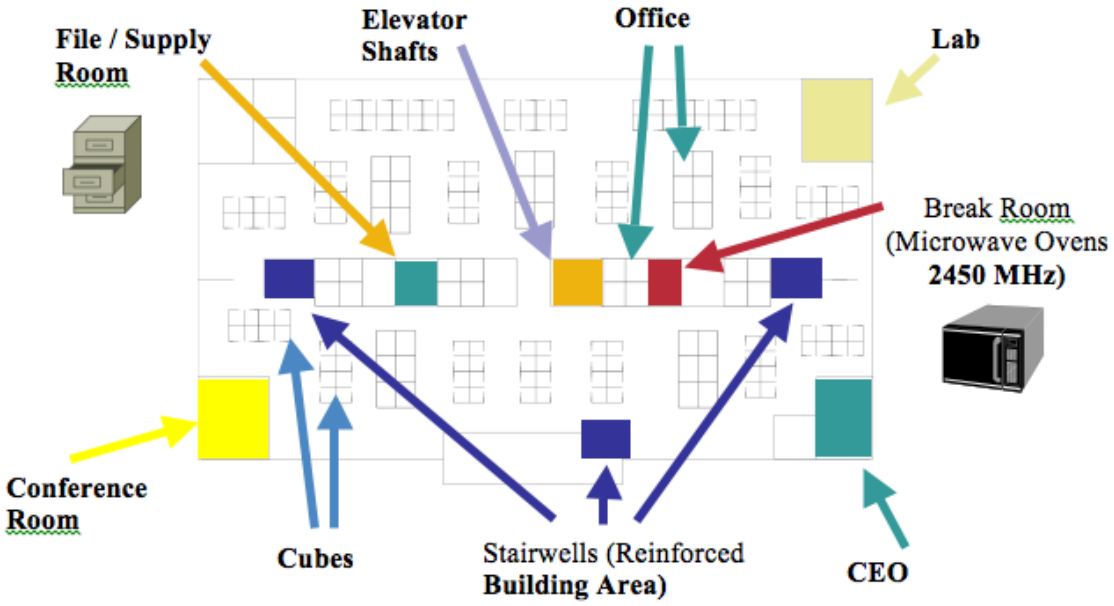
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

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.

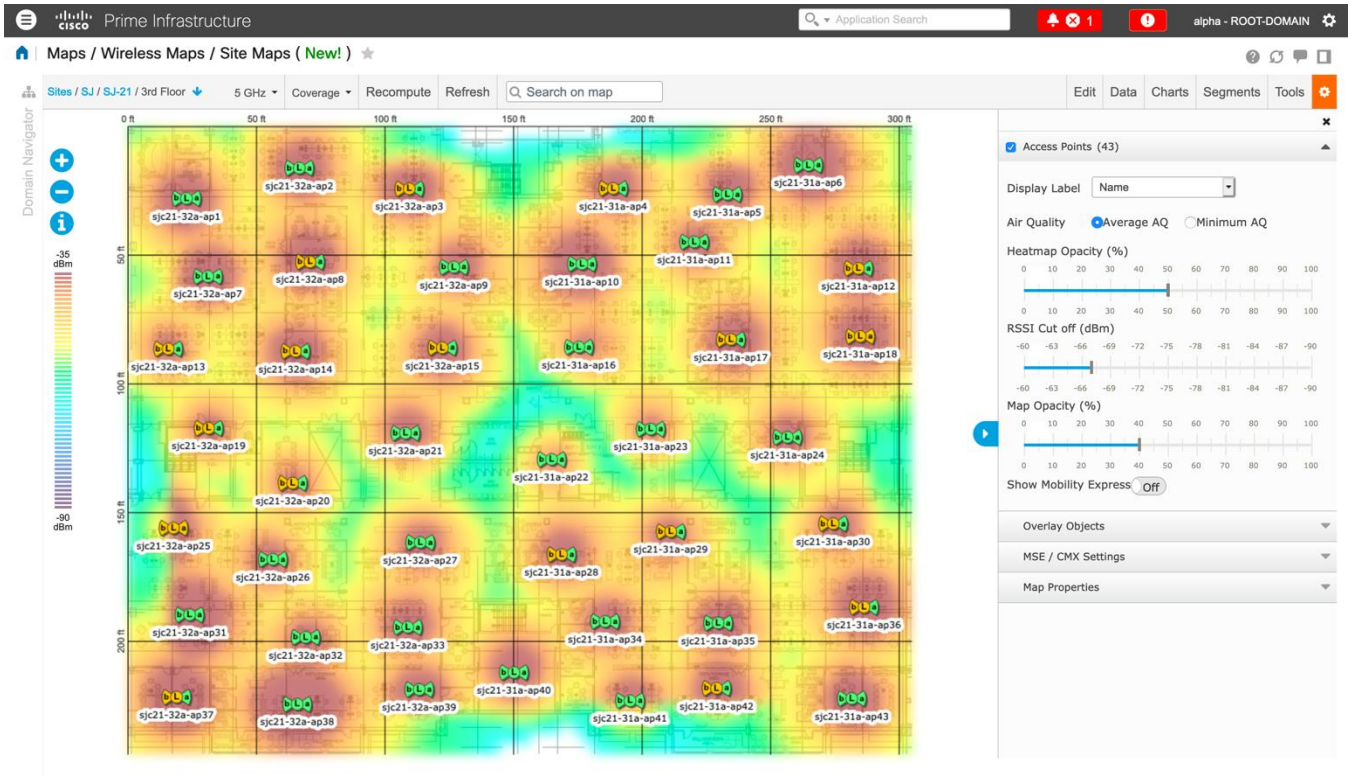
However there are products that also utilize the non-licensed 5 GHz frequency (e.g. 5.8 GHz cordless phones, which can impact UNII-3 channels).



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 IP Phone 8821 and 8821-EX both have a single antenna, therefore it supports up to MCS 7 data rates for 802.11n (up to 150 Mbps) and up to MCS 9 data rates for 802.11ac (up to 433 Mbps).

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

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

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

The recommended data rate configurations are the following:

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, HT MCS 0 - MCS 7, (HT MCS 8 - MCS 31)	6, 9 Mbps

802.11g/n	12 Mbps	18-54 Mbps, HT MCS 0 - MCS 7, (HT MCS 8 - MCS 31)	1, 2, 5.5, 6, 9, 11 Mbps
802.11b/g/n	11 Mbps	12-54 Mbps, HT MCS 0 - MCS 7, (HT MCS 8 - 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 or 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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:

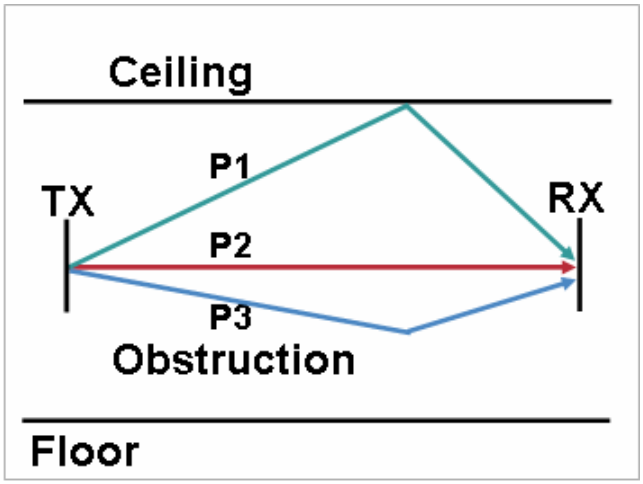
Data Corruption
Occurs when multipath is so severe that the receiver is unable to detect the transmitted information.

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 IP Phone 8821 and 8821-EX support the following wireless security features.

WLAN Authentication

- WPA2 and WPA (802.1x authentication)
- WPA2-PSK and WPA-PSK (Pre-Shared key)
- EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- PEAP-GTC (Protected Extensible Authentication Protocol - Generic Token Card)
- PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2)
- 802.11r / Fast Transition (FT)
- CCKM (Cisco Centralized Key Management)

- None

WLAN Encryption

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

Note: The access point must support AES (CCMP128) as TKIP can only be used as the broadcast/multicast cipher.

WPA3 is not supported.

802.1x-SHA2 key management is not supported.

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

Shared Key authentication is not supported.

The Cisco Wireless IP Phone 8821 and 8821-EX also support the following additional security features.

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

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

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

The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (the Cisco Wireless IP Phone 8821 and 8821-EX) and the RADIUS server. The server sends an Authority ID (AID) to the client, which in turn selects the appropriate PAC. The client returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its primary-key. Both endpoints now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must enable don the RADIUS server.

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

The Cisco Wireless IP Phone 8821 and 8821-EX currently support automatic provisioning of the PAC only, so enable **Allow anonymous in-band PAC provisioning** on the RADIUS server.

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

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

If anonymous PAC provisioning is not allowed in the production wireless LAN environment then a staging RADIUS server can be setup for initial PAC provisioning of the Cisco Wireless IP Phone 8821 and 8821-EX.

This requires that the staging RADIUS server be setup as a secondary EAP-FAST server and components are replicated from the production primary EAP-FAST server, which include user and group database and EAP-FAST primary key and policy info.

Ensure the production primary EAP-FAST RADIUS server is setup to send the EAP-FAST primary keys and policies to the staging secondary EAP-FAST RADIUS server, which will then allow the Cisco Wireless IP Phone 8821 and 8821-EX to use the provisioned PAC in the production environment where **Allow anonymous in-band PAC provisioning** is disabled.

When it is time to renew the PAC, then authenticated in-band PAC provisioning will be used, so ensure that **Allow authenticated in-band PAC provisioning** is enabled.

Ensure that the Cisco Wireless IP Phone 8821 and 8821-EX have connected to the network during the grace period to ensure it can use its existing PAC created either using the active or retired primary key in order to get issued a new PAC.

Is recommended to only have the staging wireless LAN pointed to the staging RADIUS server and to disable the staging access point radios when not being used.

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

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

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

A certificate is required to be installed.

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

EAP-TLS may also require a user account to be created on the authentication server matching the common name of the certificate imported into the Cisco Wireless IP Phone 8821 or 8821-EX.

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

Protected Extensible Authentication Protocol (PEAP)

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

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

PEAP-GTC and PEAP-MSCHAPv2 are supported inner authentication protocols.

PEAP requires that a user account be created on the authentication server.

The authentication server can be validated via importing a certificate into the Cisco Wireless IP Phone 8821 and 8821-EX.

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	DSCP	802.1p	WMM UP	Protocol
Voice	EF (46)	5	6	RTP (UDP 16384 - 32767)
Call Control	CS3 (24)	3	4	SIP (TCP/UDP 5060 - 5061)

- 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 IP Phone 8821 and 8821-EX and the Cisco Unified Communications Manager, refer to the **Cisco Unified Communications Manager TCP and UDP Port Usage** document at this URL:

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

Call Admission Control (CAC)

Call Admission Control can be enabled on the access point.

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

Pre-Call Admission Control

If Call Admission Control is enabled on the access point, the Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 or 8821-EX establishes the call.

If the access point rejects the call and the Cisco Wireless IP Phone 8821 or 8821-EX 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 IP Phone 8821 or 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX will send an ADDTS request during the roam to the new access point, which embedded in the reassociation request frame.

Traffic Classification (TCLAS)

Traffic Classification (TCLAS) helps to ensure that the access point properly classifies voice packets.

Without proper classification, voice packets will be treated as best effort, which will defeat the purpose of TSPEC and QoS in general.

TCP and UDP port information will be used to set the UP (User Priority) value.

The previous method of classification depends upon preservation of DSCP value throughout the network, where the DSCP value maps to a particular queue (BE, BK, VI, VO).

However, the DSCP values are not always preserved as this can be viewed as a security risk.

Using port based QoS policies is inadequate for CAPWAP based wireless LAN solutions as all data packets use the same UDP port (CAPWAP = UDP 5246) and the access point uses the outside QoS marking to determine which queue the packets should be placed in.

With TCLAS, DSCP preservation is not a requirement.

Call Admission Control must be enabled on the access point in order to enable TCLAS.

TCLAS will be negotiated within the ADDTS packets, which are used to request bandwidth in order to place or receive a call.

QoS Basic Service Set (QBSS)

There are three different versions of QoS Basic Service Set (QBSS) that the Cisco Wireless IP Phone 8821 and 8821-EX support.

The first version from Cisco was on a 0-100 scale and was not based on clear channel assessment (CCA), so it does not account for channel utilization, but only the 802.11 traffic traversing that individual access point's radio. So it does not account for other 802.11 energy or interferers using the same frequencies.

QBSS is also a part of 802.11e, which is on a 0-255 scale and is CCA based. So this gives a true representation on how busy the channel is. The max threshold is also defined on the client side, which is set to 105.

The second version from Cisco is based on the 802.11e version, but allows the default max threshold of 105 to be optionally configured.

Each version of QBSS can be optionally be configured on the access point.

Wired QoS

Configure QoS settings and policies for the necessary network devices.

Configuring Cisco Switch Ports for WLAN Devices

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

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

Enable COS trust for Cisco Wireless LAN Controller

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

Enable DSCP trust for Cisco Access Points

```
mls qos
!
interface X
 mls qos trust dscp
```

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

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 IP Phone 8821 and 8821-EX default to Auto for the 802.11 mode, which allows the Cisco Wireless IP Phone 8821 and 8821-EX to connect to either 5 GHz or 2.4 GHz and enables interband roaming support.

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

802.1x authentication is required in order to utilize CCKM.

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

When 802.11r (FT) or CCKM is utilized, roaming times can be reduced 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.

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

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

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

Over the Air

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

Over the Distribution

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

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

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

The Cisco Wireless IP Phone 8821 and 8821-EX 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-FAST	WPA2	AES
802.11r (FT)	EAP-TLS	WPA2	AES
802.11r (FT)	PEAP-GTC	WPA2	AES
802.11r (FT)	PEAP-MSCHAPv2	WPA2	AES
CCKM	EAP-FAST	WPA2, WPA	AES, TKIP
CCKM	EAP-TLS	WPA2, WPA	AES, TKIP
CCKM	PEAP-GTC	WPA2, WPA	AES, TKIP
CCKM	PEAP-MSCHAPv2	WPA2, WPA	AES, TKIP

Note: If deploying the Cisco Wireless IP Phone 8821 or 8821-EX 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 IP Phone 8821 or 8821-EX, 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).

The access point must support AES (CCMP128) as TKIP can only be used as the broadcast/multicast cipher.

Interband Roaming

The Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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.

Scanning

There are three different scan modes (**Continuous**, **Auto**, **Single AP**), which can be configured for the Cisco Wireless IP Phone 8821 and 8821-EX in the Cisco Unified Communications Manager.

When using multiple access points where seamless roaming is required, **Continuous** (default) or **Auto** scan mode should be enabled (**Single AP** scan mode should not be used if multiple access points exist).

Continuous scan mode is the default scan mode, which enables seamless roaming, but power consumption is higher.

Continuous scan mode is the recommended scan mode for most environments where frequent roaming occurs, while also meeting minimum battery life requirements.

When on an active call with **Continuous** or **Auto** scan mode enabled, the Cisco Wireless IP Phone 8821 and 8821-EX will be continuously scanning regardless of the current call state (idle or on call) or current access point signal level (RSSI).

When in idle (not on an active call) and **Continuous** scan mode is enabled, then the Cisco Wireless IP Phone 8821 and 8821-EX will also be continuously scanning.

When in idle with **Auto** scan mode, scans will only occur when the pre-defined RSSI threshold is held for the pre-defined duration.

Continuous scan mode is recommended for environments where frequent roams occur or where smaller cells (pico cells) exist.

Continuous scan mode can also help with location tracking.

Auto scan mode can increase idle battery life, but roaming performance may be decreased. Since the phone is not continuously scanning for the best available AP, it may not be connected to the best AP when using **Auto** scan. This may result in some interruptions in connectivity when the phone moves quickly away from the current AP.

If using only one access point, select **Single AP** mode on the Cisco Wireless IP Phone 8821 and 8821-EX to reduce scanning and optimize battery life.

Power Management

When the access point supports Proxy ARP, the idle battery life will be optimized. Proxy ARP allows the Cisco Wireless IP Phone 8821 and 8821-EX to remain in sleep mode longer versus waking up at each Delivery Traffic Indicator Message (DTIM) period to check for incoming broadcasts.

To optimize battery life, the Cisco Wireless IP Phone 8821 and 8821-EX will utilize either U-APSD or PS-POLL power save methods 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 IP Phone 8821 and 8821-EX primarily use U-APSD when in idle or on call.

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

Wireless LAN is automatically disabled temporarily when Ethernet is connected by docking the Cisco Wireless IP Phone 8821 or 8821-EX when a USB to Ethernet dongle is attached, but will be automatically re-enabled once Ethernet is disconnected.

Use of a supported USB to Ethernet dongle is for initial provisioning purposes only and not to convert the Cisco Wireless IP Phone 8821 or 8821-EX to a wired IP phone.

Delivery Traffic Indicator Message (DTIM)

The Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX do not have to wake up at DTIM.

For optimal battery life and performance, 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 IP Phone 8821 or 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX support the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure that IGMP snooping is also enabled on all switches.

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

Configuring the Cisco Wireless LAN

Cisco AireOS Wireless LAN Controller and Lightweight Access Points

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

- Ensure **802.11r (FT)** or **CCKM** is **Enabled**
- Set **Quality of Service (QoS)** to **Platinum**
- Set the **WMM Policy** to **Required**
- Ensure **802.11k** is **Disabled**
- Ensure **802.11v** is **Disabled**
- 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 IP Phone 8821 and 8821-EX 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**.

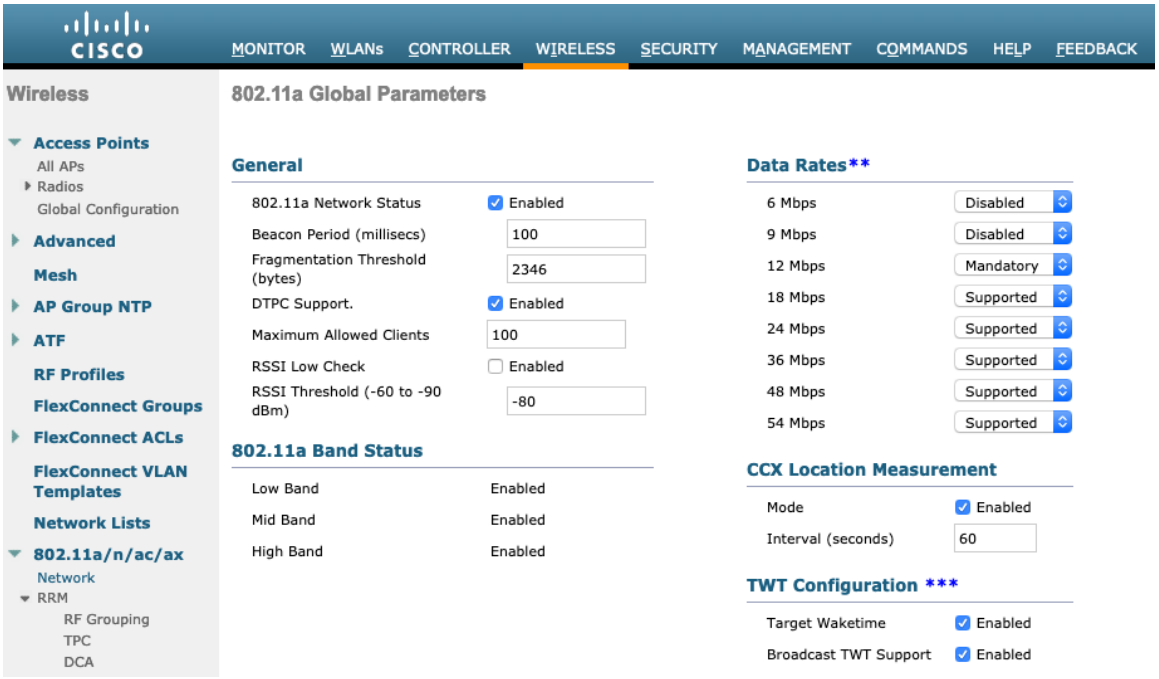
Set the **Beacon Period** to **100 ms**.

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.

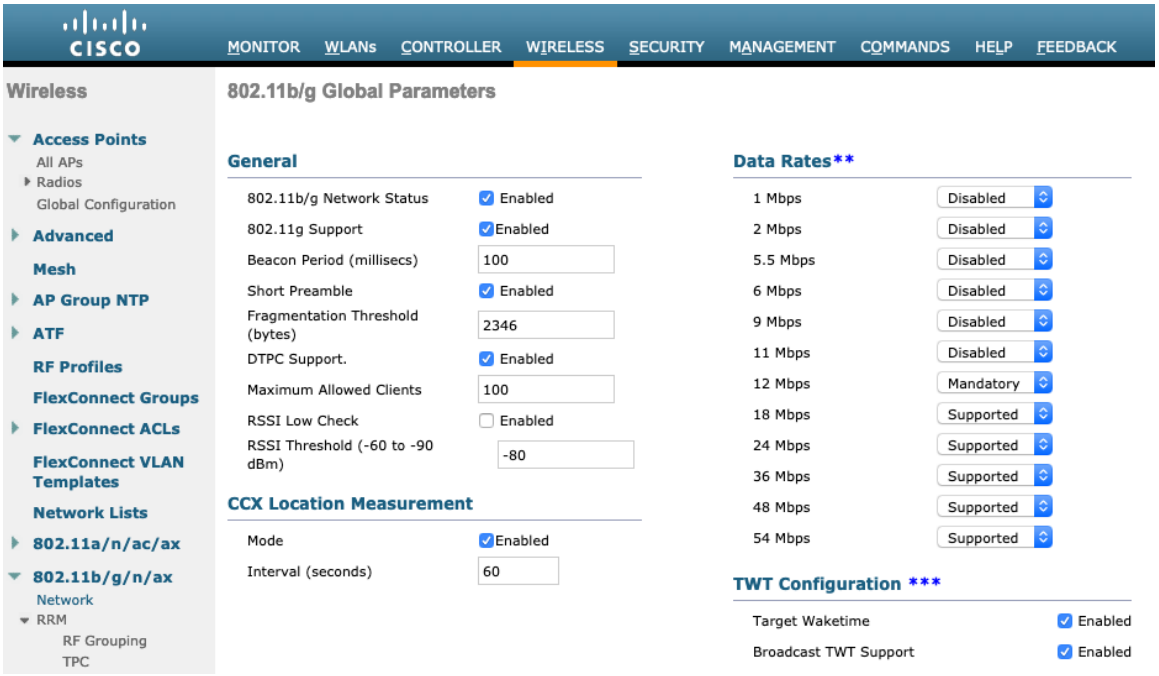
Ensure **DTPC Support** is enabled.

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

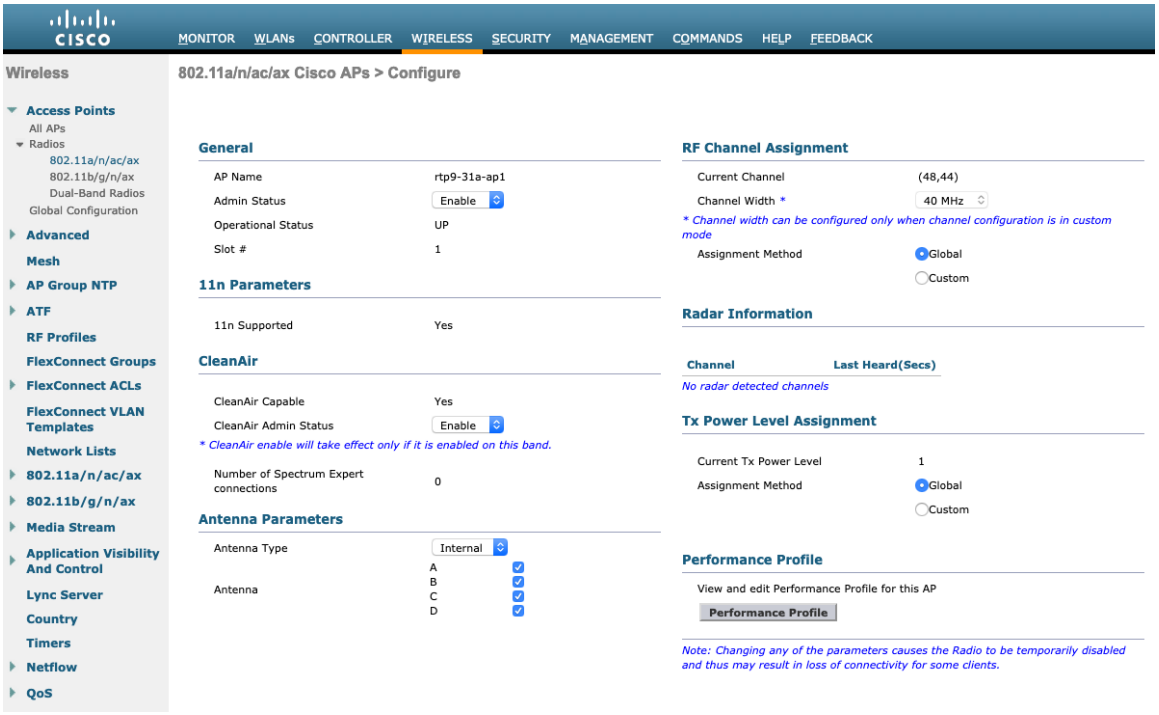
(Cisco Controller) >config 802.11b beamforming ap <ap_name> enable

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**

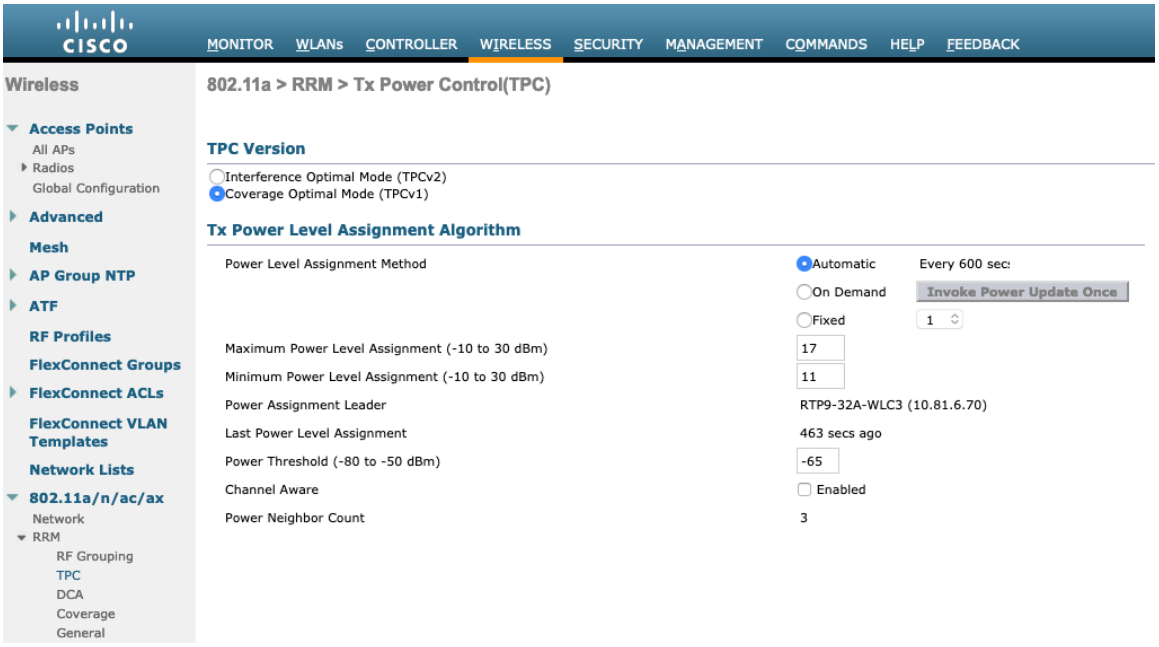


Auto RF (RRM)

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.

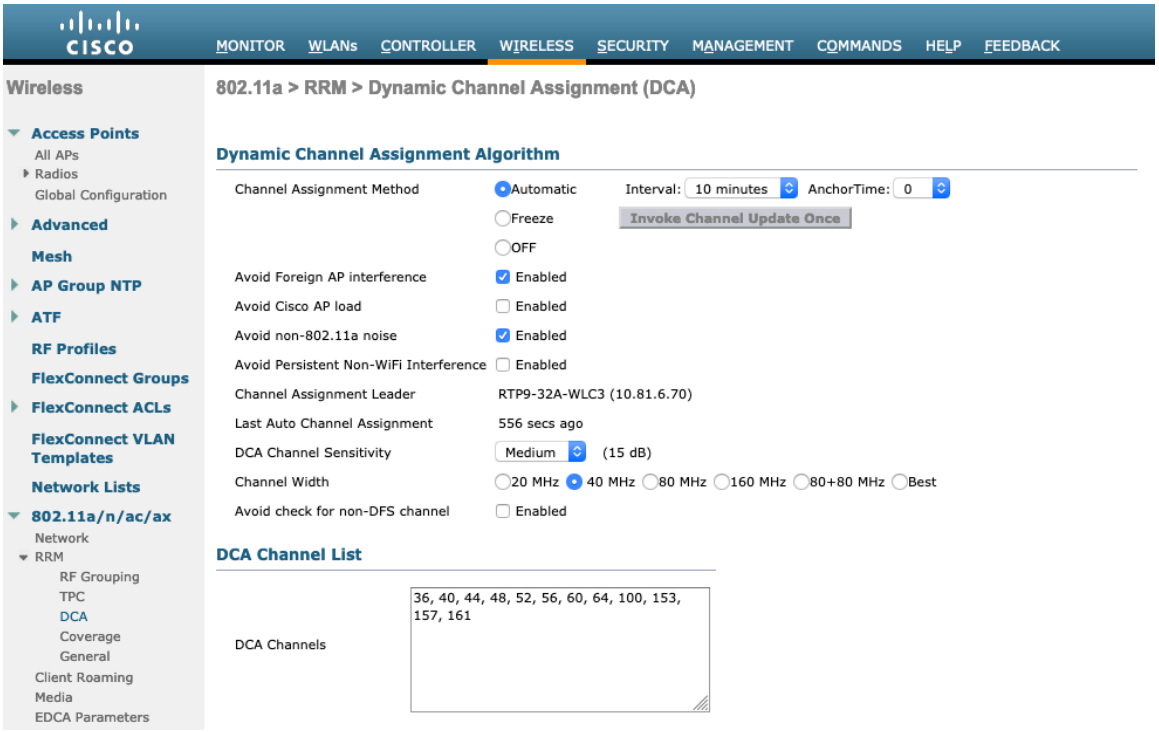
If using automatic power level assignment, a maximum and minimum power level can be specified.



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.

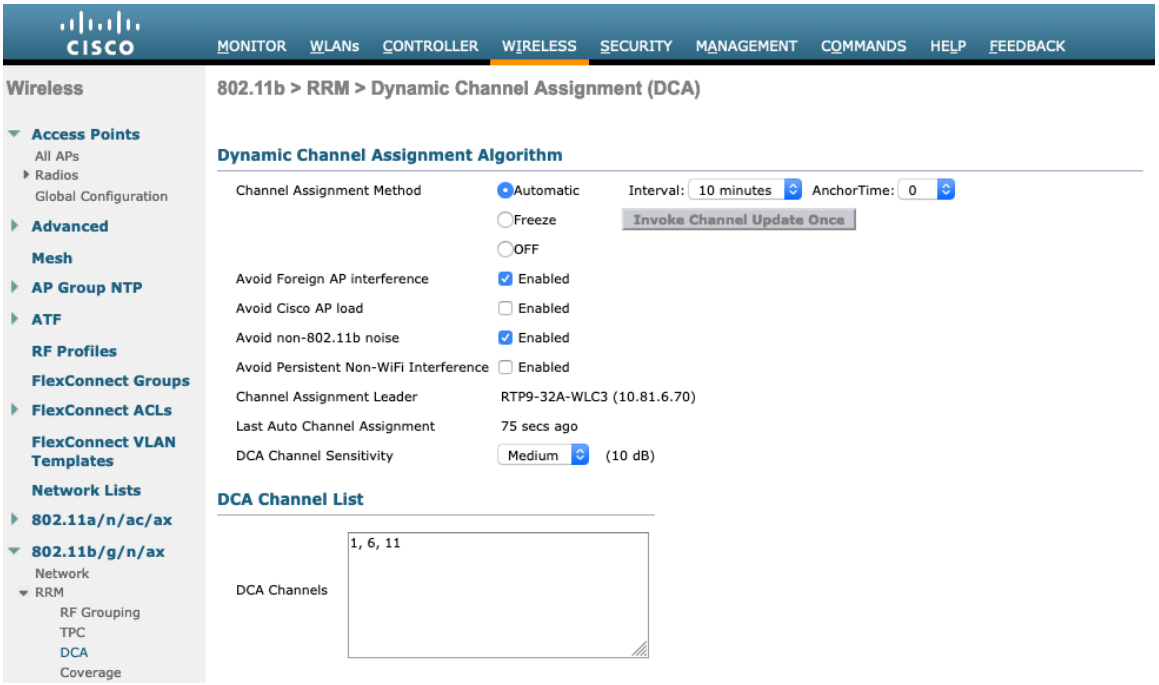
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

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.

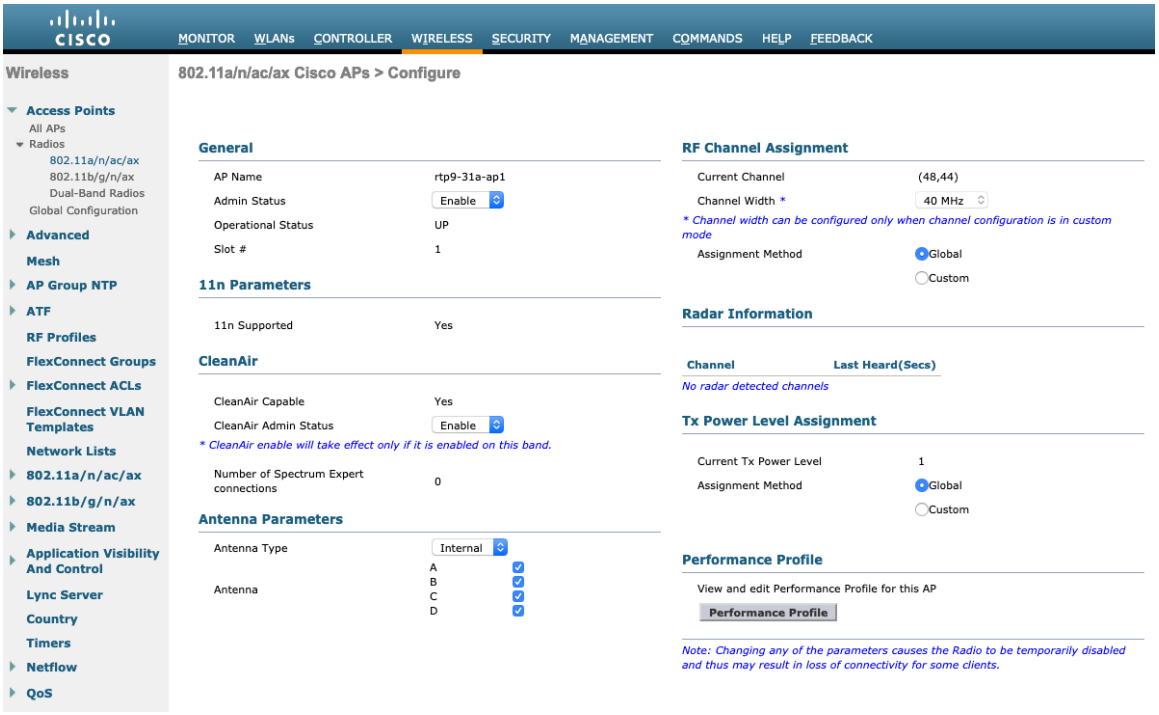
Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

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 IP Phone 8821 and 8821-EX 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.

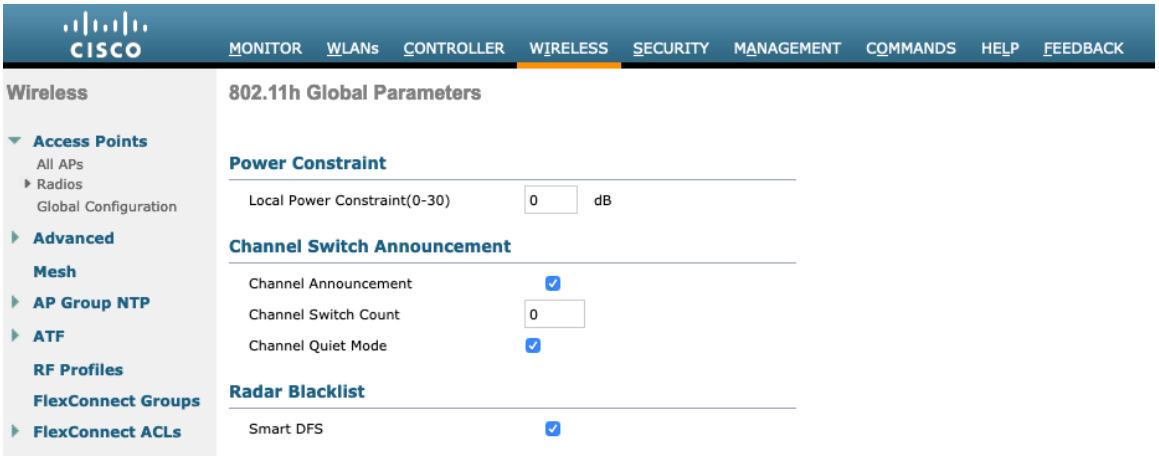
LLM is not supported on the Cisco 802.11n/ac Access Points.

DFS (802.11h)

Power Constraint should be left un-configured or set to 0 dB as DTPC will be used by the Cisco Wireless IP Phone 8821 and 8821-EX 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**.



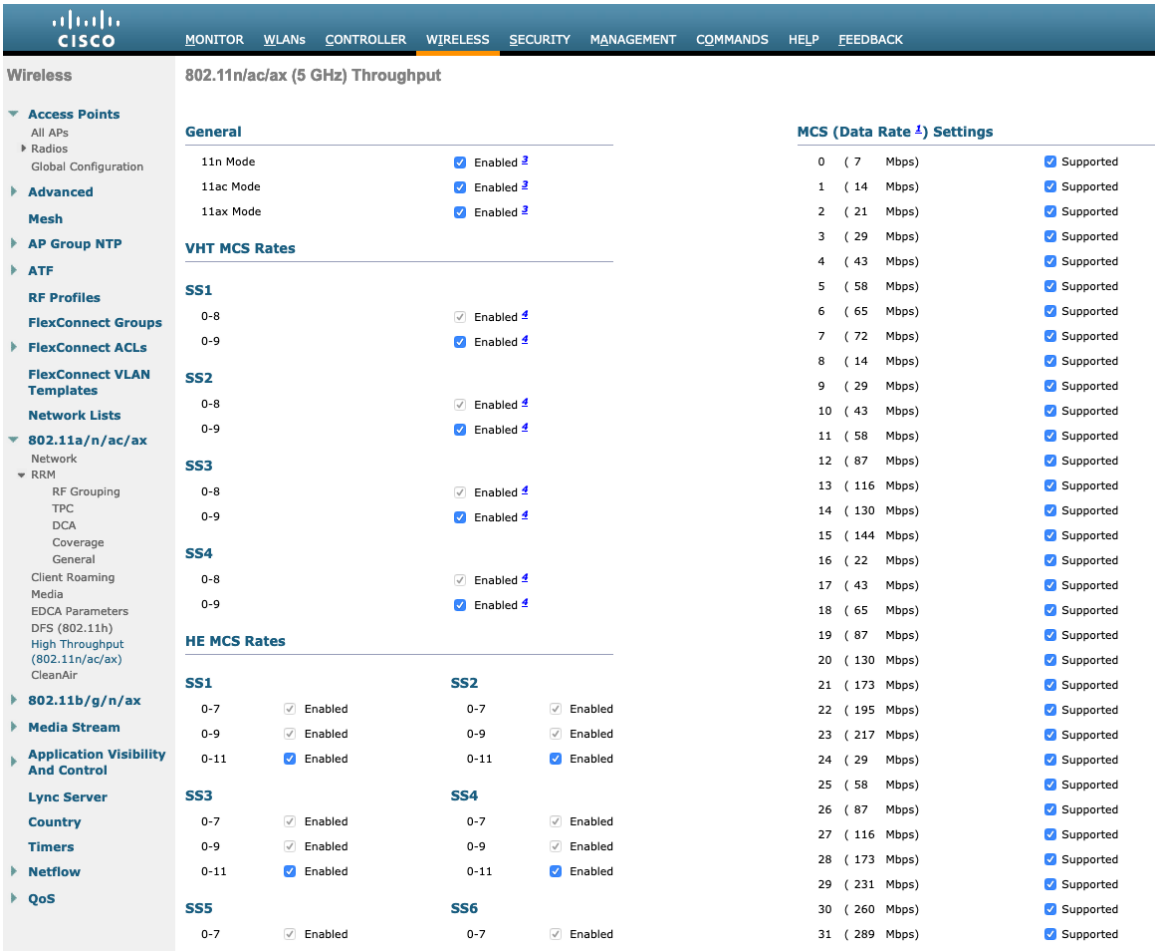
High Throughput (802.11n/ac)

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 IP Phone 8821 and 8821-EX support HT MCS 0 - MCS 7 and VHT MCS 0 - MCS 9 data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n/ac clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of those higher data rates.



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 IP Phone 8821 and 8821-EX.

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 IP Phone 8821 and 8821-EX 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

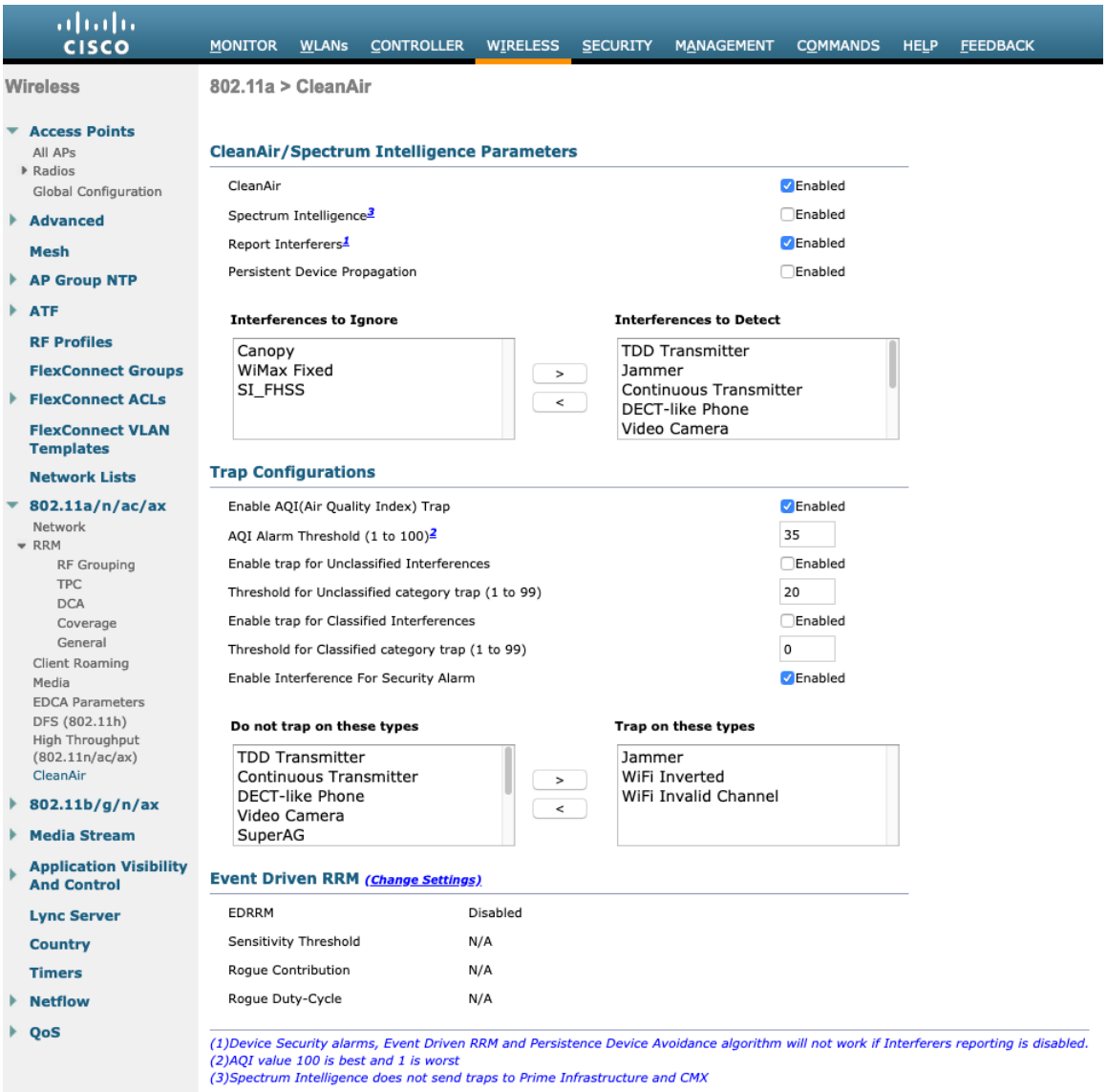
Priority 5..... Enabled

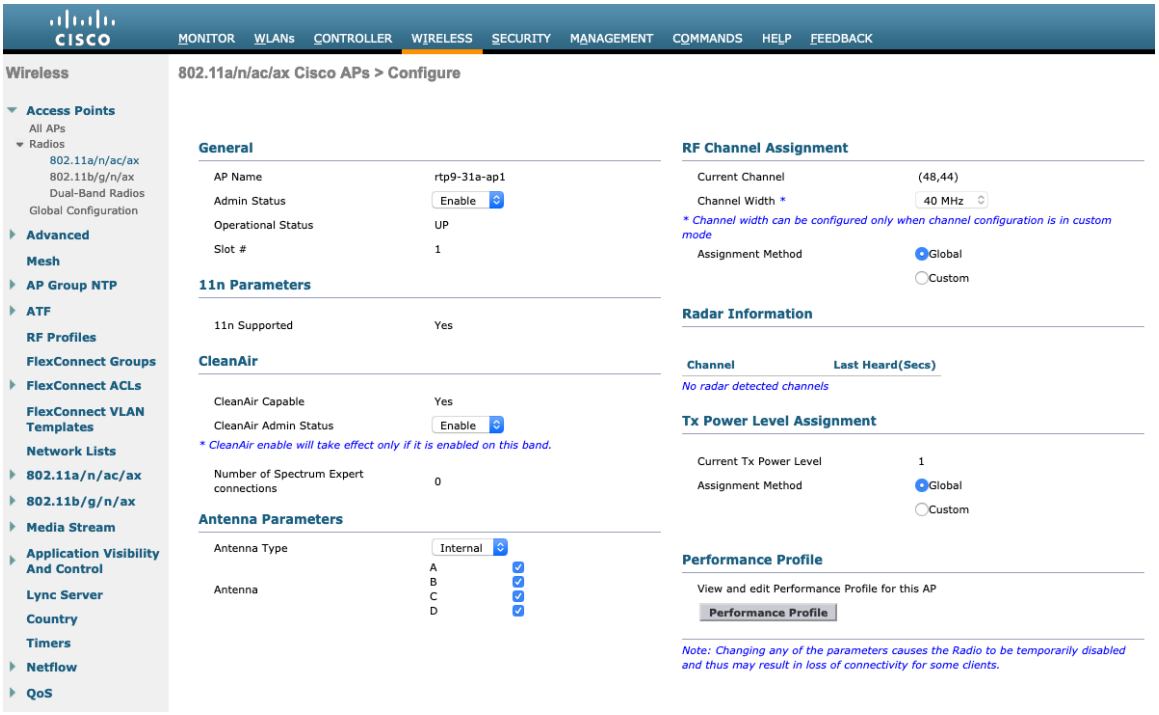
Priority 6..... Disabled

Priority 7..... Disabled

CleanAir

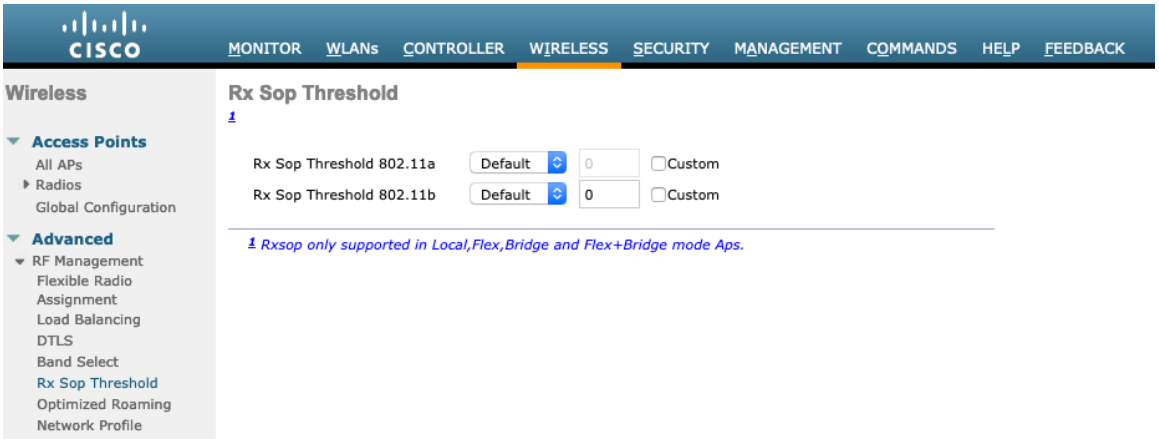
CleanAir should be **Enabled** when utilizing Cisco access points with CleanAir technology in order to detect any existing interferers.





Rx Sop Threshold

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



Note: It is important to note that adjusting **Rx SOP Threshold** may impact the interoperability of the Cisco Wireless IP Phone 8821 and 8821-EX with Cisco APs.

WLAN Settings

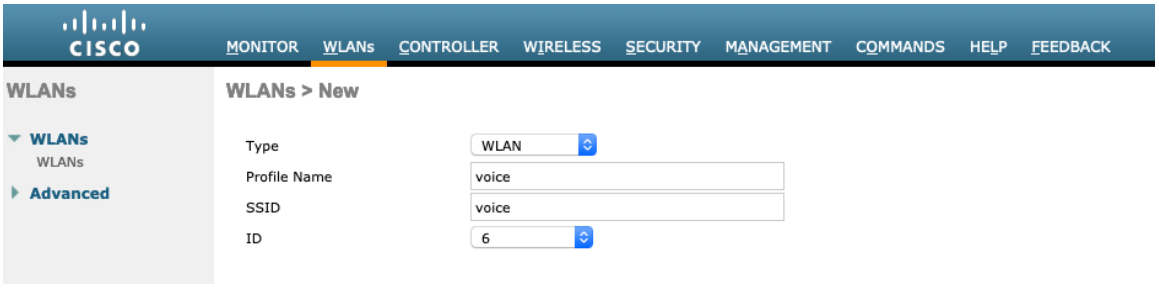
It is recommended to have a separate SSID for the Cisco Wireless IP Phone 8821 and 8821-EX.

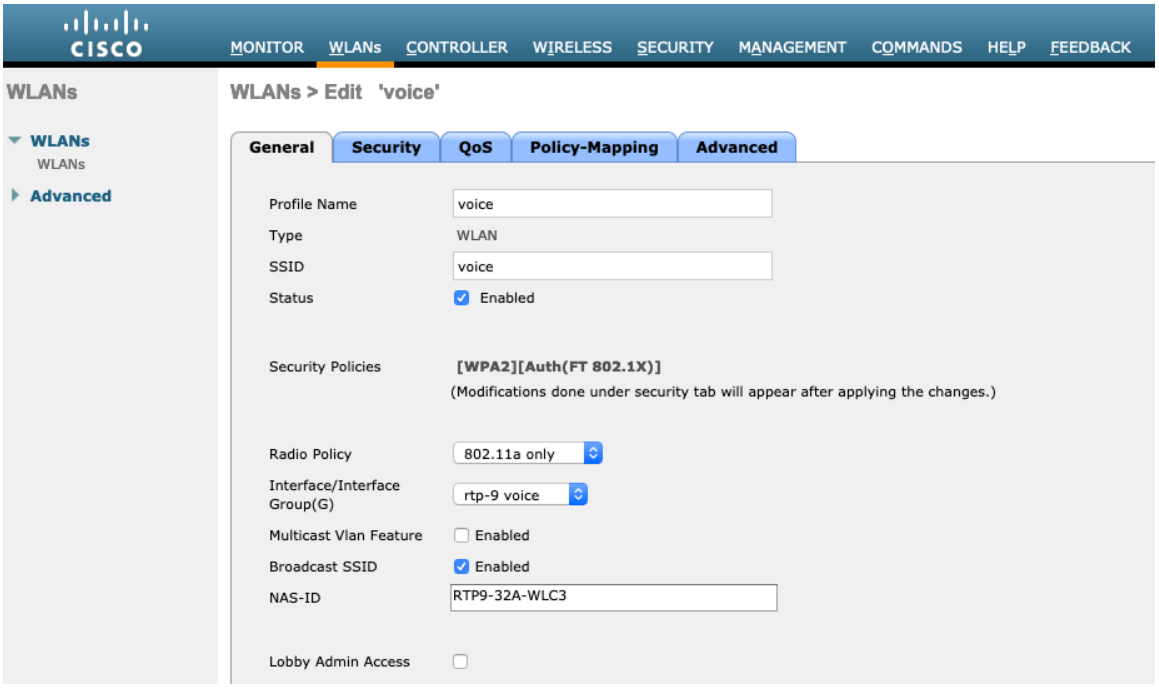
However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

The SSID to be used by the Cisco Wireless IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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.



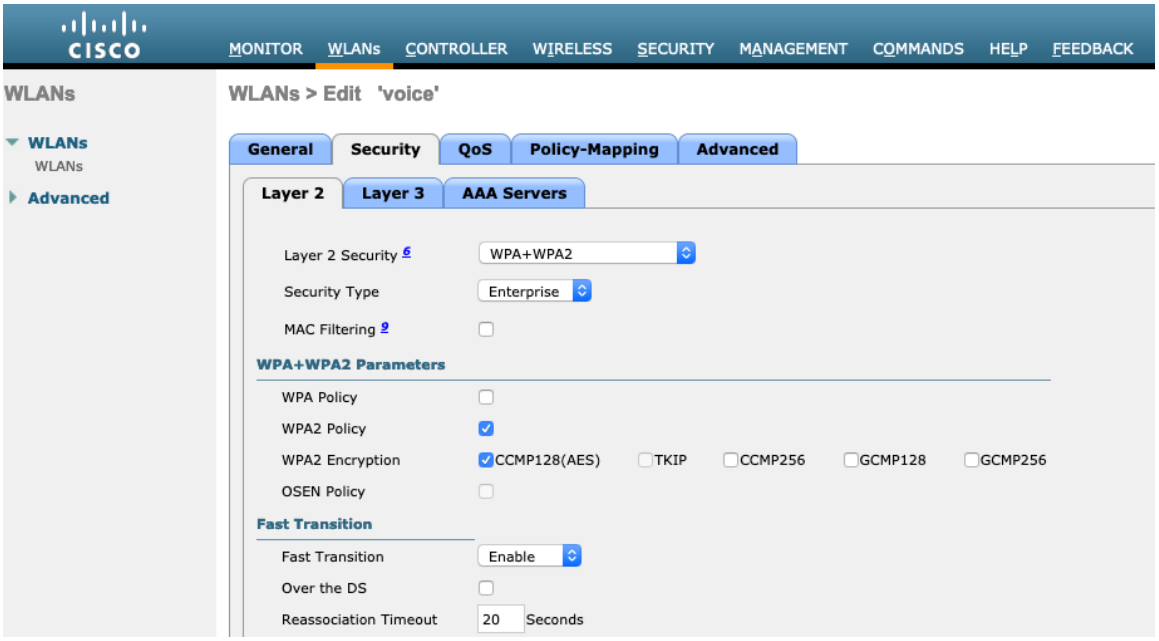


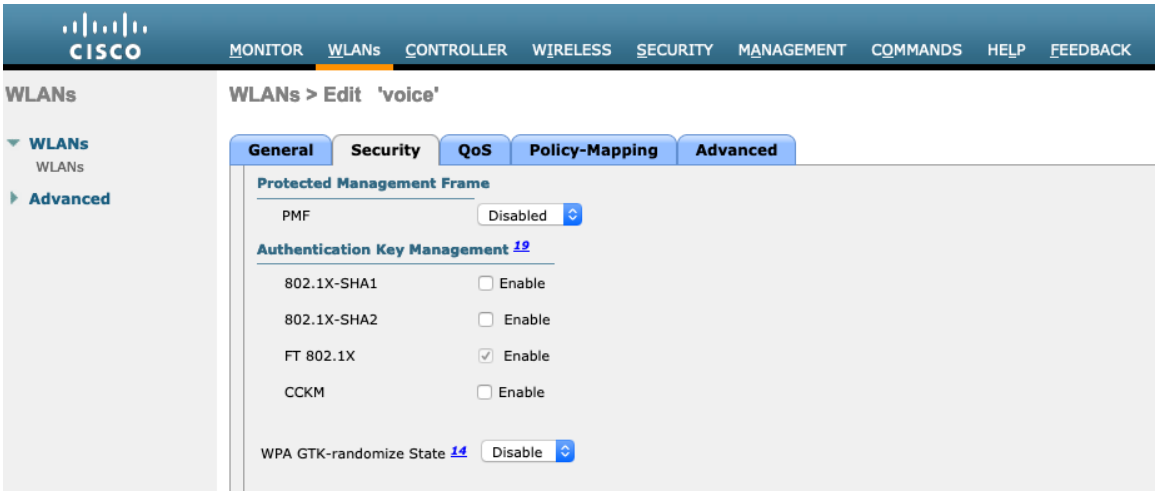
To utilize 802.11r (FT) for fast secure roaming, check the box to enable Fast Transition.

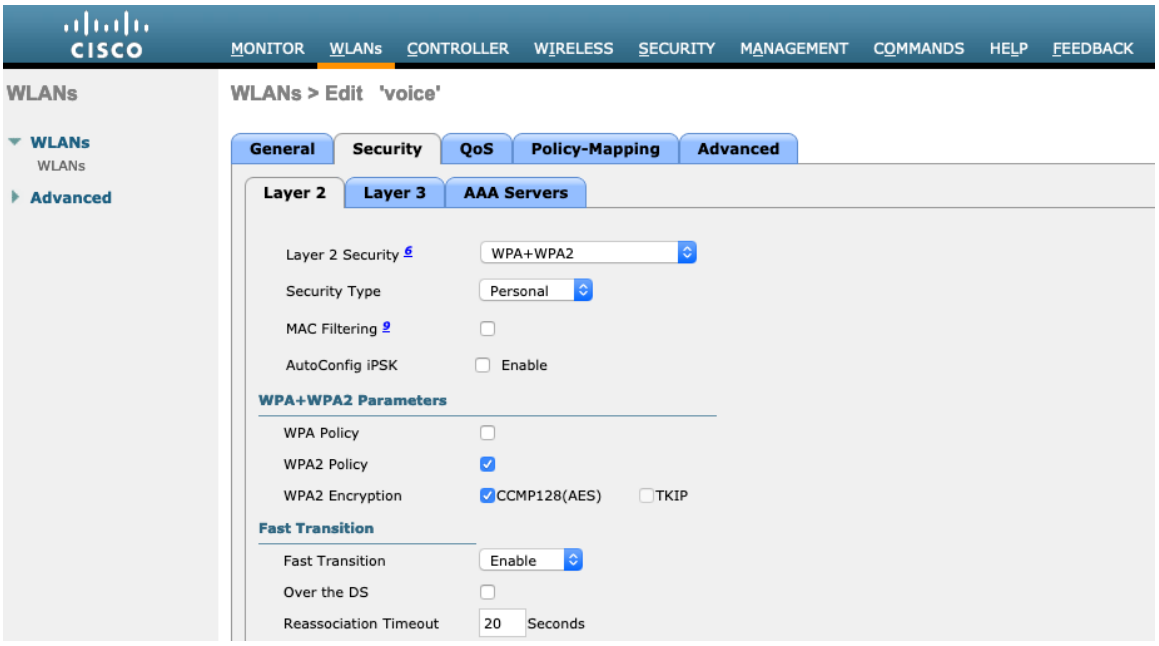
Is recommended to uncheck **Over the DS** to utilize the Over the Air method instead of the Over the Distribution System method.

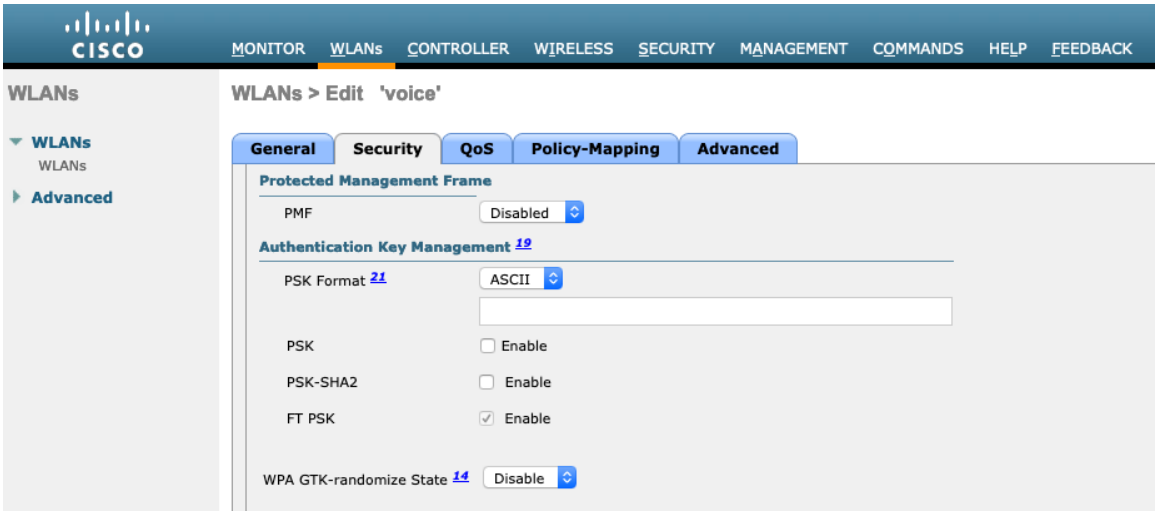
Protected Management Frame should be set to **Optional** or **Disabled.**

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.

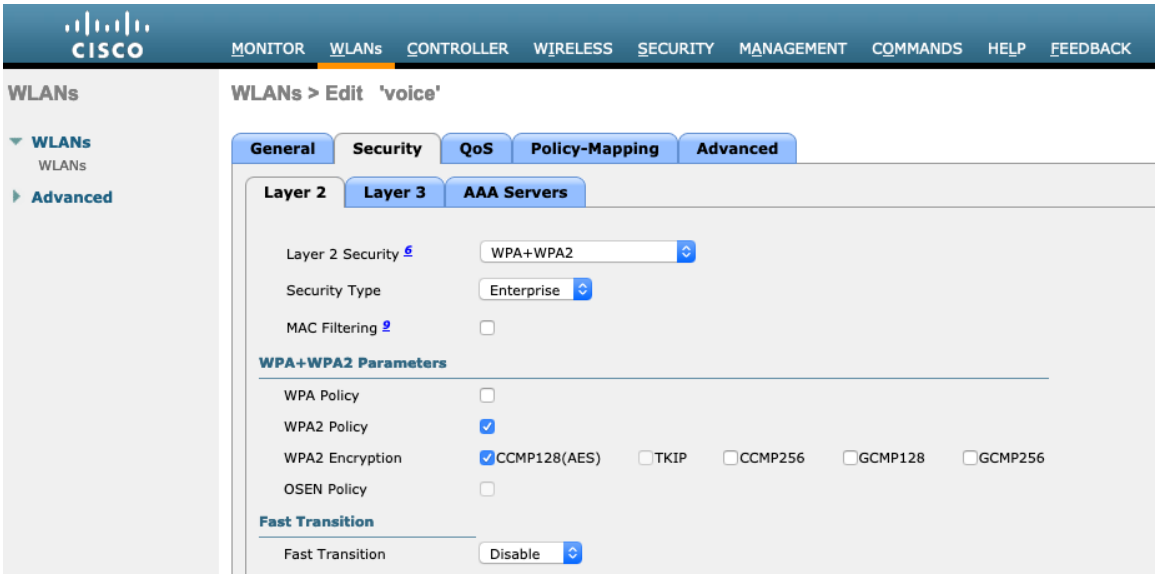

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'voice'
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security 6 WPA+WPA2
Security Type Enterprise
MAC Filtering 9
WPA+WPA2 Parameters
WPA Policy
WPA2 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.



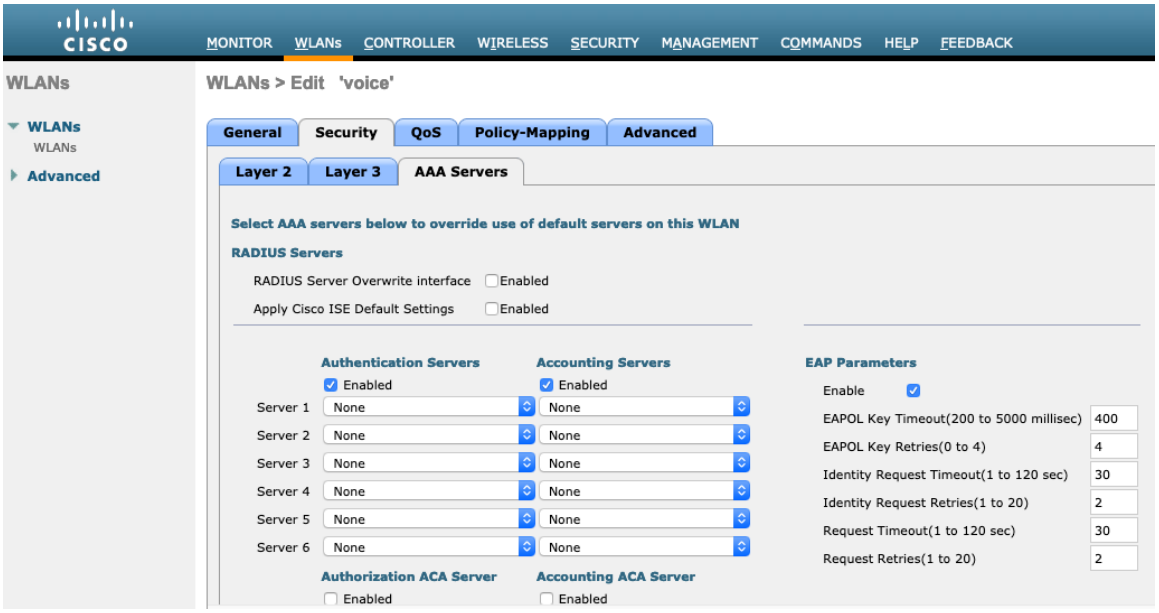
802.1x, CCKM and/or PSK may also be enabled if wanting to utilize the same SSID for various type of voice clients, where some clients do not support 802.11r (FT) depending on whether 802.1x or PSK is being utilized.

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.

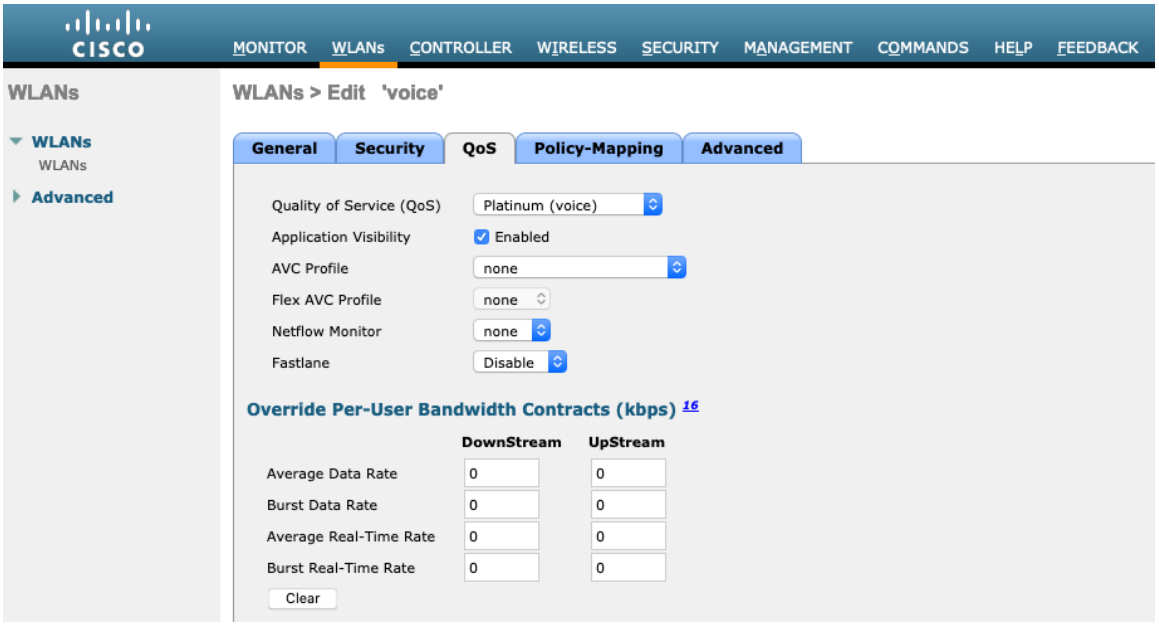


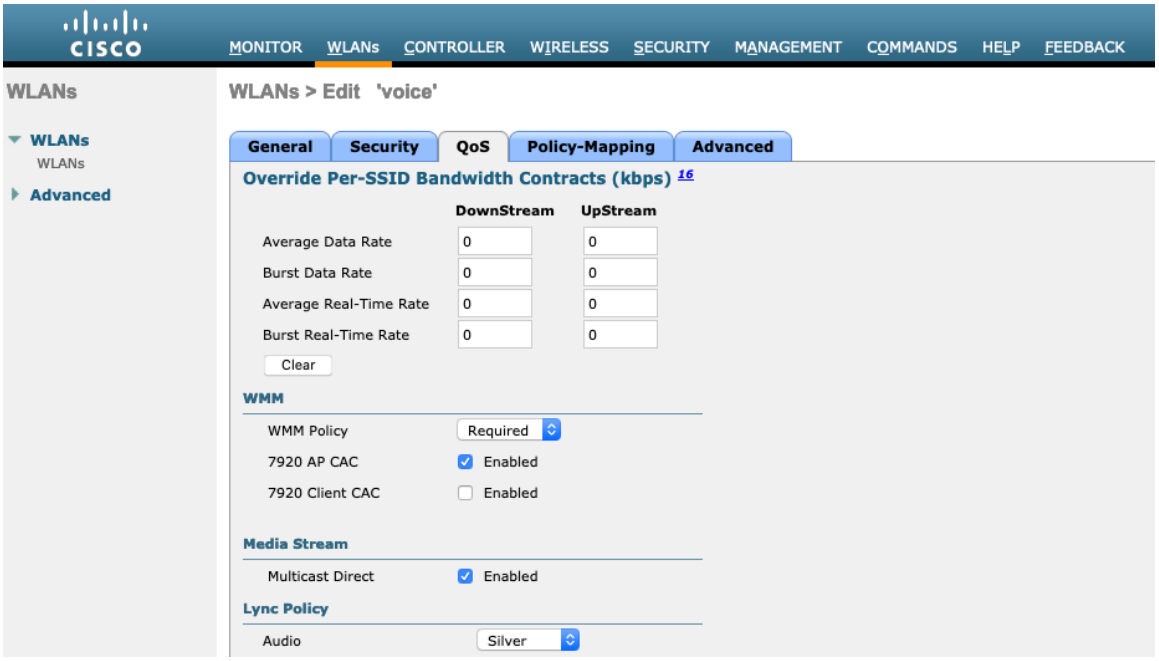
The WMM policy should be set to **Required** only if the Cisco Wireless IP Phone 8821 and 8821-EX or other WMM enabled phones will be using this SSID.

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 IP Phone 8821 and 8821-EX, 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.

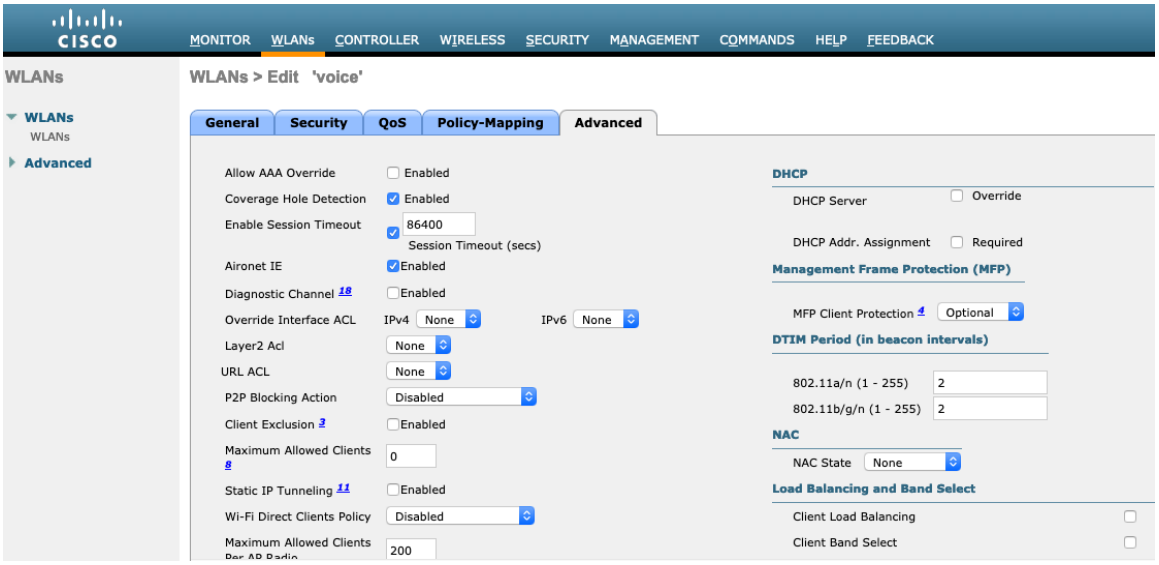
Management Frame Protection should be set to **Optional** or **Disabled.**

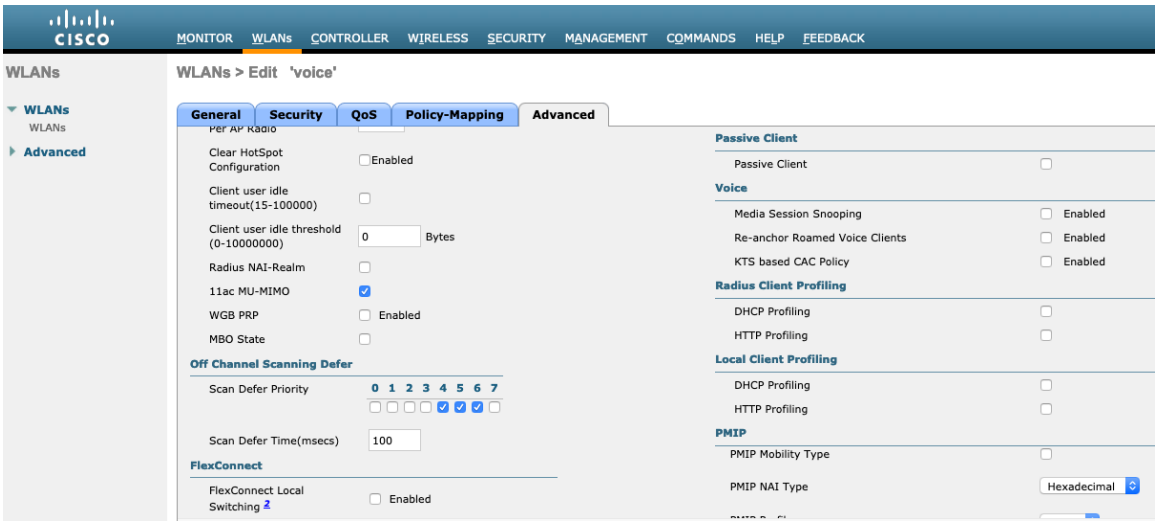
Use a **DTIM Period** of **2** with a beacon period of **100 ms**.

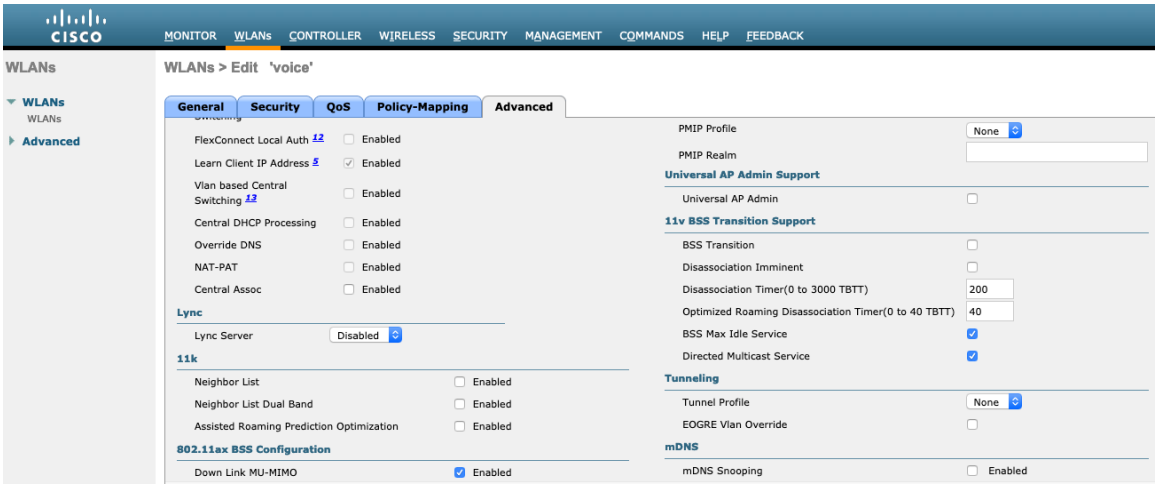
Ensure **Client Load Balancing** and **Client Band Select** are disabled.

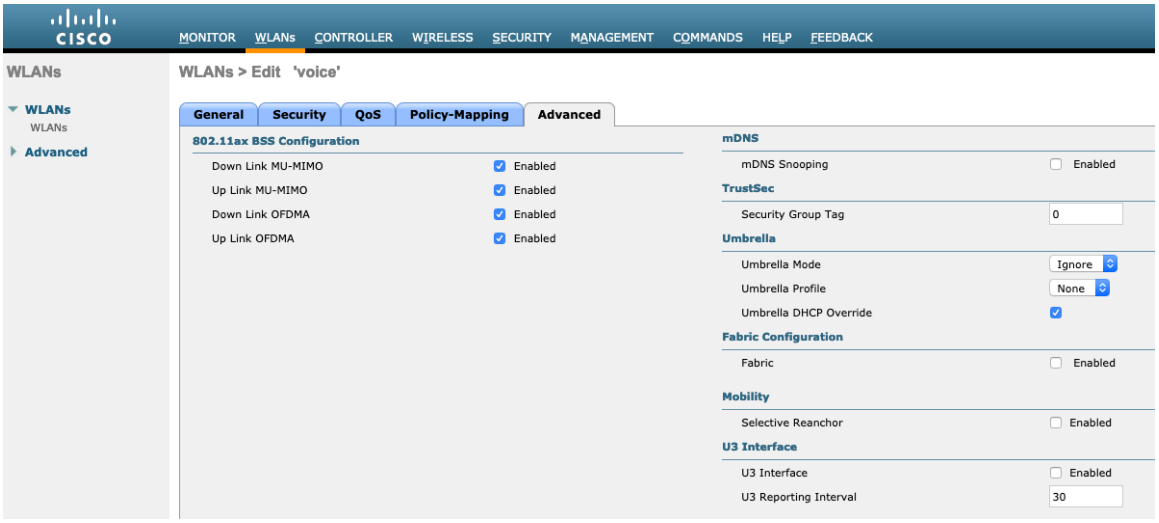
It is recommended to set **Re-anchor Roamed Voice Clients** to disabled as this can cause brief interruptions with wireless LAN connectivity when a call is terminated after performing an inter-controller roaming.

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



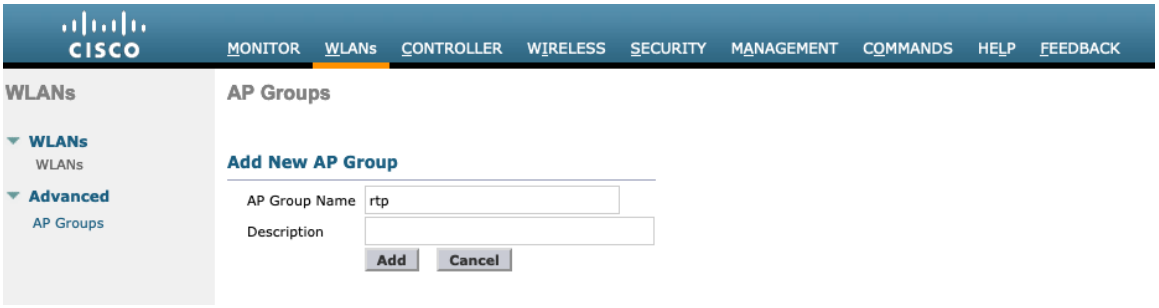


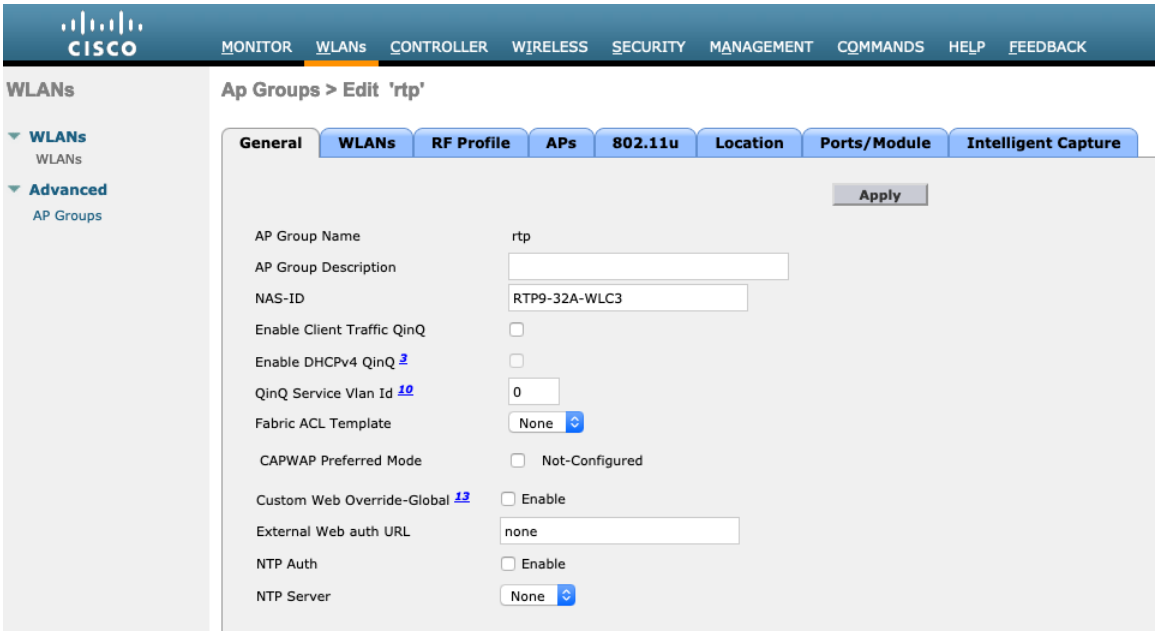




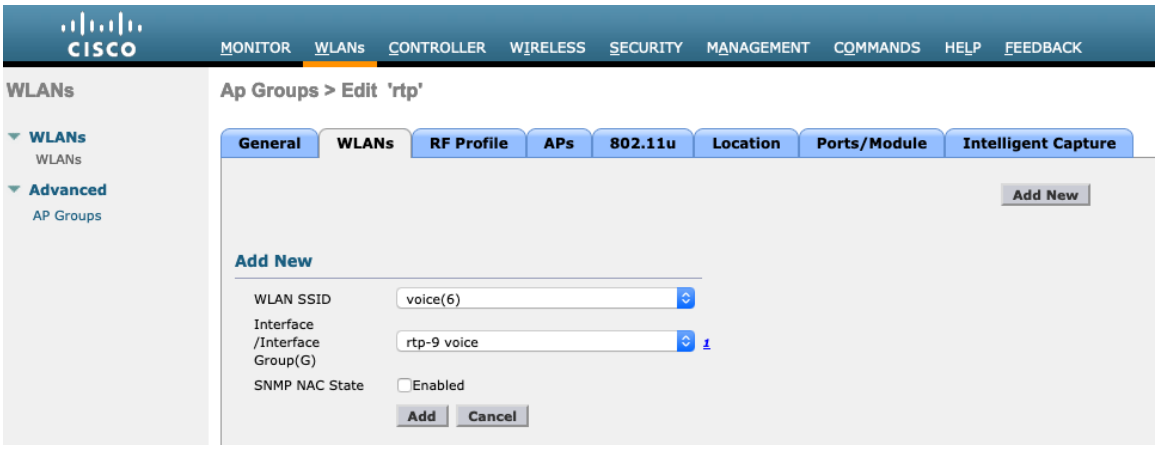
AP Groups

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.



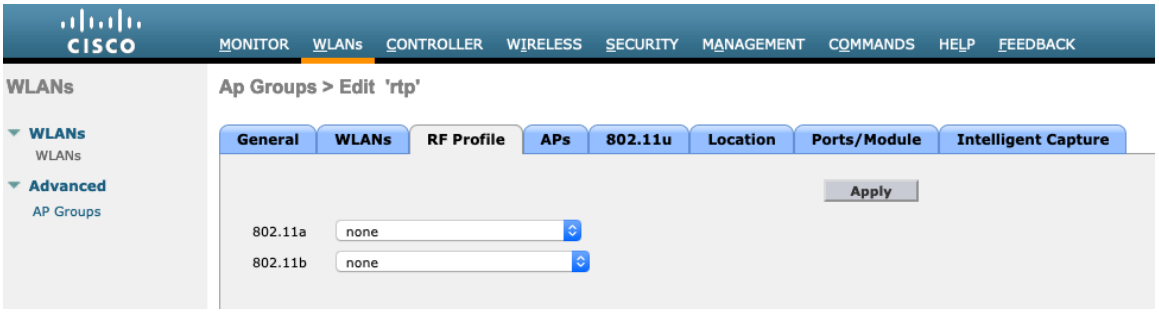


On the **WLANs** tab, select the desired SSIDs and interfaces to map to then select **Add**.



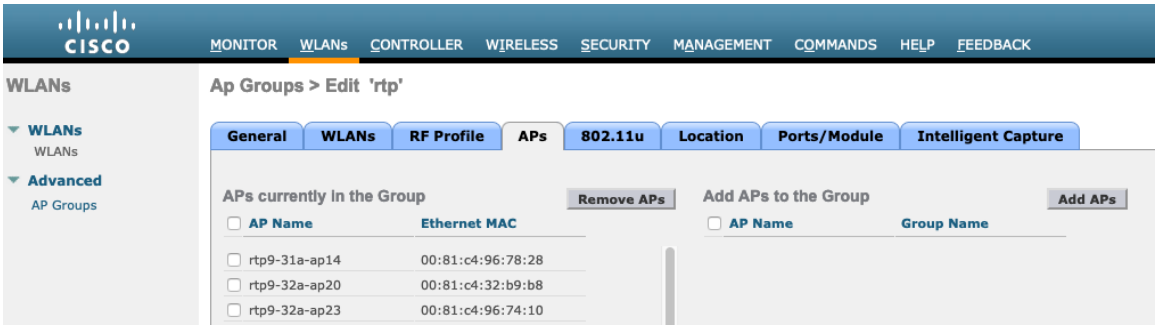
On the **RF Profile** tab, select the desired 802.11a or 802.11b RF Profile, then select **Apply**.

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.

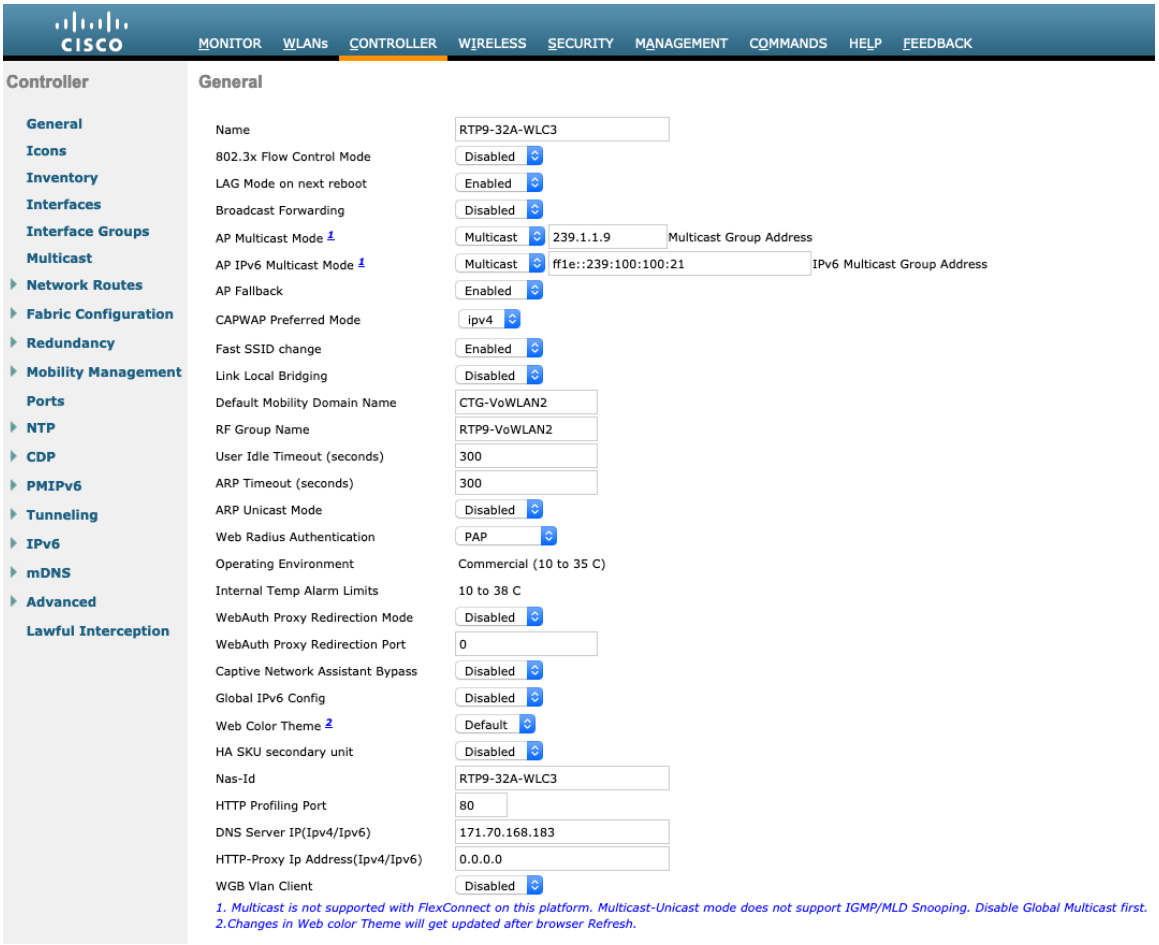


Controller Settings

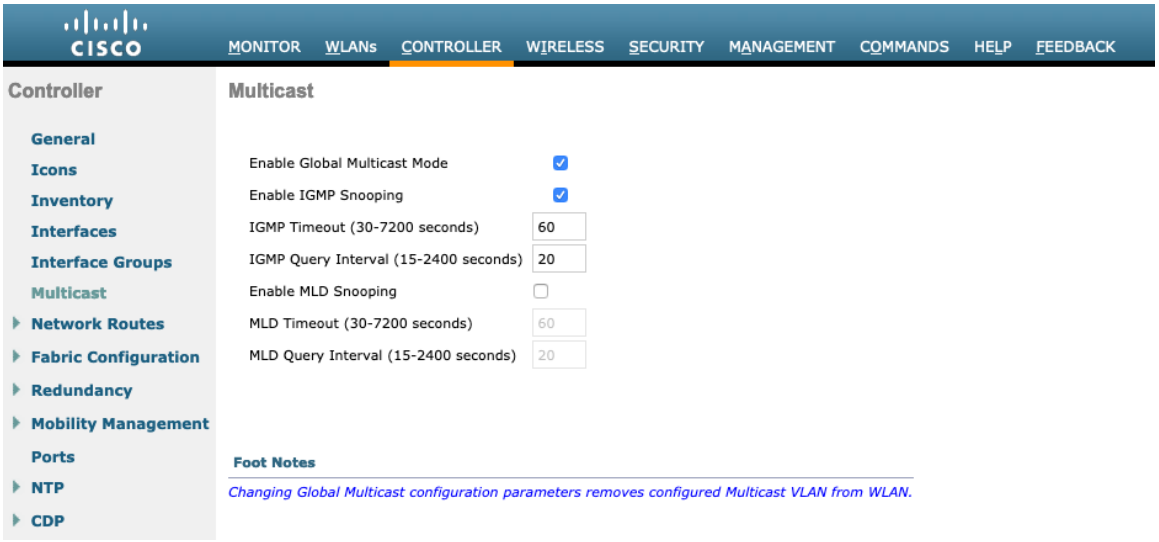
Ensure the Cisco Wireless LAN Controller hostname is configured correctly.

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

Configure the desired AP multicast mode.

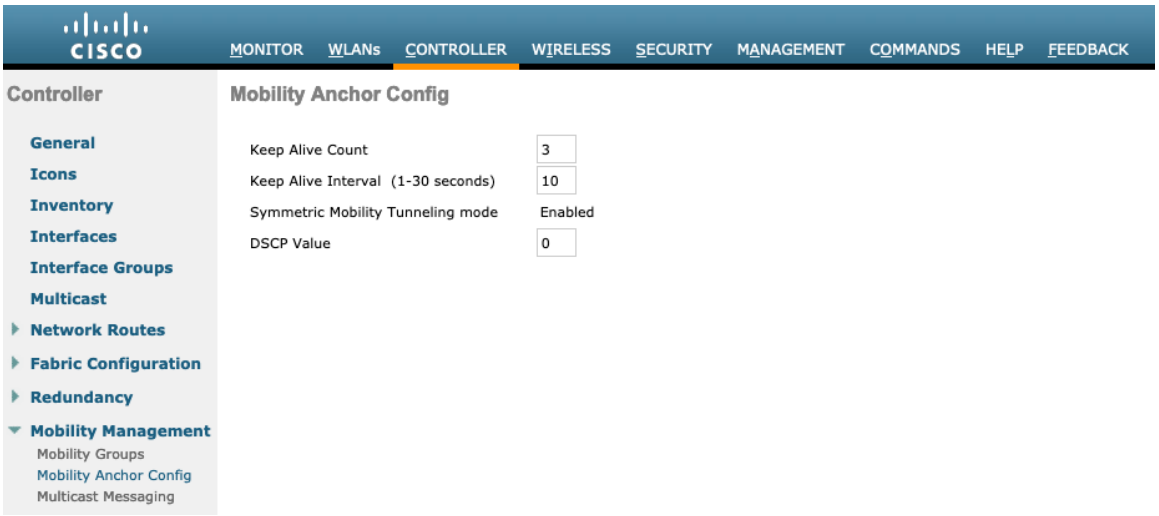


If utilizing multicast, then **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be enabled.

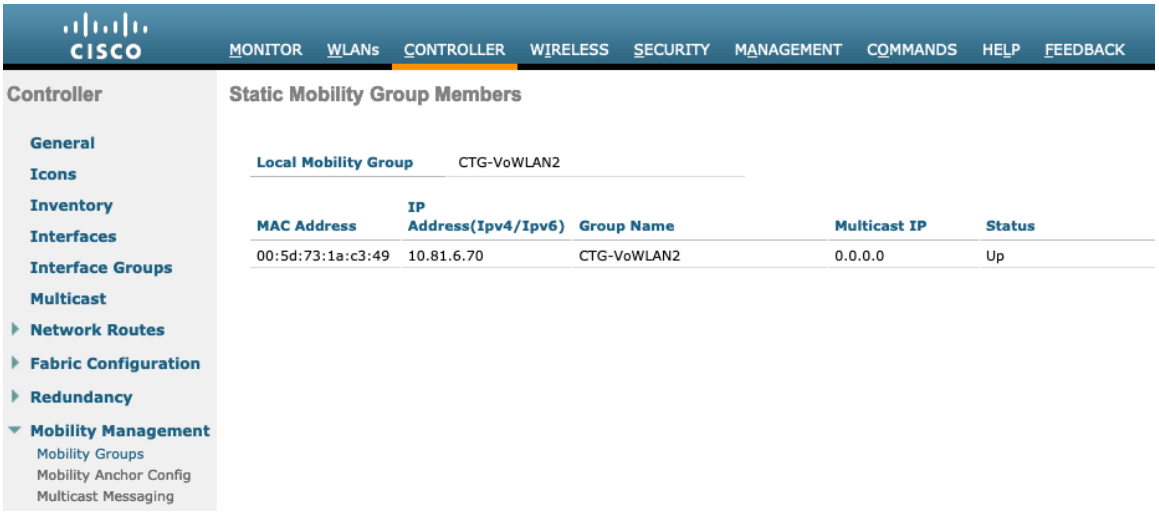


If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling** should be **Enabled**.

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)

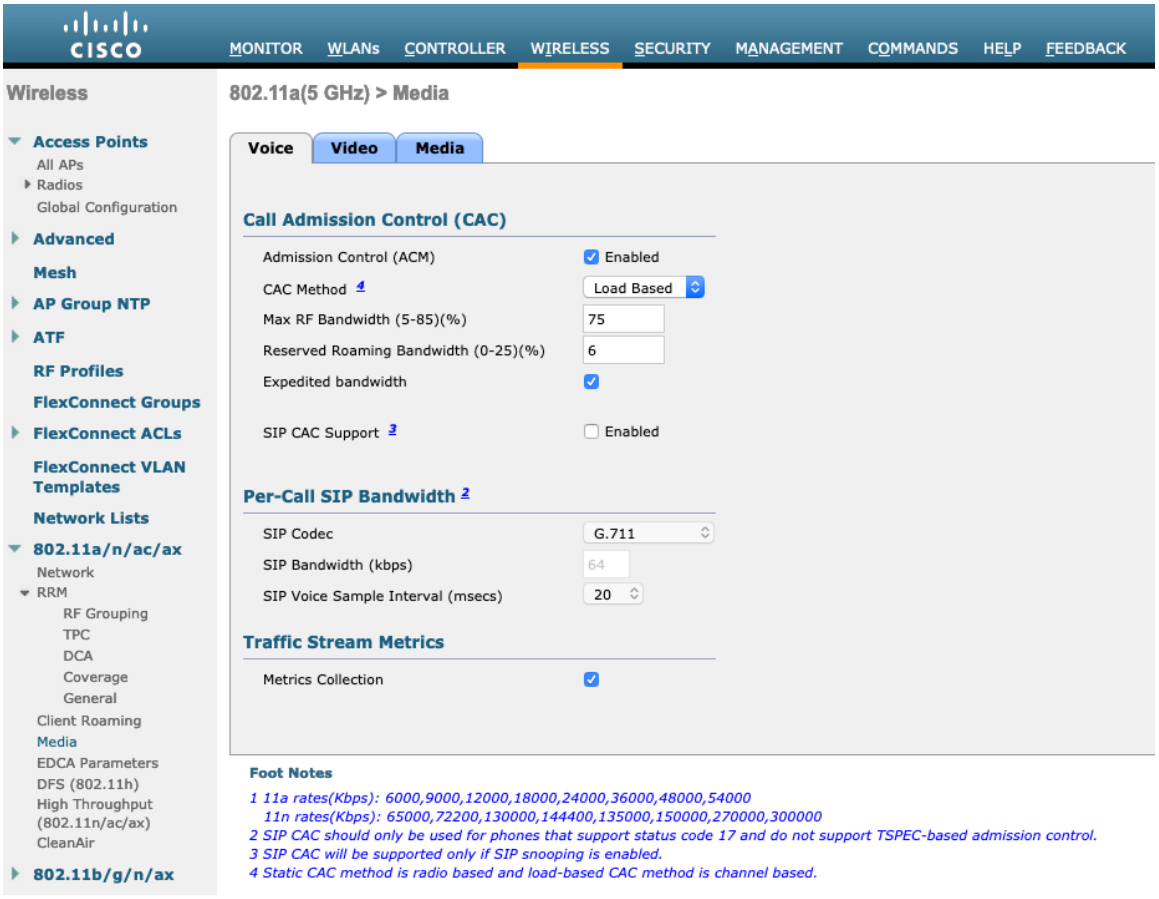
It is recommended to enable **Admission Control Mandatory** for **Voice** and configure the maximum bandwidth and reserved roaming bandwidth percentages for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

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

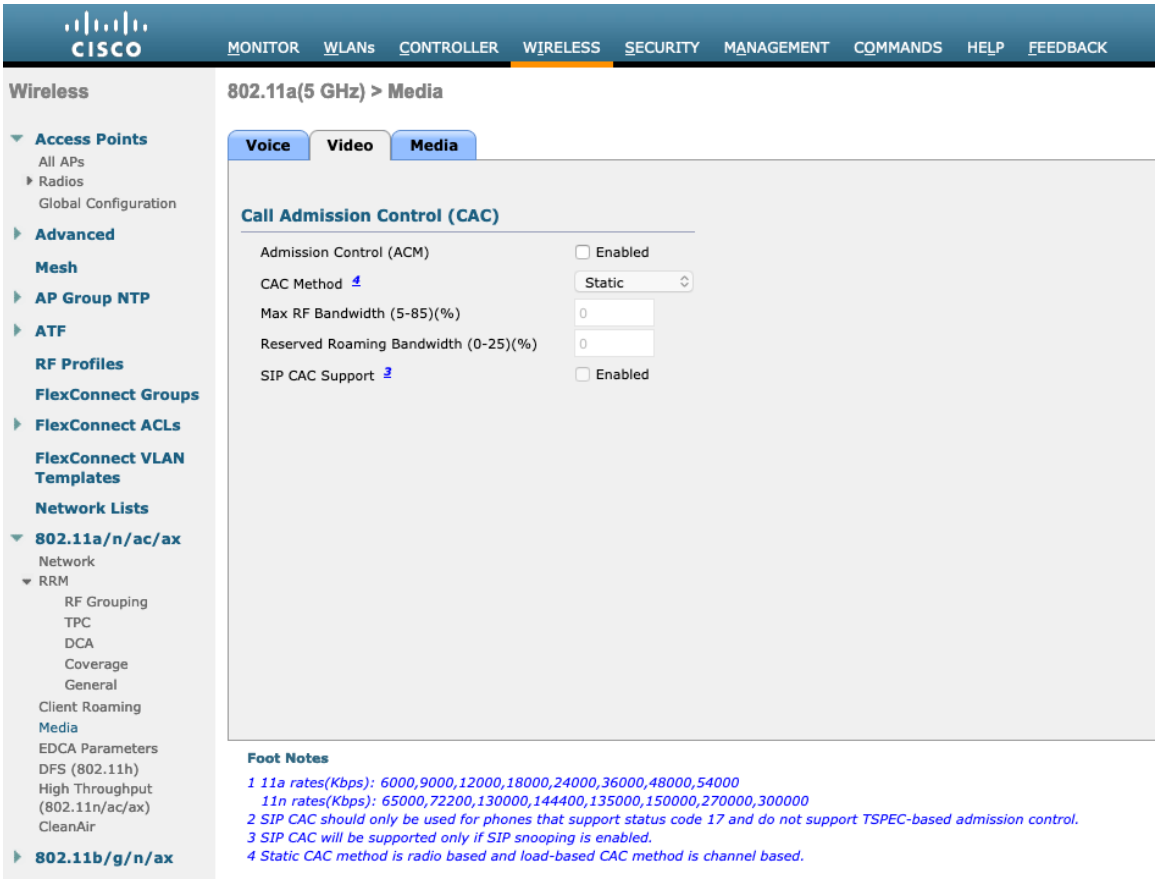
Roaming clients are not limited to using the reserved roaming bandwidth, but roaming bandwidth is to reserve some bandwidth for roaming clients in case all other bandwidth is utilized.

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

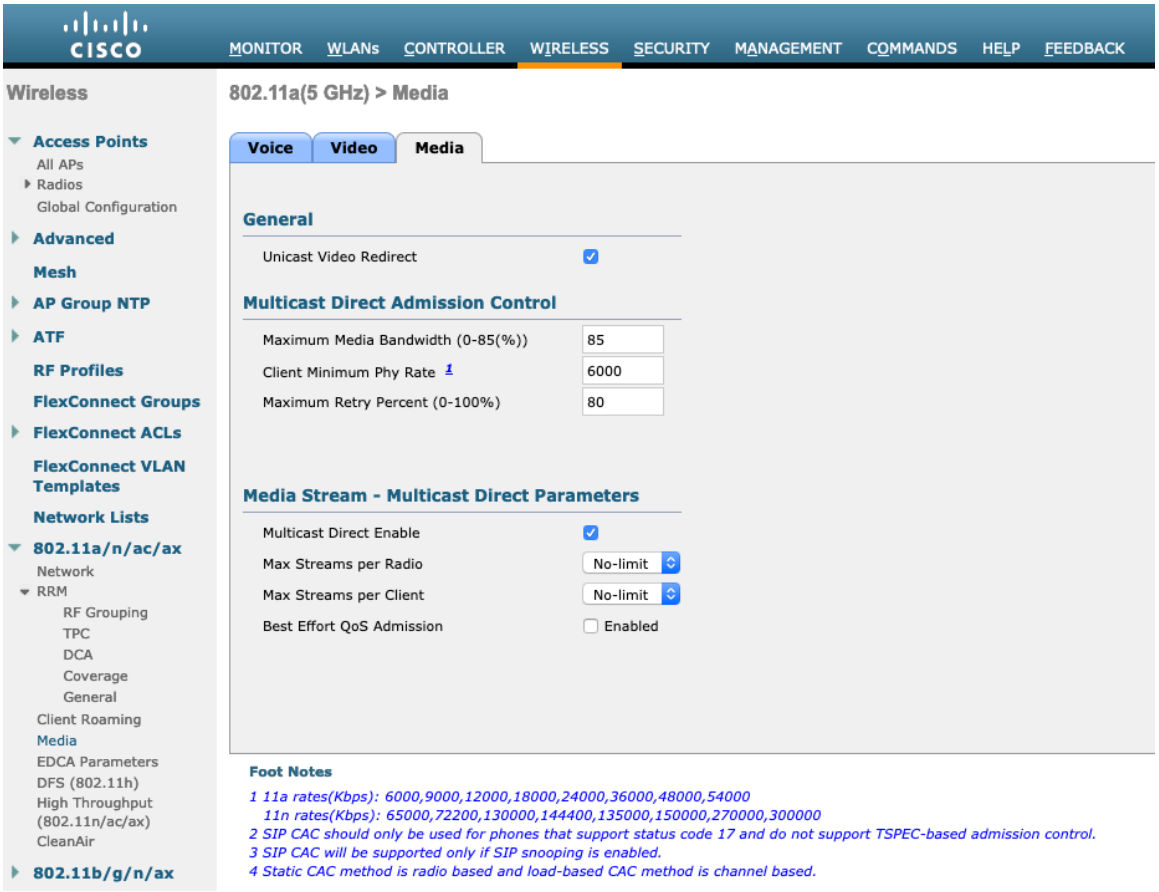
Dot11-Phone Mode (7920)..... ap-cac-limit
Wired Protocol..... None

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

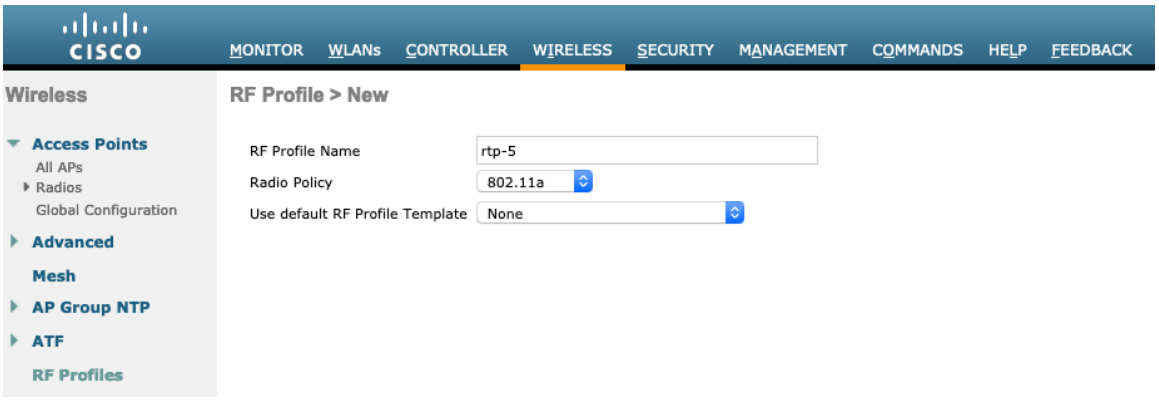
RF Profiles can be created to specify which frequency bands, data rates, RRM settings, etc. a group of access points should use.

It is recommended to have the SSID used by the Cisco Wireless IP Phone 8821 and 8821-EX to be applied to 5 GHz radios only.

RF Profiles are applied to an AP group once created.

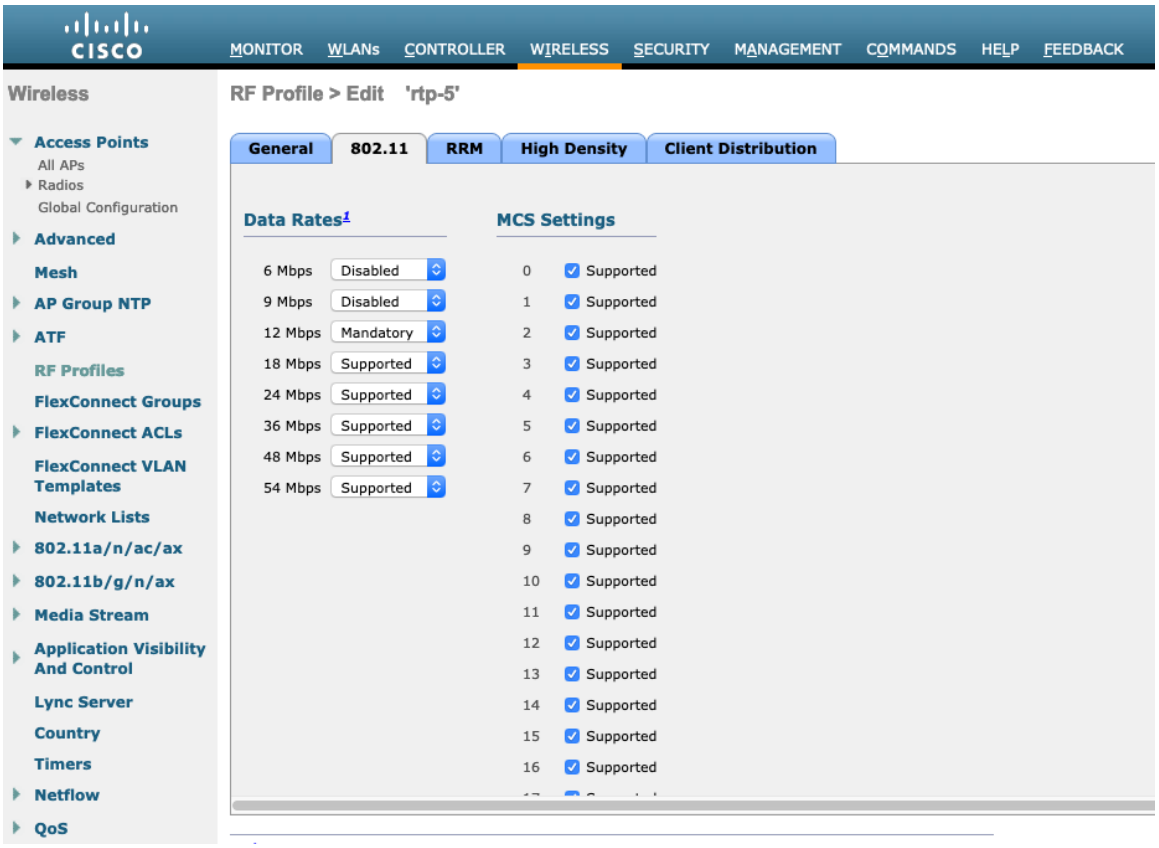
When creating an RF Profile, the **RF Profile Name** and **Radio Policy** must be defined.

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

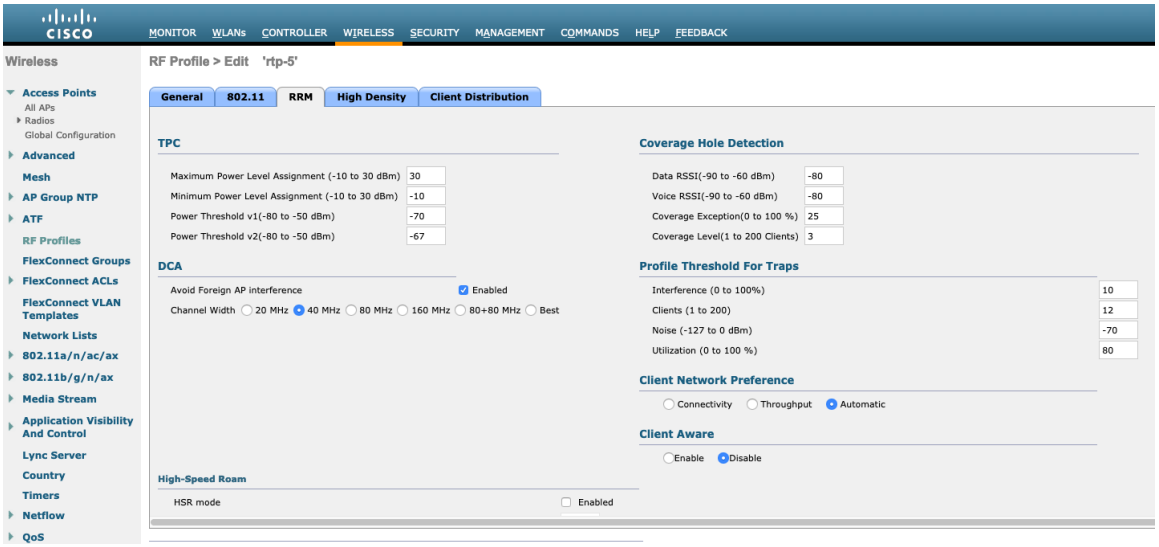


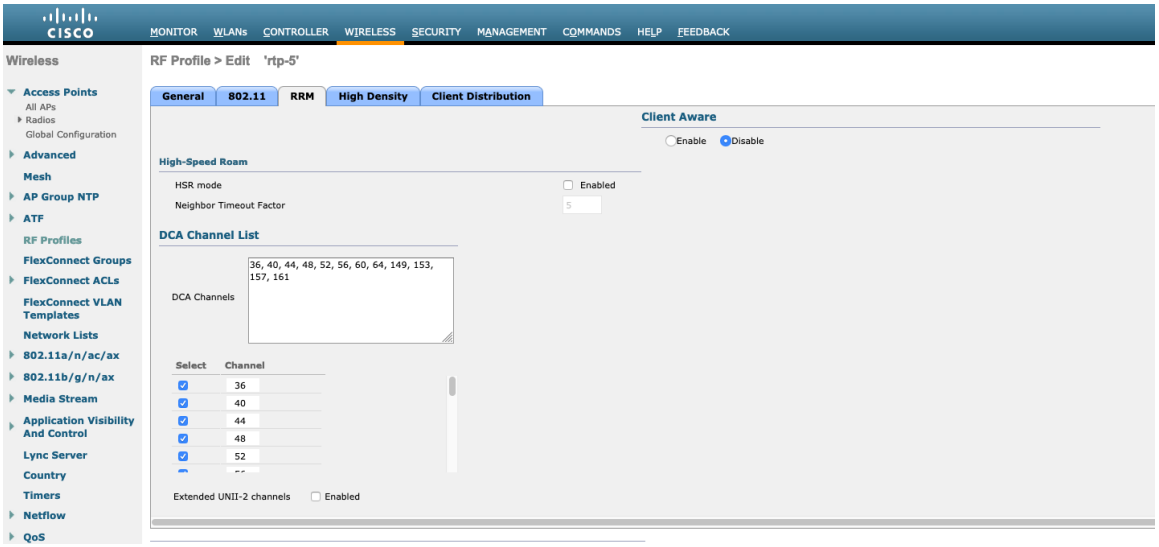
On the **802.11** tab, configure the data rates as desired.

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.



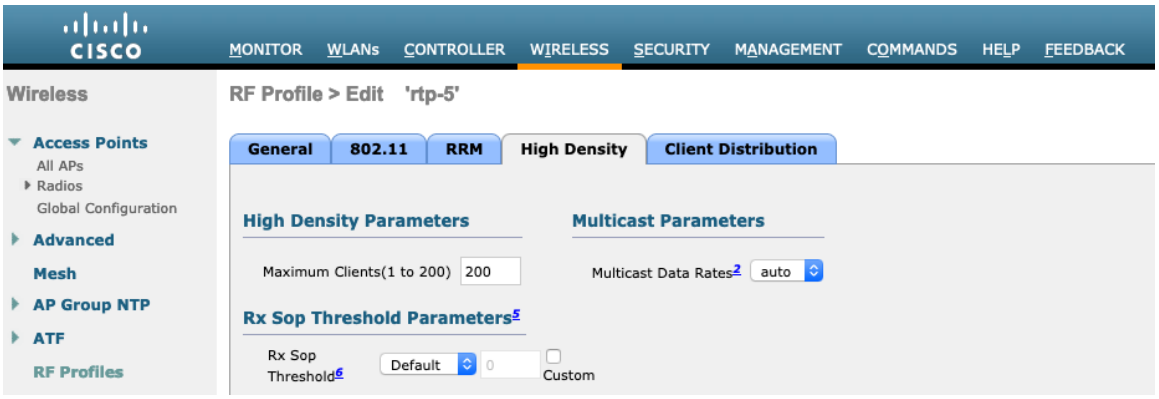
On the **RRM** tab, the **Maximum Power Level Assignment** and **Minimum Power Level Assignment** settings as well as other **DCA**, **TPC**, and **Coverage Hole Detection** settings can be configured.





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**.

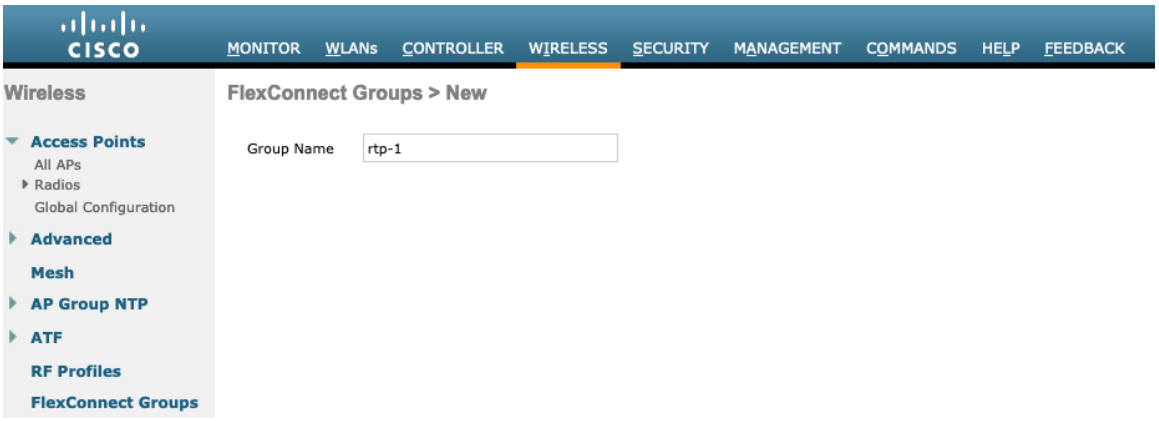


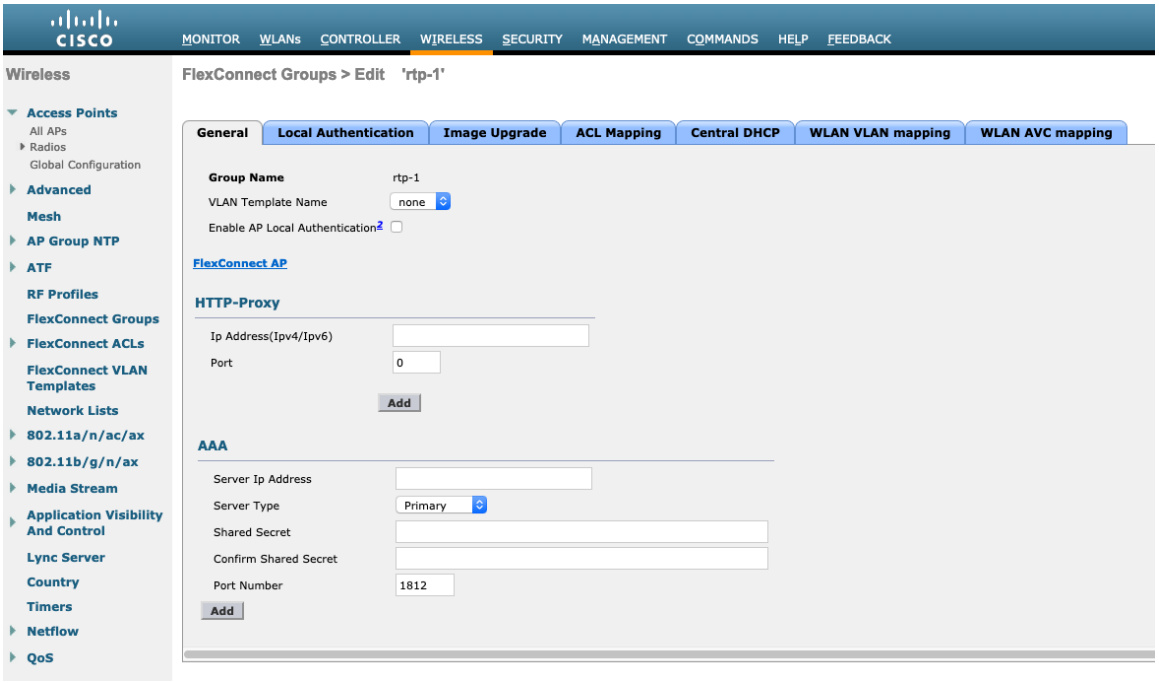
Note: It is important to note that adjusting **Rx SOP Threshold** may impact the interoperability of the Cisco Wireless IP Phone 8821 and 8821-EX with Cisco APs.

FlexConnect Groups

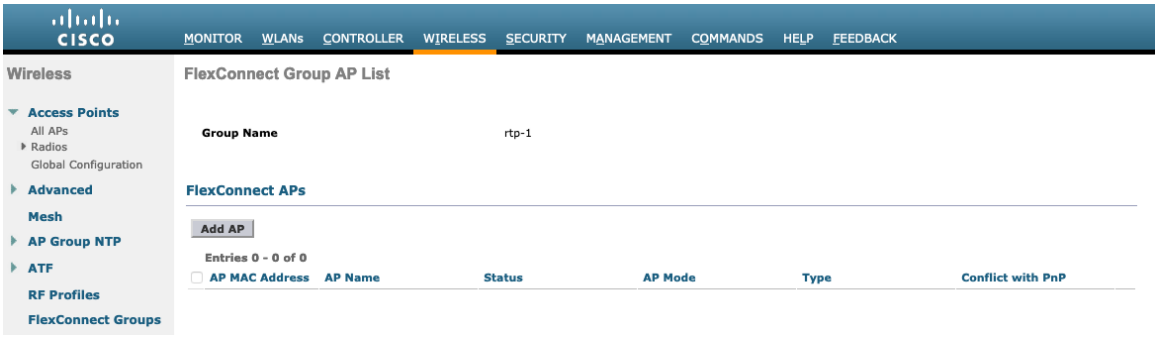
All access points configured for FlexConnect mode need to be added to a FlexConnect Group.

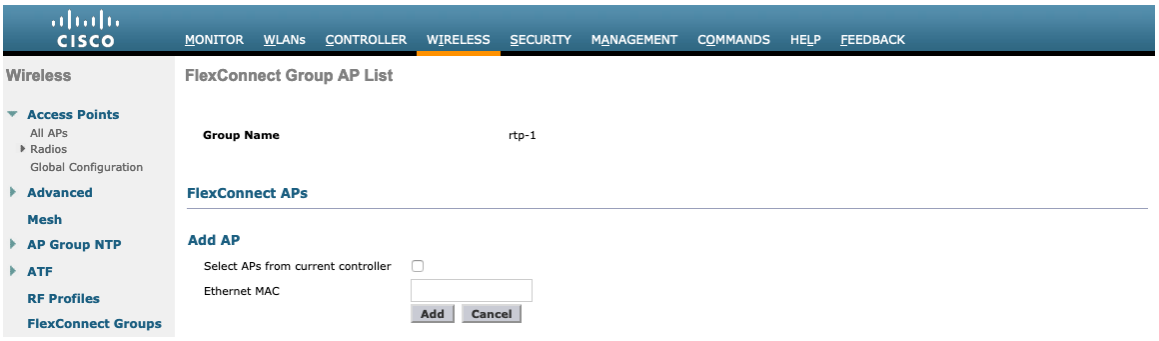
If utilizing 802.11r (FT) or CCKM, then seamless roams can only occur when roaming to access points within the same FlexConnect Group.





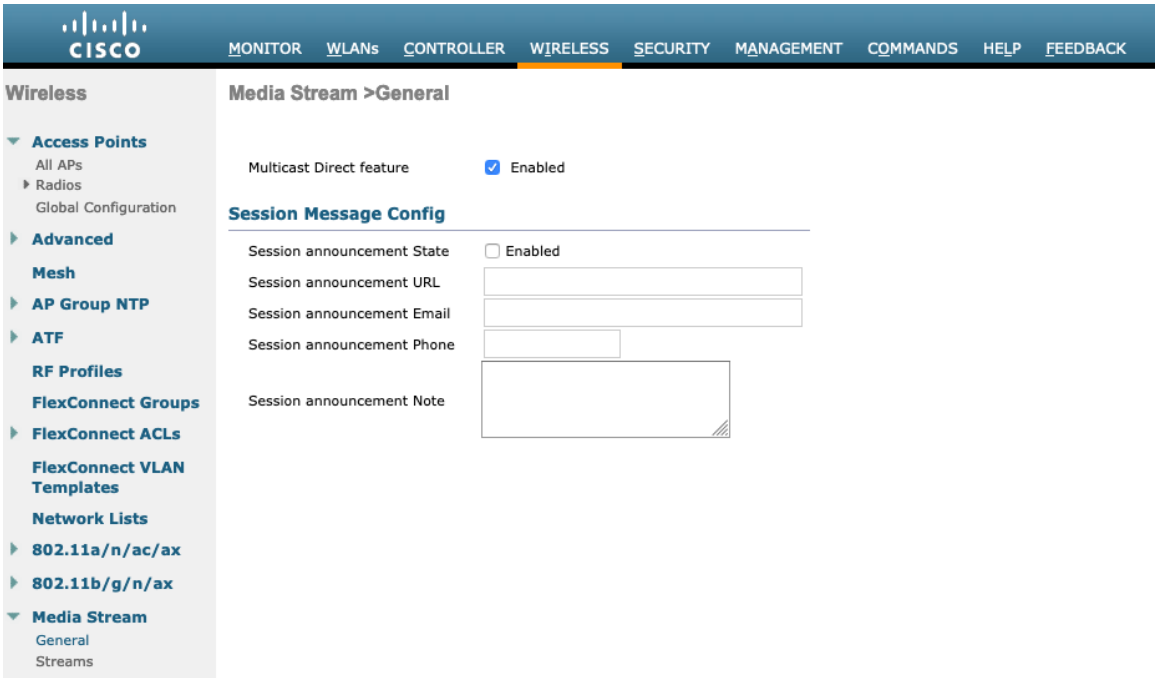
The maximum number of access points allowed per FlexConnect Group is limited, which is WLC model specific.



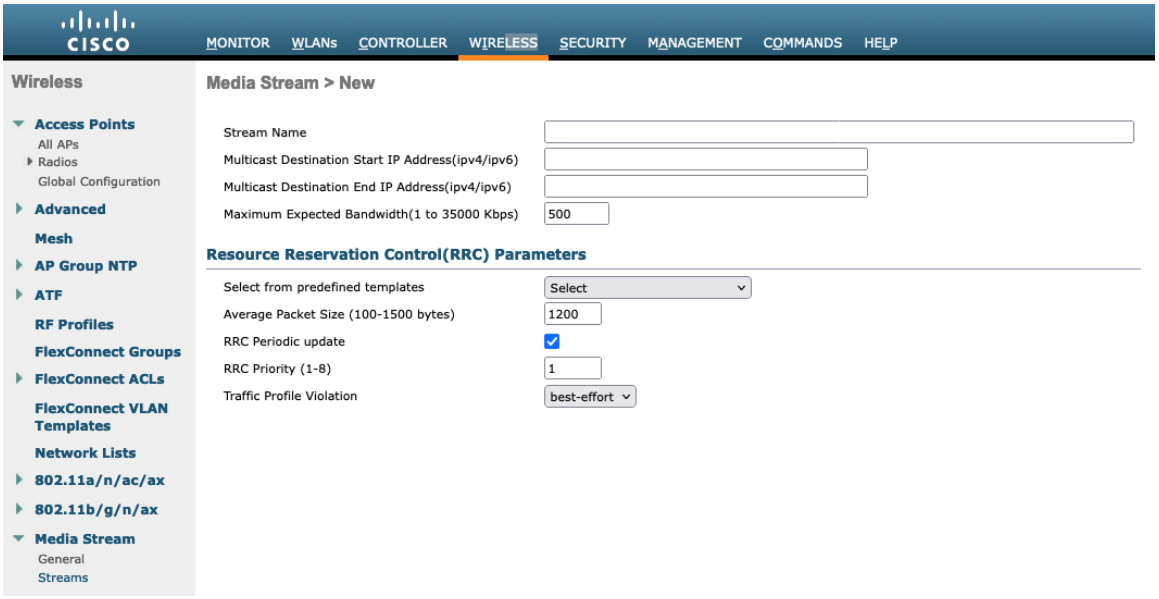


Multicast Direct

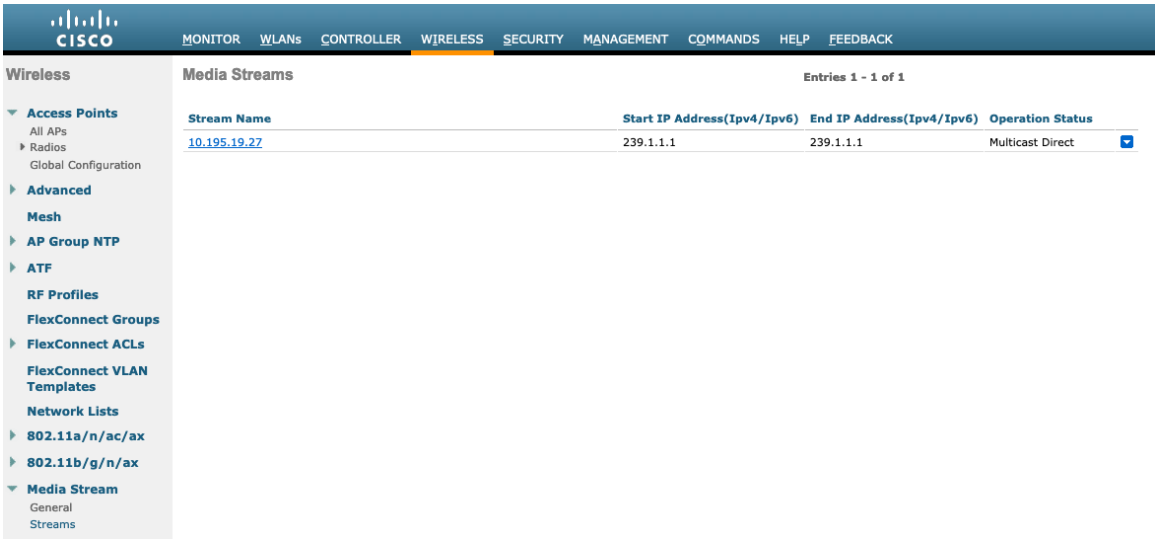
In the Media Stream settings, **Multicast Direct feature** should be enabled.



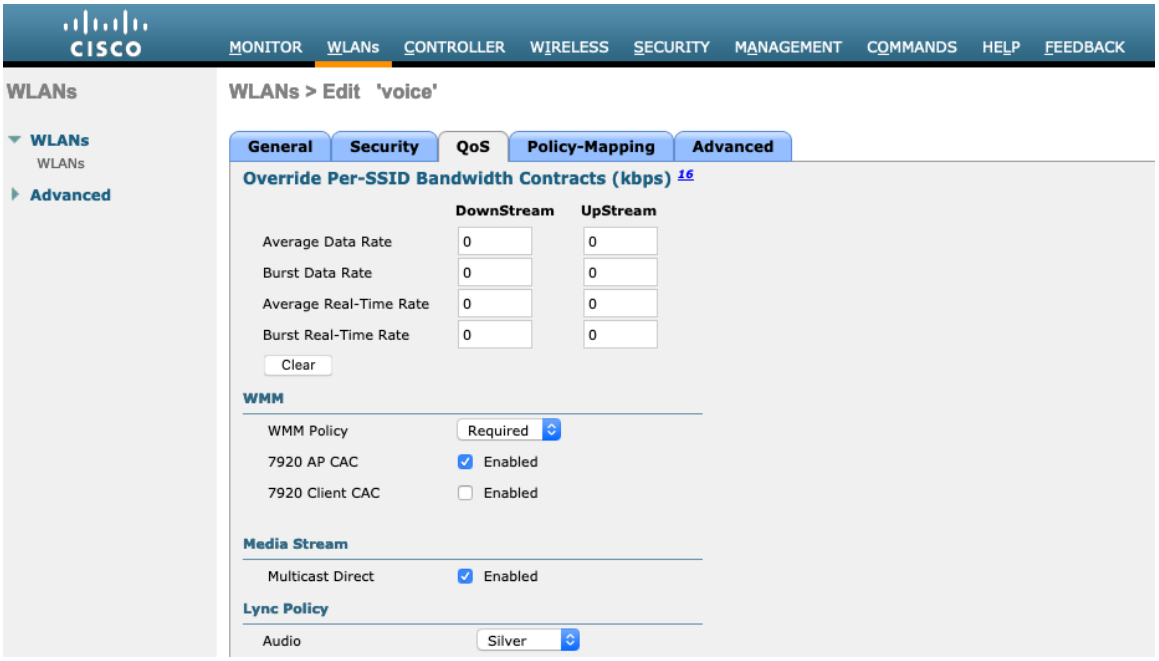
Then configure the media streams as necessary.



Once saved, then the media stream will be displayed.



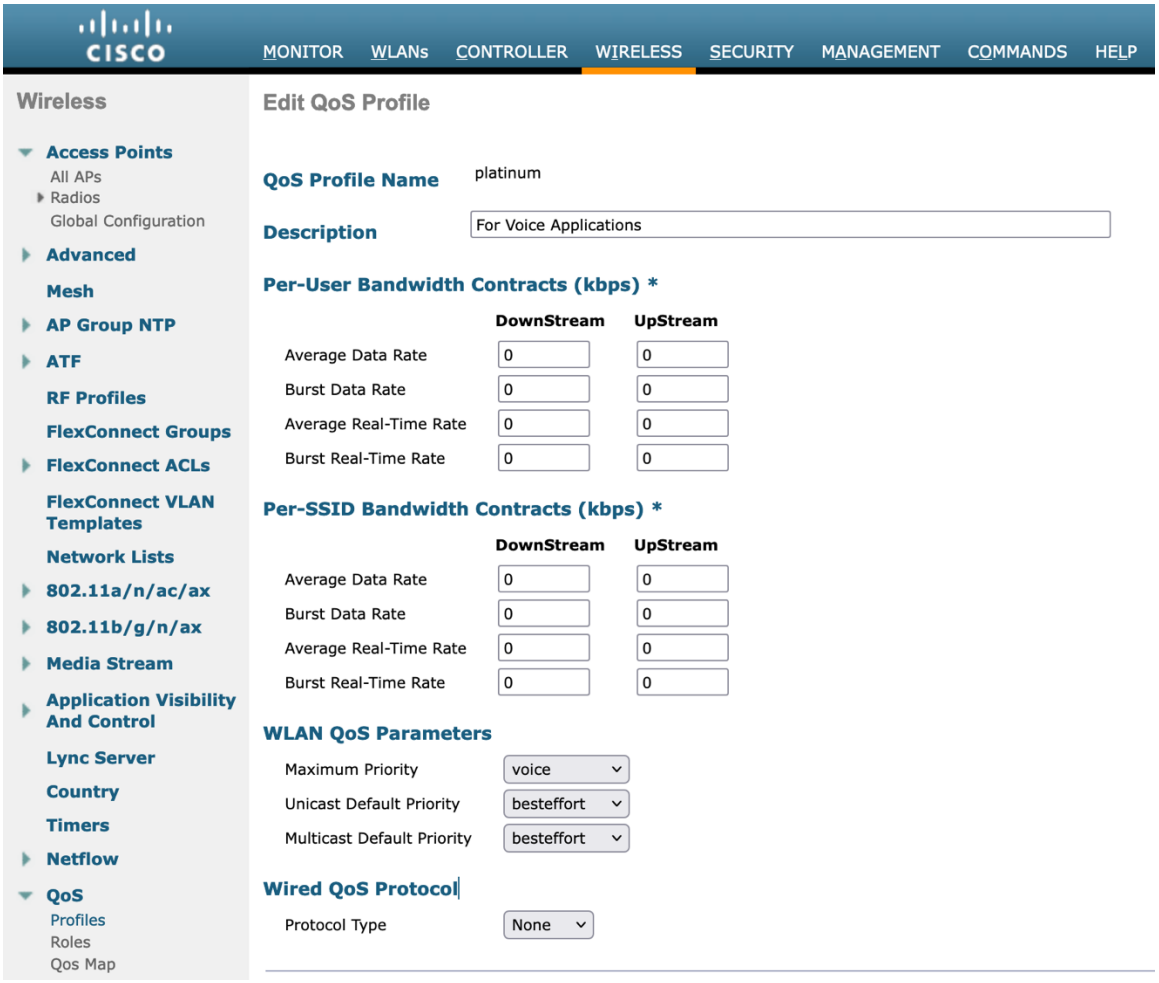
After **Multicast Direct feature** is enabled, then there will be an option to enable **Multicast Direct** in the QoS menu of the WLAN configuration.

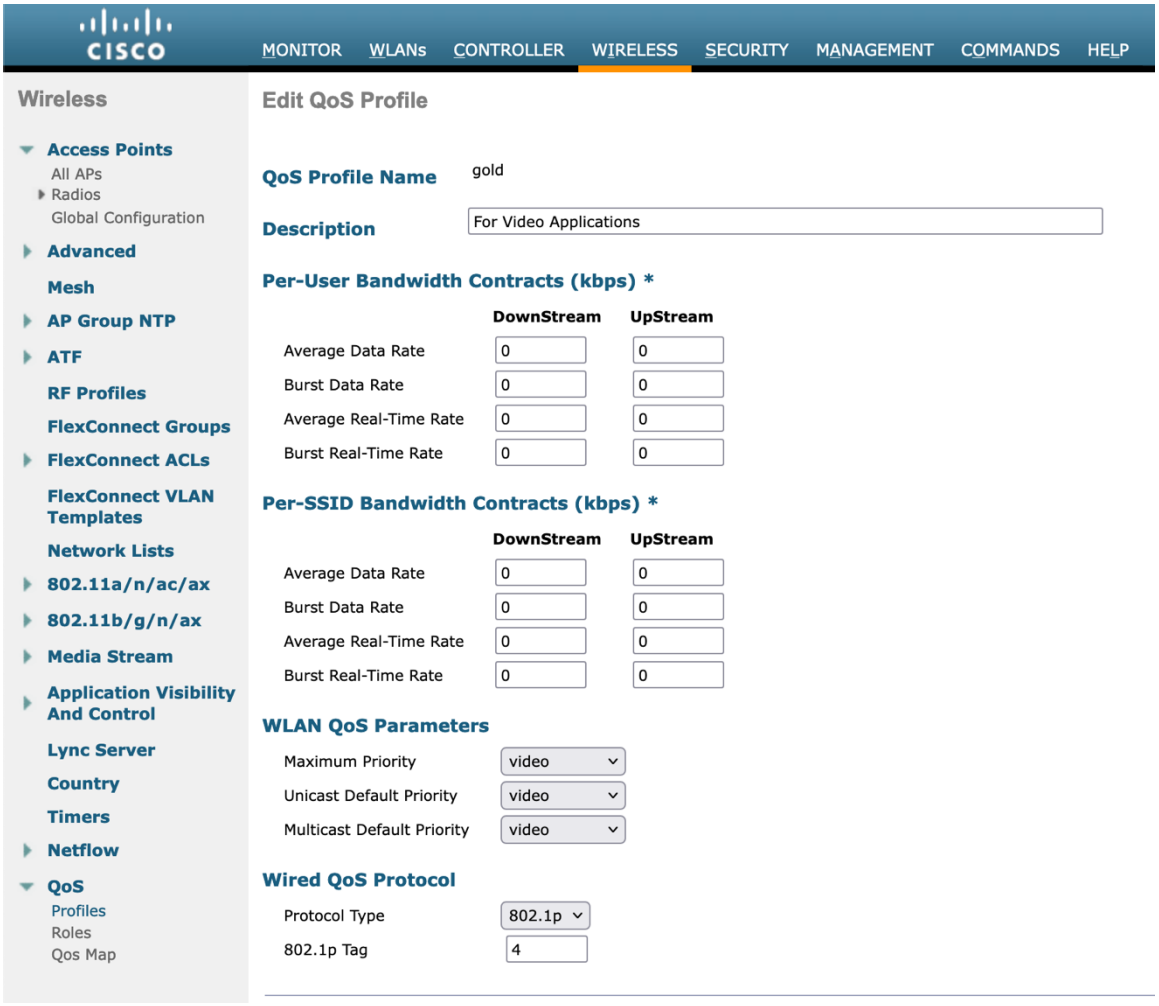


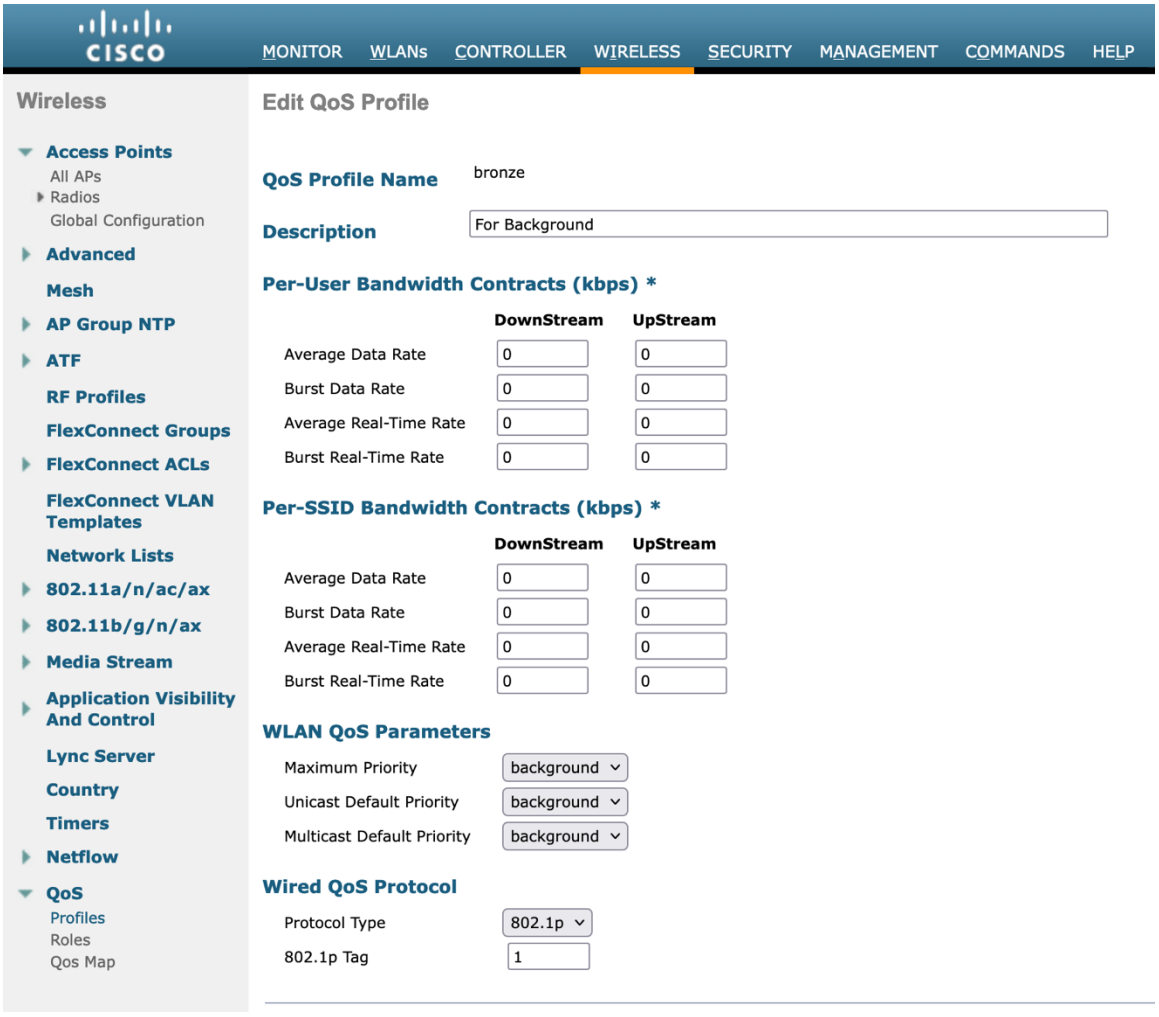
QoS Profiles

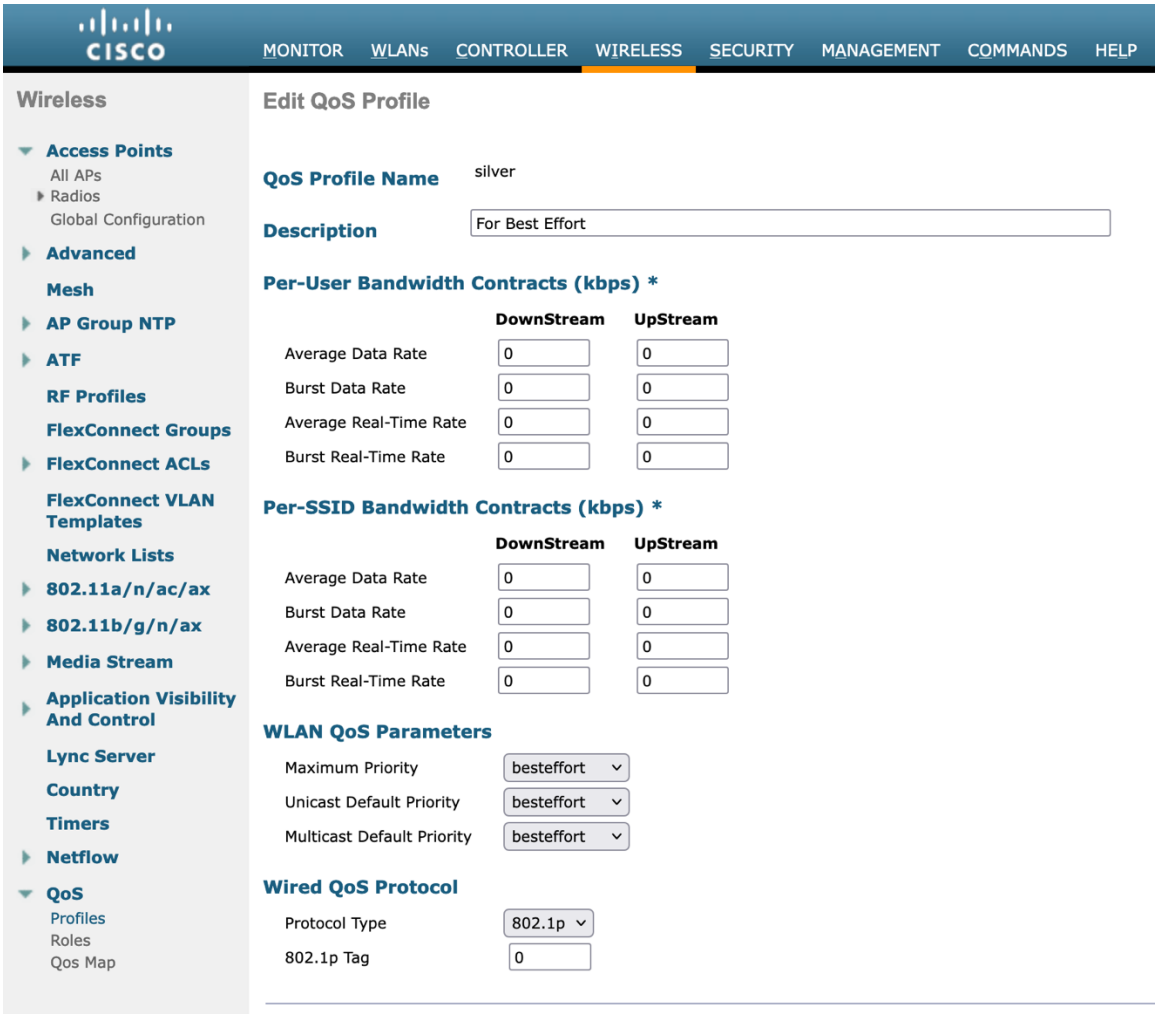
Configure the four QoS profiles per below.

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


CISCO
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
0
Per-SSID Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
0
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


CISCO
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

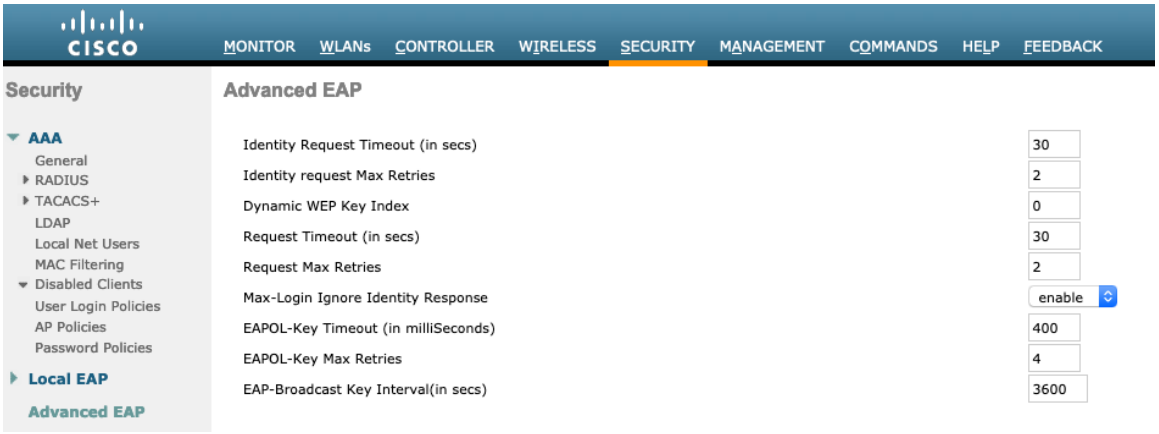


Advanced Settings

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 IP Phone 8821 and 8821-EX 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.

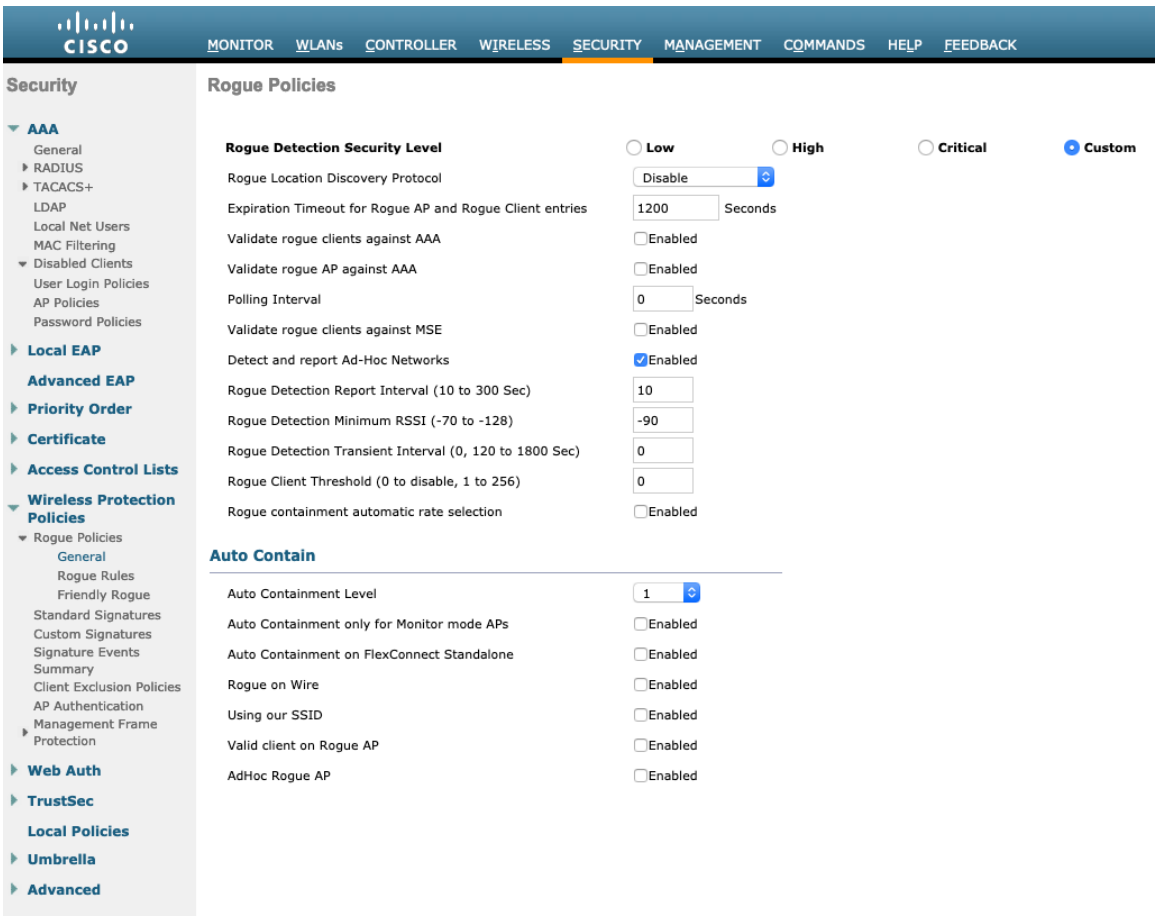
```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id >
```

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**
- Ensure **802.11k** is **Disabled**
- Ensure **802.11v** is **Disabled**
- 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

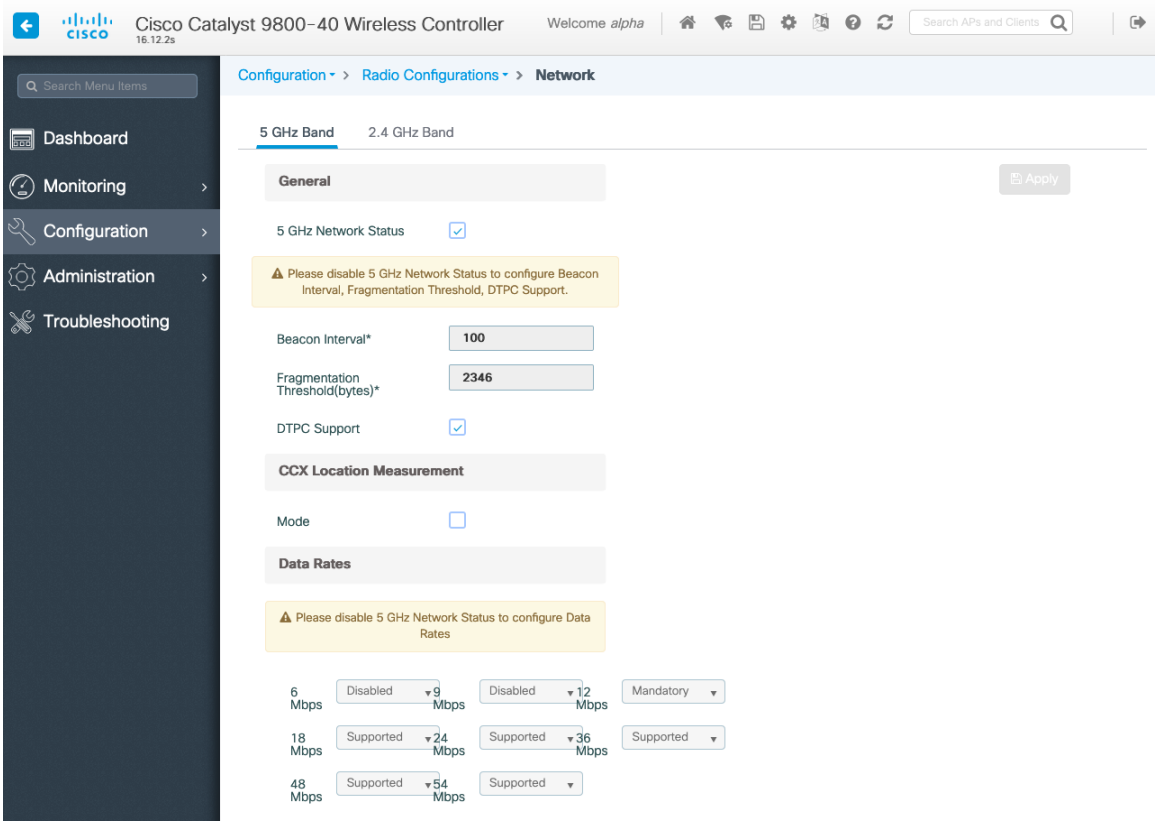
It is recommended to have the Cisco Wireless IP Phone 8821 and 8821-EX operate on the 5 GHz band only due to having many channels available and not as many interferers as the 2.4 GHz band has.

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**.

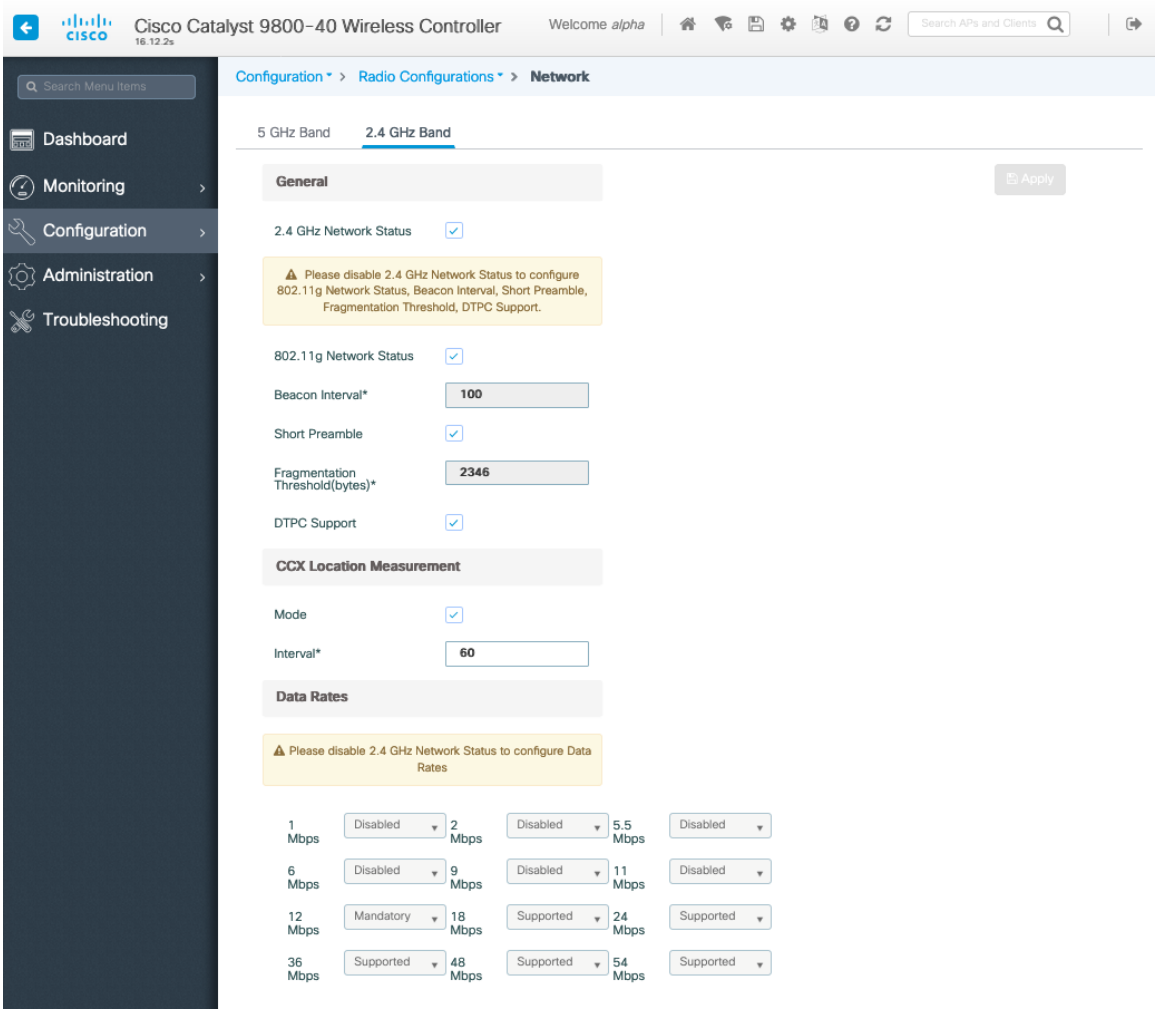
Set the **Beacon Period** to **100 ms**.

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).



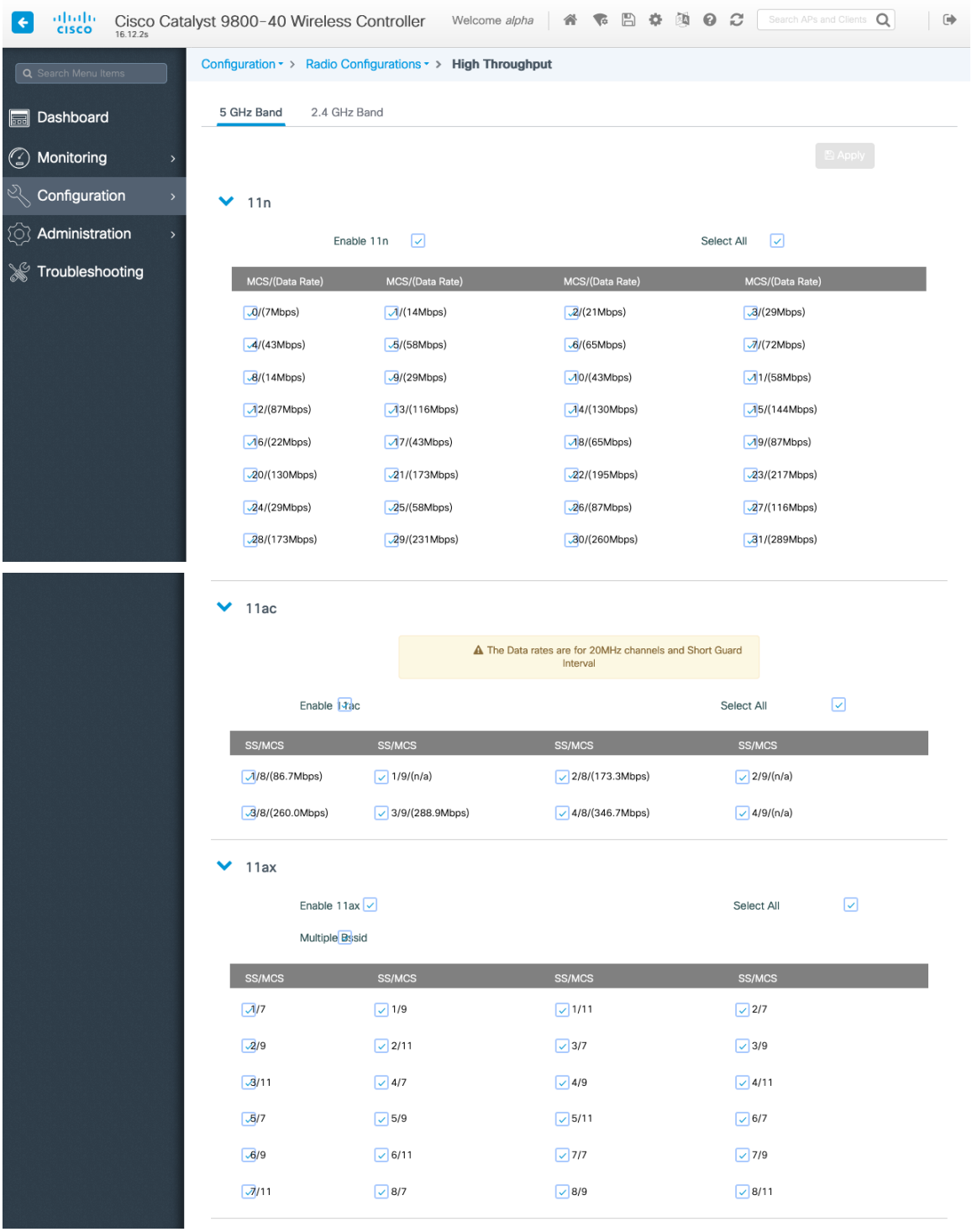
High Throughput (802.11n/ac)

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 IP Phone 8821 and 8821-EX support HT MCS 0 - MCS 7 and VHT MCS 0 - MCS 9 data rates only, but higher MCS rates can optionally be enabled if there are other 802.11n/ac clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of those higher data rates.



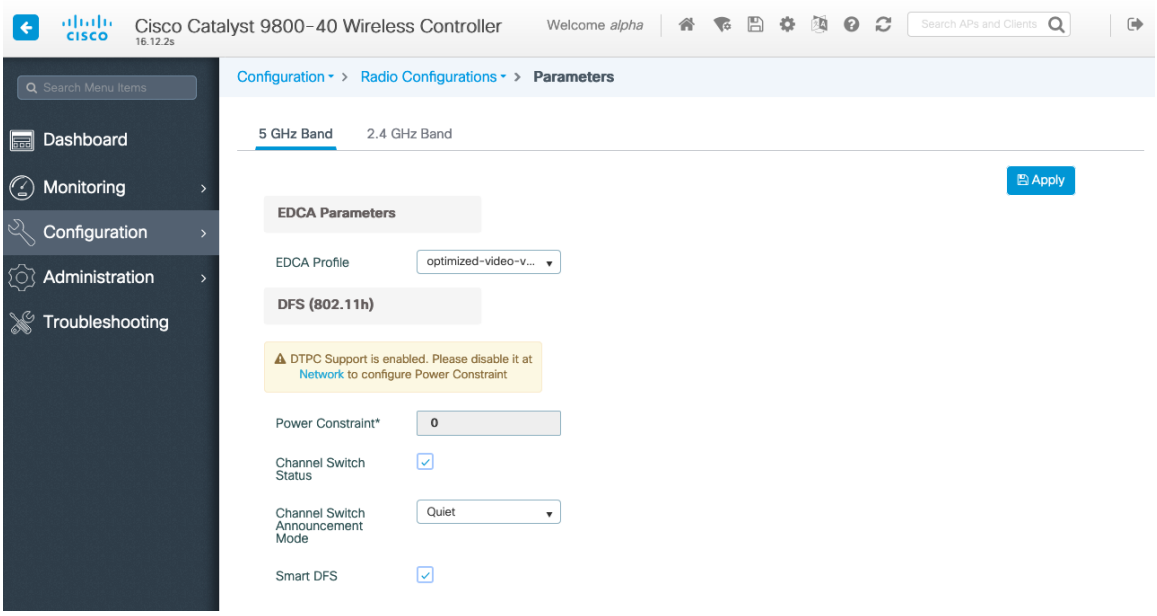
Parameters

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

In the DFS (802.11h) section, **Power Constraint** should be left un-configured or set to 0 dB as DTPC will be used by the Cisco Wireless IP Phone 8821 and 8821-EX to control the transmission power.

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

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

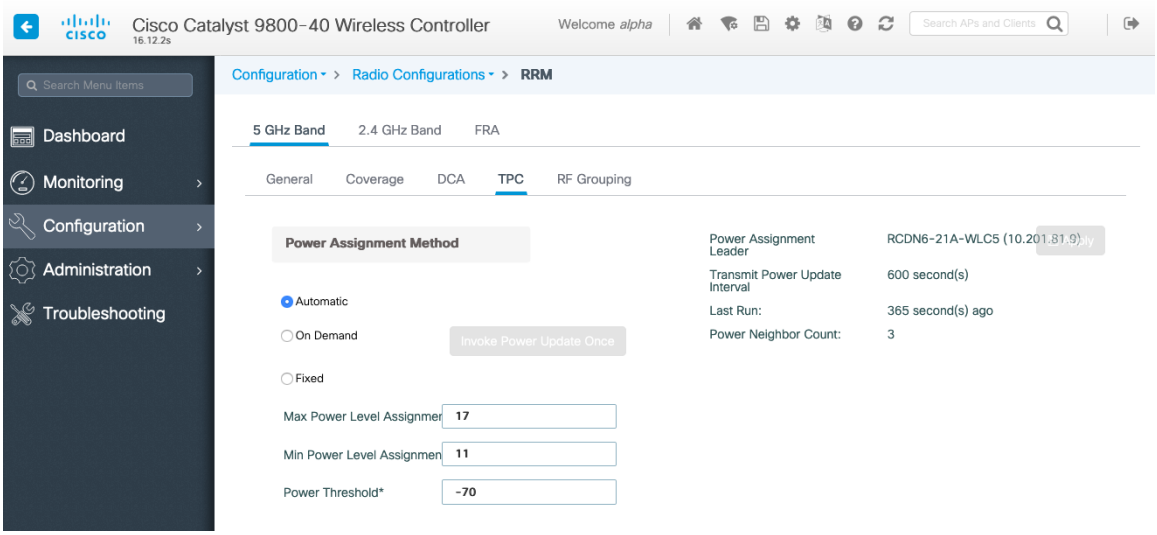


RRM

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.

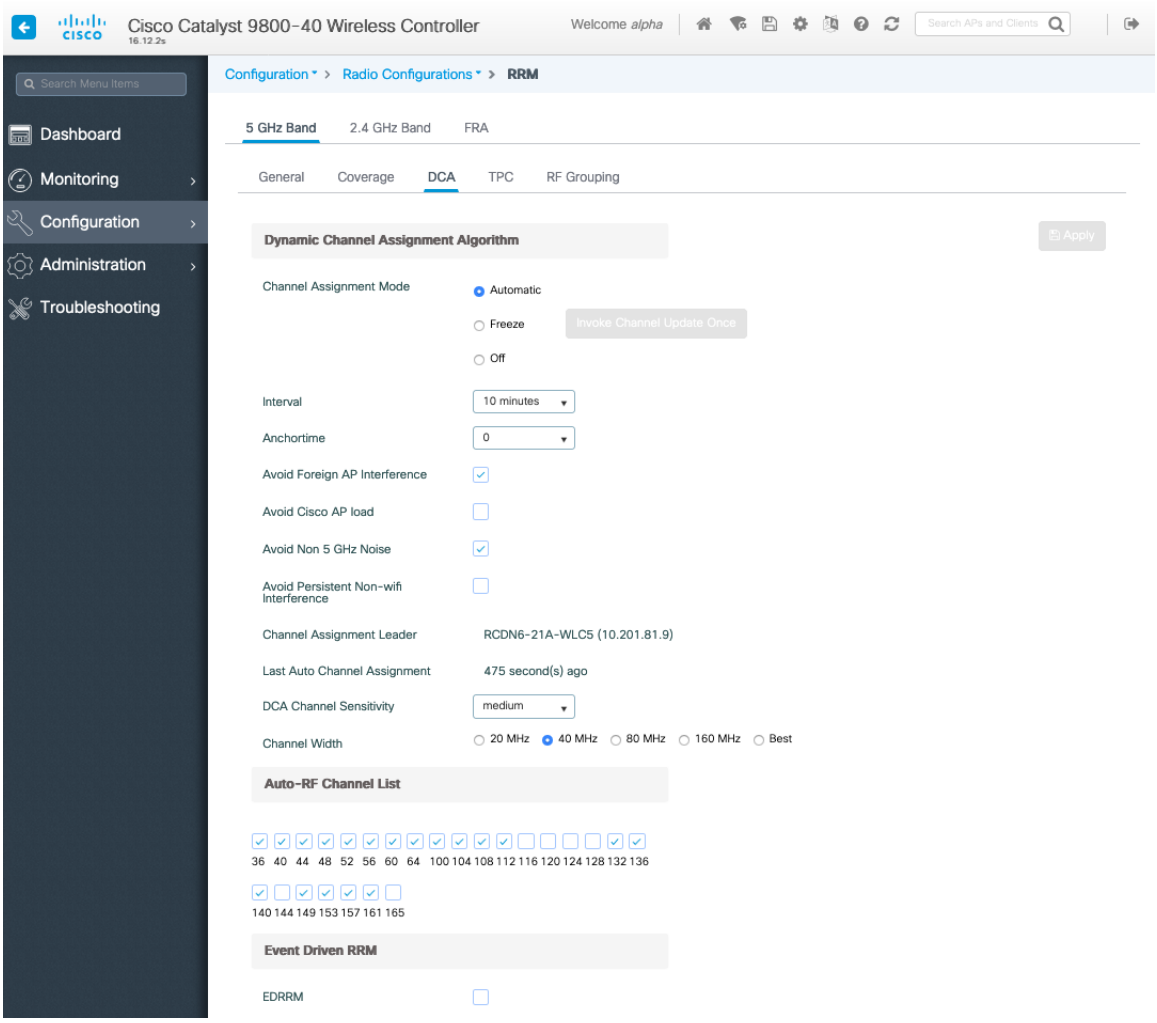
If using automatic power level assignment, a maximum and minimum power level can be specified.



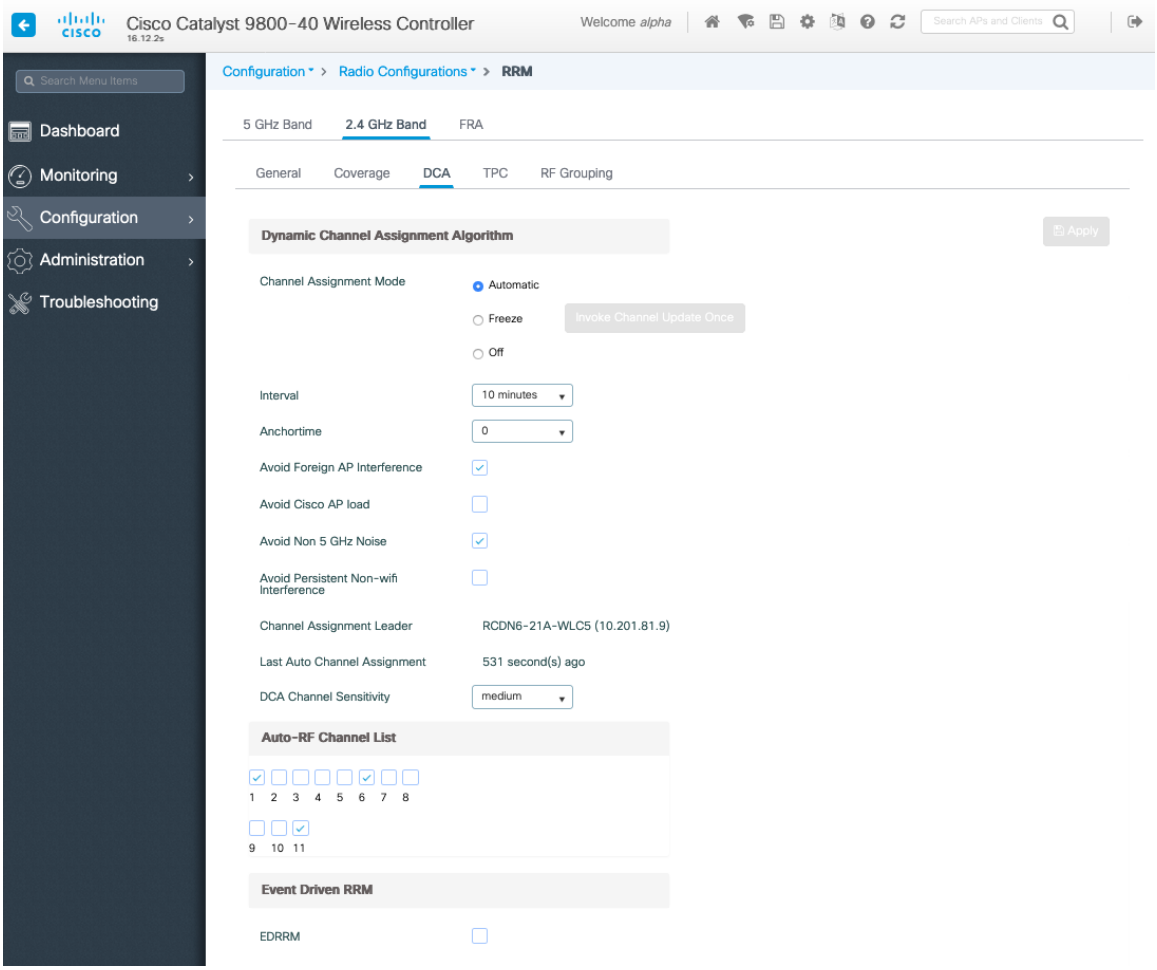
If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.

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.



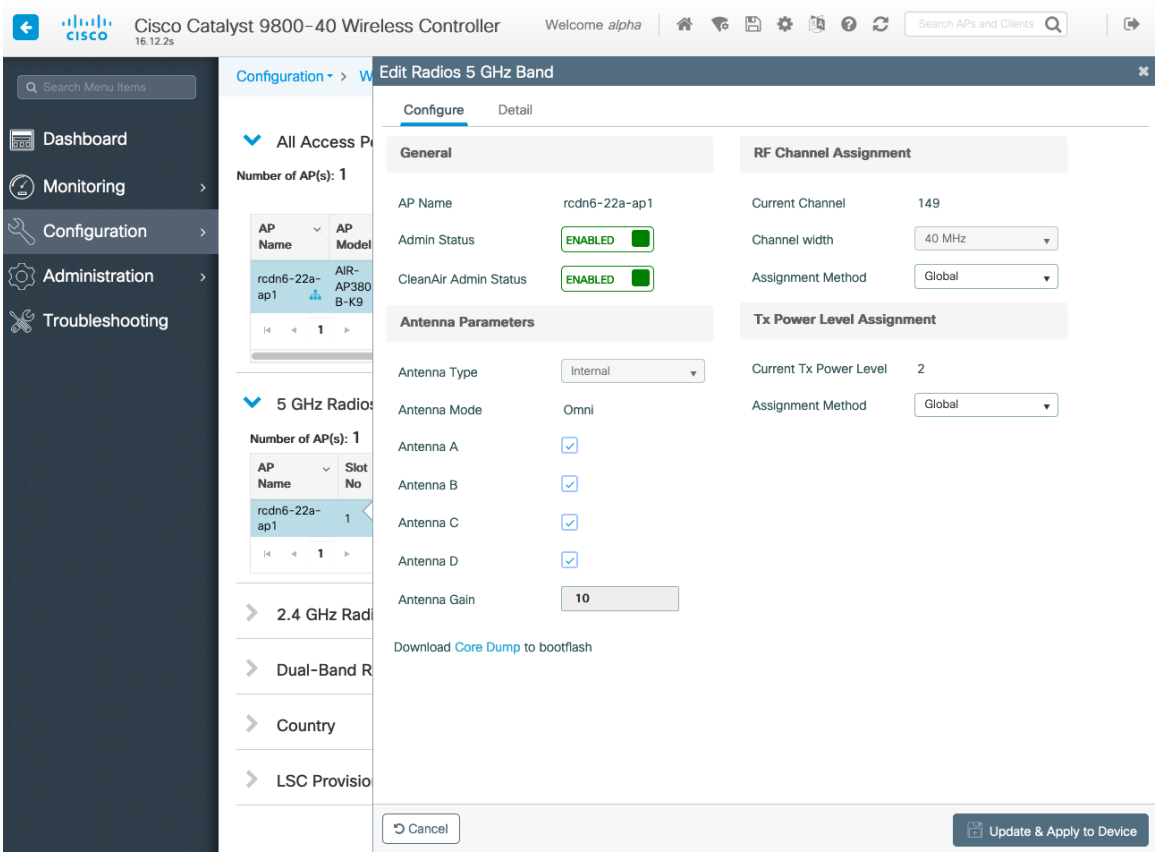
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

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.

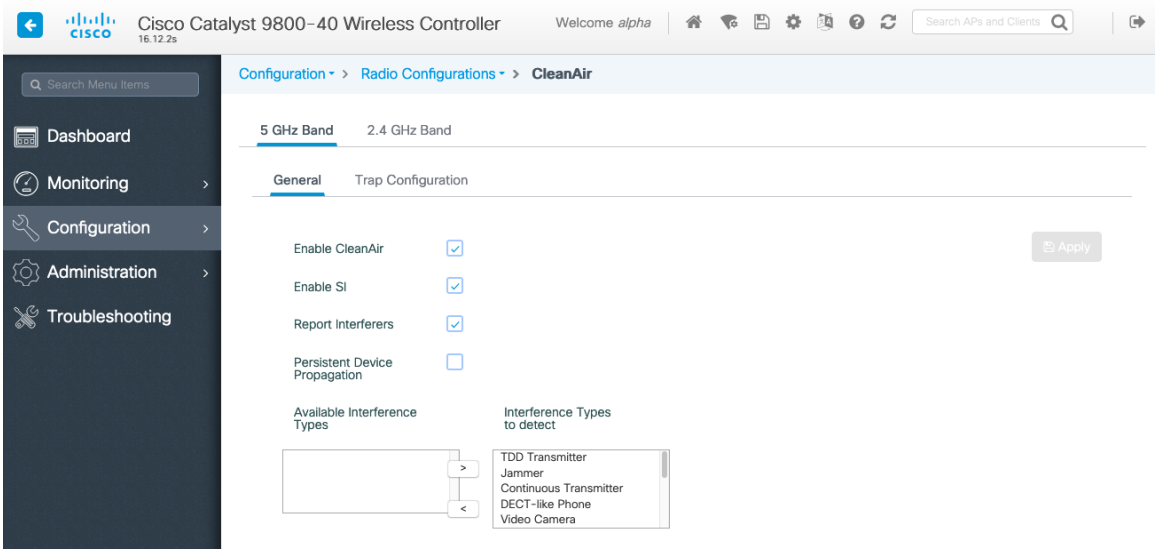
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

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

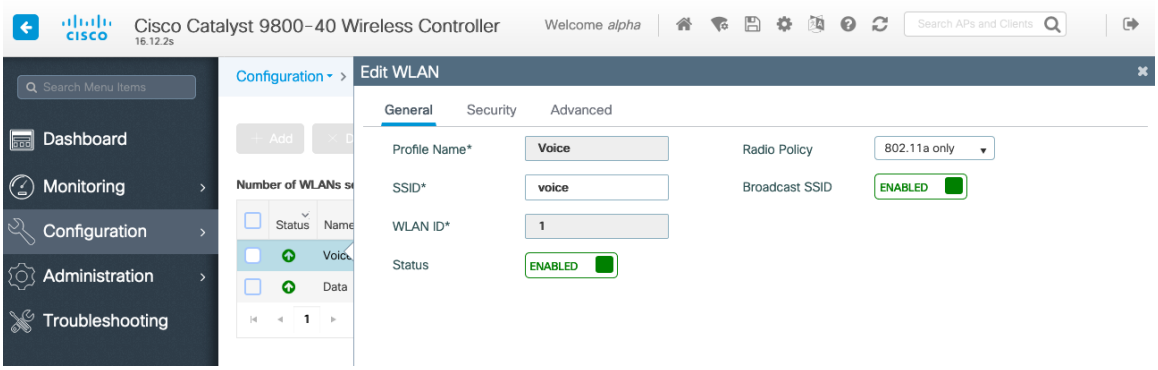
It is recommended to have a separate SSID for the Cisco Wireless IP Phone 8821 and 8821-EX.

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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX 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.

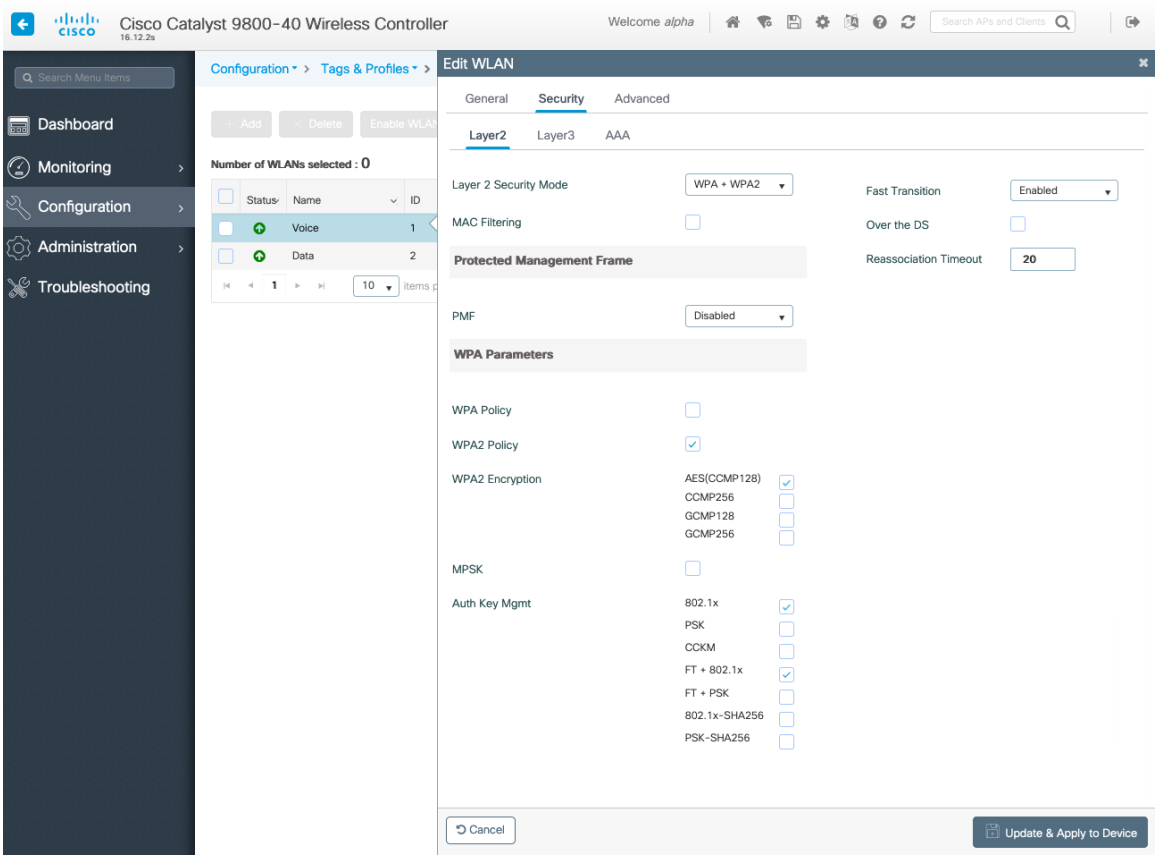


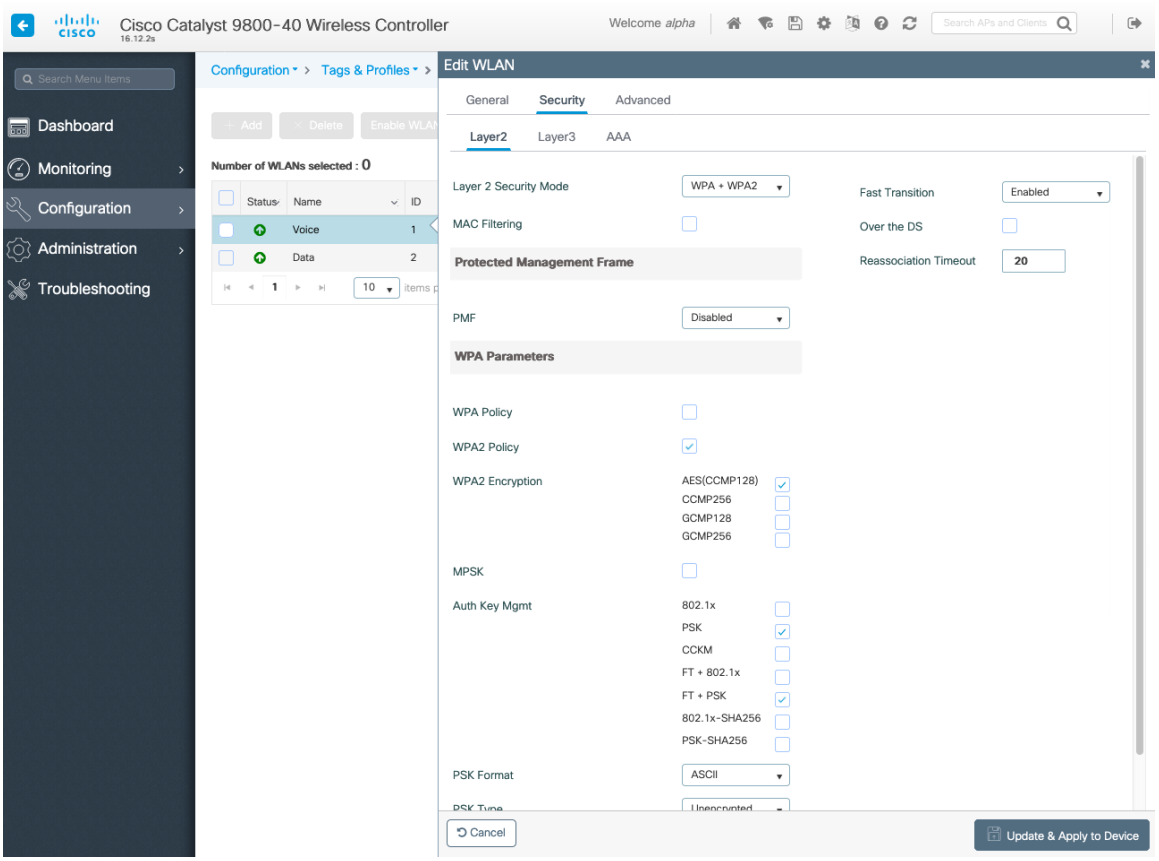
To utilize 802.11r (FT) for fast secure roaming, set **Fast Transition** to **Enabled**.

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

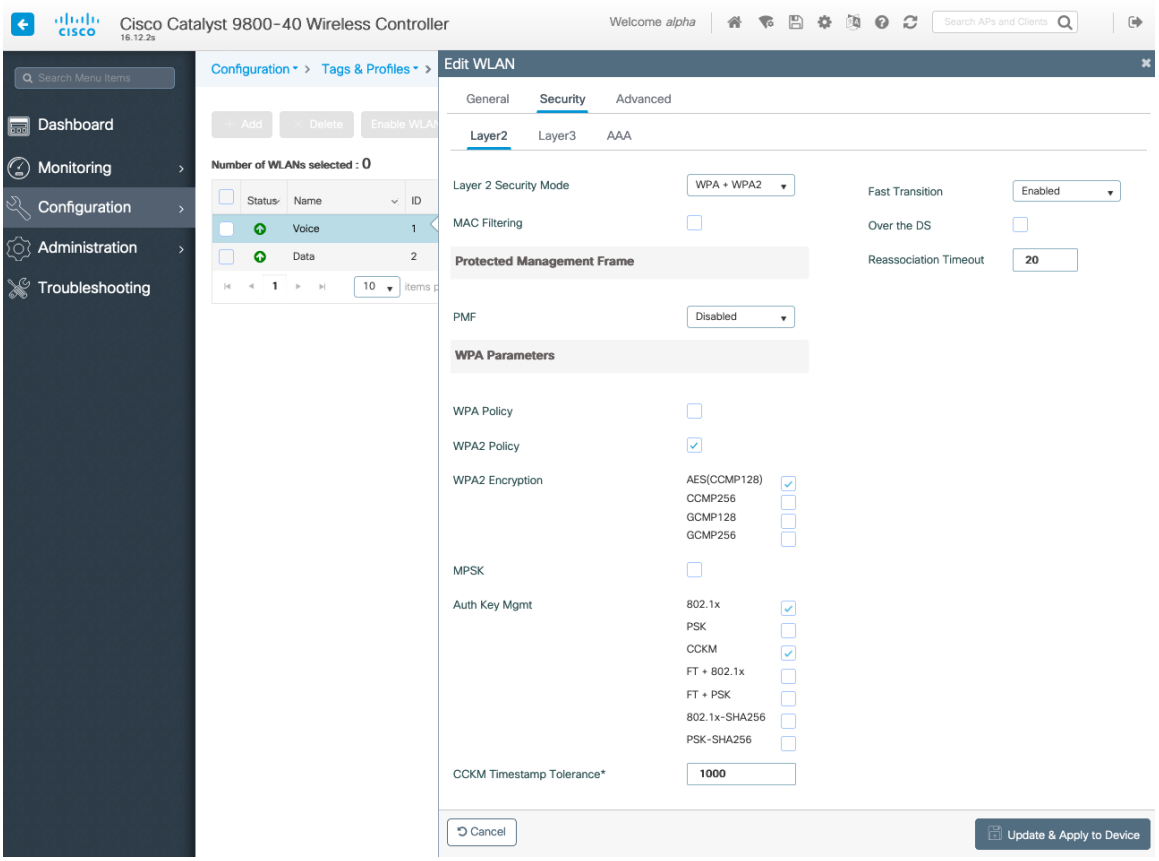

Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles >
Add
Delete
Enable WLAN
Number of WLANs selected : 0
Status
Name
ID
Voice
1
Data
2
10
items p
Edit 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.

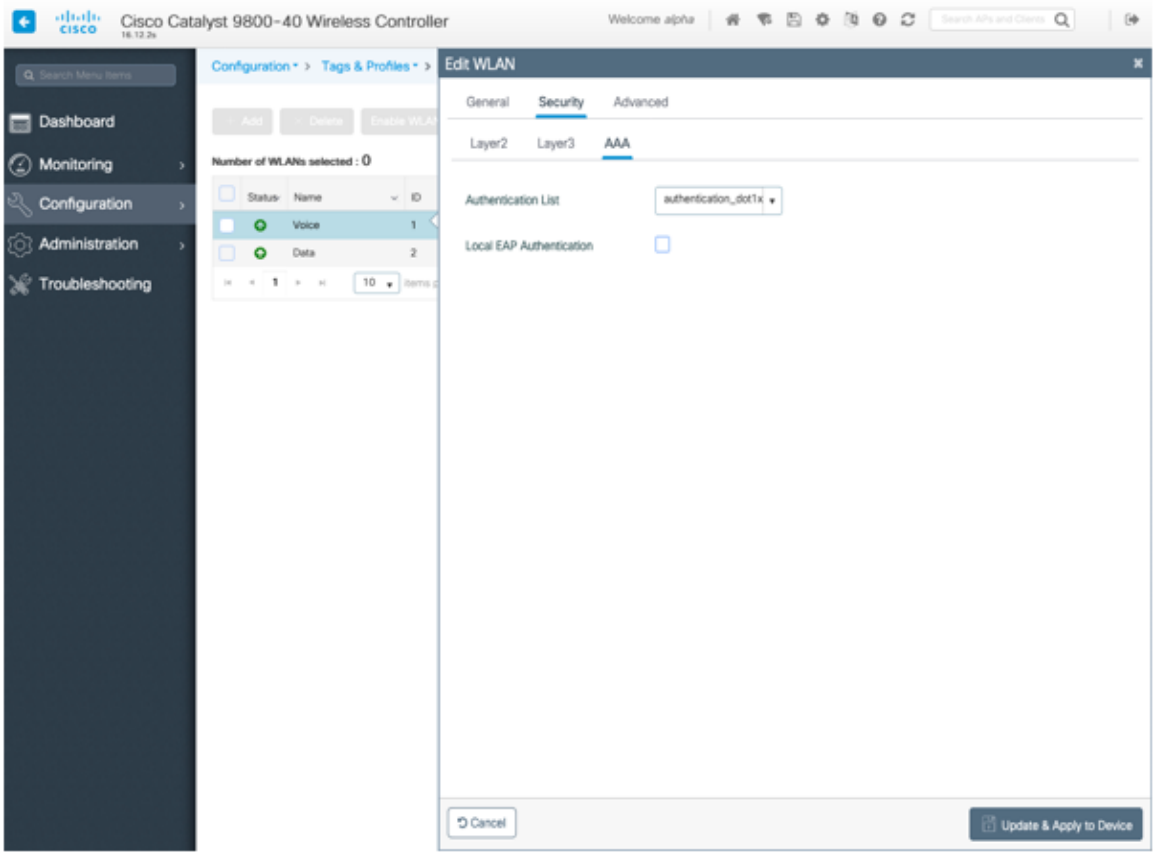
To utilize CCKM for fast secure roaming, enable WPA2 policy with AES encryption and 802.1x + CCKM for authenticated key management type.

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 IP Phone 8821 and 8821-EX roaming experience.



If using 802.1x, configure the AAA Authentication List that maps to the RADIUS Servers defined in the RADIUS Server Groups.



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 IP Phone 8821 and 8821-EX 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 IP Phone 8821 and 8821-EX, then ensure the WMM policy is set to **Allowed.**

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

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

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

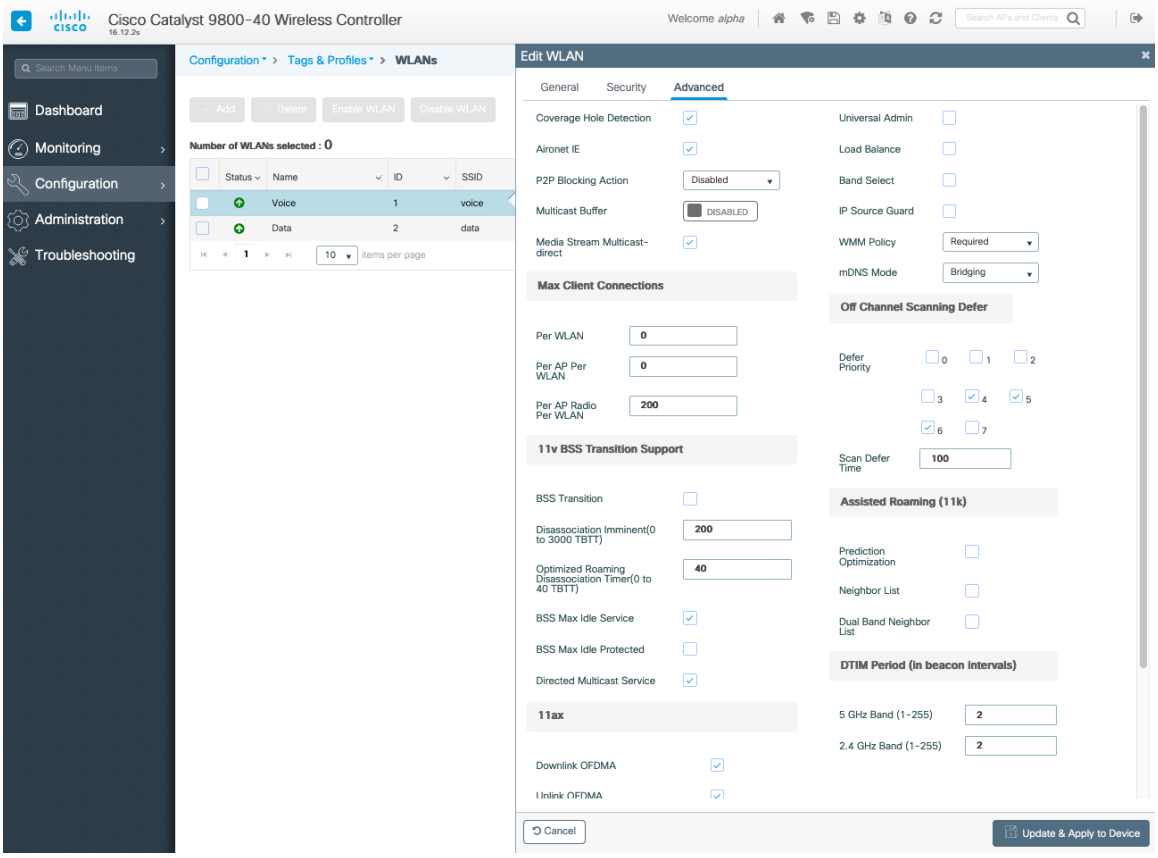
If using best effort applications frequently or if DSCP values for priority applications (e.g. voice and call control) are not preserved to the access point, then is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well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

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

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

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

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

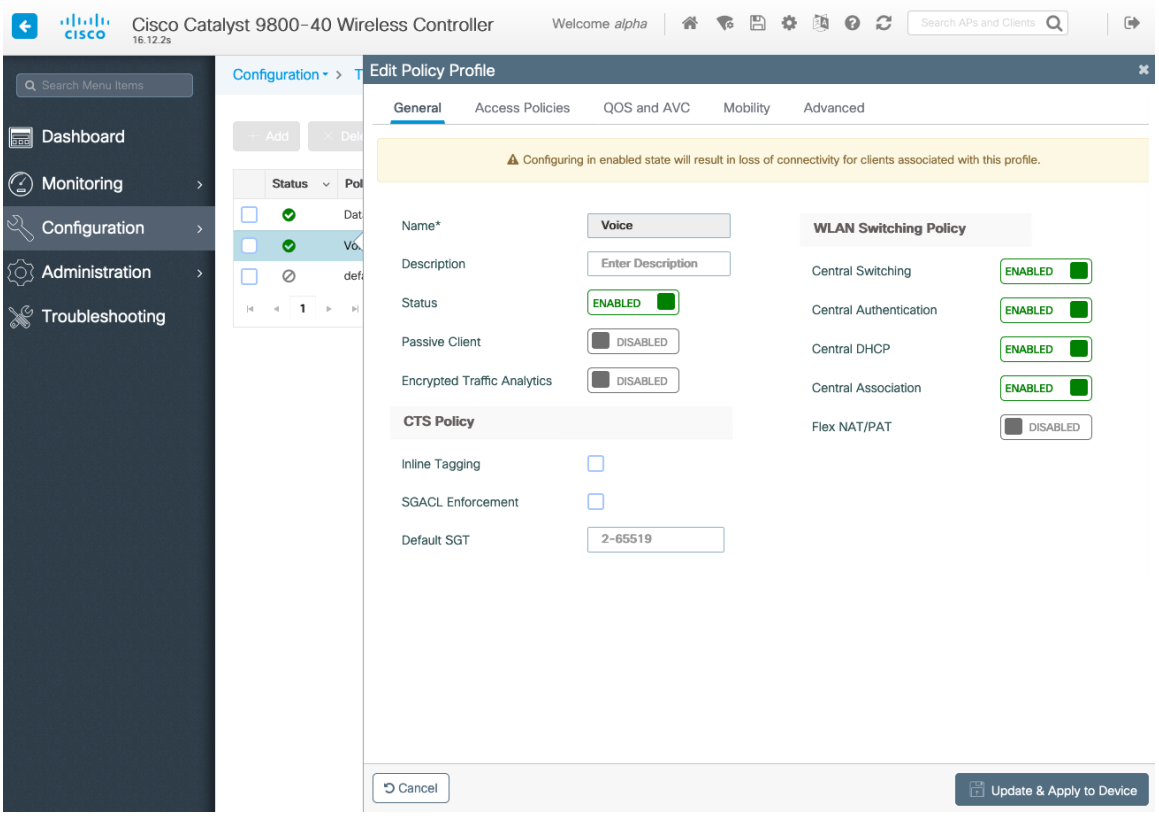


Policy Profiles

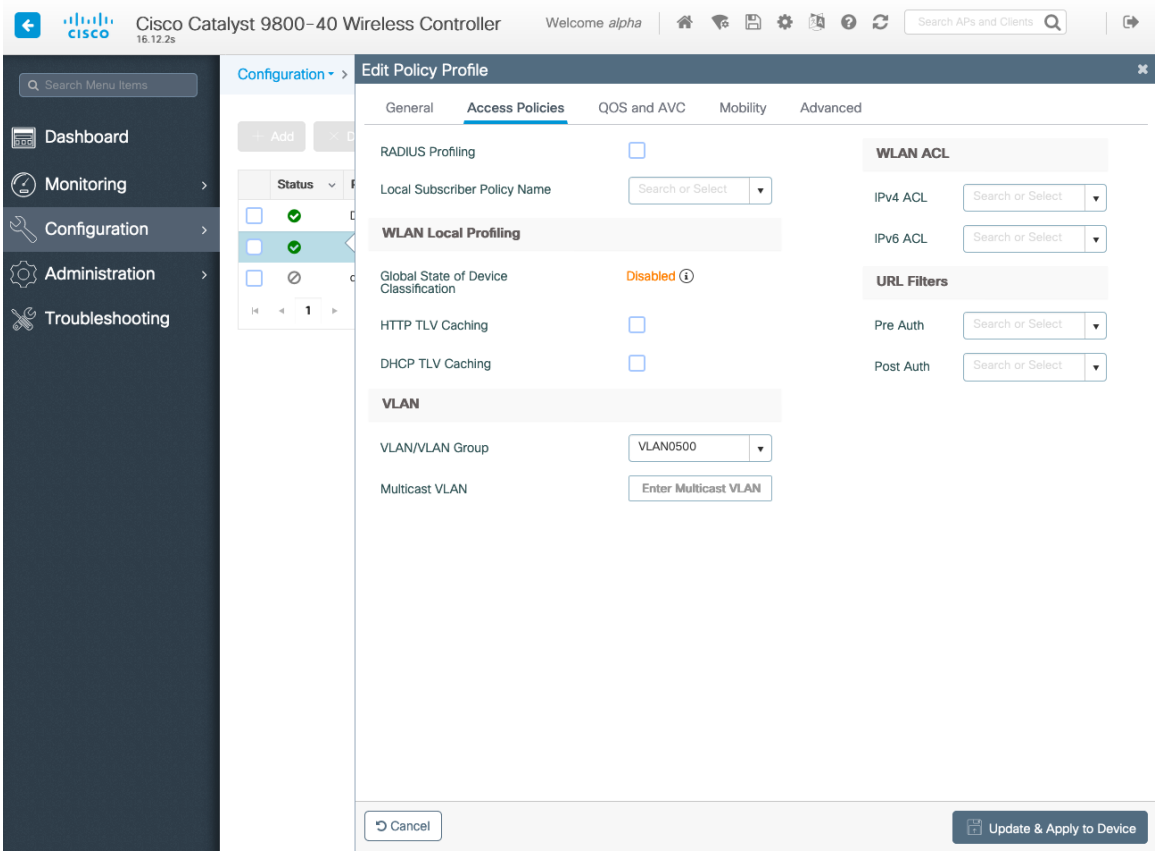
Policy Profiles are used to define additional settings regarding access, QoS, Mobility, and advanced settings.

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

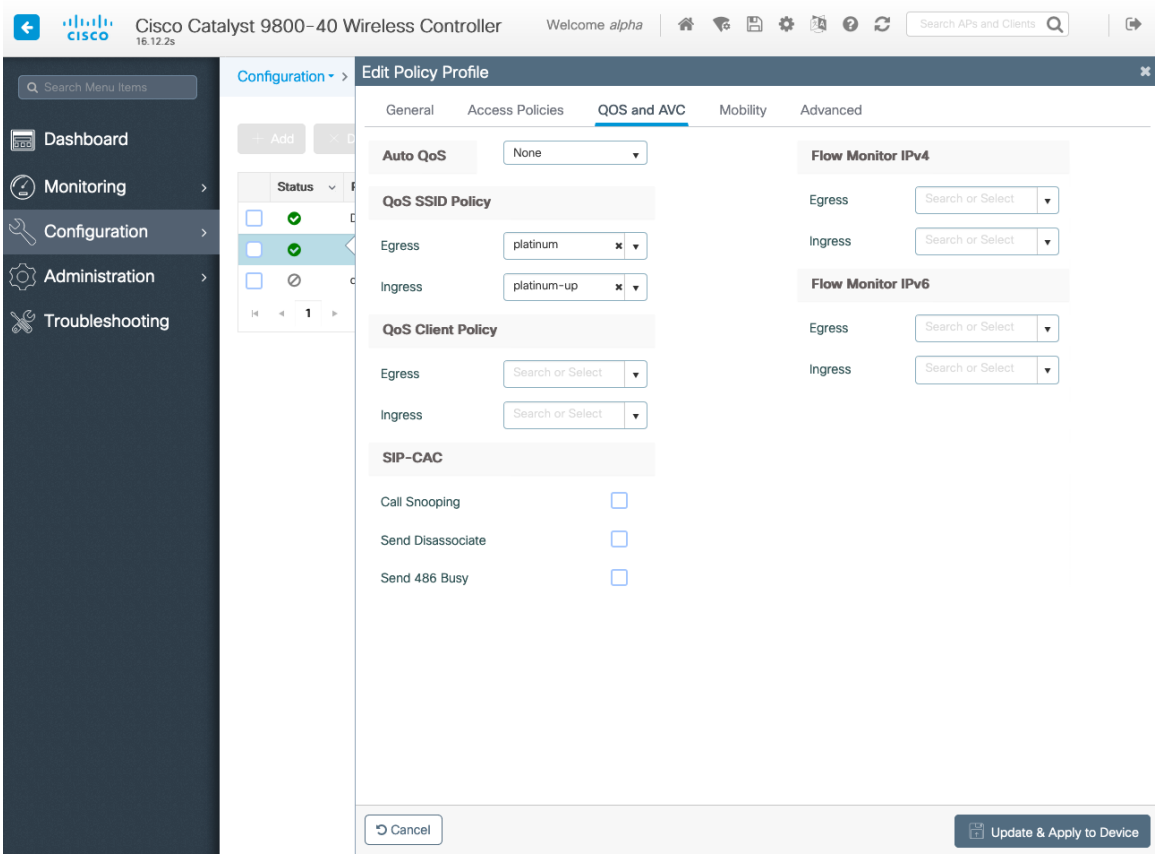
Ensure the **Status** of the policy profile is **Enabled**.



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



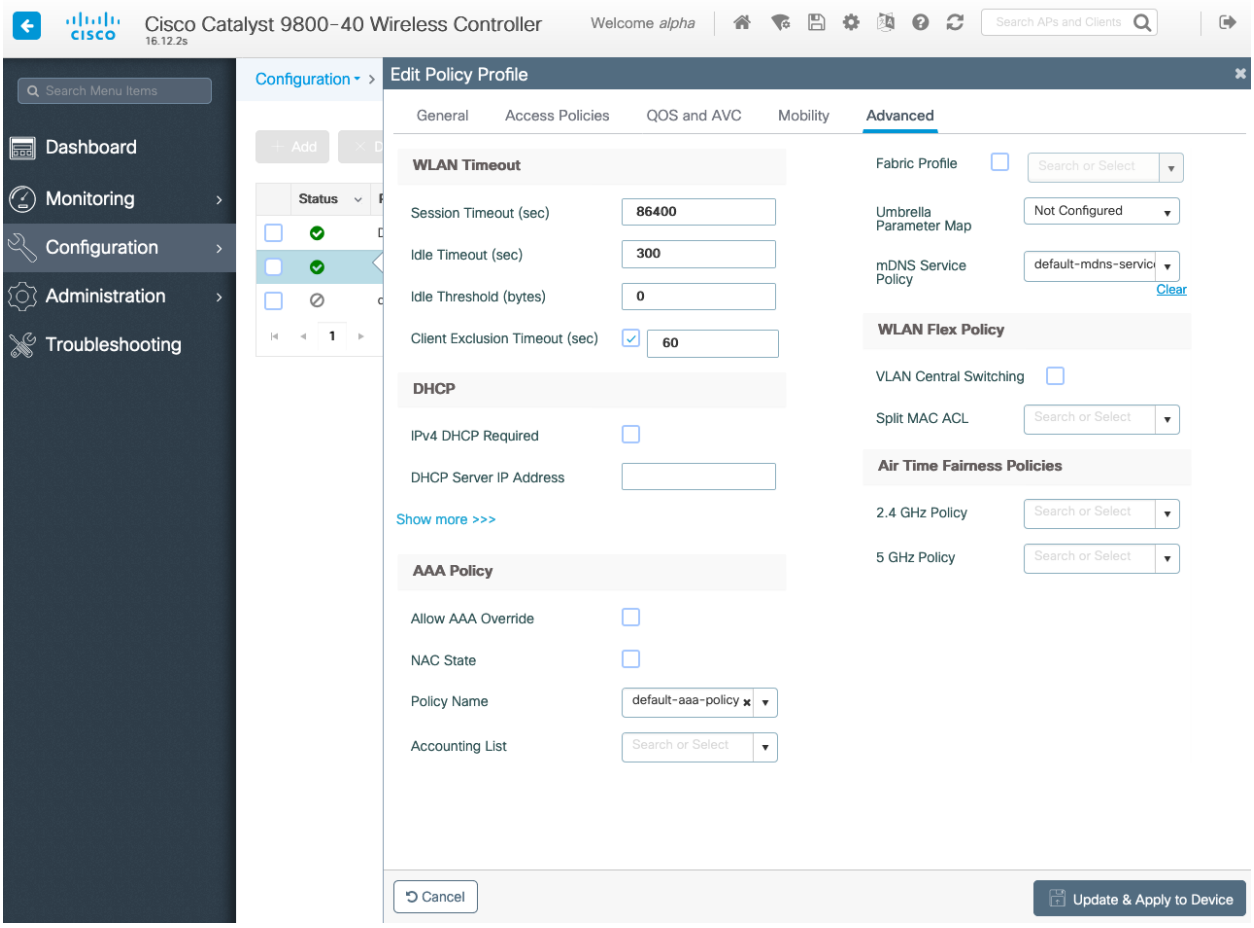
Ensure the QoS SSID Policy is set to **Platinum** for egress and **Platinum-up** for ingress.



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

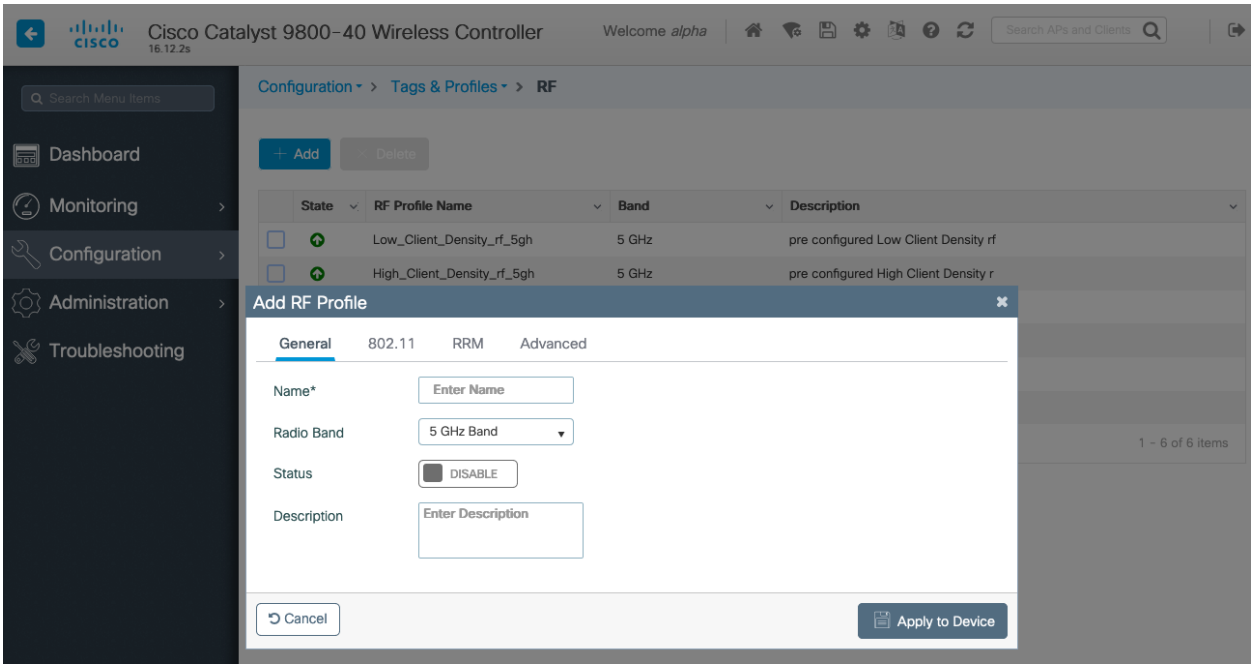
RF Profiles can be created to specify which frequency bands, data rates, RRM settings, and advanced settings a group of access points should use.

It is recommended to have the SSID used by the Cisco Wireless IP Phone 8821 and 8821-EX 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.

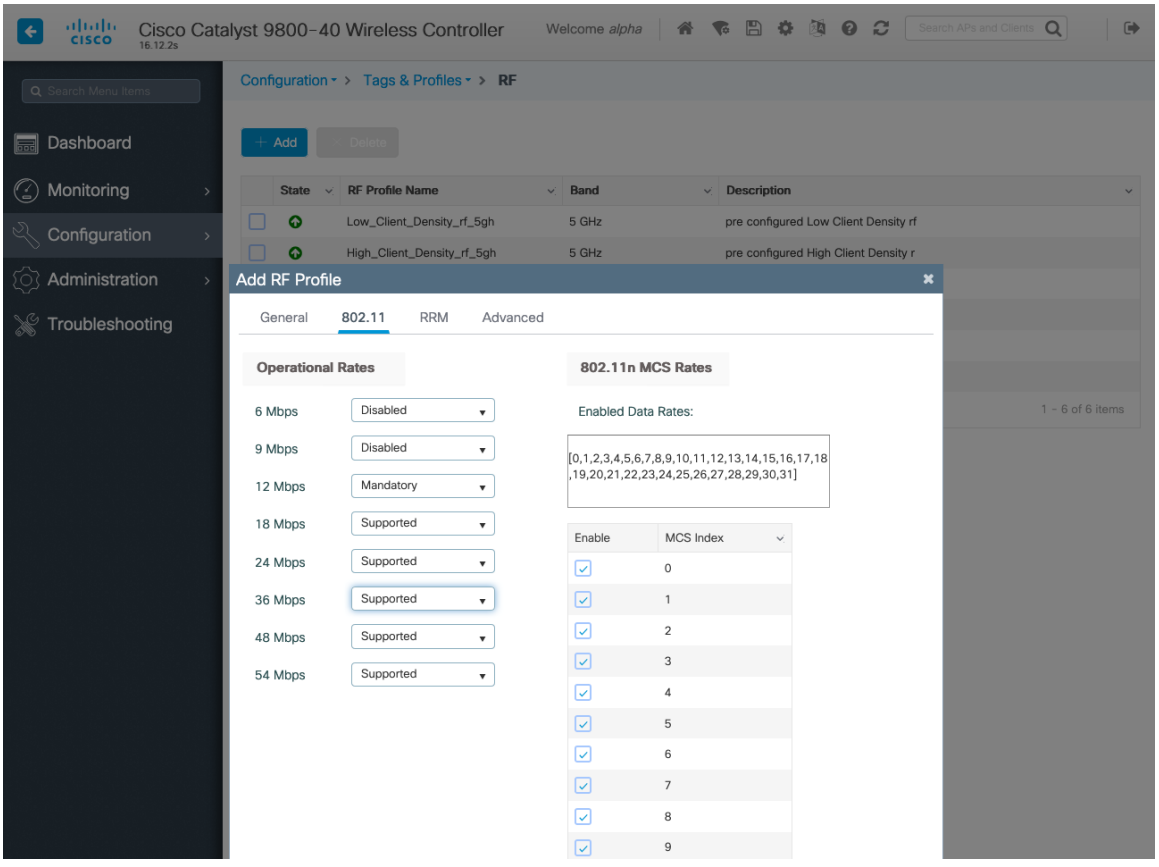
When creating an RF Profile, the **Name** and **Radio Band** must be defined.

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

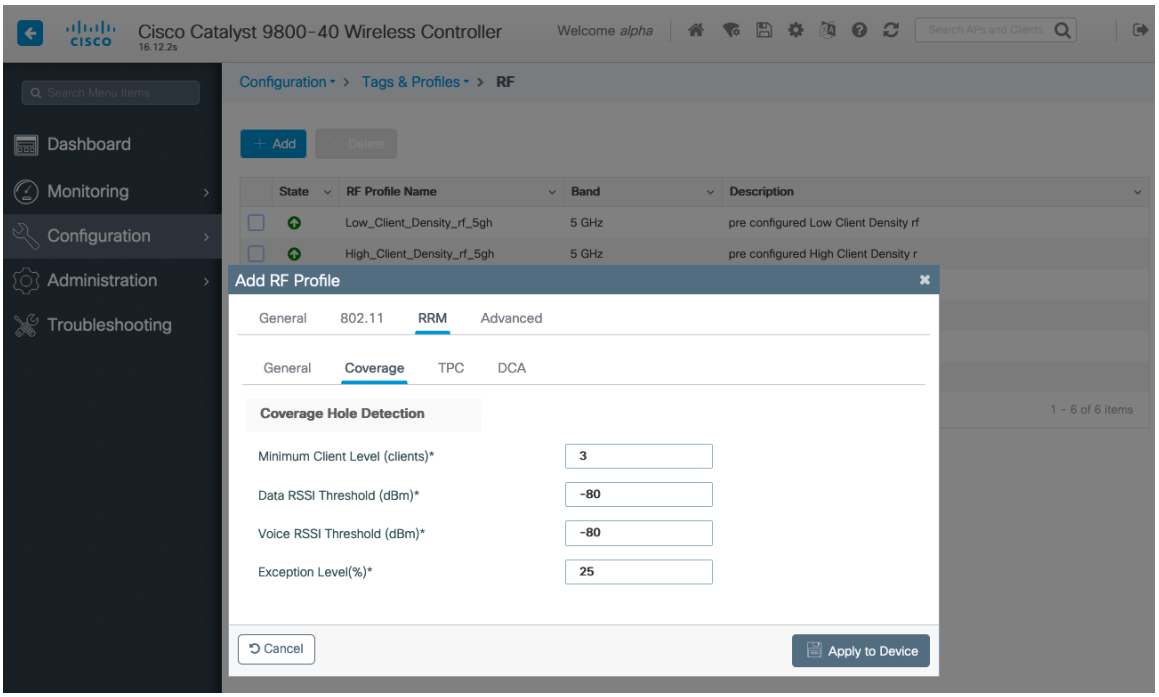


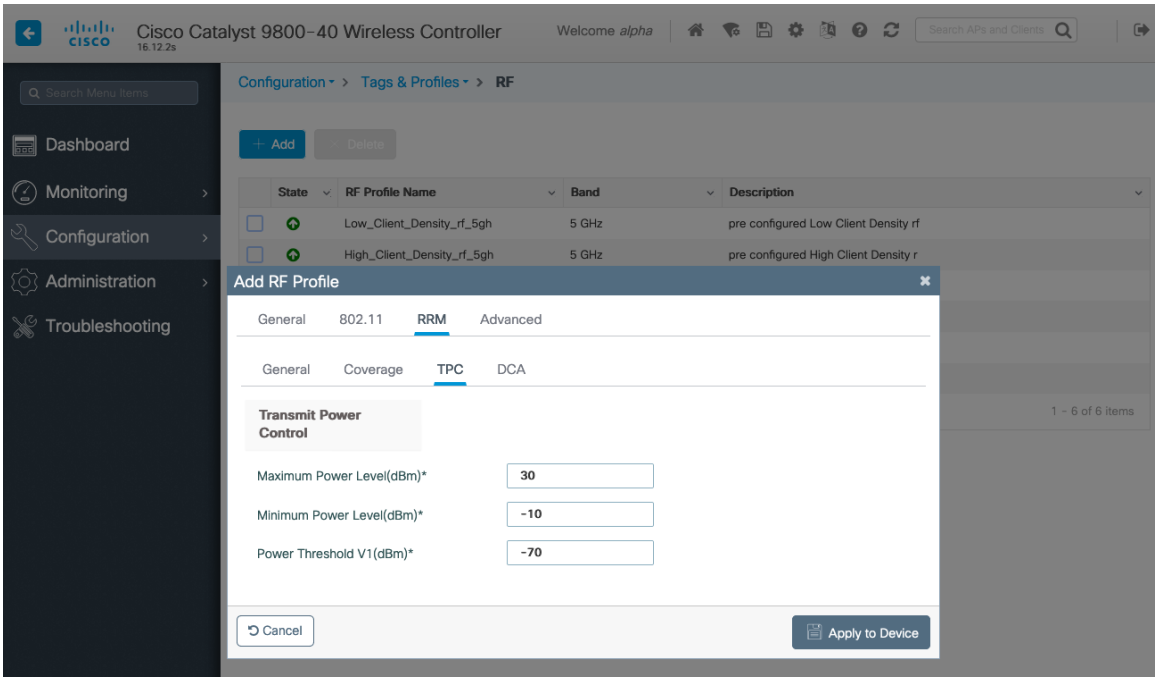
On the **802.11** tab, configure the data rates as necessary.

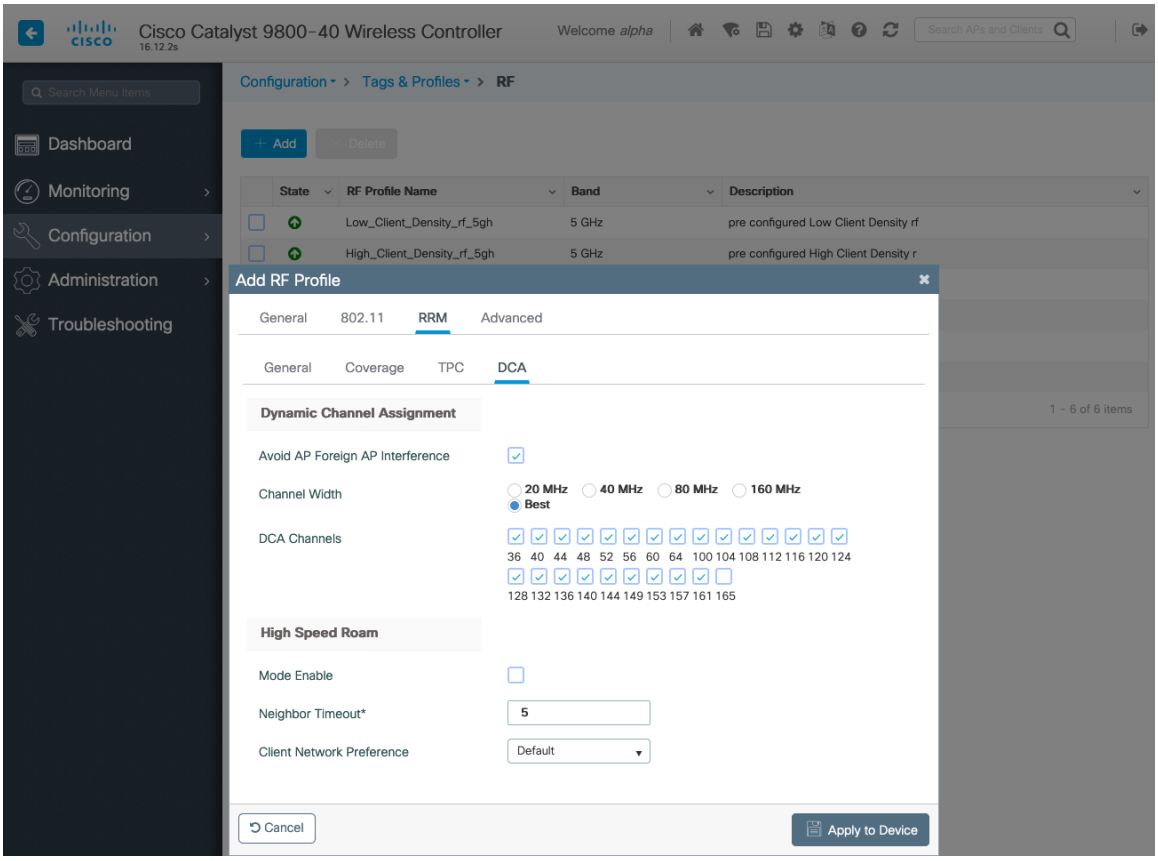
Is recommended to enable 12 Mbps as **Mandatory** and 18 Mbps and higher as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.



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.

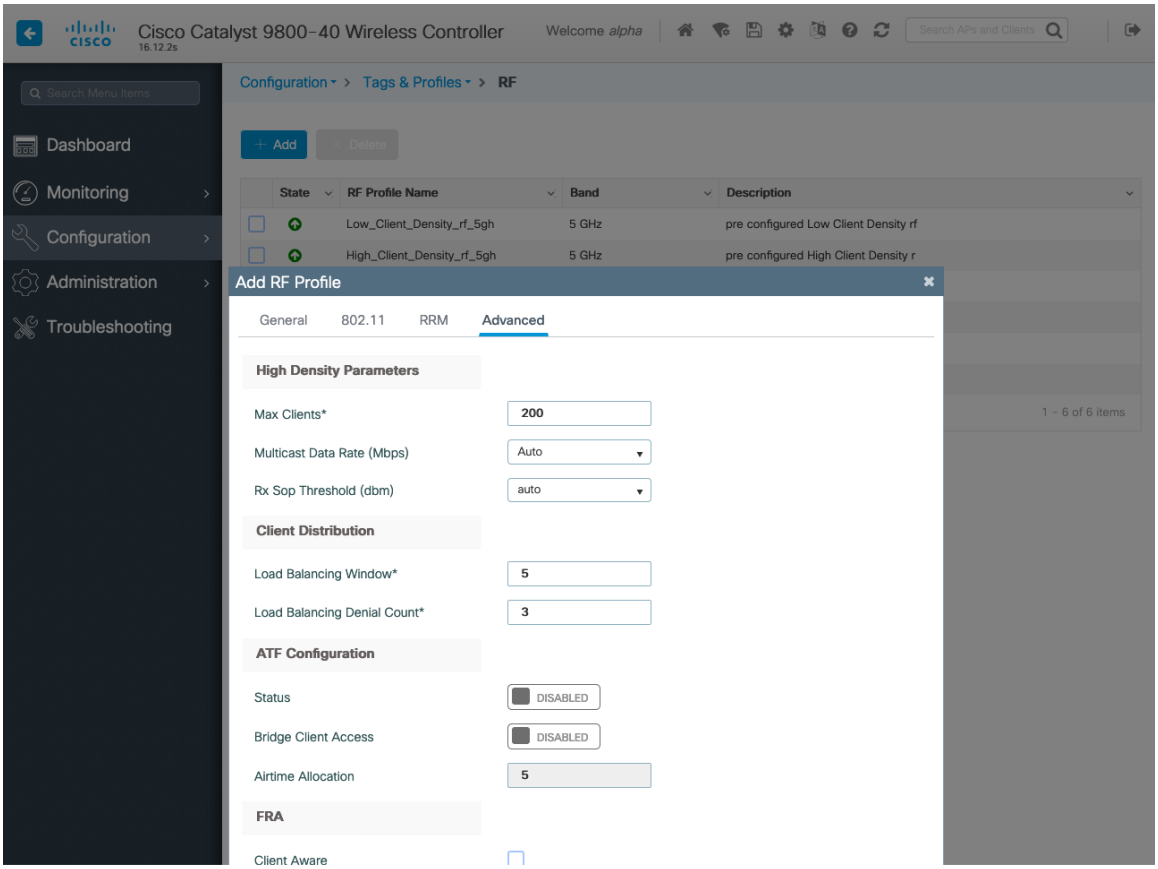

Cisco Catalyst 9800-40 Wireless Controller
16.12.2s
Welcome alpha
Search APs and Clients
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Tags & Profiles > RF
Add
Delete
State
RF Profile Name
Band
Description
Low_Client_Density_rf_5gh
5 GHz
pre configured 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**.



Note: It is important to note that adjusting **Rx SOP Threshold** may impact the interoperability of the Cisco Wireless IP Phone 8821 and 8821-EX with Cisco APs.

Flex Profiles

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

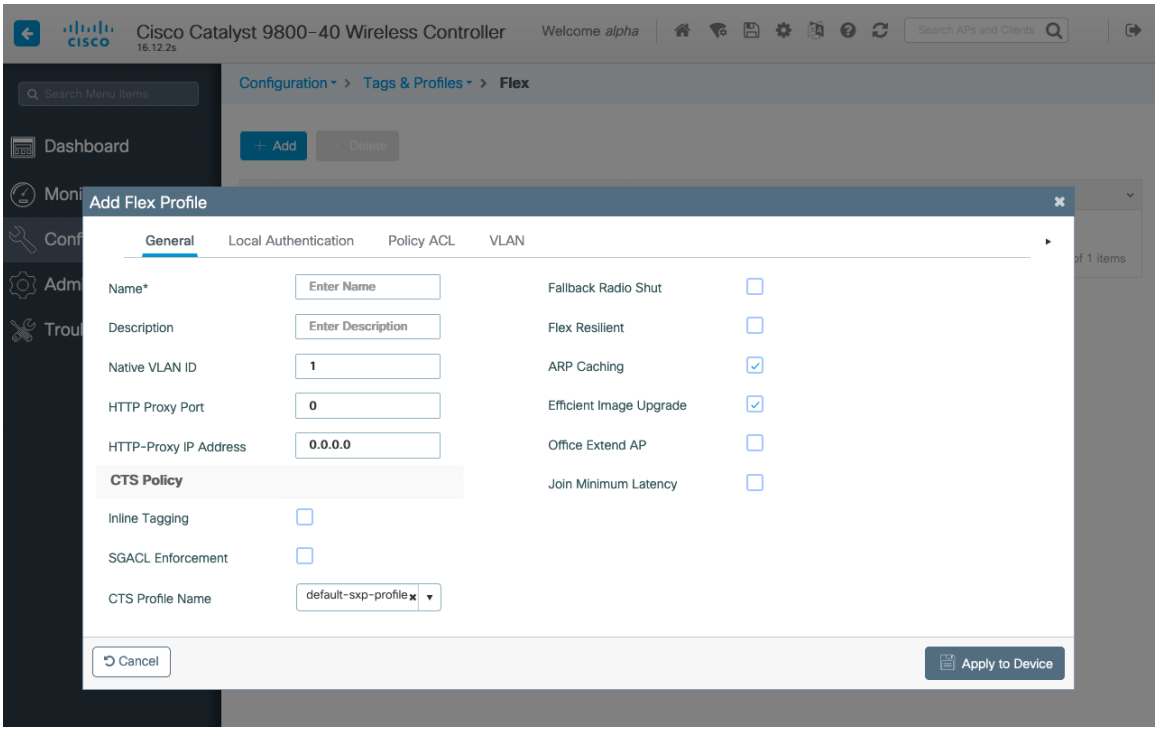
Flex Profiles are then mapped to a Site Tag, which then can be applied to an access point.

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.



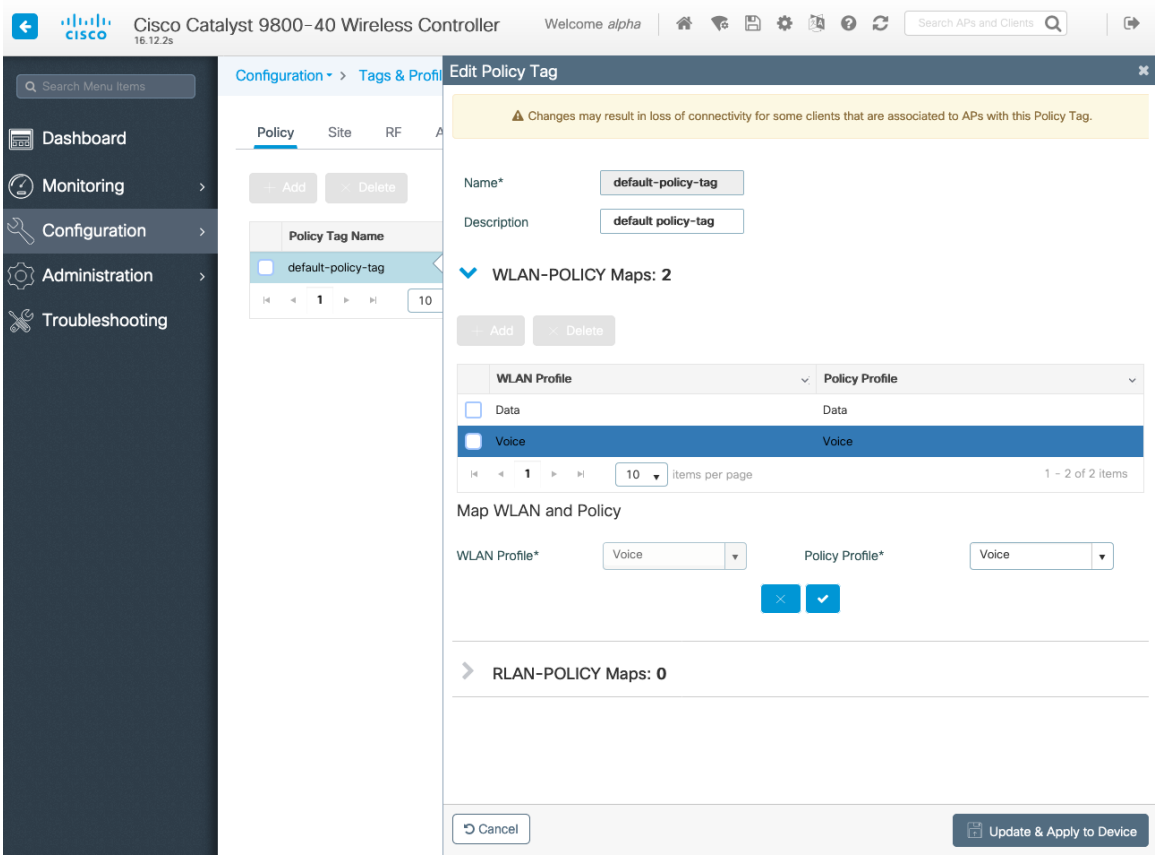
Tags

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.



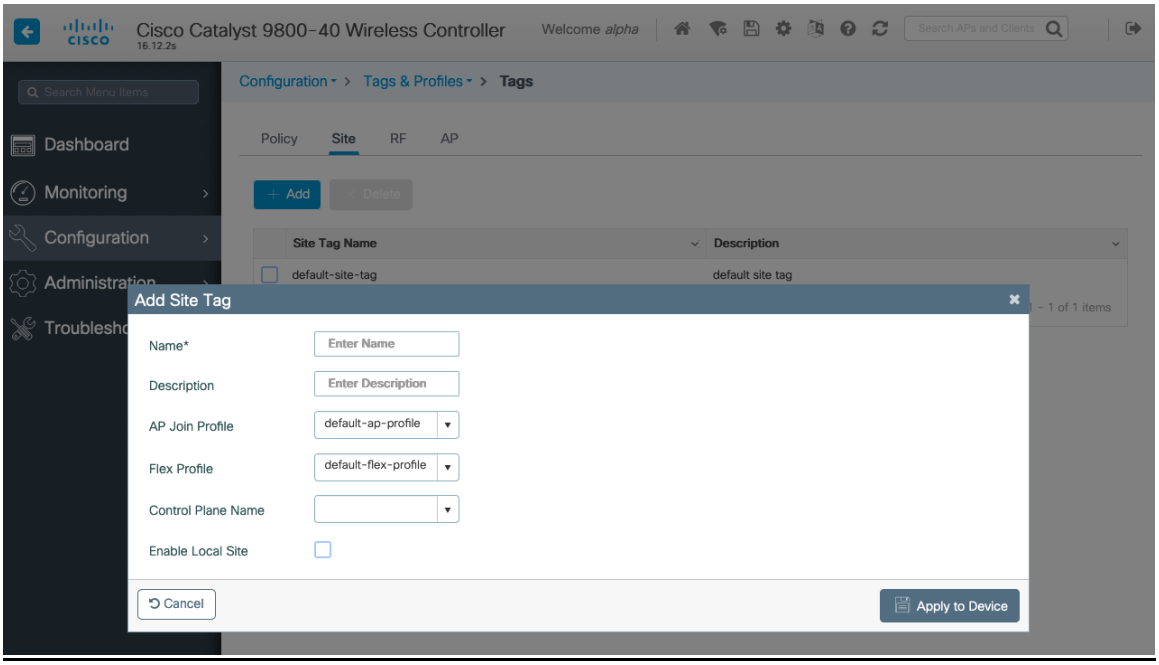
Site Tag

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**.

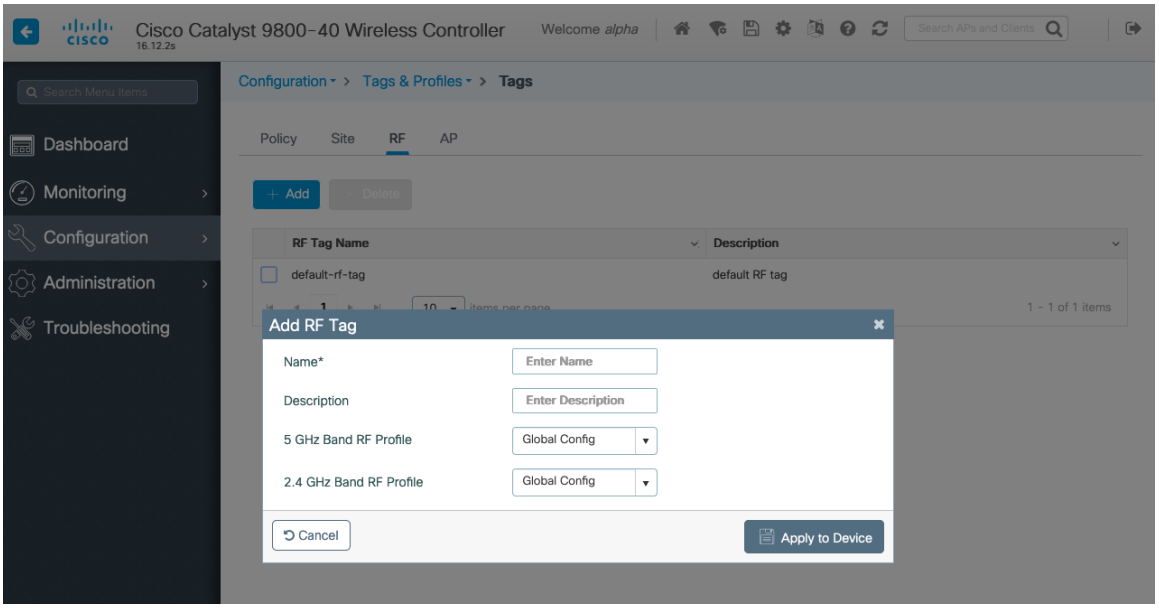


RF Tag

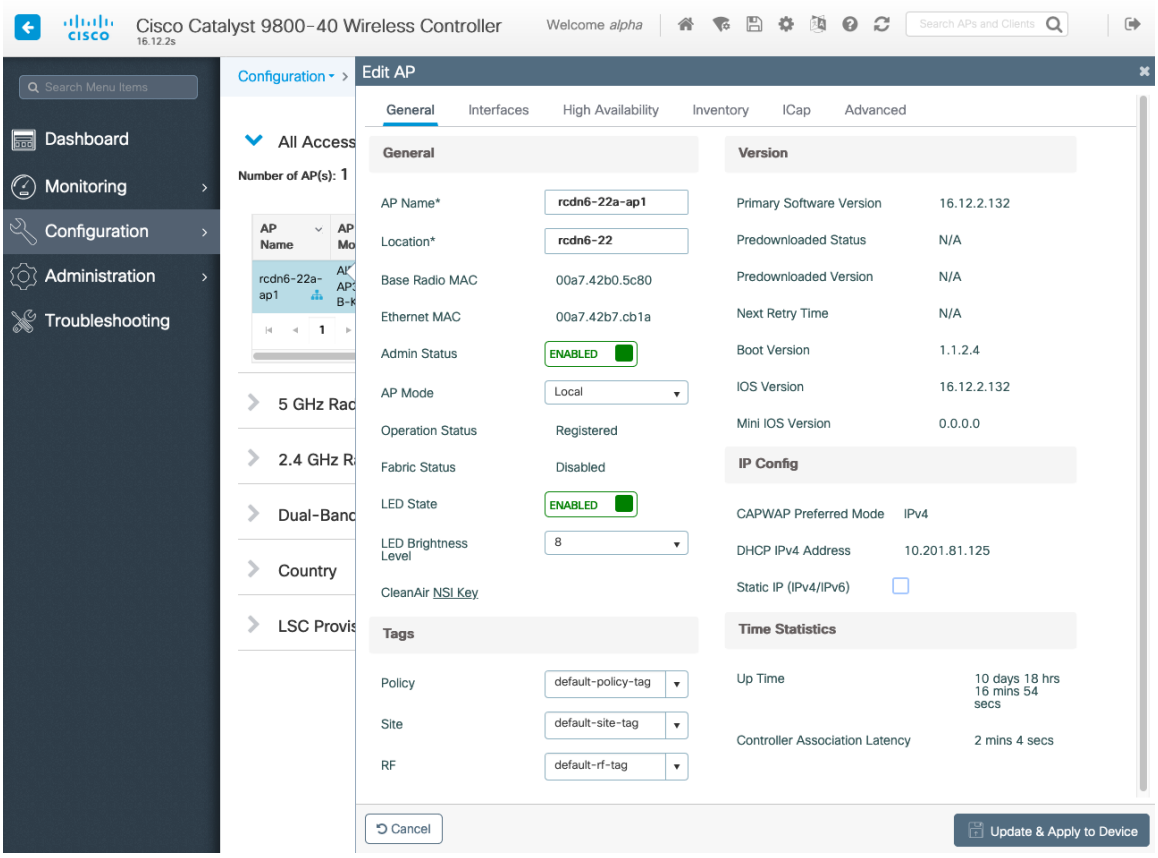
RF Tags define which RF Profiles should be used for 2.4 GHz and 5 GHz.

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

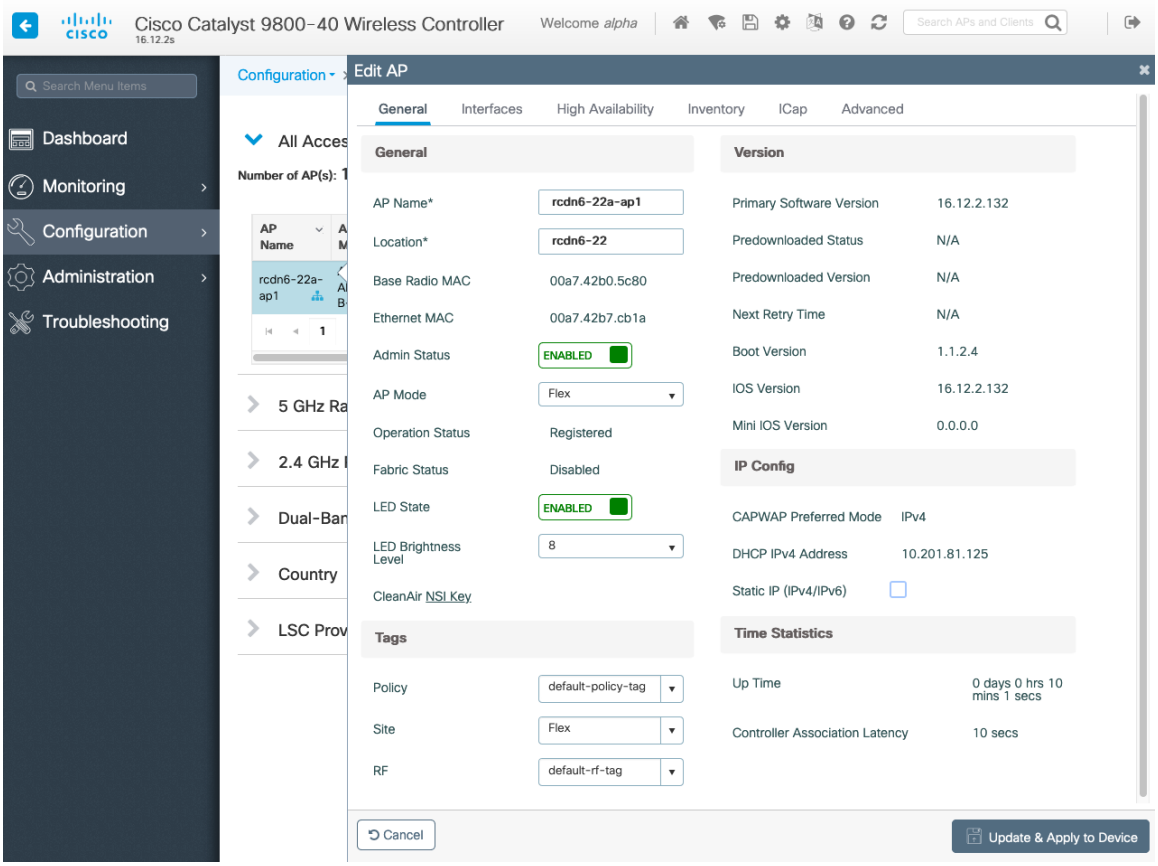
When creating a RF Tag, select the **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be used.



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



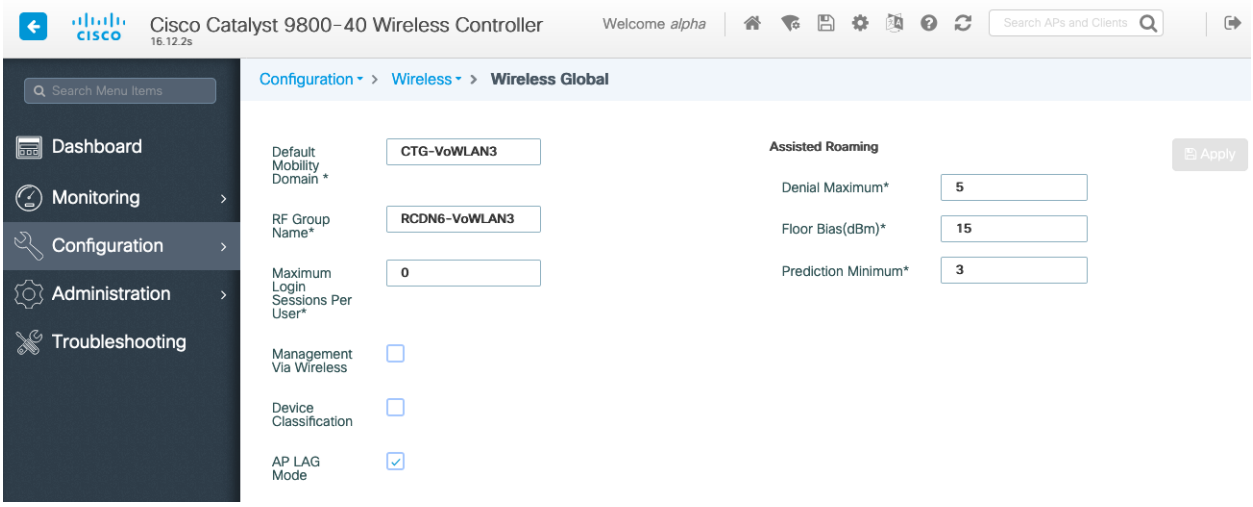
If a Site Tag is applied including a configured Flex Profile, then the **AP Mode** will be changed to **Flex** automatically.



Controller Settings

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

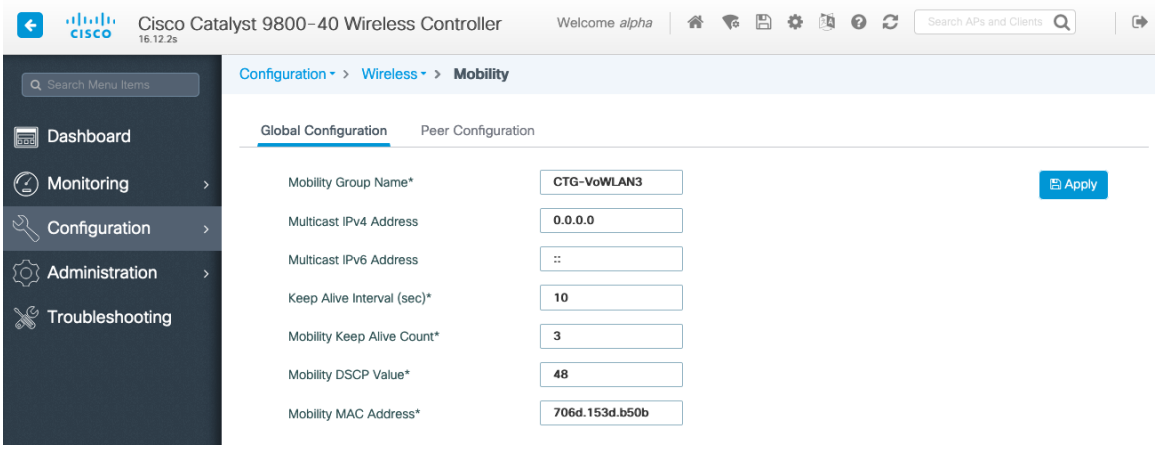
Enable **AP LAG Mode**.

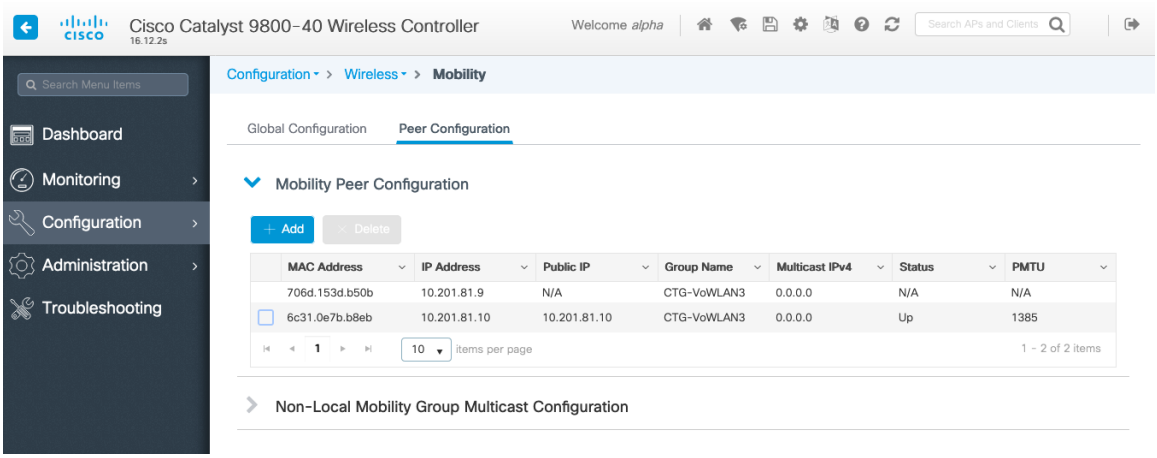


Mobility Settings

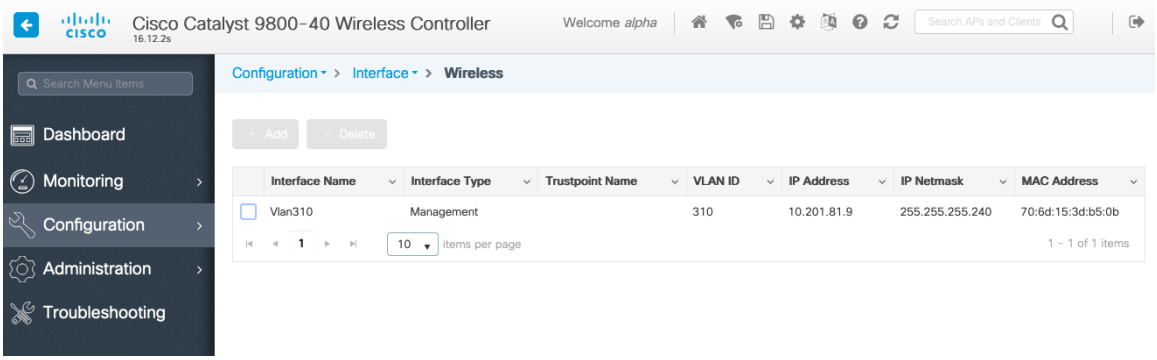
When multiple Cisco Wireless LAN Controllers are to be in the same mobility group, then the IP address and MAC address of each Cisco Wireless LAN Controller should be added to the Mobility Peer configuration.

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.

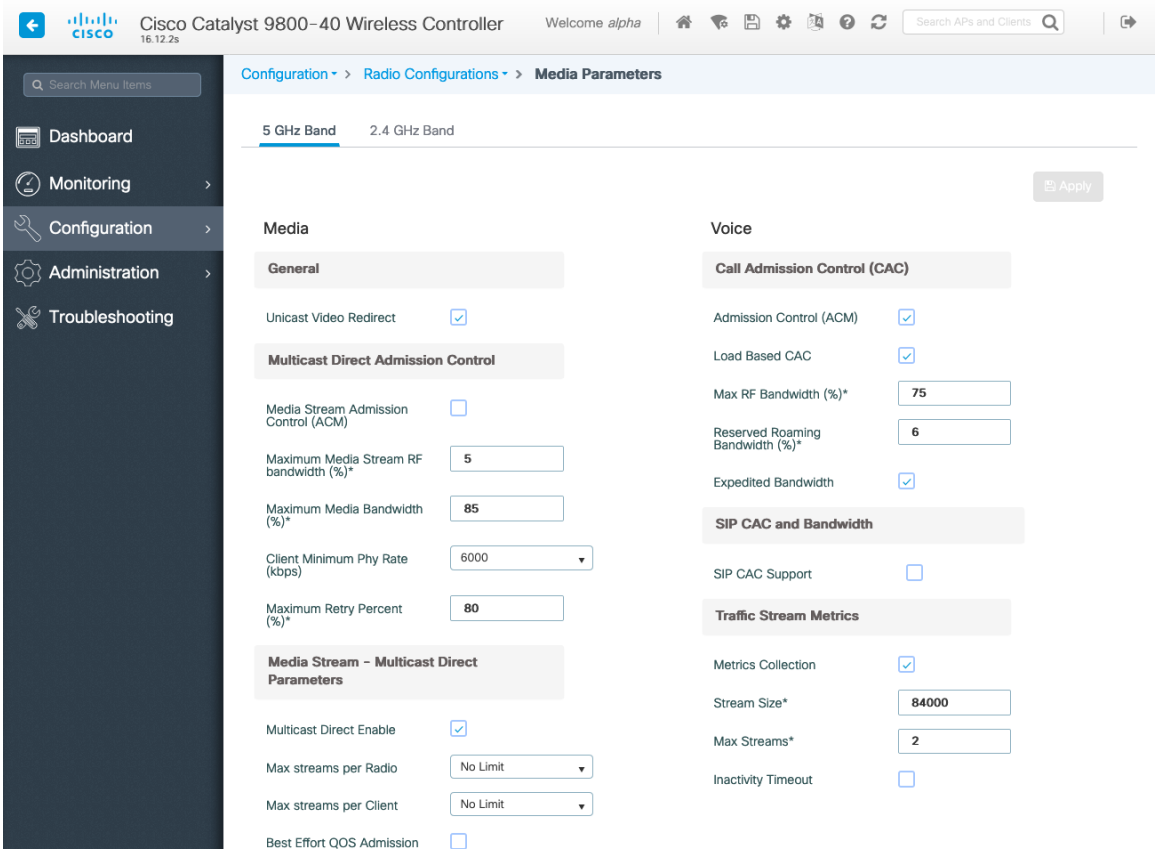
Load Based CAC will account for all energy on the channel.

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.

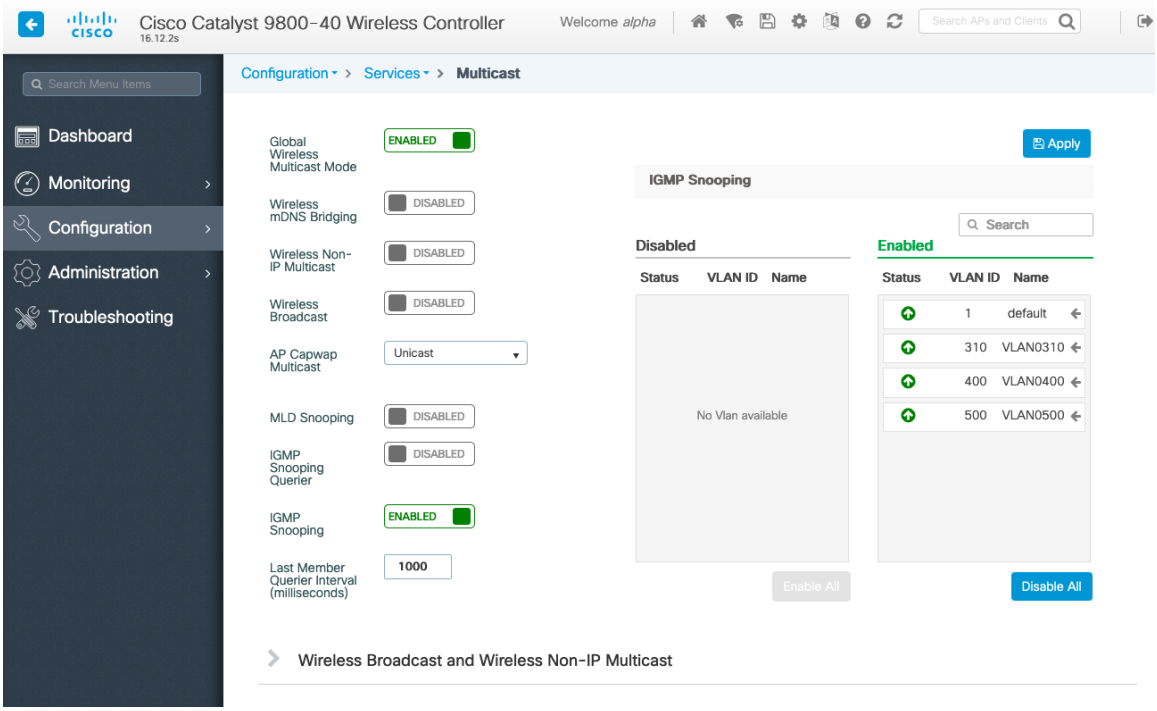
Ensure the **Inactivity Timeout** is Disabled.

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

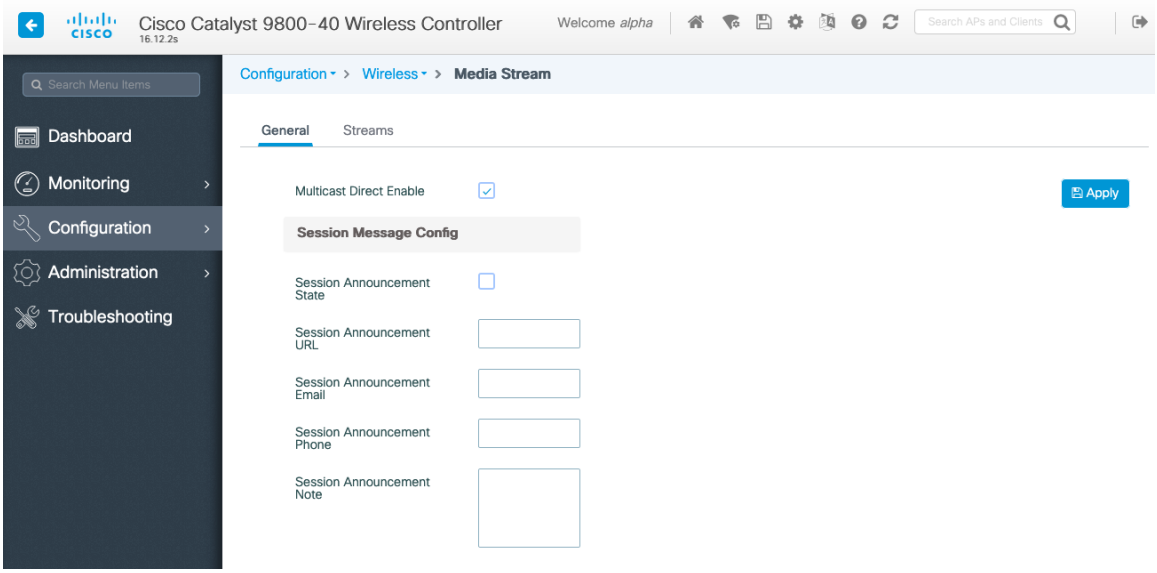


Multicast

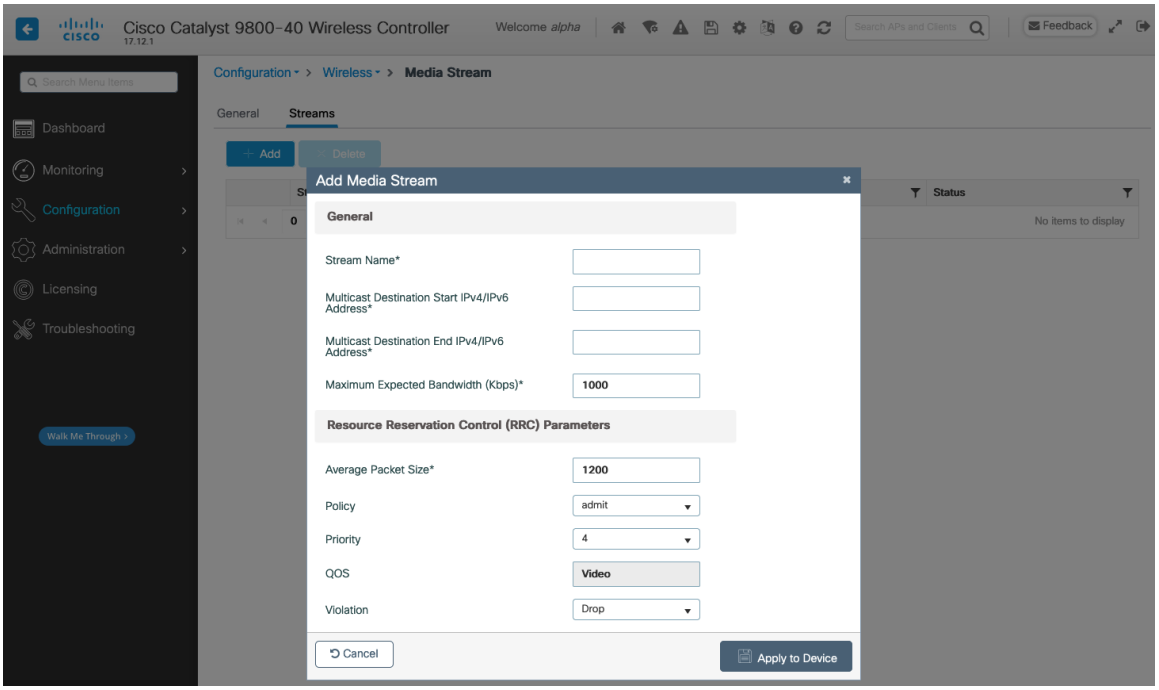
If utilizing multicast, then **Global Wireless Multicast Mode** and **IGMP Snooping** should be **Enabled**.



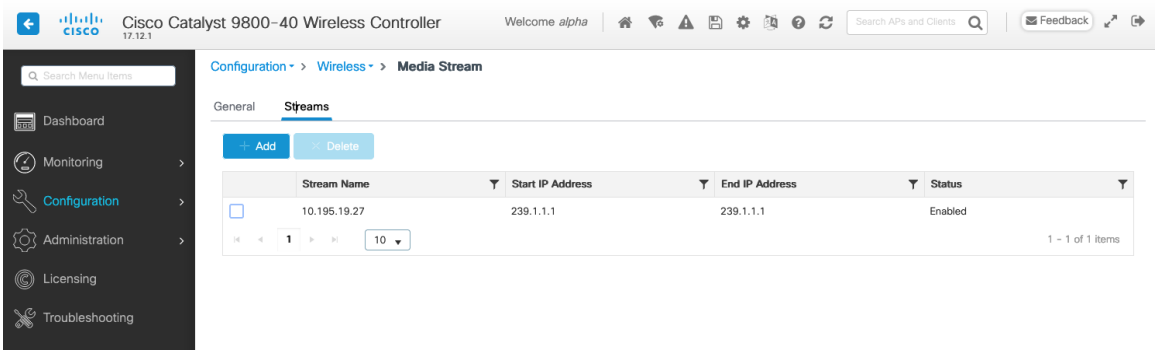
In the Media Stream settings, **Multicast Direct Enable** should be **Enabled**.



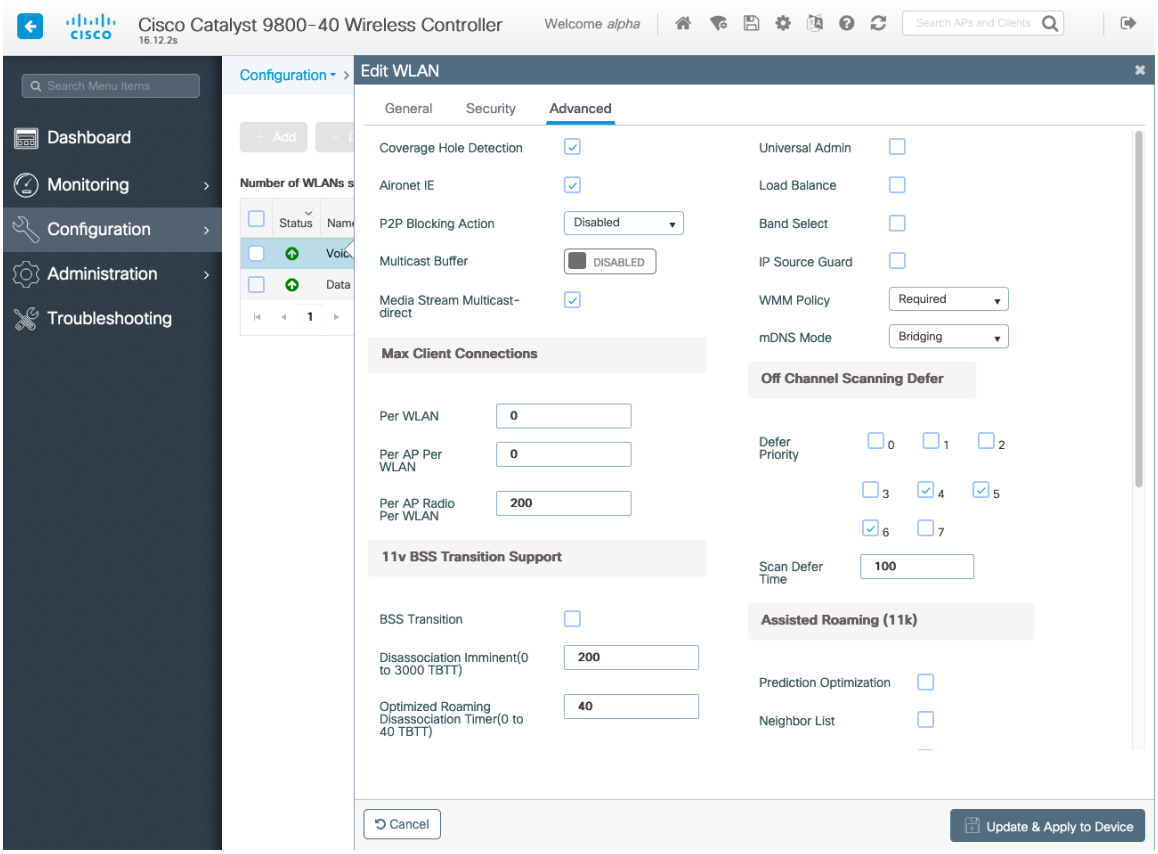
Then configure the media streams as necessary.



Once saved, then the media stream will be displayed.



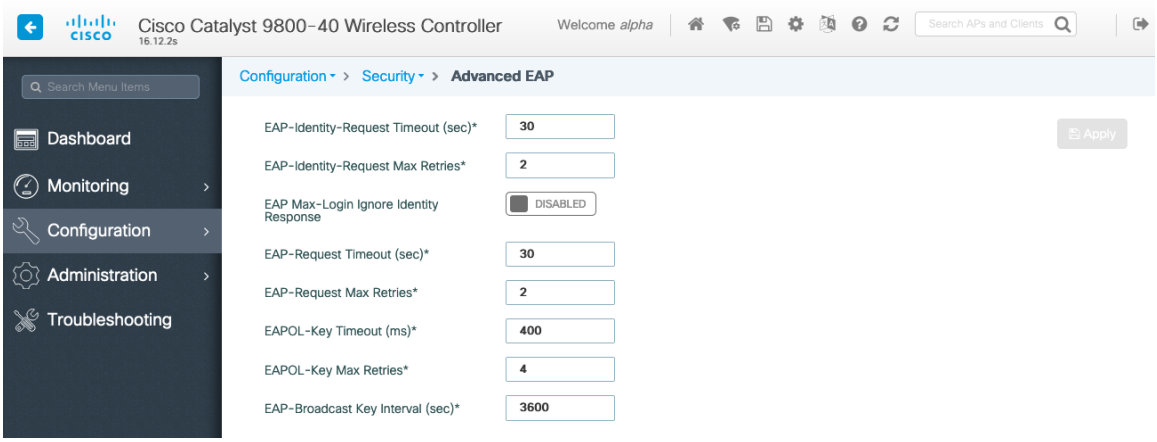
And enable **Multicast Direct** in the WLAN configuration.



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.

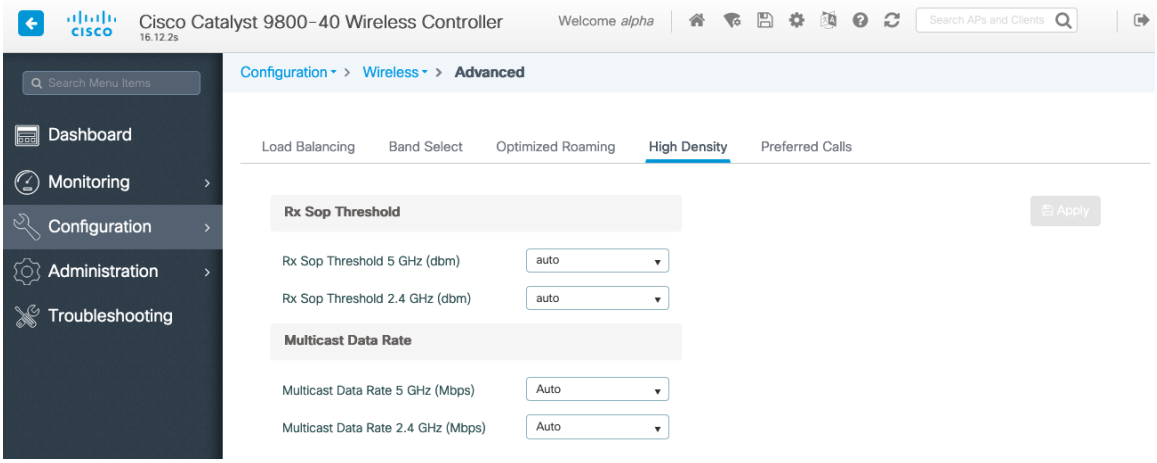
If using 802.1x, then using the default values where the **EAPOL-Key Timeout** is set to 1000 milliseconds and **EAPOL-Key Max Retries** are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.

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

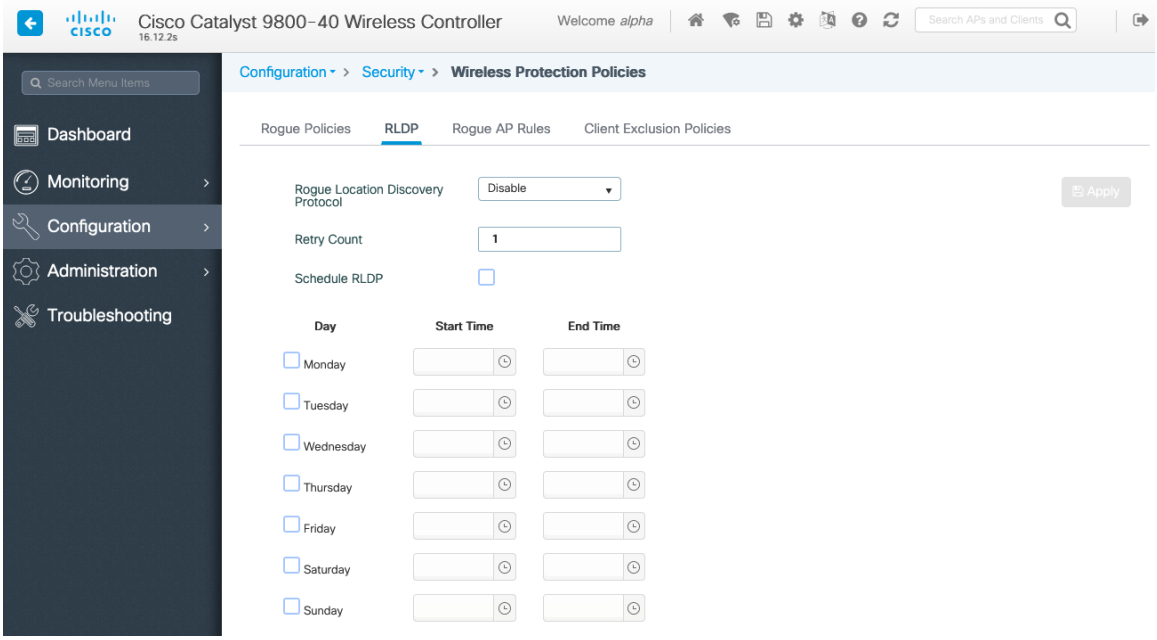
It is recommended to use the default value (**Auto**) for **Rx Sop Threshold**.



Note: It is important to note that adjusting **Rx SOP Threshold** may impact the interoperability of the Cisco Wireless IP Phone 8821 and 8821-EX with Cisco APs.

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

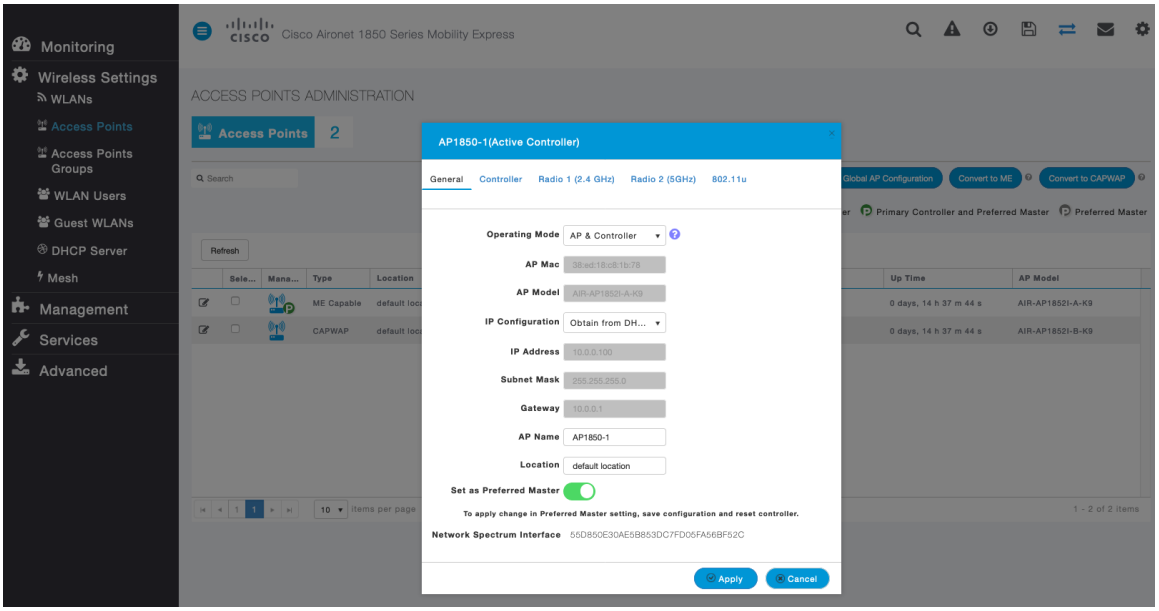
When configuring Cisco Mobility Express and Lightweight Access Points, use the following guidelines:

- Ensure **802.11r (FT)** or **CCKM** is **Enabled**

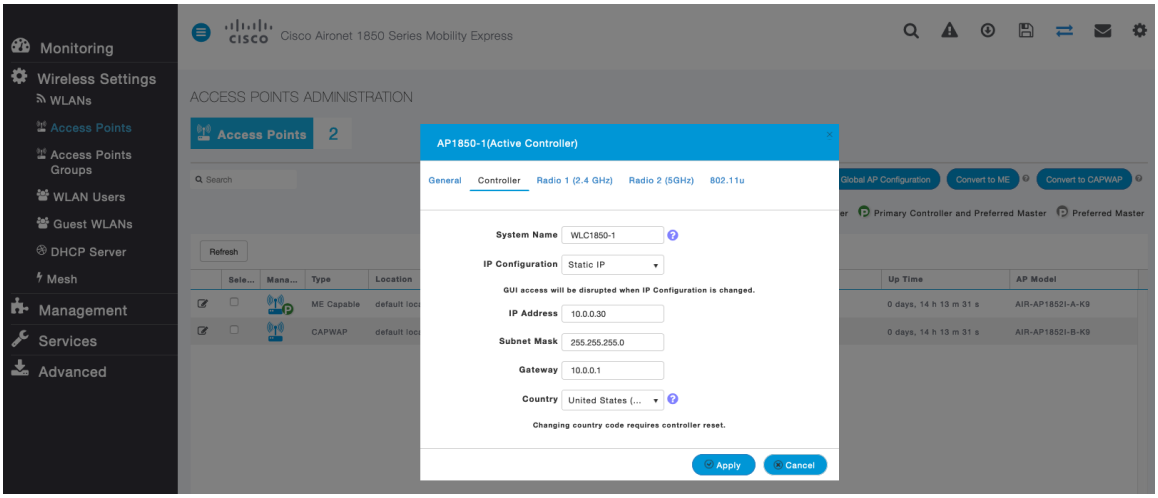
- Set **Quality of Service (QoS)** to **Platinum**
- Ensure **802.11k** is **Disabled**
- Ensure **802.11v** is **Disabled**
- Disable **P2P (Peer to Peer) Blocking Action**
- Set **Client Band Select** to **Disabled**
- Set **Client Load Balancing** to **Disabled**
- Configure the **Data Rates** as 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 IP Phone 8821 and 8821-EX 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).

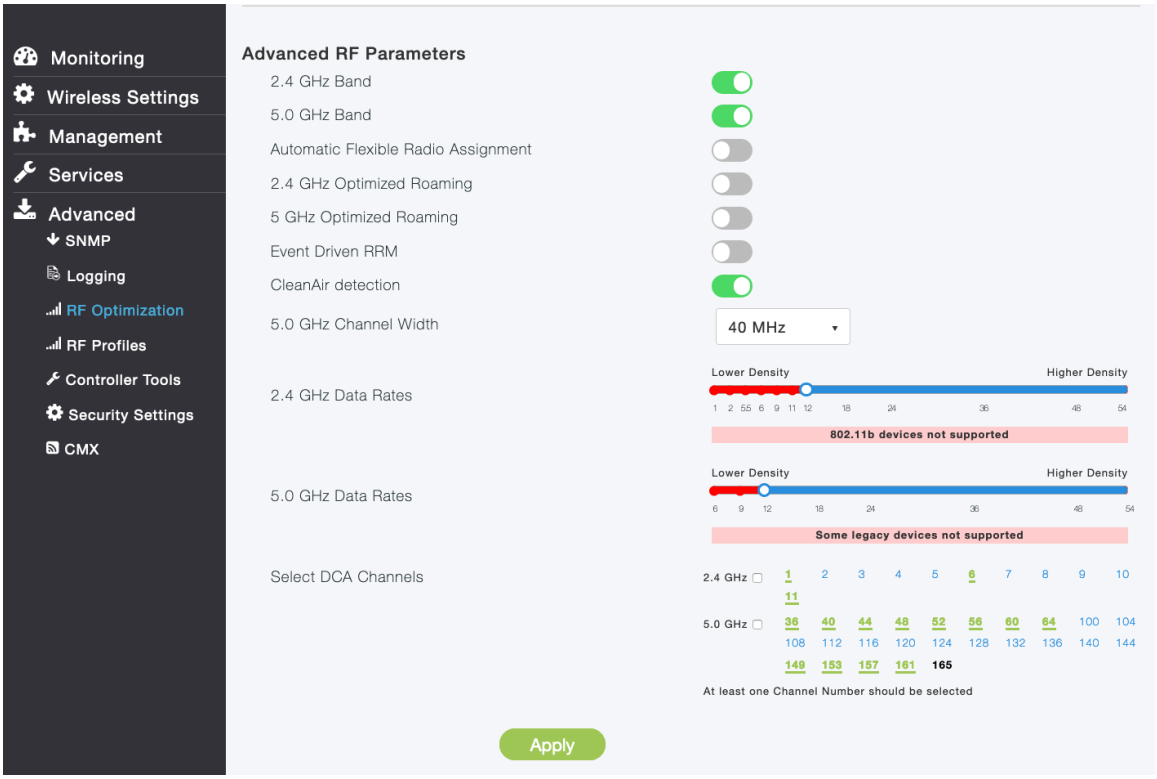
If using 5 GHz, the number of channels can be limited (e.g. 12 channels only) to avoid any potential delay of access point discovery due to having to scan many channels.

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.

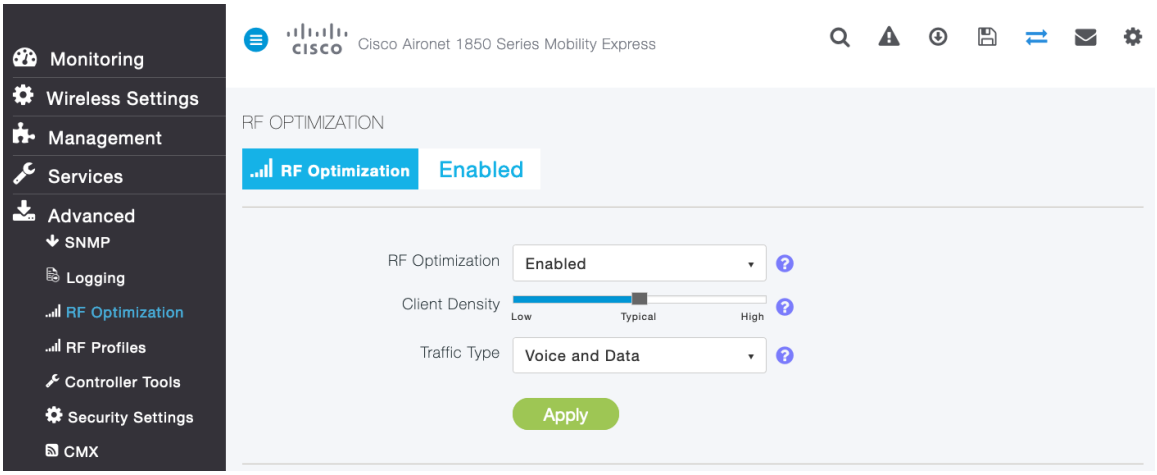
CleanAir detection should be **Enabled** when utilizing Cisco access points with CleanAir technology in order to detect any existing interferers.



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.

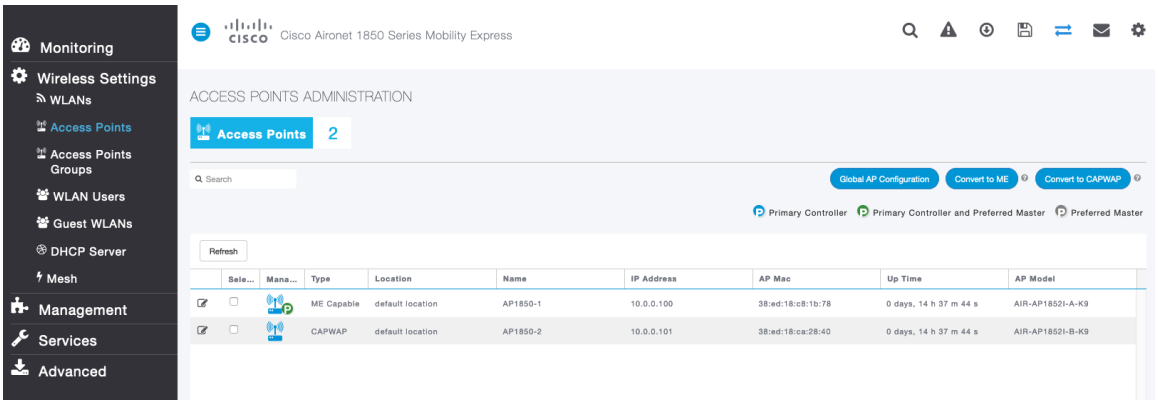
Other access points can be enabled for automatic assignment method and account for the access points that are statically configured.

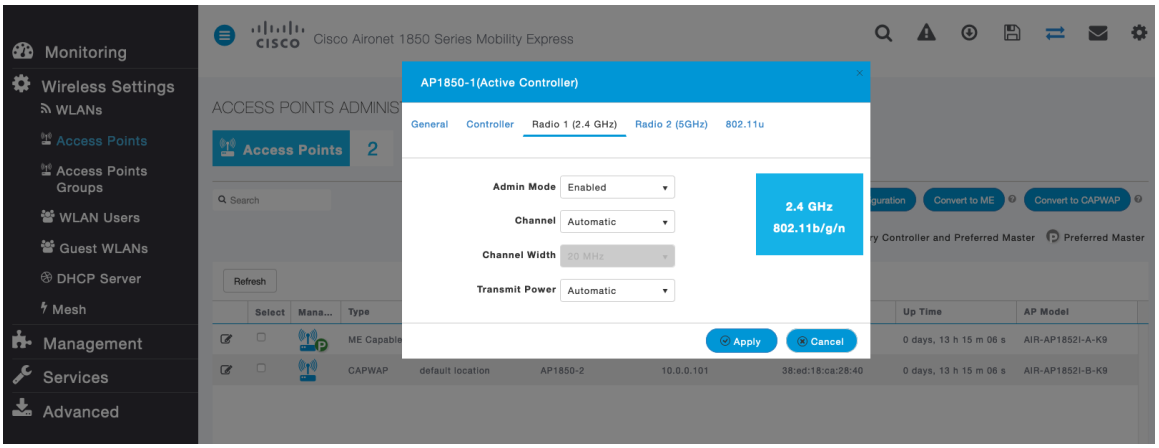
This may be necessary if there is an intermittent interferer present in an area.

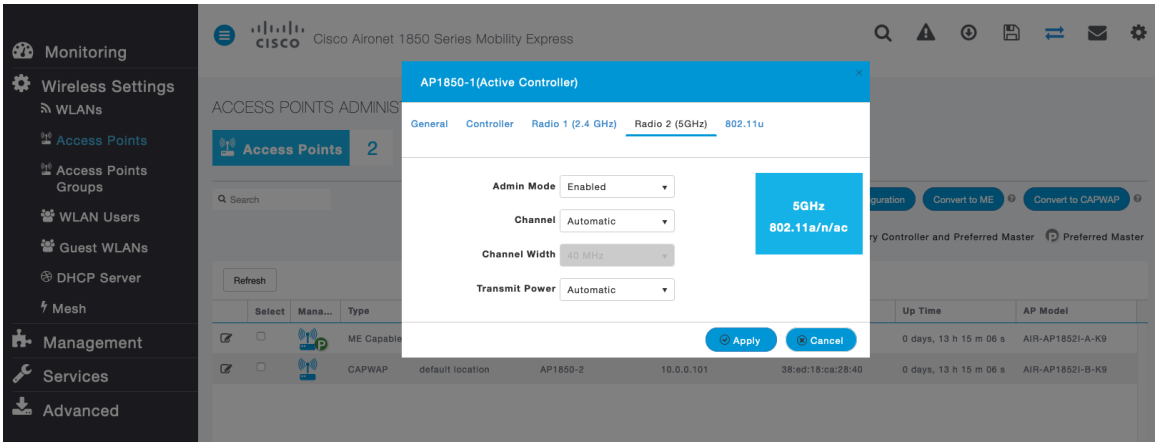
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

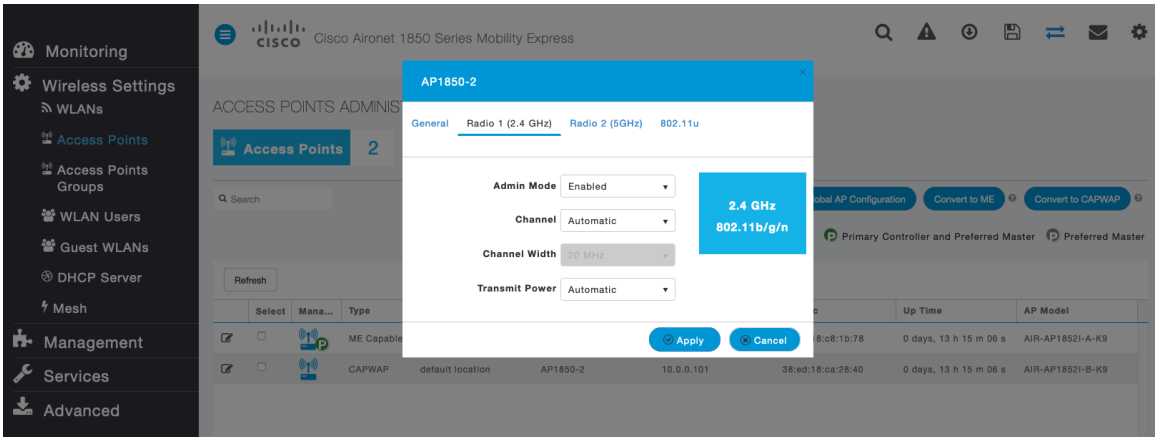
It is recommended to use channel bonding only if using 5 GHz.

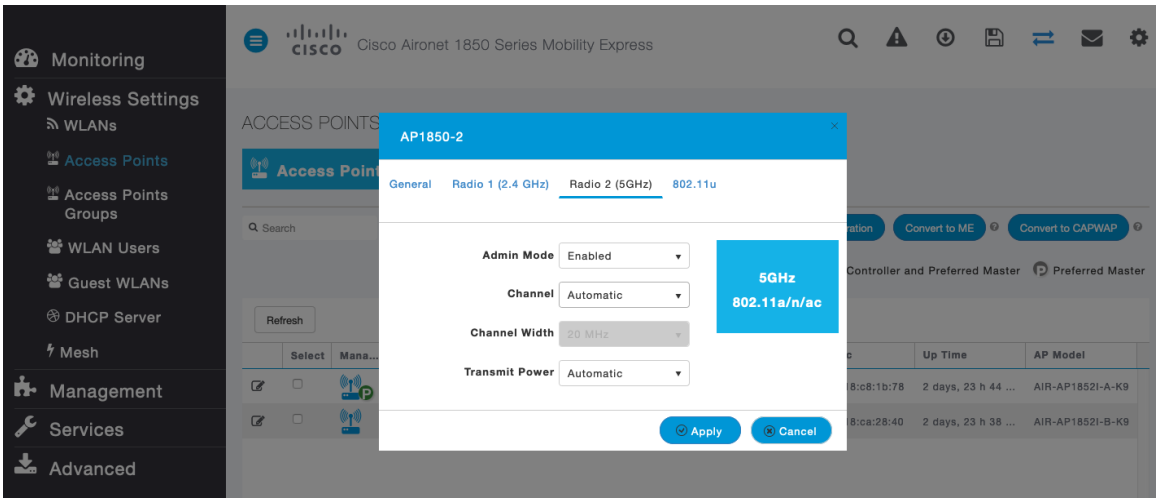
It is recommended to utilize the same channel width for all access points.











WLAN Settings

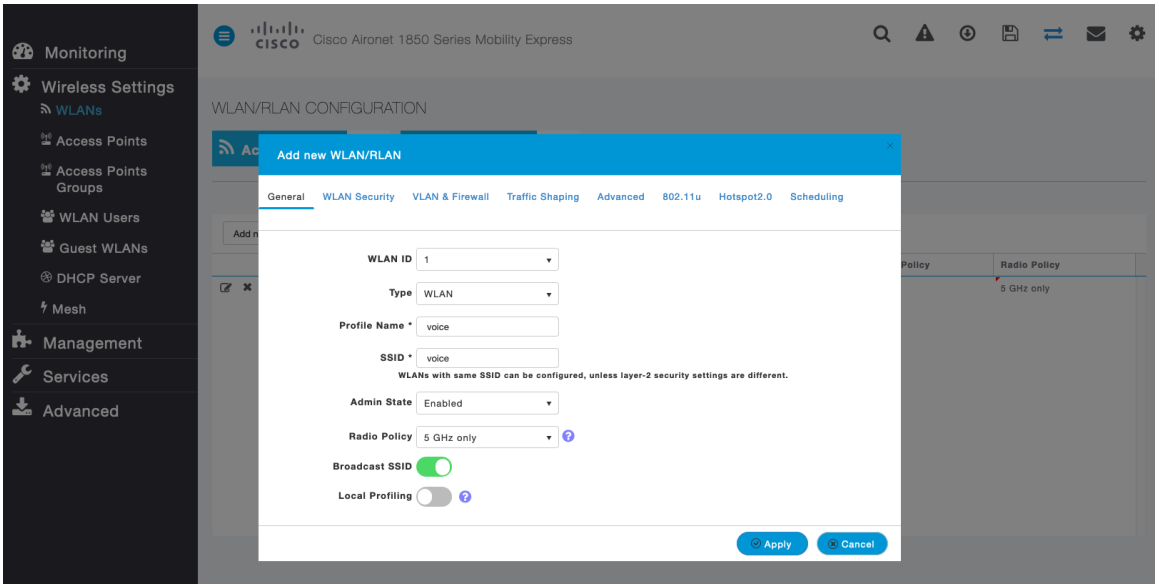
It is recommended to have a separate SSID for the Cisco Wireless IP Phone 8821 and 8821-EX.

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

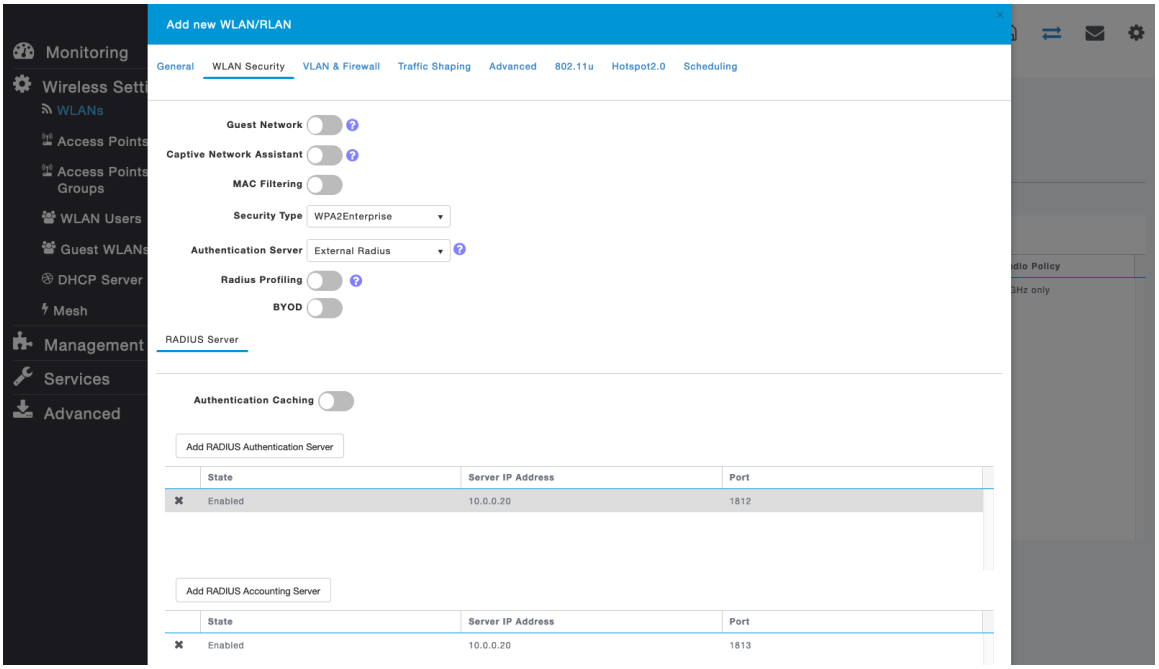
The SSID to be used by the Cisco Wireless IP Phone 8821 and 8821-EX can be configured to only apply to a certain 802.11 radio type (e.g. 5 GHz only).

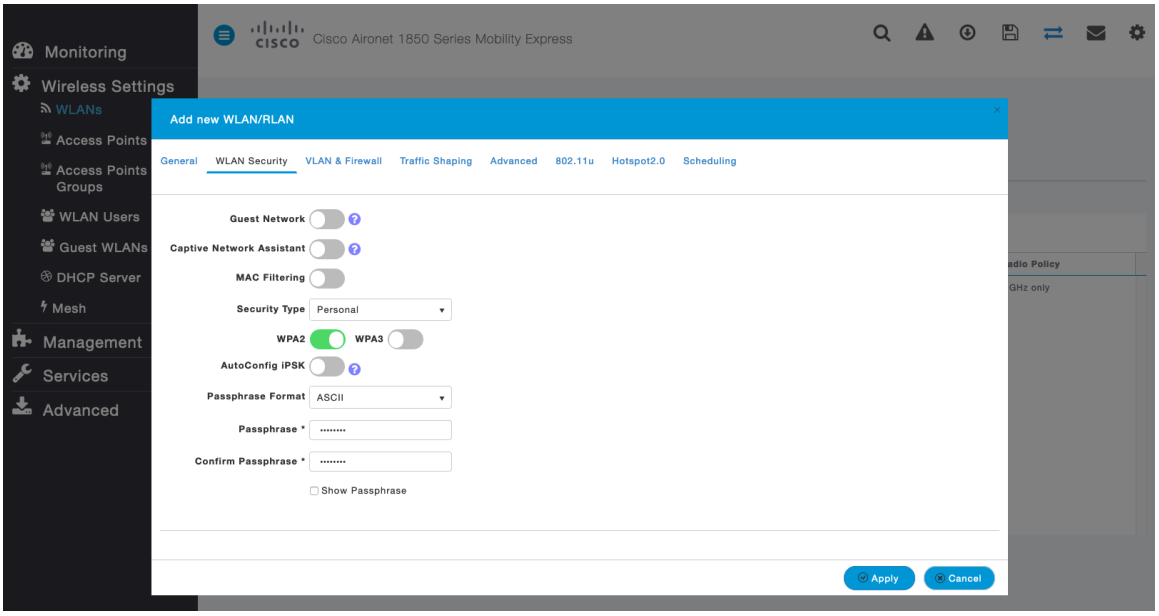
It is recommended to have the Cisco Wireless IP Phone 8821 and 8821-EX operate on the 5 GHz band only due to have many channels available and not as many interferers as the 2.4 GHz band has.

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.

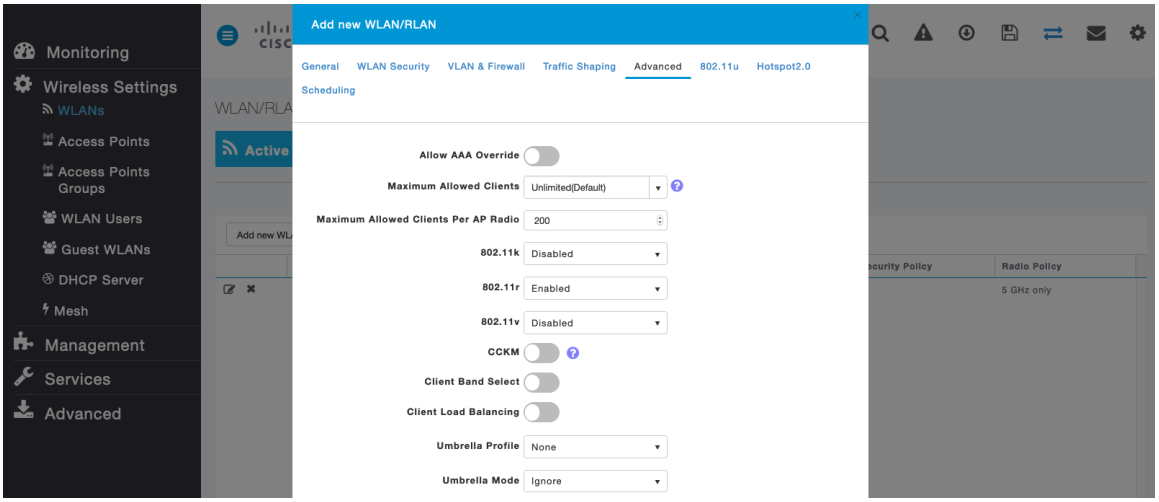




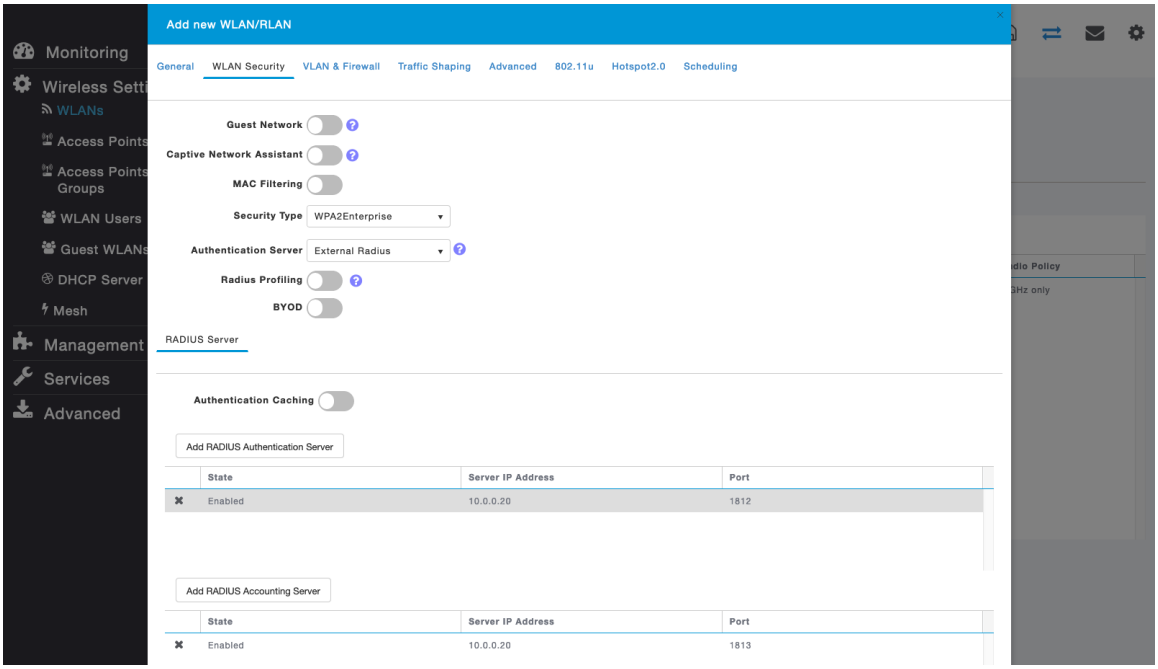
Set **802.11r** to **Enabled** in the **Advanced** tab of the WLAN configuration.

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

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



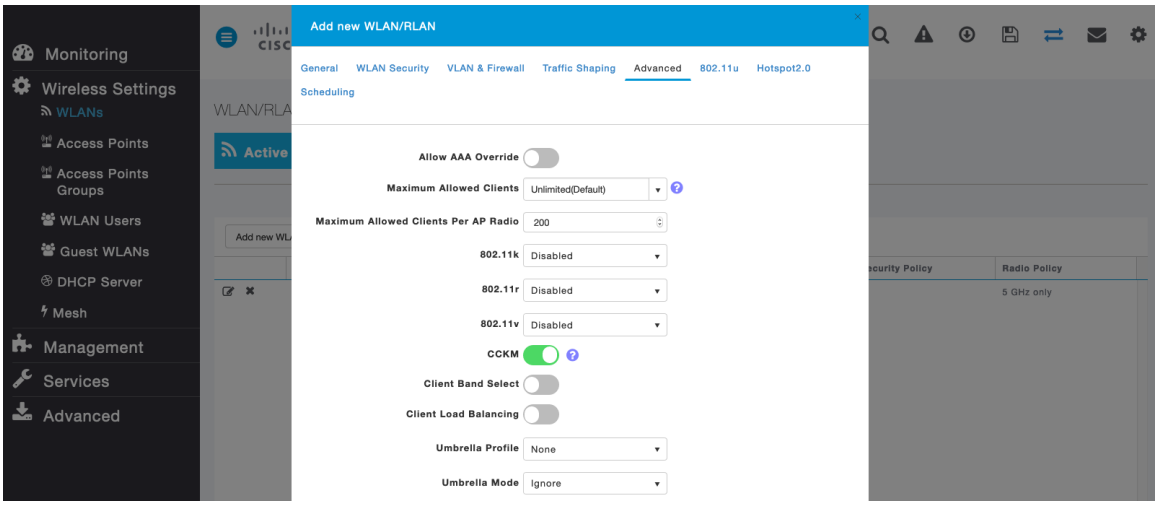
To utilize CCKM for fast secure roaming, set **Security Type** to **WPA2Enterprise**.



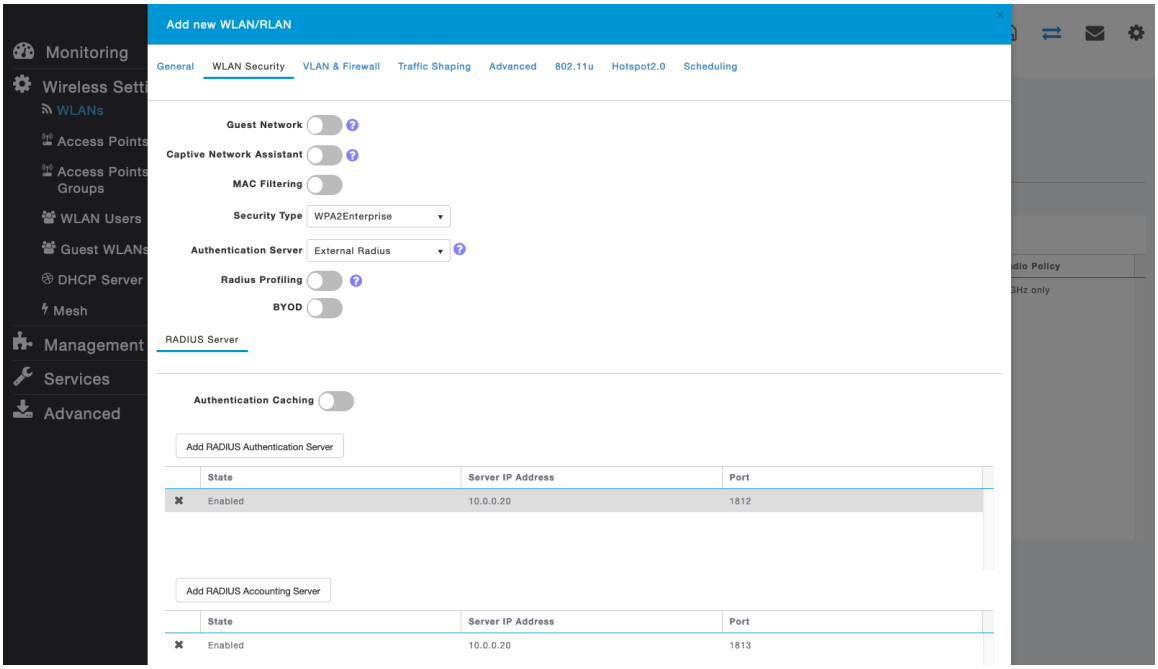
Set **CCKM** to **Enabled** in the **Advanced** tab of the WLAN configuration.

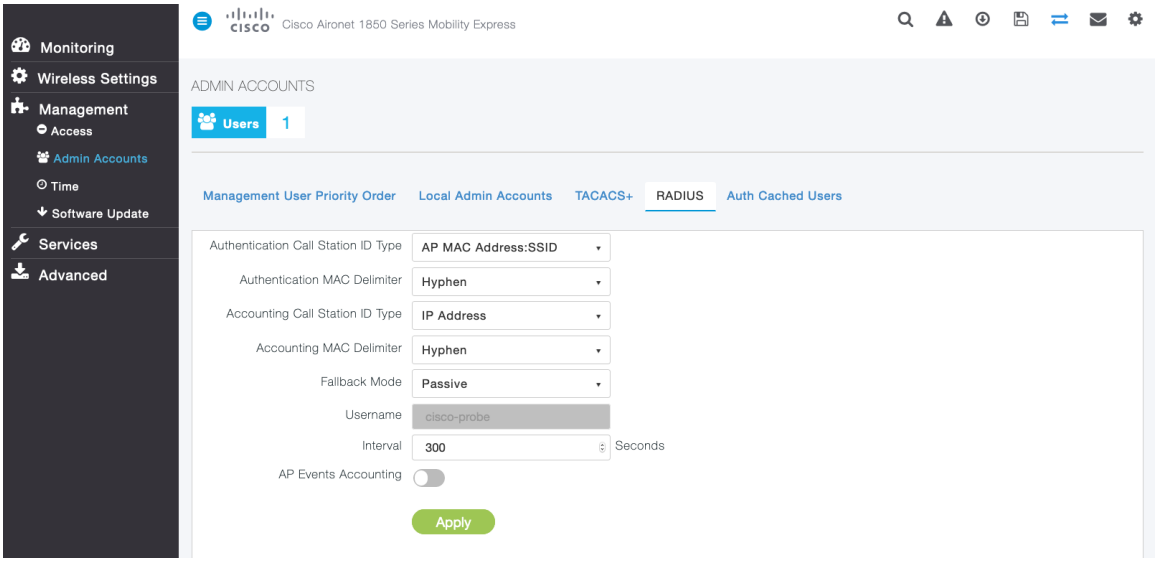
Ensure **Client Band Select** and **Client Load Balancing** are disabled.

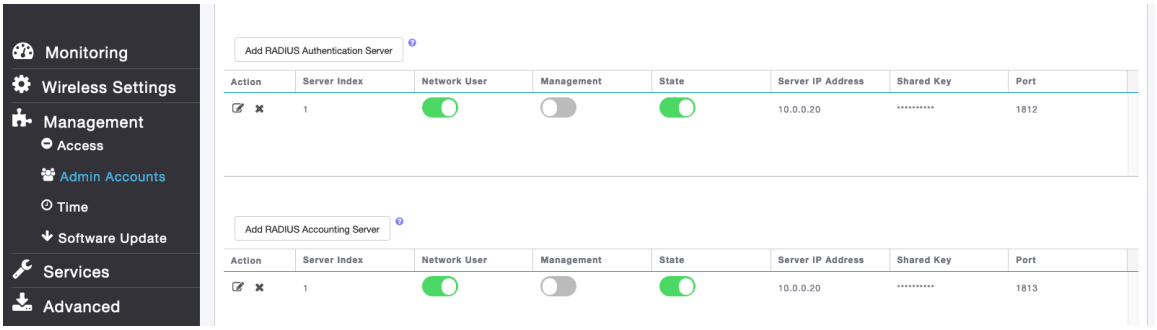
802.11k and 802.11v are not supported, therefore should be disabled.



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

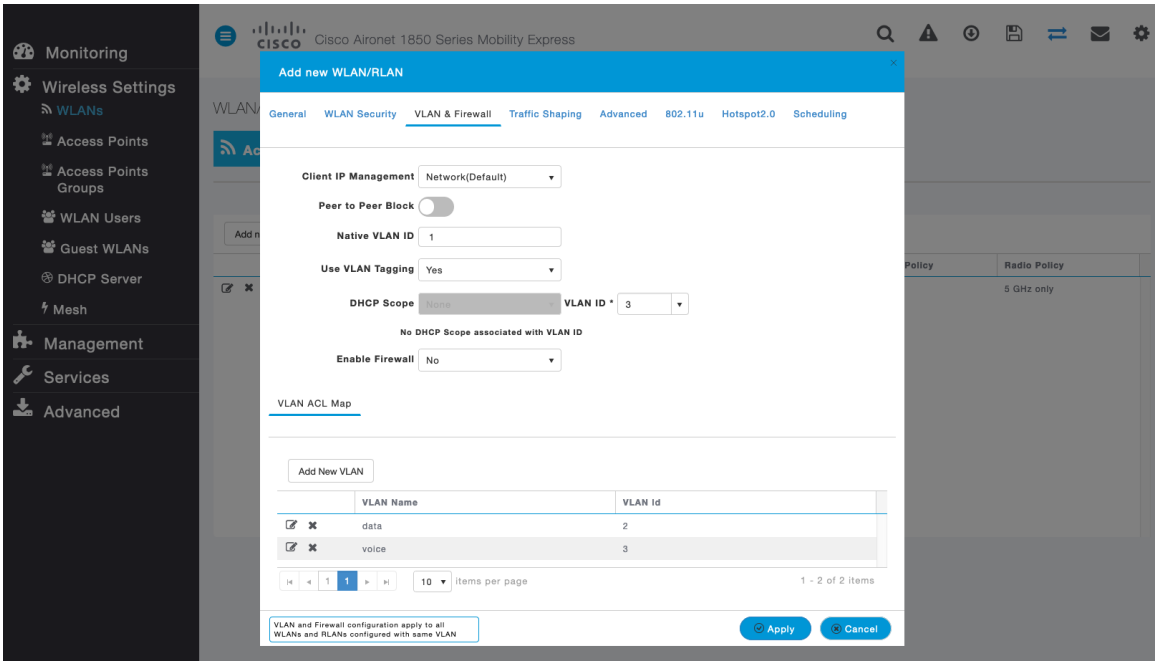




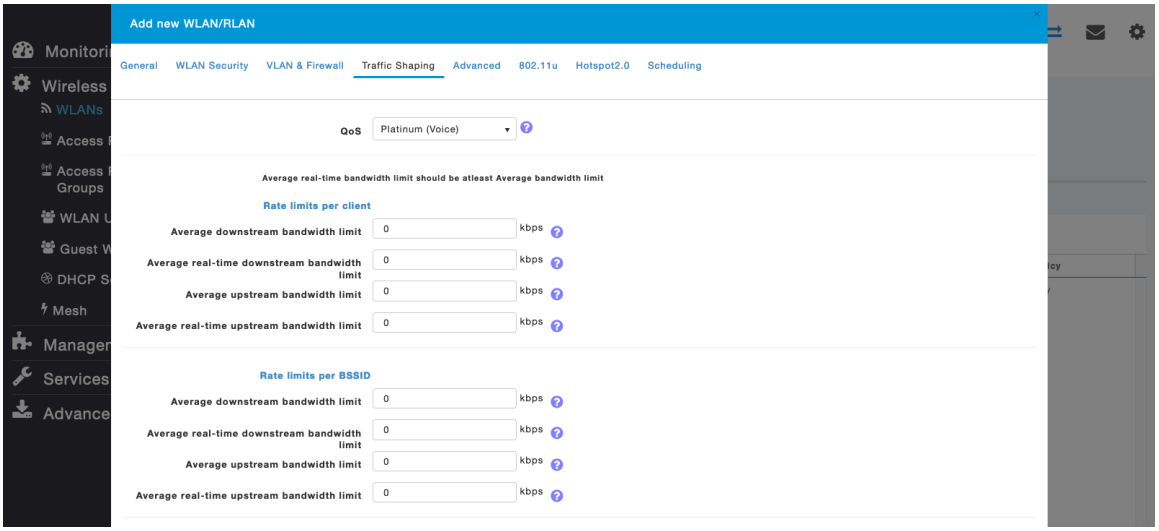


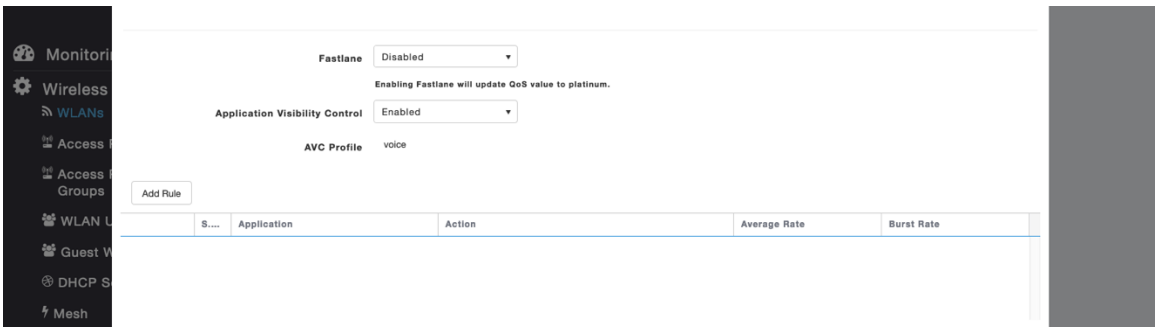
Configure the **Native VLAN ID** and **VLAN ID** for the WLAN as necessary.

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

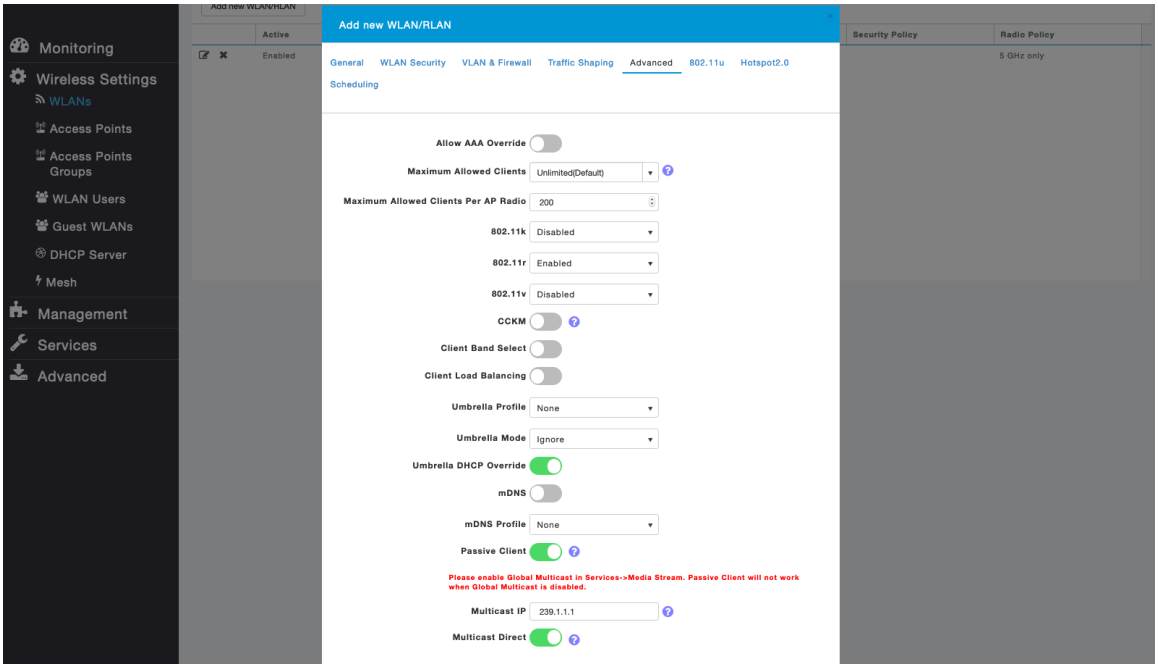


Ensure **Platinum (Voice)** is selected for **QoS**.



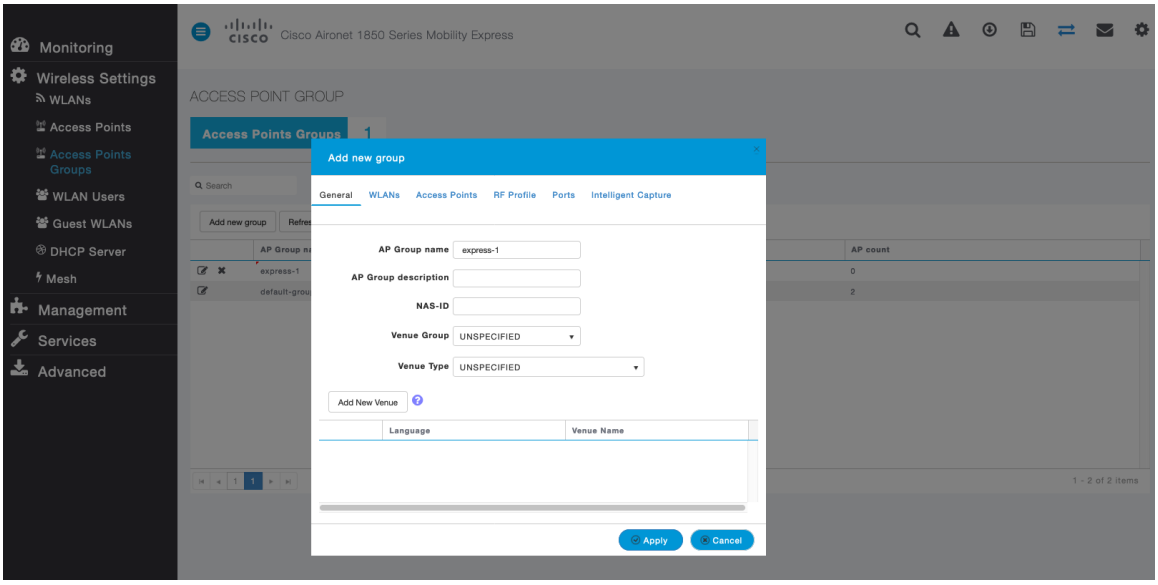


The **Maximum Allowed Clients** and **Maximum Allowed Clients Per AP Radio** can be configured as necessary.

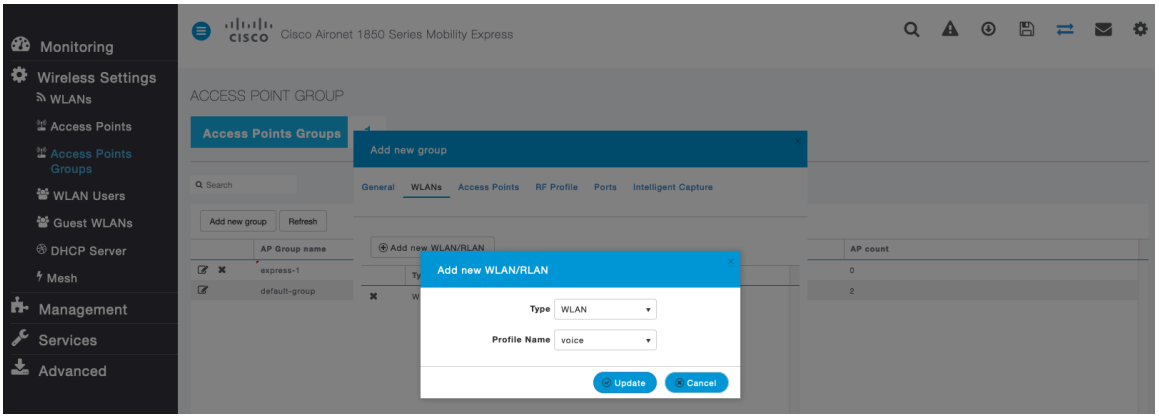


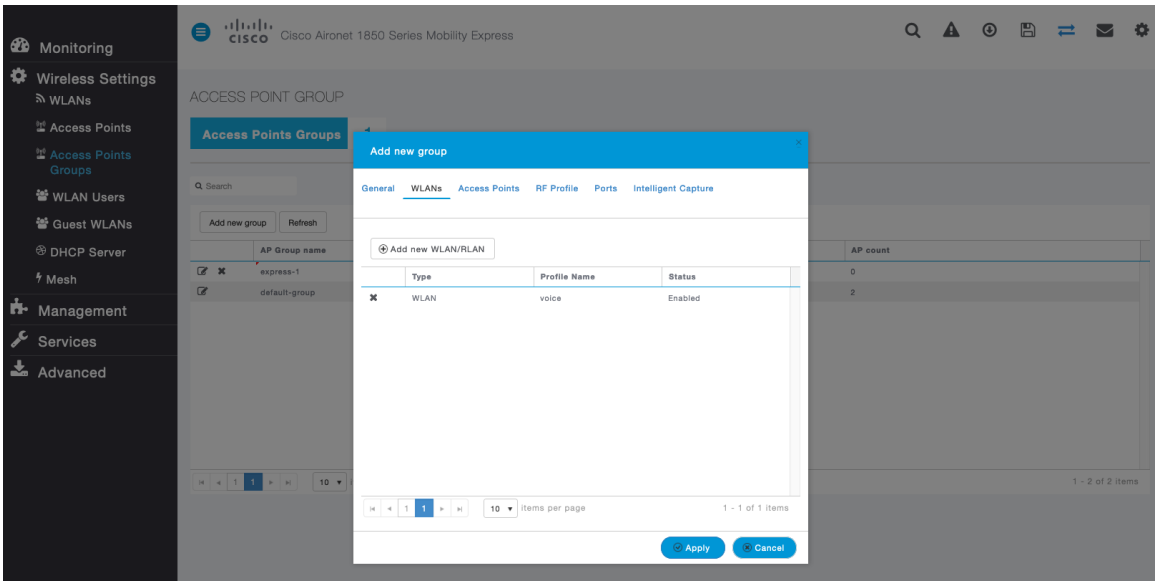
AP Groups

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



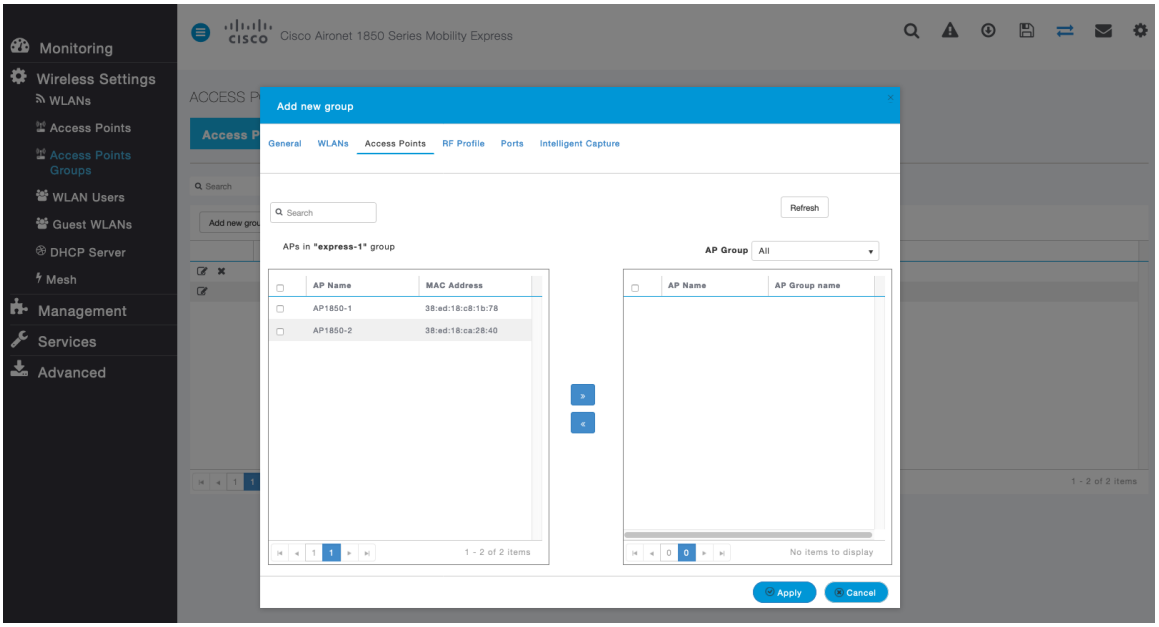
On the **WLANs** tab, select the desired WLANs and interfaces to map to then select **Add**.



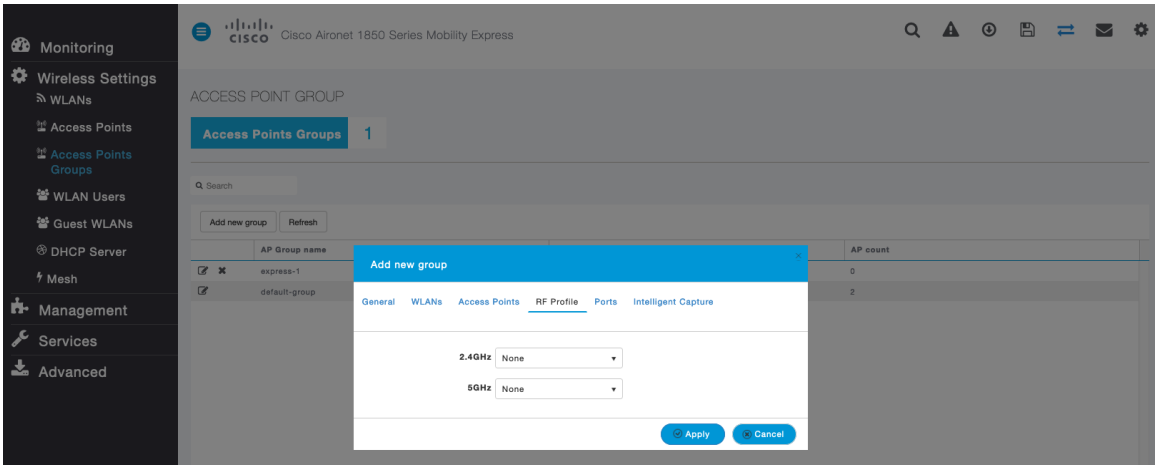


On the **Access Points** tab, select the desired access points then select **Apply**.

Those access points will then reboot.



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



RF Profiles

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

It is recommended to have the SSID used by the Cisco Wireless IP Phone 8821 and 8821-EX to be applied to 5 GHz radios only.

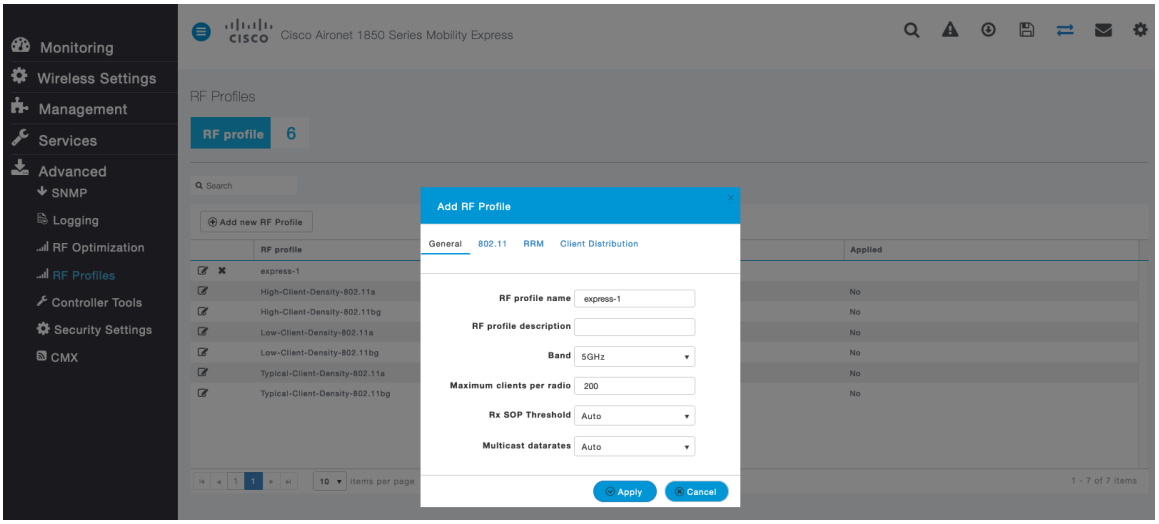
RF Profiles are applied to an AP group once created.

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**.

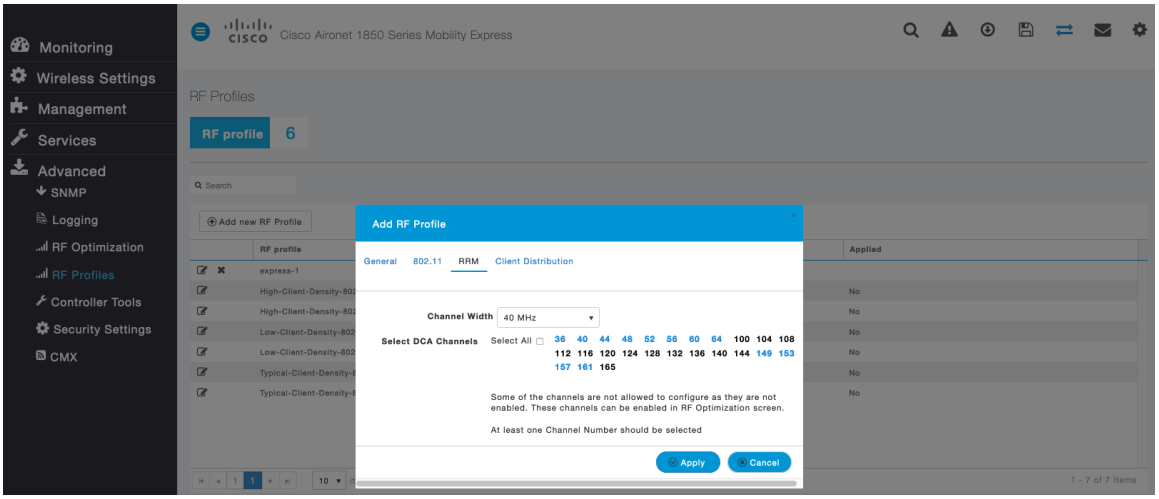


Note: It is important to note that adjusting **Rx SOP Threshold** may impact the interoperability of the Cisco Wireless IP Phone 8821 and 8821-EX with Cisco APs.

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.

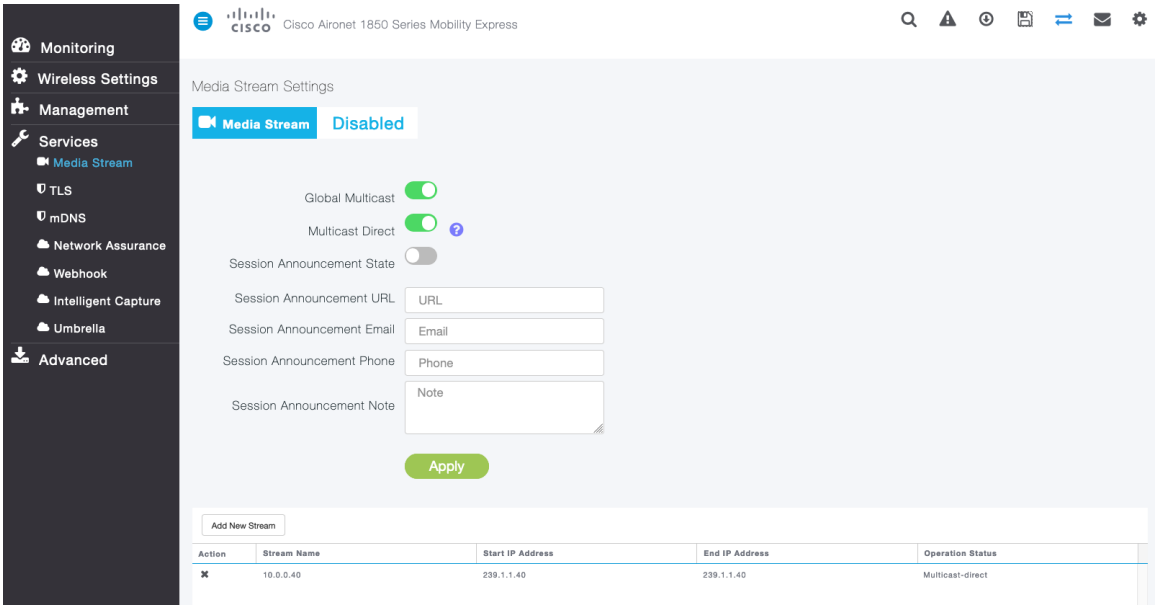
On the **RRM** tab, the **Channel Width** settings and **DCA Channels** can be configured.



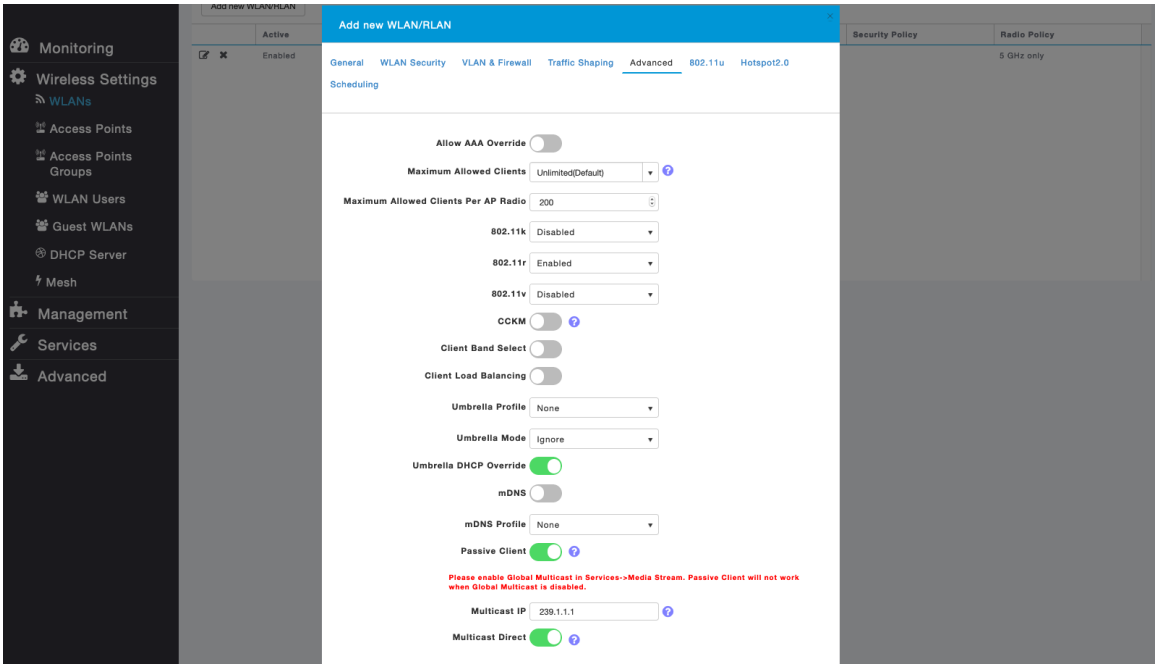
Multicast Direct

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

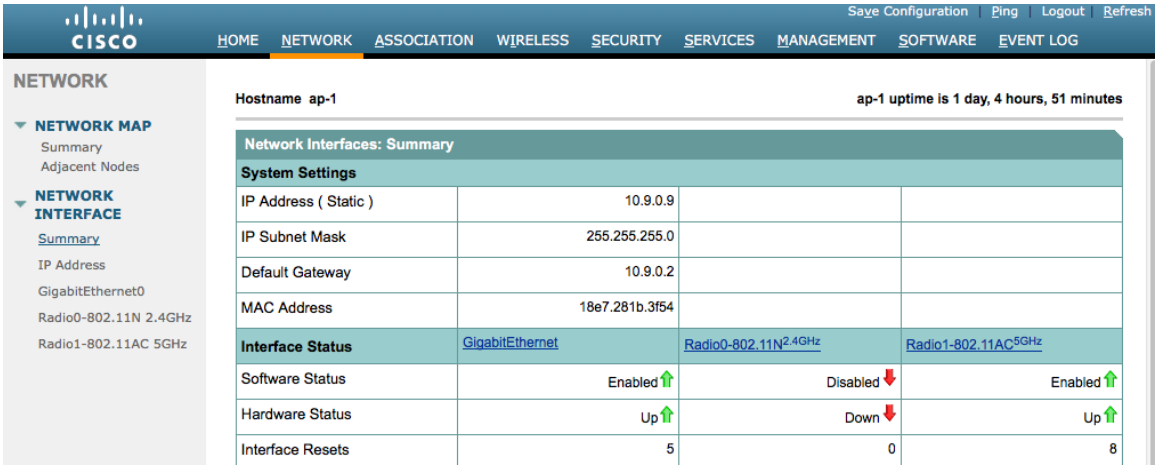
When configuring Cisco Autonomous Access Points, use the following guidelines:

- Ensure **802.11r (FT)** or **CCKM** is **Enabled**
- Ensure **802.11k** is **Disabled**
- Ensure **802.11v** is **Disabled**
- 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 IP Phone 8821 and 8821-EX 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.

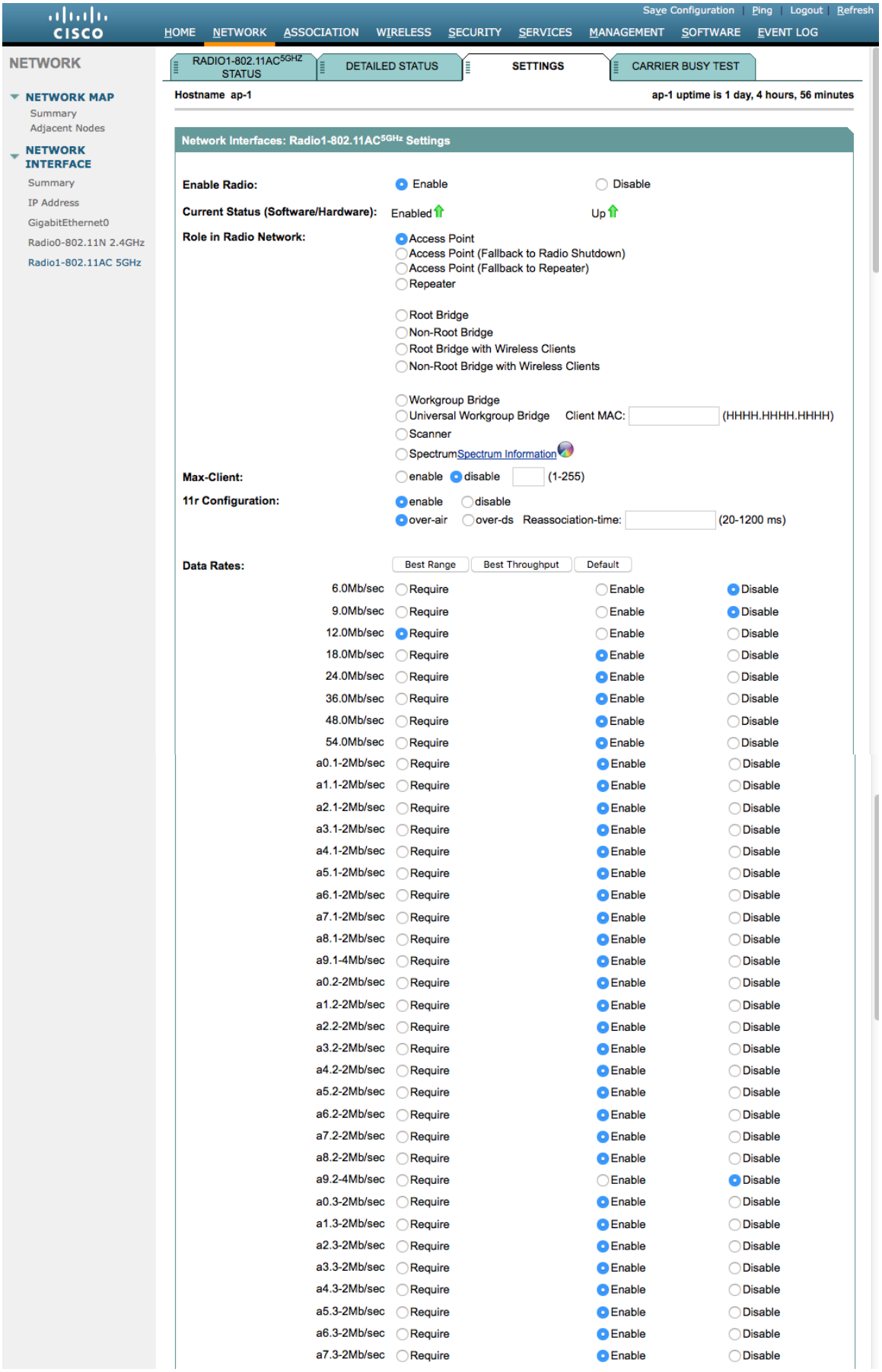
It is recommended to utilize the same channel width for all access points.

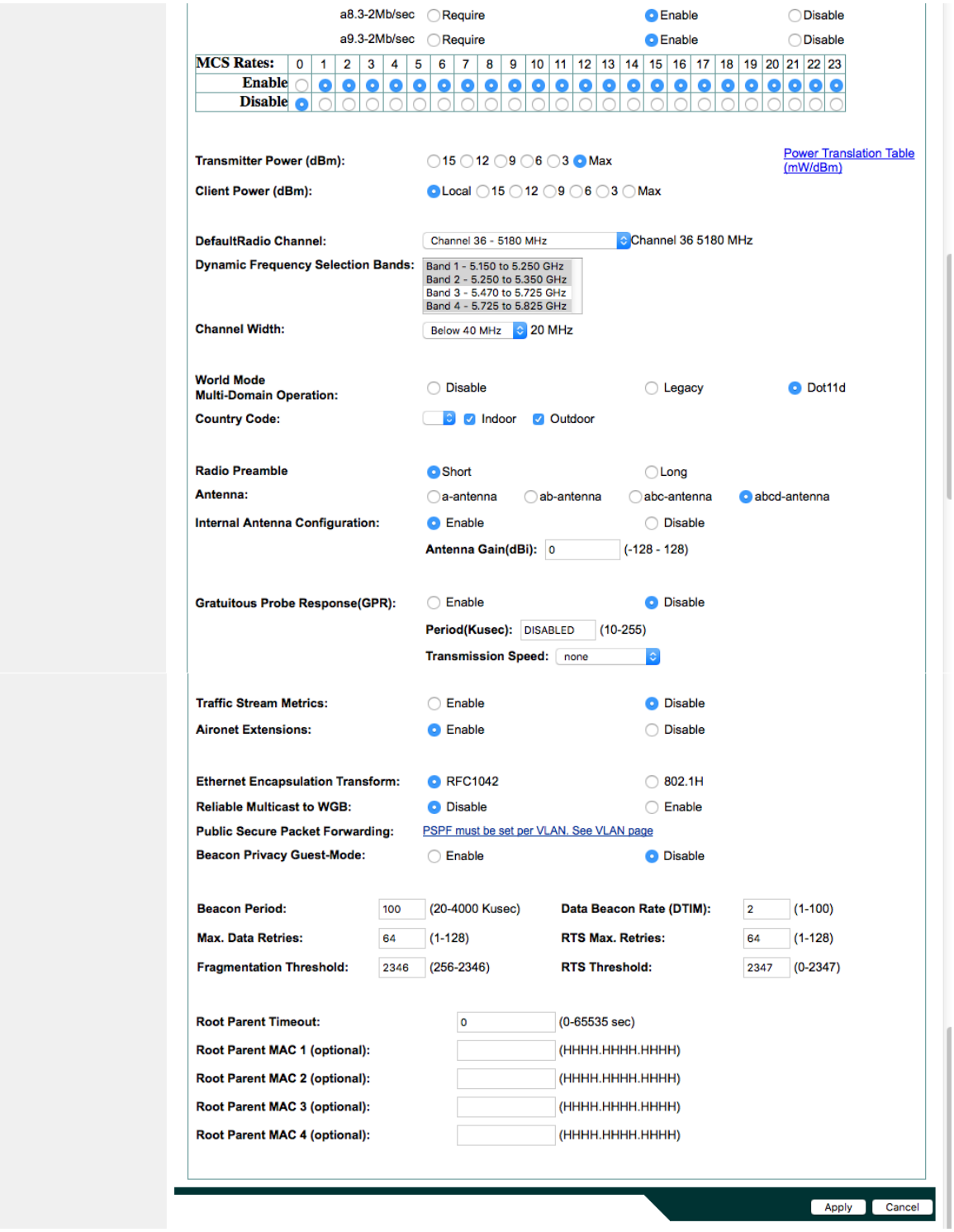
Ensure **Client Power** is configured properly. Do not use default setting of **Max** power for client power on Cisco Autonomous Access Points as that will not advertise DTPC to the client.

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

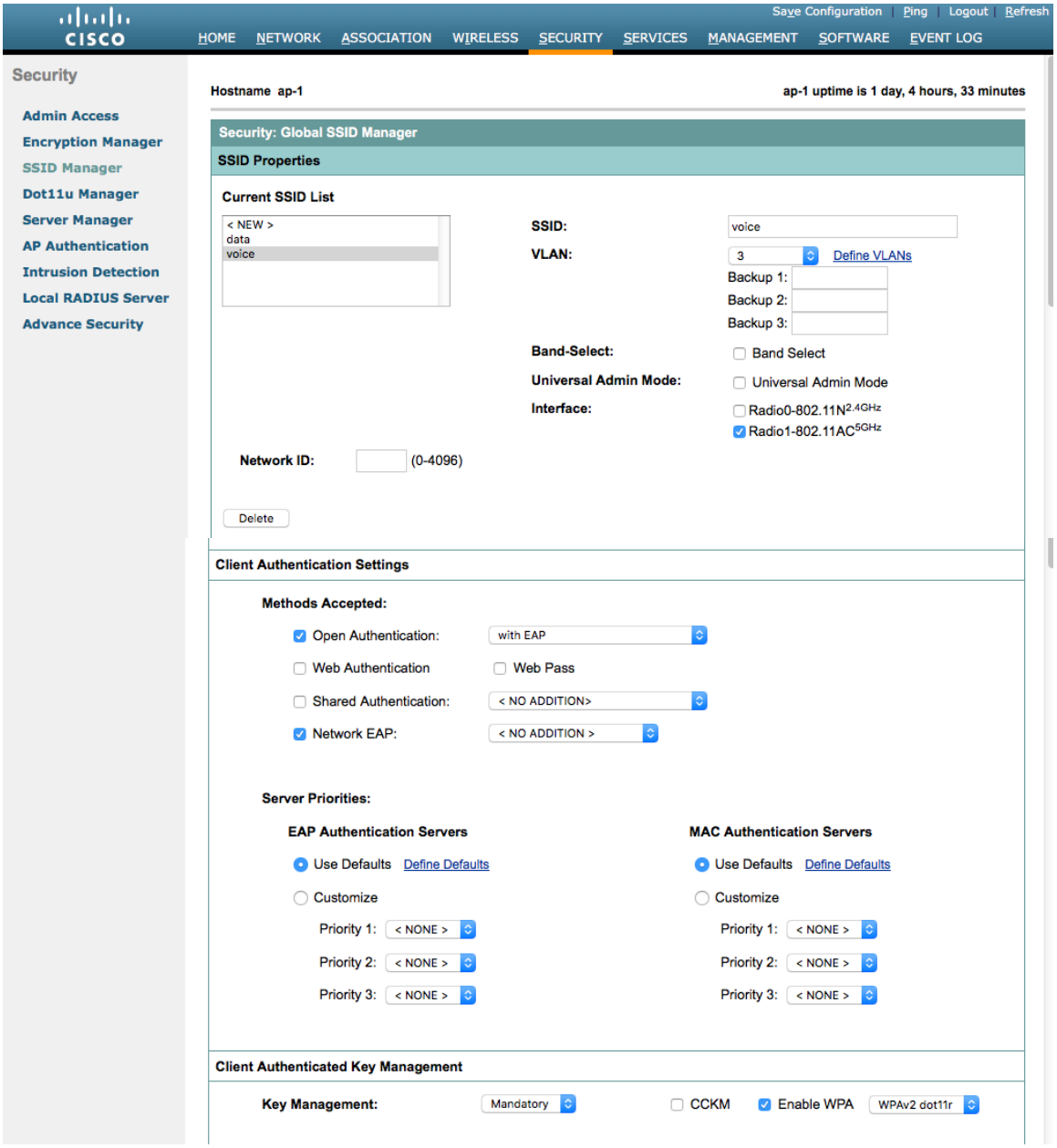
It is recommended to have a separate SSID for the Cisco Wireless IP Phone 8821 and 8821-EX.

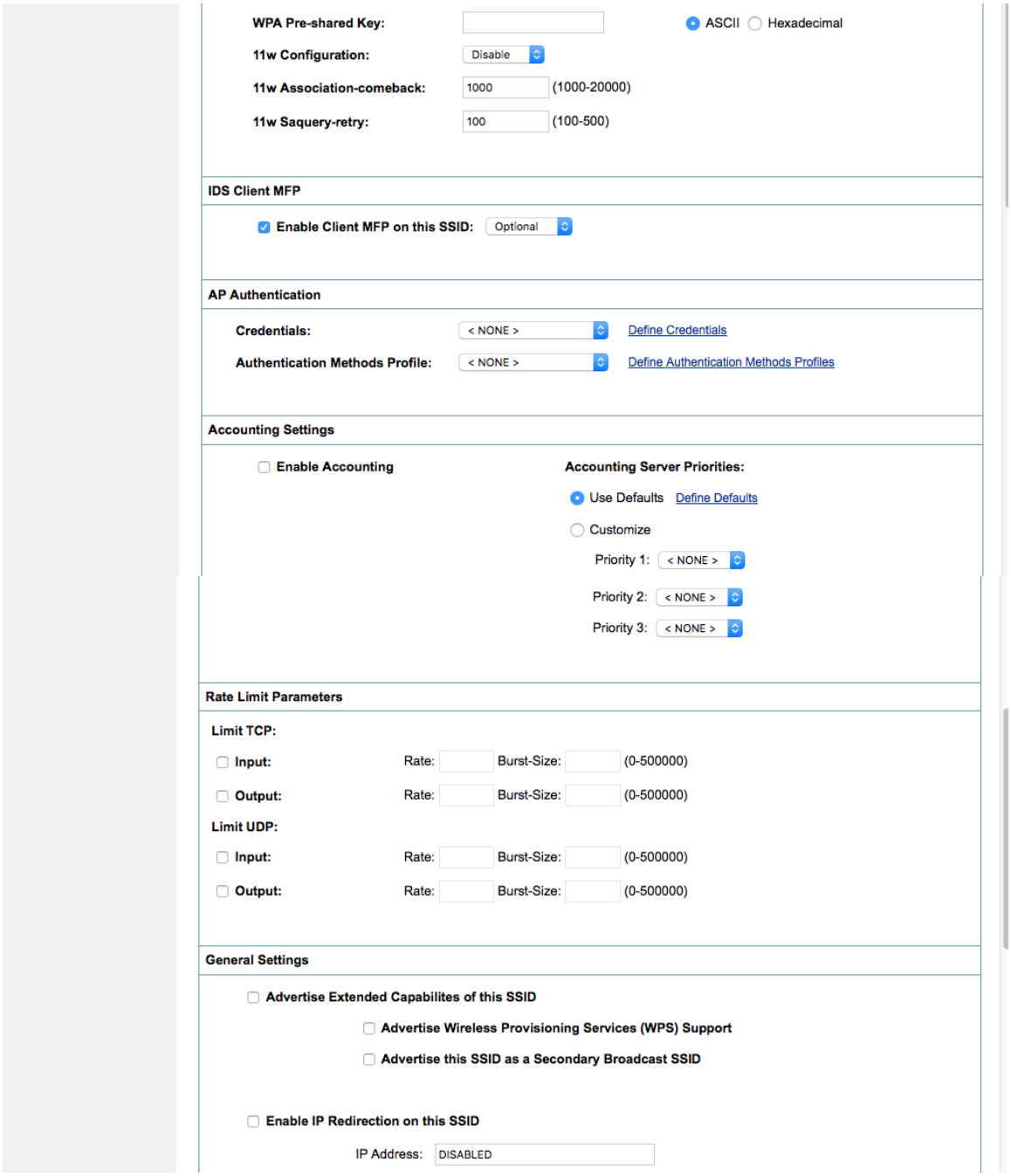
However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

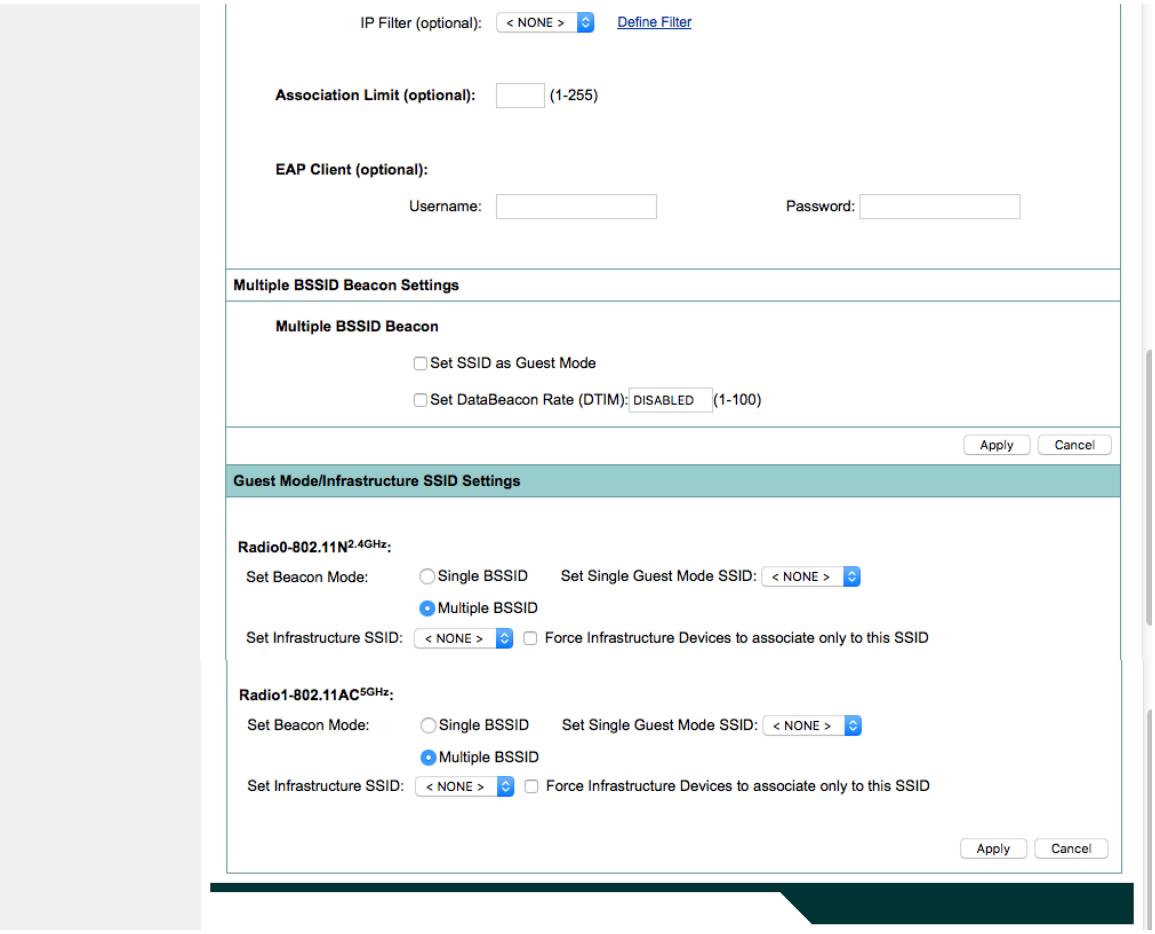
The SSID to be used by the Cisco Wireless IP Phone 8821 and 8821-EX can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

Enable **WPA2** key management.

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

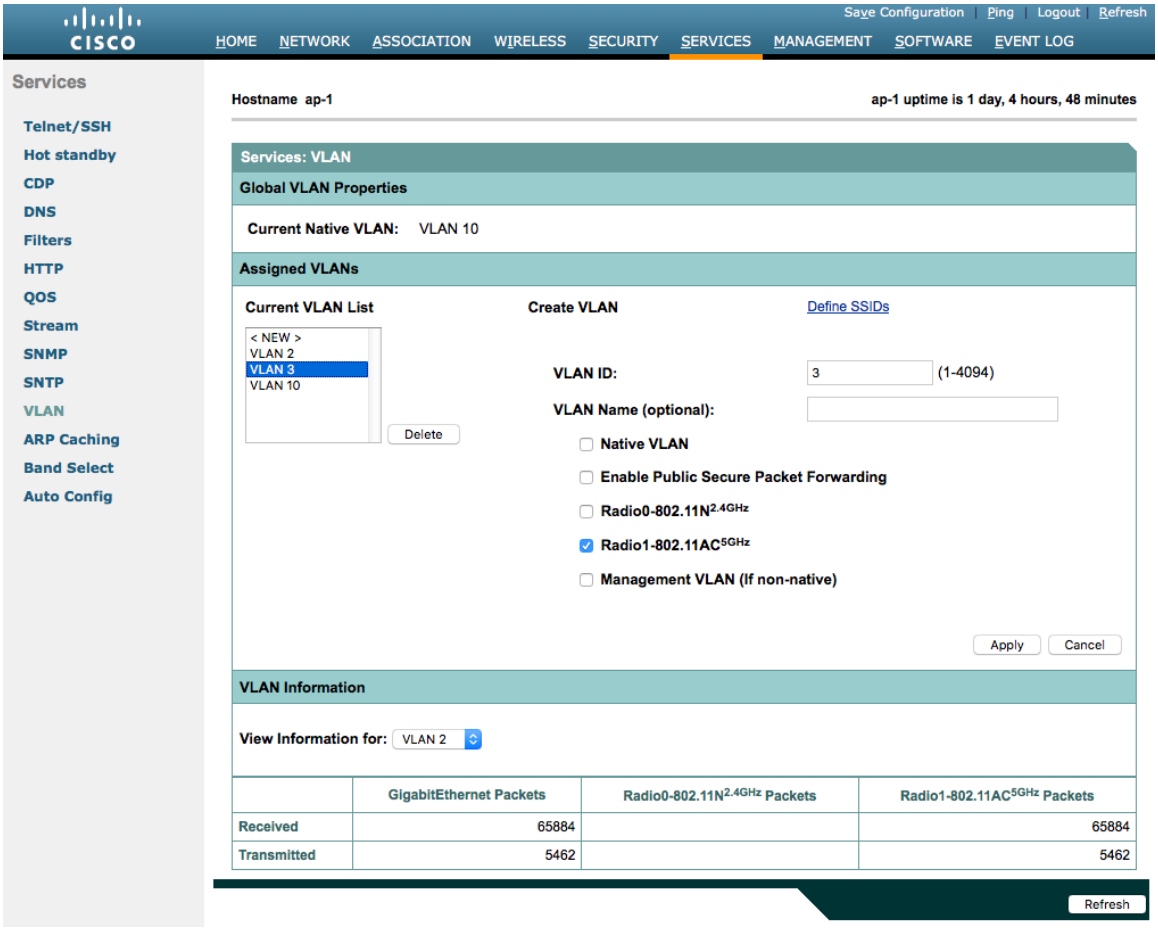



WPA Pre-shared Key:
ASCII
Hexadecimal
11w Configuration:
Disable
11w Association-comeback:
1000
(1000-20000)
11w Saquery-retry:
100
(100-500)
IDS Client MFP
Enable Client MFP on this SSID:
Optional
AP Authentication
Credentials:
< NONE >
Define Credentials
Authentication Methods Profile:
< NONE >
Define 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

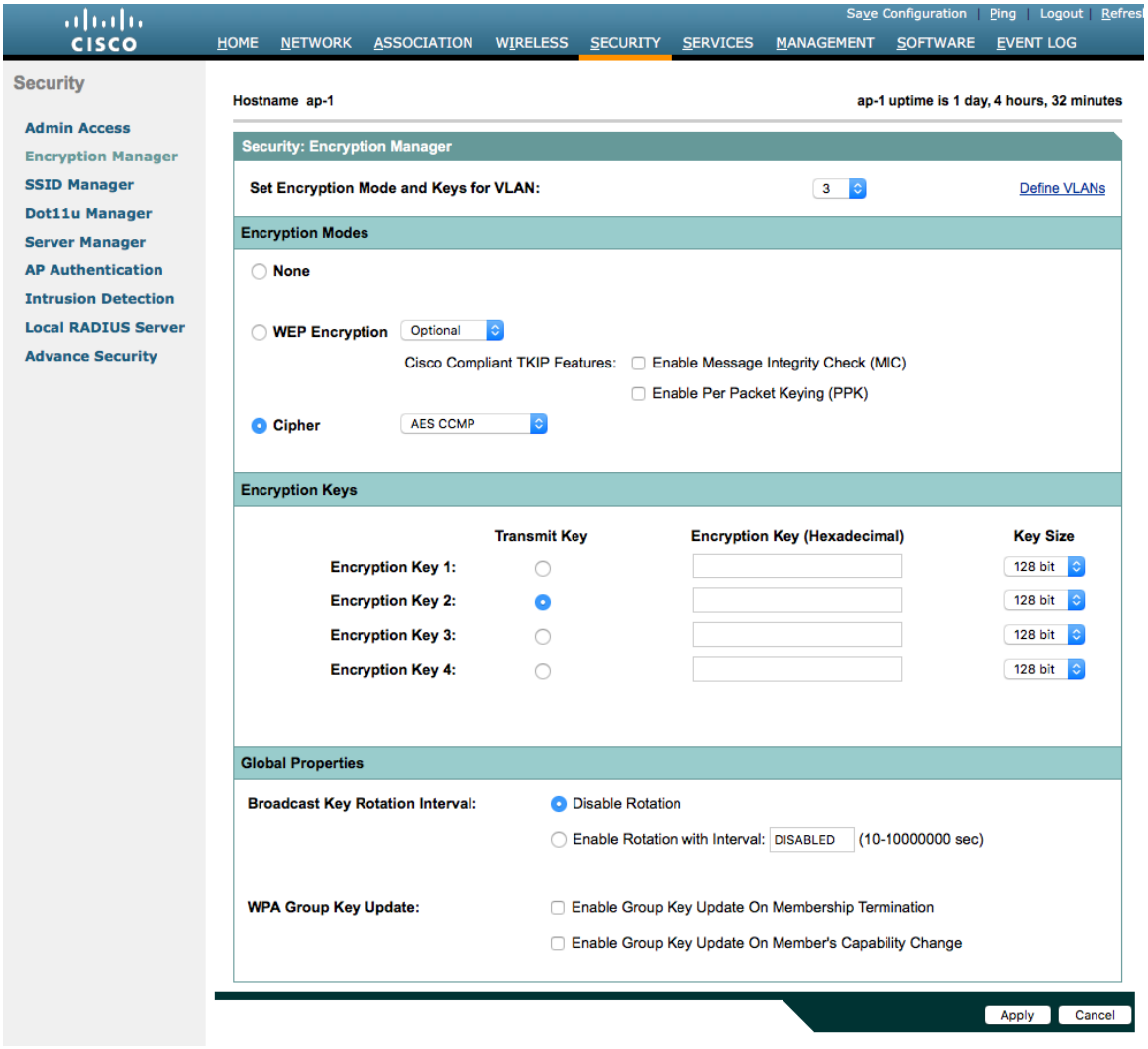


Segment wireless voice and data into separate VLANs.

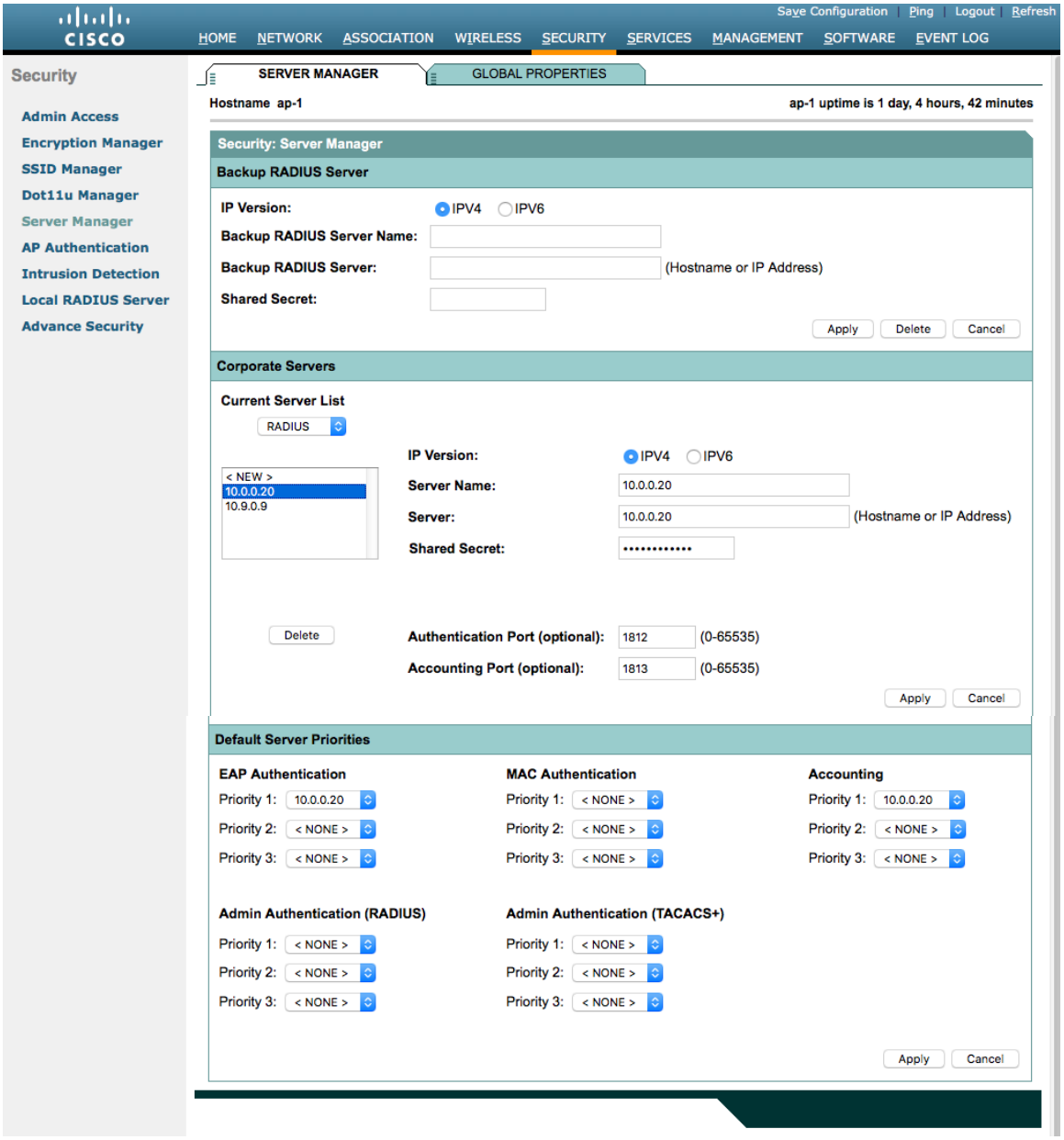
Ensure that Public Secure Packet Forwarding (PSPF) is not enabled for the voice VLAN as this will prevent clients from communicating directly when associated to the same access point. If PSPF is enabled, then the result will be no way audio.



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



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

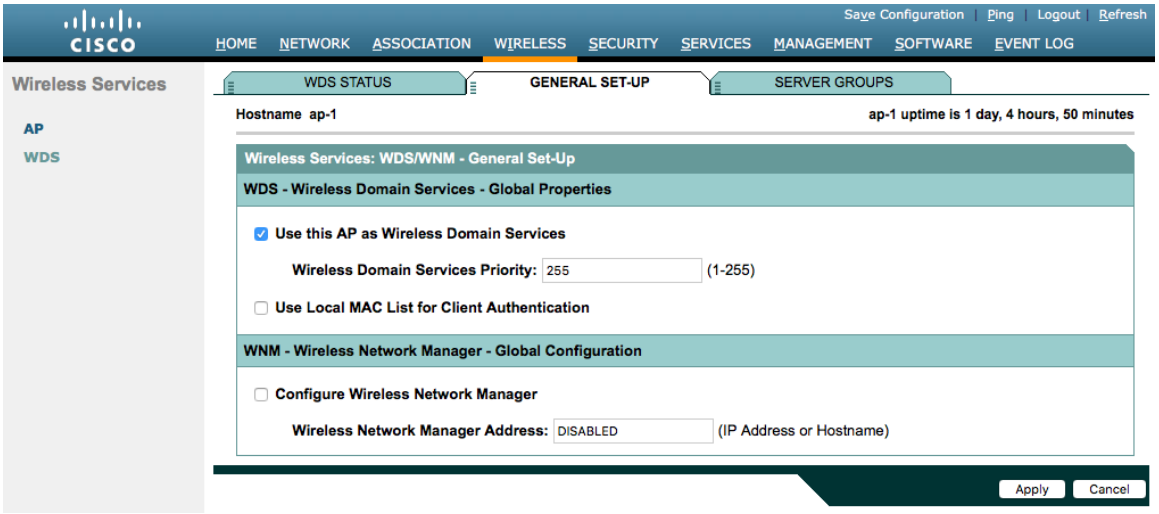


Wireless Domain Services (WDS)

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.

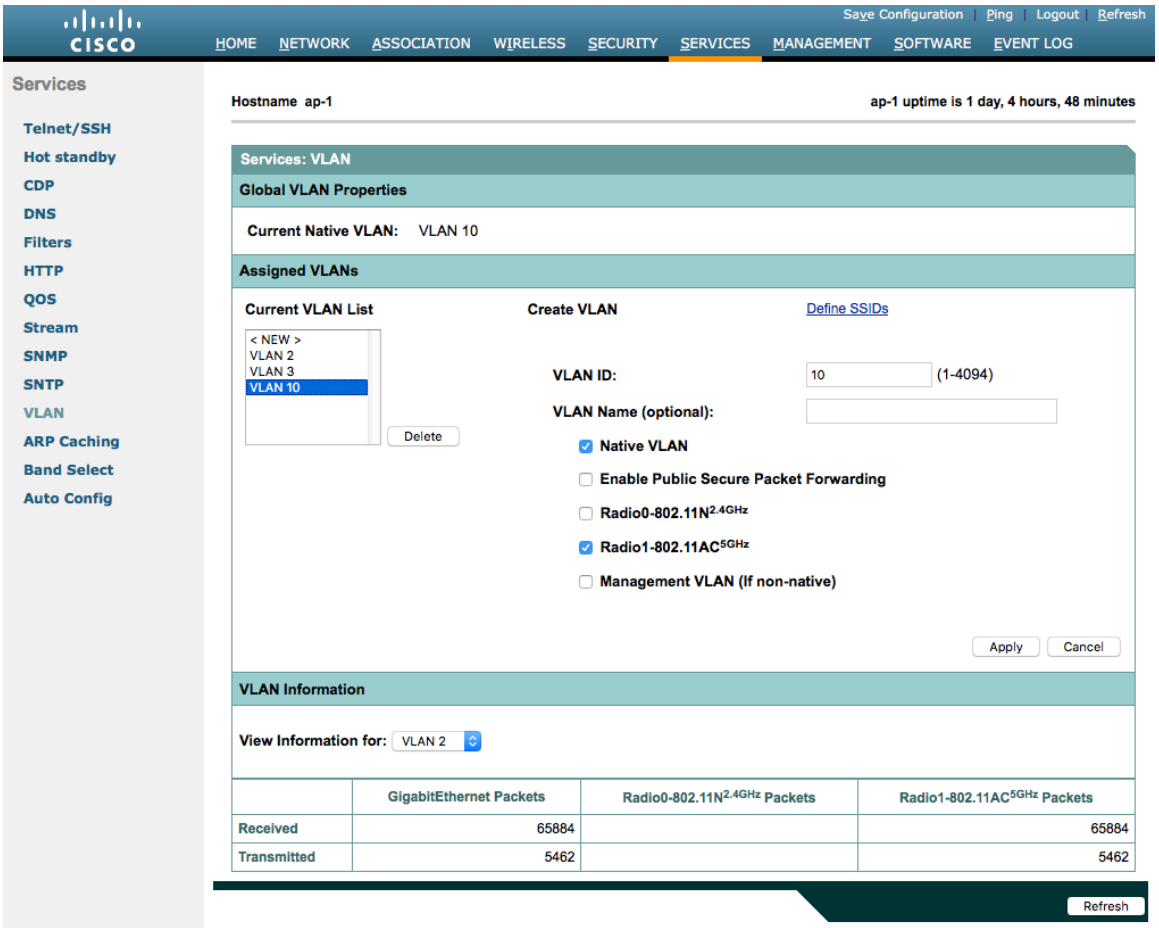
Configure the primary WDS server with the highest priority (e.g. 255) and the backup WDS server with a lower priority (e.g. 254).



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.

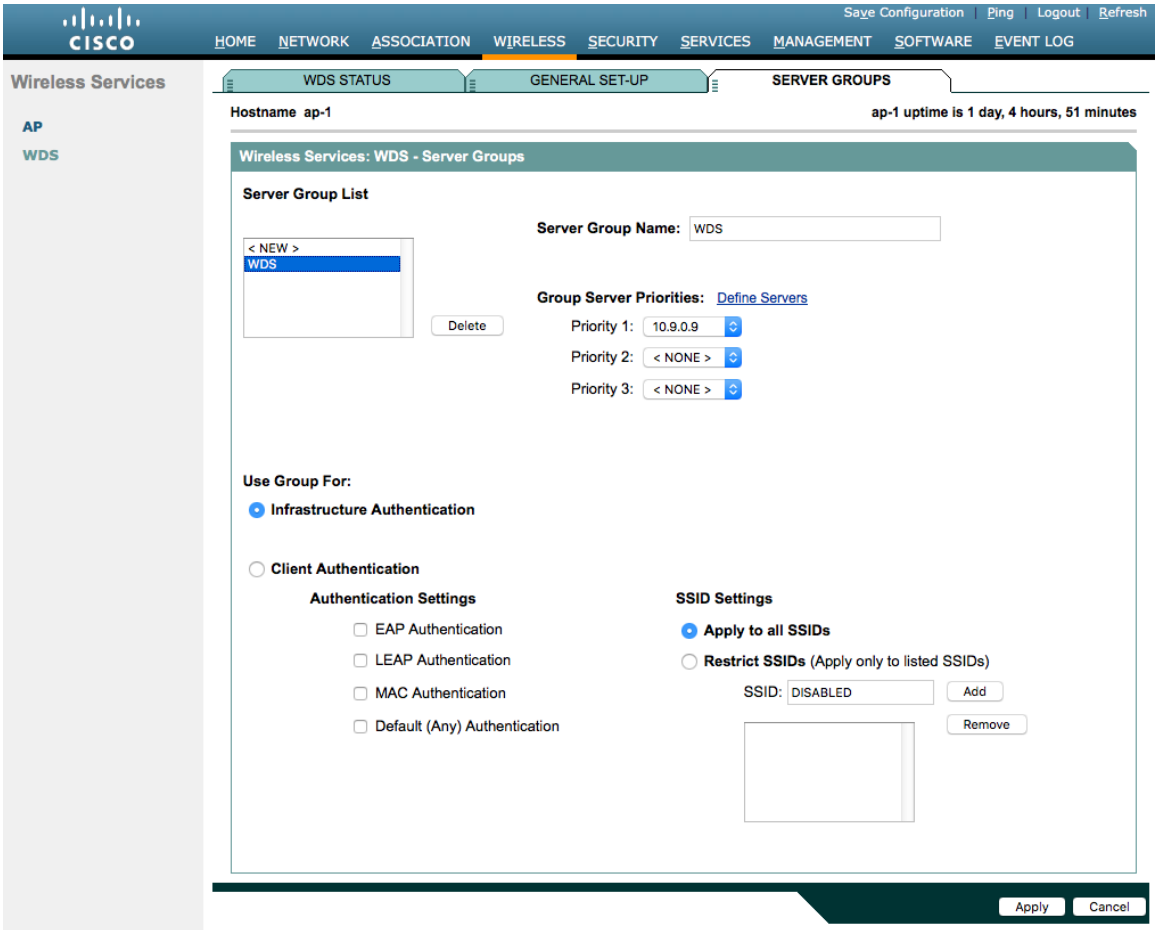


Server groups for Wireless Domain Services must be defined.

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

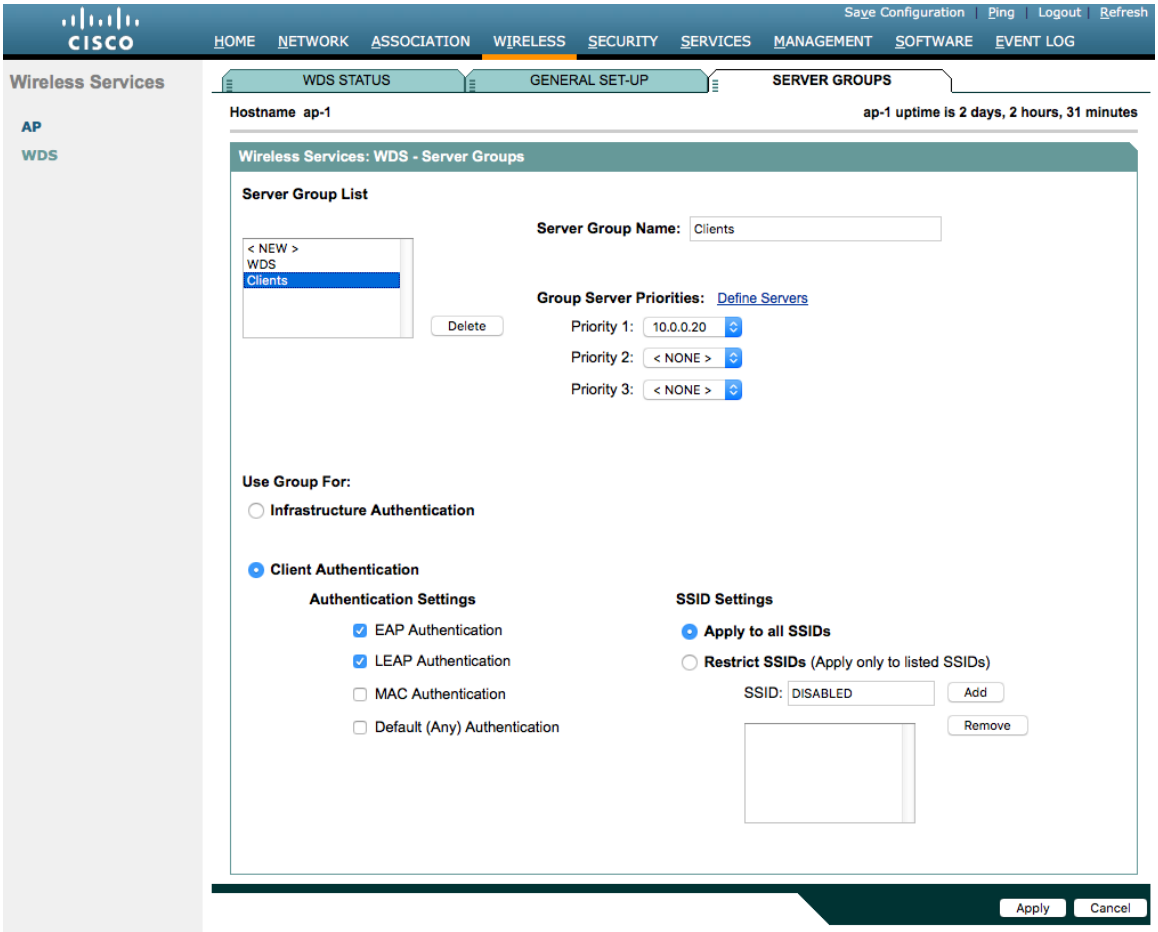
Is recommended to use local RADIUS for infrastructure authentication.

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.

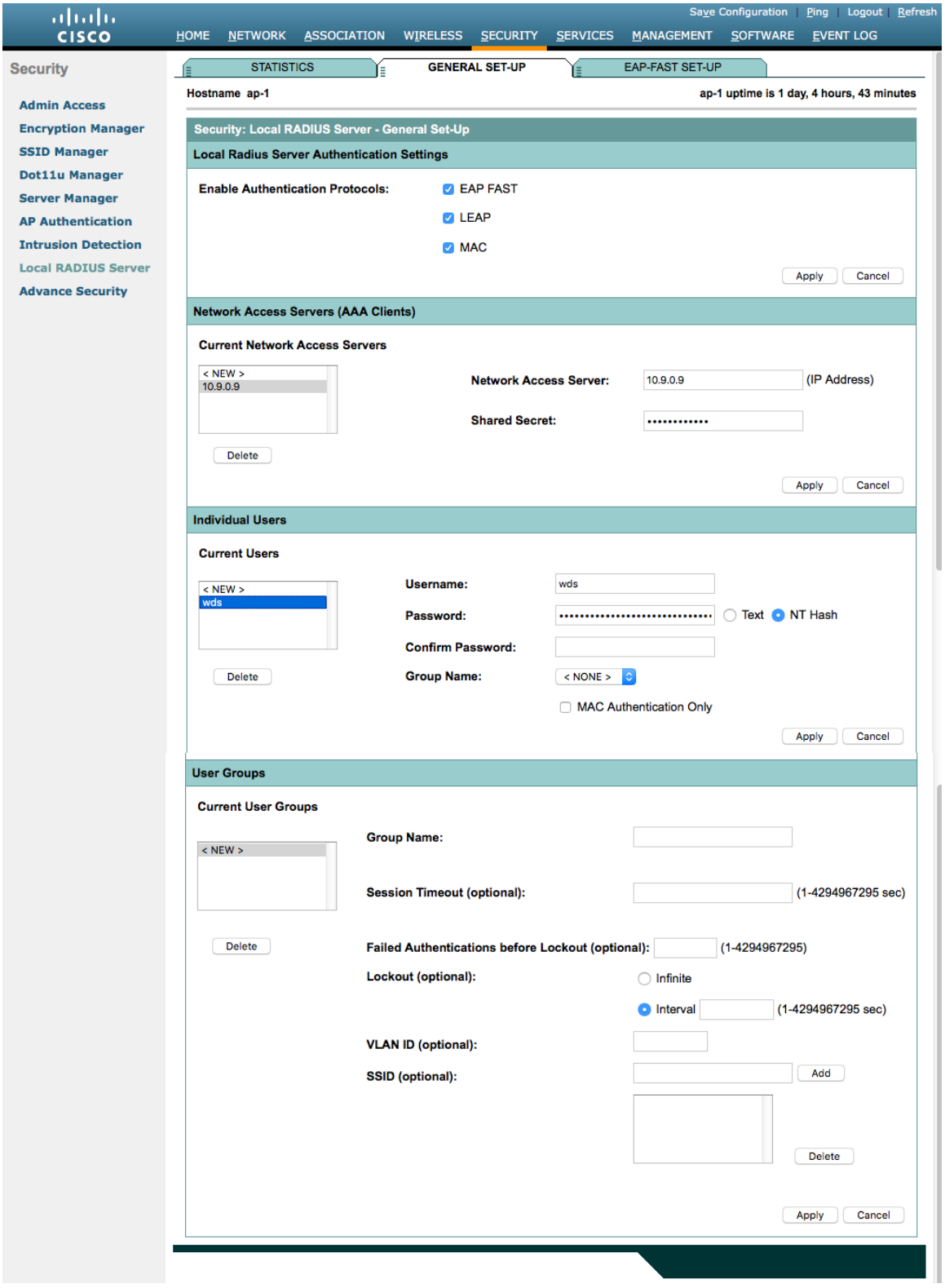


To utilize local RADIUS for infrastructure authentication, enable all authentication protocols.

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.

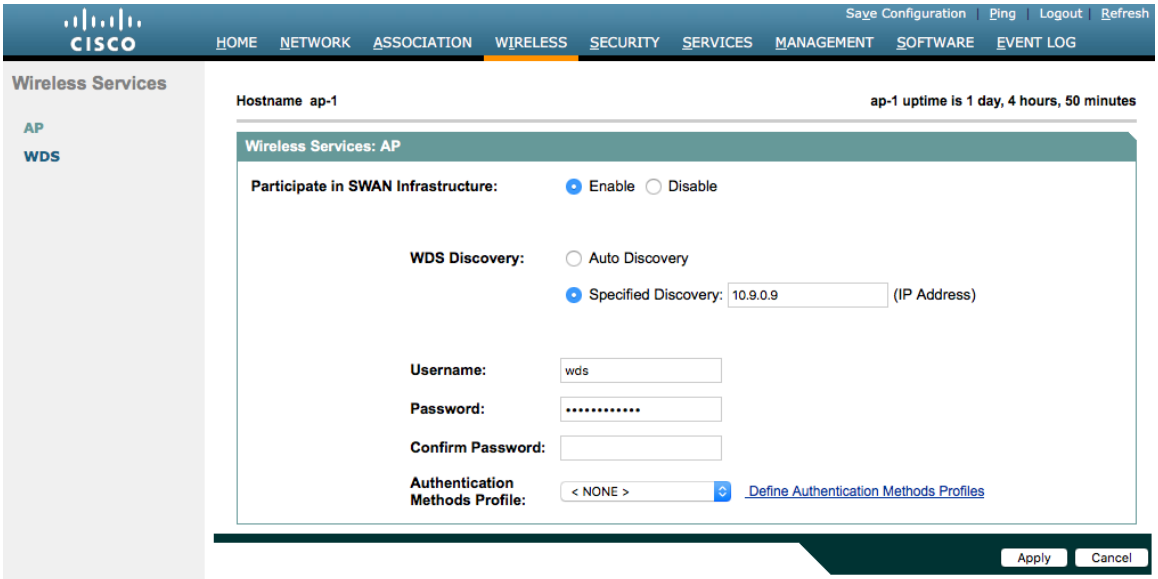


Once the desired access points have been configured successfully to enable Wireless Domain Services, then all access points including those serving as WDS servers need to be configured to be able to authenticate to the WDS servers.

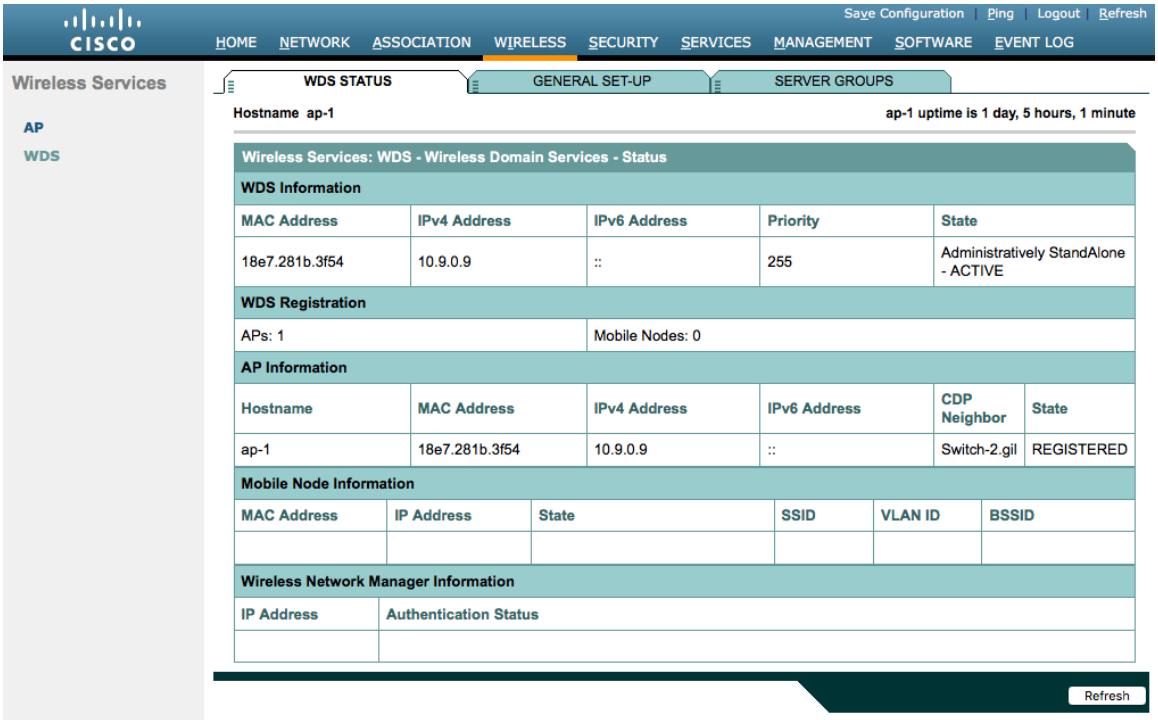
Enable **Participate in SWAN Infrastructure**.

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.



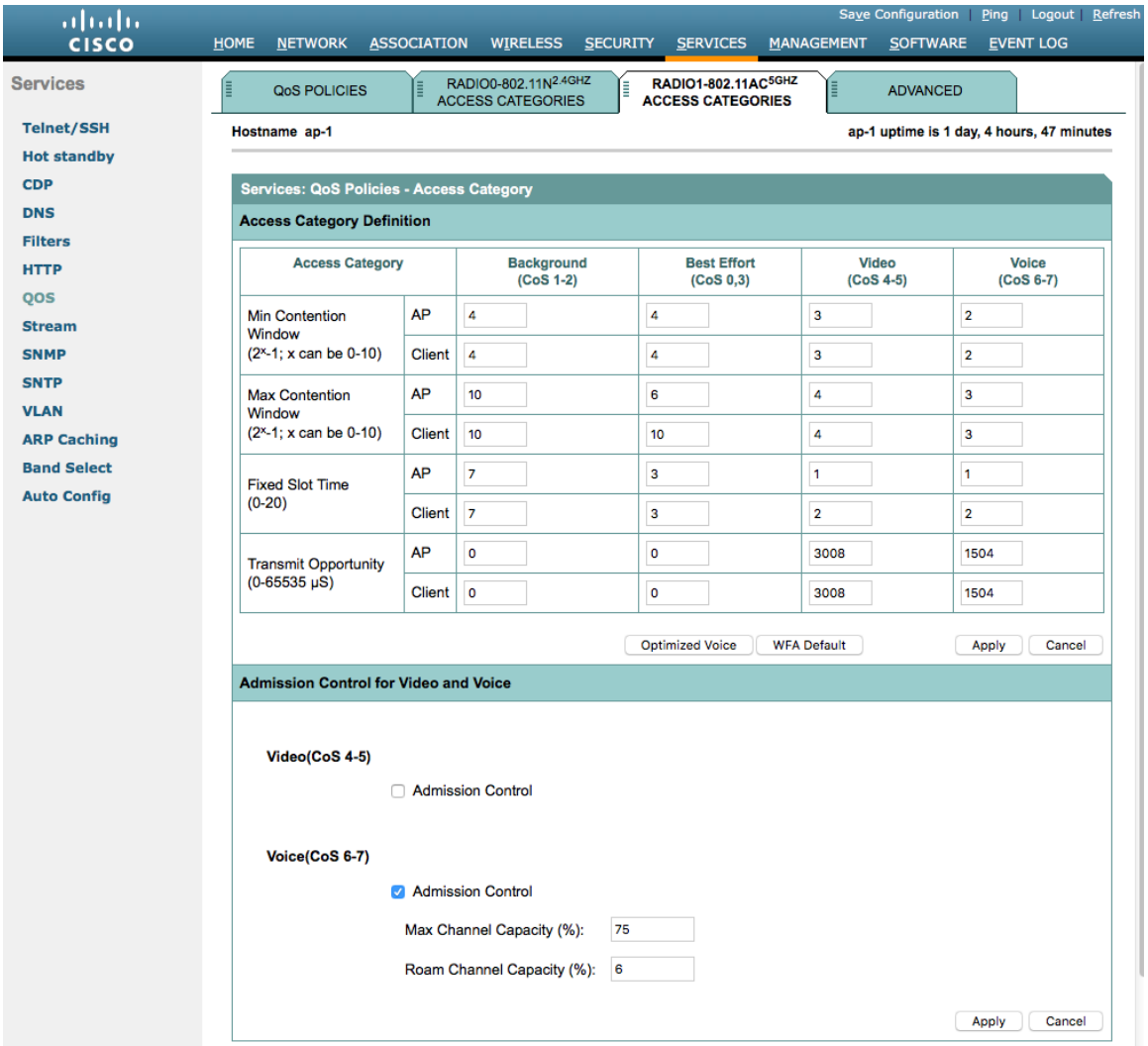
Call Admission Control (CAC)

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.

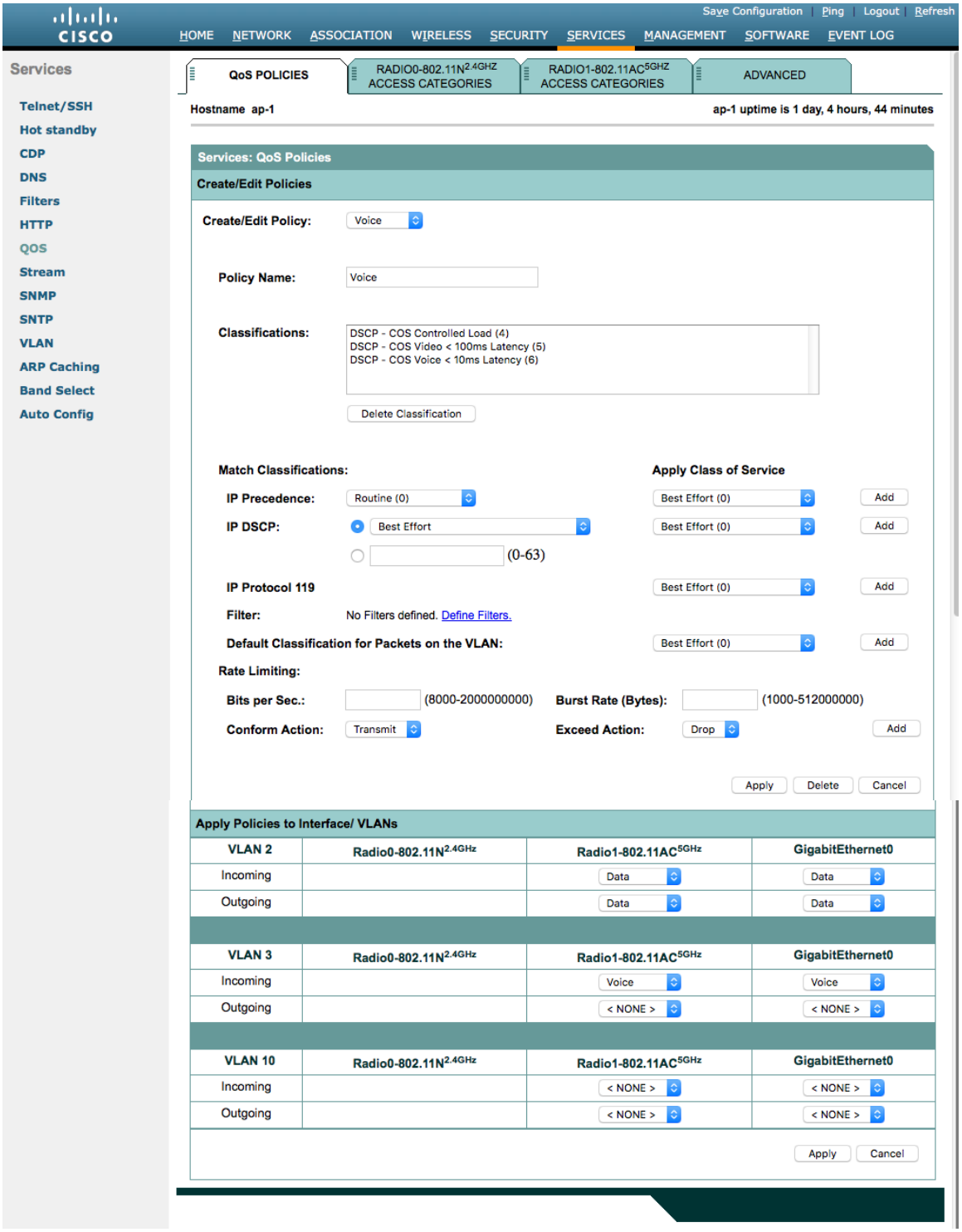
```
dot11 ssid voice
   vlan 3
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa version 2 dot11r
   admit-traffic
```



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.

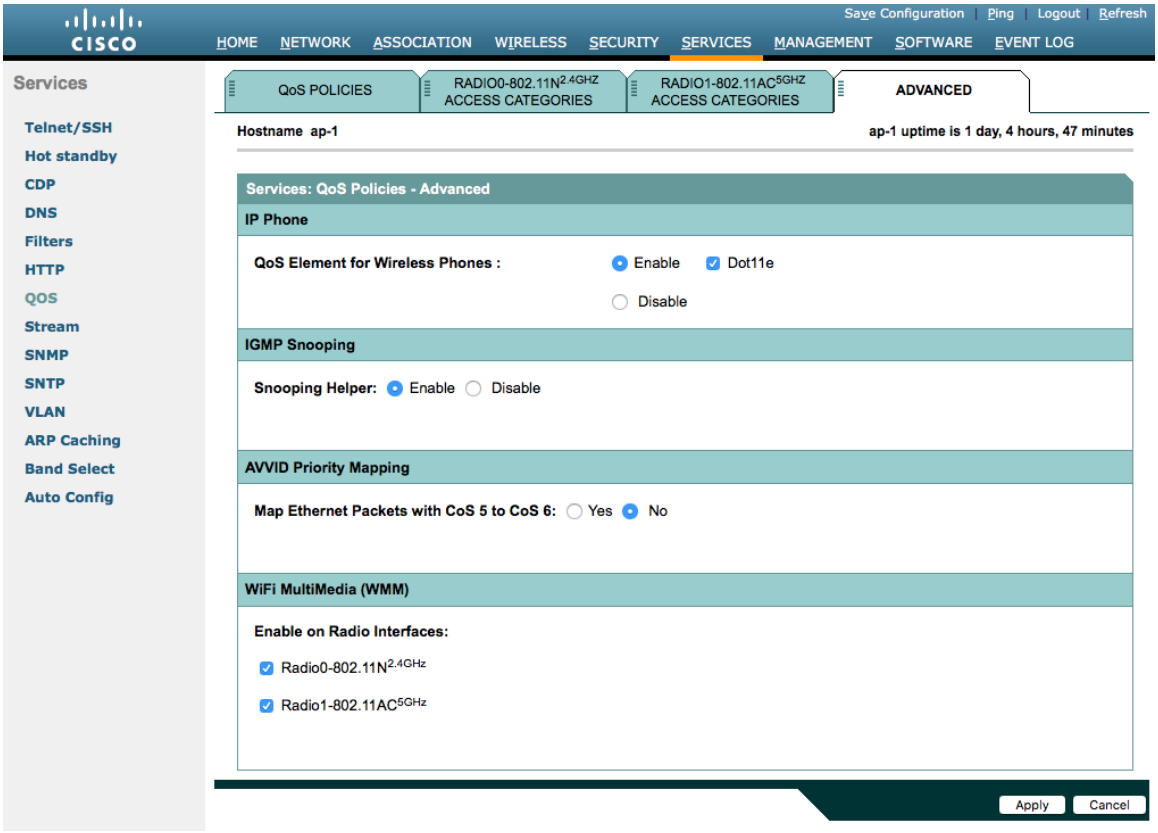


To enable QBSS, select **Enable** and check **Dot11e**.

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

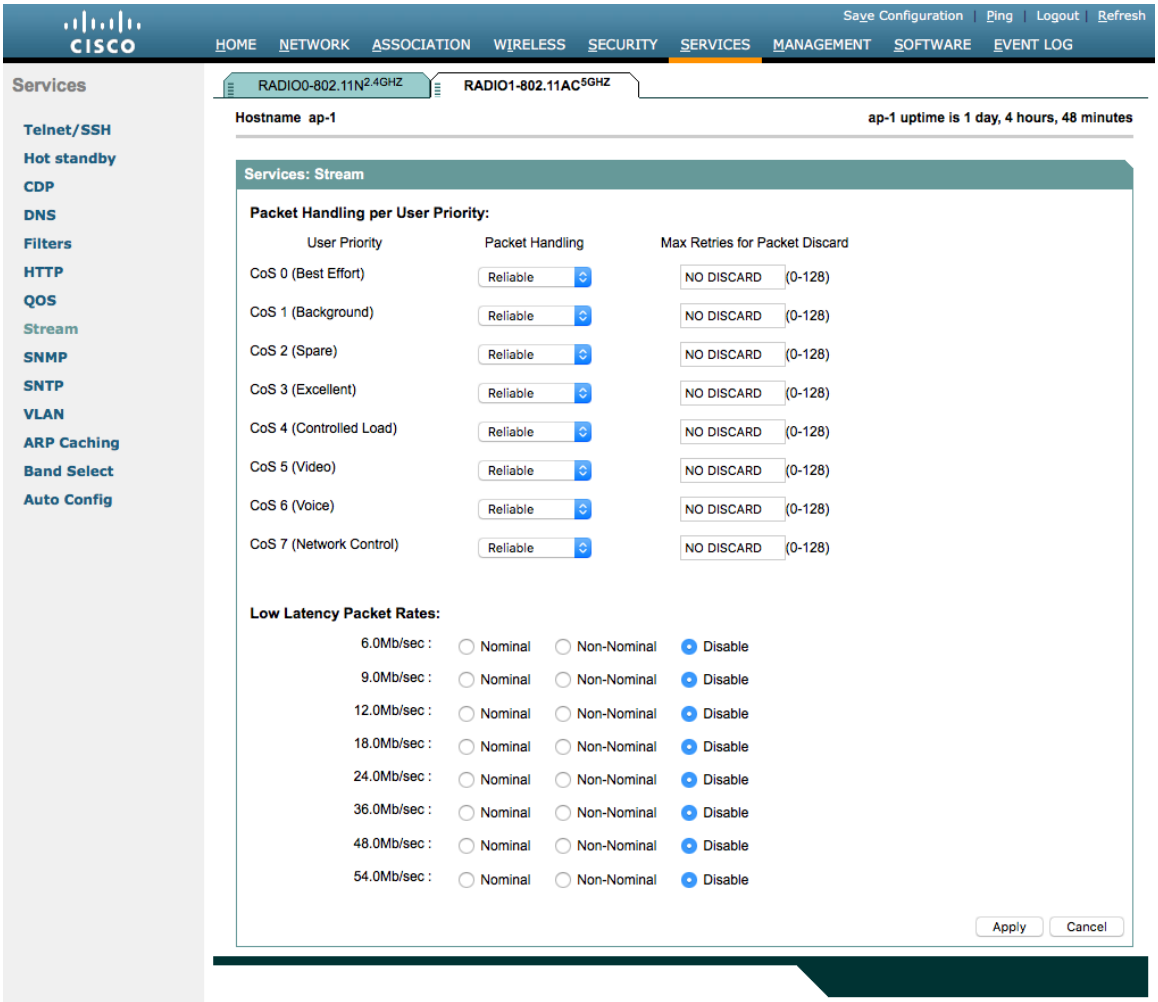
Ensure **IGMP Snooping** is enabled.

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.

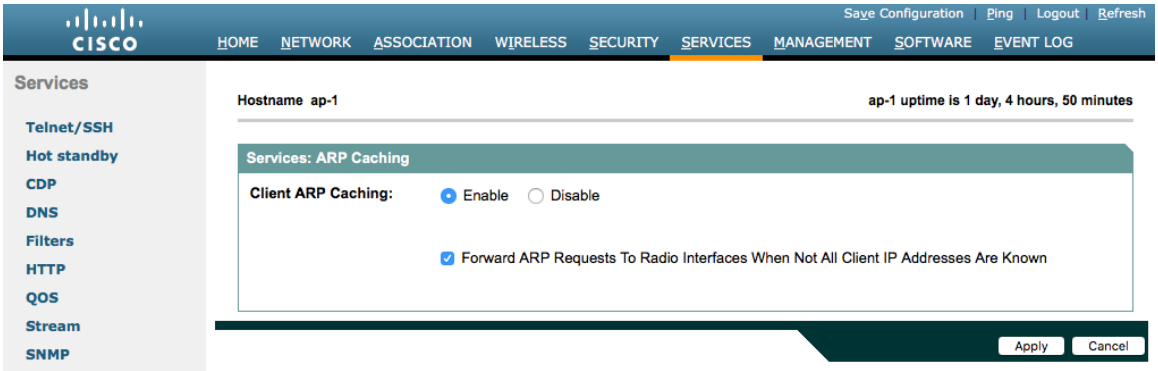


Power Management

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

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

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



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:

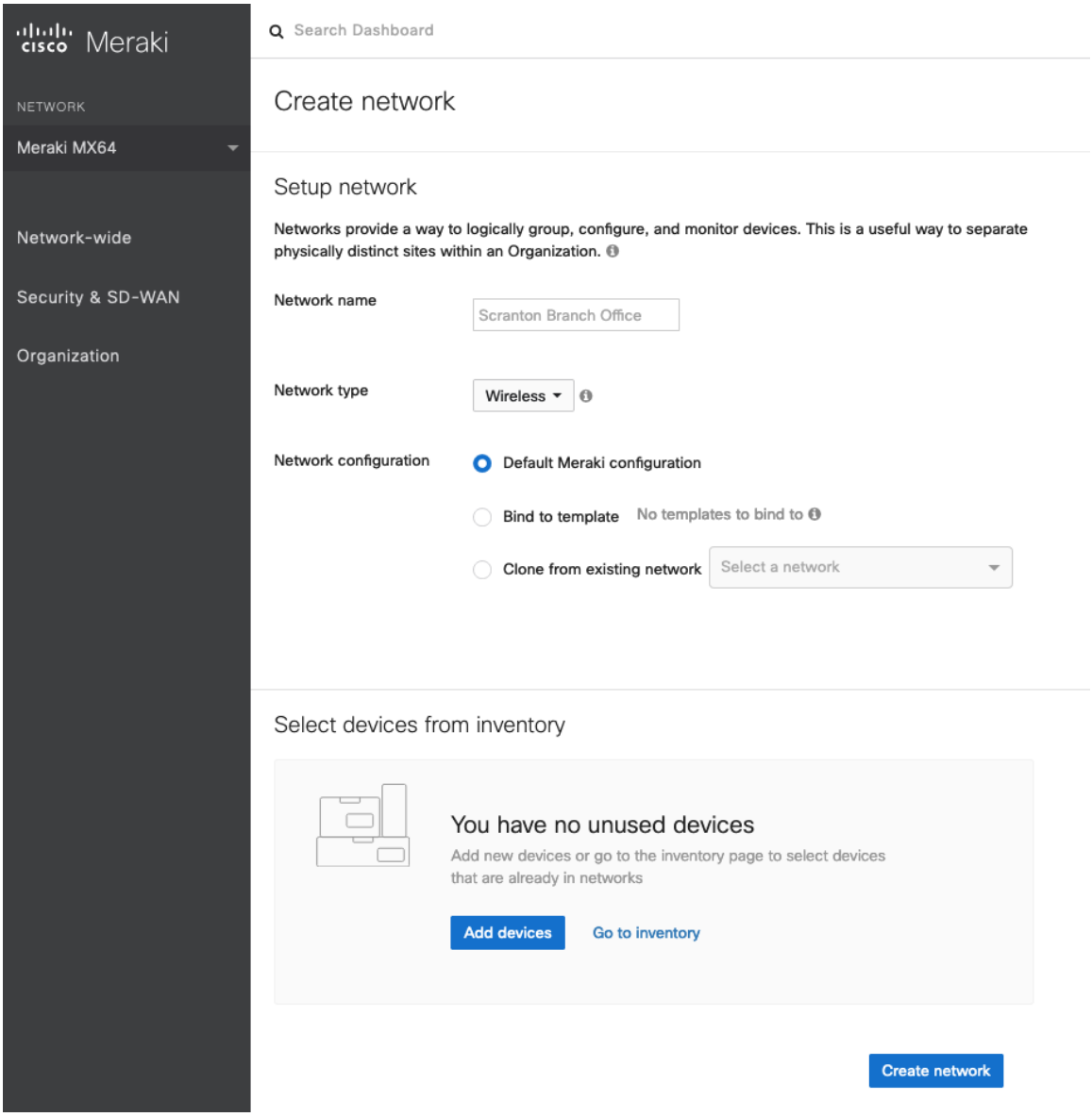
- Enable **802.11r** for **WPA2-Enterprise** or **Pre-shared key**
- Set **Splash page** to **None**
- Enable **Bridge mode**
- Enable **VLAN tagging**
- Set **Band selection** to **5 GHz band only**
- Configure the **Data Rates** as necessary
- Configure **Quality of Service (QoS)**

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**.

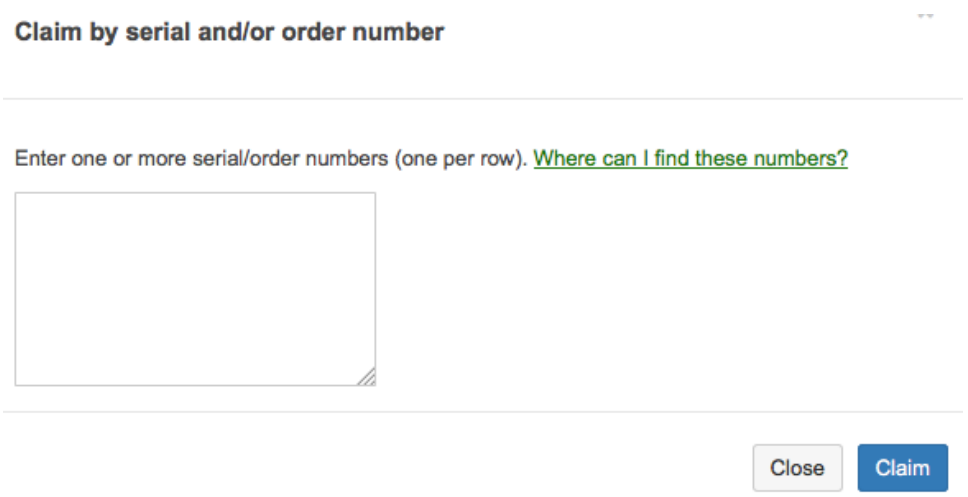


Cisco Meraki access points can be claimed either by specifying the serial number or order number.

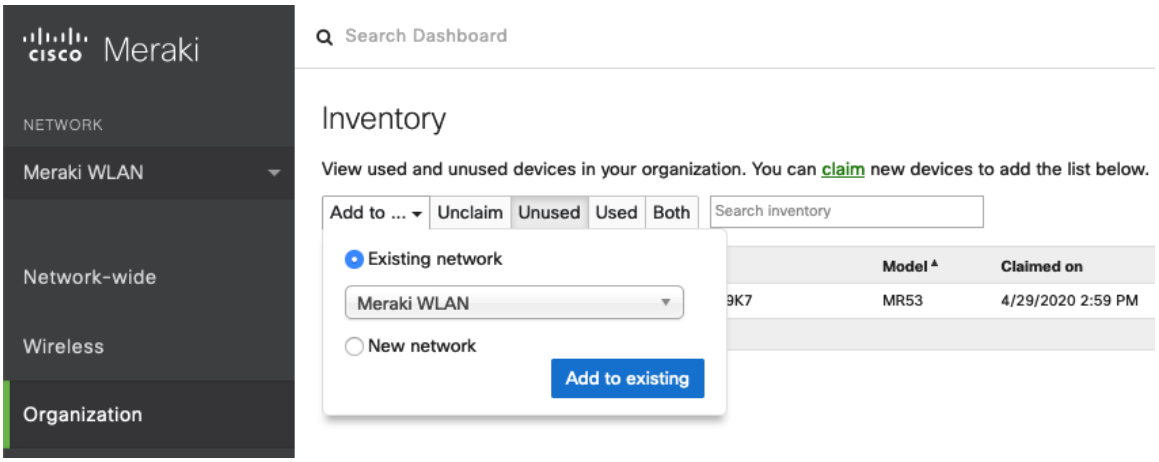
Once claimed, those Cisco Meraki access points will then be listed in the available inventory.

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

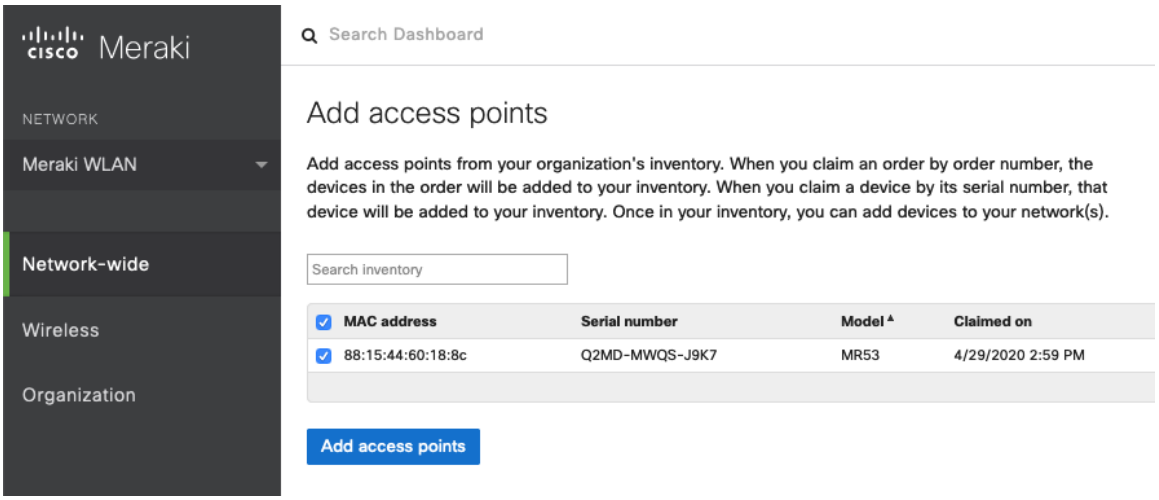
Access points can also be claimed by selecting **Add APs** on the **Wireless > Monitor > Access points** page, then selecting **Claim**.



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

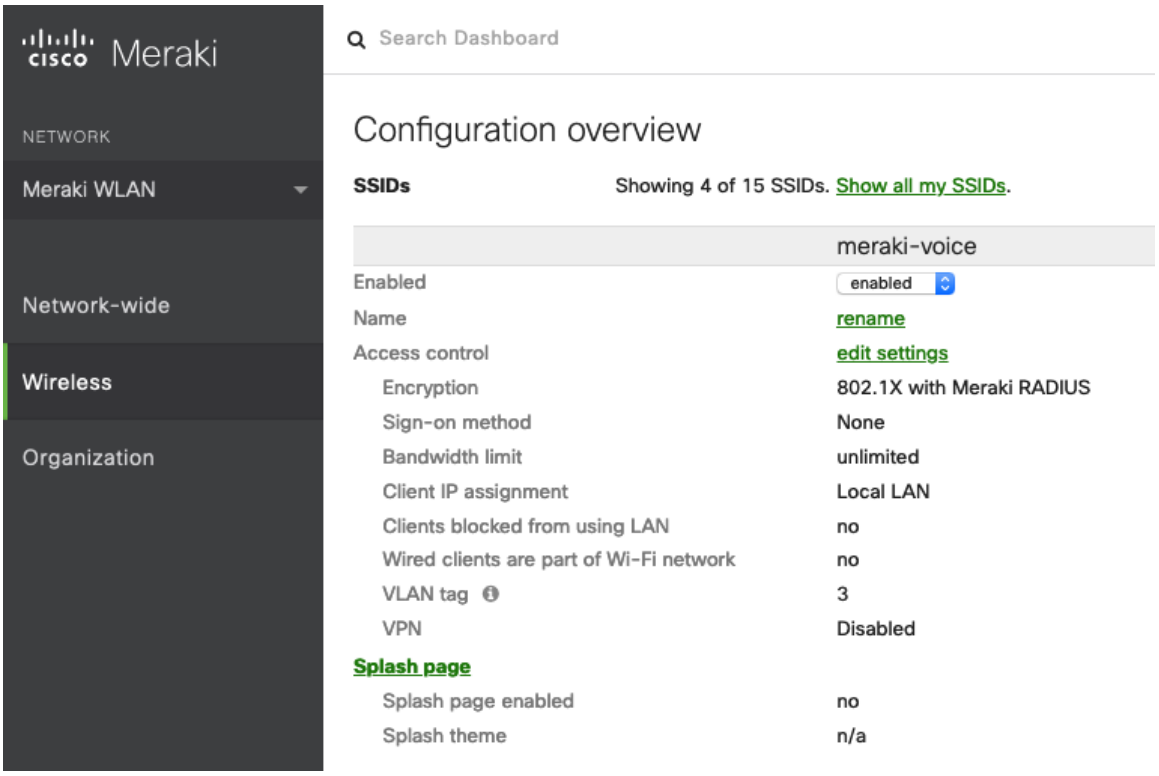
To create a SSID, select the desired network from the drop-down menu then select **Wireless > Configure > SSIDs**.

It is recommended to have a separate SSID for the Cisco Wireless IP Phone 8821 and 8821-EX; 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.

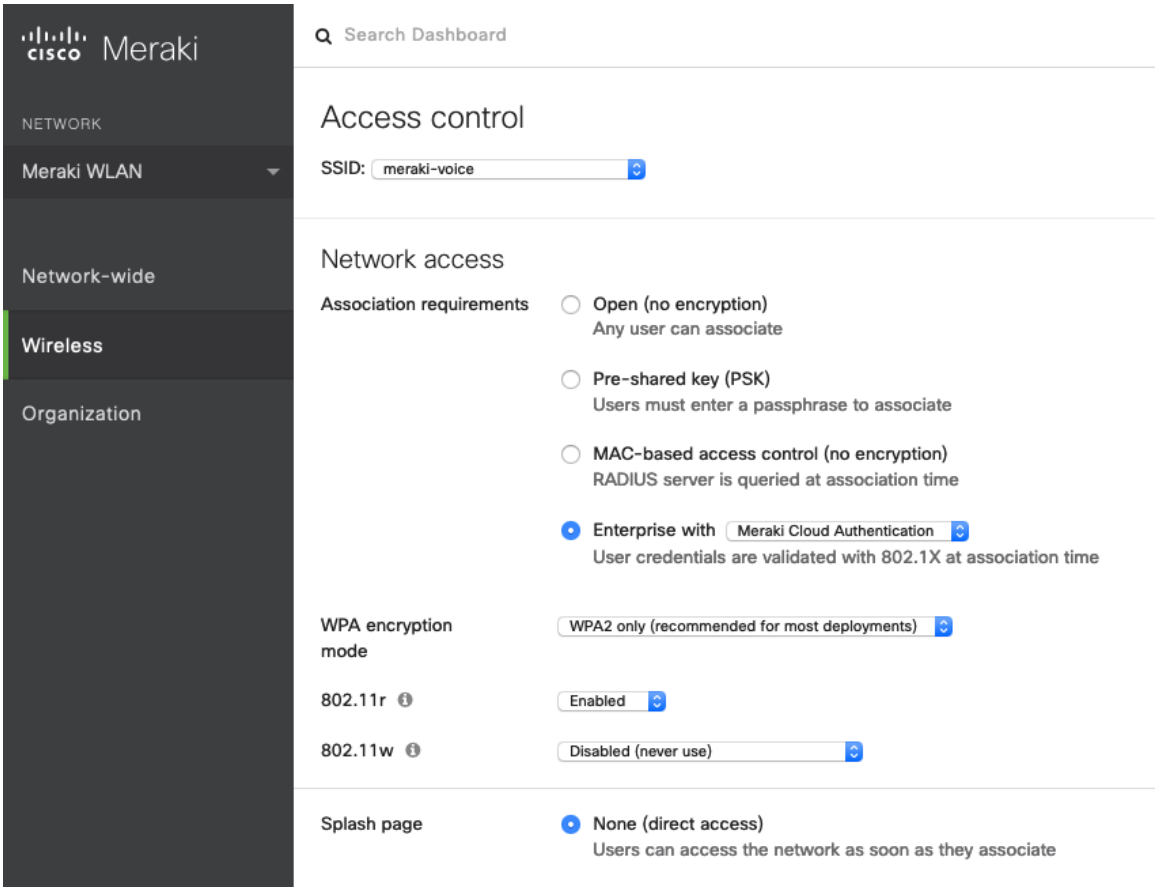
The Cisco Meraki authentication server or an external RADIUS server can be utilized when selecting **WPA2-Enterprise**.

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.

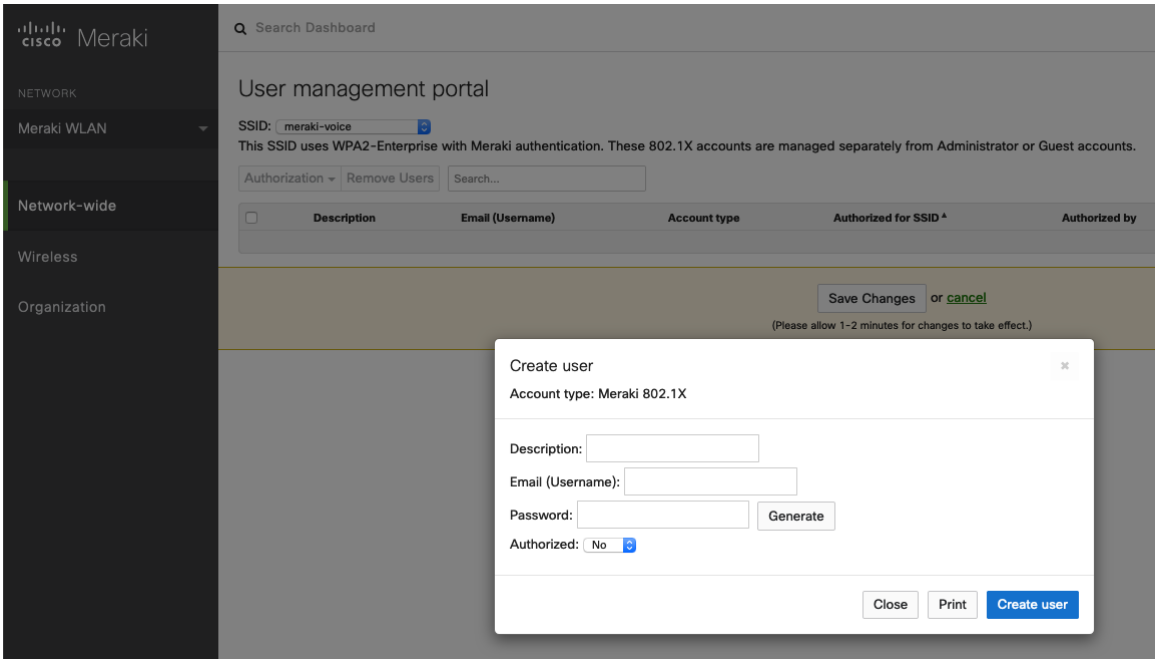
Ensure Splash page is set to **None** to enable direct access.



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 IP Phone 8821 and 8821-EX will be configured to use for 802.1x authentication.

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



On the **Wireless > Configure > Access control** page, recommend to enable **Bridge mode**, where the Cisco Wireless IP Phone 8821 and 8821-EX 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.

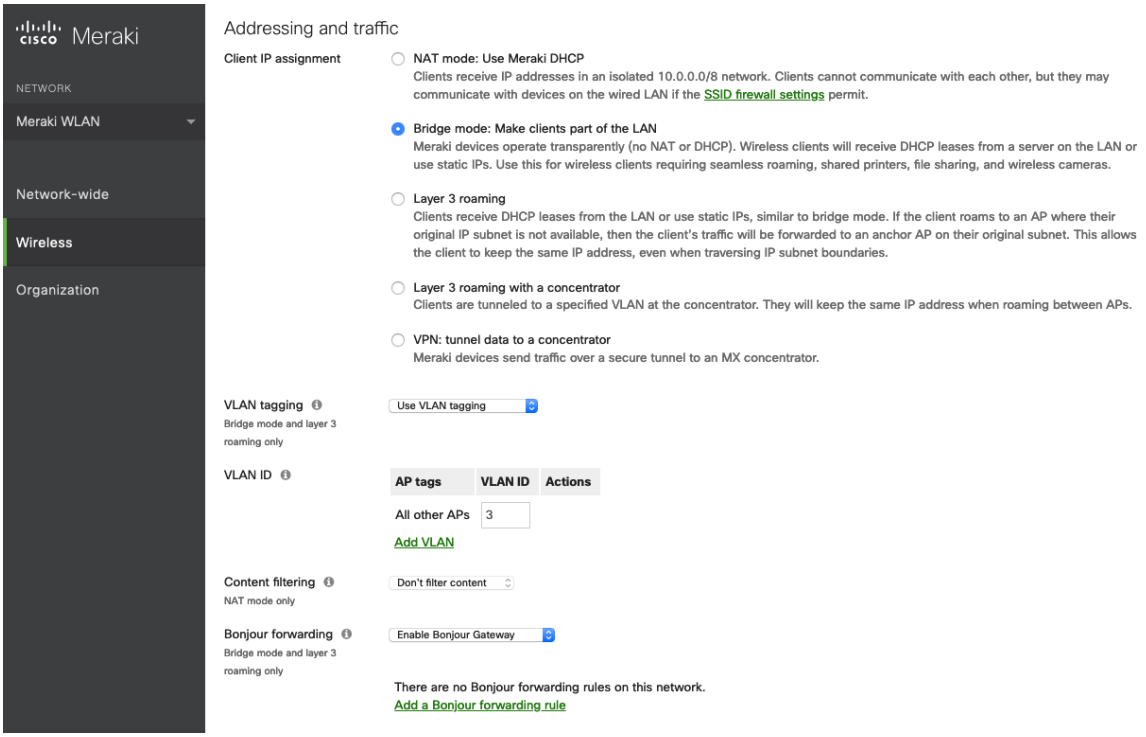
If VLAN tagging is utilized, ensure that the Cisco Meraki access point is connected to a switch port configured for trunk mode allowing that VLAN.

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
```



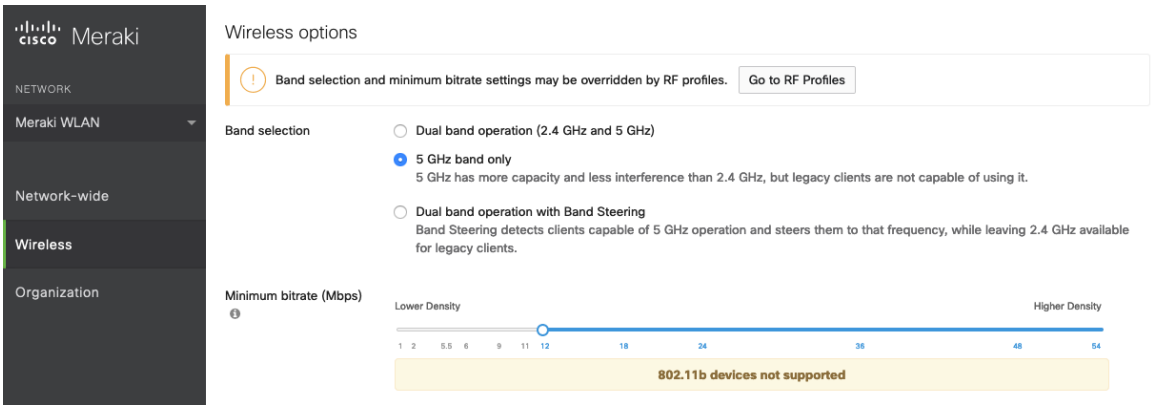
On the **Wireless > Configure > Access control** page, the frequency band for the SSID to be used by the Cisco Wireless IP Phone 8821 and 8821-EX can be configured as necessary.

It is recommended to select **5 GHz band only** to have the Cisco Wireless IP Phone 8821 and 8821-EX 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.

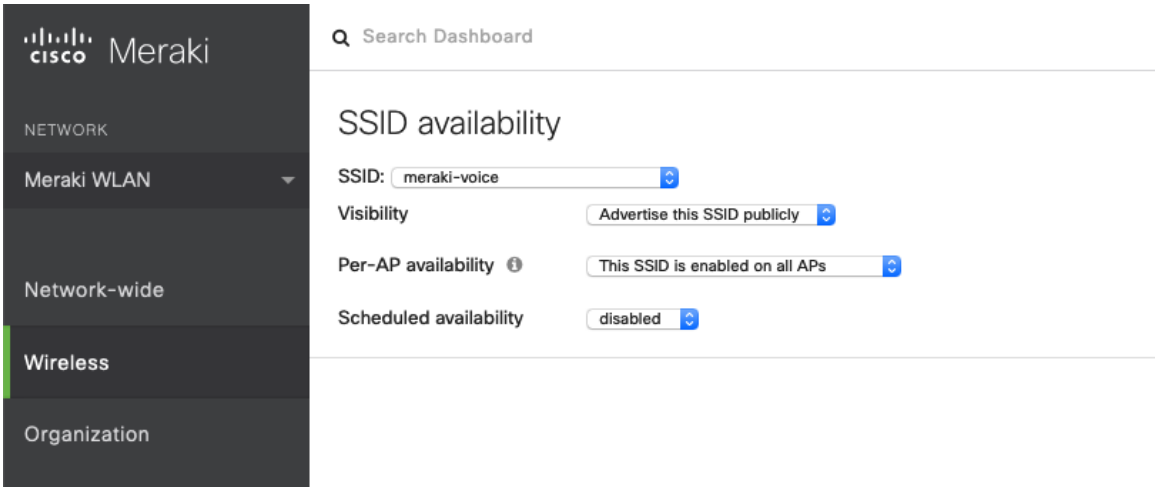
Cisco Meraki access points currently utilize a DTIM period of **1** with a beacon period of **100 ms**; which both are non-configurable.



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**.

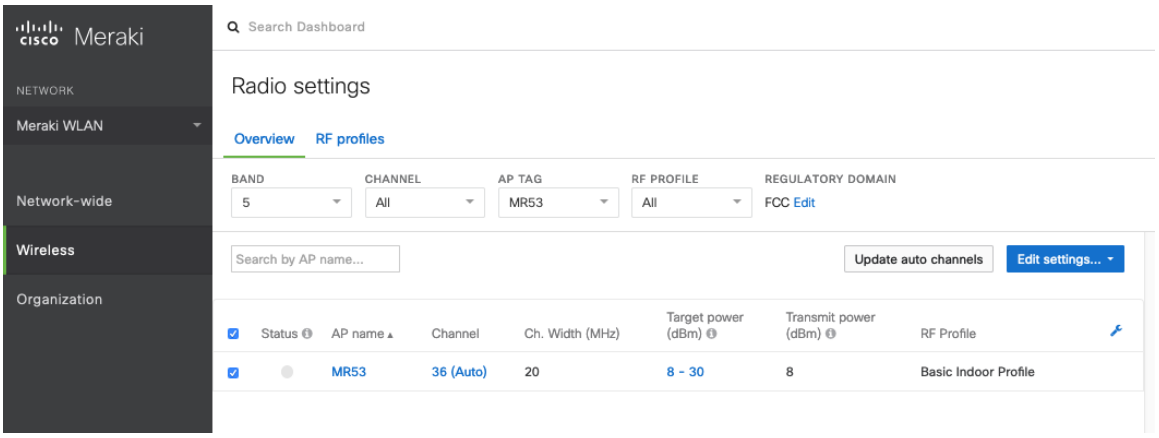


Radio Settings

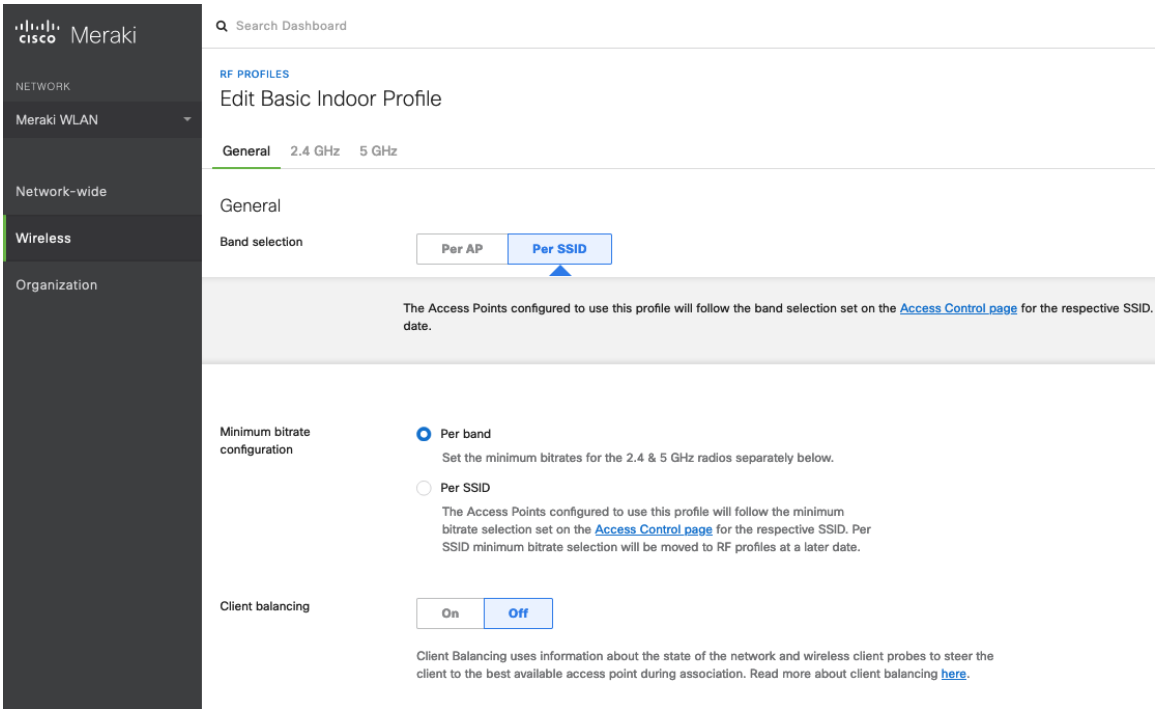
On the **Wireless > Configure > Radio settings** page, access points can be configured in bulk or by individual access point to define the automatic or manual channel and transmit power settings.

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.

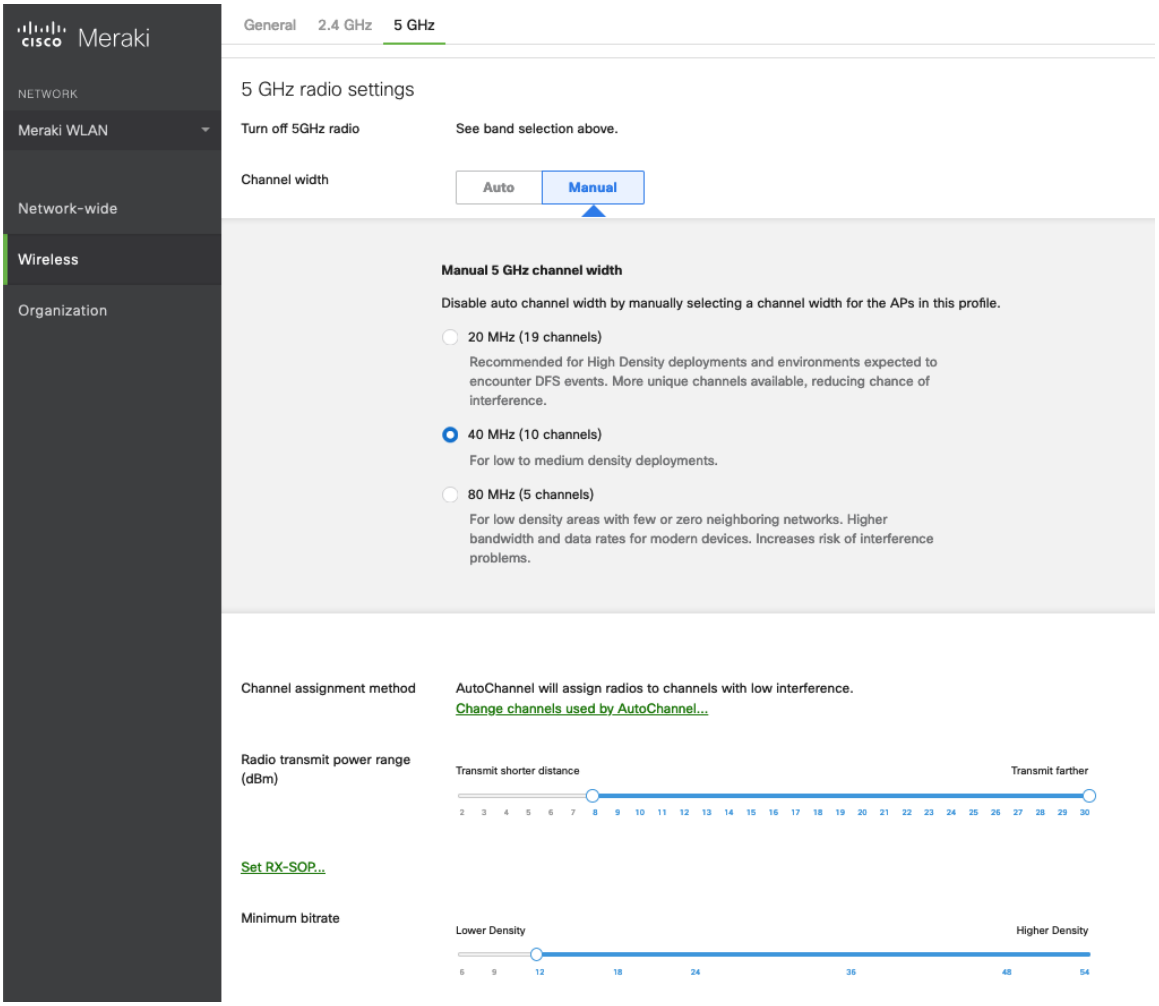
5 GHz channels to be used by **AutoChannel** can also be configured in the RF Profile.

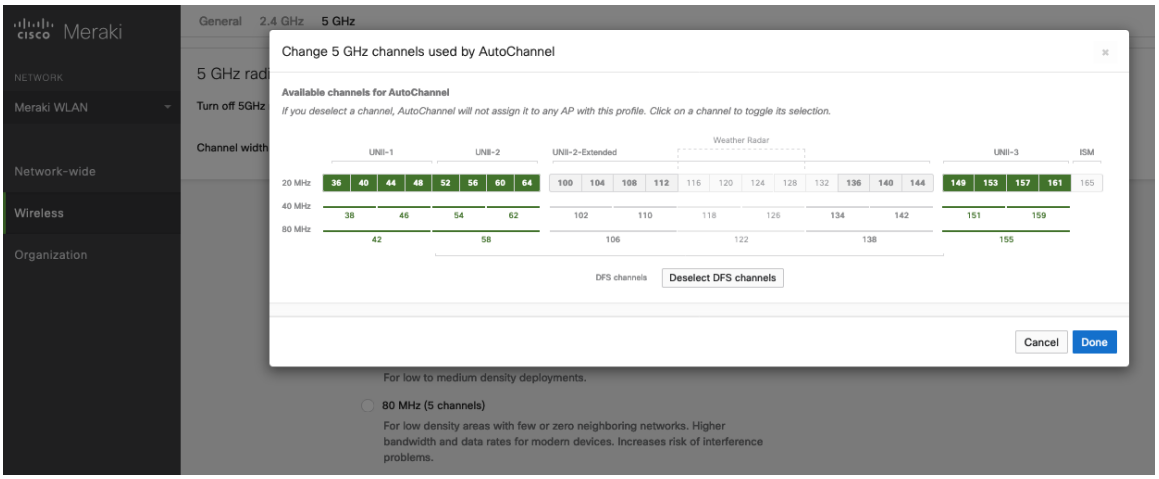
2.4 GHz channels used by **AutoChannel** are limited to channels 1, 6, and 11 only.

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 IP Phone 8821 and 8821-EX will utilize the maximum transmit power supported for the current channel and data rate.

Firewall and Traffic Shaping

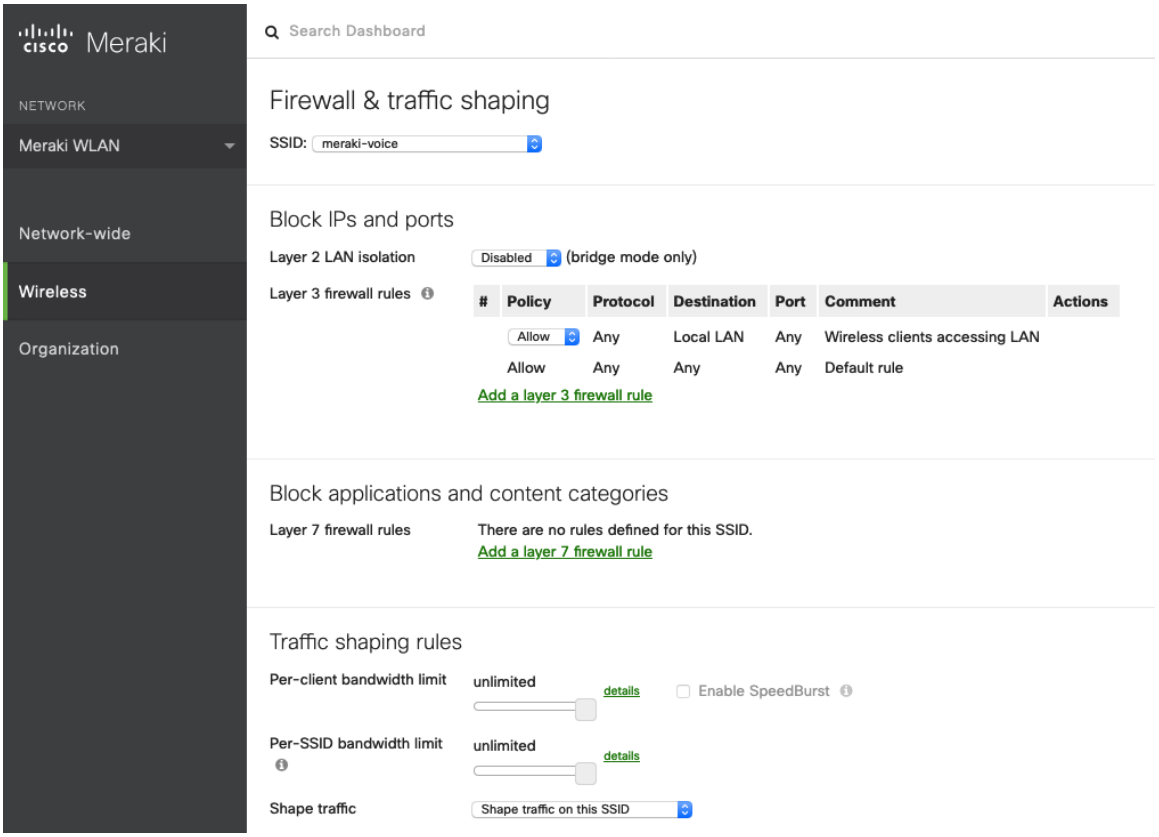
On the **Wireless > Configure > Firewall & traffic shaping** page, firewall and traffic shaping rules can be defined.

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 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 IP Phone 8821 and 8821-EX device type in the Cisco Unified Communications Manager, the corresponding device package COP file 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 package 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.

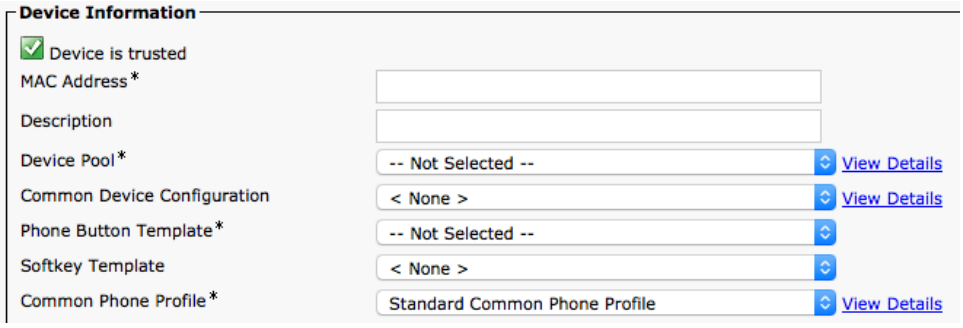
  Note: The Cisco CallManager Service on subscriber nodes do not need to be restarted.

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 IP Phone 8821 or 8821-EX to the Cisco Unified Communications Manager it must be provisioned using the wireless LAN MAC address.

The wireless LAN MAC address of the Cisco Wireless IP Phone 8821 or 8821-EX can be found by navigating to **Settings** > **Phone information** > **Model information**.

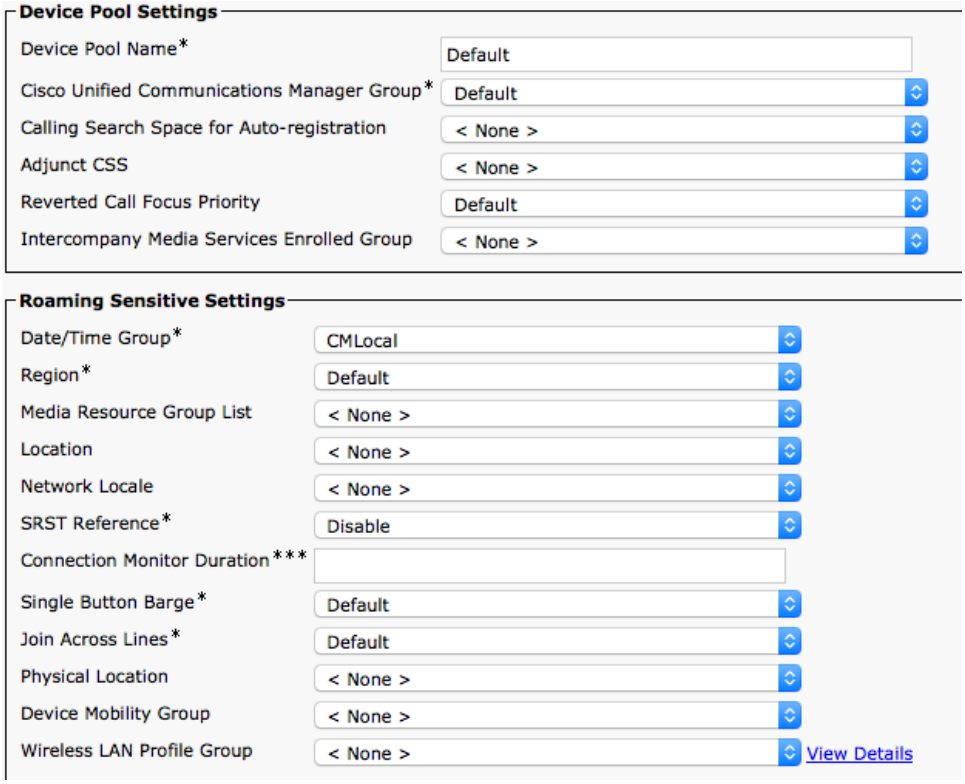


Device Pools

When creating a new Cisco Wireless IP Phone 8821 or 8821-EX, 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.

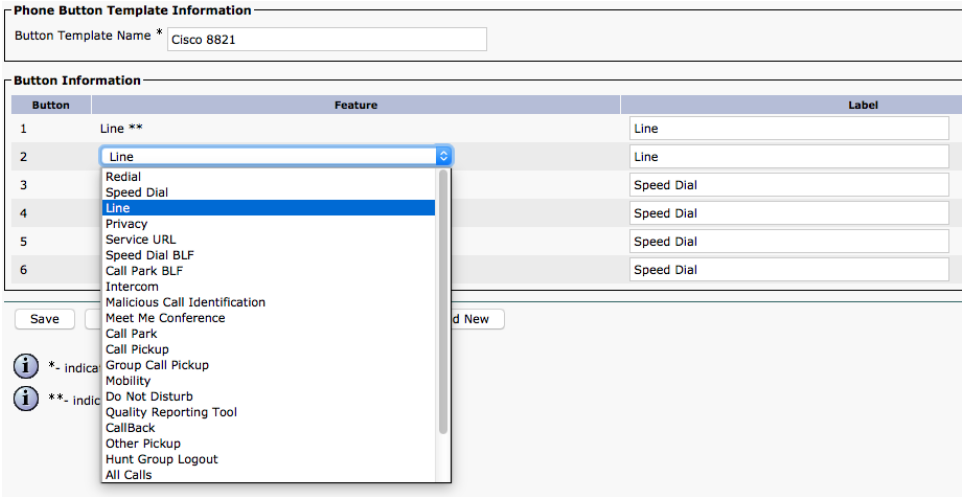
Device Pools can be used to either group devices per location, per model type, etc.



Phone Button Templates

When creating a new Cisco Wireless IP Phone 8821 or 8821-EX, a **Phone Button Template** must be configured.

Custom phone button templates can be created with the option for many different features.



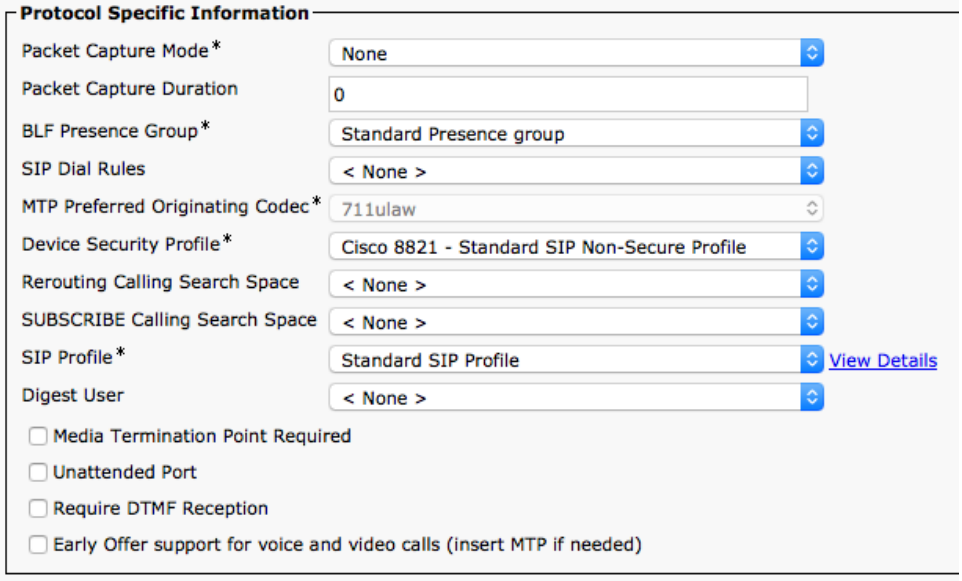
Security Profiles

When creating a new Cisco Wireless IP Phone 8821 or 8821-EX, a **Device Security Profile** must be configured.

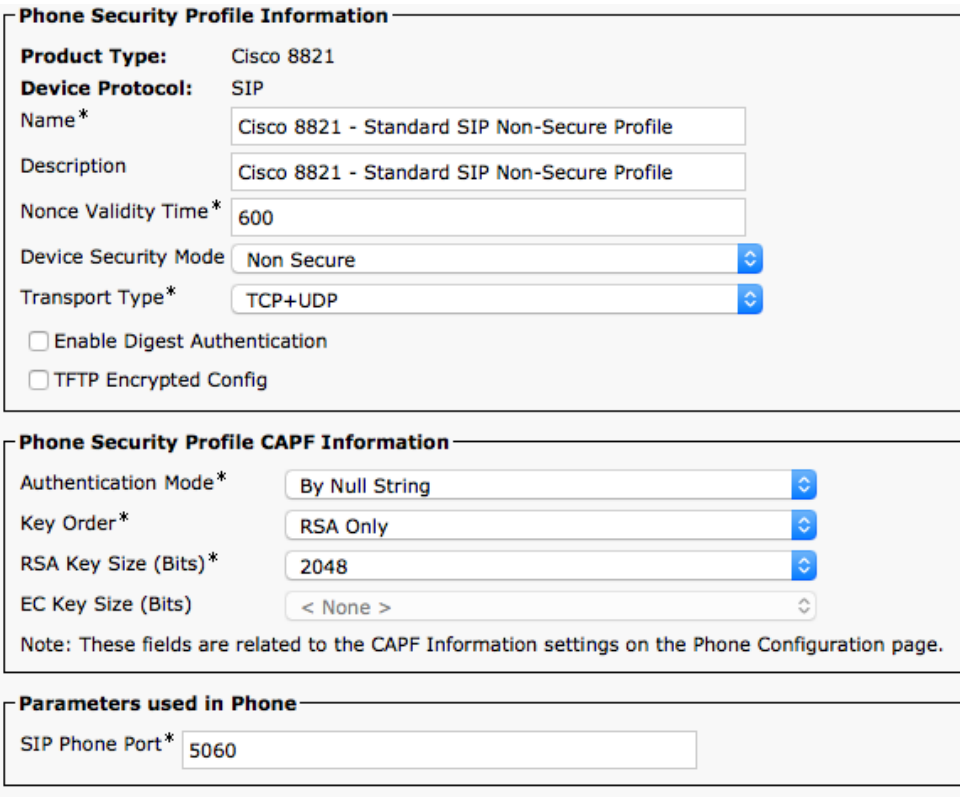
Security profiles can be utilized to enable authenticated mode or encrypted mode, where signaling, media and configuration file encryption is then enabled.

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

The Cisco Wireless IP Phone 8821 and 8821-EX have a Manufacturing Installed Certificate (MIC), which can be utilized with a security profile as well.



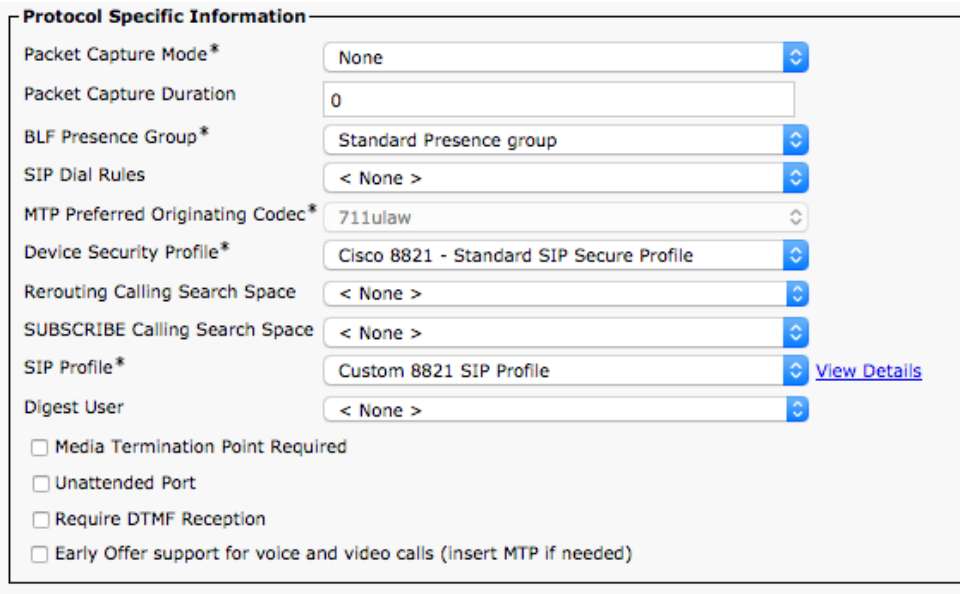
The default device security profile is the model specific **Standard SIP Non-Secure Profile**, which does not utilize encryption.



SIP Profiles

When creating a new Cisco Wireless IP Phone 8821 or 8821-EX, a **SIP Profile** must be configured.

It is recommended to create a custom SIP Profile for the Cisco Wireless IP Phone 8821 and 8821-EX (do not use the **Standard SIP Profile** or **Standard SIP Profile for Mobile Device**).



To create a custom SIP Profile for the Cisco Wireless IP Phone 8821 or 8821-EX, 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)

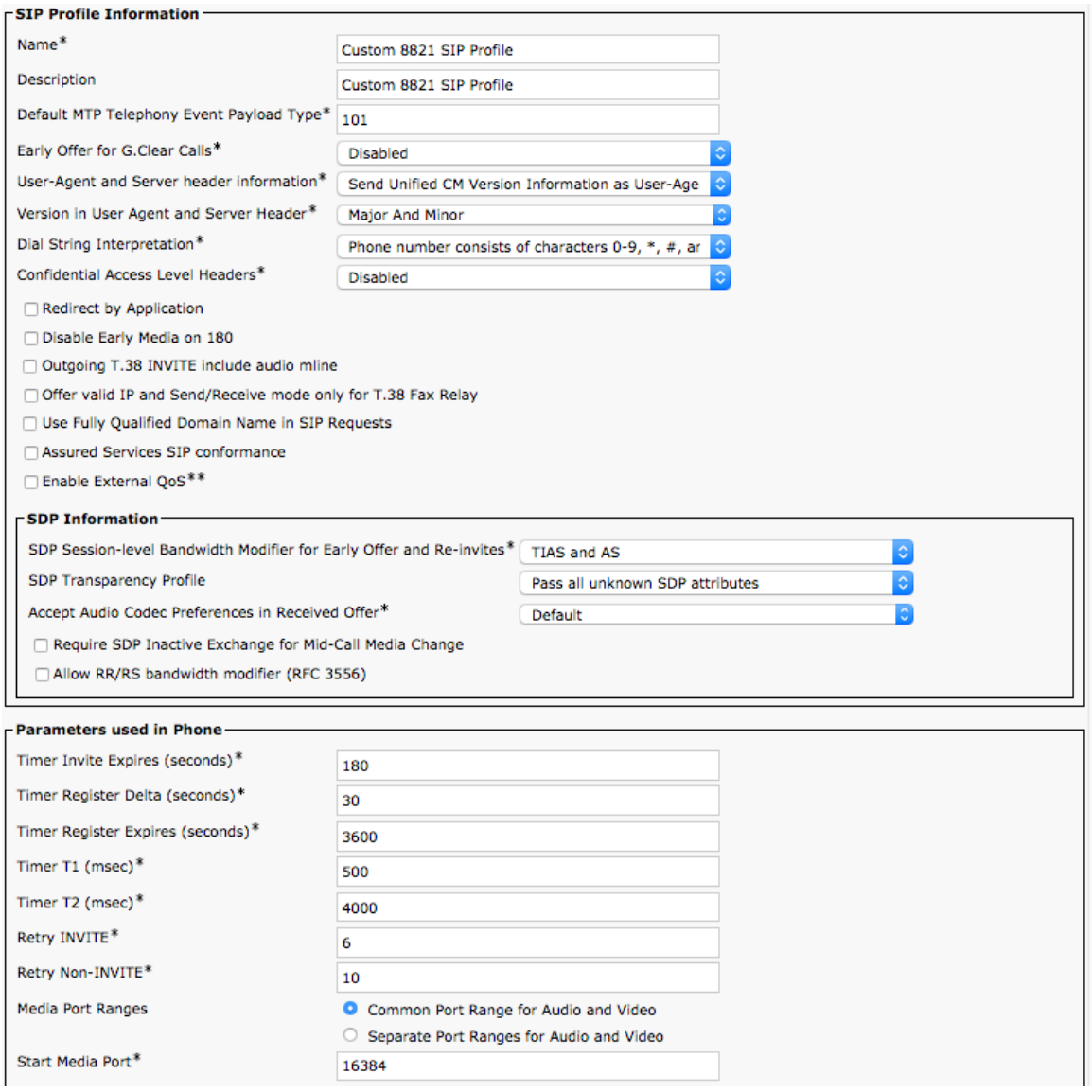
Timer Keep Alive Expires (seconds) = 300 (default = 120)

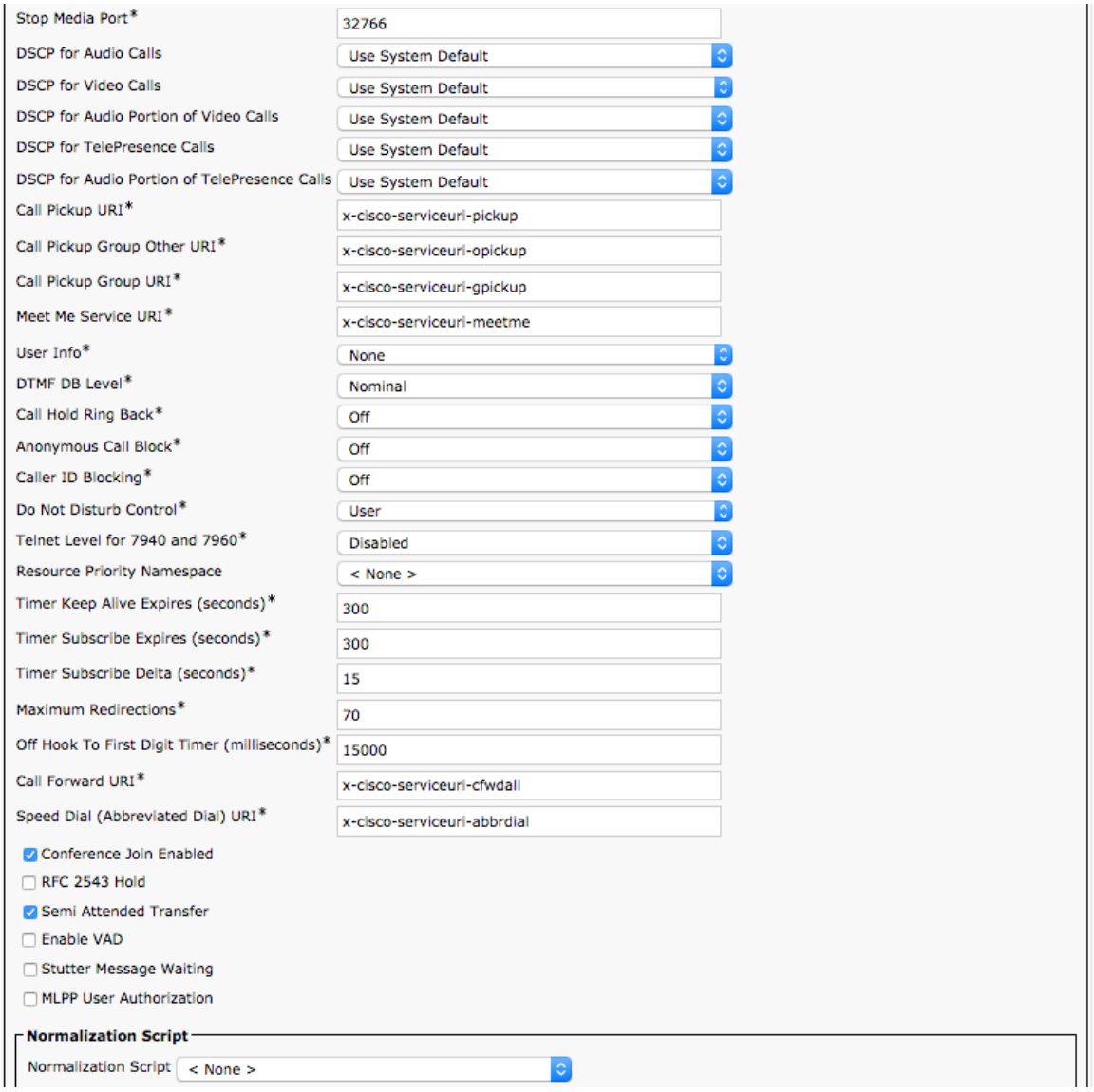
Timer Subscribe Expires (seconds) = 300 (default = 120)

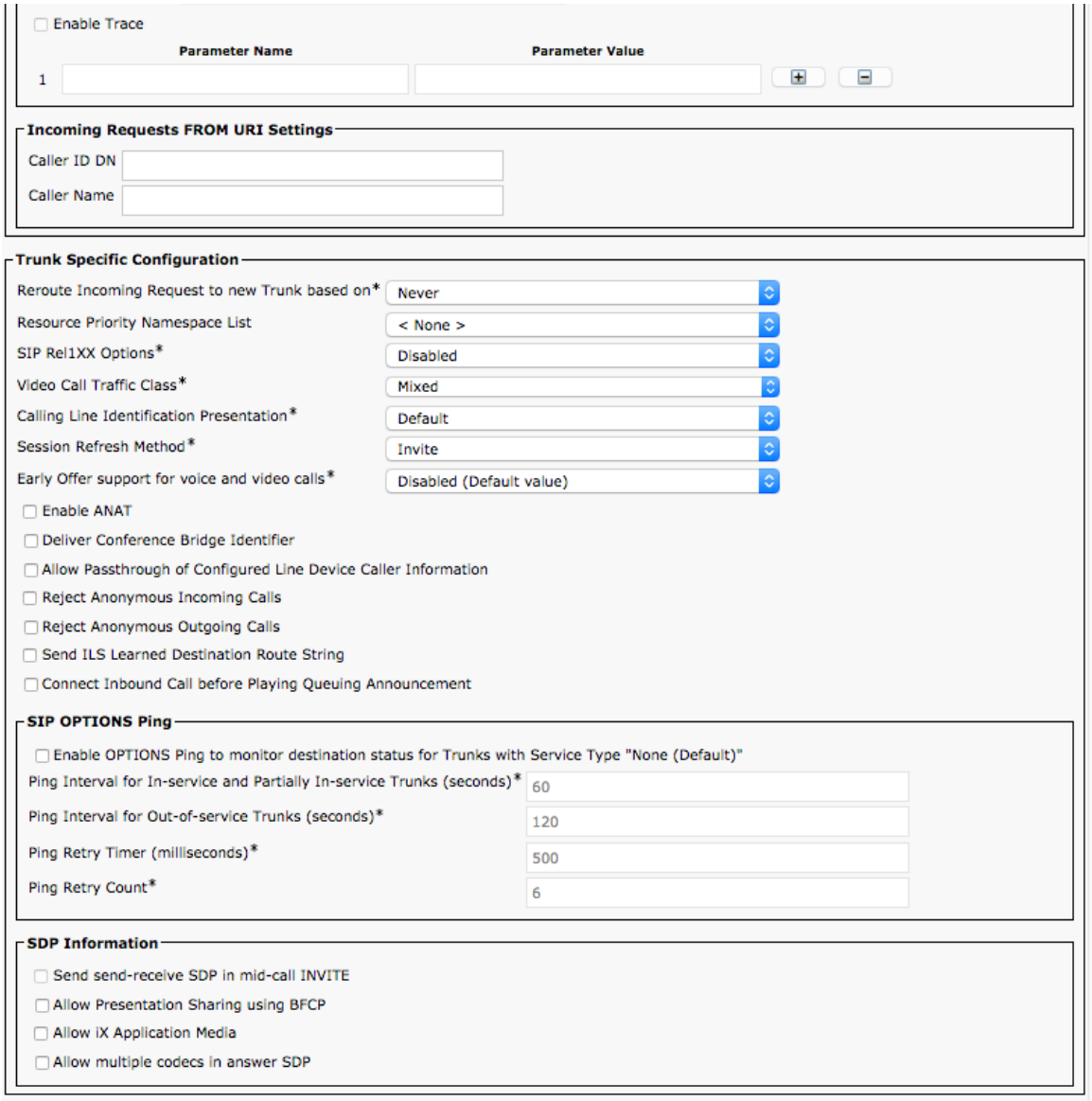
Timer Subscribe Delta (seconds) = 15 (default = 5)

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

Custom SIP Profile Example




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 Bluetooth can be configured on an enterprise phone, common phone profile or individual phone level.

Bluetooth is enabled by default for the Cisco Wireless IP Phone 8821 and 8821-EX.

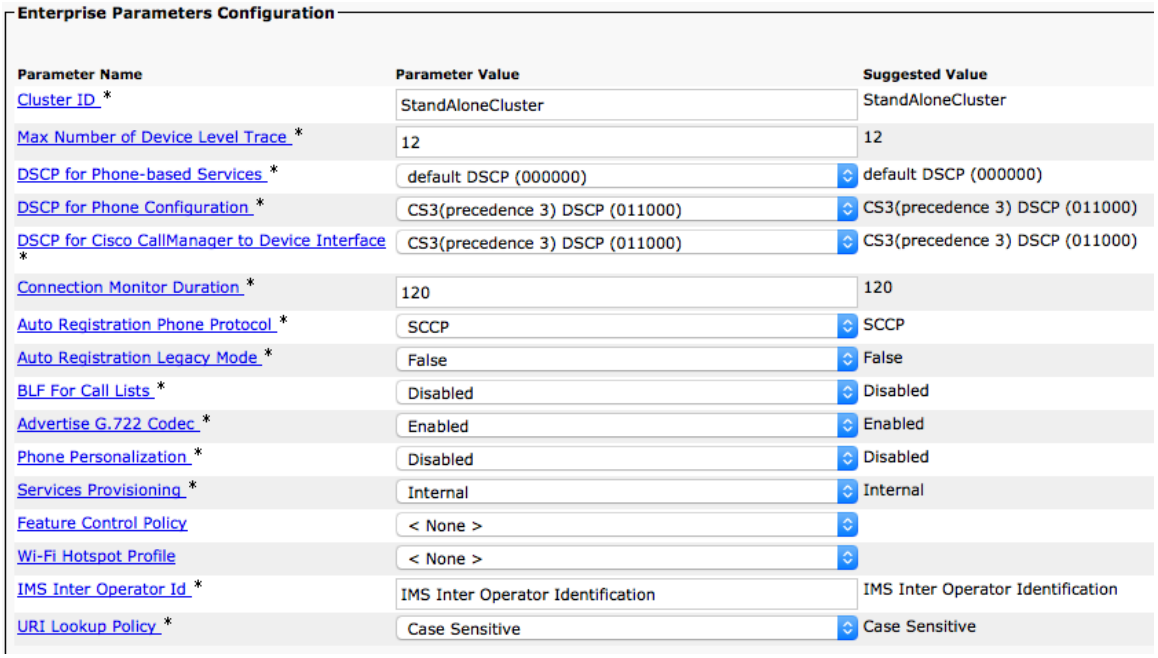
Override common settings can be enabled at either configuration level.

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.



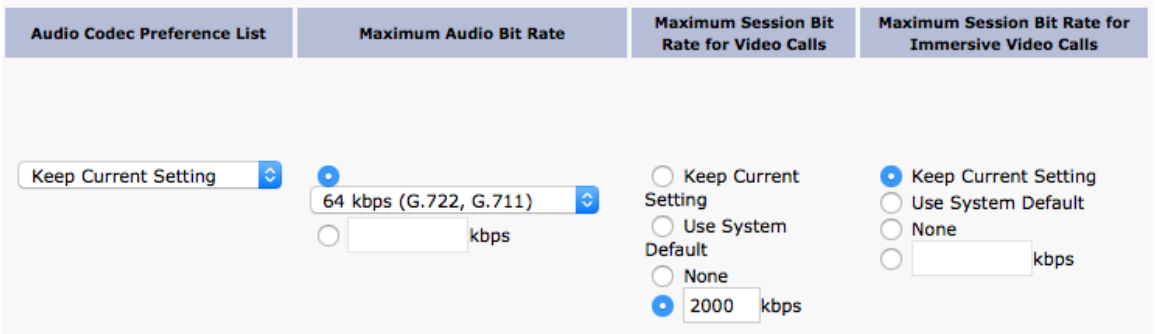
G.722 and iSAC Advertisement

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

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

Audio 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
iSAC	32 Kbps
iLBC	16 Kbps
G.729	8 Kbps

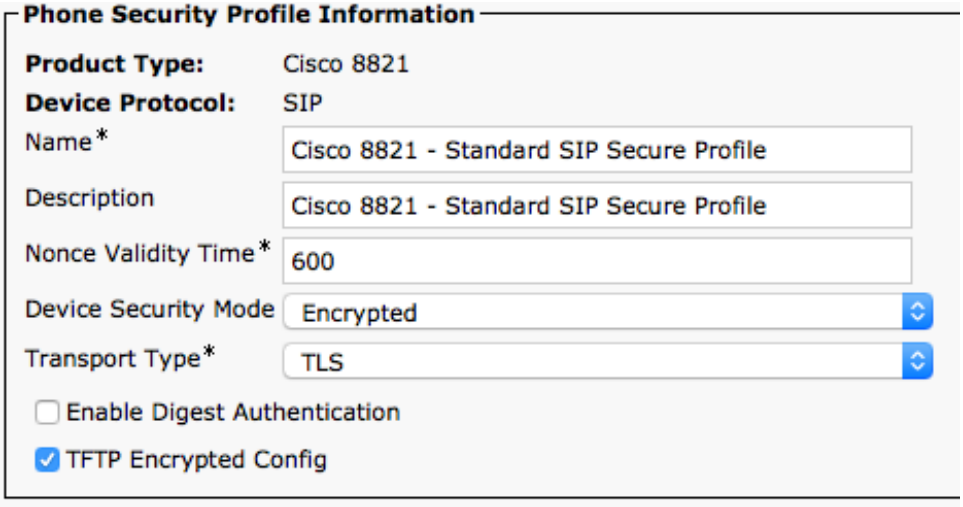
Wireless LAN Profiles

With Cisco Unified Communications Manager 10.0 release and later, the Cisco Wireless IP Phone 8821 and 8821-EX can be provisioned with Wireless LAN Profiles via the Cisco Unified Communications Manager.

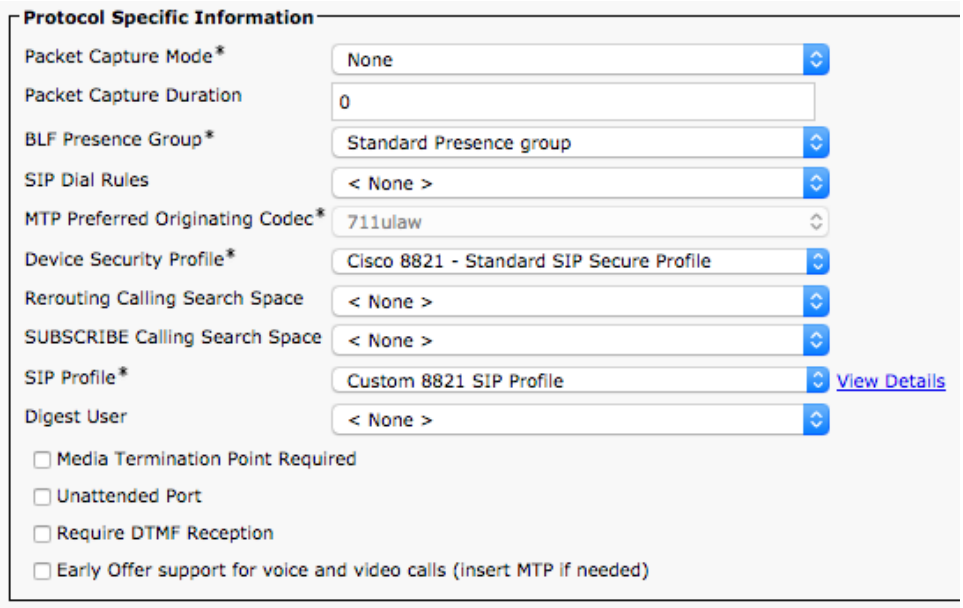
With Cisco Unified Communications Manager 11.0 and later, EAP-TLS support is included.

Use the following guidelines to configure a Wireless LAN profile within Cisco Unified Communications Manager to then apply to a Cisco Wireless IP Phone 8821 or 8821-EX.

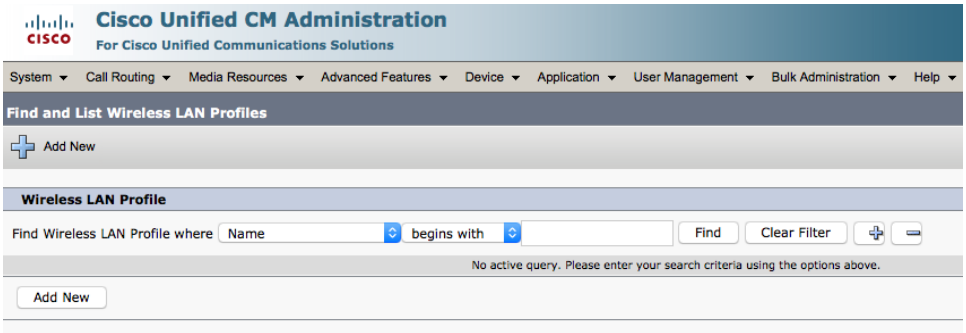
- Prior to creating a Wireless LAN Profile and associating it to a Cisco Wireless IP Phone 8821 and 8821-EX, the Cisco Wireless IP Phone 8821 and 8821-EX should be configured to utilize a security profile in which TFTP encryption is enabled so Wireless LAN Profile data is not passed down to the Cisco Wireless IP Phone 8821 and 8821-EX in clear text via TFTP.



- Once the security profile has been created, it then needs to be applied to the Cisco Wireless IP Phone 8821 and 8821-EX to enable TFTP encryption for that Cisco Wireless IP Phone 8821's and 8821-EX's configuration files.
- Select the configured security profile from the **Device Security Profile** drop-down menu.

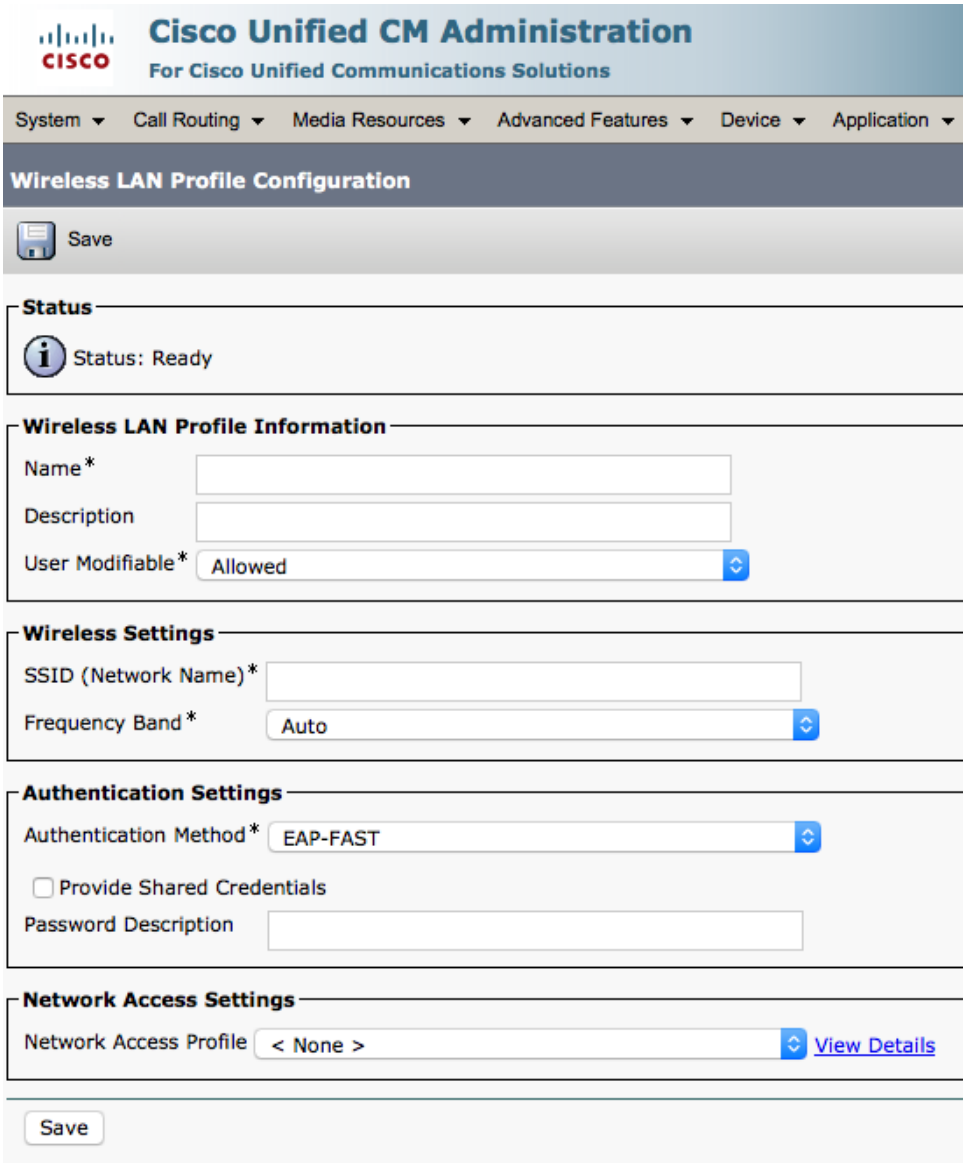


- To create a Wireless LAN Profile, navigate to **Device > Device Settings > Wireless LAN Profile** within the Cisco Unified Communications Manager's Administration interface.
- From the Wireless LAN Profile page, select **Add New**.



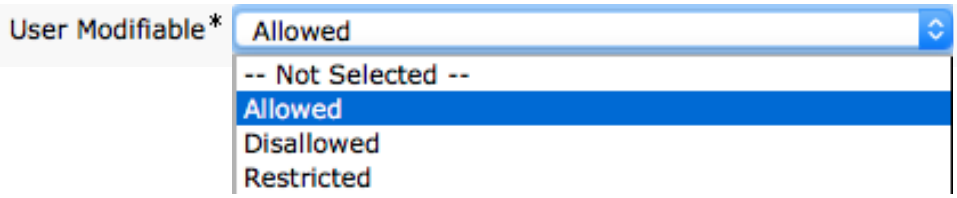
- A Wireless LAN Profile can then be created where the **Name**, **Description**, **Wireless Settings** (**SSID**, **Frequency Band**, **User Modifiable**), and **Authentication Settings** are specified.

- Below are Wireless LAN Profile defaults:
  - **Frequency Band** = Auto
  - **User Modifiable** = Allowed
  - **Authentication Method** = EAP-FAST

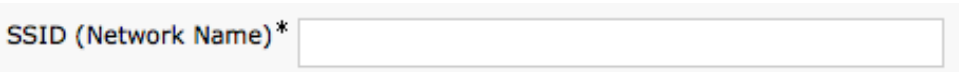


- Enter a **Name** for the Wireless LAN Profile containing up to 50 characters.
- A **Description** containing up to 63 characters can optionally be configured.

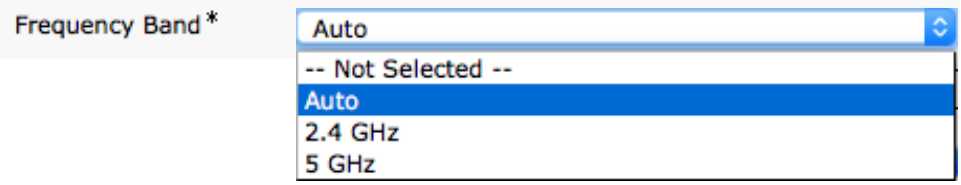
- Select the desired **User Modifiable** option.
  - **Allowed** - The user has the capability to change any Wireless LAN settings (e.g. Enable/Disable, SSID, Frequency Band, Authentication Method, Username and Password, PSK Passphrase, WEP Key) locally on the endpoint.
  - **Disallowed** - The user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



- Enter an **SSID** containing up to 32 ASCII characters.

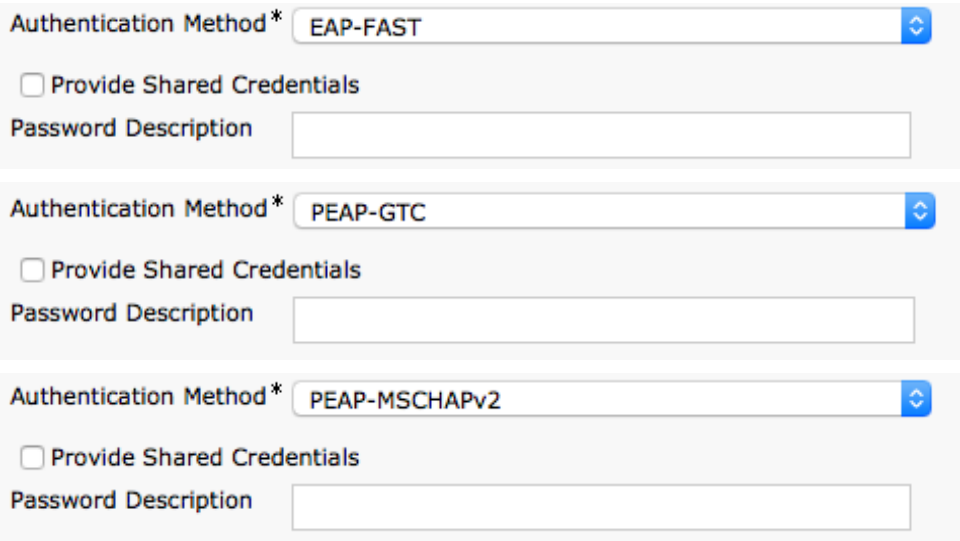


- Select the desired **Frequency Band** option.
  - **Auto** = Give preference to 5 GHz channels, but operates on both 5 GHz and 2.4 GHz channels
  - **2.4 GHz** = Operates on 2.4 GHz channels only
  - **5 GHz** = Operates on 5 GHz channels only

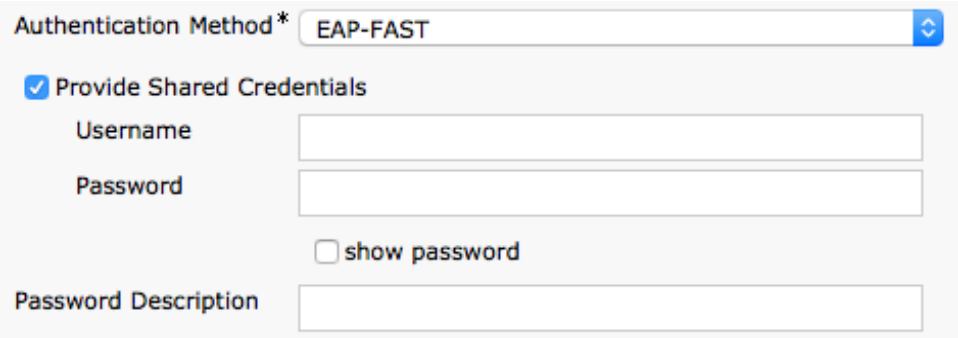


- Select the desired **Authentication Method** option.

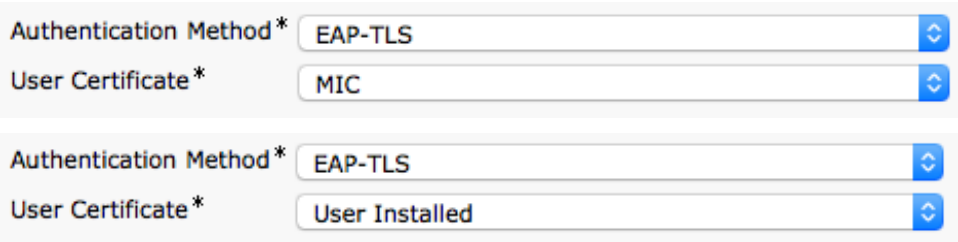
- If **EAP-FAST**, **PEAP-MSCHAPv2**, or **PEAP-GTC** is selected then the option to enter shared credentials (Username and Password) is available.
- If **Provide Shared Credentials** is not checked, then the Username and Password will need to be configured locally on the Cisco Wireless IP Phone 8821 and 8821-EX by the admin or user.



- If **Provide Shared Credentials** is checked, then the specified **Username** and **Password** will be utilized for all Cisco Wireless IP Phone 8821 and 8821-EX that utilize this Wireless LAN Profile.
- Up to 64 characters can be entered for the Username and Password.
- A **Password Description** can optionally be entered.

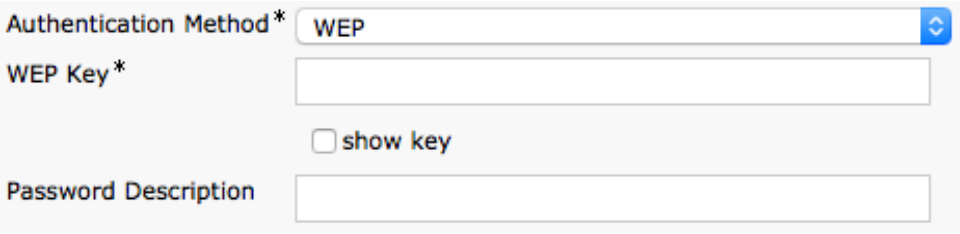


- If **EAP-TLS** is selected then **User Certificate** must be configured to specify the type of user certificate to utilize for EAP-TLS authentication.
- Can set **User Certificate** to **MIC** (Manufacturing Installed Certificate) or **User Installed**.

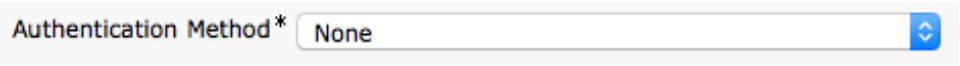


- If **PSK** is selected to utilize Pre-Shared Key authentication, then a **PSK Passphrase** must be entered.
- The **PSK Passphrase** must be in one of the following formats:
  - 8-63 ASCII character string
  - 64 HEX character string
- A **Password Description** can optionally be entered.

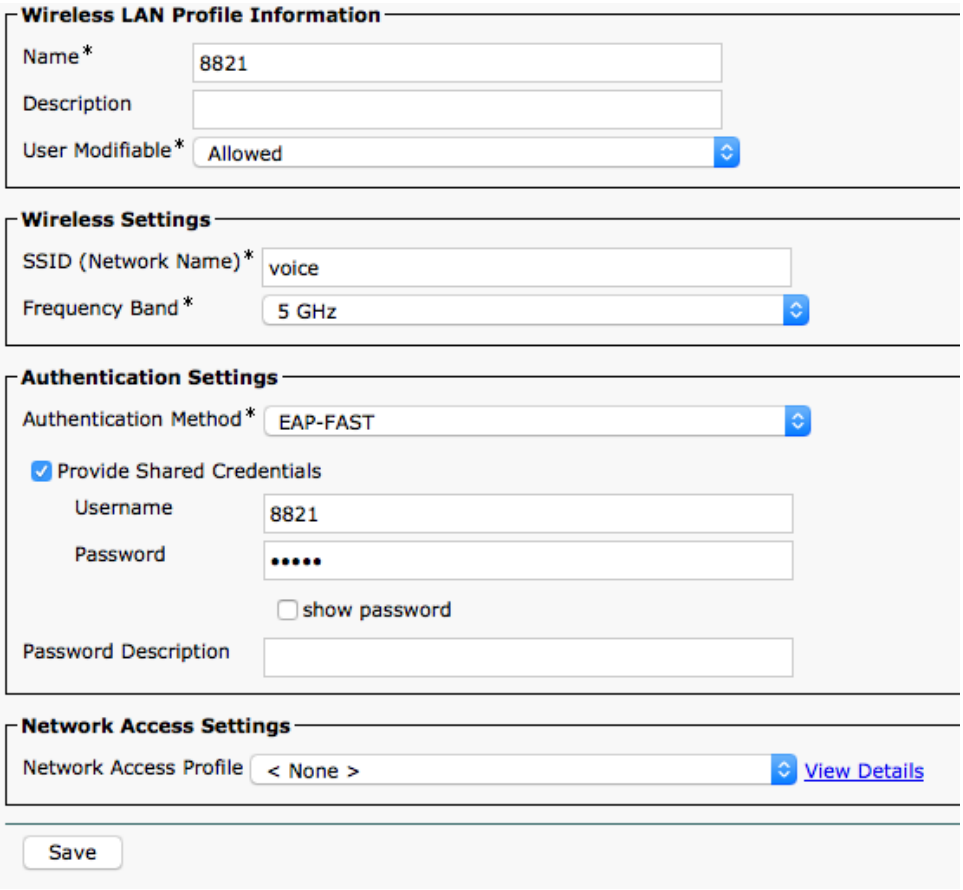
- If **WEP** is selected to utilize static WEP (Wired Equivalent Privacy) authentication, then a **WEP Key** must be entered.
- Only WEP key 1 is supported, so need to ensure that the entered key matches transmit key on the access point side.
- The **WEP Key** must be in one of the following formats:
  - **40/64 Bit Key** = 5 digit ASCII or 10 digit HEX character string
  - **104/128 Bit Key** = 13 digit ASCII or 26 digit HEX character string
- A **Password Description** can optionally be entered.



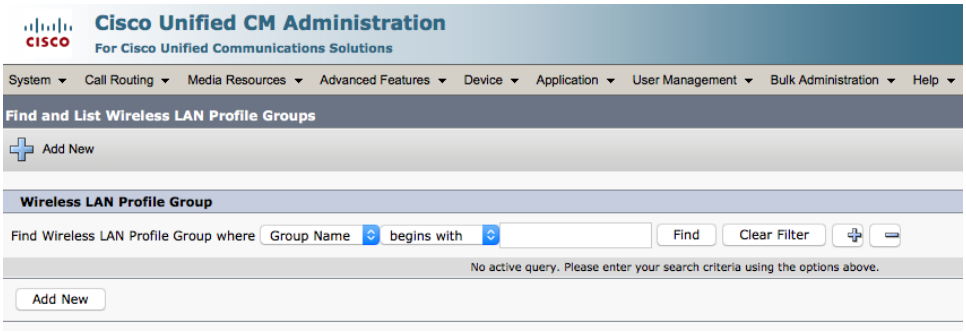
- If **None** is selected, then no authentication is required and no encryption will be utilized.



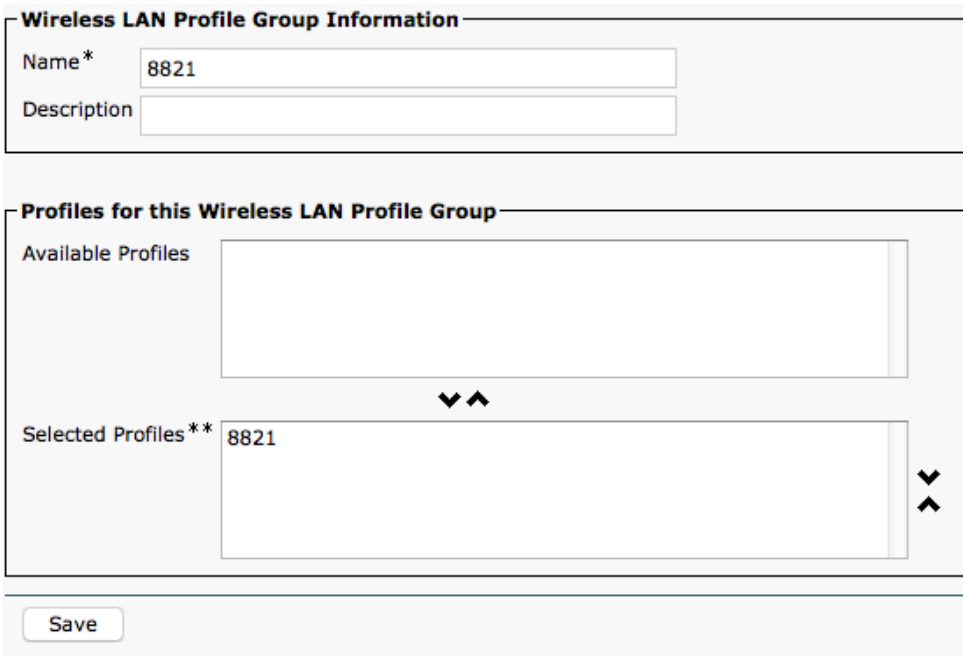
- Select **Save** once the Wireless LAN Profile configuration is complete.
- The Cisco Wireless IP Phone 8821 and 8821-EX do not support the **Network Access Profile** option.



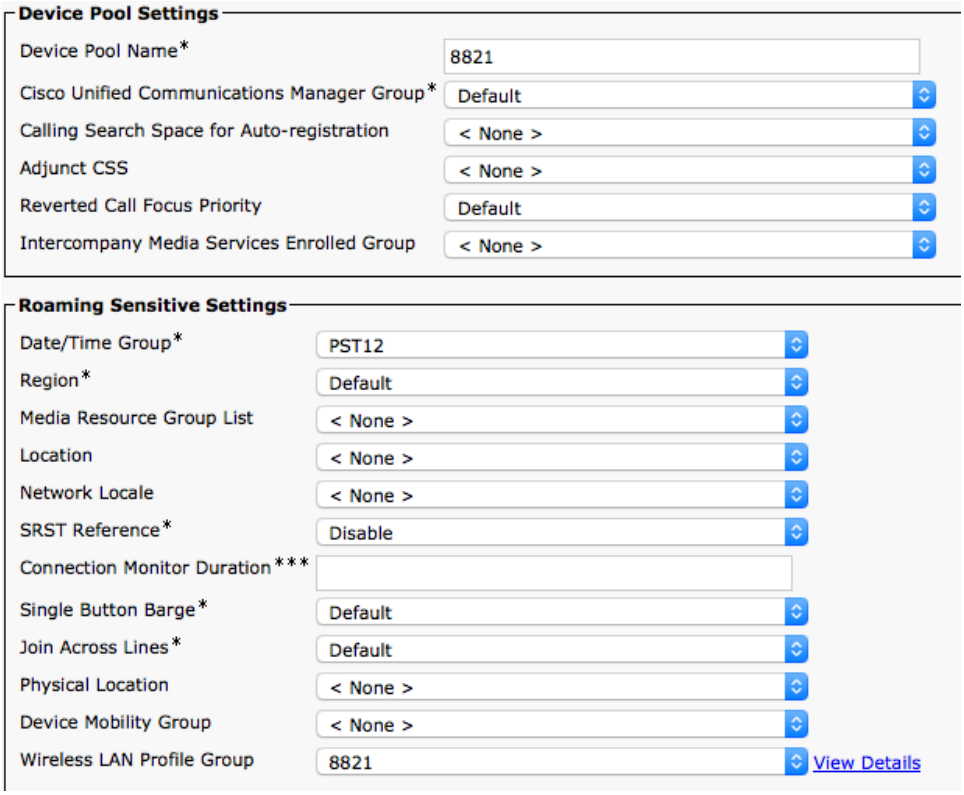
- To create a Wireless LAN Profile Group, navigate to **Device > Device Settings > Wireless LAN Profile Group** within the Cisco Unified Communications Manager's Administration interface.
- From the Wireless LAN Profile Group page, select **Add New**.



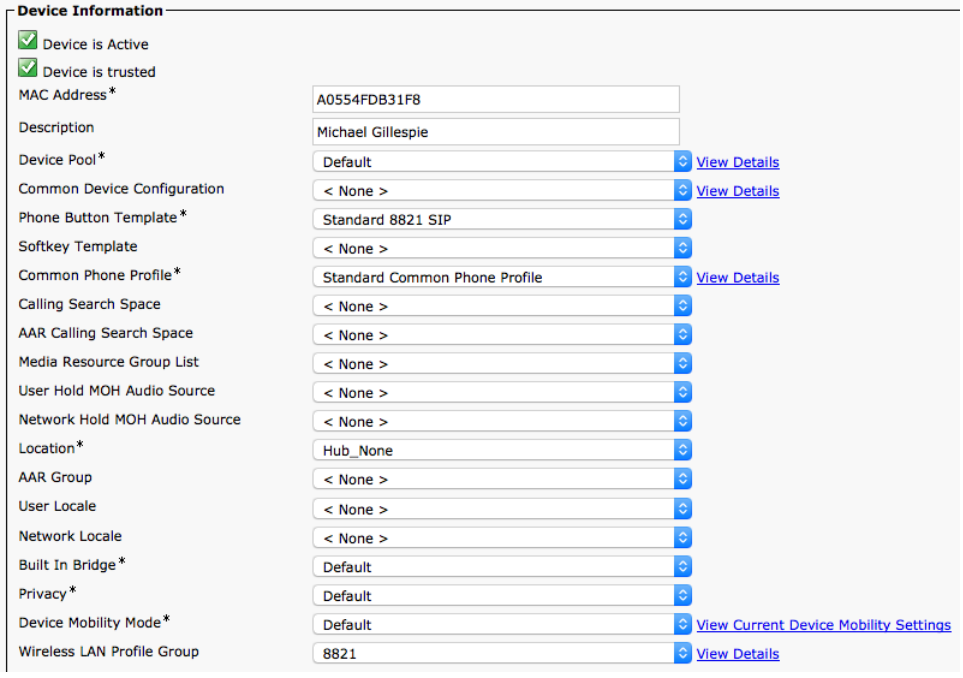
- A Wireless LAN Profile Group can then be created where the Name, Description, and Wireless LAN Profiles are specified.
- Up to **4** Wireless LAN Profiles can be added to a Wireless LAN Profile Group.
- Select **Save** once the Wireless LAN Profile Group configuration is complete.



- Once the Wireless LAN Profile Group has been created, it can be applied to a Device Pool or an individual Cisco Wireless IP Phone 8821 and 8821-EX.
- To apply a Wireless LAN Profile Group to a device pool, navigate to **System > Device Pool** within the Cisco Unified Communications Manager's Administration interface.
- Create a Device Pool as necessary and put the desired Cisco Wireless IP Phone 8821 and 8821-EX into this Device Pool.
- Once the Device Pool has been created, configure the Wireless LAN Profile Group then select **Save**.
- Once the Wireless LAN Profile Group has been applied to the Device Pool, select **Apply Config** for the Cisco Wireless IP Phone 8821 and 8821-EX to download the Wireless LAN Profile Group configuration.



- To apply a Wireless LAN Profile Group to an individual Cisco Wireless IP Phone 8821 and 8821-EX, navigate to **Device > Phone** within the Cisco Unified Communications Manager's Administration interface.
- Navigate to the desired Cisco Wireless IP Phone 8821 and 8821-EX, configure the Wireless LAN Profile Group then select **Save**.
- Once the Wireless LAN Profile Group has been applied to the individual Cisco Wireless IP Phone 8821 and 8821-EX, select **Apply Config** for the Cisco Wireless IP Phone 8821 and 8821-EX to download the Wireless LAN Profile Group configuration.



Note: The Cisco Wireless IP Phone 8821 and 8821-EX currently do not support use of the **LSC** (Locally Significant Certificate) as the **User Certificate** for EAP-TLS.

For more information about TCP and UDP ports used by the Cisco Wireless IP Phone 8821 and 8821-EX 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

Cisco Unified Communications Manager Express

With release 10.5 of Cisco Unified Communications Manager Express, the Cisco Wireless IP Phone 8821 and 8821-EX are to utilize the fast track method utilizing the Cisco Unified IP Phone 9971 as the reference model (use 7975 as reference model if needing softkey template support).

With release 11.0 and 11.5 of Cisco Unified Communications Manager Express, the Cisco Wireless IP Phone 8821 and 8821-EX can utilize the Cisco IP Phone 8861 as the reference model.

With release 11.7 and later of Cisco Unified Communications Manager Express, there is native support for the Cisco Wireless IP Phone 8821 and 8821-EX, therefore can use the Cisco IP Phone 8821 as the model type.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/feature/phone_feature/phone_feature_support_guide.html#_Toc436645184

Sample Configuration

```
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname CME
!
boot-start-marker
boot system flash:c2900-universalk9-mz.SPA.156-1.T0a.bin
boot-end-marker
!
aqm-register-fnf
!
logging buffered 51200 warnings
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
ethernet lmi ce
clock timezone EST -5 0
clock summer-time EST recurring
!
```

```
ip domain name cisco.com
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
cts logging verbose
!
crypto pki trustpoint TP-self-signed-2915022231
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2915022231
 revocation-check none
 rsakeypair TP-self-signed-2915022231
!
crypto pki certificate chain TP-self-signed-2915022231
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32393135 30323232 3331301E 170D3132 30373033 30333039
  35395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 39313530
  32323233 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100ABC4 D23F5B00 36665DDC 86171E19 CE92D3E5 A0576068 3AADCD26 89C3B795
  1B4518BE 2B173A5C 60A82125 80935C29 1027DE28 FCF05E62 18A07C10 C59D34ED
  9A14CCD7 3981E1BB 20445CFC 99686D13 D84C6B03 4D84B448 1102A0CF AE333B48
  CBF5B85F 6842A40B C9555AB0 0C283E66 0341DD0C D0BBEB8D DCA8AE00 0DAF3083
  8E170203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14D881B2 7EF36719 1DC028ED 84384303 685250E6 E6301D06
  03551D0E 04160414 D881B27E F367191D C028ED84 38430368 5250E6E6 300D0609
  2A864886 F70D0101 05050003 81810011 2DB8EA5C 2D588D18 1CB78EE2 0FBAE777
  716B441C 9389C987 612BBBEA 7B9E30CB 4BAF41A7 0F0DB51D E4F45FB2 F8A139B3
  70DF1E94 A7EE4F81 B08E3F21 C0743E56 59D42988 D7FAB957 FADBBFE0 A77F404F
  634BDD93 87559D1D CCA93BCA 87899A98 C151CF62 EF183C8E CB2C9DFC 71F45AE0
  92A26FBF CBA7FA2B F9C5DB6D EEC936
        quit
!
voice-card 0
!
voice service voip
 no ip address trusted authenticate
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 no supplementary-service sip moved-temporarily
 sip
  bind control source-interface GigabitEthernet0/0
  bind media source-interface GigabitEthernet0/0
  registrar server expires max 1000 min 800
  no call service stop
!
voice register global
 mode  cme
 source-address 10.0.0.10 port 5060
 max-dn 40
 max-pool 42
 load 8821 sip8821.11-0-6SR5-5
 authenticate register
 olsontimezone America/New_York version 2010o
```

```
 timezone 12
 create profile sync 0089201122844265
!
voice register dn  1
 number 1101
 name 8821-1
 label 1101
 mwi
!
voice register dn  2
 number 1102
 name 8821-2
 label 1102
 mwi
!
voice register dn 10
 number 1110
 intercom speed-dial 1000
!
voice register pool  1
 busy-trigger-per-button 2
 id mac A055.4FDB.31F8
 session-transport tcp
 type 8821
 number 1 dn 1
 number 6 dn 10
 dtmf-relay rtp-nte
 username 8821-1 password <REMOVED>
 codec g711ulaw
 no vad
 paging-dn 1
!
voice register pool  2
 busy-trigger-per-button 2
 id mac A055.4FDB.31F9
 session-transport tcp
 type 8821
 number 1 dn 2
 number 6 dn 10
 dtmf-relay rtp-nte
 username 8821-2 password <REMOVED>
 codec g711ulaw
 no vad
 paging-dn 1
!
license udi pid CISCO2901/K9 sn <REMOVED>
!
username <REMOVED> privilege 15 password 7 <REMOVED>
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 10.0.0.10 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
!
tftp-server flash:/8821/sip8821.11-0-6SR5-5.loads alias sip8821.11-0-6SR5-5.loads
tftp-server flash:/8821/dtblob8821.HE-01-011.sbn alias dtblob8821.HE-01-011.sbn
tftp-server flash:/8821/fbi8821.HE-01-014.sbn alias fbi8821.HE-01-014.sbn
tftp-server flash:/8821/kern8821.11-0-6SR5-5.sbn alias kern8821.11-0-6SR5-5.sbn
tftp-server flash:/8821/rootfs8821.11-0-6SR5-5.sbn alias rootfs8821.11-0-6SR5-5.sbn
tftp-server flash:/8821/sb28821.HE-01-024.sbn alias sb28821.HE-01-024.sbn
tftp-server flash:/8821/vc48821.11-0-6SR5-5.sbn alias vc48821.11-0-6SR5-5.sbn
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
sip-ua
 timers connection aging 20
!
gatekeeper
 shutdown
!
telephony-service
 max-ephones 25
 max-dn 25
 ip source-address 10.0.0.10 port 2000
 url authentication http://10.0.0.10/CCMCIP/authenticate.asp
 cnf-file perphone
 olsontimezone America/New_York version 2010o
 time-zone 12
 max-conferences 8 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
ephone-dn 1
 number 1000
 paging
!
```

```
ephone-dn 2
 number 1001
 intercom 1000
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 privilege level 15
 transport input telnet ssh
line vty 5 15
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp source GigabitEthernet0/0
ntp server 10.0.0.2
!
end
```

Product Specific Configuration Options

In Cisco Unified Communications Manager Administration, the following configuration options are available for the Cisco Wireless IP Phone 8821 and 8821-EX.

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 IP Phone 8821 Configuration Options

Field Name	**Description**

Disable Speakerphone	This parameter disables the speakerphone functionality. Disabling speakerphone functionality will not affect the headset. You can use lines and speed dials with headset/handset.
Disable Speakerphone and Headset	This parameter disables all speakerphone and headset functions.
Settings Access	This parameter specifies whether the Settings menu on the phone is functional. When Settings Access is enabled, you can change the phone configuration, ring type, etc. on the phone. When Settings Access is disabled, configuration changes are not allowed. When Settings Access is Restricted, you can only change user preferences.
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. Features, such as QRT (Quality Report Tool), will not function properly without access to the phones web pages. This setting will also affect any serviceability application such as CiscoWorks that relies on web access.
HTTPS Server	This parameter specifies whether to permit HTTP and HTTPS or HTTPS only connections if Web Access is enabled.
Disable TLS 1.0 and TLS 1.1 for Web Access	This parameter indicates to disable TLS 1.0 and TLS 1.1 when using https for web access.
Web Admin	This parameter controls the accessibility of the Web Admin interface, which operates independently from the Web Access parameter. If disabled, then the Web Admin interface is not available. If enabled, then the Web Admin interface is available, but also requires the Admin Password to be specified.
Admin Password	This parameter specifies the password to access the phone's Web Admin interface. Enter a 8-127 character password.
Bluetooth	This parameter specifies whether the phone's Bluetooth is enabled or disabled.
Out of Range Alert	This parameter controls the frequency of audible alerts when the phone is out of range of an access point. If disabled, the phone does not play audible alerts. If enabled, the phone can beep once or regularly at a selected interval (10, 30, or 60 seconds) when it is out of range of an access point and once the phone is reconnected to an access point, audible alerts will stop.
Scan Mode	This parameter controls when the phone performs scanning. If Continuous is selected, then the phone scans continuously even when it is not in a call. If Auto is selected, then the phone scans when it is in a call or when the received strength signal indicator (RSSI) threshold has been met when not in a call. If Single AP is selected, then the phone does not scan except when first powered on or when the connection is lost.
Application URL	This parameter specifies the URL which the phone utilizes for application services including Push To Talk (PTT).
Application Request Timer	This parameter specifies the maximum time that the phone will wait for application requests to complete. If the application request can not be completed within the specified time, a failure response will be reported to the application. Use the higher value when you expect the requests will take longer to complete. Use the lower value when the application can not wait long enough to receive the successful or failure responses.

Application Button Activation Timer	This parameters specifies the amount of time one must hold down the Application Button to activate the application specified in the Application URL. The timer values are in seconds. A value of 0 indicates that a simple push of the Application Button will active the application. For non-zero values, the application is activated after the specified timer value expires.
Application Button Priority	This parameter specifies the priority of the Application Button relative to all other tasks on the phone. If set to Low, then the Application Button only works when the phone is idle and on the main screen. If set to Medium, then the Application Button takes precedence over all tasks on the phone except when the phone keypad is locked. If set to High, then the Application Button takes precedence over all tasks on the phone even if the phone keypad is locked.
Emergency Numbers	This parameter specified 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.
Dialing Mode	This parameter controls the behavior of the "Send" (green) key when it is pressed. If On-hook Dialing is selected, then the phone will remain on-hook. If Off-hook Dialing is selected, then phone sends an off-hook message.
Power Off in Multicharger	This parameter specifies whether the phone should power off when it is placed in a Multicharger or not.
Background Image	This parameter specifies the default wallpaper file. The administrator controls access to the phone’s wallpaper list.
Home Screen	This parameter sets the phone's default home screen to Application View or Line View.
Left Softkey	This parameter determines whether a shortcut to Favorites, Local Contacts, or Voicemail will be displayed in the left softkey list or not.
Voicemail Access	This parameter enables or disables access to Voicemail.
Applications Access	This parameter enables or disables access to Applications.
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.
Recording Tone Local Volume	This parameter can be used to configure the volume of the recording tone that the local party hears. This volume applies regardless of the actual device used for hearing (handset, speakerphone, headset). The volume should be in the range of 0% to 100%, with 0% being no tone and 100% being at the same level as the current volume setting. The default value is 20%.
Recording Tone Remote Volume	This parameter can be used to configure the volume of the recording tone that the remote party hears. The volume should be in the range of 0% to 100%, with 0% being less than -66dBM and 100% being -4dBM. The default value is -10dBM or 50%.
Recording Tone Duration	This parameter specifies the length of time in milliseconds for which the recording tone is inserted in the audio stream. The default for this parameter is set

	to the value in the Network locale file for this field. The valid range for this parameter is a value between 1 and 3000 milliseconds.
Remote Log	This parameter specifies where to send the log data by serviceability. If enabled, the log data will be copied by serviceability to the place specified by Log Server. If disabled, the log data will not be copied by serviceability to the place specified by Log Server.
Log Profile	This parameter specified the pre-defined logging profile.
Log Server	This parameter specifies an IP address and port of a remote system where log messages are sent. The format is:xxx.xxx.xxx.xxx:ppppp@@options. Options will be format as base=x;pfs=y; base value range is 0~7,pfs value range is 0~1. And the two parameters are optional. Absence of pfs or base, pfs will be set to the default value 0 and base will be set to the default value 7.
Cisco Discover Protocol (CDP)	This parameter allows the administrator to enable or disable Cisco Discovery Protocol (CDP).
SSH Access	This parameter specifies whether the phone will accept SSH connections. Disabling SSH Access will prevent access to the phone via SSH.
Ring Locale	This parameter specified the ring cadence. The phone has distinctive ring for On-net/Off-net or line based, but its ring cadence is fixed, and it is based on US standard only. Ring cadence in US standard is opposite to Japan standard. To support Japan ring cadence, the ring cadence should be configurable according to Ring Locale.
TLS Resumption Timer	This parameter specifies the maximum session resumption time allowed. The current TLS session to support TLS session resumption is HTTPS client. The HTTPS client sessions support configurable session resumption timer. If the value is set to 0, TLS session resumption will be disabled.
Record Call Log From Shared Line	This parameter specifies whether to record call log from shared line or not.
Minimum Ring Volume	This parameter controls the minimum ring volume on the phone. This value is set by the administrator, and can not be changed by an end user. The end user can increase the ring volume, but may not decrease the ring volume below the level defined. The minimum ring volume range is from 0 to 15, with 0 (silent) being the default value.
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.
WLAN SCEP Server	This parameter specifies the SCEP Server the phone will use to obtain certificates for WLAN authentication. Enter the hostname or the IP address (using standard IP addressing format) of the server.
WLAN Root CA Fingerprint (SHA256 or SHA1)	This parameter specifies the SHA256 or SHA1 fingerprint of the Root CA to use for validation during the SCEP process when issuing certificates for WLAN authentication. It is recommended to utilize the SHA256 fingerprint, which can be obtained via OpenSSL (e.g. openssl x509 -in rootca.cer -noout -sha256 -

	fingerprint) or using a Web Browser to inspect the certificate details. Enter the 64 hexadecimal character value for the SHA256 fingerprint or the 40 hexadecimal character value for the SHA1 fingerprint with a common separator (colon, dash, period, space) or without a separator. If using a separator, then the separator should be consistently placed after every 2, 4, 8, 16, or 32 hexadecimal characters for a SHA256 fingerprint or every 2, 4, or 8 hexadecimal characters for a SHA1 fingerprint.
Console Access	This parameter specifies whether the serial console is enabled or disabled.
Gratuitous ARP	This parameter specifies whether the phone will learn MAC addresses from Gratuitous ARP responses. Disabling the phones ability to accept Gratuitous ARP will prevent applications which use this mechanism for monitoring and recording of voice streams from working. If monitoring capability is not desired, disable this parameter.
Show All Calls On Primary Line	This parameter specifies whether all calls presented to this device will be shown on the primary line or not.
Advertise G.722 and iSAC Codecs	This parameter specifies whether the phone will advertise the G.722 codec 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 support), and Enabled (this phone will advertise G.722 support).
Revert to All Calls	This parameter specifics whether the phone will revert to All Calls after any call is ended or not if the call is on a filter other than Primary line, All Calls, or Alerting Calls.
DF Bit	This parameter configures the DF bit in IP header.
Lowest Alerting Line State Priority	This parameter specifies the alert state when using shared lines. When disabled and there is an incoming call alerting on the shared line, the LED/Line state icon will reflect the alerting state instead of Remote-In-Use. When enabled, will see the Remote-In-Use state when there is call alerting on the shared line.
Divert Alerting Call	Control whether or not to show the Decline softkey for Incoming Call Alert.
Allow Vibrate URI When On Call	Control whether or not to allow the Vibrate URI command within an XSI message when on call.
Customer Support Use	This parameter specifies some special issue. Please split the special issue ID with ";".
Customer support upload URL	This URL is used to upload problem report files when the user has run the "Problem Report Tool" on the endpoint.
Battery Lifetime Alert	Remind users to check/replace the battery based on the phone use time.
Battery Lifetime Alert Interval	Battery lifetime alert interval.
Battery SN Reminder	Remind user to check battery serial number every time after phone boots up.

XML Syntax

To configure product specific configuration options for the Cisco Wireless IP Phone 8821 and 8821-EX with Cisco Unified Communications Manager Express, add the necessary options under **telephony-service**.

service phone <module> <value>

Field Name	Module	Value
Disable Speakerphone	disableSpeaker	**false = Disabled** true = Enabled
Disable Speakerphone and Headset	disableSpeakerAndHeadset	**false = Disabled** true = Enabled
Settings Access	settingsAccess	0 = Disabled **1 = Enabled** 2 = Restricted
Web Access	webAccess	0 = Enabled **1 = Disabled**
HTTPS Server	webProtocol	**0 = http and https Enabled** 1 = https only
Disable TLS 1.0 and TLS 1.1 for Web Access	tls12Only	0 = **Disabled** 1 = Enabled
Web Admin	webAdmin	**0 = Disabled** 1 = Enabled
Admin Password	adminPassword	8 to 127 character string
Bluetooth	bluetooth	0 = Disabled **1 = Enabled**
Out of Range Alert	outOfRangeAlert	**0 = Disabled** 1 = Beep Once 2 = Beep every 10 seconds 3 = Beep every 30 seconds 4 = Beep every 60 seconds
Scan Mode	scanningMode	0 = Auto 1 = Single AP **2 = Continuous**
Application URL	applicationURL	Up to 256 character string
Application Request Timer	appRequestTimer	**0 = 5 seconds**

		1 = 20 seconds
Application Button Activation Timer	appButtonTimer	**0 = Disabled** 1 = 1 seconds 2 = 2 seconds 3 = 3 seconds 4 = 4 seconds 5 = 5 seconds
Application Button Priority	appButtonPriority	**0 = Low** 1 = Medium 2 = High
Emergency Numbers	specialNumbers	Up to 16 character string
Dialing Mode	sendKeyAction	**0 = On-hook Dialing** 1 = Off-hook Dialing
Power Off in Multicharger	powerOffWhenCharging	**0 = Disabled** 1 = Enabled
Background Image	defaultWallpaperFile	Up to 64 character string
Home Screen	homeScreen	**0 = Application View** 1 = Line View
Left Softkey	leftSoftkey	0 = None **1 = Favorites** 2 = Local Contacts 3 = Voicemail
Voicemail Access	accessVoicemail	0 = Disabled **1 = Enabled**
Applications Access	accessApps	0 = Disabled **1 = Enabled**
Recording Tone	recordingTone	**0 = Disabled** 1 = Enabled
Recording Tone Local Volume	recordingToneLocalVolume	0-100 **(Default = 20)**
Recording Tone Remote Volume	recordingToneRemoteVolume	0-100 **(Default = 50)**
Recording Tone Duration	recordingToneDuration	1-3000
Remote Log	remoteLog	**0 = Disabled** 1 = Enabled

Log Profile	logProfile	0 = Default **1 = Preset** 2 = Telephony
Log Server	logServer	Up to 256 character string
Cisco Discover Protocol (CDP)	cdpEnable	0 = Disabled **1 = Enabled**
SSH Access	sshAccess	0 = Enabled **1 = Disabled**
Ring Locale	RingLocale	**0 = Default** 1 = Japan
TLS Resumption Timer	TLSResumptionTimer	0-3600 **(Default = 3600)**
Record Call Log From Shared Line	logCallFromSharedLine	**0 = Disabled** 1 = Enabled
Minimum Ring Volume	minimumRingVolume	**0 = Silent** 1 = Volume Level 1 2 = Volume Level 2 3 = Volume Level 3 4 = Volume Level 4 5 = Volume Level 5 6 = Volume Level 6 7 = Volume Level 7 8 = Volume Level 8 9 = Volume Level 9 10 = Volume Level 10 11 = Volume Level 11 12 = Volume Level 12 13 = Volume Level 13 14 = Volume Level 14 15 = Volume Level 15
Load Server	loadServer	Up to 256 character string
WLAN SCEP Server	wlanScepServer	Up to 256 character string
WLAN Root CA Fingerprint (SHA256 or SHA1)	wlanRootCaFingerprint	Up to 95 character string
Console Access	ConsoleAccess	0 = Enabled **1 = Disabled**

Gratuitous ARP	garp	0 = Enabled **1 = Disabled**
Show All Calls On Primary Line	allCallsOnPrimary	**0 = Disabled** 1 = Enabled
Advertise G.722 and iSAC Codecs	g722CodecSupport	**0 = Use System Default** 1 = Disabled 2 = Enabled
Revert to All Calls	revertToAllCalls	**0 = Disabled** 1 = Enabled
DF Bit	dfBit	**0 = 0** 1 = 1
Lowest Alerting Line State Priority	lowAlertState	**0 = Disabled** 1 = Enabled
Divert Alerting Call	divertAlertingCall	0 = Disabled **1 = Enabled**
Allow Vibrate URI When On Call	vibrateURIOnCall	**0 = Disabled** 1 = Enabled
Customer Support Use	customerSupportUse	Up to 64 character string
Customer support upload URL	problemReportUploadURL	Up to 256 character string
Battery Lifetime Alert	batteryLifetimeAlert	**0 = Disabled** 1 = Enabled
Battery Lifetime Alert Interval	batteryLifetimeAlertInterval	**4 = 24 Months** 1 = 6 Months 2 = 12 Months 3 = 18 Months
Battery SN Reminder	batterySnReminder	**0 = Disabled** 1 = Enabled
CME Intercom to Application Button Mapping	thumbButton1	PTTH1 = Map to Line 1 PTTH2 = Map to Line 2 PTTH3 = Map to Line 3 PTTH4 = Map to Line 4 PTTH5 = Map to Line 5 PTTH6 = Map to Line 6

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

The **Application URL** configuration determines whether the **Application Button** will be configured as a service URL button or as a speed dial.
The **Application URL** can be configured to link to a Push To Talk server for quick access. (e.g. http://x.x.x.x:8085/PushToTalk/displayPhoneGroupsMenu.do?sep=#DEVICENAME#)
To configure the application button as a speed dial, enter in the format as **Dial:X** (e.g. Dial:911).

For more information on these features, see the **Cisco Wireless IP Phone 8821 Series Administration Guide** or the Cisco Wireless IP Phone 8821 Series Release Notes.

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-maintenance-guides-list.html

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html

Configuring the Cisco Wireless IP Phone 8821 and 8821-EX

Wi-Fi Profile Configuration

To configure the Wi-Fi settings on the Cisco Wireless IP Phone 8821 and 8821-EX, either use the desktop charger or default Wi-Fi profile to connect to a Cisco Unified Communications Manager, use the phone's admin webpage interface, or use the local user interface and keypad.

Automatic Provisioning

For automatic provisioning of the Wi-Fi Profiles, the Cisco Wireless IP Phone 8821 and 8821-EX needs to be connected to a network either while docked with a supported USB to Ethernet dongle connected in the back of the dock or using the default Wi-Fi settings (**SSID** = **cisco** and **Security Mode** = **None**), which has connectivity to the Cisco Unified Communications Manager.

The Voice VLAN feature is supported as of the 11.0(3) release, but was not in previous releases so the native VLAN was utilized.

The VLAN of the switch port in which the USB to Ethernet dongle is connected to (Voice VLAN if enabled) must have connectivity to the CUCM and that VLAN must offer DHCP option 150 pointing it to the CUCM.

Wired 802.1x authentication and DHCP snooping features are not supported when using the USB to Ethernet dongle, so need to ensure the switchport is configured properly.

Use of a supported USB to Ethernet dongle is for initial provisioning purposes only and not to convert the Cisco Wireless IP Phone 8821 or 8821-EX to a wired IP phone. Voice calls over Ethernet are not supported.

The following USB to Ethernet dongles are supported.

- Apple USB 2.0 Ethernet Adapter (www.apple.com)
- Belkin B2B048 USB 3.0 Gigabit Ethernet Adapter (www.belkin.com)
- D-Link DUB-E100 USB 2.0 Fast Ethernet Adapter (www.dlink.com)
- Linksys USB3GIG USB 3.0 Gigabit Ethernet Adapter (www.linksys.com)
- Linksys USB300M USB 2.0 Ethernet Adapter (www.linksys.com)

With connectivity to a Cisco Unified Communications Manager 10.0 or later, Wi-Fi profile configuration data can be downloaded and applied to the Cisco Wireless IP Phone 8821 and 8821-EX.

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

For more information, see the **Cisco Unified Communications Manager > Wireless LAN Profiles** section.

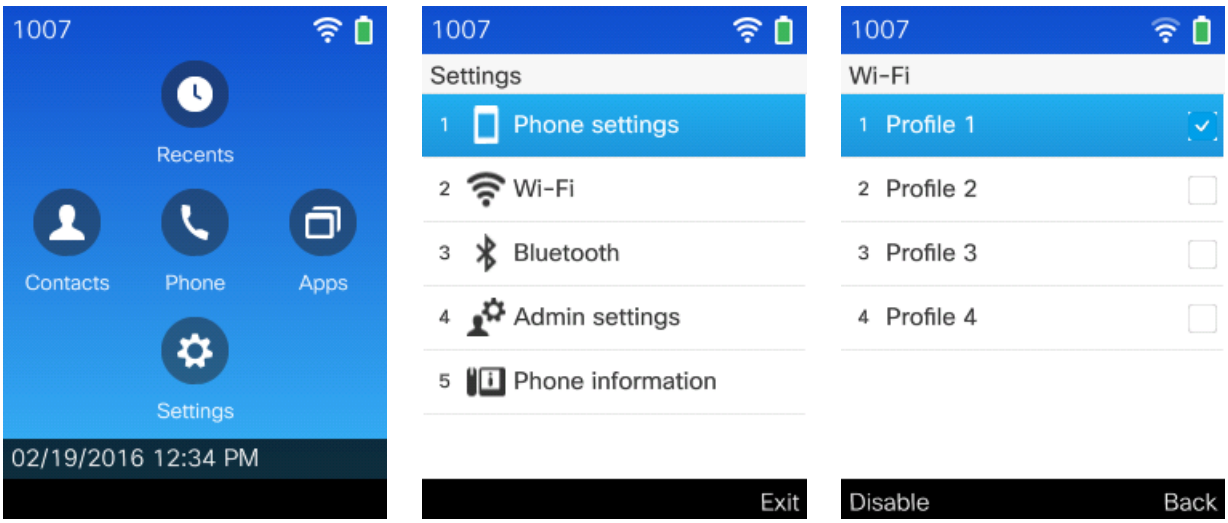
Certificates can also be automatically installed utilizing a network connection.

For more information, see the **Simplified Certificate Enrollment Protocol (SCEP)** section.

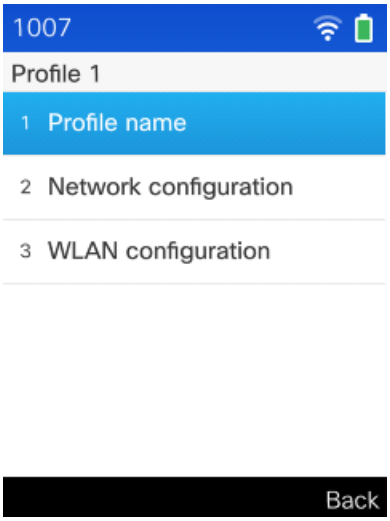
Local User Interface

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

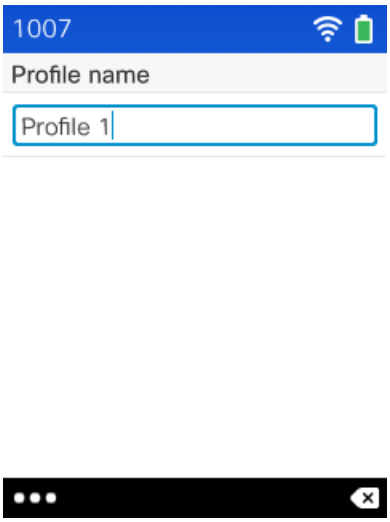
- Use the 5-way navigation button to navigate to **Settings** > **Wi-Fi**, then select the desired profile to configure.
- Up to 4 Wi-Fi profiles can be configured.



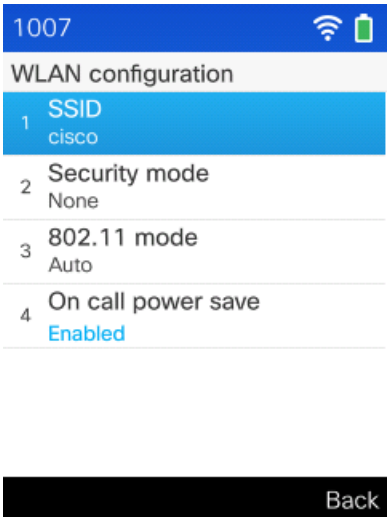
- Then select either **Profile name**, **Network configuration**, or **WLAN configuration** using the 5-way navigation button.



- **Profile name** configuration is optional, but if selected, then can enter a custom name.
- Select **Save** under **…** to save the changes or **Cancel** under **...** to dismiss the changes.
- Defaults to **Profile 1**, **Profile 2**, **Profile 3**, **Profile 4**.



- Select **WLAN configuration** to configure the WLAN parameters including **SSID**, **Security mode**, **802.11 mode**, and **On call power save**.
- Press the 5-way navigation's middle button to toggle an option and to enter edit mode.
- Only Profile 1 is **Enabled** by default.
- Only Profile 1's **SSID** defaults to **cisco**; others are null.
- All profiles default to **Security mode** = **None**, **802.11 mode** = **Auto**, and **On call power save** = **Enabled**.



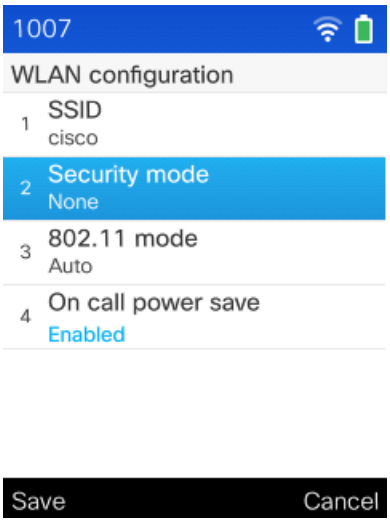
- Select **SSID** then enter the SSID for the desired WLAN.
- Select **Save** under **…** to save the changes or **Cancel** under **...** to dismiss the changes.

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

Security Mode	802.1x Type	Key Management	Encryption
None	N/A	None	None
WEP	N/A	Static	WEP
PSK	N/A	WPA2, WPA	AES, TKIP
EAP-FAST	EAP-FAST	WPA2, WPA	AES, TKIP
EAP-TLS	EAP-TLS	WPA2, WPA	AES, TKIP
PEAP-GTC	PEAP-GTC	WPA2, WPA	AES, TKIP

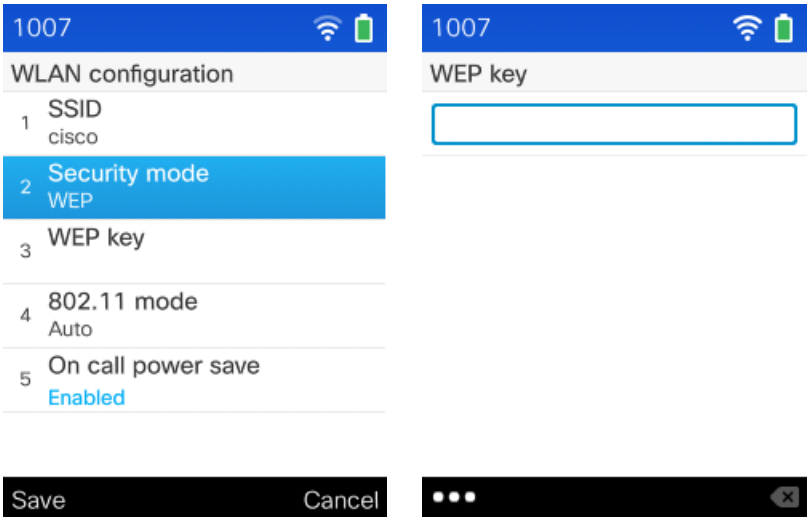
PEAP-MSCHAPv2	PEAP-MSCHAPv2	WPA2, WPA	AES, TKIP

- To utilize open security, set **Security mode** = **None**.
- Select **Save** to save the changes or **Cancel** to dismiss the changes.



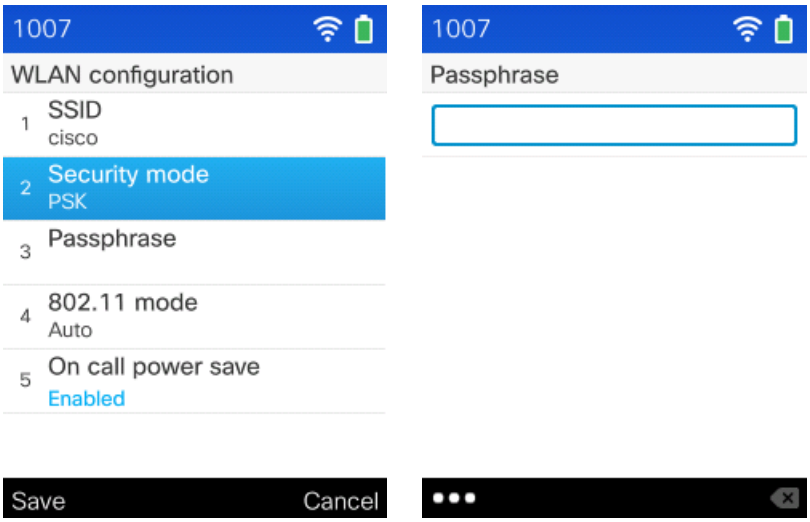
- To utilize WEP security, set **Security mode** = **WEP** then enter the 40/104 or 64/128 ASCII or HEX **WEP key**.
- Only key index 1 is supported, so will want to ensure that only key index 1 is configured on the access point.
- Select **Save** to save the changes or **Cancel** to dismiss the changes.

Key Style	Key Size	Characters
ASCII	40/64 bit	5
ASCII	104/128 bit	13
HEX	40/64 bit	10 (0-9, A-F)
HEX	104/128 bit	26 (0-9, A-F)

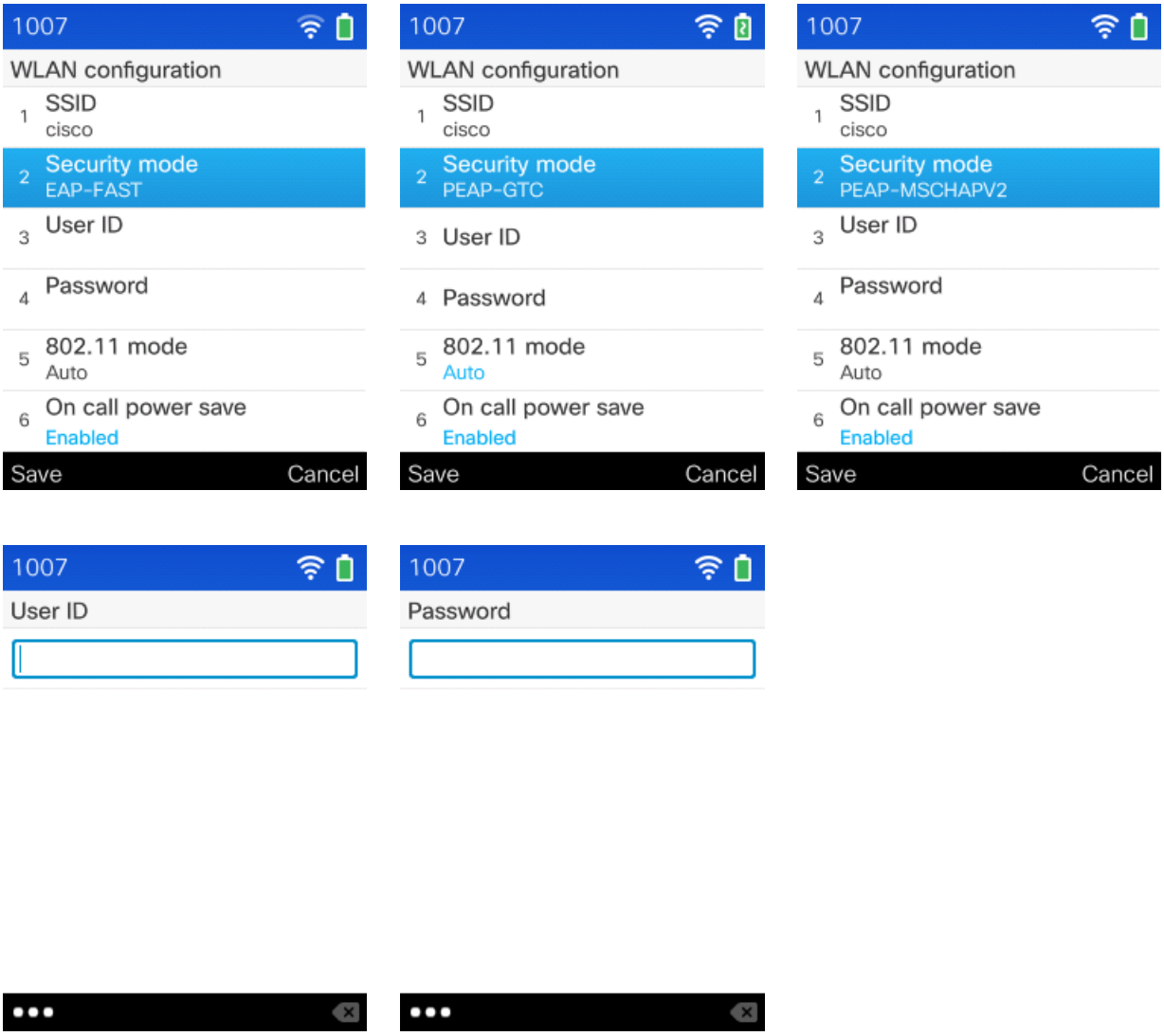


- To utilize **PSK** security, set **Security mode** = **PSK** then enter the 8-63 ASCII or 64 HEX **Passphrase**.
- Select **Save** to save the changes or **Cancel** to dismiss the changes.

Key Style	Characters
ASCII	8-63
HEX	64 (0-9,A-F)

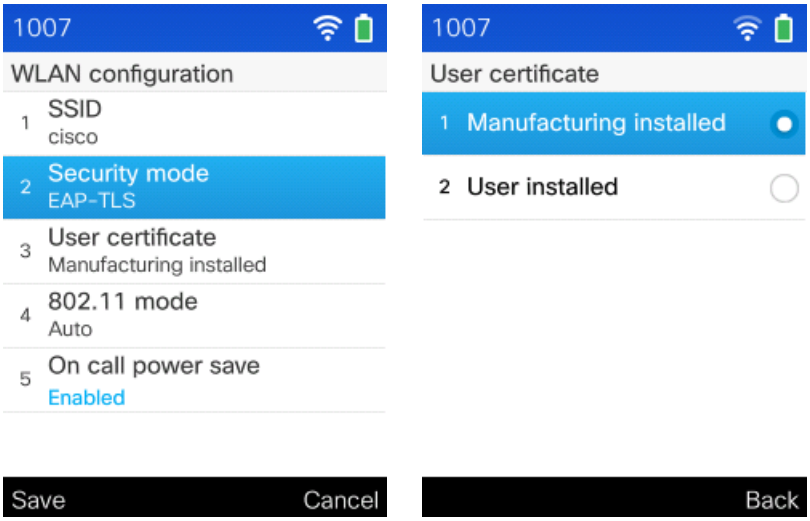


- To utilize **EAP-FAST**, **PEAP-GTC**, or **PEAP-MSCHAPv2**, set the **Security mode** accordingly, then the **User ID** and **Password** must be configured.
- The root CA certificate of the CA chain that issues the RADIUS server certificates can optionally be installed either via SCEP, manually via the admin webpage, or via TFTP download if wanting to enable server validation. Server validation is automatically enabled once a server certificate is installed.
- Select **Save** to save the changes or **Cancel** to dismiss the changes.

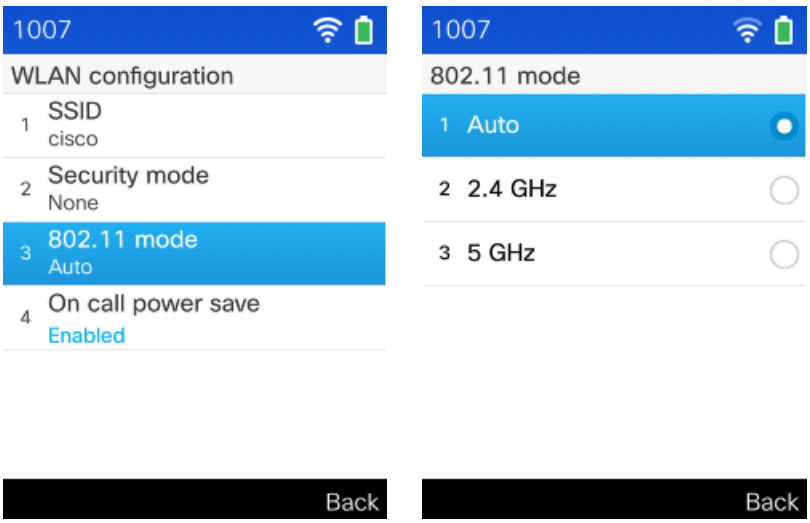


- If selecting EAP-TLS as the security mode, then must configure the type of user certificate to use.

  If **User installed** is selected, then will need to have a user certificate installed either manually via the admin webpage or via SCEP.
- Select **Save** to save the changes or **Cancel** to dismiss the changes.
- The root CA certificate of the CA chain that issues the RADIUS server certificates can optionally be installed to enable server validation when using EAP-TLS. Server validation is automatically enabled once a server certificate is installed.

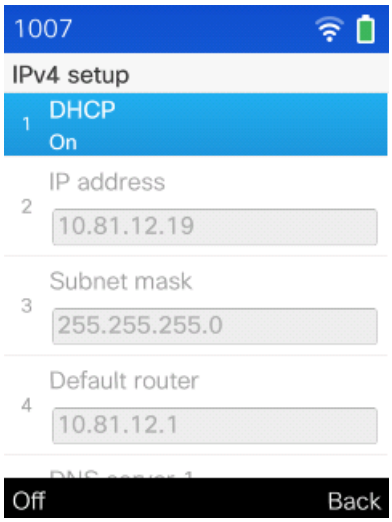


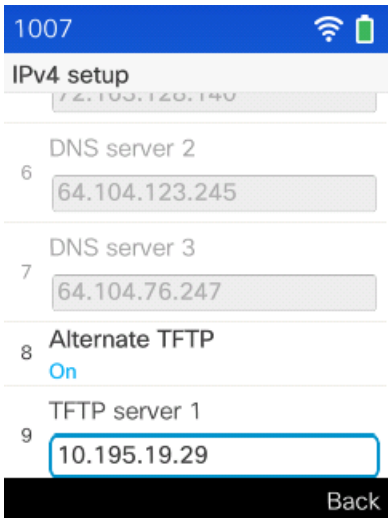
- Select one of the following 802.11 modes to set the frequency band, then **Save**.
  - Auto
  - 2.4 GHz
  - 5 GHz
- **Auto** mode (default mode) will scan both 2.4 GHz and 5 GHz channels, but will give preference to the 5 GHz frequency band.
- **2.4 GHz** mode will only scan 2.4 GHz channels and **5 GHz** mode will only scan 5 GHz channels, then will attempt to associate to an available access point.
- It is recommended to set the frequency band on the Cisco Wireless IP Phone 8821 and 8821-EX to 5 GHz when wanting to utilize the 5 GHz frequency band only, which prevents scanning and potentially roaming to the 2.4 GHz frequency band.
- Select **Save** to save the changes or **Cancel** to dismiss the changes.



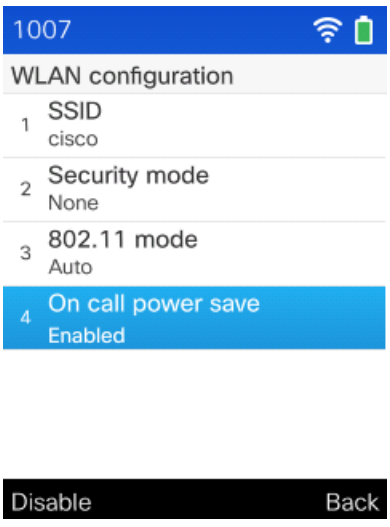
- If **Network configuration** is selected, then can configure IP settings including DHCP and Alternate TFTP.
- Press the 5-way navigation's middle button to toggle an option or to enter edit mode.
- If option 150 or 66 is not configured to provide the TFTP Server's IP address via the network's DHCP scope, then set **Alternate TFTP** to **On** and enter the IP address for the TFTP Server.

- Select **Save** to save the changes or **Cancel** to dismiss the changes.
- Ensure to select **Erase** if prompted, when configuring Alternate TFTP.

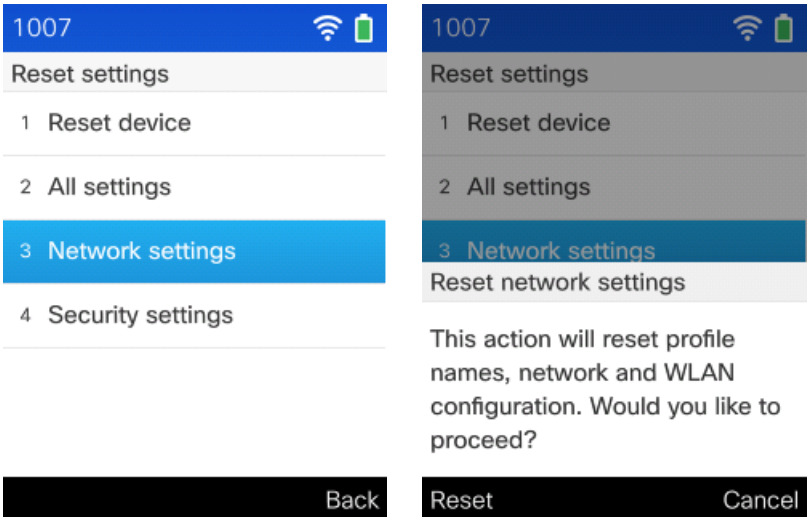




- **On call power save** defaults to **Enabled**.
- When **Enabled**, the phone will utilize U-APSD when on call.
- This parameter does not alter power save when in idle as the phone will always utilize U-APSD when not on call.
- **On call power save** should only be set to **Disabled** if required for troubleshooting purposes.
- Select **Save** to save the changes or **Cancel** to dismiss the changes.



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



Note: 802.11r (FT) or CCKM will be negotiated if enabled on the access point when using EAP-FAST, EAP-TLS, PEAP-GTC, or PEAP-MSCHAPv2, where preference is given to 802.11r (FT).

The access point must support AES (CCMP128) as TKIP can only be used as the broadcast/multicast cipher.

WPA3 is not supported.

802.1x-SHA2 key management is not supported.

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

WEP128 is listed as WEP104 on the Cisco Wireless LAN Controllers.

For more information, refer to the **Cisco Wireless IP Phone 8821 Series Administration Guide** at this URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-maintenance-guides-list.html

Admin Webpage

The admin webpage interface for the Cisco Wireless IP Phone 8821 and 8821-EX can be accessed via Wi-Fi or USB.

- For the Wi-Fi method, the phone is defaulted with SSID = cisco and Security Mode = None.
- For the USB method, ensure the phone is connecting to a Windows 7, 8, 10 or Mac OS X computer.
  A driver is not required for Windows but is required for Mac OS X (http://joshuawise.com/horndis).
  Then set a static IP address for the network interface created on the computer (e.g. 192.168.1.101 /24 as the phone uses 192.168.1.100 /24).

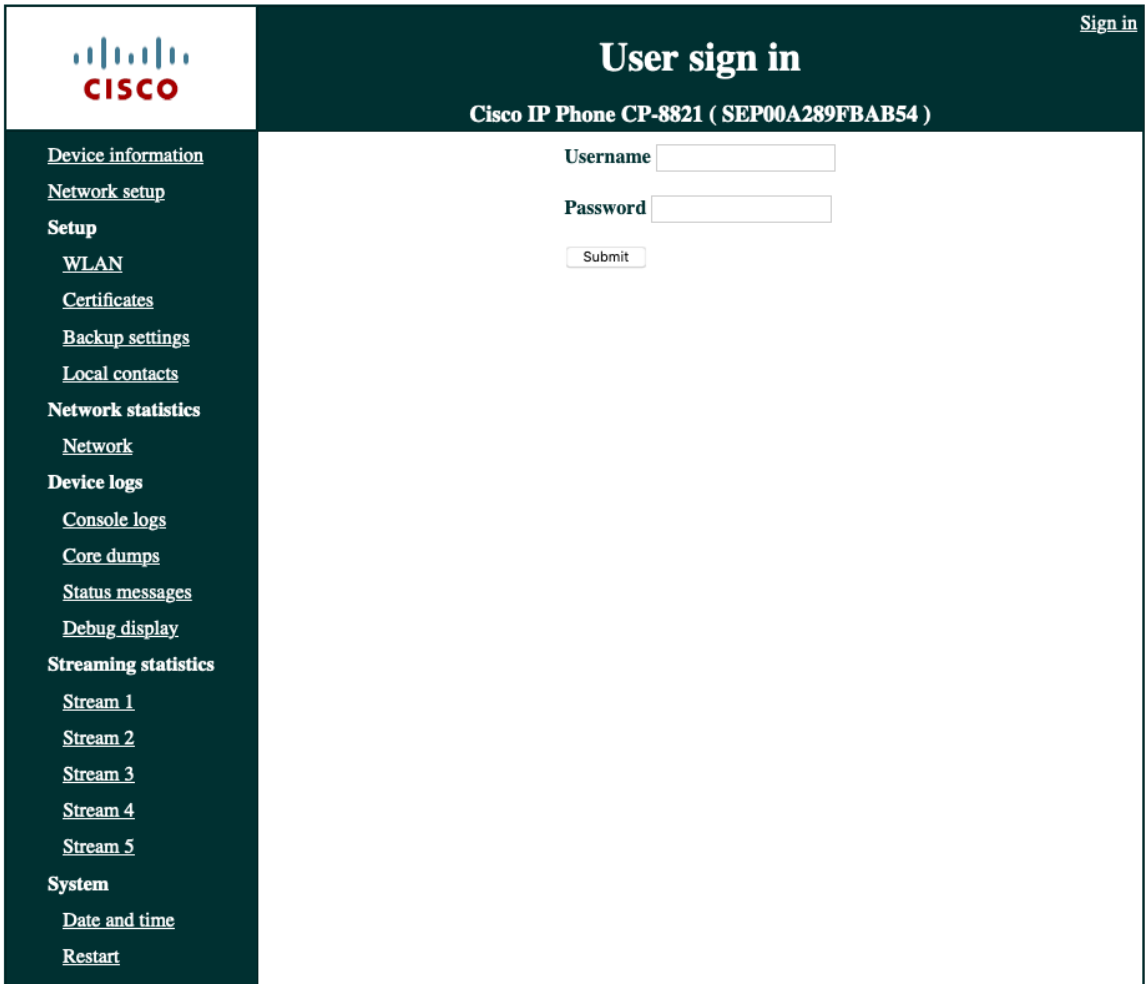
Use the following guidelines to configure the Wi-Fi Profiles via the phone's admin webpage interface.

- Browse to https://x.x.x.x:8443 when **Web Admin** is **Enabled** and **Admin Password** has been defined.

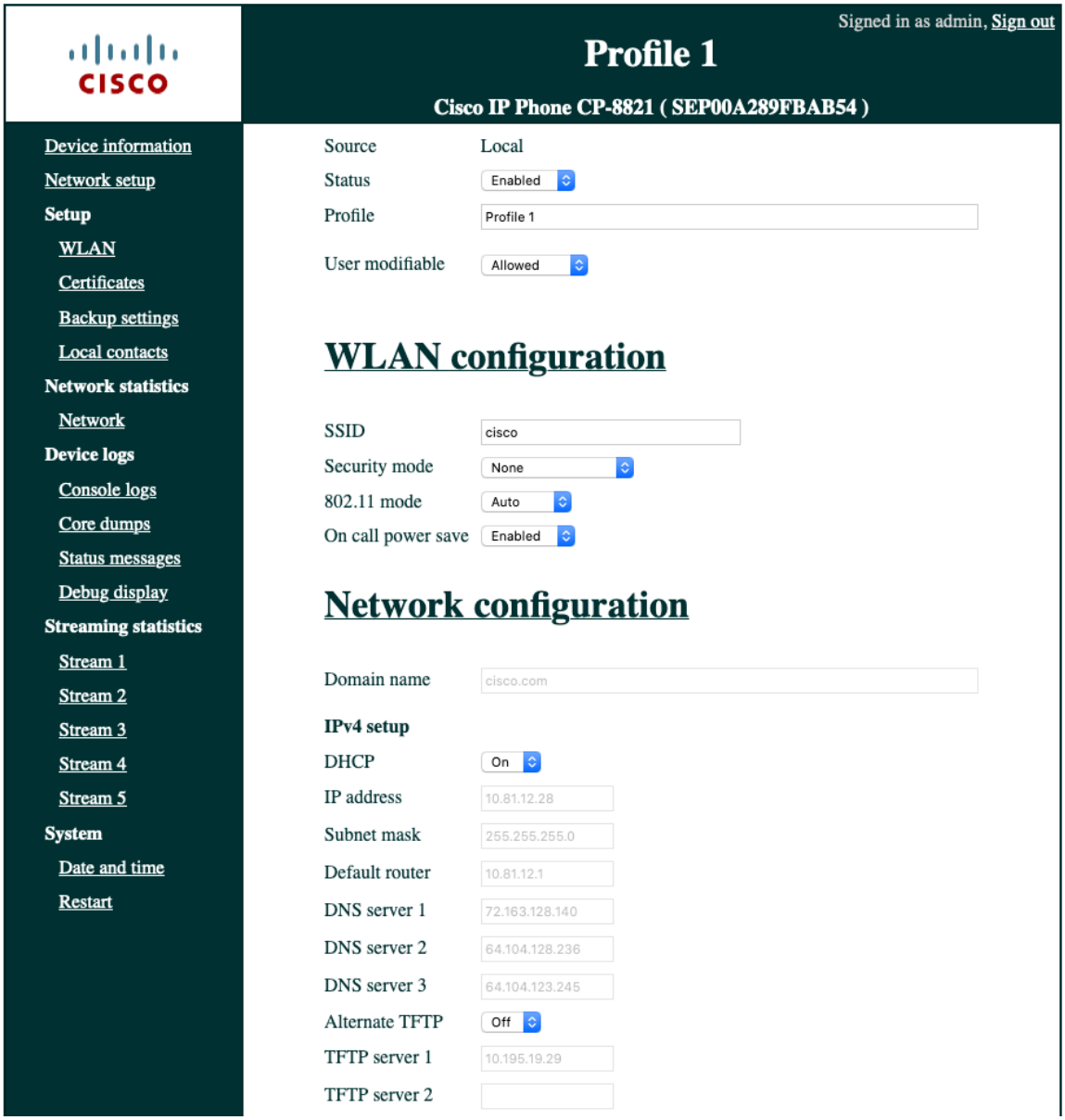
  For out of box / factory reset, **Web Admin** is enabled temporarily, but may get disabled once the phone registers to Cisco Unified Communications Manager as Web Admin is Disabled by default in Cisco Unified Communications Manager.

- Enter **admin** as the **Username** and the string defined for the **Admin Password** for **Password**, then select Submit.

  For out of box / factory reset, the **Admin Password** is temporarily set to **Cisco**.



- To create a configuration file to be used for all Cisco Wireless IP Phone 8821 and 8821-EX, browse to the admin webpage of the out of box or factory defaulted Cisco Wireless IP Phone 8821 or 8821-EX.
- Select **WLAN** menu option then configure the necessary profiles where the SSID, 802.11 Mode, Security Mode, etc. must be specified.
- For EAP-TLS, the **User Certificate** can be set to **User Installed** or **Manufacturing Installed** (will be defaulted to **Manufacturing Installed**).
- For PEAP with Server Validation or EAP-TLS, upload the **Server (Root CA) Certificate**.
- The **Server (Root CA) Certificate** does not need to be configured at the WLAN Profile level.



- Once the Wi-Fi Profile configuration is complete, the configuration can be exported by selecting **Backup Settings** menu option.
- Prior to selecting **Export**, enter an **Encryption Key** (8-127characters) to encrypt the export template.
- Save the file to the local PC after selecting **Export** for later use.
- Any pre-existing **Server (Root CA) Certificates** will be included in the exported configuration.

- To apply the exported configuration file, select **Backup Settings** on the phone's admin webpage.
- Prior to selecting **Import**, browse to the template to be applied and enter the **Encryption Key** that was specified during the template export process previously.
- The Cisco Wireless IP Phone 8821 and 8821-EX will need to be restarted after the template is uploaded.

Bulk Deployment Utility

The Bulk Deployment Utility (BDU) for the Cisco Wireless IP Phone 8821 and 8821-EX can be utilized for initial deployment or after the phones have been deployed.

The BDU provides quick provisioning and deployment when unique 802.1x accounts are used with EAP-FAST, PEAP-GTC, or PEAP-MSCHAPV2 or when a common set of credentials are used by all phones (e.g. PSK or a single 802.1x account).

A personal computer running Microsoft Windows or Apple OS X with Java installed is required. Java can be downloaded at https://java.com/en/download.

The BDU requires firmware version 11.0(3)SR4 or later for the Cisco Wireless IP Phone 8821 Series.

The BDU does not support certificate provisioning, however the phones can download certificates via Simple Certificate Enrollment Protocol (SCEP) or be manually installed via the phone's admin webpage interface (https://x.x.x.x:8443), where x.x.x.x is the IP address of the phone. You can also place a Root CA certificate on the TFTP Server (named **WLANRootCA.cer**), which automatically downloads to the phone.

Create Wi-Fi Profiles

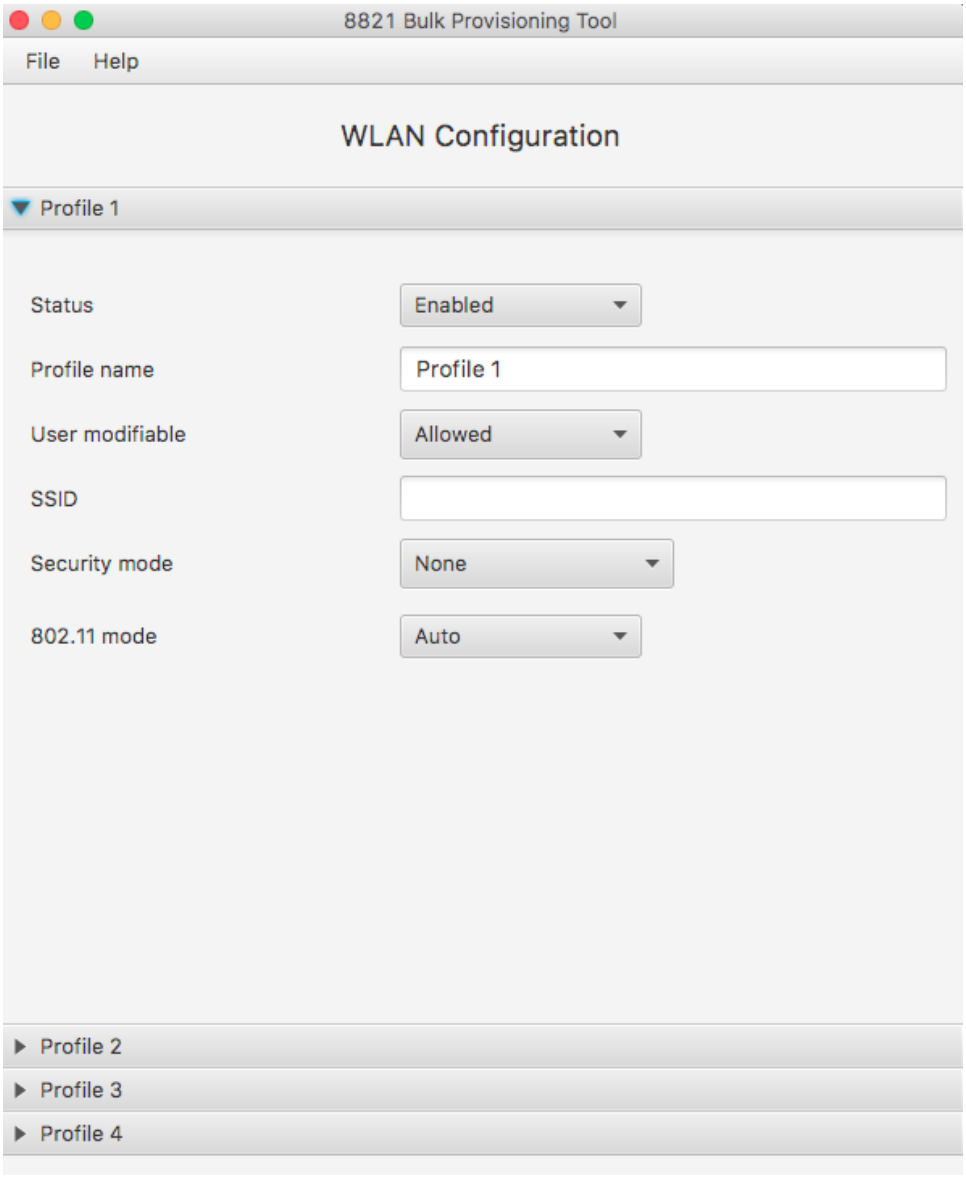
Once **882xBD.1-0.jar** is downloaded from Cisco.com, double-click the file to launch the BDU.

Prior to exporting TFTP downloadable configuration file(s), the Wireless LAN configuration parameters must be specified.

1. Configure the **Status** per Wi-Fi profile as necessary.
    - **Enabled** (Profile 1 is enabled by default)
    - **Disabled** (Profiles 2-4 are disabled by default)
2. Configure the **Profile name** per Wi-Fi profile as necessary.
    - A string with up to 32 characters is allowed.
3. Configure **User modifiable** per Wi-Fi profile as necessary.
    - **Allowed** = The user has the capability to change any Wireless LAN settings (e.g. Enable/Disable, SSID, Frequency Band, Authentication Method, Username and Password, PSK Passphrase, WEP Key) locally on the endpoint.

- **Disallowed** = The user is unable to change any Wireless LAN settings.
- **Restricted** = The user is only able to change certain Wireless LAN settings (e.g. User ID and Password)

4. Configure the **SSID** per Wi-Fi profile as necessary.
   - A string with up to 32 characters is allowed.
5. Configure the **Security mode** per Wi-Fi profile as necessary.
   - **None**
   - **WEP**
     - Requires **WEP key** to be entered.
   - **PSK**
     - Requires **Passphrase** to be entered.
   - **EAP-FAST**
     - Requires **User ID** and **Password** to be populated either automatically via CSV file or manually.
     - Check **Provide shared credentials** to manually specify the **User ID** and **Password**.
     - Uncheck **Provide shared credentials** to use a CSV file to specify the **User ID** and **Password**.
   - **EAP-TLS**
     - Requires **User certificate** to be set to either **Manufacturing installed** or **User installed**.
   - **PEAP-GTC**
     - Requires **User ID** and **Password** to be populated either automatically via CSV file or manually.
     - Check **Provide shared credentials** to manually specify the **User ID** and **Password**.
     - Uncheck **Provide shared credentials** to use a CSV file to specify the **User ID** and **Password**.
   - **PEAP-MSCHAPV2**
     - Requires **User ID** and **Password** to be populated either automatically via CSV file or manually.
     - Check **Provide shared credentials** to manually specify the **User ID** and **Password**.
     - Uncheck **Provide shared credentials** to use a CSV file to specify the **User ID** and **Password**.
6. Configure the **802.11 mode** per Wi-Fi profile as necessary.
   - **Auto** = Gives priority to 5 GHz frequencies over 2.4 GHz frequencies.
   - **2.4 GHz** = Uses 2.4 GHz frequencies only.
   - **5 GHz** = Uses 5 GHz frequencies only.



Note: If you plan to use unique 802.1x accounts with the Bulk Export method, the username and password do not need to be specified; they will be specified in the CSV file.

The BDU does not support static IP addresses, therefore DHCP (including TFTP) is used.

Export Configuration Files

Once the Wireless LAN configuration parameters are specified, then the TFTP downloadable configuration file(s) can be exported by selecting **File** > **Export** from the BDU.

There are two methods for exporting configuration files (**Bulk Export** and **Default Export**), which is auto-determined based on the selected security mode and whether unique credentials are specified or not.

If you need to deploy the phones with unique 802.1x accounts utilizing EAP-FAST, PEAP-GTC, or PEAP-MSCHAPV2, then the **Bulk Export** method is selected automatically.

If you need to deploy the phones with identical wireless LAN settings (e.g. None, WEP, PSK, EAP-TLS, or single user account with EAP-FAST, PEAP-GTC, PEAP-MSCHAPV2), then the **Default Export** method is selected automatically.

Bulk Export

The Bulk Export method uses the common Wireless LAN configuration parameters specified when creating the template, and prompt for a CSV file, which will contain the phone MAC address, username, and password.

A sample CSV file (**userinfo.csv**), available at **Help > Userinfo template export**, can be used as a template.

Below is the file format for the **userinfo.csv** file.

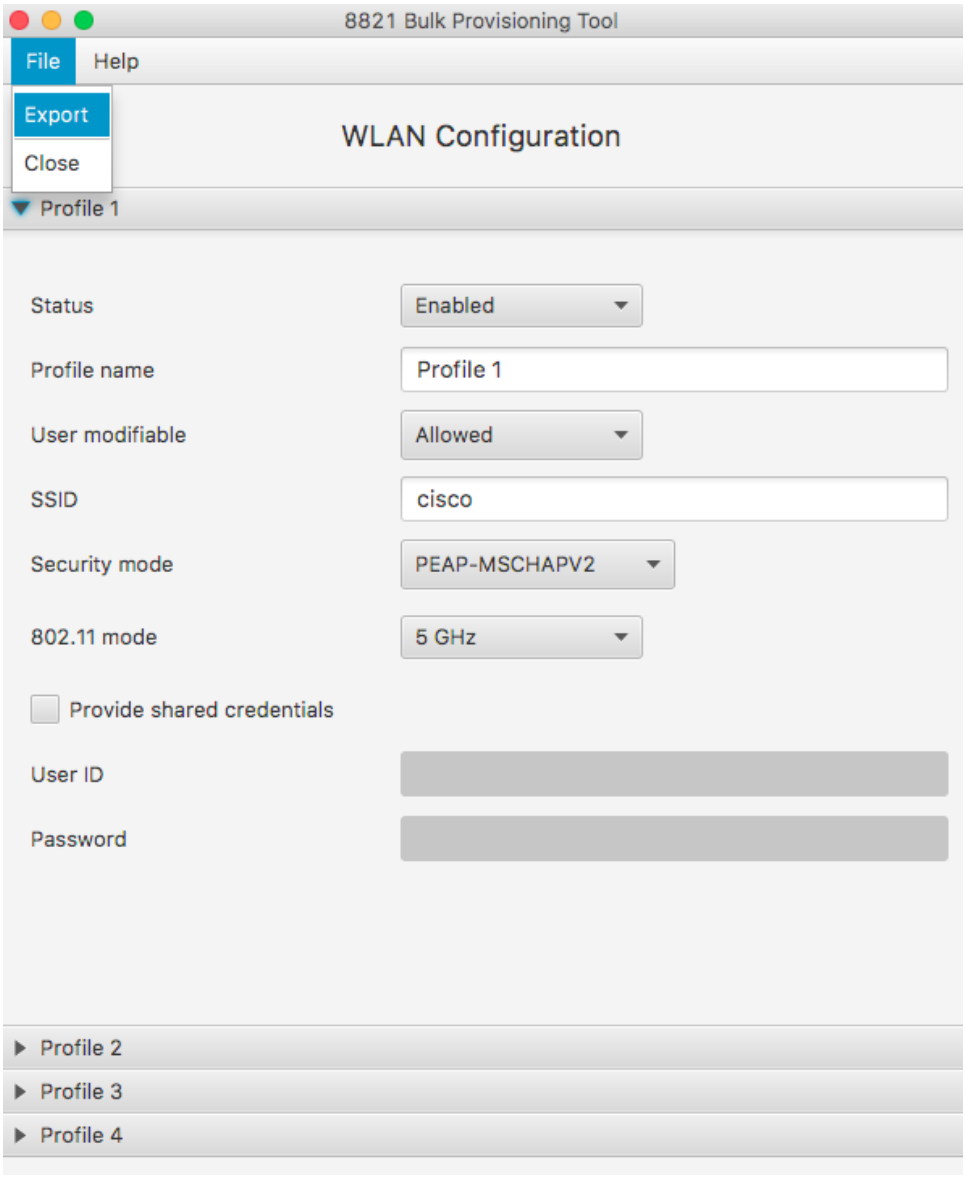
MAC,Username,Password

00EBD5DB019C,Joe,Lee

Up to 5,000 entries are supported per CSV file.

After the CSV file is imported, TFTP downloadable configuration files for each phone are automatically created and exported to the location specified.

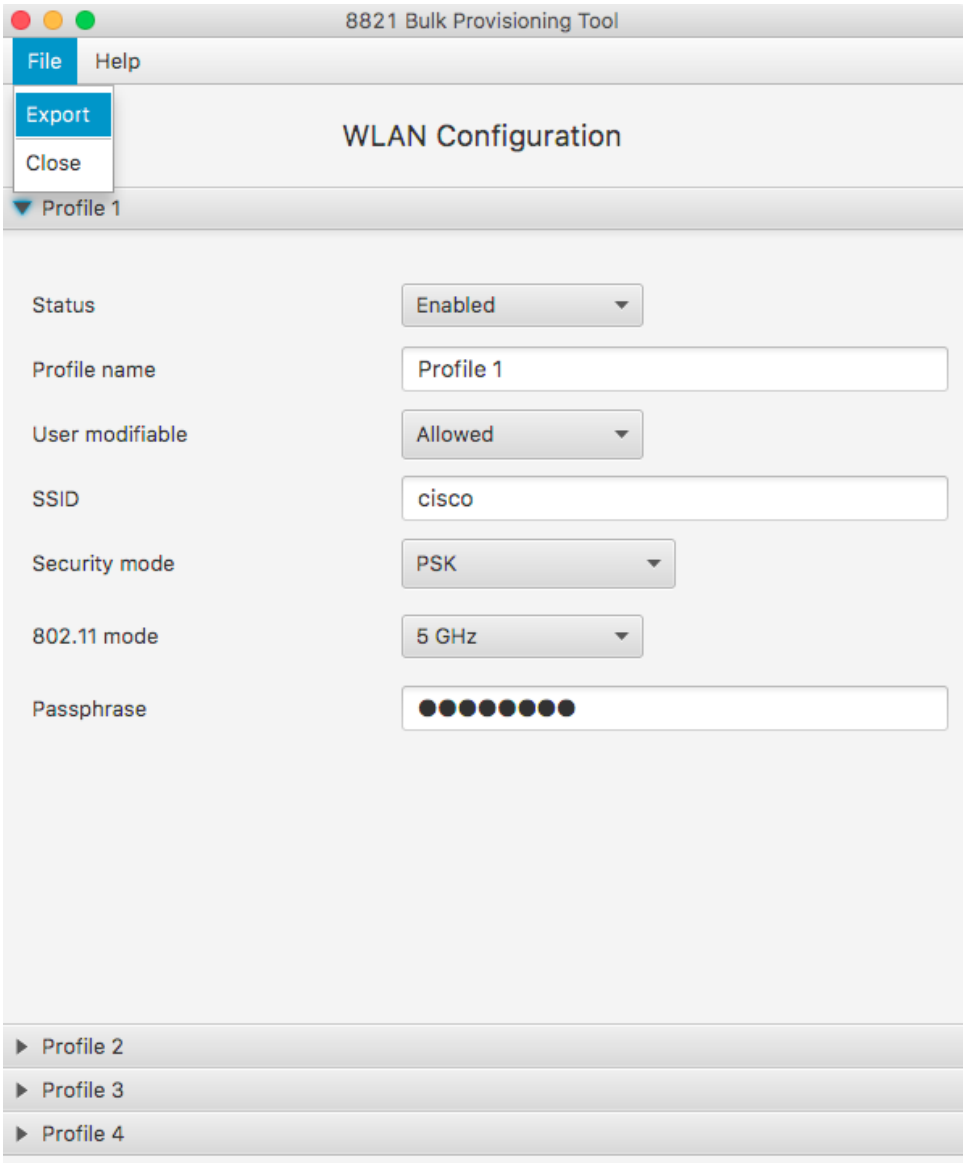
The exported file names are in the format of **8821-WLAN<MAC>.xml**, which the phone attempts to TFTP download when the phone is powered on or re-provisions.

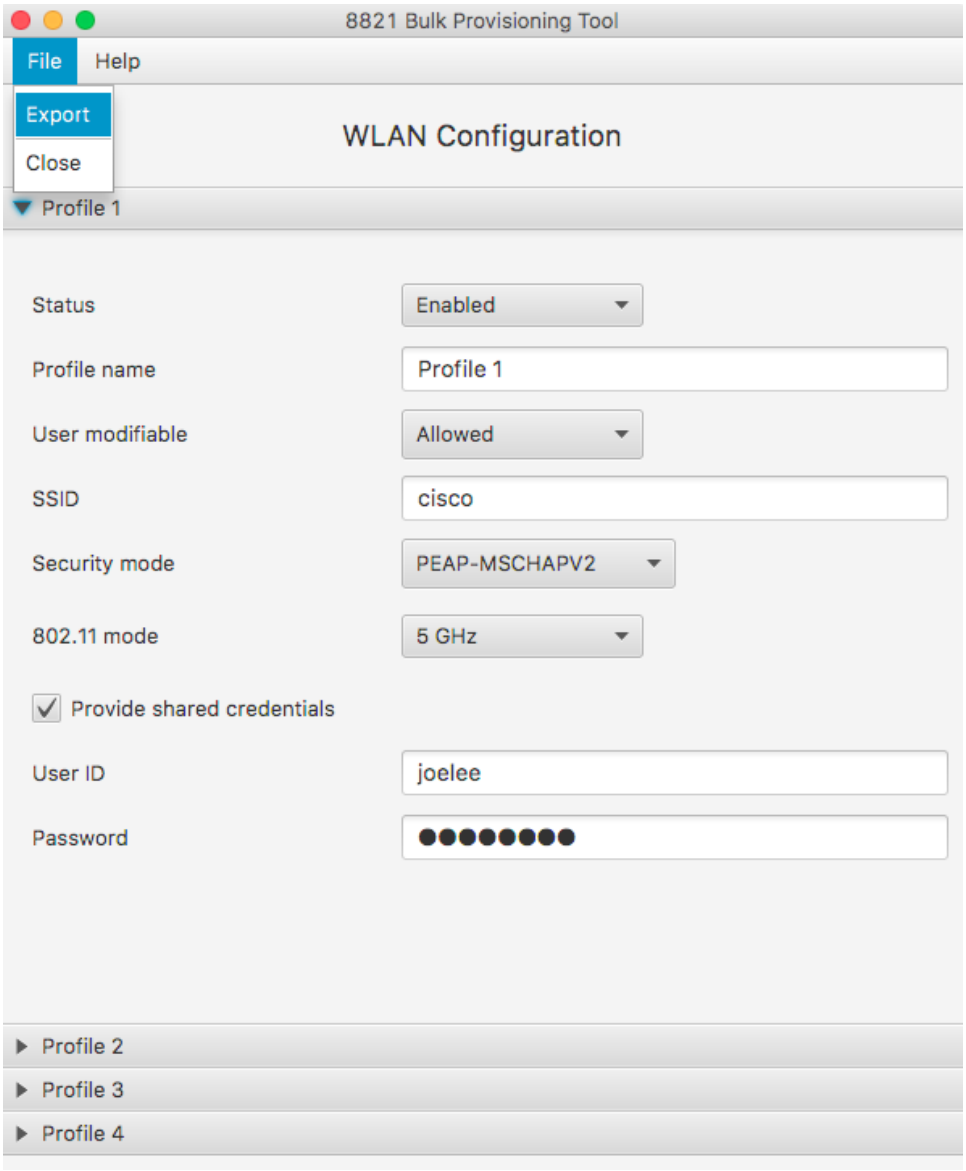


Default Export

The Default Export method uses the common Wireless LAN configuration parameters specified when creating the template and a TFTP downloadable configuration file will be automatically created and exported to the location specified.

The exported file name will be **8821-WLANDefault.xml**, which the phone attempts to TFTP download when the phone is powered on or re-provisions.


8821 Bulk Provisioning Tool
File
Help
Export
Close
WLAN Configuration
Profile 1
Status
Enabled
Profile name
Profile 1
User modifiable
Allowed
SSID
cisco
Security mode
PSK
802.11 mode
5 GHz
Passphrase
Profile 2
Profile 3
Profile 4



Push Configuration Files to the Cisco 8821 and 8821-EX

The BDU does not have TFTP server capabilities, therefore either the TFTP server on Cisco Unified Communications Manager / Cisco Unified Communications Manager Express or a third-party TFTP server will be required to host the phone configuration files once exported.

For initial deployment, use one of the following methods:

- Connect the phone to an Ethernet network while docked with a supported USB to Ethernet dongle connected to obtain IP settings via DHCP (including TFTP server) where the phone can TFTP download the phone configuration file.
- Connect the phone to a wireless LAN using the default SSID (cisco) to obtain IP settings via DHCP (including TFTP server) where the phone can TFTP download the phone configuration file.

For post-deployment, where phones are already being utilized on the production wireless LAN, copy the phone configuration files to the TFTP server that the phones are pointed to, then reset the phones to reconnect to the production wireless LAN. The phone then attempts to TFTP download the phone configuration file. The TFTP service may need to be restarted prior to resetting the phones depending on which type of TFTP server is utilized.

After the phone receives the configuration file, the phone will re-provision with the new settings and attempt to join the intended wireless LAN.

If currently docked with an active USB to Ethernet connection, the phone attempts to join the wireless LAN once undocked.

Certificate Management

The Cisco Wireless IP Phone 8821 and 8821-EX can utilize X.509 digital certificates for EAP-TLS or to enable Server Validation when using PEAP-GTC or PEAP-MSCHAPV2.

A User Certificate can be installed either automatically via Simple Certificate Enrollment Protocol (SCEP) or manually via the phone's admin webpage interface (https://x.x.x.x:8443).

A Server Certificate can be installed either automatically via Simple Certificate Enrollment Protocol (SCEP), manually via the phone's admin webpage interface (https://x.x.x.x:8443), or via TFTP download.

The TFTP download method can help when the RADIUS servers are issued certificates from a different CA chain than the CA chain used for issuing client certificates or if wanting to quickly enable Server Validation for PEAP.

To install a Server Certificate via the TFTP download method, rename the Root CA certificate to **WLANRootCA.cer** then copy it to the CUCM TFTP servers and restart the TFTP service for those CUCM servers.

Only 1 user certificate is allowed and up to 3 server certificates (1 per installed method; SCEP, manual, TFTP) are allowed.

Once a certificate is installed, Server Validation is automatically enabled if configured for EAP-TLS, PEAP-GTC, or PEAP-MSCHAPV2.

Microsoft® Certificate Authority (CA) servers are recommended. Other CA server types may not be completely interoperable with the Cisco Wireless IP Phone 8821 and 8821-EX.

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.

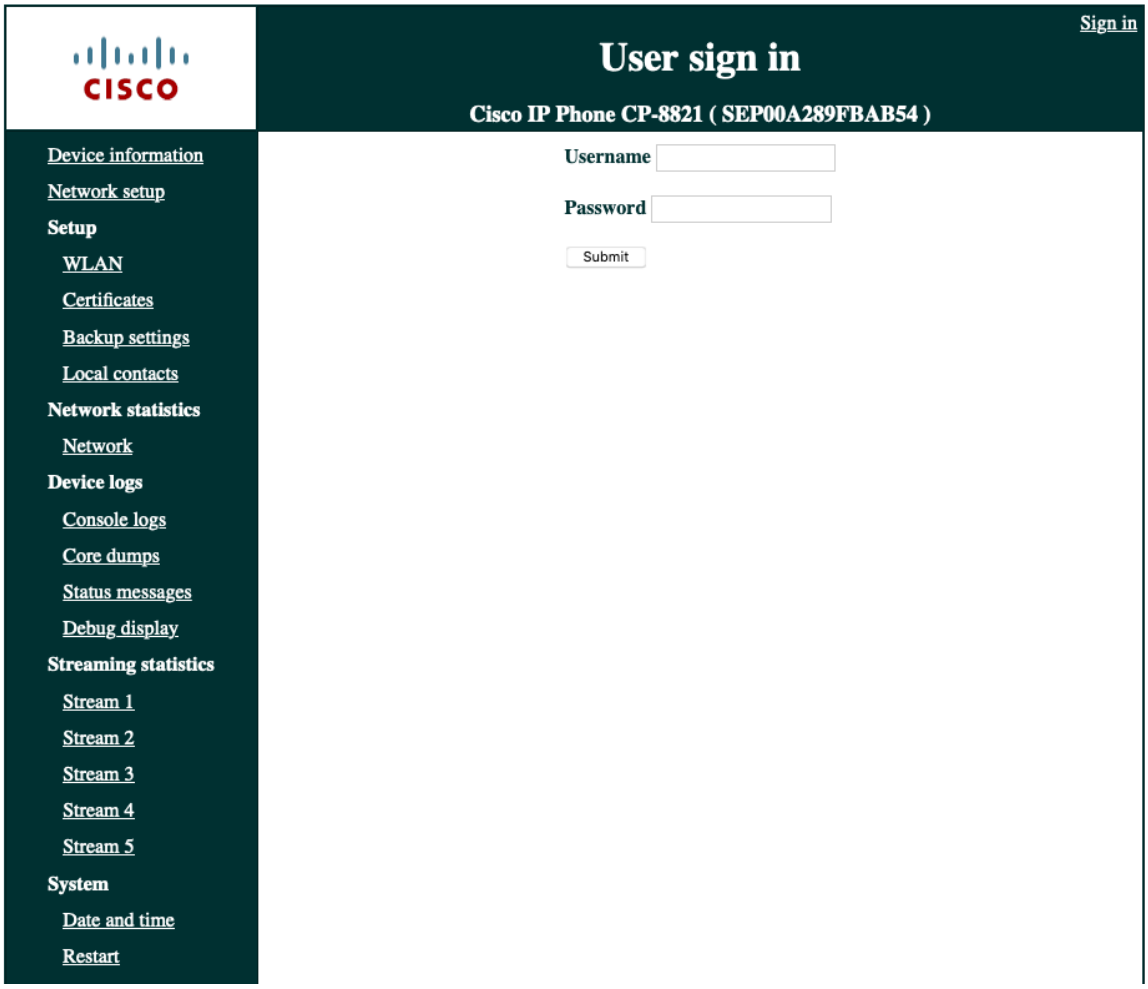
Ensure Client Authentication is listed in the Enhanced Key Usage section of the user certificate details.

Manual Installation

For out of box (factory reset) manual installation, the admin webpage interface is **Enabled**, the username is fixed to **admin**, and the password is temporarily set to **Cisco**.

The temporary password will no longer be available once the phone registers to Cisco Unified Communications Manager.

The admin webpage interface will be **Disabled** on the phone once it registers to Cisco Unified Communications Manager regardless if it contains support for the **Web Admin** and **Admin Password** options.



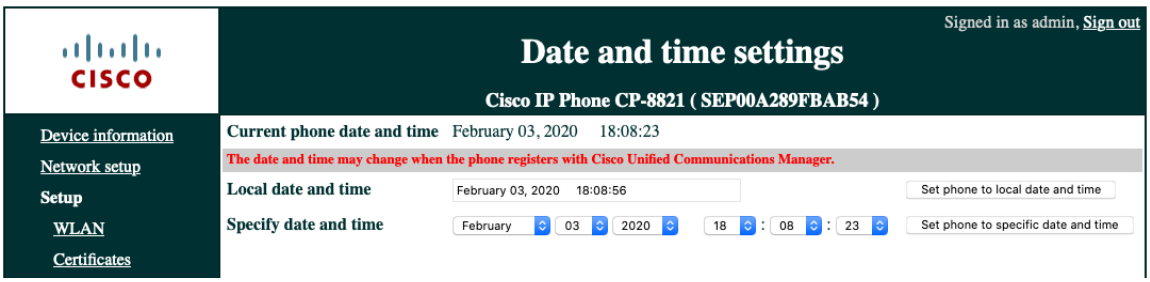
Once the phone has registered to CUCM, set **Web Admin** to **Enabled** in CUCM to enable the admin webpage interface.

Then configure **Admin Password** by specifying a 8-127 character string.

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

For out of box (factory reset), will need to ensure the date and time is configured correctly.

Can set the **Date and time** by syncing to the local machine or setting the **Date and time** manually.



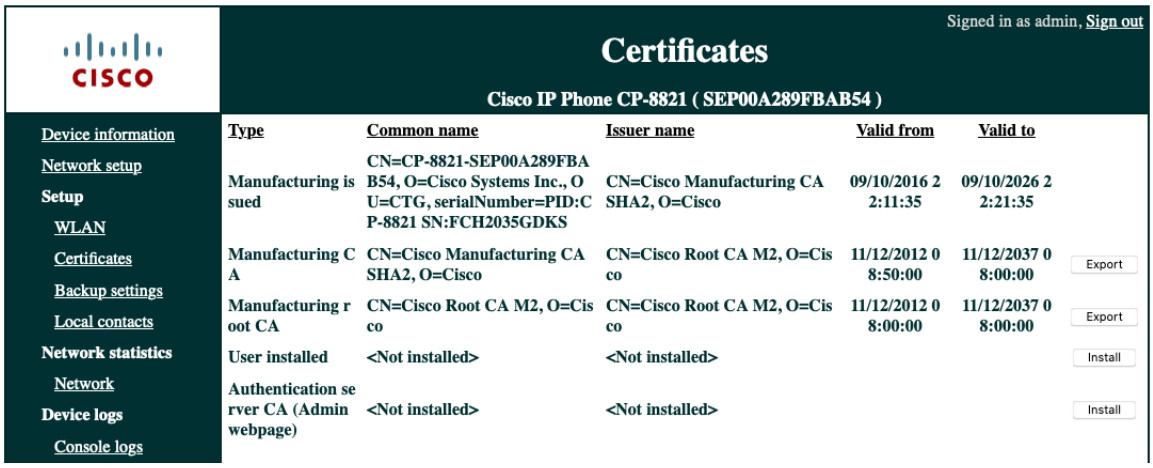
Can utilize either the internal Manufacturing Installed Certificate (MIC) or a custom User Installed certificate to be used as the User Certificate for EAP-TLS.

Manufacturing Installed Certificate (MIC)

The pre-installed Manufacturing Installed Certificate (MIC) can be used as the **User Certificate** for **EAP-TLS**.

The MIC's CA chain must be exported and added to the RADIUS server's trust list if wanting to use the **MIC** as the **User Certificate** for **EAP-TLS**.

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



User Installed Certificate

To manually install a user certificate for **EAP-TLS**, select **Install** for **User Installed** on the main certificates webpage.

Select **Browse** to point to the user certificate in **PKCS #12** format (.p12 or .pfx).

Enter the **Extract password**, then select **Upload**.

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

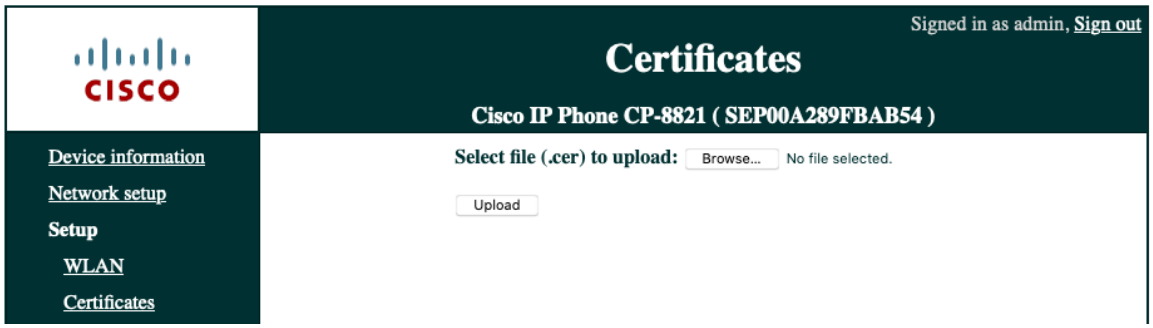
Will need to restart the Cisco Wireless IP Phone 8821 or 8821-EX after all certificates are installed.

Server Certificate

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

To manually install a server certificate, select **Install** for **Authentication Server CA** on the main certificates webpage.

Select **Browse** to point to the server certificate with **PEM (Base-64)** or **DER** encoding.



Will need to restart the Cisco Wireless IP Phone 8821 or 8821-EX after all certificates are installed.

Simple Certificate Enrollment Protocol (SCEP)

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

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

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

For initial certificate enrollment via SCEP, the Cisco Wireless IP Phone 8821 and 8821-EX needs to be connected to a network either while docked with a supported USB to Ethernet dongle connected in the back of the dock or using the default Wi-Fi settings (i.e. SSID = cisco and Security Mode = None), which has connectivity to the Cisco Unified Communications Manager.

Use of a supported USB to Ethernet dongle for initial provisioning purposes only and not to convert the Cisco Wireless IP Phone 8821 or 8821-EX to a wired IP phone.

The following USB to Ethernet dongles are supported.

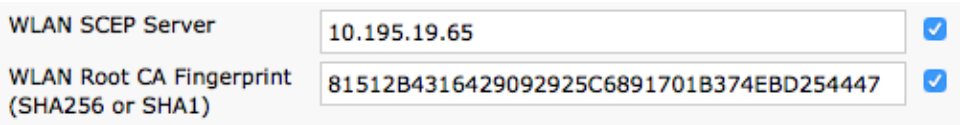
- Apple USB 2.0 Ethernet Adapter (www.apple.com)
- Belkin B2B048 USB 3.0 Gigabit Ethernet Adapter (www.belkin.com)
- D-Link DUB-E100 USB 2.0 Fast Ethernet Adapter (www.dlink.com)
- Linksys USB3GIG USB 3.0 Gigabit Ethernet Adapter (www.linksys.com)
- Linksys USB300M USB 2.0 Ethernet Adapter (www.linksys.com)

The Cisco Wireless IP Phone 8821 and 8821-EX utilize the following parameters defined in Cisco Unified Communications Manager for SCEP requests.

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

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

Removing these parameters will disable SCEP.



The Cisco Wireless IP Phone 8821 and 8821-EX then sends a SCEP enroll request to the SCEP RA including the phone's Manufacturing Installed Certificate (MIC) as the Proof of Identity (POI).

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

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

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

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

The Cisco Wireless IP Phone 8821 and 8821-EX will periodically check the user and server certificate expiration periods.

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

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

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

If the **WLAN SCEP Server** or **WLAN Root CA Fingerprint (SHA256 or SHA1)** has been modified, then the Cisco Wireless IP Phone 8821 and 8821-EX will attempt to update the CA and user certs immediately.

Certificate Authority (CA) Configuration

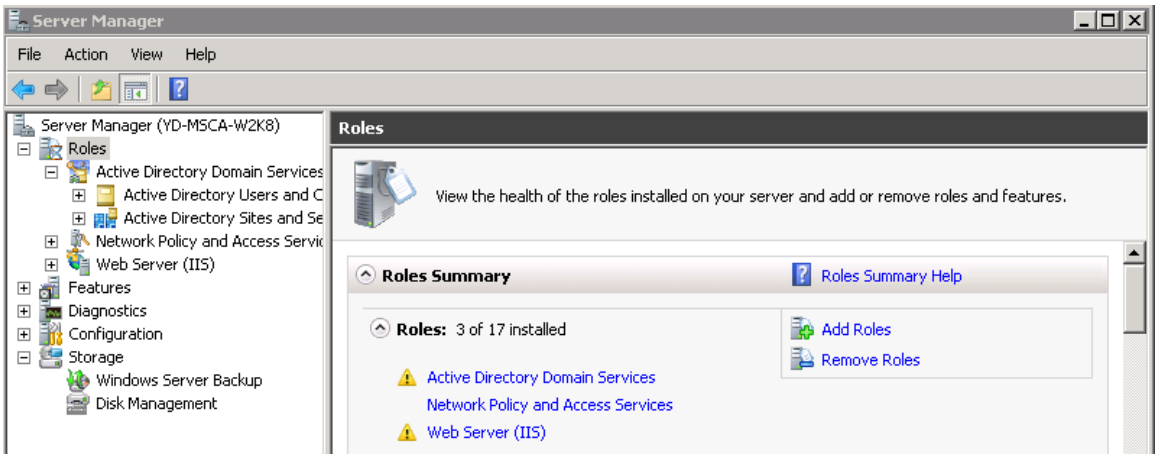
Is recommended to use Microsoft® Certificate Authority (CA) servers.

Use the following guidelines to configure the Microsoft CA.

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

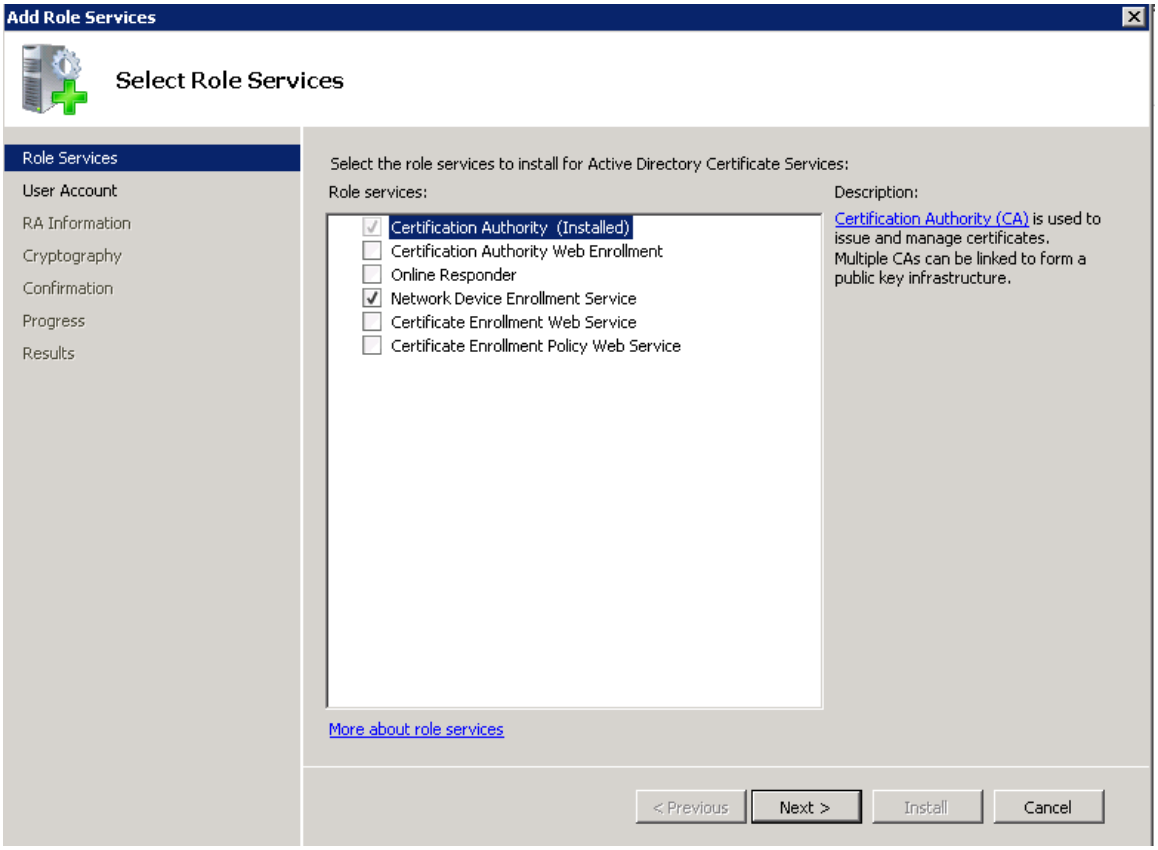
- Make **Administrator** a member of **IIS_IUSERS** group by going to **MemberOf** tab of user property screen.

- Launch **Server Manager**, then click **Add roles**.



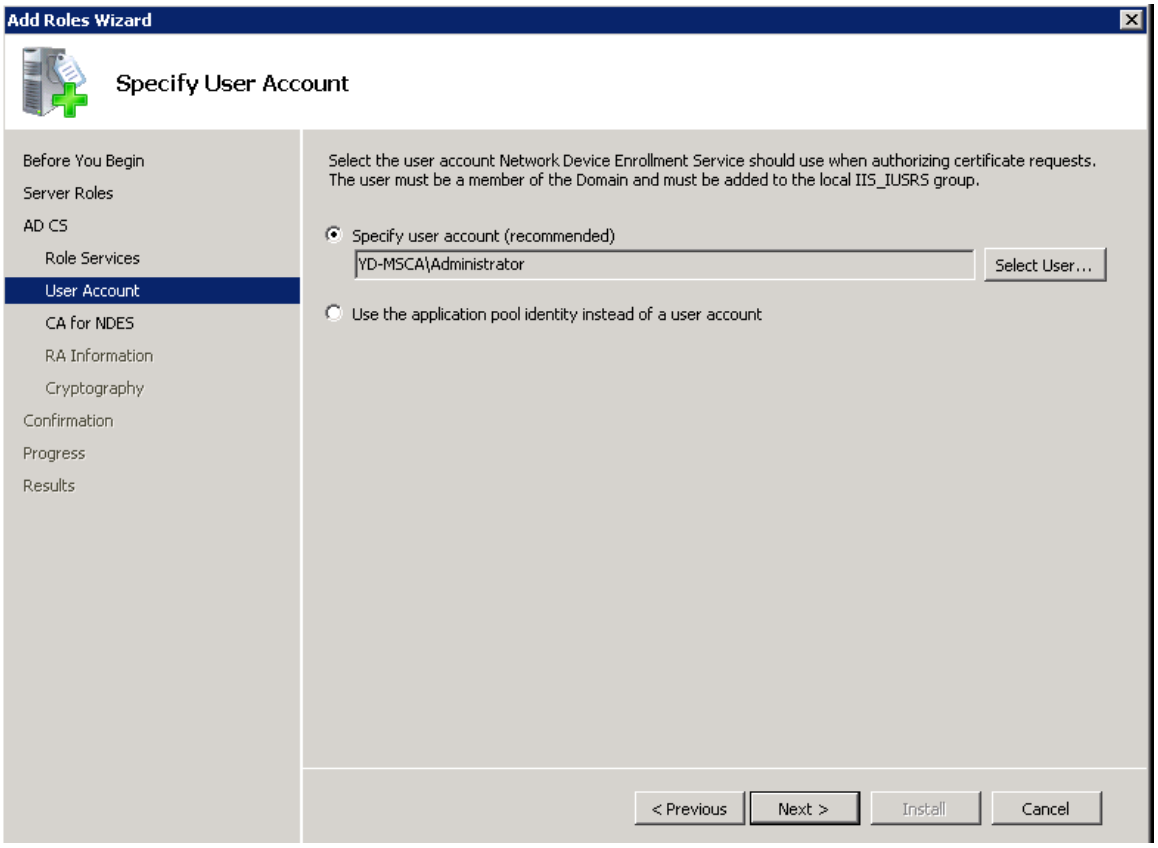
- On the **Select Server Role** page, select the **Active Directory Certificate Services** role, then click **Next**.

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

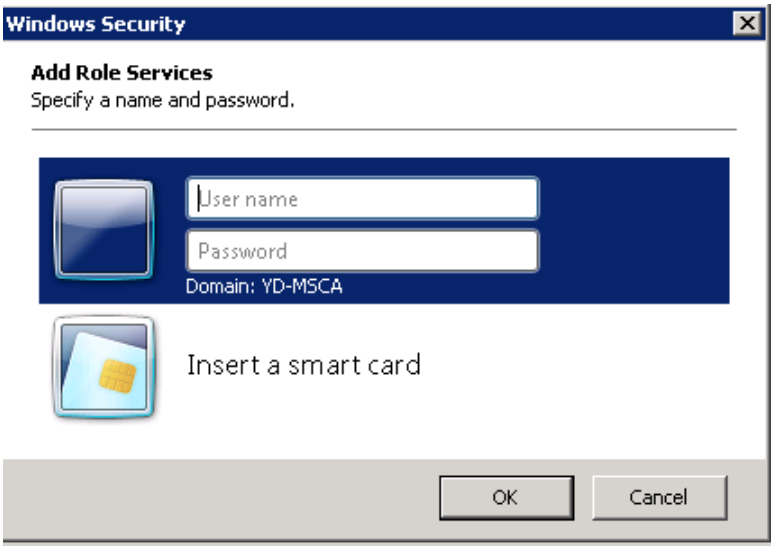


- The wizard will detect whether all the required dependencies are installed. If any dependencies are missing, you will be prompted with a dialog box explaining what is missing and requesting your permission to install the dependencies. Click **Yes** to continue the installation.

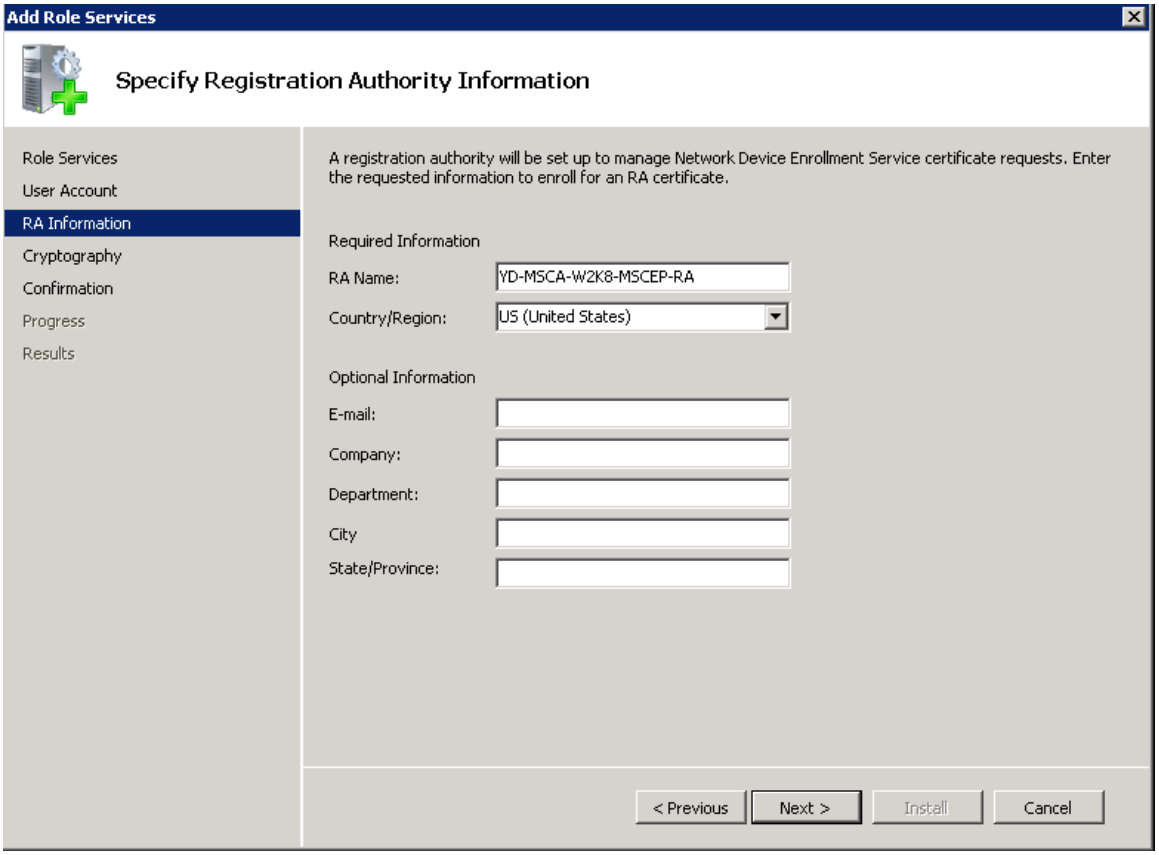
- Click **User Account** under **Role Services** and then click **Select User…**.



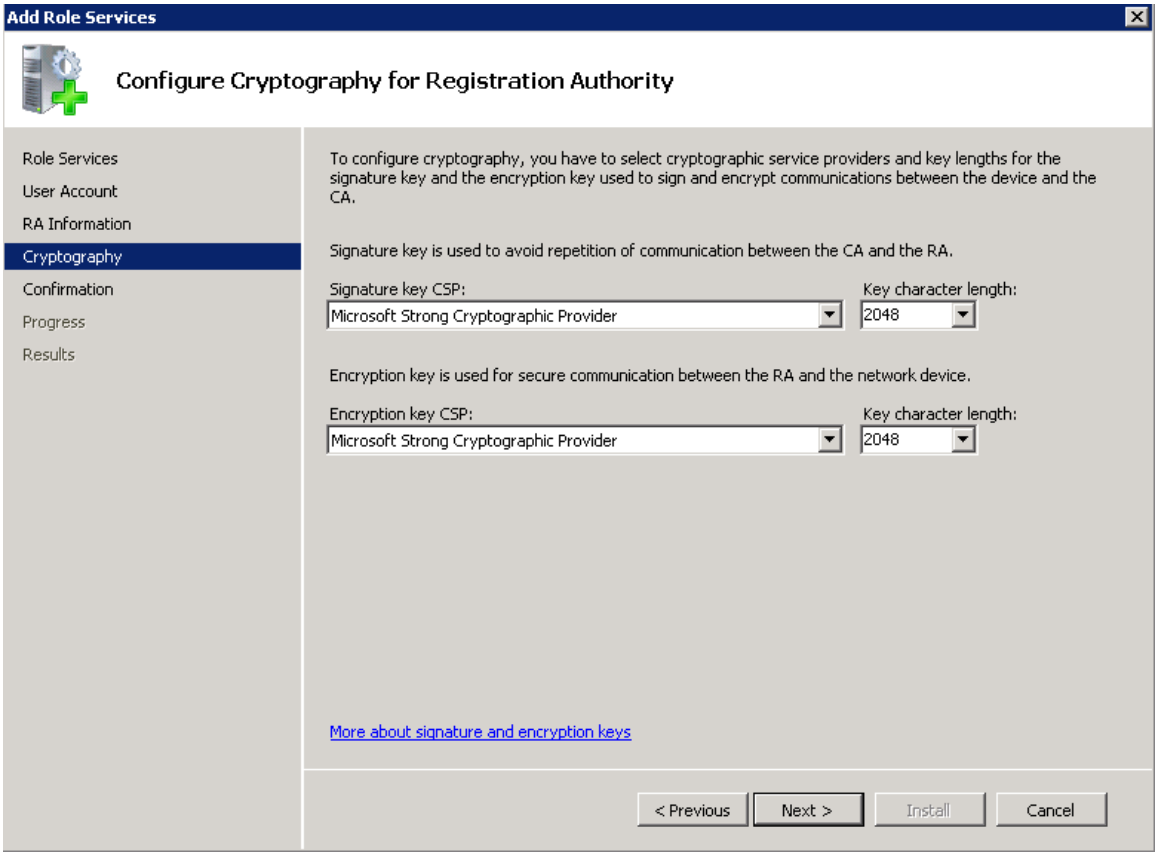
- Type in **Administrator** as the user name, then enter the password.



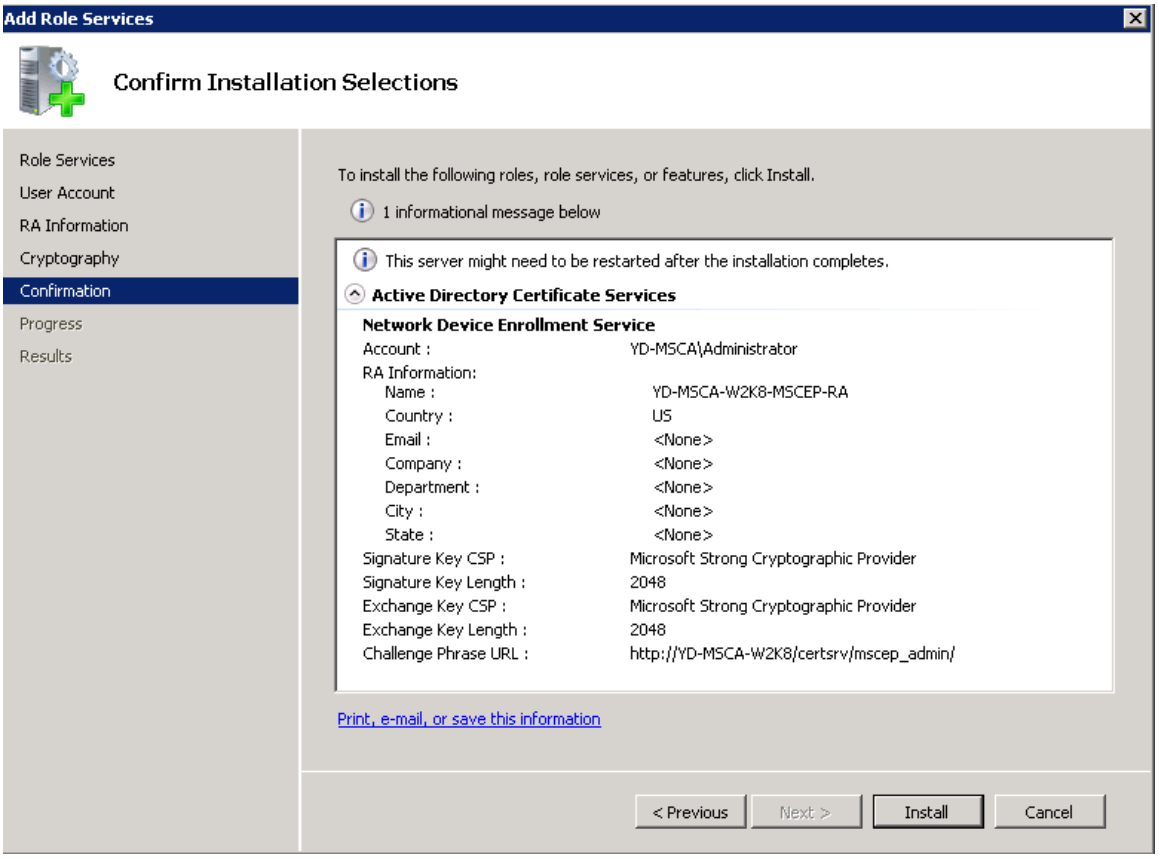
- Enter the Registration Authority information.



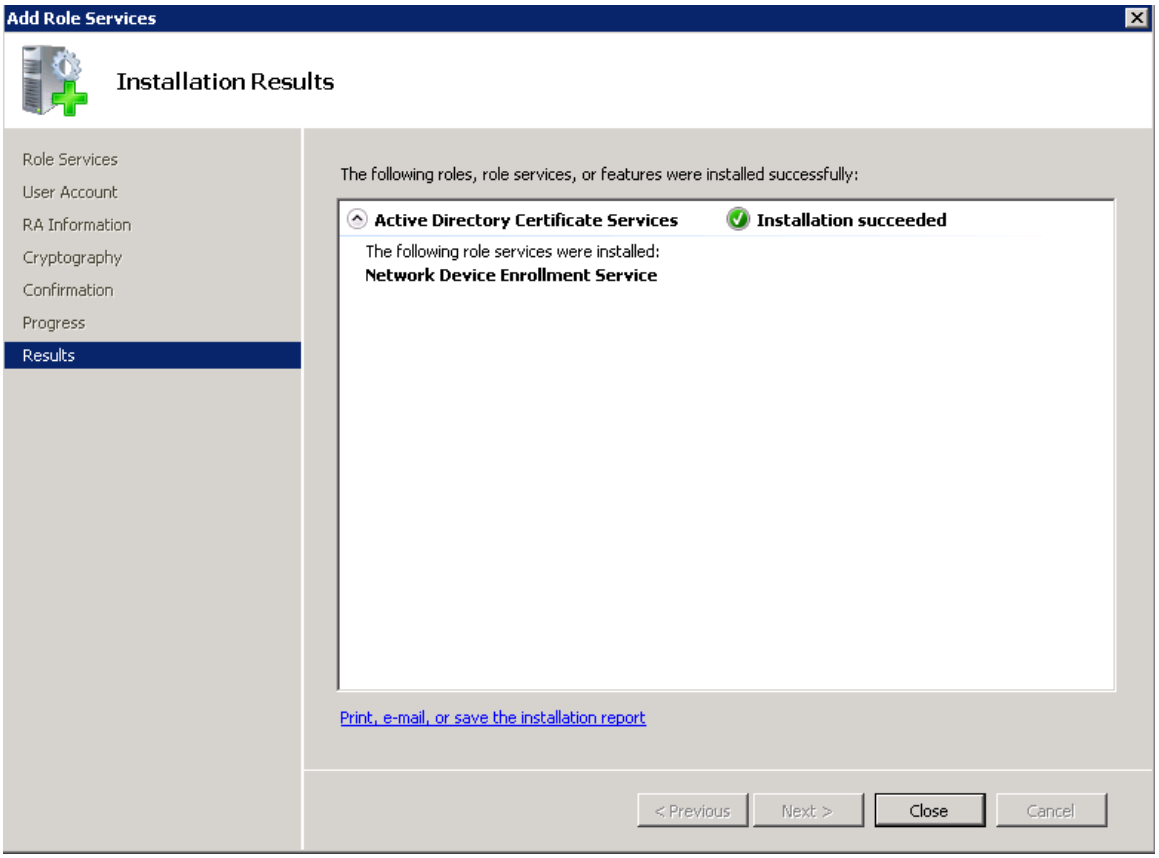
- Select **Microsoft Strong Cryptographic Provider** for **Signature Key CSP** and **Encryption key CSP**.
- Select **2048** for **Key character length**.



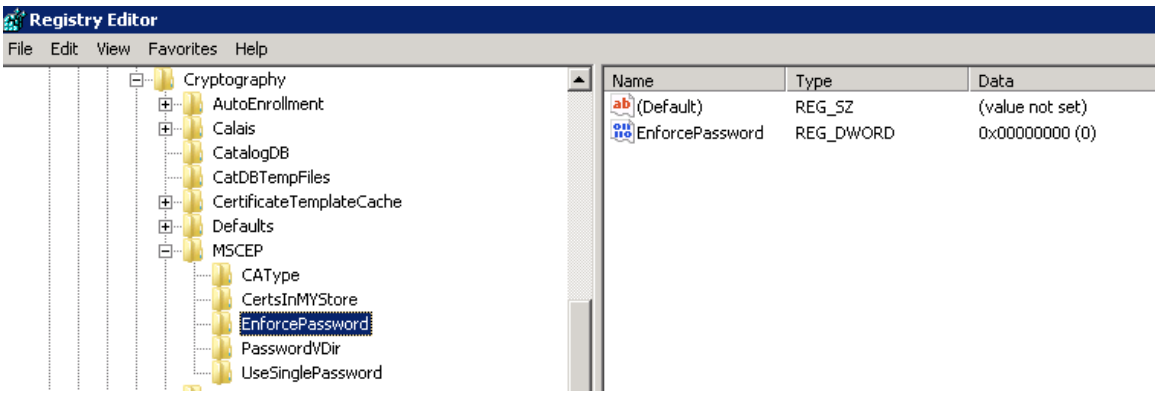
- Select **Install**.



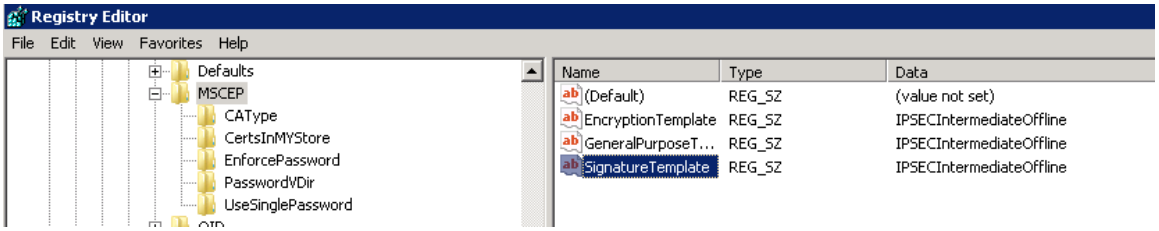
- A confirmation page will be displayed if the installation was successful.



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

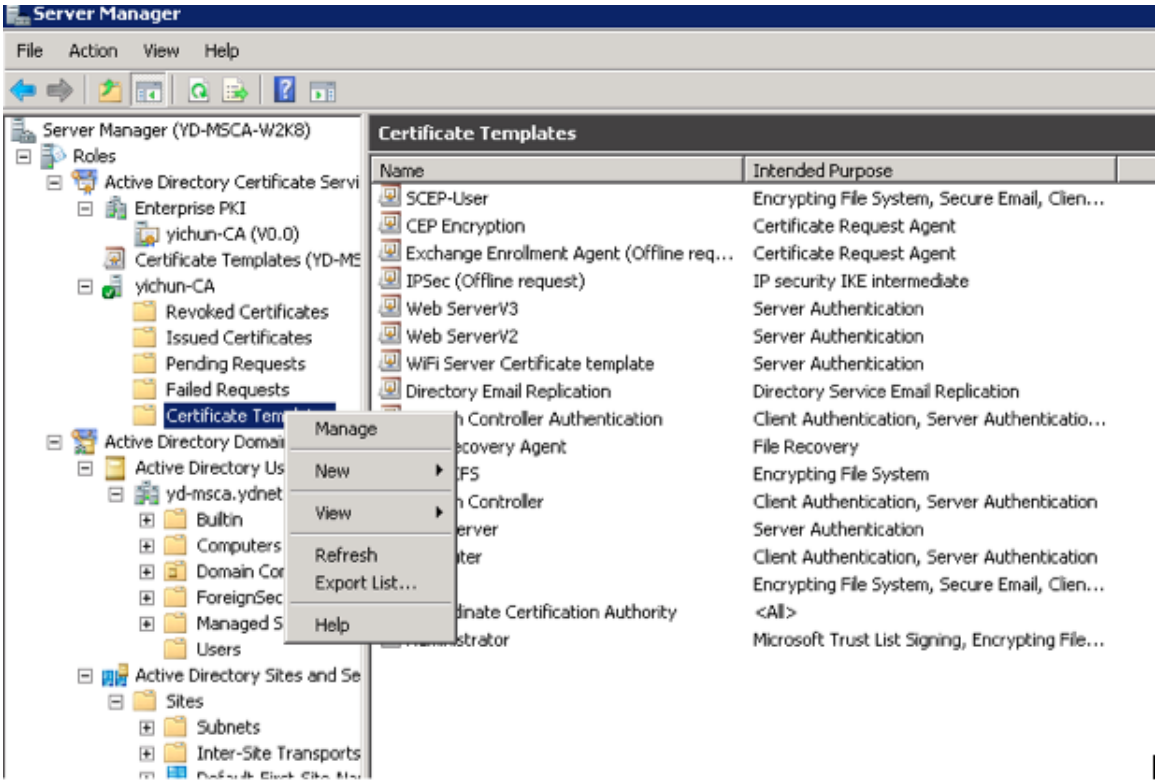


- SCEP uses the certificate template that is set in the registry for issuing certificates. (**HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**)

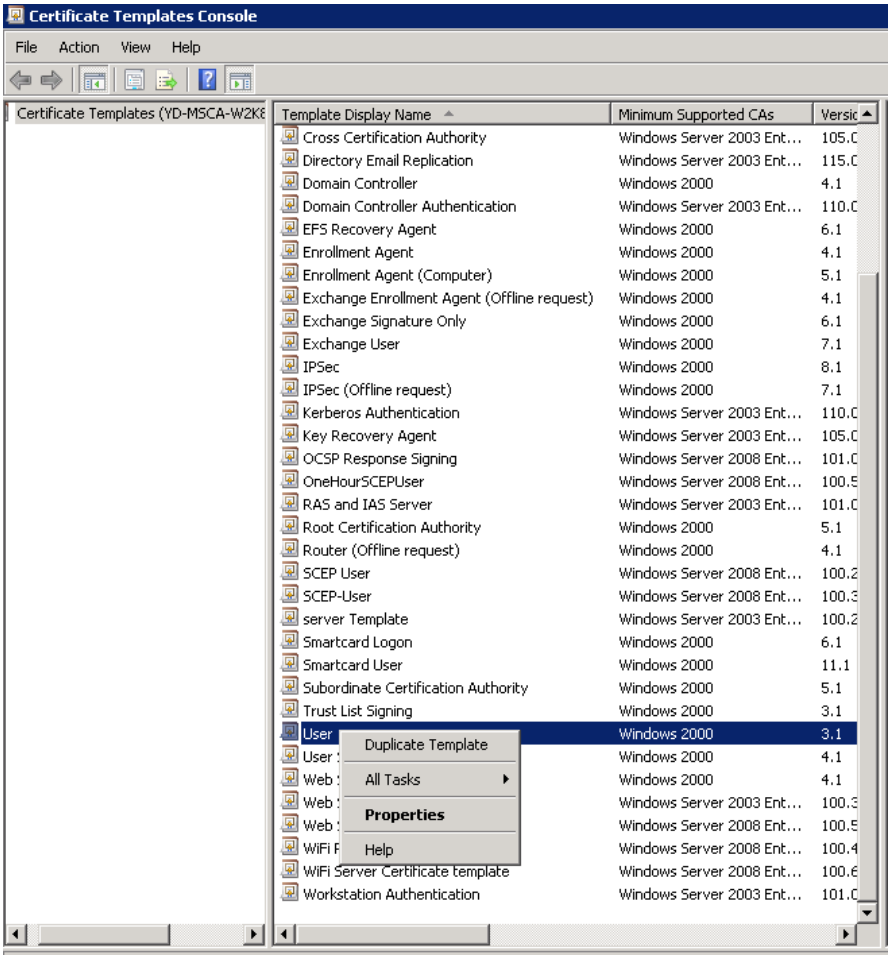


- Typically the RA will have a longer period (same as that of the CA certificate).
- The default template used for RA to be enrolled to the SCP server is **IPSECIntermediateOffline** as highlighted above.
- Make sure a correct template is set to the above registries before enrolling the RA to the SCEP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

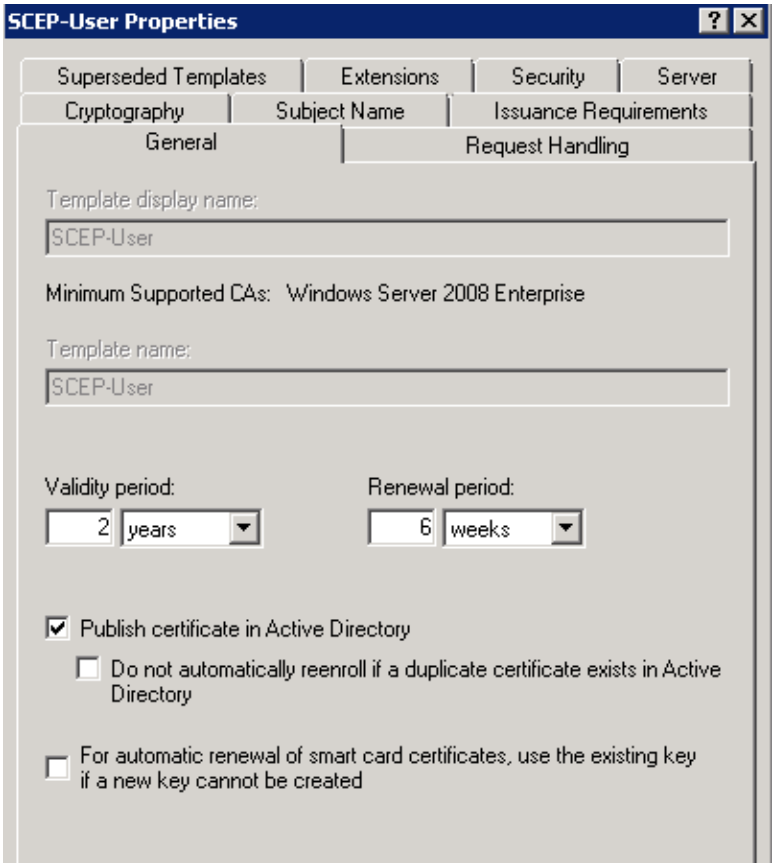
- Right click **Certificate Templates** then select **Manage**.



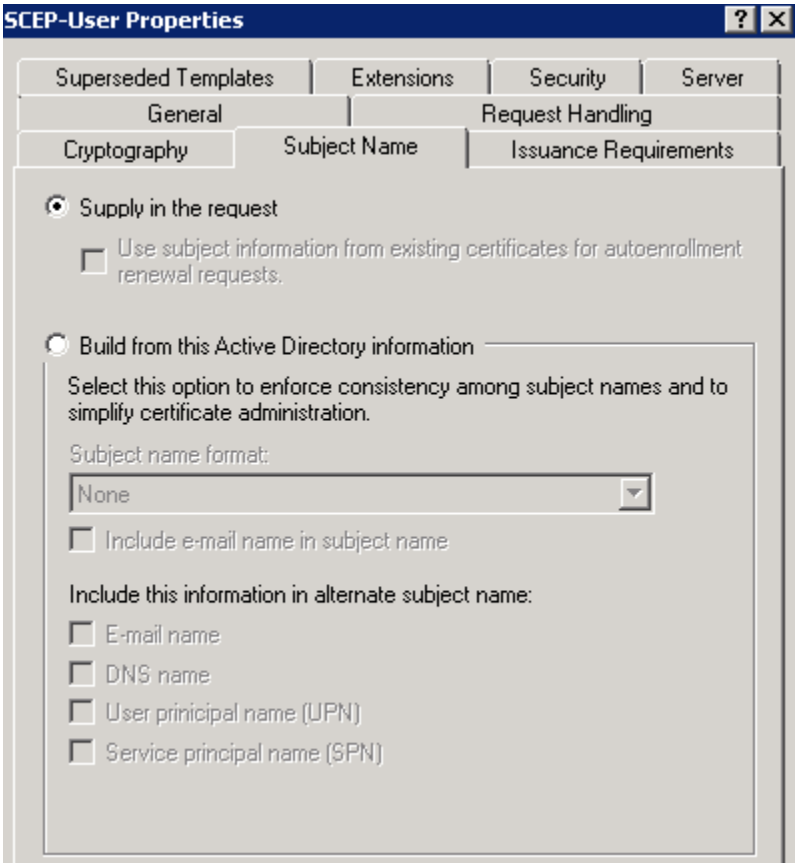
- Right click **User template** then select **Duplicate Template**.
- Select **Windows Server 2003 2008 Template**.
- Under the **General** tab, change template name and validity period.
- Under the **Extensions** tab, ensure the following:
    - **Client Authentication** is set as one of the application policies
    - **Key Usage** has **Digital Signature** attribute



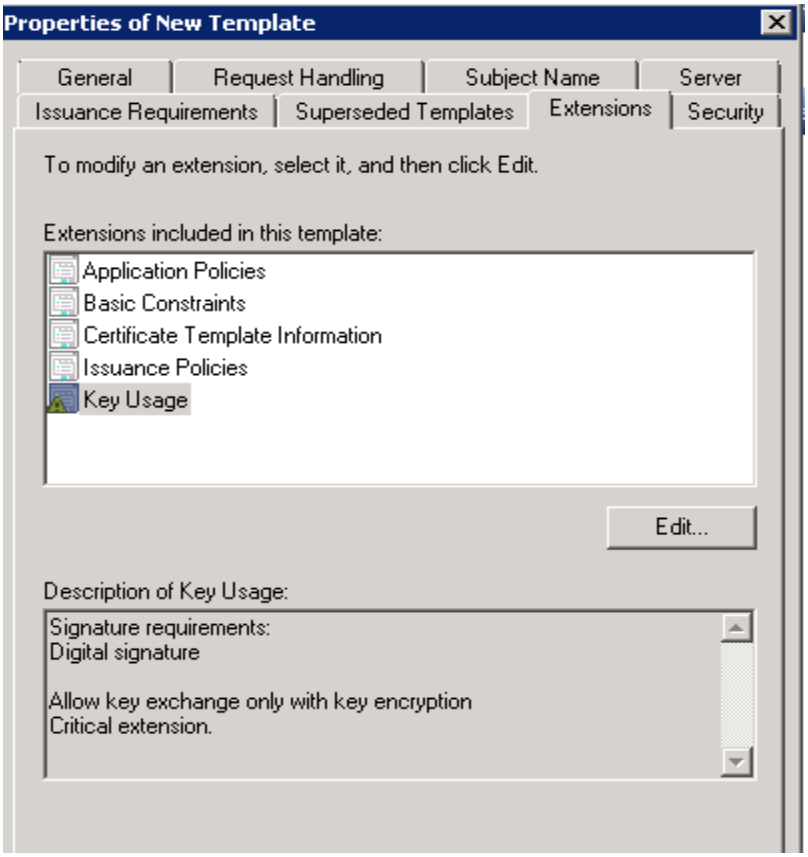
- Configure the **Validity Period** on the **General** tab as necessary.



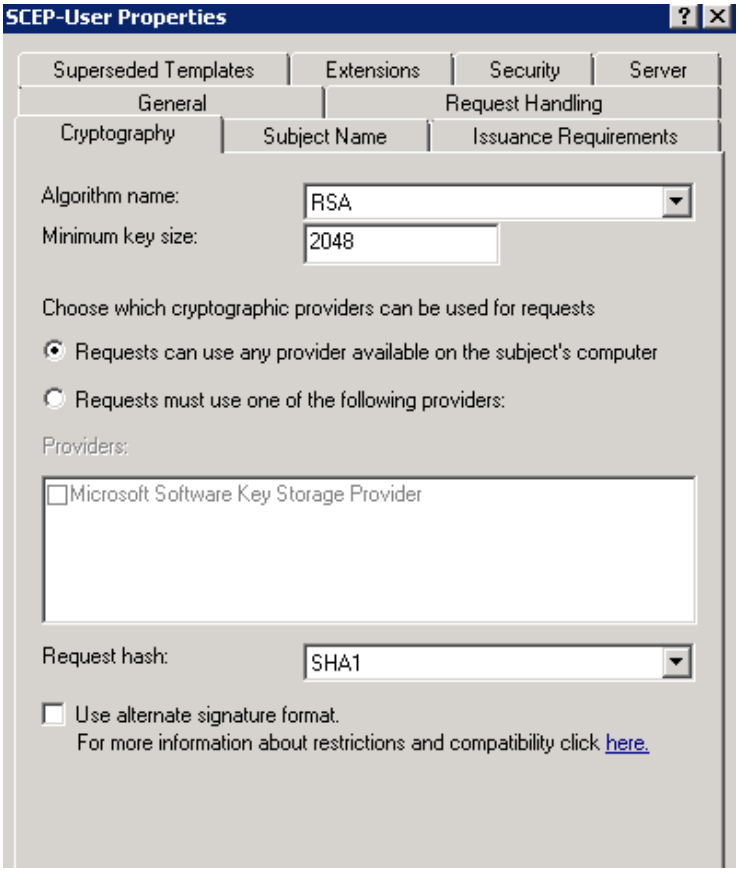
- Configure **Subject Name** tab as shown below.



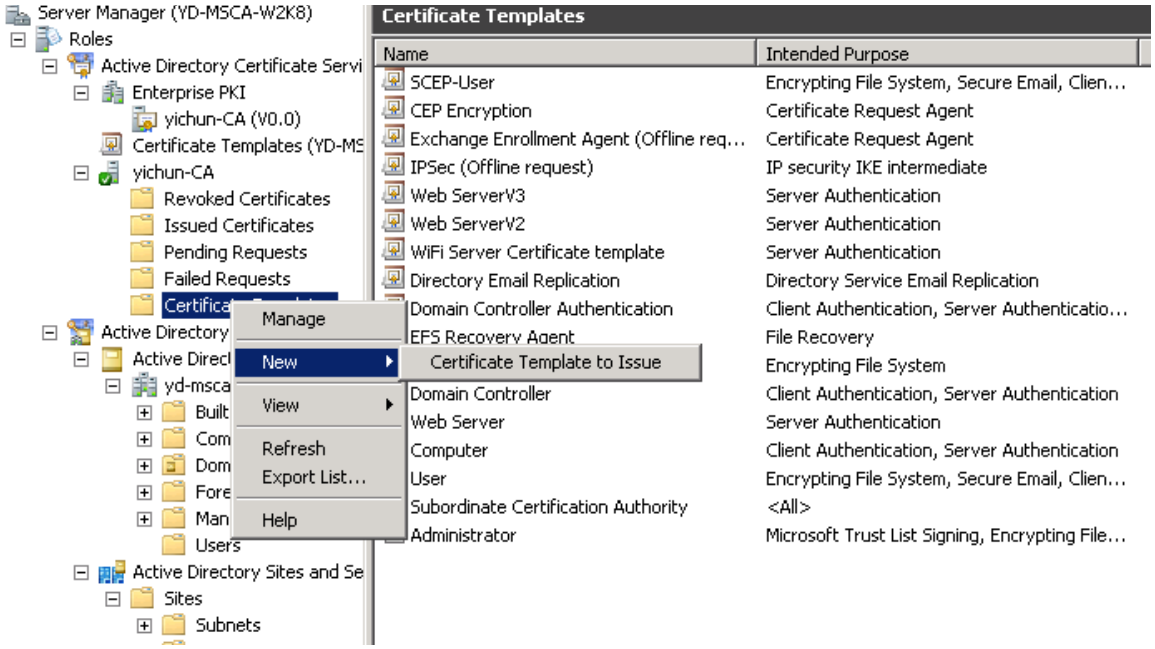
- Configure **Extensions** tab as shown below.



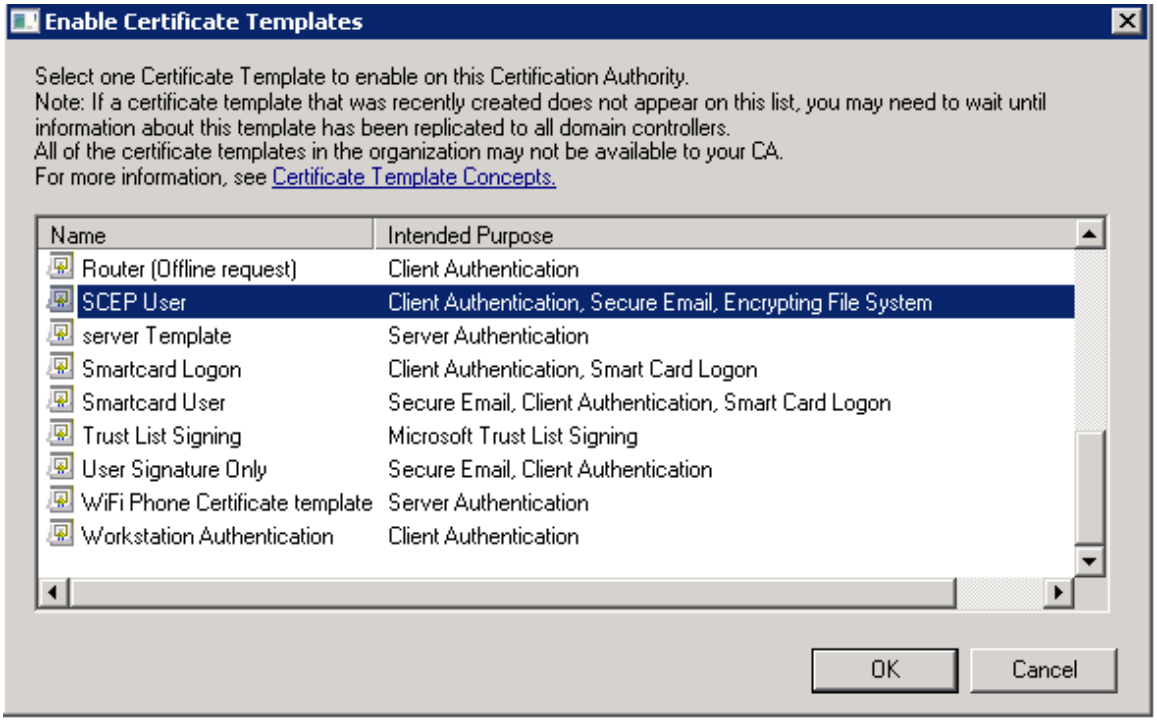
- Configure **Algorithm Name**, **Minimum Key Size**, and **Request Hash** as necessary on the **Cryptography** tab.



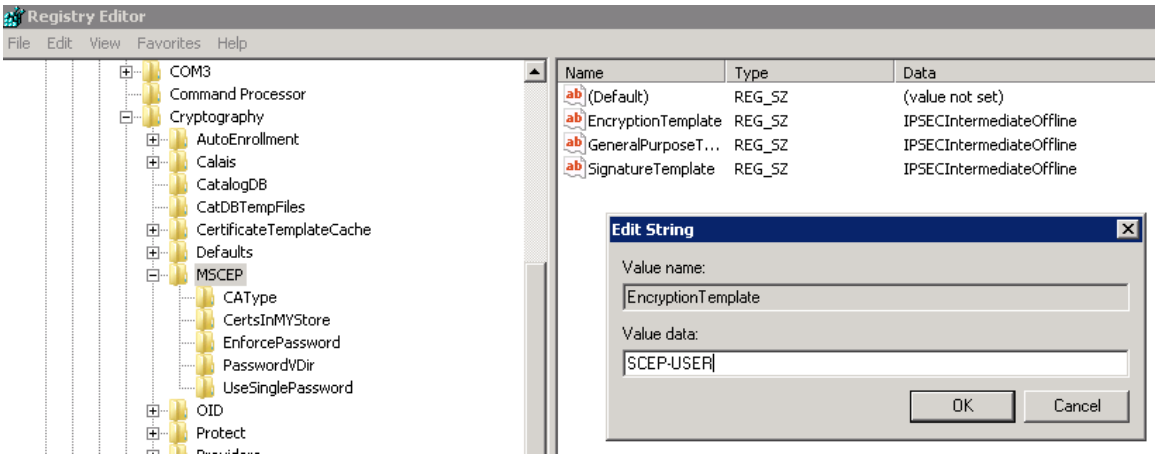
- Enable the newly created template by right clicking **Certificate Templates** then selecting **New > Certificate Template to Issue**.



- Select **SCEP User** template.



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

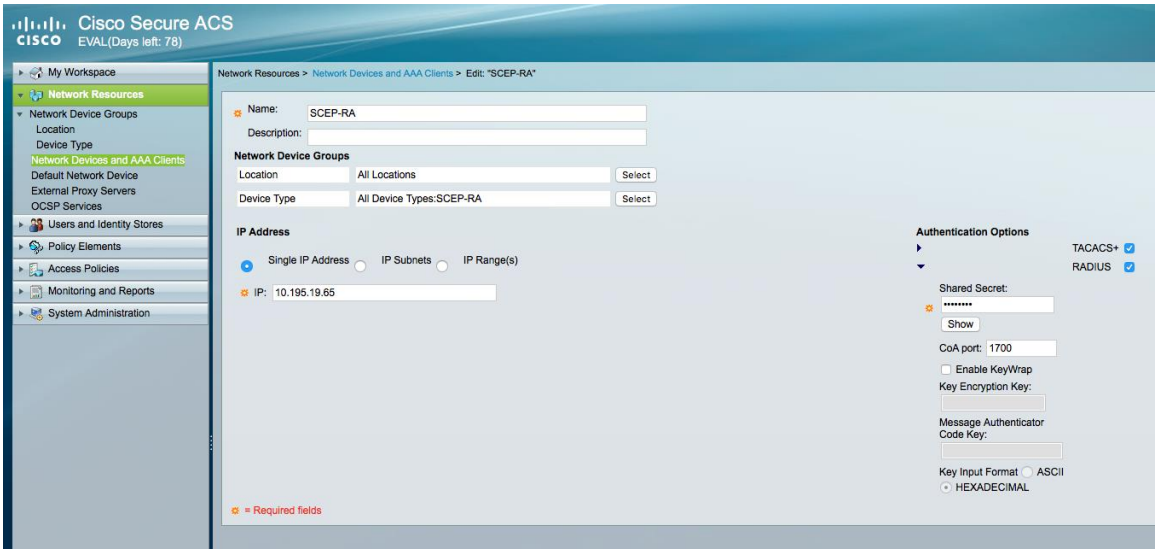


- Go to **IIS** > **Application Pools** to stop then start the SCEP service for the new template to take effect.

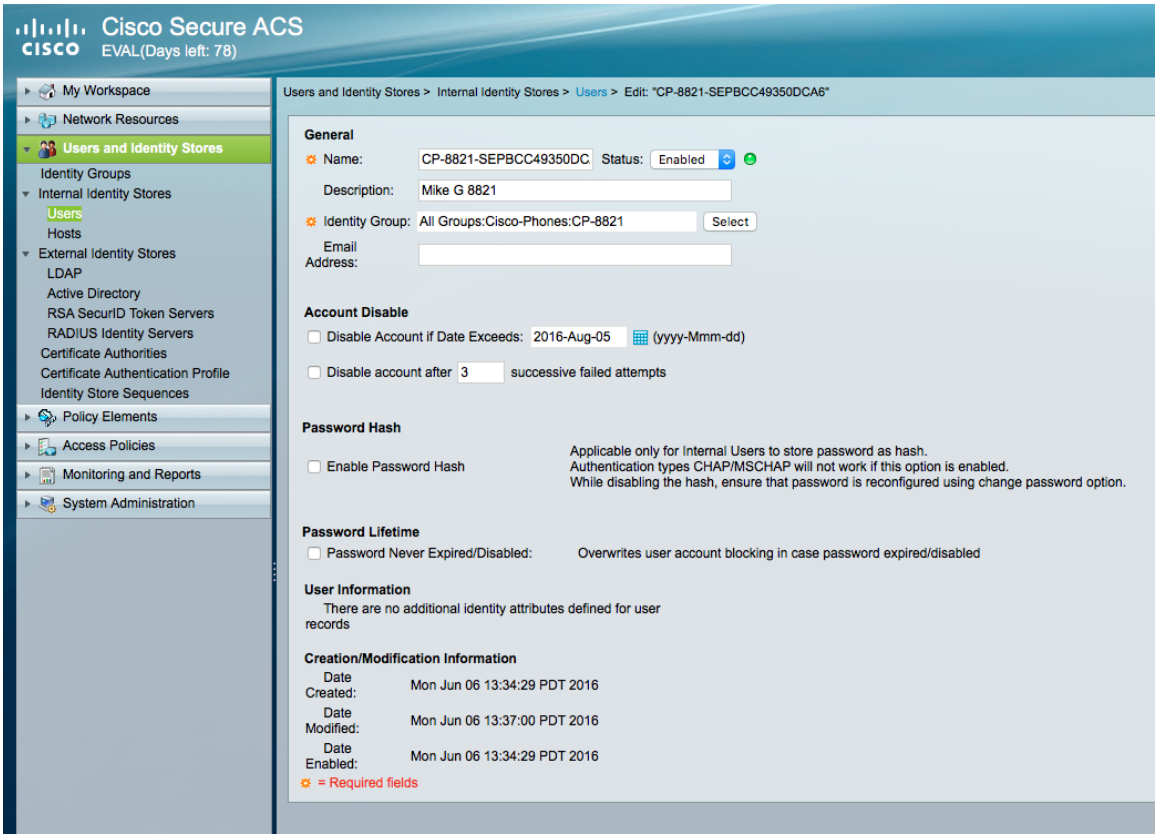
RADIUS Configuration

Use the following guidelines to configure the RADIUS server.

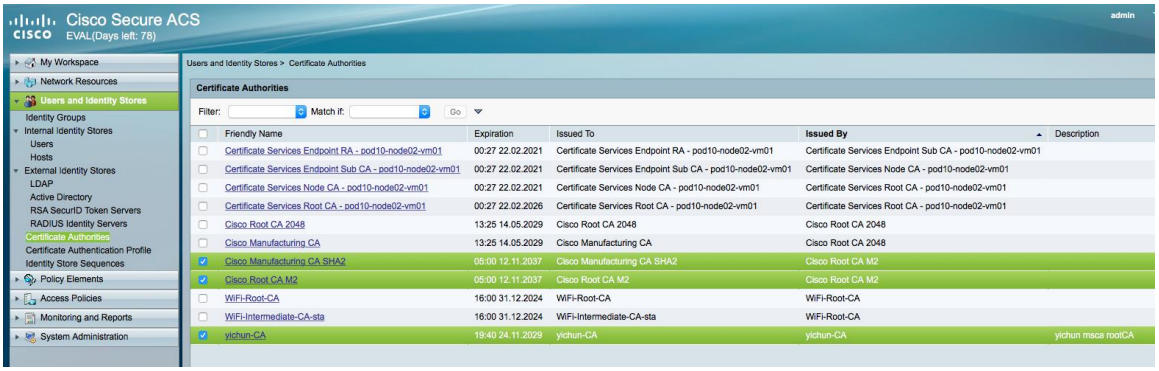
- Add the SCEP RA under **Network Device and AAA Clients**.
- Configure the RADIUS shared secret that the SCEP RA is currently configured for.



- Create a user account matching the common name of the phone's Manufacturing Installed Certificate (MIC) with the password set to **cisco** (e.g. CP-8821-SEPxxxxxxxxxxxx).

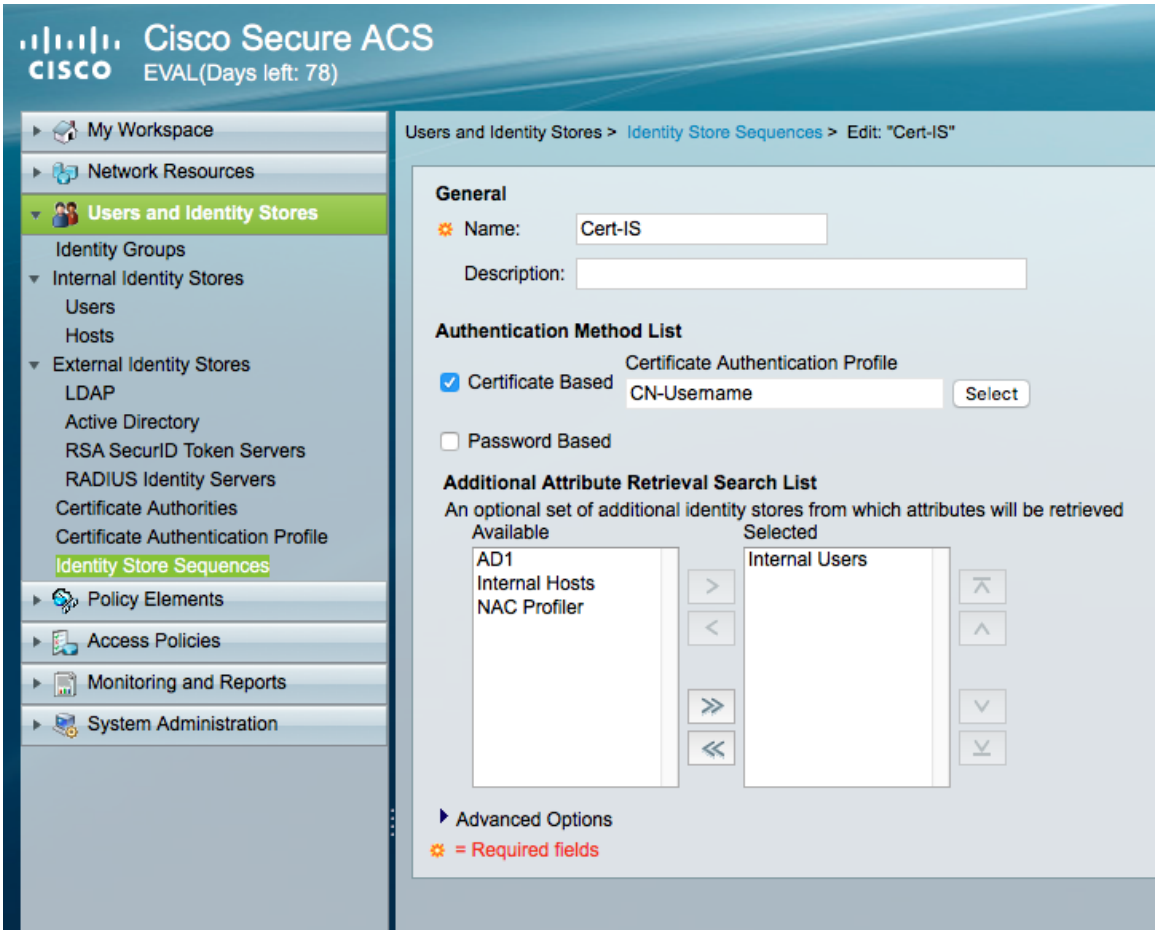


- Add the Cisco Manufacturing CA chain to the RADIUS trust list as well as any other CA chains utilized for authentication.

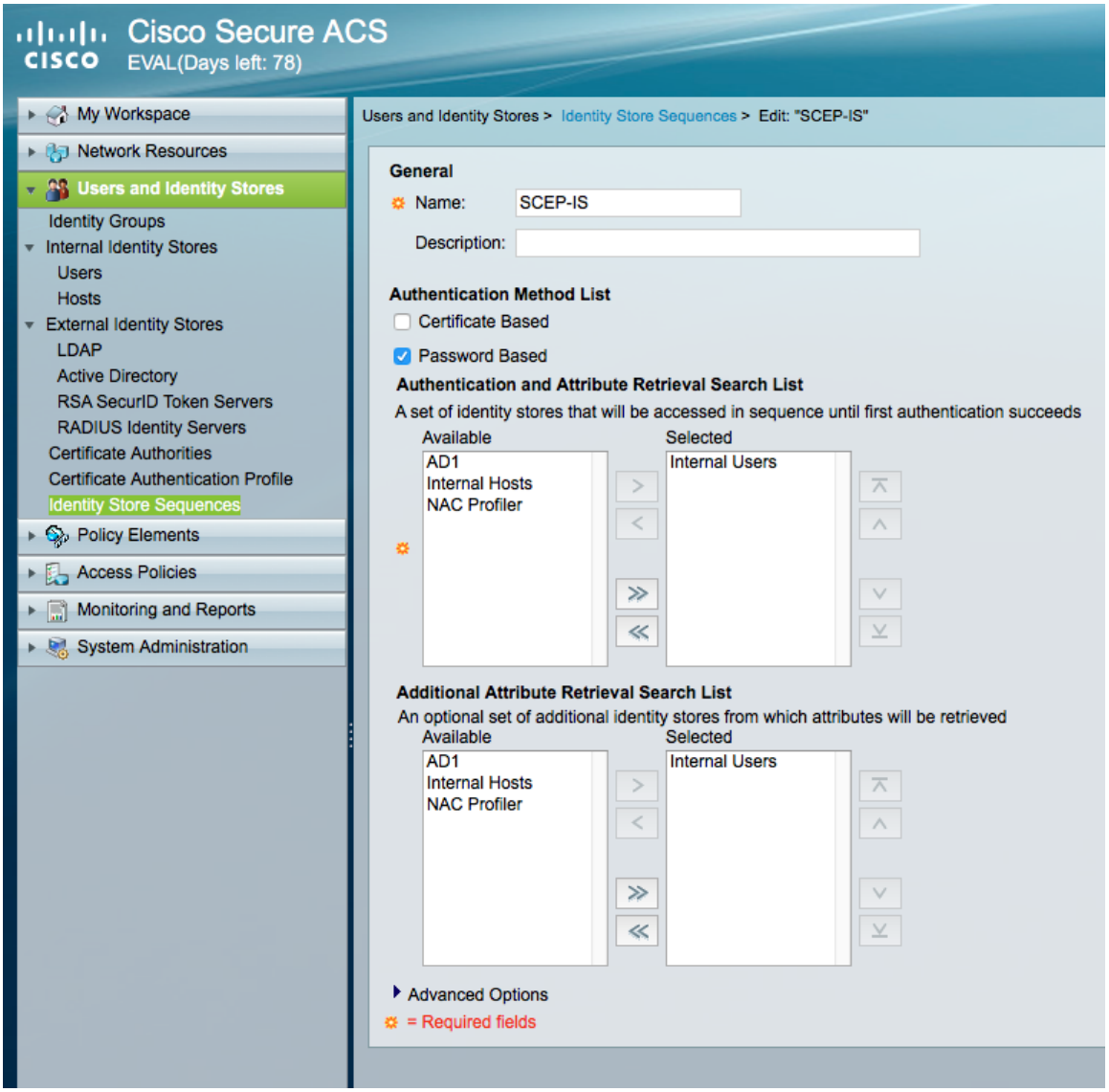


- Create a **Certificate Authentication Profile**.

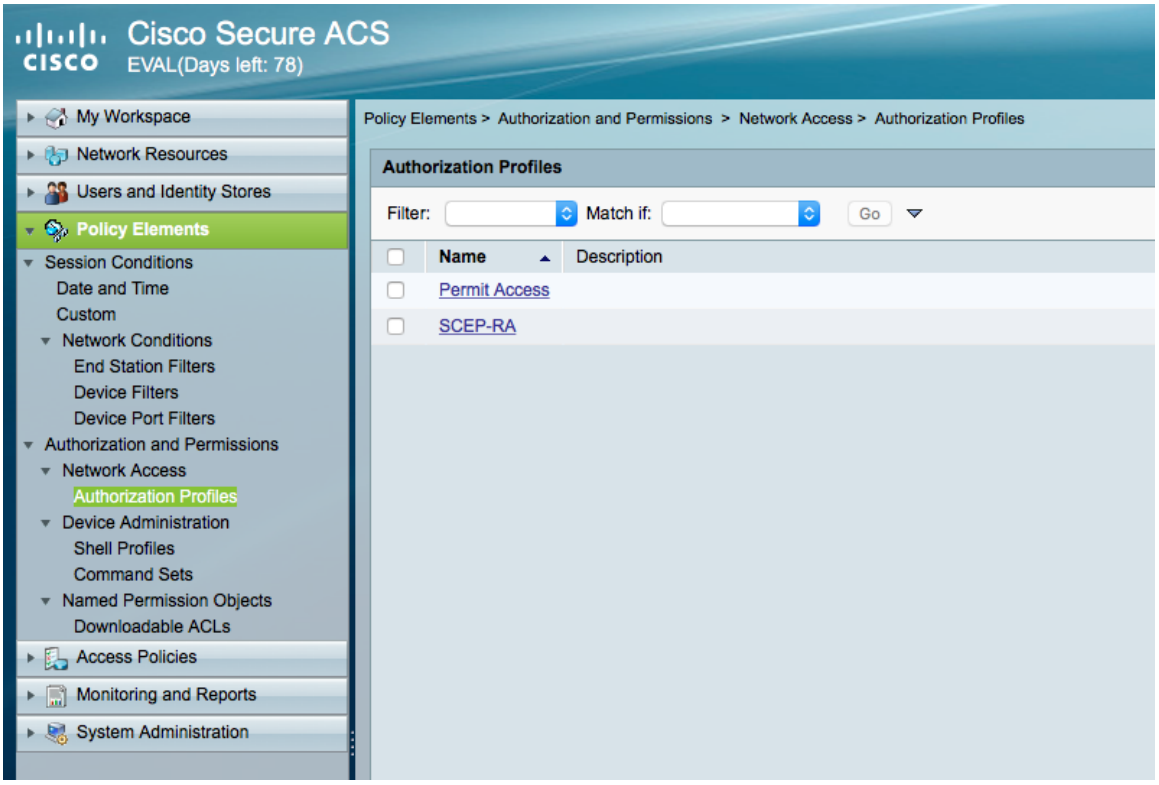
- Create an **Identity Store Sequence** to be used for EAP-TLS authentication.
- Check **Certificate Based,** select the newly created **Certificate Authentication Profile**, and select **Internal Users** as the additional identity store.

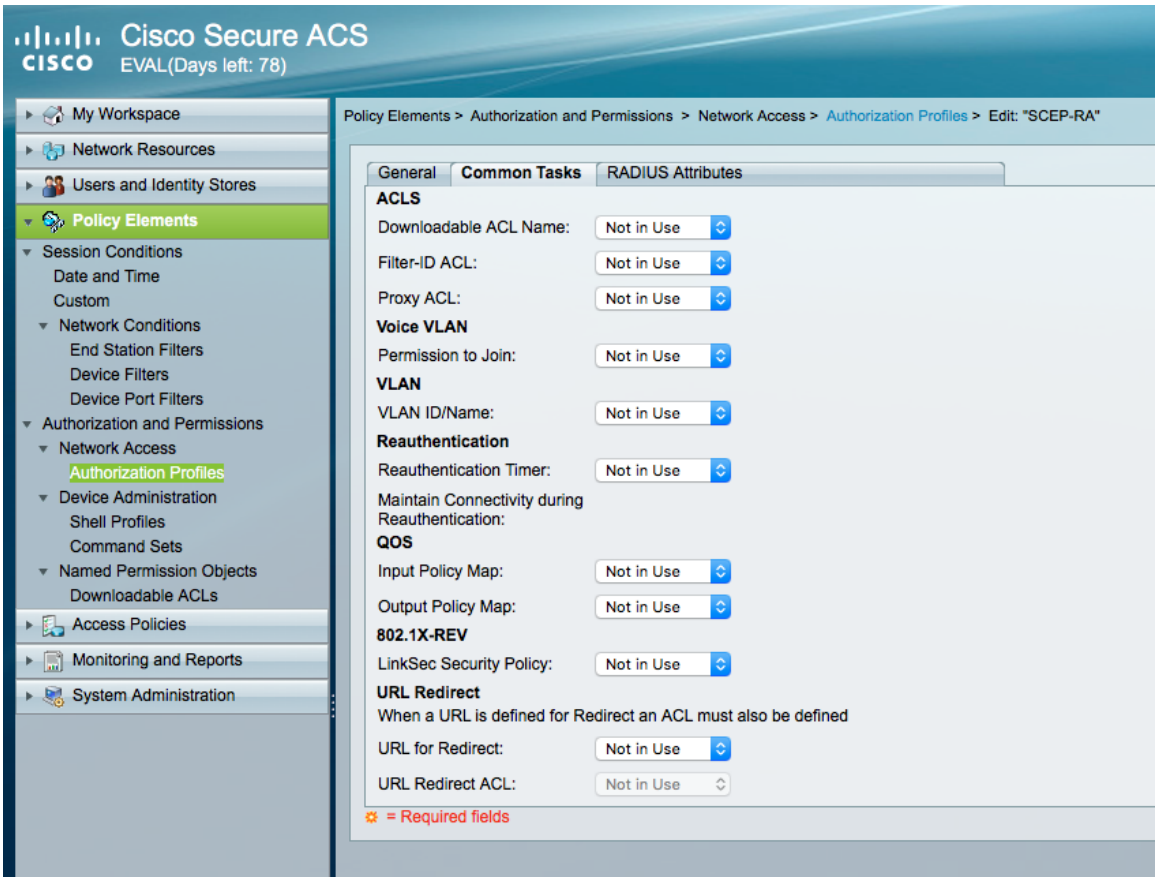


- Create an **Identity Store Sequence** to be used for SCEP authentication.
- Check **Password Based,** select the newly created **Certificate Authentication Profile**, and select **Internal Users** as the identity store.

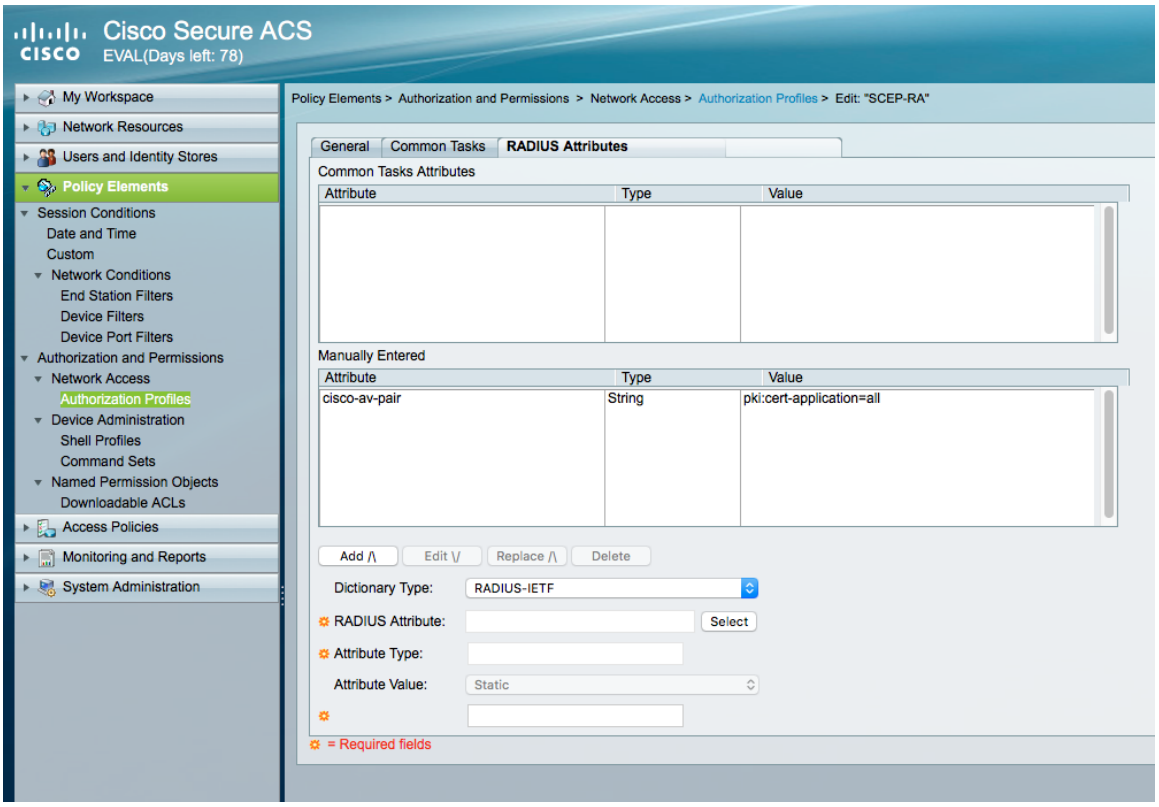


- Create an **Authorization Profile** to be used for SCEP authorization.

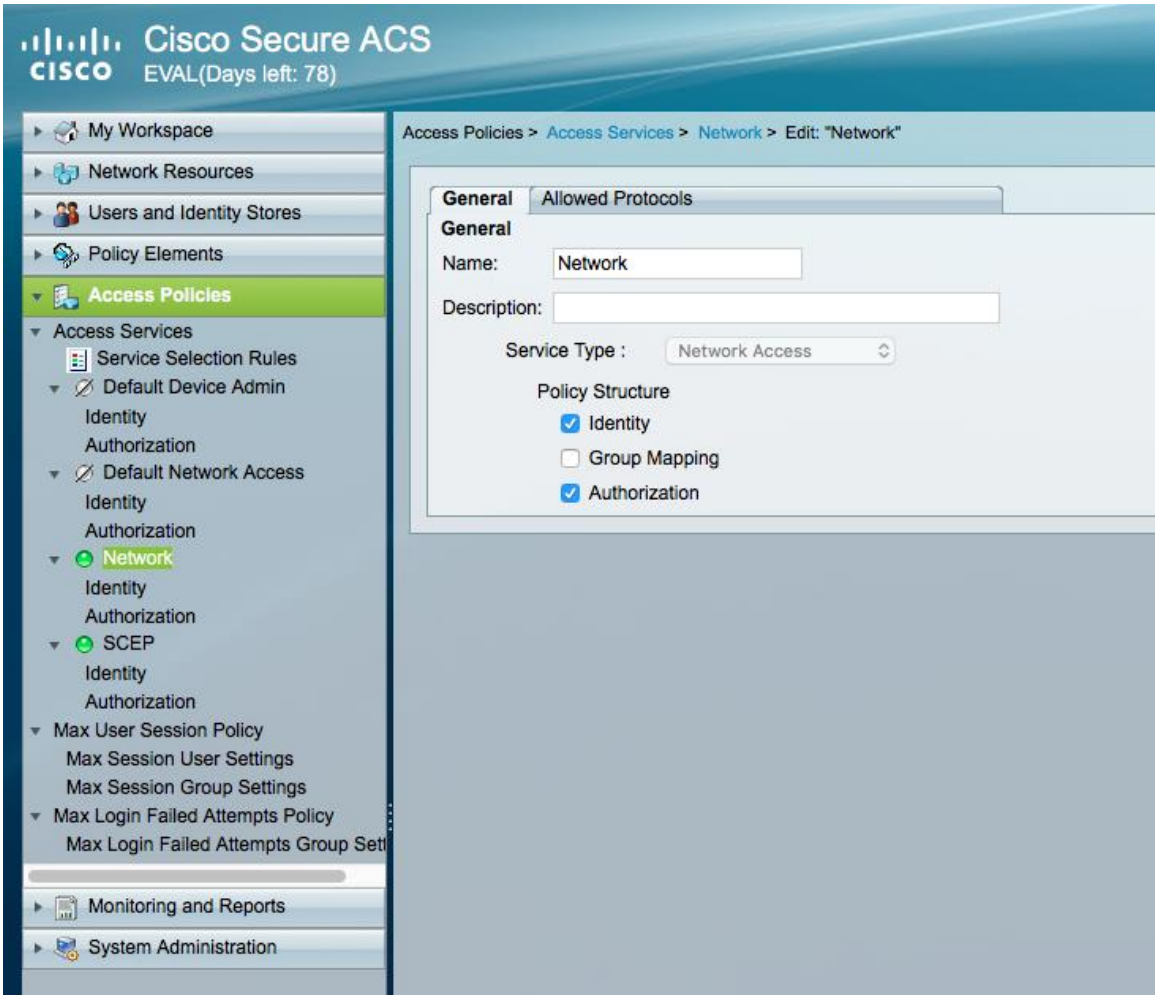




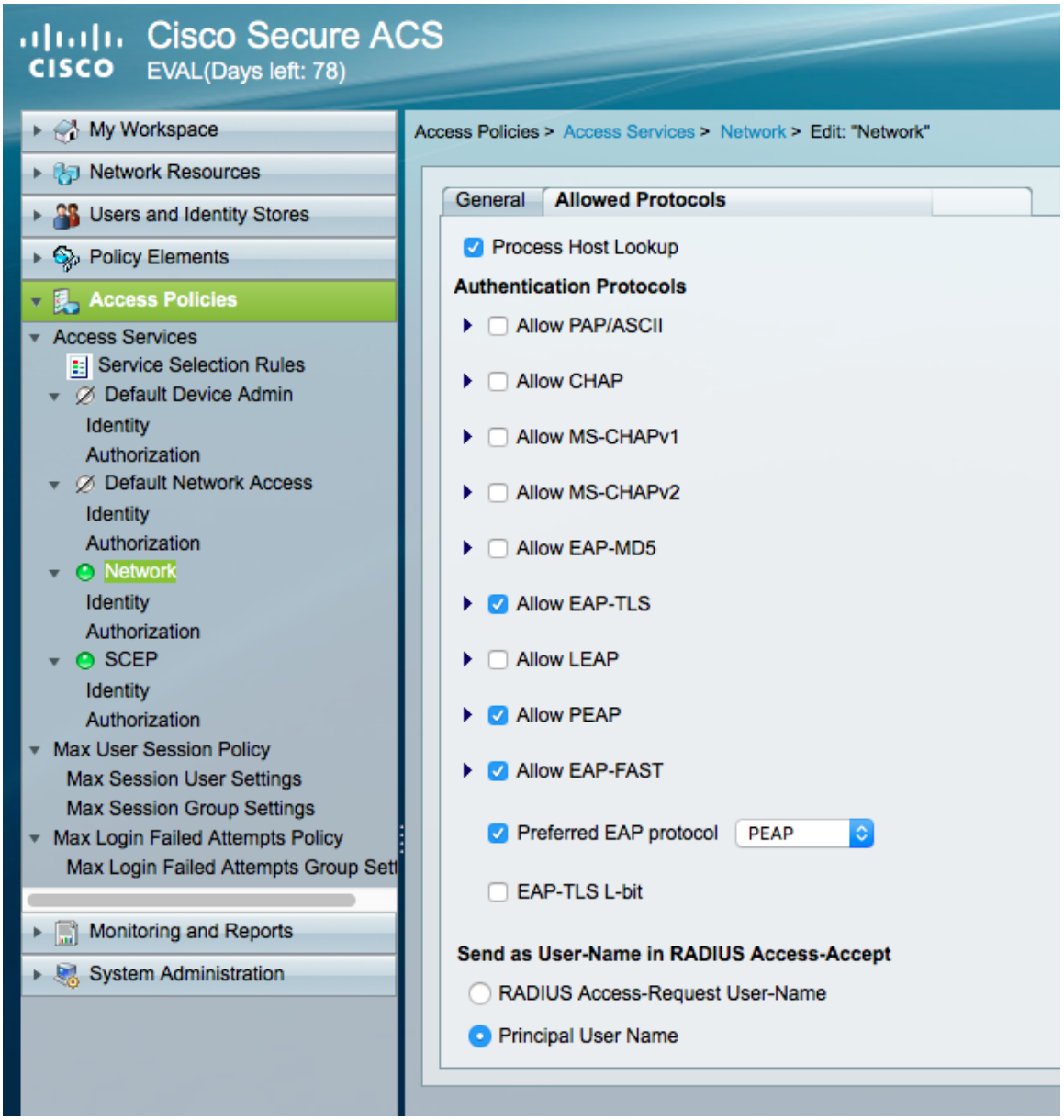
- Under the **RADIUS Attributes** tab, add the **cisco-av-pair** attribute where the **Type** is set to **String** and **Value** is set to **pki:cert-application=all**.



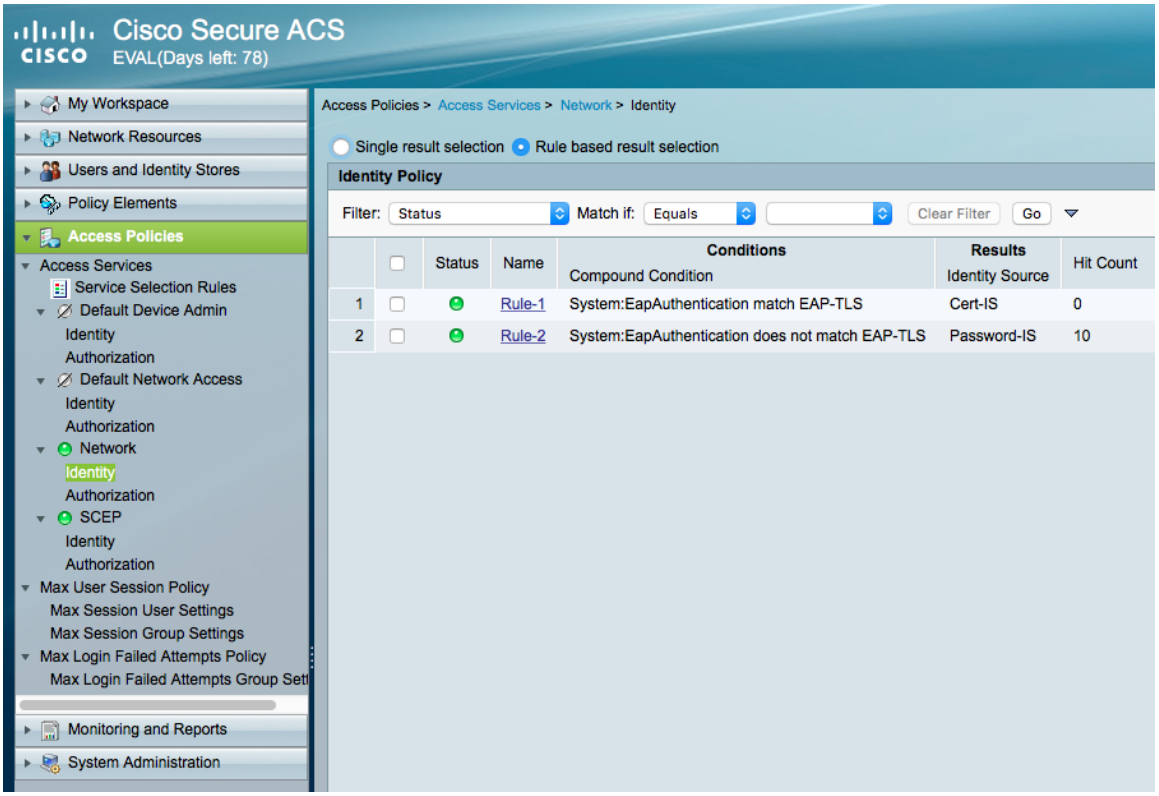
- Create an **Access Policy** to be used for EAP-TLS authentication.



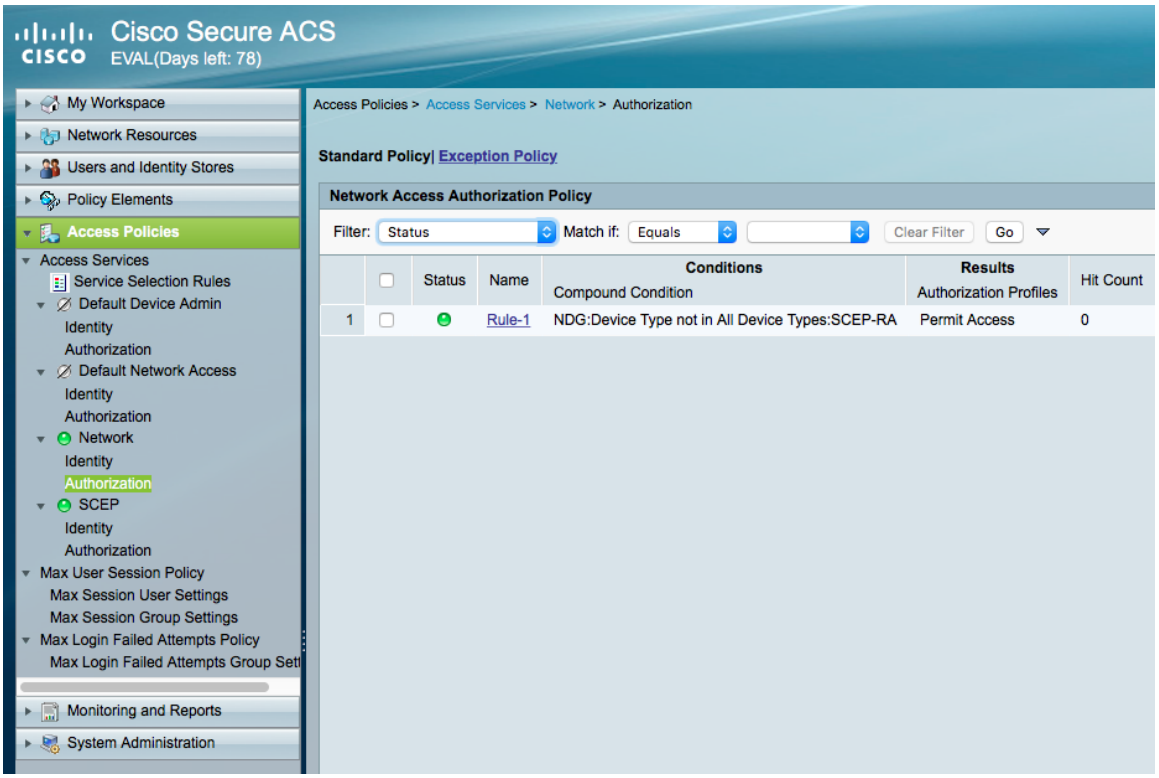
- For the **Access Service** for EAP-TLS authentication, need to ensure that **EAP-TLS** is enabled.



- Under **Identity**, rules can be defined to match EAP type then determine which identity source to use for authentication.

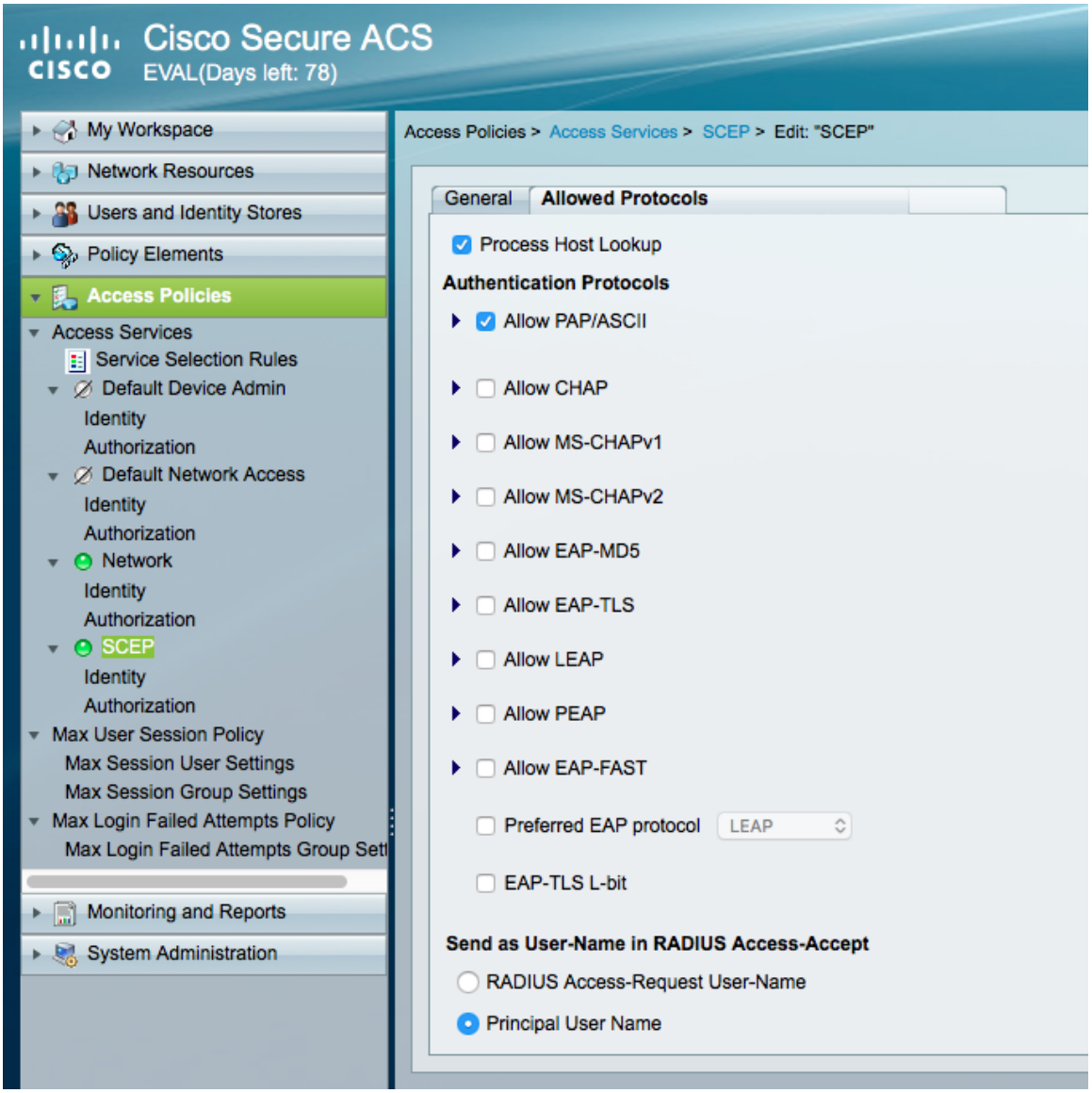


- Under **Identity**, rules can be defined to match various conditions then determine which authorization profile to use.

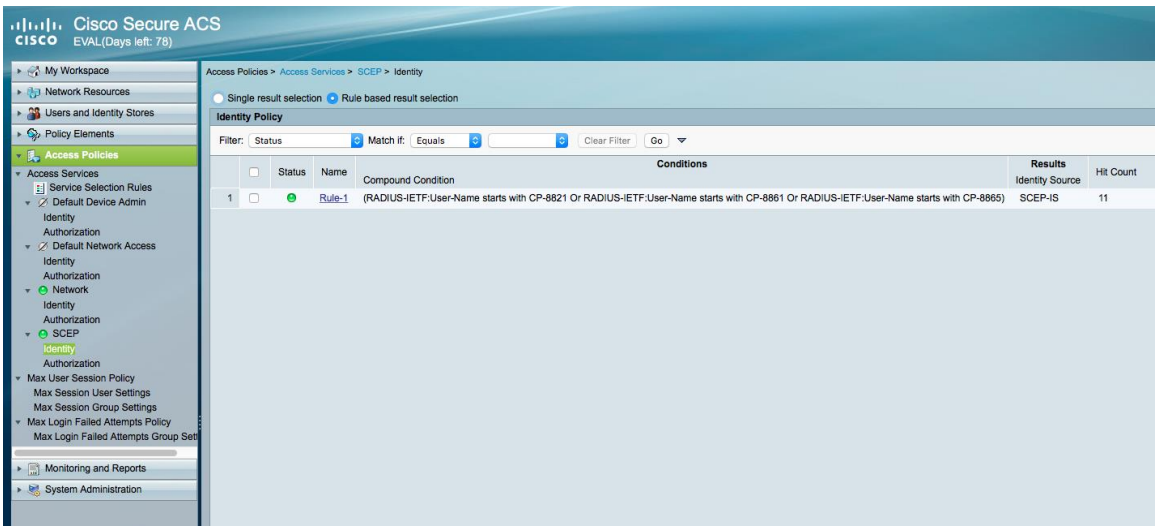


- Create an **Access Policy** to be used for SCEP authentication.

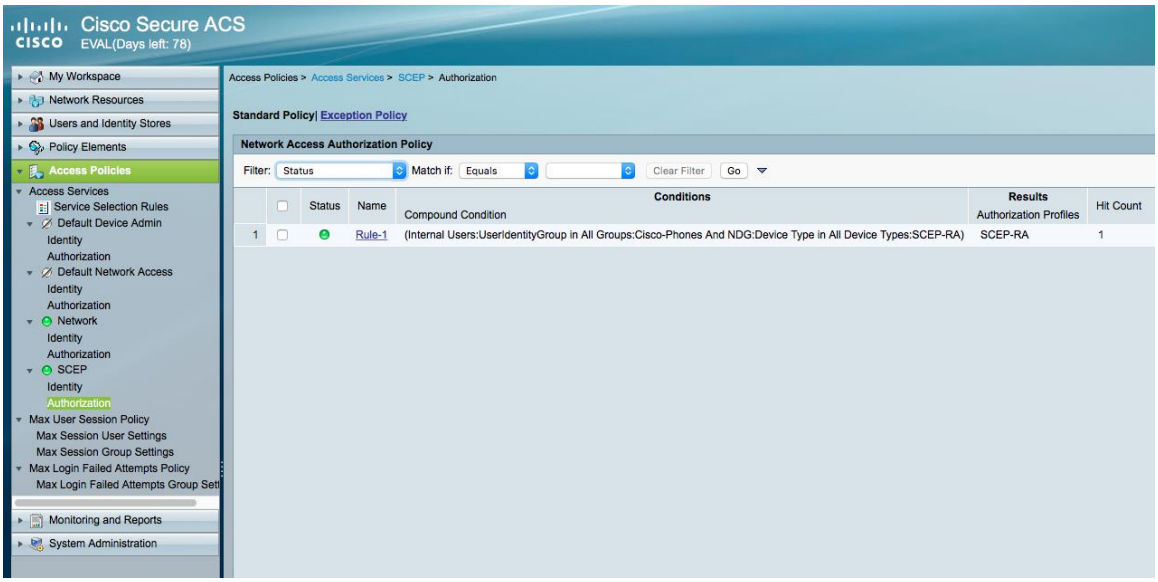
- For the **Access Service** for SCEP authentication, need to ensure that **PAP/ASCII** is enabled.



- Under **Identity**, rules can be defined to match various conditions then determine which identity source to use for authentication.



- Under **Identity**, rules can be defined to match various conditions then determine which authorization profile to use.



SCEP RA Configuration

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

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

- Enable HTTP server on the Cisco IOS router.

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

- Configure a RADIUS server for device authentication.

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

- Configure a PKI trustpoint for the MIC's CA chain to validate the phone's MIC.

ISR_RA# **configure terminal**

ISR_RA(config)# **crypto pki trustpoint MIC_trustpoint**

ISR_RA(ca-trustpoint)# **authorization list PhoneList**

ISR_RA(ca-trustpoint)# **authorization username subjectname commonname**

ISR_RA(ca-trustpoint)# **exit**

ISR_RA(config)# **crypto pki trustpoint MIC_trustpoint**

ISR_RA(ca-trustpoint)# **enrollment terminal**

ISR_RA(ca-trustpoint)# **revocation-check none**

ISR_RA(ca-trustpoint)# **exit**

ISR_RA(config)# **crypto pki authenticate MIC_trustpoint**

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

-----BEGIN CERTIFICATE-----

MIIEZTCCA02gAwIBAgIBAjANBgkqhkiG9w0BAQsFADArMQ4wDAYDVQQKEwVDaXNj
bzEZMBcGA1UEAxMQQ2lzY28gUm9vdCBDQSBNMjAeFw0xMjExMTIxMzUwNThaFw0z
NzExMTIxMzAwMTdaMDYxDjAMBgNVBAoTBUNpc2NvMSQwIgYDVQQDExtDaXNjbyBN
YW51ZmFjdHVyaW5nIENBIFNIQTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQD0NktCAjJn3kk98hU7wUVp6QlOFrlItEce6CpbfYpeLdUeZduAo+S0otzT
lJwS2BlMhZtacu9vUpfmW9w7nQo9zVT3eyPuhF/6/9TEdVBn75zb5CfV+E6ld+fH
nuPiFyBu+HDDJRd373Op+957IdoWyPvD8hHR1HJGFJ3JJKBg0UScL4JCwleu98Xq
/yPlAqBhExa7a2/fqSmZA0vZIG1bBfWZY8ZtSeTxKg3eWynV+xElabHqTDMYWf+2
obs4YB5lINTbYgHyRETP6T8Xr6TtD0h3654OUHcW+1meBu/jctluMKppeSjVtrof
5vt+pbkCg0iQAAjsL0qczT3yaNXvAgMBAAGjggGHMIIBgzAOBgNVHQ8BAf8EBAMC
AQYwEgYDVR0TAQH/BAgwBgEB/wIBADBcBgNVHSAEVTBTMFEGCisGAQQBCRUBEgAw
QzBBBggrBgEFBQcCARY1aHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtp
L3BvbGljaWVzL2luZGV4Lmh0bWwwHQYDVR0OBBYEFHrXeZXKu0gruFUU/aPAD7yn
D5YZMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jcmwvY3JjYW0yLmNybDB8BggrBgEFBQcBAQRwMG4wPgYIKwYBBQUH
MAKGMmh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9jcmNh
bTIuY2VyMCwGCCsGAQUFBzABhiBodHRwczovL3Rvb2xzLmNpc2NvLmNvbS9wa2kv
b2NzcDAfBgNVHSMEGDAWgBTJAPkfih/CZr2l0m1lDiIuNMMFoDANBgkqhkiG9w0B
AQsFAAOCAQEAc1k2rH6YT4juFxs9q7ObzfcKbNvOyDsaU7av4IHFXmn/JxfnBmUv
YxAI2Hx3xRb0KtG1JGkffQjVAtBboTXynLaQso/jj46ZOubIF8y6Ho3nTAv7Q6VH
kqSCdZClVu91zbHV9FFYQzJxjw1QgB0a4ItS4yhdmgl3oDNEcb3trQezrQ3/857/
ISqBGVLEbKHOu8H6zOLhxAgZ08ae1oQQQJowki0Ibd+LRLGovtEwLg8yyqiTIGve
7VFL2sRa8Z3rK9tlwKVH2kpFKNAeN3rfKFqr0/weR0cyKpmLMrSBTBZcxQcJCYF4
X6FO/32KOqcxJFIOKGVIUjvAvioOqoducw==

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

Trustpoint 'MIC_trustpoint' is a subordinate CA and holds a non self-signed cert.

Certificate has the following attributes:

Fingerprint MD5: AC14F08F C3780F8F D9EEE6C9 39111280

Fingerprint SHA1: 90B2E06B 7AD5DAFF CFD43187 2909F381 37471BF8

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

ISR_RA(config)# exit

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

ISR_RA# **configure terminal**
ISR_RA(config)# **crypto pki trustpoint MSCA**
ISR_RA(ca-trustpoint)# **enrollment mode ra**
ISR_RA(ca-trustpoint)# **enrollment url http://10.81.116.249/certsrv/mscep/mscep.dll**
ISR_RA(ca-trustpoint)# **serial-number**
ISR_RA(ca-trustpoint)# **fingerprint 81512B4316429092925C6891701B374EBD254447**
ISR_RA(ca-trustpoint)# **revocation-check none**
ISR_RA(ca-trustpoint)# **rsakeypair MSCA_Key 2048**
ISR_RA(ca-trustpoint)# **exit**
ISR_RA(config)# **crypto pki server MSCA**
ISR_RA(cs-server)# **grant auto trustpointMIC_trustpoint**
ISR_RA(cs-server)# **hash sha1**
ISR_RA(cs-server)# **mode ra transparent**
ISR_RA(cs-server)# **no shutdown**
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Re-enter password:
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 22 seconds)
Certificate has the following attributes:
Fingerprint MD5: CDE40276 04A28DA8 BDE5DF48 0BC1A8F7
Fingerprint SHA1: 81512B43 16429092 925C6891 701B374 EBD254447
Trustpoint Fingerprint: AE5CDEF2 A633DEF4 1D5A5104 7D6A8BD7 E08B576C
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.%
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: **ISR_RA**
% The serial number in the certificate will be: **<REMOVED>**
% Include an IP address in the subject name? [no]: **no**
Request certificate from CA? [yes/no]: **yes**
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose MSCA' command will show the fingerprint.
% Enrollment in progress...
ISR_RA(cs-server)#% Exporting Certificate Server signing certificate and keys...
Feb 17 15:21:42: CRYPTO_PKI: Certificate Request Fingerprint MD5: CDE40276 04A28DA8 BDE5DF48 0BC1A8F7
Feb 17 15:21:42: CRYPTO_PKI: Certificate Request Fingerprint SHA1: AE5CDEF2 A633DEF4 1D5A5104 7D6A8BD7 E08B576C
Feb 17 15:21:43: %PKI-6-CERTRET: Certificate received from Certificate Authority

Feb 17 15:21:48: %PKI-6-CS_ENABLED: Certificate server now enabled.
ISR_RA(cs-server)# **end**

Sample Configuration

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SCEP-RA
!
boot-start-marker
boot system flash c3845-advsecurityk9-mz.151-4.M10.bin
boot-end-marker
!
enable password <REMOVED>
!
aaa new-model
!
aaa authentication login default local
aaa authorization network PhoneList group radius
!
aaa session-id common
!
dot11 syslog
ip source-route
!
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
crypto pki server MSCA
 grant auto trustpoint MIC_trustpoint
 hash sha1
 mode ra transparent
crypto pki token default removal timeout 0
!
crypto pki trustpoint MIC_trustpoint
 enrollment terminal
 revocation-check none
 authorization list PhoneList
 authorization username subjectname commonname
!
crypto pki trustpoint MSCA
 enrollment mode ra
 enrollment url http://10.81.116.249:80/certsrv/mscep/mscep.dll
 serial-number
 fingerprint 81512B4316429092925C6891701B374EBD254447
 revocation-check none
 rsakeypair MSCA_Key 2048
!
crypto pki certificate chain MIC_trustpoint
 certificate ca 02
```

30820465 3082034D A0030201 02020102 300D0609 2A864886 F70D0101 0B050030
2B310E30 0C060355 040A1305 43697363 6F311930 17060355 04031310 43697363
6F20526F 6F742043 41204D32 301E170D 31323131 31323133 35303538 5A170D33
37313131 32313330 3031375A 3036310E 300C0603 55040A13 05436973 636F3124
30220603 55040313 1B436973 636F204D 616E7566 61637475 72696E67 20434120
53484132 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A
02820101 00F4364B 42023267 DE493DF2 153BC145 69E9094E 16B948B4 471EE82A
5B7D8A5E 2DD51E65 DB80A3E4 B4A2DCD3 949C12D8 194C859B 5A72EF6F 5297E65B
DC3B9D0A 3DCD54F7 7B23EE84 5FFAFFD4 C4755067 EF9CDBE4 27D5F84E A577E7C7
9EE3E217 206EF870 C3251777 EF73A9FB DE7B21DA 16C8FBC3 F211D1D4 7246149D
C924A060 D1449C2F 8242C257 AEF7C5EA FF23E502 A0611316 BB6B6FDF A9299903
4BD9206D 5B05F599 63C66D49 E4F12A0D DE5B29D5 FB112569 B1EA4C33 1859FFB6
A1BB3860 1E6520D4 DB6201F2 4444CFE9 3F17AFA4 ED0F4877 EB9E0E50 7716FB59
9E06EFE3 72D96E30 AA697928 D5B6BA1F E6FB7EA5 B9028348 900008EC 2F4A9CCD
3DF268D5 EF020301 0001A382 01873082 0183300E 0603551D 0F0101FF 04040302
01063012 0603551D 130101FF 04083006 0101FF02 0100305C 0603551D 20045530
53305106 0A2B0601 04010915 01120030 43304106 082B0601 05050702 01163568
7474703A 2F2F7777 772E6369 73636F2E 636F6D2F 73656375 72697479 2F706B69
2F706F6C 69636965 732F696E 6465782E 68746D6C 301D0603 551D0E04 1604147A
D77995CA BB482BB8 5514FDA3 C00FBCA7 0F961930 41060355 1D1F043A 30383036
A034A032 86306874 74703A2F 2F777777 2E636973 636F2E63 6F6D2F73 65637572
6974792F 706B692F 63726C2F 63726361 6D322E63 726C307C 06082B06 01050507
01010470 306E303E 06082B06 01050507 30028632 68747470 3A2F2F77 77772E63
6973636F 2E636F6D 2F736563 75726974 792F706B 692F6365 7274732F 63726361
6D322E63 6572302C 06082B06 01050507 30018620 68747470 733A2F2F 746F6F6C
732E6369 73636F2E 636F6D2F 706B692F 6F637370 301F0603 551D2304 18301680
14C900F9 1F8A1FC2 66BDA5D2 6D650E22 2E34C305 A0300D06 092A8648 86F70D01
010B0500 03820101 00735936 AC7E984F 88EE171B 3DABB39B CDF70A6C DBCEC83B
1A53B6AF E081C55E 69FF2717 E706652F 631008D8 7C77C516 F42AD1B5 24691F7D
08D502D0 5BA135F2 9CB690B2 8FE38F8E 993AE6C8 17CCBA1E 8DE74C0B FB43A547
92A48275 90A556EF 75CDB1D5 F4515843 32718F0D 50801D1A E08B52E3 285D9A09
77A03344 71BDEDAD 07B3AD0D FFF39EFF 212A8119 52C46CA1 CEBBC1FA CCE2E1C4
0819D3C6 9ED68410 409A3092 2D086DDF 8B44B1A8 BED1302E 0F32CAA8 93206BDE
ED514BDA C45AF19D EB2BDB65 C0A547DA 4A4528D0 1E377ADF 285AABD3 FC1E4747
322A998B 32B4814C 165CC507 09098178 5FA14EFF 7D8A3AA7 3124520E 28654852
3BC0BE2A 0EAA876E 73
quit
crypto pki certificate chain MSCA
certificate 4F35C0050000000002F8
308205FF 308204E7 A0030201 02020A4F 35C00500 00000002 F8300D06 092A8648
86F70D01 010B0500 30593113 3011060A 09922689 93F22C64 01191603 636F6D31
15301306 0A099226 8993F22C 64011916 0579646E 65743117 3015060A 09922689
93F22C64 01191607 79642D6D 73636131 12301006 03550403 13097969 6368756E
2D434130 1E170D31 36303532 34323333 3333385A 170D3136 30373035 32333333
33385A30 2E311430 12060355 0405130B 46545831 32343441 32484131 16301406
092A8648 86F70D01 09021307 53434550 2D524130 82012230 0D06092A 864886F7
0D010101 05000382 010F0030 82010A02 82010100 F3679949 C1F3E530 C4CF0C9B
D20F82FE 7959ABAC AE40DF8E 16783930 E91D50BA B31E8DAB 8264BF8E B929A3D3
7CC284FB CE81306B A396D5B9 F5D12AD2 7508A000 36F95EDC 3DA8749D 9752B869
C799D0E7 1896DD83 56FE89B9 DF333CC9 0A480AB2 BF4FFCB9 8E407880 01C055BE
8A98F9E4 6C2026AC 34B1F52D FC1DD7A8 FC89CC97 0CE71A6D 9CBF6280 728230E6
A5866A09 7FE181ED 6B2EB712 BD34C3F3 8A1C3EDD 05E8AF0C 09D1476A 0CB47150
A7CC2BBE EEE35F30 193F893D 530F110C EB2BFE68 7D69FA54 2CAD61FE 41900DE9
7FEACFAB DCF72D2F EED90BB4 1E03F1E3 B5472BCD 2B0B3D37 4E1CC375 34C66C49
6BD821AA 2F9165BF 22B9E4B7 C8DB9061 C920FA5D 02030100 01A38202 F2308202
EE300E06 03551D0F 0101FF04 04030205 A0301D06 03551D0E 04160414 986F9130
BCF33BE4 79317708 ECE4E226 9F6A7E0A 301F0603 551D2304 18301680 14769747

5B67C892 C5DF1F03 06D761CA 3ACC560B 603081D5 0603551D 1F0481CD 3081CA30
81C7A081 C4A081C1 8681BE6C 6461703A 2F2F2F43 4E3D7969 6368756E 2D43412C
434E3D59 442D4D53 43412D57 324B382C 434E3D43 44502C43 4E3D5075 626C6963
2532304B 65792532 30536572 76696365 732C434E 3D536572 76696365 732C434E
3D436F6E 66696775 72617469 6F6E2C44 433D7964 2D6D7363 612C4443 3D79646E
65742C44 433D636F 6D3F6365 72746966 69636174 65526576 6F636174 696F6E4C
6973743F 62617365 3F6F626A 65637443 6C617373 3D63524C 44697374 72696275
74696F6E 506F696E 743081C4 06082B06 01050507 01010481 B73081B4 3081B106
082B0601 05050730 028681A4 6C646170 3A2F2F2F 434E3D79 69636875 6E2D4341
2C434E3D 4149412C 434E3D50 75626C69 63253230 4B657925 32305365 72766963
65732C43 4E3D5365 72766963 65732C43 4E3D436F 6E666967 75726174 696F6E2C
44433D79 642D6D73 63612C44 433D7964 6E65742C 44433D63 6F6D3F63 41436572
74696669 63617465 3F626173 653F6F62 6A656374 436C6173 733D6365 72746966
69636174 696F6E41 7574686F 72697479 30150603 551D1101 01FF040B 30098207
53434550 2D524130 3E06092B 06010401 82371507 0431302F 06272B06 01040182
37150887 D0FB2482 F5B91683 ED970E82 C2E50087 B2F57E81 0C81839C 39868BB0
09020164 02010430 29060355 1D250422 30200608 2B060105 05070302 06082B06
01050507 0304060A 2B060104 0182370A 03043035 06092B06 01040182 37150A04
28302630 0A06082B 06010505 07030230 0A06082B 06010505 07030430 0C060A2B
06010401 82370A03 04304406 092A8648 86F70D01 090F0437 3035300E 06082A86
4886F70D 03020202 0080300E 06082A86 4886F70D 03040202 00803007 06052B0E
03020730 0A06082A 864886F7 0D030730 0D06092A 864886F7 0D01010B 05000382
0101002A DE5C497F 48C03272 3EF18668 C86A28AA 075ADDA0 14CD4741 A3436095
F3B80053 07A6F2C5 02D116F7 D95C8B1B 9D6722E4 2DF4A074 DE705C8B 561BD450
08E36D0E 68234021 6A47137F 7EBB5341 609A6EBC EF1D1732 42AE2C78 1D5D14EC
561CE4F6 E6054DFE 4CD262C3 5FDD276D 9D101A49 C6423D94 31D2BD9A 8DB0261D
39FB0767 711E3142 85B09135 70207D91 3DA00878 CA4D8890 73D790F8 1C905389
BB129BC1 0DE4B8CA 6B008913 DD9F5E96 DBD3051E 98BA689E E3D32B86 15E5A162
B1C69135 EF9982E6 5BC60BA6 17DBB8BF 5319CF3E 3793F494 C507D2FD B7AC7499
43D43722 ADC22571 FEF9D0C1 5233023E 5B5EB92F AF35F2A7 A953B7F3 6E228A1F 9D09A2
quit
certificate ca 1E2F4A24A762A0A9456EC2983E7F6D1D
308203A5 3082028D A0030201 0202101E 2F4A24A7 62A0A945 6EC2983E 7F6D1D30
0D06092A 864886F7 0D01010B 05003059 31133011 060A0992 268993F2 2C640119
1603636F 6D311530 13060A09 92268993 F22C6401 19160579 646E6574 31173015
060A0992 268993F2 2C640119 16077964 2D6D7363 61311230 10060355 04031309
79696368 756E2D43 41301E17 0D313431 31323530 33333033 315A170D 32393131
32353033 34303330 5A305931 13301106 0A099226 8993F22C 64011916 03636F6D
31153013 060A0992 268993F2 2C640119 16057964 6E657431 17301506 0A099226
8993F22C 64011916 0779642D 6D736361 31123010 06035504 03130979 69636875
6E2D4341 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A
02820101 008C280C 3896265F 1CF3BE24 89CC87A8 8DDD2674 5C0C53D5 0903B64A
D9D184C7 FB25114F 8D97F477 1E555923 3170B999 FC1DB0A0 B73DBBFA AD742BFA
77C69924 0F89FCA3 72B12430 753CA6E9 53992989 845EE0AC 26F2A3CF 2A1C0E6D
68983231 1FB8F71C 878E4A4F 6828F6D5 E6FE03AD 6A09CEE7 0458AE7E 1E83D2DB
66CF9DDB B6E7C32F BA88675B 65A39F13 F6C26B5A 692E14B2 7149C470 F06687C9
DA27BA7D 68F68CDC 43406E1D 25D013ED CC37C38C 268BFD53 460539E7 FF75AC24
FB210259 3AC480AA 75CCFA00 98B423F8 4BCC0297 ECD4E4F7 0A3F41E5 97086DEA
8FD818EB 01E5FF66 D984A379 9298FFEC 65DD902C A7757358 0AECDA0B D794E150
5237FBBE F5020301 0001A369 30673013 06092B06 01040182 37140204 061E0400
43004130 0E060355 1D0F0101 FF040403 02018630 0F060355 1D130101 FF040530
030101FF 301D0603 551D0E04 16041476 97475B67 C892C5DF 1F0306D7 61CA3ACC
560B6030 1006092B 06010401 82371501 04030201 00300D06 092A8648 86F70D01
010B0500 03820101 007D4DAD 1170BBD8 2D9A2FB5 4B2B6A52 ECF5AF2B 4AB7D9D7
EACA3085 7083958A 49ED5EC1 3331E97F 6DD88E2F 40C3968F AB6CBB86 86A8402A
5940CC72 1B1AB153 572443CA B2FF8AB4 730A0206 9359D9E3 6DFF8B47 B3AE34ED
B007C8B2 0E126243 C32FCFB6 7BF76A1B 7233D92E 4336BEB8 D9672598 ABE97BD3

```
  AE4949D1 97B6A380 08AC4ABB 23A30B34 27A0A112 C63D6BFD 476C4F4B 2DBBB200
  D5BDF499 F5068067 85123637 E3EBF106 7D2AF2D0 87DCF856 34E937BF 246C41BD
  C0781E14 A22BCC66 2151F46B 5AD4314C 345E8871 41830E80 5D5A8416 21C5220D
  409449E6 E2161582 2113833C 982B68AE 1B5E206E BC535C5B A28E1210 E7FB5296
  27DB54AF 20A3FA02 5A
       quit
!
license udi pid CISCO3845-MB sn <REMOVED>
archive
 log config
  hidekeys
username <REMOVED>privilege 15 password 0 <REMOVED>
!
redundancy
!
interface GigabitEthernet0/0
 ip address 10.195.19.65 255.255.255.128
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
ip default-gateway 10.195.19.1
ip forward-protocol nd
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.195.19.1
!
radius server MyRadius
 address ipv4 10.195.19.63 auth-port 1812 acct-port 1813
 key <REMOVED>
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 transport input all
line vty 5 15
 exec-timeout 0 0
 transport input all
!
scheduler allocate 20000 1000
end
```

Certificate Removal

Certificates can be removed either via the admin webpage interface or via the local user interface.

To remove a certificate via the admin webpage, select **Delete** for the corresponding certificate, then restart the phone once a certificate has been removed.

Bluetooth Settings

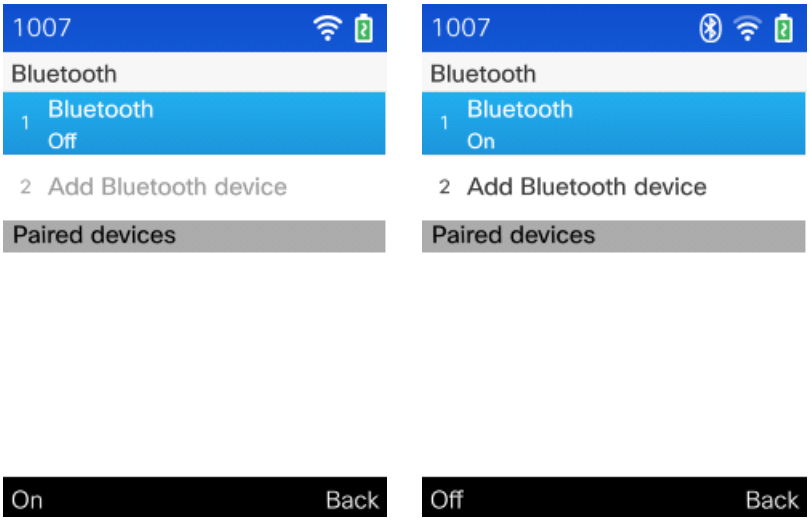
The Cisco Wireless IP Phone 8821 and 8821-EX include Bluetooth support, which enables hands-free communications.

To pair a Bluetooth headset to the Cisco Wireless IP Phone 8821 and 8821-EX, follow the instructions below.

- Navigate to **Settings** > **Bluetooth**.
- Ensure that **Bluetooth** is set to **On**.

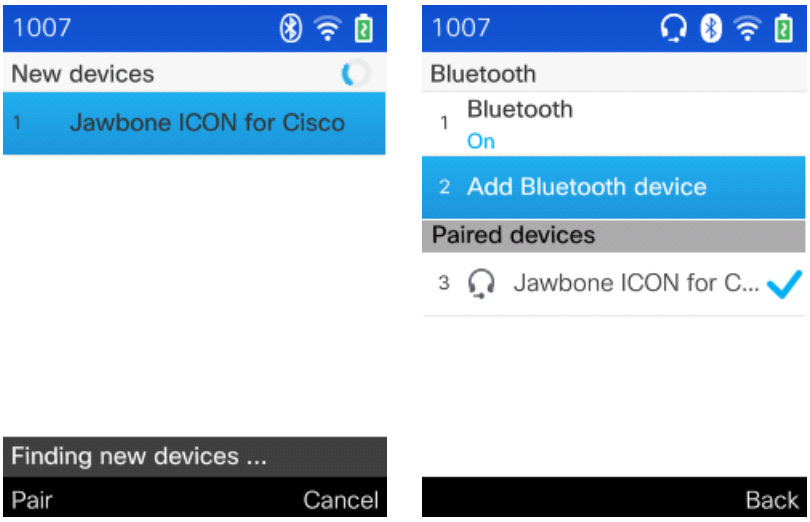
  Ensure **Bluetooth** is enabled in the Cisco Unified Communications Manager.
- Select **Add Bluetooth device**.

  Ensure the Bluetooth device is in pairing mode.

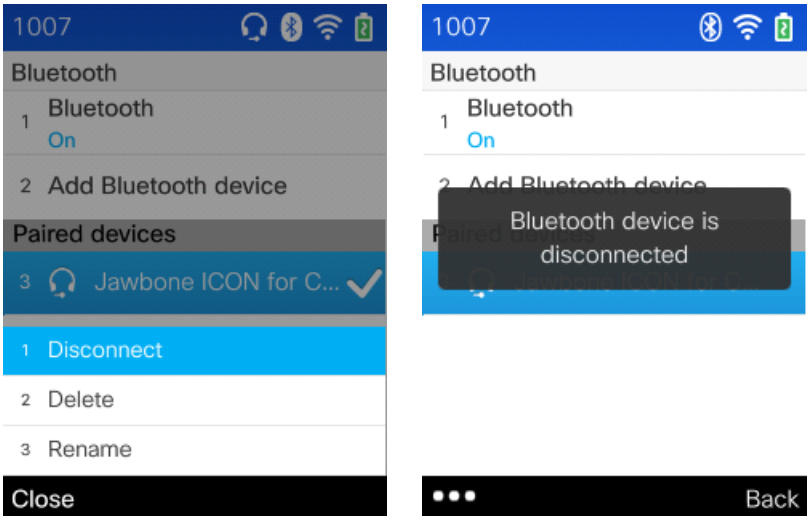


- Select the Bluetooth device after it is displayed in the list.

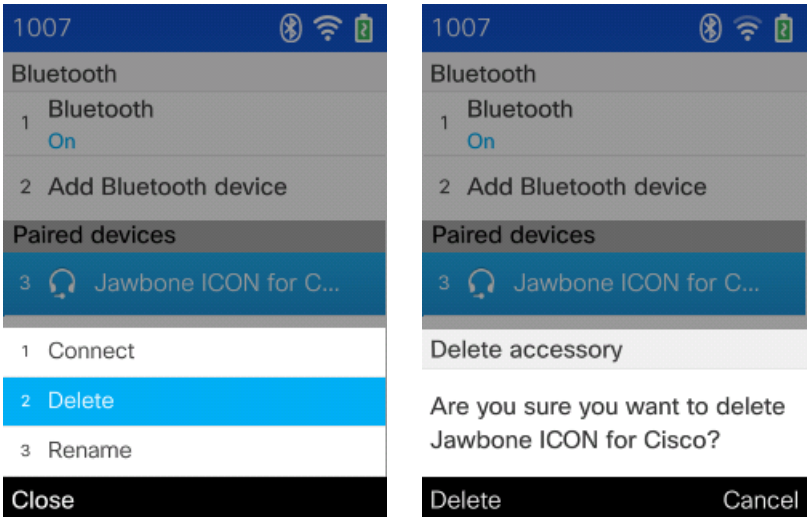
- The Cisco Wireless IP Phone 8821 and 8821-EX will then attempt to pair automatically with the Bluetooth device. If unsuccessful, enter the pin code when prompted.
- Once paired, then the Cisco Wireless IP Phone 8821 and 8821-EX will attempt to connect to the Bluetooth device.



- Selecting the Bluetooth device then selecting **Disconnect** will disconnect that currently connected Bluetooth device.



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



Local Contacts

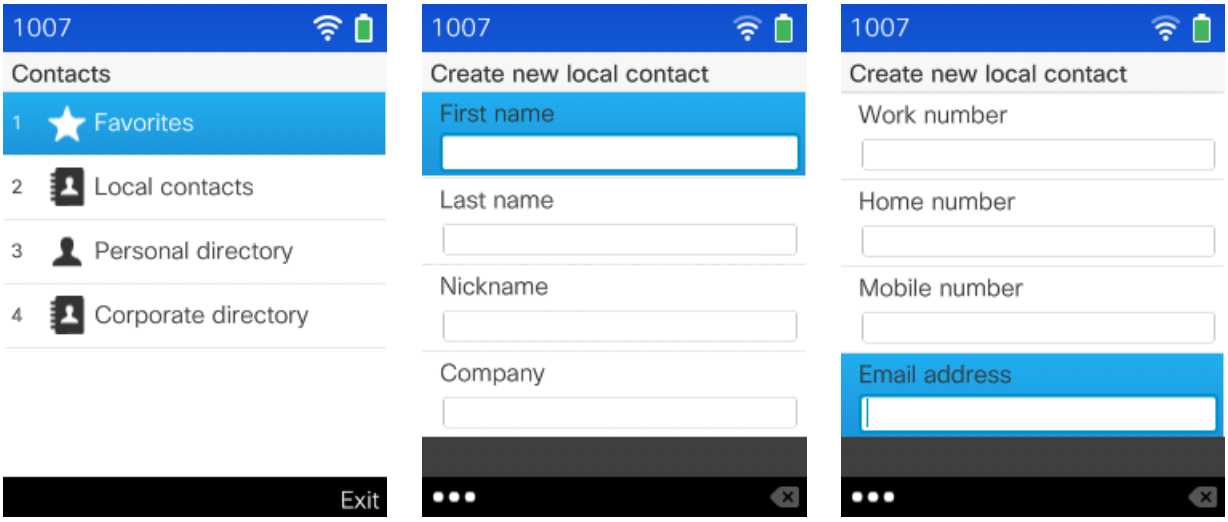
As of the 11.0(4) release, the Cisco Wireless IP Phone 8821 Series contains local phone book support.

Local Contacts and **Favorites** can be used to quickly access frequently dialed #s.

Up to 200 **Local Contacts** and 50 **Favorites** can be configured.

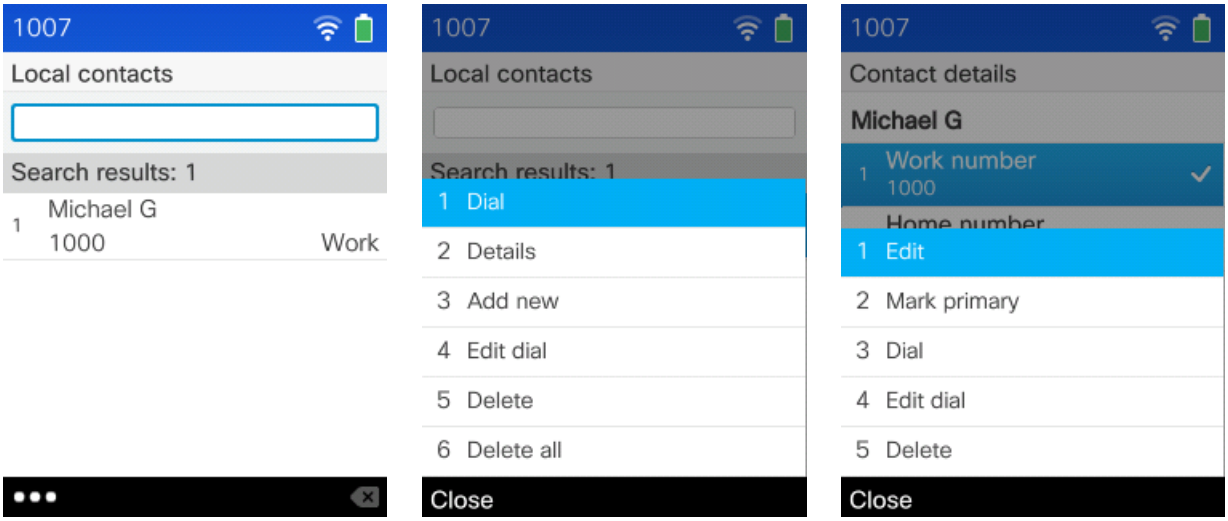
Can add **Local Contacts** either individually via the keypad or in bulk via the phone's admin webpage.
Either **First name** or **Last name** and at least one number are required to be entered.

When the data has been entered, select the left softkey then **Save**.



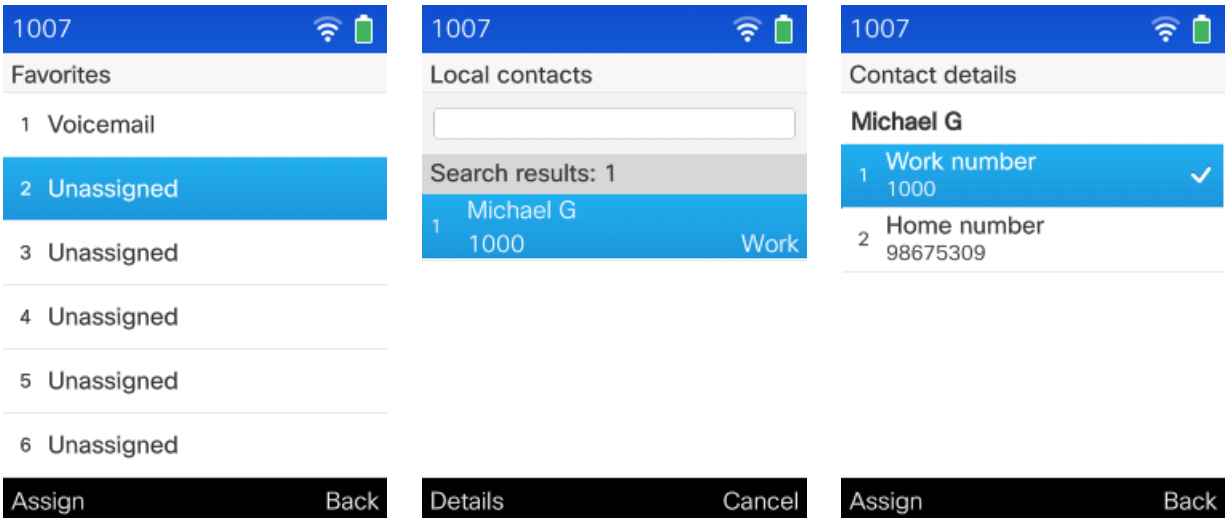
Can press the green button or **Dial** softkey when a **Local Contacts** entry is highlighted to dial that primary number.

Select the left softkey then **Details** to see the info for the highlighted entry.

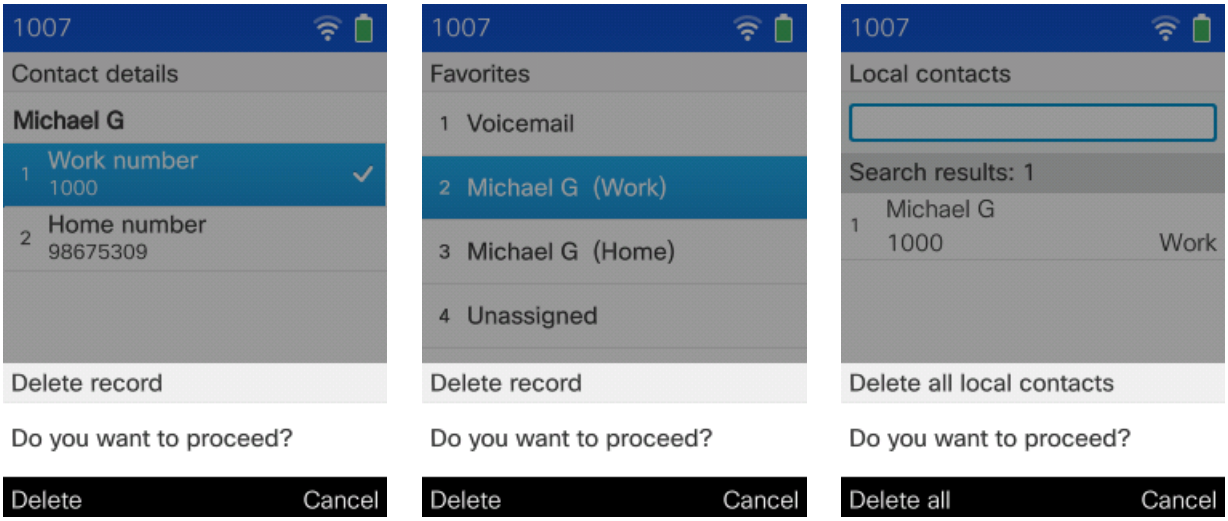


Can add **Favorites** either individually via the keypad or in bulk via the phone's admin webpage.
Can press the green button when a **Favorites** slot # is highlighted to dial that number.

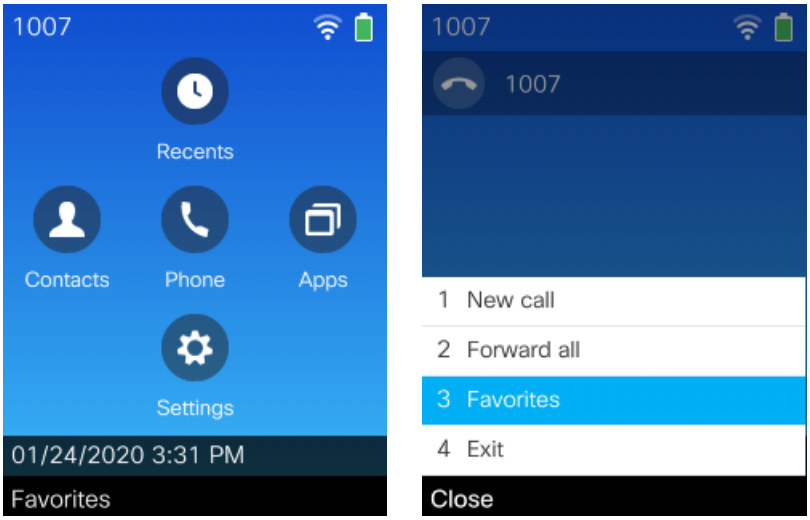
From the home screen, can press and hold the Favorite slot # to dial that associated Favorite # (for a 2 digit Favorite #, enter the first digit then press and hold the last digit).



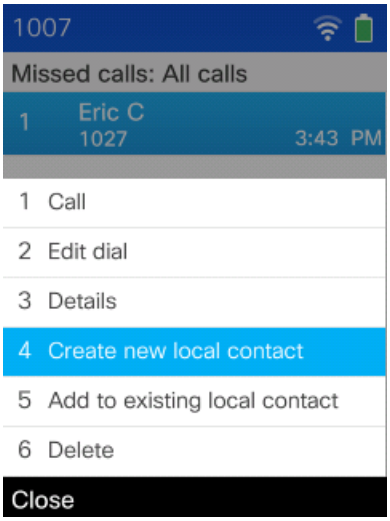
Can delete **Local Contacts** and **Favorites** either individually or in bulk via the keypad or in bulk via the phone's admin webpage.
Selecting **Delete All** in **Local Contacts** will also clear all assigned **Favorites** as well.

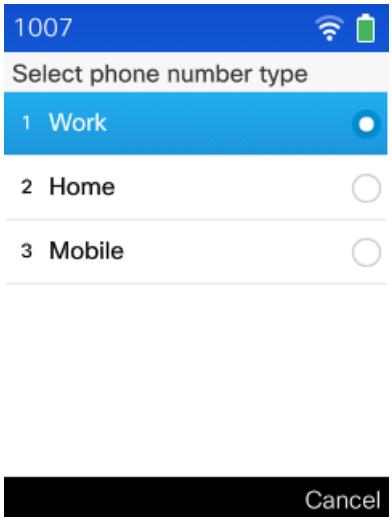


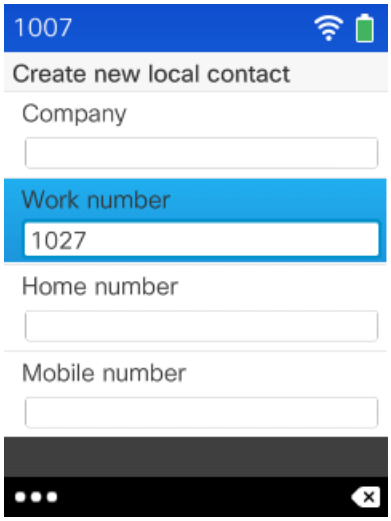
The 11.0(5) release enables access to **Favorites** via the left softkey on the home screen or in line view for quicker access to frequently dialed numbers.

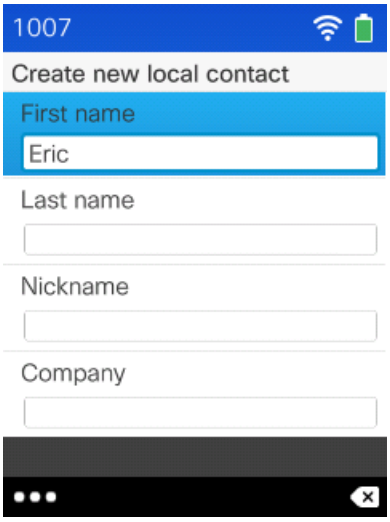


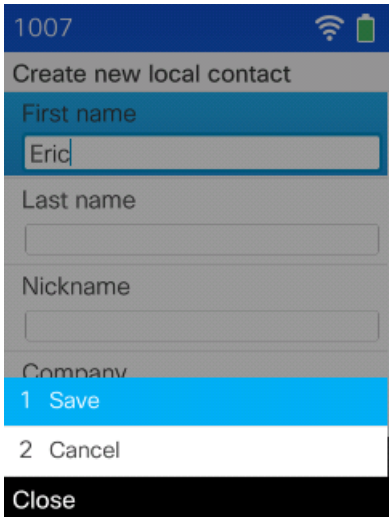
The 11.0(5) release enables the capability to create a new local contact or add to an existing local contact for a recently received call, missed call, or placed call via the **Recents** menu.

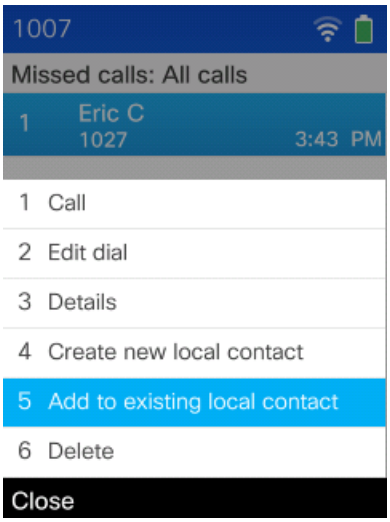

1007
Missed calls: All calls
1 Eric C
1027
3:43 PM
1 Call
2 Edit dial
3 Details
4 Create new local contact
5 Add to existing local contact
6 Delete
Close

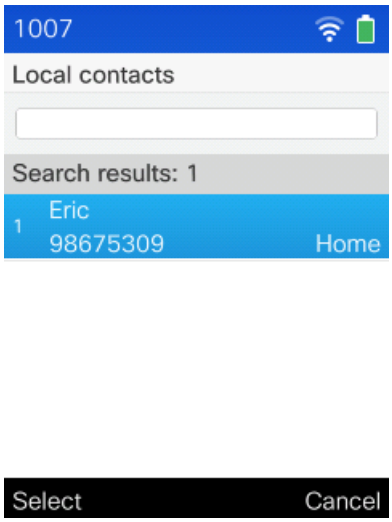

1007
Select phone number type
1 Work
2 Home
3 Mobile
Cancel

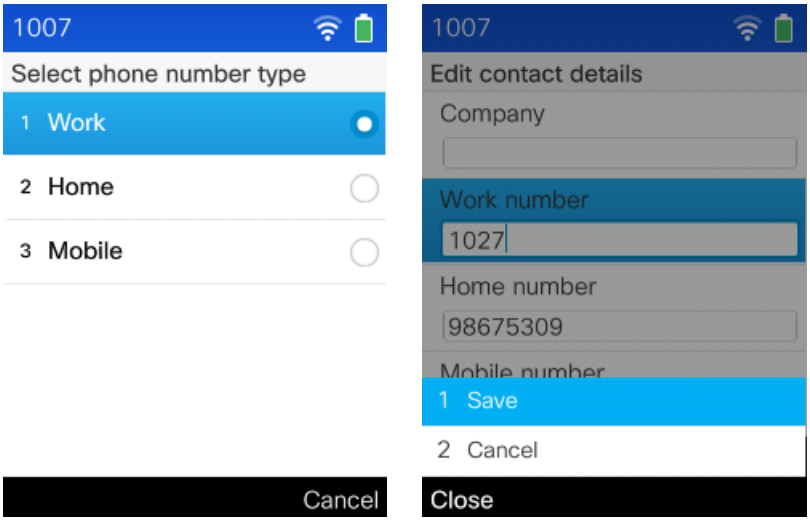

1007
Create new local contact
Company
Work number
1027
Home number
Mobile number


1007
Create new local contact
First name
Eric
Last name
Nickname
Company


1007
Create new local contact
First name
Eric
Last name
Nickname
1 Save
2 Cancel
Close


1007
Missed calls: All calls
1 Eric C
1027
3:43 PM
1 Call
2 Edit dial
3 Details
4 Create new local contact
5 Add to existing local contact
6 Delete
Close

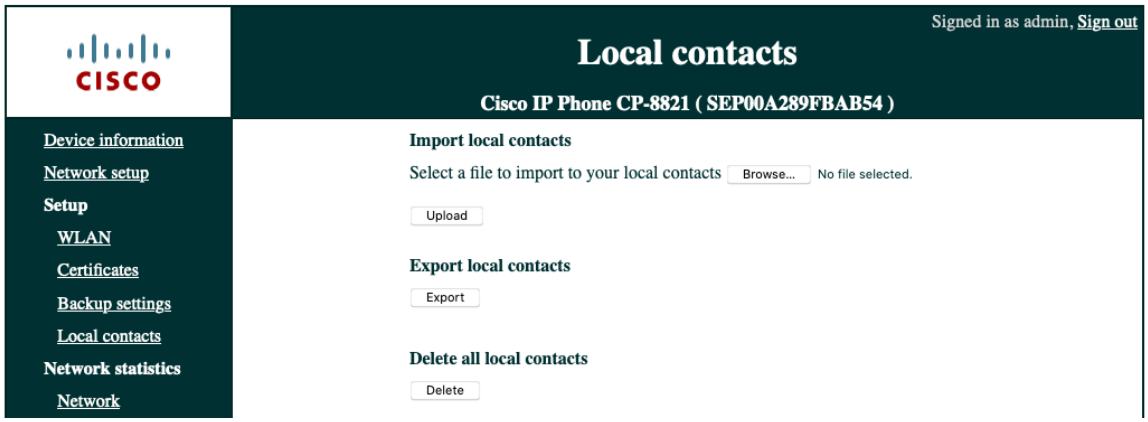

1007
Local contacts
Search results: 1
1 Eric
98675309
Home
Select
Cancel



To access **Import**, **Export**, and **Delete All** options via the admin webpage ensure **Web Admin** is set to **Enabled** and an **Admin Password** is configured.

Local Contacts and **Favorites** can be imported, exported, and removed from the phone's admin webpage when **Web Admin** is **Enabled** (https://x.x.x.x:8443).

Local Contacts and **Favorites** can be imported and exported in CSV format only.



Use the following CSV format to import **Local Contacts** and **Favorites**.

For **Work number**, **Home number**, **Mobile number**, enter the exact number to be dialed from the phone.

For **Work primary**, **Home primary**, **Mobile primary**, configure only one of these values to be **true**, where the other two are configured as **false**.

For **Work favorite**, **Home favorite**, **Mobile favorite**, configure the Favorite slot # for any numbers to be added to Favorites (e.g. enter 2 for **Work** favorite to map the **Work number** to Favorite slot #2; Favorite slot # 1 is reserved for voicemail).

Sample CSV Format

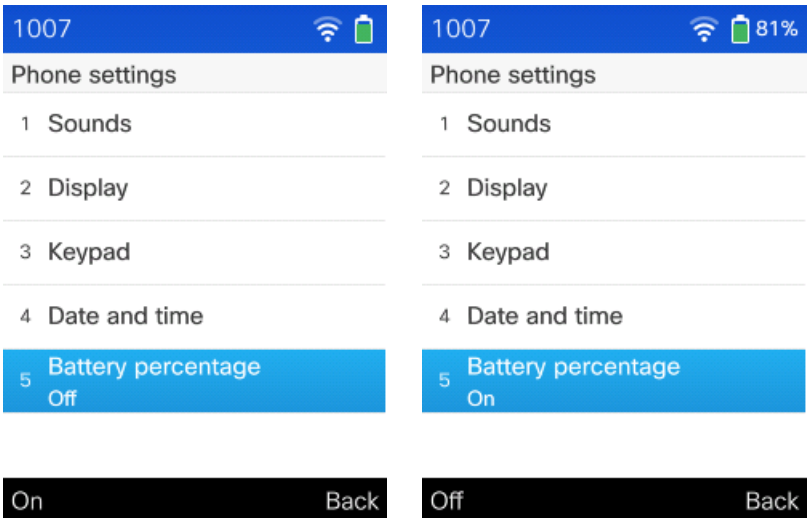
First name, Last name, Nickname, Company, Work number, Home number, Mobile number, Email address, Work primary, Home primary, Mobile primary, Work favorite, Home favorite, Mobile favorite
Michael,G,,Cisco,1000,98675309,,michael@cisco.com,true,false,false,2,3,

Battery Status

With the 11.0(5) release, the Cisco Wireless IP Phone 8821 Series has the capability to display the battery status as a percentage.

By default, the battery percentage is **Off**, but can be set to **On** by selecting **Settings** > **Phone settings** > **Battery percentage**.

When charging while powered off, the battery status percentage will be displayed regardless of the configuration in Settings.



Upgrading Firmware

Cisco Unified Communications Manager

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

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

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 IP Phone 8821 or 8821-EX then downloads the firmware files to flash if it is not running the specified image already.

The Load Server can be specified as an alternate TFTP server to retrieve firmware files, which is located in the product specific configuration section of Cisco Wireless IP Phone 8821 and 8821-EX within Cisco Unified Communications Manager Administration. Download the firmware in ZIP file format, extract the contents, then copy those files to the load server.

Cisco Unified Communications Manager Express

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

Example:

```
tftp-server flash:/8821/sip8821.11-0-6SR5-5.loads alias sip8821.11-0-6SR5-5.loads
tftp-server flash:/8821/dtblob8821.HE-01-011.sbn alias dtblob8821.HE-01-011.sbn
tftp-server flash:/8821/fbi8821.HE-01-014.sbn alias fbi8821.HE-01-014.sbn
tftp-server flash:/8821/kern8821.11-0-6SR5-5.sbn alias kern8821.11-0-6SR5-5.sbn
tftp-server flash:/8821/rootfs8821.11-0-6SR5-5.sbn alias rootfs8821.11-0-6SR5-5.sbn
tftp-server flash:/8821/sb28821.HE-01-024.sbn alias sb28821.HE-01-024.sbn
tftp-server flash:/8821/vc48821.11-0-6SR5-5.sbn alias vc48821.11-0-6SR5-5.sbn
!
voice register global
 load 8821 sip8821.11-0-6SR5-5
```

IP Phone Services

The Cisco Wireless IP Phone 8821 and 8821-EX are capable of supporting Extensible Markup Language (XML) applications.

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

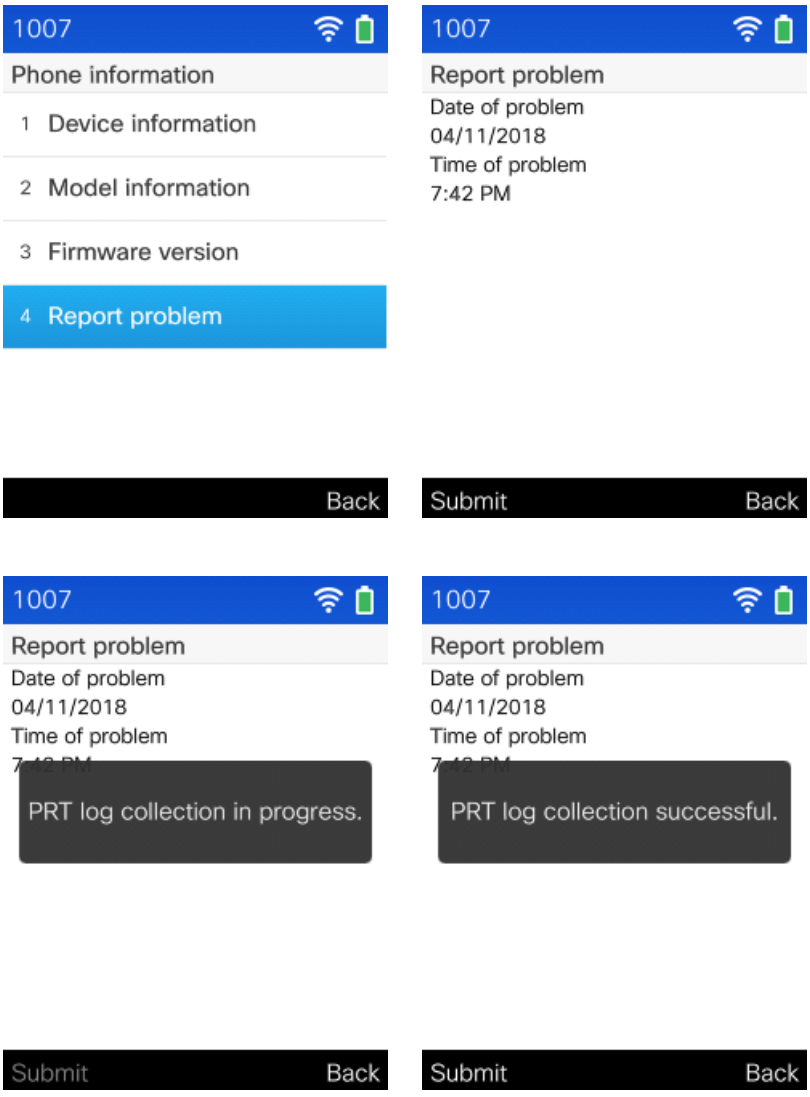
Troubleshooting

Problem Report Tool

Local User Interface

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

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 **Console Logs**.



With the 11.0(5) release a Problem Report Tool (PRT) log can also be generated via the admin webpage (https://x.x.x.x:8443) at **Device logs** > **Console logs** by selecting **Report problem**.

Extensible Markup Language (XML)

The 11.0(5) release enables the capability to generate a Problem Report Tool (PRT) via XSI commands.

- Use the following XSI command to submit a PRT log generation request.

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="Device:GeneratePRT"/>
</CiscoIPPhoneExecute>
```

- If there is no pending PRT log collection in process, then the request was successful and return the following.

```
<CiscoIPPhoneResponse>
  <ResponseItem URL="Device:GeneratePRT" Data="Success" Status="0"/>
</CiscoIPPhoneResponse>
```

- If there is a pending PRT log collection in process, then the request will fail and return the following.

```
<CiscoIPPhoneResponse>
  <ResponseItem URL="Device:GeneratePRT" Data="There is pending PRT" Status="6"/>
</CiscoIPPhoneResponse>
```

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 IP Phone 8821 and 8821-EX information can be gathered remotely by accessing the phone's standard or admin webpage interfaces.

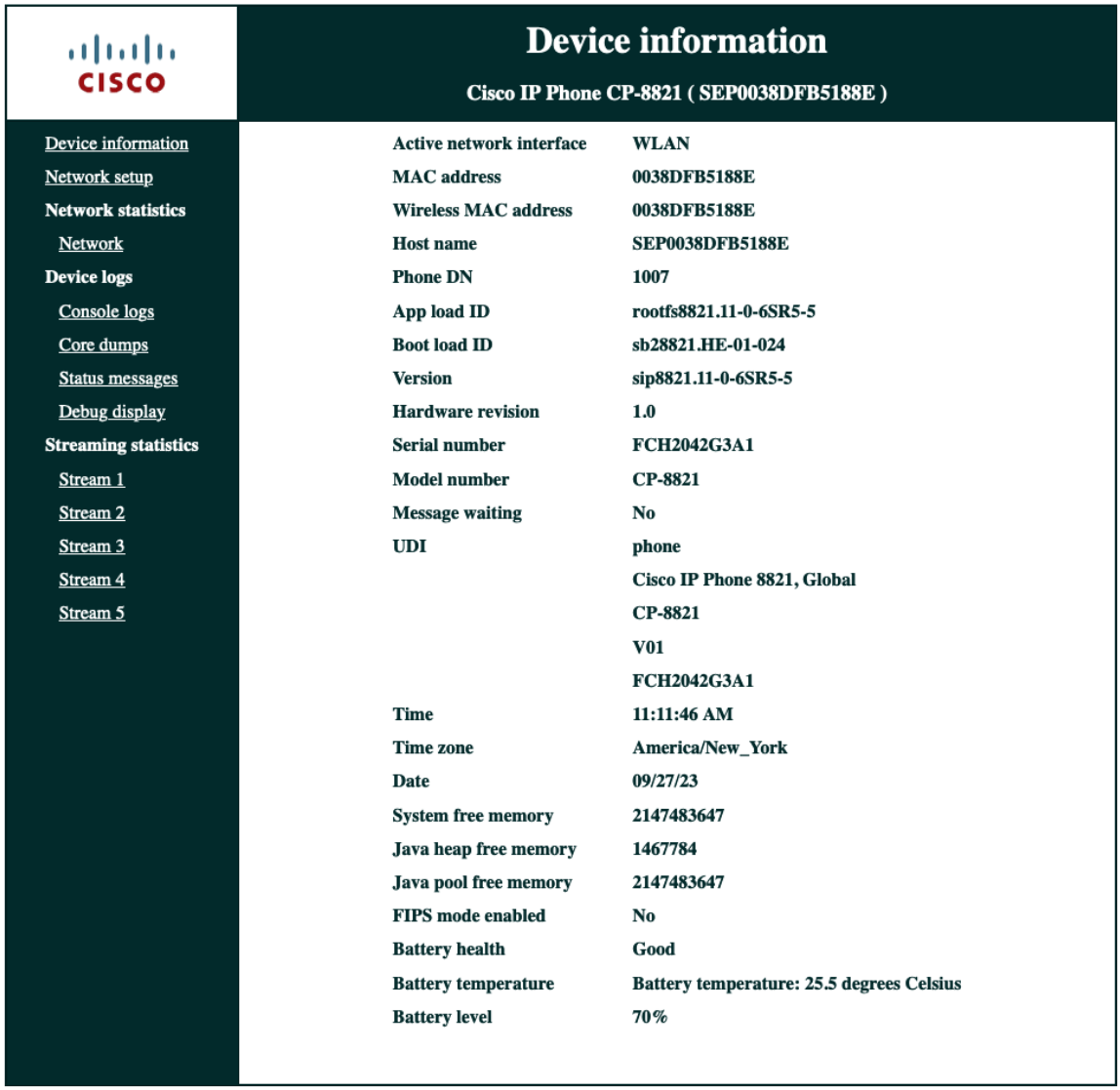
The standard webpage interface (https://x.x.x.x) contains read-only information regarding device information, network setup, streaming statistics, device logs etc. To access the standard webpage interface, **Web Access** must be enabled in Cisco Unified Communications Manager.

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

Device Information

The Cisco Wireless IP Phone 8821 and 8821-EX provide device information, where network status, MAC address and version information is displayed.

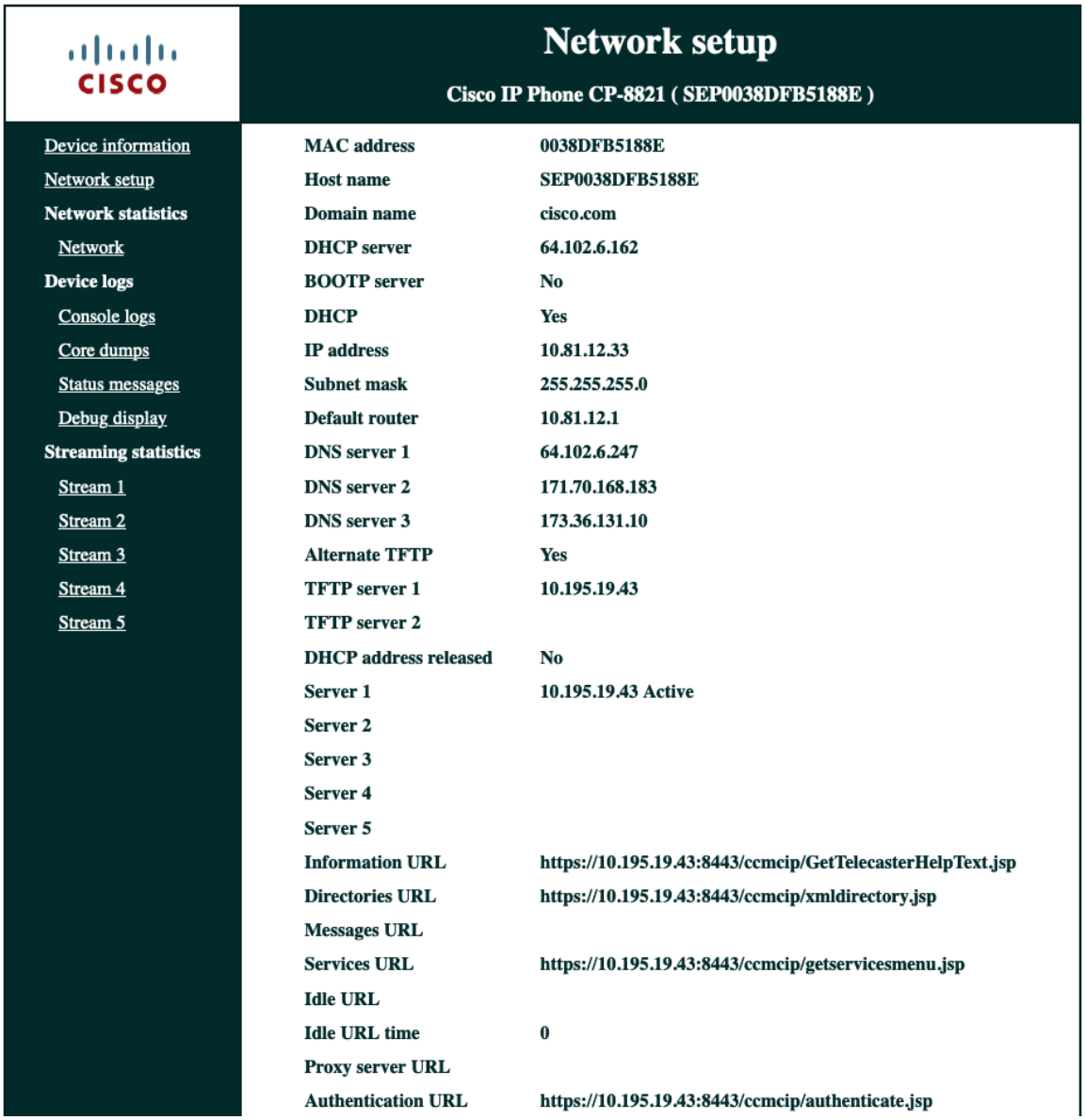
Browse to the standard web interface (https://x.x.x.x) of the Cisco Wireless IP Phone 8821 or 8821-EX then select **Device information** to view this information.



Network Setup

The Cisco Wireless IP Phone 8821 and 8821-EX provide network setup information, where network information is displayed.

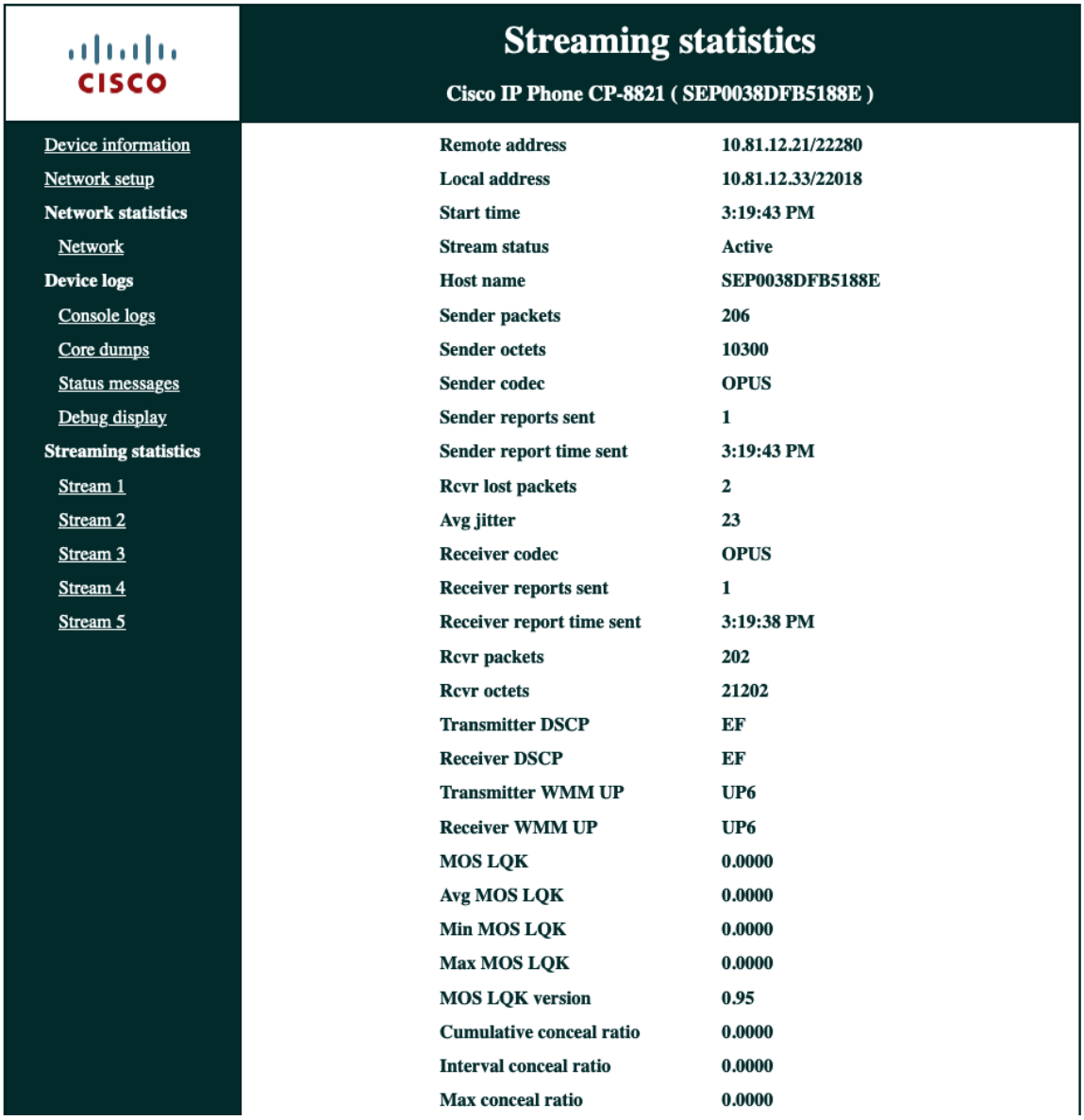
Browse to the standard web interface (https://x.x.x.x) of the Cisco Wireless IP Phone 8821 or 8821-EX then select **Network setup** to view this information.



Streaming Statistics

The Cisco Wireless IP Phone 8821 and 8821-EX provide call statistic information, where codec type, jitter and packet count info, etc. is displayed.

Browse to the standard web interface (https://x.x.x.x) of the Cisco Wireless IP Phone 8821 or 8821-EX then select the necessary menu item under **Streaming statistics** to view this information.

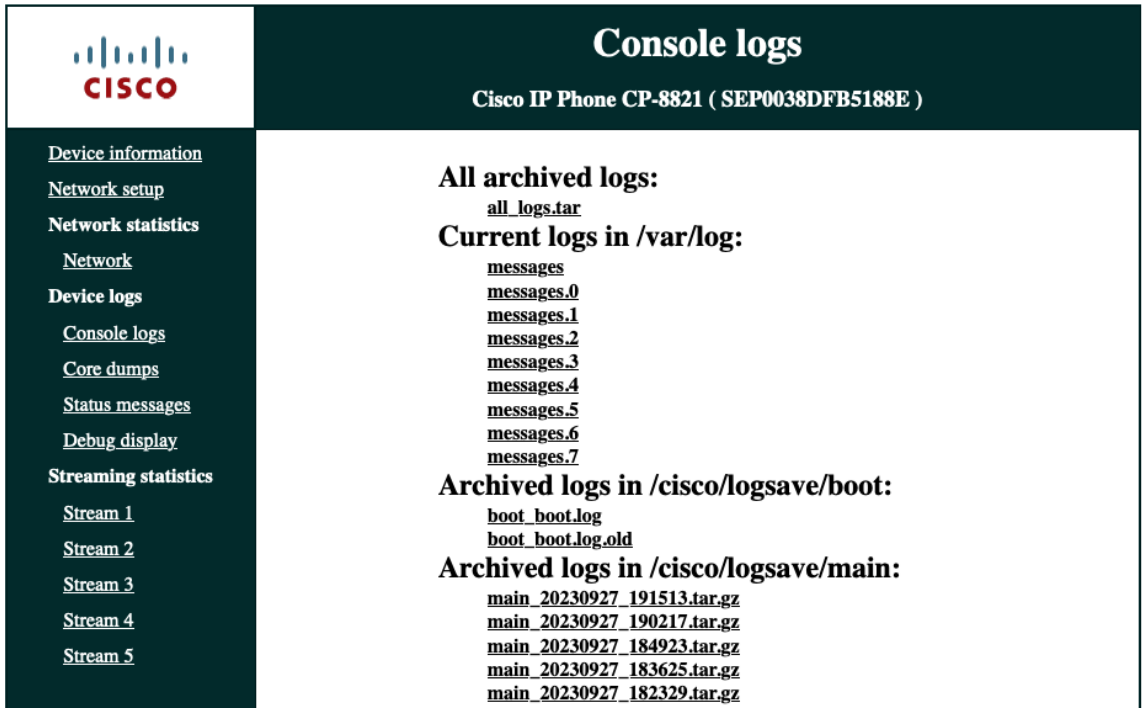


Device Logs

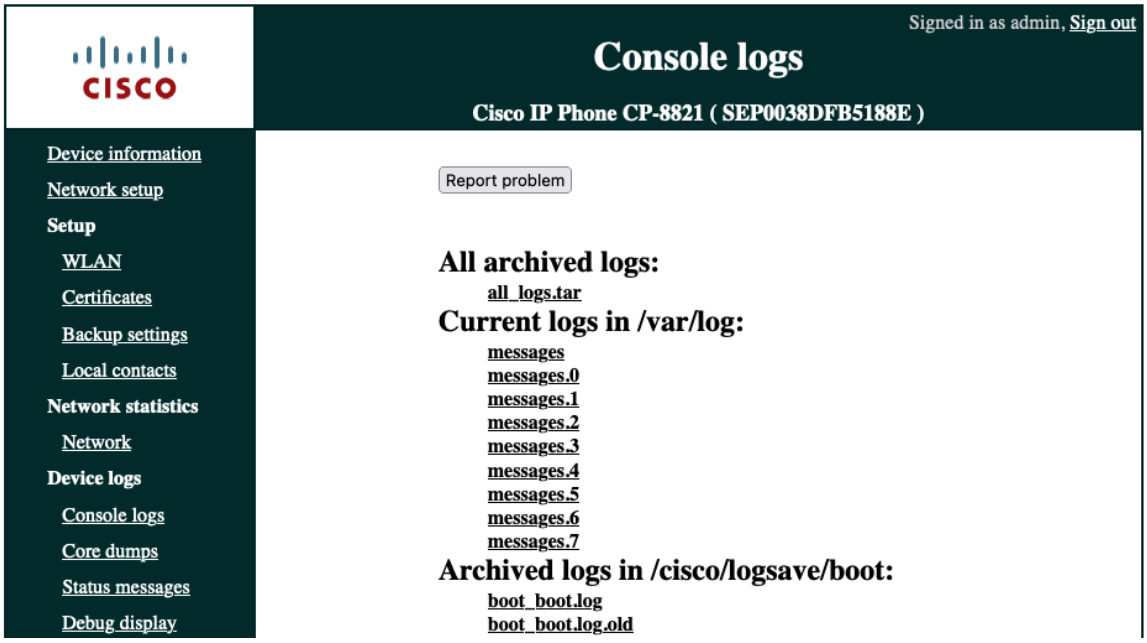
Console logs, core dumps, status messages, and debug display can be obtained from the web interface of Cisco Wireless IP Phone 8821 or 8821-EX for troubleshooting purposes.

Console Logs

Browse to the standard web interface (https://x.x.x.x) of the Cisco Wireless IP Phone 8821 or 8821-EX then select **Console Logs** to view this information.



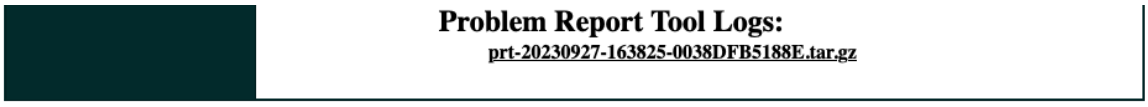
The 11.0(5) release enables the capability to generate a Problem Report Tool (PRT) log via the admin webpage (https://x.x.x.x:8443) at **Device logs** > **Console logs** by selecting **Report problem**.



PRT collection in progress will be displayed after **Report problem** has been selected.

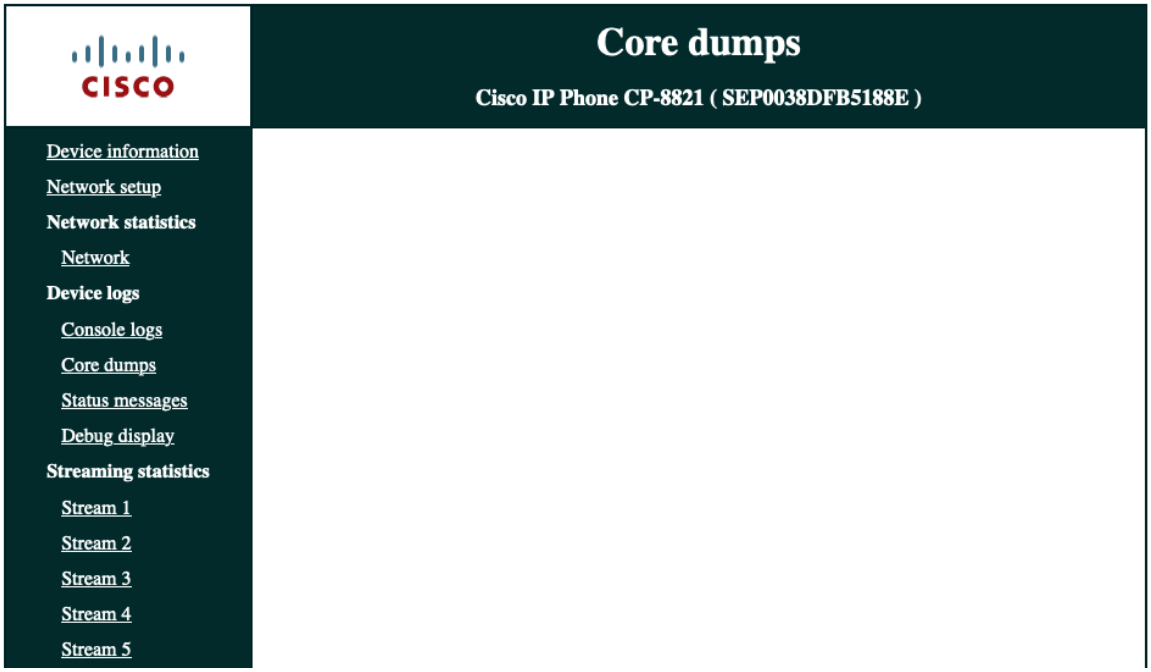
PRT collection complete will be displayed when the PRT log collection has completed and the file is available for download.

The PRT log will remain (even if the phone is rebooted) until the PRT log collection process is invoked again.



Core Dumps

Browse to the standard web interface (https://x.x.x.x) of the Cisco Wireless IP Phone 8821 or 8821-EX then select **Core dumps** to view this information.

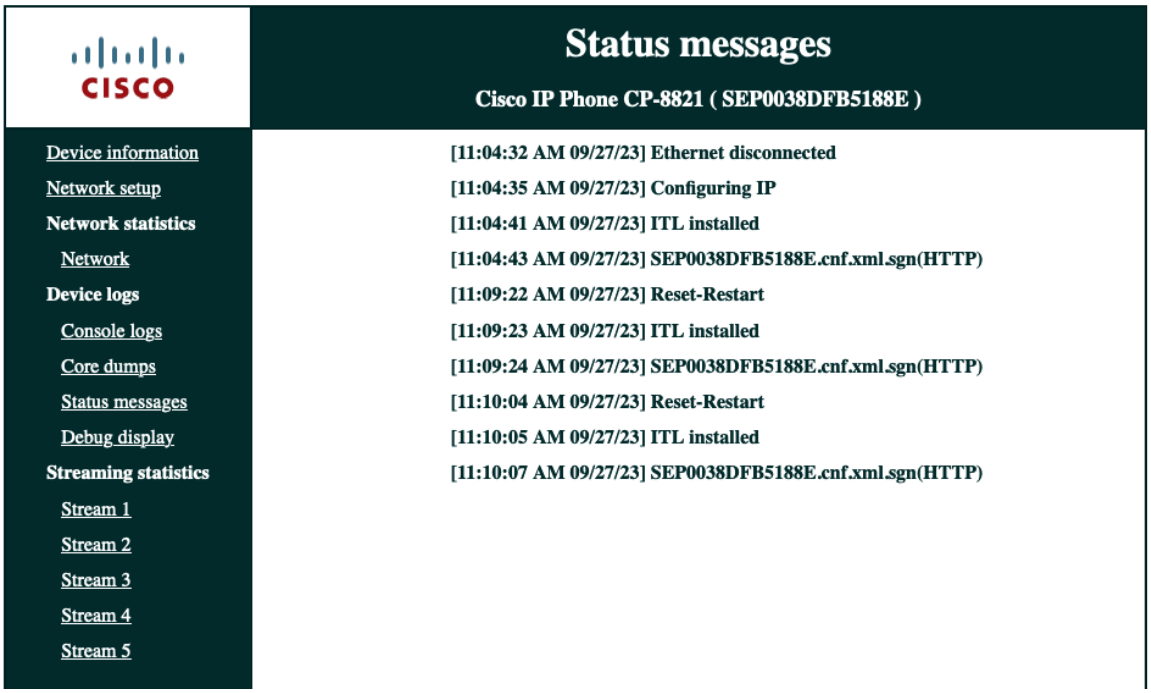


The 11.0(5) release enables the capability to generate or delete a Java core dump log via the admin webpage (https://x.x.x.x:8443) at **Device logs** > **Core dumps**.

The Java core dump log will remain until the phone is rebooted or the Java core dump log collection process is invoked again.

Status Messages

Browse to the standard web interface (https://x.x.x.x) of the Cisco Wireless IP Phone 8821 or 8821-EX then select **Status messages** to view this information.

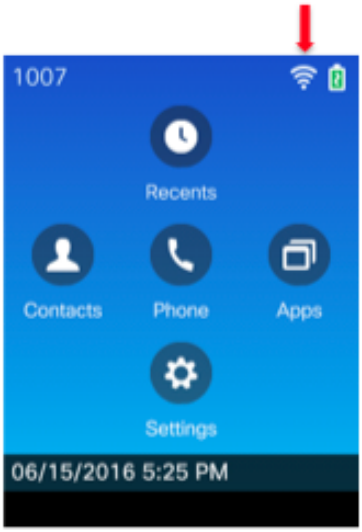


Debug Display

Browse to the standard web interface (https://x.x.x.x) of the Cisco Wireless IP Phone 8821 or 8821-EX then select **Debug display** to view this information.

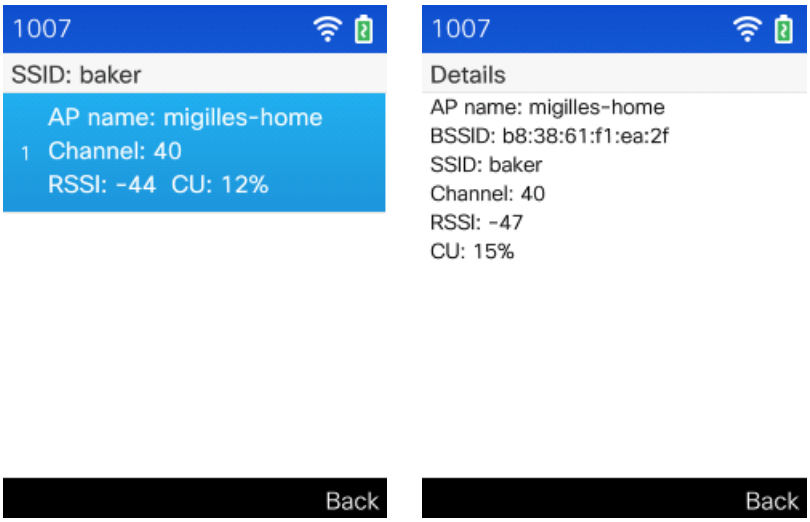
WLAN Signal Indicator

The WLAN signal indicator is displayed in the upper right hand corner of the main screen when the Cisco Wireless IP Phone 8821 and 8821-EX are connected to an access point.



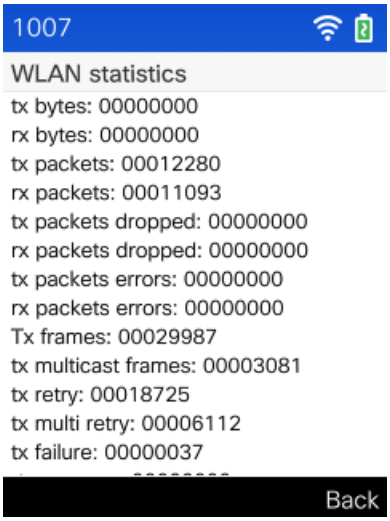
Neighbor List

Current access point and neighbor access point details can be viewed by selecting **Settings > Admin settings > Neighbor list**. AP name, BSSID, SSID, Channel, RSSI, and CU (Channel Utilization) information will be displayed.



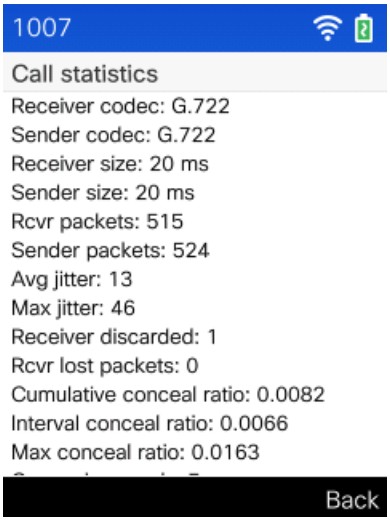
WLAN Statistics

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



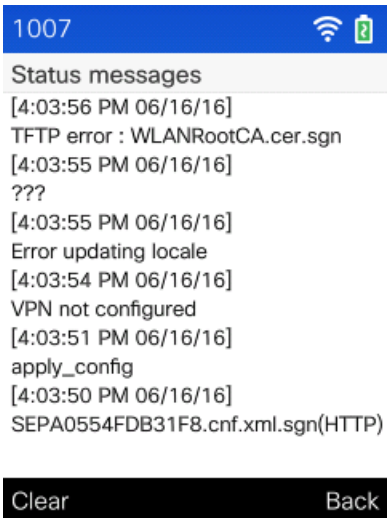
Call Statistics

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



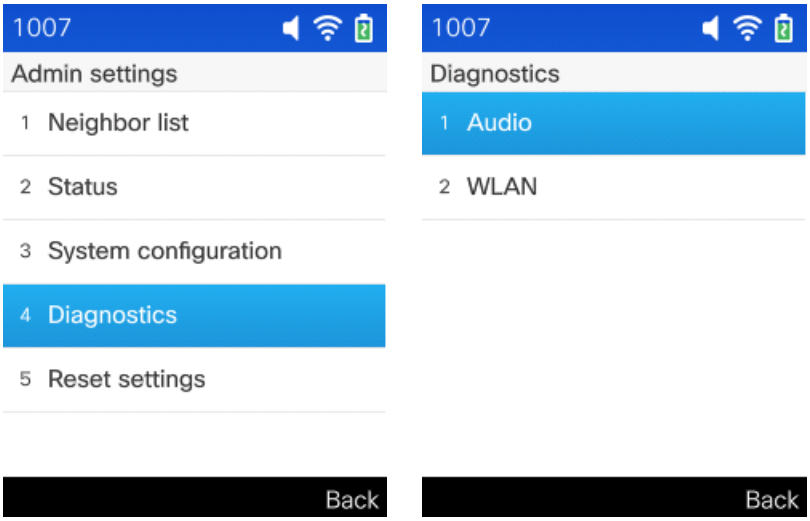
Status Messages

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



Diagnostics

Audio and WLAN Diagnostics are integrated tools which can be utilized to help troubleshoot various issues.

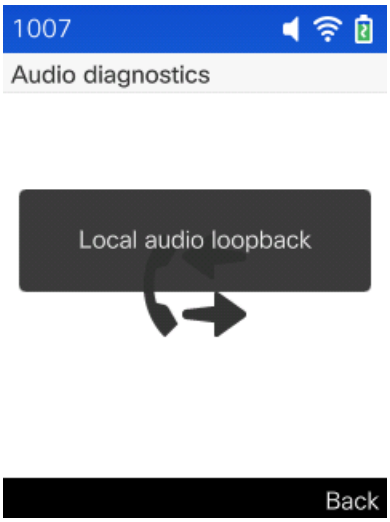


Audio Diagnostics

Audio Diagnostics can help triage audio hardware components (microphone, handset speaker, handsfree speaker) when selecting **Settings** > **Admin settings** > **Diagnostics** > **Audio**.

Once selected, then can speak into the microphone, where the audio will then be played to the handsfree speaker by default.

Press the audio path button (right side of the phone) to toggle the audio output between the handsfree speaker and handset speaker.



WLAN Diagnostics

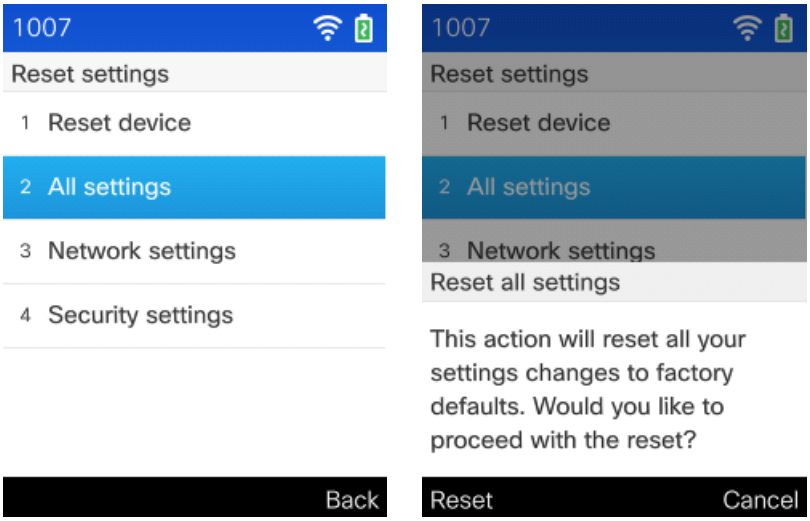
WLAN Diagnostics can display details for each access point that matches a configured Wi-Fi Profile when selecting **Settings** > **Admin settings** > **Diagnostics** > **WLAN**.

AP name, BSSID, SSID, Frequency, Current channel, Last RSSI, Beacon Interval, Data rate, DTIM, Country code, Channel, Power constraint, Power limit, CU, Station count, Admission capacity, WMM, UAPSD, Proxy ARP, CCX, and Access category information will be displayed.

Restoring Factory Defaults

The configuration of the Cisco Wireless IP Phone 8821 and 8821-EX can be reset to factory defaults by selecting **Applications > Admin settings > Reset settings > All settings**.

A confirmation screen will appear where **Reset** must be selected to proceed with the factory data reset.



If the Cisco Wireless IP Phone 8821 or 8821-EX is not able to boot properly, a factory reset can also be initiated via the following procedure:

- Turn the phone off by pressing the **Red** button.
- Press and hold the **#** key, then power on the phone via the **Red** button.
- Keep the **Red** button and the **#** key held down until the LED changes to **Amber**.
- Once the LED changes to **Amber**, release the **Red** button and the **#** key.
- Then press **1 2 3 4 5 6 7 8 9 * 0 #**.
- The LED will blink **Green** to indicate the factory reset sequence has been accepted; otherwise will blink **Red** to indicate factory reset has not been accepted.
- The Cisco Wireless IP Phone 8821 or 8821-EX will then continue the normal boot process and have the factory settings restored.

To boot the alternate image, perform the following procedure.

- Turn the phone off by pressing the **Red** button.
- Press and hold the ***** key, then power on the phone via the **Red** button.
- Keep the **Red** button and the ***** key held down until the LED changes to **Red**.
- Once the LED changes to **Red**, release the **Red** button and the ***** key.
- The Cisco Wireless IP Phone 8821 or 8821-EX will then boot using the alternate image.

Note: Prior to attempting to boot the alternate image, ensure the phone load specified in Cisco Unified Communications Manager for that individual phone matches the alternate image name; otherwise the phone may simply re-apply the previous load once it connects to Cisco Unified Communications Manager.

Capturing a Screenshot of the Phone Display

The current display of the Cisco Wireless IP Phone 8821 or 8821-EX can be captured by browsing to http://x.x.x.x/CGI/Screenshot, where **x.x.x.x** is the IP address of the Cisco Wireless IP Phone 8821 or 8821-EX. At the prompt enter the username and password for the account that the Cisco Wireless IP Phone 8821 or 8821-EX is associated to in Cisco Unified Communications Manager.

Additional Documentation

Cisco Wireless IP Phone 8821 and 8821-EX Data Sheets

https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/wireless-ip-phone-8821/datasheet-c78-737346.html

https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/wireless-ip-phone-8821-ex/datasheet-c78-737347.html

Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-maintenance-guides-list.html

Cisco Wireless IP Phone 8821 and 8821-EX User Guide

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html

Cisco Wireless IP Phone 8821 and 8821-EX Quick Start Guide

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html

Cisco Wireless IP Phone 8821 Series Accessory Guide

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html

Cisco Wireless IP Phone 8821 Series Release Notes

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html

Cisco Wireless IP Phone 8821 Series Software

https://software.cisco.com/download/home/284729655

Cisco Unified Communications Manager

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/series.html

Cisco Unified Communications Manager Express

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/series.html

Cisco Voice Software

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

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 IP Phone 8821 and 8821-EX 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, Cisco 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.

© 2023 Cisco Systems, All rights reserved.